



Présentations d'opérades et systèmes de réécriture

Yves Guiraud

► To cite this version:

Yves Guiraud. Présentations d'opérades et systèmes de réécriture. Autre [cs.OH]. Université Montpellier II - Sciences et Techniques du Languedoc, 2004. Français. tel-00006863

HAL Id: tel-00006863

<https://tel.archives-ouvertes.fr/tel-00006863>

Submitted on 10 Sep 2004

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Présentations d'opérades et systèmes de réécriture

Yves Guiraud

Institut de Mathématiques et de Modélisation de Montpellier

UMR CNRS 5149

Université Montpellier II

`guiraud@math.univ-montp2.fr`

17 mai 2004

Table des matières

Aperçu	7
Introduction	9
Qu'est-ce que la réécriture ?	9
Quelques exemples de systèmes de réécriture	11
La réécriture de mots	11
Les réseaux de Petri	12
La réécriture de termes	14
Le λ -calcul	15
Élimination et bases de Gröbner	16
La réécriture topologique : les mouvements de Reidemeister	16
Catégorification et réécriture	18
Catégorifions encore	19
Organisation	20
1 Relations binaires ou systèmes de réécriture abstraits	23
1.1 Définitions	23
1.2 Principaux critères de terminaison et de confluence	29
1.3 Comparaison de systèmes de réécriture	33
1.4 Réécriture abstraite et langage des catégories	34
2 Présentations de monoïdes ou systèmes de réécriture de mots	37
2.1 La catégorie des monoïdes et le foncteur monoïde libre	37
2.2 Modules, idéaux et relations de réduction sur un monoïde	40
2.3 Contextes sur un monoïde	43
2.4 Présentation d'un monoïde et problème de mots	46
2.5 Problème de mots et réécriture	49
2.6 Terminaison et ordres de réduction	50
2.7 Confluence et paires critiques	53
2.7.1 La présentation classique	54
2.7.2 Une approche algébrique des paires critiques	58

2.8	Procédures de complétion pour les présentation de monoïdes	61
2.8.1	La procédure basique	61
2.8.2	Limitations de la procédure basique	63
2.8.3	Procédures de complétion abstraites et preuves	65
3	Présentations d'opérades	69
3.1	Des mots aux opérateurs	70
3.1.1	Discussion	75
3.2	Opérades libres et quotients	78
3.2.1	Présentation d'une petite catégorie par graphe et relations	78
3.2.2	Opérade librement engendrée par une signature	79
3.2.3	Limites et colimites dans les catégories des signatures et des opérades	83
3.2.4	Opérade quotient.	86
3.3	Présentations d'opérades	92
3.3.1	Modules sur une opérade	92
3.3.2	Idéal engendré par une famille de relations	94
3.4	Contextes et construction alternative de l'idéal engendré par des relations .	95
3.4.1	Module libre engendré par une signature	96
3.4.2	Contextes sur une opérade	98
3.5	Retour aux présentations de monoïdes	100
3.6	Présentation d'une opérade et problème de mots	101
3.7	Terminaison d'une présentation d'opérade	102
3.7.1	Ordres de réduction sur une opérade	103
3.7.2	Une technique classique d'interprétation en réécriture de termes . .	104
3.7.3	Un rapide aperçu de la technique améliorée	105
3.7.4	L'opérade $\mathcal{O}(X, Y, M)$	106
3.7.5	Un ordre de réduction sur $\mathcal{O}(X, Y, M)$	111
3.7.6	Le résultat	113
3.7.7	Un premier exemple : la présentation $L(\mathbb{Z}_2)$	114
3.8	Confluence locale d'une présentation d'opérade	122
3.8.1	Paires critiques d'une présentation d'opérade	122
3.8.2	Calcul des paires critiques	125
3.9	Structures de données pour les opérades libres	127
3.9.1	Première structure	128
3.9.2	Deuxième structure	129
4	Présentations de monoïdes commutatifs ou réseaux de Petri	137
4.1	Une description succincte des réseaux de Petri	137
4.2	Un survol des présentations de monoïdes commutatifs	139
4.3	Les réseaux de Petri sont des présentations de monoïdes commutatifs . . .	142
4.4	Présentation d'opérade associée à une présentation de monoïde commutatif	144

4.5	Un ordre de réduction particulier	146
5	Réécriture de termes et présentations d'opérades	149
5.1	Systèmes de réécriture de termes	149
5.1.1	Termes et règles de réécriture	149
5.1.2	Contextes, substitutions et relations de réduction	150
5.1.3	Ordres de réduction sur un ensemble de termes	152
5.2	Interprétation algébrique des termes	153
5.2.1	Algèbre sur une opérade	153
5.2.2	L'ensemble des termes vu comme une algèbre	156
5.2.3	Règles linéaires à gauche et uniformisation	157
5.3	Opérades cartésiennes et signatures algébriques	159
5.3.1	Opérades cartésiennes : définition et exemple fondamental	159
5.3.2	Opérade cartésienne libre engendrée par une signature algébrique	165
5.3.3	Une présentation convergente de l'opérade cartésienne libre	168
5.3.4	Terminaison de $(\Sigma^c, R_{\Delta, \Sigma})$	171
5.3.5	Confluence de $(\Sigma^c, R_{\Delta, \Sigma})$	179
5.4	Une autre version de l'opérade cartésienne libre engendrée par une signature algébrique	219
5.4.1	Construction de $\mathbb{T}\Sigma$	219
5.4.2	L'opérade cartésienne $\mathbb{T}\Sigma$ est librement engendrée par Σ	224
5.5	Liens entre un système de réécriture de termes et sa présentation associée	227
5.5.1	Simulation des étapes de réduction	227
5.5.2	Terminaison	230
5.5.3	Confluence	237
5.6	Et les systèmes non linéaires à gauche ?	238
5.6.1	Réécriture de termes modulo commutativité	238
5.6.2	Le cas des systèmes non linéaires	240
6	Vers une présentation diagrammatique du λ-calcul ?	243
6.1	Le λ -calcul	243
6.1.1	Ensemble des λ -termes formels	243
6.1.2	Ensemble des λ -contextes	245
6.1.3	Relation d' α -conversion et λ -termes	246
6.1.4	Les deux règles de réécriture du λ -calcul	248
6.2	Le premier modèle : la logique combinatoire	249
6.3	D'autres termes : les calculs de substitutions explicites	251
6.4	Troisième voie : divers calculs graphiques	254
6.4.1	Le calcul de Lamping	254
6.4.2	Les réseaux d'interaction	254
6.4.3	Les réseaux de preuves	255

6.5	Une présentation d'opérades associée au λ -calcul?	256
6.5.1	Une opérade souveraine pour le λ -calcul linéaire	256
6.5.2	Un premier problème : les flèches inutiles	260
6.5.3	Le problème majeur : l'extension au λ -calcul	261
6.6	Vers une dimension supérieure	265
A	Opérades et autres structures de l'algèbre universelle	267
A.1	Opérades et opérades classiques	267
A.2	Opérades, PRO et PROP	269
A.3	Opérades et théories algébriques	271
B	Présentation du C-monoïde initial et λ-calcul avec substitutions explicites	275
B.1	La structure de C -monoïde	276
B.2	Le système de réécriture \mathbb{K}	276
B.2.1	Signature et règles de réécriture de \mathbb{K}	276
B.2.2	La relation K_0 termine	278
B.2.3	La relation K termine	279
B.2.4	La relation K est confluente	283
B.2.5	La relation KB est confluente	288
B.3	Définition du déliement	295
B.3.1	Définition du déliement sur les λ -termes formels	295
B.3.2	Définition du déliement sur les λ -contextes	297
B.4	Le système de réécriture \mathbb{K} ne simule pas complètement le λ -calcul	300
B.4.1	Le déliement est compatible avec l' α -conversion	300
B.4.2	Le déliement préserve les étapes de β -réduction	304
B.4.3	Le déliement préserve seulement la β -normalisation	310
	Bibliographie	313

Aperçu

Ce travail a pour objectif premier d'introduire la notion de présentation d'opérade comme cadre formel pour la réécriture sur des objets de dimension 2, c'est-à-dire possédant deux lois de composition, l'une horizontale, l'autre verticale.

Nous étudions la catégorie des opérades, dans une version généralisée, ainsi que les ingrédients essentiels permettant de calculer à l'aide de tels objets. En particulier, le théorème 3.17 donne une technique d'interprétation pour prouver la terminaison de présentations d'opérades. Ce résultat nous permet d'obtenir le théorème 3.18 qui démontre la conjecture de Yves Lafont concernant la terminaison de sa présentation de $L(\mathbb{Z}_2)$. En conséquence, on en déduit le théorème 5.47, qui assure la convergence de $L(\mathbb{Z}_2)$ et donne ainsi la première présentation convergente d'opérade pour une théorie équationnelle commutative.

Ces systèmes de calcul possèdent de forts liens avec les systèmes de réécriture plus classiques : les théorèmes 3.11 et 4.5 montrent que les présentations d'opérades généralisent les présentations de monoïdes, ou systèmes de réécriture de mots, et les présentations de monoïdes commutatifs, ou réseaux de Petri ; le théorème 5.40 prouve que l'on peut associer, à tout système de réécriture de termes linéaire à gauche, une présentation d'opérade qui le simule, c'est-à-dire qui le contient et rend explicites les opérations de gestion des ressources, duplication et effacement, sans changer ses propriétés de terminaison et de confluence.

Enfin, les présentations d'opérades sont confrontées à une limitation, la simulation du λ -calcul, qu'elles ne semblent pas pouvoir réaliser sans passer encore en dimension supérieure.

Introduction

Qu'est-ce que la réécriture ?

La réécriture est à la fois une méthode de calcul effectif et un modèle pour les systèmes à évolutions discrètes et locales. On peut la voir apparaître à de nombreux endroits, mais l'arithmétique élémentaire reste le thème le plus classique pour une introduction.

En effet, l'addition d'entiers naturels fournit un bon exemple de la nécessité de passer de l'égalité au calcul. Considérons :

$$2 + 2 = 4.$$

Bien que cette équation soit, parfois encore, contestée par quelques iconoclastes, tels Alphonse Allais, [All89], ou Houston Euler, [Eul98], elle est, de nos jours, généralement admise. En revanche, il est moins connu que :

$$1 + 37 + 152 + 17 + 23 + 65 + 41 + 21 + 87 + 99 + 55 + 875 + 7 + 56 + 102 = 1638.$$

À moins que ce ne soit 1622 ? Le manque de réponse immédiate montre que, dans ce cas, on est plutôt enclin à dire que la partie droite de l'équation est le *résultat* d'un calcul effectué à partir de la partie gauche.

Le fait est que, pour la première équation, le cerveau humain fait immédiatement le calcul ou, mieux encore, reconnaît un graphisme connu : ainsi, on oublie qu'il peut exister un calcul partant de $2 + 2$ et donnant 4. En revanche, dans le second cas, on est obligé de recourir à l'utilisation d'instruments de calculs, comme un papier et un stylo ou, plus moderne, une machine, qu'elle soit à calculer ou encore un ordinateur.

Pour un tel automate, les deux cas sont similaires : les parties gauches des égalités sont ce que l'utilisateur lui donne comme valeurs en entrée, les parties droites, ce que la machine répond comme résultat. On préfère alors remplacer l'égalité par un autre symbole, non symétrique, pour traduire cette différence de statut. Ainsi, on écrit $2 + 2 \rightarrow 4$ plutôt que $2 + 2 = 4$, pour montrer le *sens* du calcul et, souvent, son caractère irréversible ; on

parle alors de *réductions* plutôt que d'égalités.

Les deux parties de ces réductions ne sont pas exprimées dans le même langage : les données sont des sommes formelles d'entiers, c'est-à-dire des suites finies d'entiers séparés par des symboles $+$, les résultats sont des entiers. Les sommes formelles sont les *termes* du calcul, construits à partir d'éléments atomiques ou *générateurs*, les entiers, selon une certaine grammaire ou *structure* : si u et v sont deux termes, alors $u + v$ est un terme.

En réalité, le langage des résultats est contenu dans celui des entrées : en effet, on peut très bien donner 2 comme entrée à la machine. Dans ce dernier cas, elle répondra d'ailleurs 2 : la machine ne sait pas faire d'opération sur 2, on dit que c'est une *forme normale* ou *irréductible* du calcul. Le but de notre machine est donc de transformer tout élément de son langage (toute somme formelle d'entiers) en une forme irréductible (un entier), de sorte que les règles élémentaires de l'arithmétique soient vérifiées : on désire que le résultat obtenu soit effectivement la somme des entiers qui lui ont été donnés.

Cette dernière exigence dépend ensuite de la manière dont la machine effectue les calculs. Étant donné qu'il serait déraisonnable d'espérer entrer dans sa mémoire le résultat de toutes les additions possibles de n'importe quel nombre d'entiers, on est obligé de trouver des étapes dans le calcul qui, mises bout à bout, donneront le résultat escompté.

Par exemple, on peut supposer que la machine effectue, à chaque fois, la somme des deux premiers entiers de la liste : $1 + 37 \rightarrow 38$, puis $38 + 152 \rightarrow 190$, etc. À chaque fois, on obtient le résultat de l'opération en remplaçant, dans le terme, le membre de gauche de la réduction par le membre de droite, sans modifier le reste du terme. Ainsi, les applications successives de $1 + 37 \rightarrow 38$ puis de $38 + 152 \rightarrow 190$ donnent :

$$\begin{array}{ll} 1 + 37 + 152 & +17 + 23 + 65 + 41 + 21 + 87 + 99 + 55 + 875 + 7 + 56 + 102 \\ \rightarrow & 38 + 152 \quad +17 + 23 + 65 + 41 + 21 + 87 + 99 + 55 + 875 + 7 + 56 + 102 \\ \rightarrow & 190 \quad +17 + 23 + 65 + 41 + 21 + 87 + 99 + 55 + 875 + 7 + 56 + 102. \end{array}$$

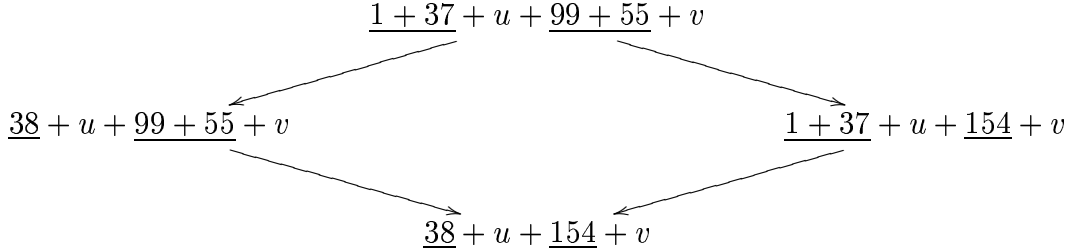
Avec ces spécifications, le nombre d'entiers dans la somme diminue de 1 à chaque opération ; on est donc assuré qu'après un nombre fini de telles additions, on aura notre résultat : on dit que le calcul *termine*, c'est-à-dire qu'il n'existe aucune somme formelle d'entiers à partir de laquelle on peut enchaîner une infinité de calculs élémentaires.

On peut éventuellement être moins directif et dire que chaque étape de calcul consiste en l'addition de deux entiers adjacents de la liste, quels qu'ils soient. Ainsi, lorsque l'on a plus de deux entiers à additionner, on a un choix à faire : est-ce que l'on commence par $1 + 37 \rightarrow 38$ ou par $99 + 55 \rightarrow 154$? Ce choix n'a aucune conséquence sur le résultat final,

car l'addition des entiers est associative :

$$(m + n) + p = m + (n + p).$$

On peut le voir sous la forme d'un *graphe de réduction* :



avec :

$$\begin{cases} u = 152 + 17 + 23 + 65 + 41 + 21 + 87 \\ v = 875 + 7 + 56 + 102. \end{cases}$$

On dit que le calcul que l'on a spécifié est *confluent* : les choix effectués au cours du calcul n'ont pas d'incidence sur le résultat final.

On a ainsi exhibé les principales notions de la réécriture, à savoir que l'on s'intéresse à des systèmes permettant de calculer des formes normales à partir de termes, selon des *règles* de calcul local ou de réécriture. L'une des principales activités est alors de montrer que le calcul est *convergent*, c'est-à-dire à la fois qu'il termine et qu'il est confluent. Le chapitre 1 est dédié à des définitions et des résultats fondamentaux concernant la réécriture, dans toute sa généralité.

Quelques exemples de systèmes de réécriture

Nous allons voir, de manière succincte, quelques exemples de systèmes de réécriture classiques.

La réécriture de mots

Les systèmes de réécriture de mots forment l'exemple le plus simple et le plus classique de systèmes de réécriture. Les générateurs sont les lettres d'un alphabet X et les termes sont tous les mots que l'on peut former avec ces lettres. Les règles sont de la forme $u \rightarrow v$, où u et v sont des mots. Une telle règle peut s'appliquer à un mot a dès que a contient u comme sous-mot ; le résultat est, dans ce cas, le mot b , obtenu en remplaçant, dans a , le sous-mot u par v .

Par exemple, si X contient deux lettres, x et y , les termes peuvent être x , xy , yy , $xxxxy$, $xyyyx$, etc. Si l'on se donne une seule règle, $yx \rightarrow xy$, on obtient un calcul qui, dans tous les mots, va progressivement ranger tous les x à gauche et les y à droite. Par exemple, on donne toutes les réductions possibles à partir de $xyxyx$:

$$\begin{array}{ccc} xyxyx & \longrightarrow & xxxyyx \\ \downarrow & & \downarrow \\ xyxxy & \longrightarrow & xxxyxy \longrightarrow xxxxyy. \end{array}$$

Le calcul est, ici, convergent, mais c'est loin d'être toujours le cas. Nous étudierons, au chapitre 2, les systèmes de réécriture de mots ou *présentations de monoïdes*. On pourra consulter [BO93] pour une référence complète.

Les réseaux de Petri

Les réseaux de Petri sont le premier exemple de réécriture graphique. *A priori*, ils semblent relativement différents de ce qui a été présenté jusqu'alors, car les termes n'ont pas de structure apparente. Mais nous verrons, au chapitre 4, qu'ils s'insèrent au contraire parfaitement bien dans ce qui a été exposé jusqu'ici.

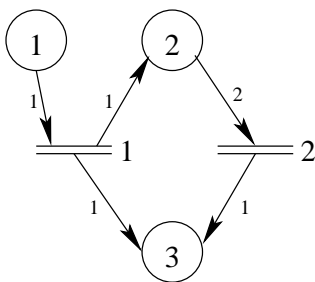


FIG. 1 – Un réseau de Petri.

Comme le montre la figure 1, un réseau de Petri est un graphe possédant des sommets de deux types : des places (les ronds) et des transitions (les doubles barres). Chaque arête possède, de plus, un entier qui lui est attaché, son poids.

Le réseau possède des états, matérialisés par des jetons disposés dans les places, et ses évolutions se font, au coup par coup, en activant une transition. Ceci se déroule de la manière suivante :

- pour chaque place d'où part une flèche arrivant sur la transition choisie, on retire autant de jetons que l'entier associé à cette flèche (on ne peut activer la transition que s'il y a suffisamment de jetons) ;

- pour chaque place où arrive une flèche qui part de la transition choisie, on rajoute autant de jetons que l'entier associé à cette flèche.

La figure 2 montre les évolutions possibles d'un réseau de Petri à partir d'un état donné. On pourra se référer à [Mur89] pour une introduction détaillée aux réseaux de Petri, à leurs diverses variantes ainsi qu'à divers problèmes de décision qui se posent lors de leur étude.

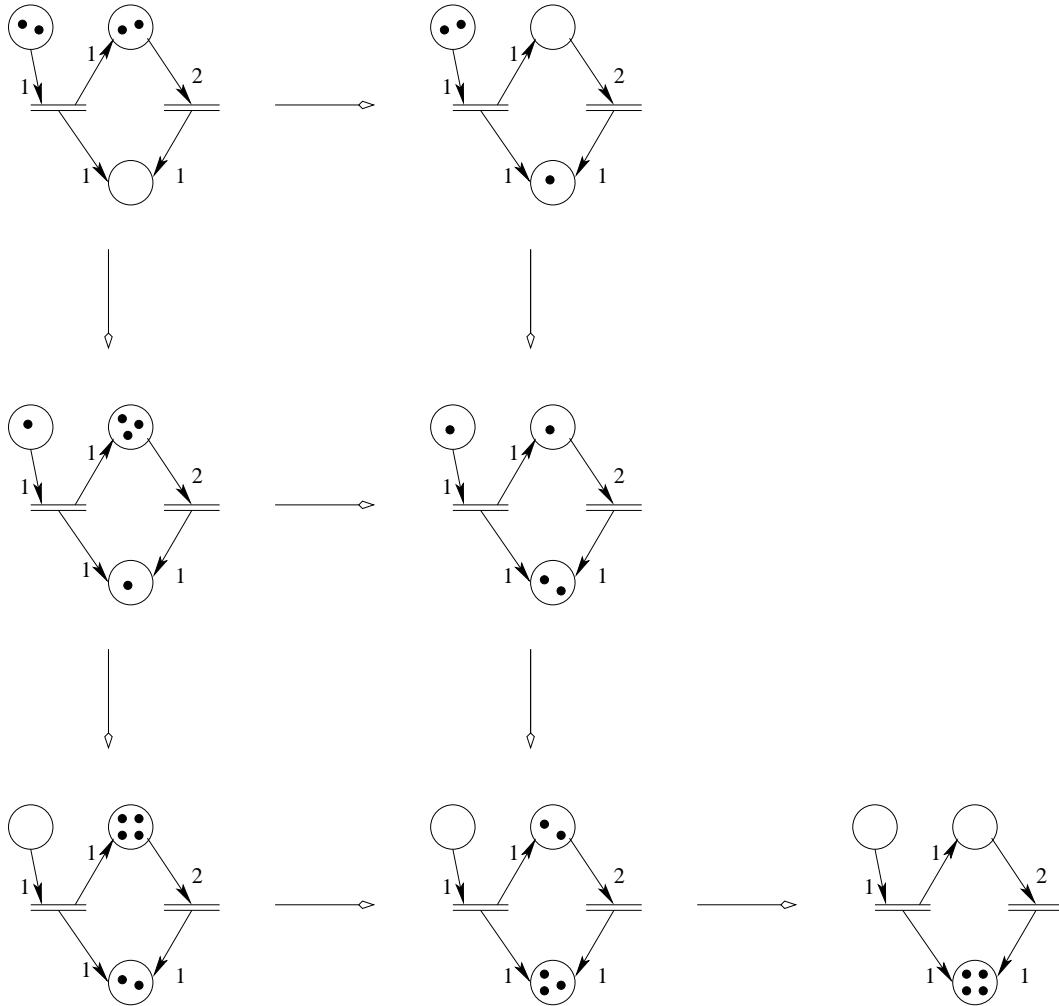


FIG. 2 – Les évolutions possibles d'un état du réseau.

La réécriture de termes

Ce domaine est l'un des sujets majeurs de la réécriture. On spécifie les termes à l'aide de constructeurs, qui sont des applications abstraites avec un certain nombre d'entrées, ainsi que des variables. Par exemple, si A est un constructeur avec 2 entrées, S en est un autre, avec 1 entrée, et Z un dernier, avec 0 entrée, on construit des termes comme x , $A(x, y)$, $A(S(x), x)$, $S(S(y))$ et $S(A(z, x))$, avec x et y des variables.

Les règles sont des couples de termes soumis à certaines restrictions dont, notamment, le fait que les variables apparaissant dans le terme de droite doivent être dans celui de gauche. Par exemple, $A(x, S(y)) \rightarrow S(A(x, y))$ et $A(x, Z) \rightarrow x$ sont des règles valides.

Nous allons seulement esquisser ici le processus d'application des règles ; le chapitre 5 contient des définitions formelles, que l'on pourra trouver détaillées dans [BN98]. En ce qui concerne notre exemple, la première règle peut s'appliquer à un terme u s'il contient, dans son écriture, un sous-terme de la forme $A(v, S(w))$, où v et w sont des termes.

Cet exemple de système de réécriture de termes permet d'ailleurs, une fois complété, d'effectuer l'addition des entiers. De plus, il est utilisable en pratique, contrairement à la procédure décrite au début de cette introduction : en effet, on en était resté à devoir disposer d'une machine qui connaît, d'avance, le résultat de l'addition de tout couple d'entiers. Ce n'est pas possible avec une machine concrète, c'est-à-dire ne disposant que d'une mémoire finie. On va donc préférer *coder* les entiers de telle sorte que l'on puisse *calculer* toute somme de deux entiers.

Ici, on utilise le codage suivant : Z désigne l'entier 0, $S(Z)$ l'entier 1, $S^2(Z) = S(S(Z))$ l'entier 2, etc. Le constructeur A est là pour coder la somme formelle de deux entiers. Donnons, à titre d'exemple, l'ensemble des règles du système :

$$\begin{aligned} A(x, Z) &\rightarrow x \\ A(x, A(y, z)) &\rightarrow A(A(x, y), z) \\ A(x, S(y)) &\rightarrow S(A(x, y)). \end{aligned}$$

La première règle dit que $n + 0 = n$, la seconde que $m + (n + p) = (m + n) + p$ et la dernière que $m + (n + 1) = (m + n) + 1$. Notons que la commutativité de l'addition, $m + n = n + m$, n'est pas forcément vraie sur tous les termes ; par contre, elle l'est sur les termes qui correspondent à des entiers : pour tous m et n , on aura bien $A(S^m(Z), S^n(Z))$ et $A(S^n(Z), S^m(Z))$ qui se réduisent tous deux en $S^{m+n}(Z)$.

Vérifions tout de même que ce système donne $2 + 2 = 4$ et non 5 :

$$\begin{aligned} A(S^2(Z), S^2(Z)) &\rightarrow S(A(S^2(Z), S(Z))) \\ &\rightarrow S^2(A(S^2(Z), Z)) \\ &\rightarrow S^2(S^2(Z)) = S^4(Z). \end{aligned}$$

Le λ -calcul

Le λ -calcul est, historiquement, un des premiers systèmes de réécriture et, certainement, le plus célèbre. Il fut créé par Alonzo Church en 1936, voir [Chu41], et décrit l'application de fonctions explicites.

Cependant, il est d'une nature algébrique extrêmement complexe, surtout dans sa version d'origine, non typée. À première vue, les λ -termes sont construits de manière similaire à des termes classiques : on a deux constructeurs λ et μ , et les λ -termes sont définis, formellement, de manière inductive, en disant que :

- toute variable est un λ -terme ;
- si x est une variable et f est un λ -terme, alors $\lambda(x, f)$ est un λ -terme, noté $\lambda x.f$;
- si f et g sont des λ -termes, alors $\mu(f, g)$ est un λ -terme, noté fg .

Le λ -terme fg désigne l'application formelle d'une fonction f à un argument g , avant toute évaluation, tandis que $\lambda x.f$ désigne l'abstraction de f selon x , c'est-à-dire la fonction qui à tout argument g associe le λ -terme $f[x := g]$, obtenu en remplaçant (presque¹) tous les x de f par g , un peu à la manière d'une fonction polynôme.

La première difficulté vient du fait que x est une variable liée ou muette dans $\lambda x.f$, comme on en trouve dans une somme, une intégrale, un quantificateur \forall ou \exists ou, encore, une fonction polynôme ; on pourra consulter [Bou39] pour de plus amples informations sur ces notions. Résumons en disant que l'on peut remplacer la variable muette x par (presque) toute autre variable y , sans changer le terme ; on appelle α -conversion cette opération.

Le λ -calcul possède deux règles, appelées respectivement β -réduction et η -réduction :

$$\begin{aligned} (\lambda x.f)g &\rightarrow_{\beta} f[x := g] \\ \lambda x.(fx) &\rightarrow_{\eta} f \quad \text{si } f \text{ ne contient pas la variable } x. \end{aligned}$$

Nous reparlerons plus formellement du λ -calcul au chapitre 6. On pourra se référer à [Bar84] pour plus de détails.

¹Les limitations seront expliquées au chapitre 6 ; leur exposé est trop technique et n'est pas nécessaire ici.

Élimination et bases de Gröbner

Les bases de Gröbner permettent de spécifier des calculs convergents sur des anneaux de polynômes. On pourra se référer à [Buc79] pour un complément d'information.

Si k est un corps commutatif et X une famille finie d'indéterminées, on note $k[X]$ l'anneau des polynômes correspondant. Toute famille $F = (f_1, \dots, f_m)$ de polynômes engendre un idéal, noté (F) et défini comme l'ensemble des sommes :

$$\sum_{i=1}^n \lambda_i \cdot p_i \cdot f_i,$$

avec les λ_i dans k et les p_i dans $k[X]$. Si l'on veut résoudre le problème de l'appartenance à (F) , c'est-à-dire de savoir décider si un polynôme donné f est dans (F) ou non, on crée un calcul à partir de F ; pour l'idée, on pose $f \rightarrow_F g$ si g est obtenu à partir de f ainsi, pour un certain i :

- $f = f' + \lambda \cdot p \cdot T(f_i)$, où $T(f_i)$ est le plus grand monôme de f_i pour un ordre bien choisi ;
- $g = f - \lambda \cdot C(f_i)^{-1} \cdot p \cdot f_i$, où $C(f_i)$ est le coefficient de $T(f_i)$ dans f_i .

On procède donc par élimination successive des polynômes de F dans f : cette procédure ressemble beaucoup à un pivot de Gauss.

Si f se réduit à 0 par ce calcul, on est sûr que $f \in (F)$. Malheureusement, la réciproque n'est pas vraie en général ; autrement dit, le calcul \rightarrow_F n'est pas toujours confluent (en revanche, il termine toujours) : il est possible que $f \in (F)$ mais que, selon les choix effectués au cours du calcul, on obtienne à la fin une forme normale distincte de 0.

C'est le principal intérêt des bases de Gröbner : le calcul \rightarrow_F est confluent (et donc convergent) si et seulement si F est une base de Gröbner.

La réécriture topologique : les mouvements de Reidemeister

Jusqu'à présent, nous n'avons montré que des exemples de systèmes de réécriture syntaxiques ; même les réseaux de Petri, qui paraissent différents, sont de tels systèmes déguisés, voir chapitre 4. Or, la topologie fournit un exemple majeur de réécriture non syntaxique : les mouvements de Reidemeister sur les nœuds et entrelacs.

Rappelons qu'un entrelacs est une famille de boucles qui s'enchevêtrent éventuellement, le tout vu dans l'espace euclidien à 3 dimensions. On les représente souvent, par commodité, comme des boucles dans le plan, avec une indication supplémentaire pour

chaque croisement de deux brins : quel brin passe au-dessus de l'autre.

Cependant, chaque entrelacs possède plusieurs représentations de ce type. On définit une relation d'équivalence permettant d'identifier les diagrammes qui représentent le même entrelacs : cette relation \equiv est engendrée par trois familles de relations locales bien connues, les mouvements de Reidemeister, montrés dans la figure 3. La figure 4 montre une suite d'équivalences engendrées par ces mouvements, permettant de prouver qu'un diagramme représente l'entrelacs trivial à une composante (une boucle sans nœud).

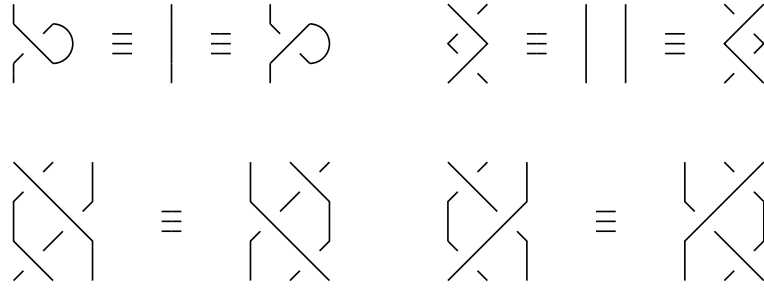


FIG. 3 – Les trois types de mouvements de Reidemeister.

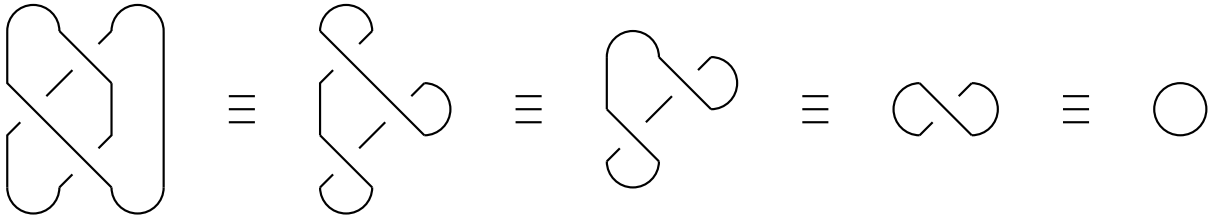


FIG. 4 – Équivalences de diagrammes d'entrelacs.

Une des questions fondamentales qui se posent est de résoudre le problème suivant : étant donnés deux diagrammes D et D' d'entrelacs, a-t-on $D \equiv D'$ ou non ? C'est-à-dire est-ce que D et D' représentent le même entrelacs ou non ?

Cette question n'est que partiellement résolue : on sait construire des objets algébriques $P(D)$ et $P(D')$, en général des polynômes, tels que, si D et D' représentent le même entrelacs, c'est-à-dire si $D \equiv D'$, alors $P(D) = P(D')$. En pratique, on utilise plutôt la réciproque : on calcule $P(D)$ et $P(D')$: si $P(D) \neq P(D')$, on est sûr que D et D' ne représentent pas le même entrelacs ; sinon, on ne peut rien dire.

La recherche d'un invariant complet, c'est-à-dire vérifiant $P(D) = P(D')$ si et seulement si $D \equiv D'$, est toujours en cours. Notons que cet invariant pourrait venir de la réécriture : si on trouve une présentation convergente équivalente aux mouvements de Reidemeister, l'application qui associerait à chaque diagramme son unique forme normale serait un invariant complet. Cependant, il est fort possible qu'une telle présentation n'existe pas. On consultera [Ada94] pour plus de détails sur les nœuds et entrelacs.

Catégorification et réécriture

L'obtention d'un système de réécriture, comme nous l'avons fait pour l'addition précédemment, est un processus de *catégorification*, comme décrit par John Baez et James Dolan dans [BD98b]. Si cette opération n'est pas encore bien formalisée, elle permet déjà de donner l'intuition de la démarche que nous avons suivie pour l'addition des entiers.

Baez et Dolan plaident le fait qu'en mathématiques, nous utilisons trop d'ensembles et pas assez de catégories. Ou, plus précisément, que nous manipulons des ensembles qui sont en fait des composantes connexes de catégories que nous avons oubliées. Plus concrètement, au lieu de considérer les « vrais » objets, on les identifie par paquets, de manière trop brutale, ce qui coûte, entre autres, la possibilité de calculer de manière effective.

Baez illustre ceci grâce à une métaphore parlant d'un Eden du calcul, à redécouvrir : dans des temps anciens, lorsque deux bergers voulaient savoir qui avait le plus de moutons, ils les alignaient les uns en face des autres, en formant des paires - des isomorphismes. S'il restait des moutons dans un des troupeaux après cette opération, c'est évidemment qu'il en contenait plus. Puis, un jour, un berger a utilisé des mots qui n'avaient pas de sens : *un, deux, trois, . . .*. Dès lors, on avait délaissé la catégorie des ensembles finis pour lui préférer l'ensemble des entiers naturels.

Nous avons déjà vu un exemple de ce phénomène, en étudiant l'addition au début de cette introduction : au lieu de manipuler des termes formés à partir des entiers, on les identifie tous aux entiers correspondant à leurs formes normales, en perdant la notion du calcul qui mène, par exemple, de $2 + 2$ à 4 . Ainsi, Baez et Dolan rappellent que l'ensemble des entiers n'est que l'ensemble des classes d'isomorphismes de la catégorie des ensembles finis qui contient, elle, beaucoup plus d'informations.

Un autre exemple, toujours tiré de [BD98b], est celui du travail d'Emmy Noëther qui, bien que la notion de catégorie n'existât pas à son époque, a montré que l'on pouvait retirer bien plus d'informations du n^{e} groupe d'homologie rationnelle, un *foncteur* défini sur la *catégorie* des espaces topologiques, que du n^{e} nombre de Betti, une *application* sur l'*ensemble* des classes d'isomorphismes d'espaces topologique. En effet, le n^{e} nombre

de Betti ne donne que la dimension de sa version catégorifiée, le n^e groupe d'homologie rationnelle.

Ce processus de catégorification est souvent utilisé pour produire des systèmes de réécriture à partir de présentations équationnelles. Au lieu de regarder des relations non orientées et de quotienter par la relation d'équivalence, donc symétrique, qu'elles engendrent, on remplace toutes les égalités par des flèches. On utilise alors une relation non symétrique et, donc, une version catégorifiée de la présentation de départ. Ainsi, on obtient un calcul correspondant à la relation d'équivalence de départ : celui-ci permet de manipuler plus facilement les éléments, notamment sur une machine, avec laquelle il est difficile d'utiliser des classes d'équivalence. Il ne reste plus qu'à trouver une version convergente de ce calcul pour savoir déterminer des représentants canoniques des classes d'équivalence de la relation de départ.

Catégorifions encore

Lorsque l'on catégorifie une présentation équationnelle, on remplace un ensemble par un graphe : on est ainsi passé d'un objet formé de 0-cellules (un ensemble) à un objet contenant à la fois des 0-cellules et des 1-cellules (un graphe). Les 0-cellules de l'ensemble de départ sont en bijection avec les composantes connexes du graphe obtenu qui contient donc plus d'informations.

Comme exemple de ce procédé de catégorification, considérons le groupe commutatif libre à deux générateurs, notés x et y . Ce groupe, noté $\mathcal{A}(x, y)$, admet la présentation suivante (en tant que groupe) :

$$\mathcal{A}(x, y) \simeq \mathcal{G}(x, y) / \equiv_1,$$

où $\mathcal{G}(x, y)$ est le groupe libre à deux générateurs et \equiv_1 la relation d'équivalence engendrée par la relation $xy = yx$. On peut catégorifier $\mathcal{A}(x, y)$ pour obtenir le groupe libre (non commutatif) à deux éléments $\mathcal{G}(x, y)$, muni de la relation $yx \rightarrow xy$.

Mais tout groupe est aussi un monoïde et, en particulier, $\mathcal{G}(x, y)$ admet la présentation, en tant que monoïde :

$$\mathcal{G}(x, y) = \langle x, x^*, y, y^* \rangle / \equiv_2,$$

où $\langle x, x^*, y, y^* \rangle$ est le monoïde libre à quatre générateurs, dont l'élément neutre est noté 1, et \equiv_2 est engendrée par les relations :

$$xx^* = x^*x = yy^* = y^*y = 1.$$

On catégorifie encore pour arriver à $\langle x, x^*, y, y^* \rangle$, muni des huit règles :

$$\begin{array}{ll} yx \rightarrow xy & y^*x \rightarrow xy^* \\ yx^* \rightarrow x^*y & y^*x^* \rightarrow x^*y^* \\ xx^* \rightarrow 1 & x^*x \rightarrow 1 \\ yy^* \rightarrow 1 & y^*y \rightarrow 1. \end{array}$$

On a donc un ensemble de termes facilement manipulables, particulièrement par une machine, puisque les éléments d'un monoïde libre sont des listes, une des structures de données de base ; on dispose aussi d'un calcul, dont on pourrait montrer qu'il est convergent, permettant de donner des formes normales pour tous les éléments et donc d'avoir une représentation fidèle du groupe de départ.

Un autre exemple de double catégorification sera donné au chapitre 5, où l'on verra que, si un système de réécriture de termes est déjà une présentation équationnelle catégorifiée, les termes sont encore des classes d'équivalence de flèches d'une catégorie monoïdale. La relation citée est engendrée par le produit cartésien de la catégorie des ensembles et nous verrons qu'il est possible de la catégorifier encore, de manière convergente.

Pour finir, remarquons que, si l'on a une relation d'équivalence présentée de manière équationnelle sur les flèches d'une catégorie, le calcul que l'on obtient en l'orientant sera donné par des 2-flèches (des flèches entre des flèches). Si ces mêmes 2-flèches sont encore munies d'une relation d'équivalence, on continue à monter en dimension, en catégorifiant à chaque fois les flèches de dimension n , ce qui en crée en dimension $n + 1$. C'est une des justifications à l'étude de la réécriture en dimension supérieure, c'est-à-dire dans des n -catégories, comme Albert Burroni et Yves Lafont l'ont initié avec [Bur93], [Laf95] et [Laf03].

Ici, nous allons nous contenter de cas particuliers de 2-catégories, les *opérades*, dans une version généralisée.

Organisation

Le **chapitre 1** contient des rappels sur les *relations binaires* ou *systèmes de réécriture abstraits*. Nous y rappelons les principales notions, ainsi que les principaux résultats de la réécriture abstraite qui sont nécessaires pour la suite.

Dans le **chapitre 2**, nous donnons une approche axée sur les structures algébriques mises en jeu pour l'étude des *systèmes de réécriture de mots*, que nous appelons *présentations de monoïdes*. Les principales notions et les résultats classiques y sont rappelés, mais

sous cet éclairage alternatif.

Les présentations d'opérades, comme cadre formel pour la réécriture portant sur des flèches de dimension 2, sont étudiées au **chapitre 3**. On y démontre aussi le théorème 3.11, faisant le lien avec les présentations de monoïdes. Le théorème 3.17 donne une technique de preuve de terminaison pour les présentations d'opérades ainsi qu'un premier exemple d'utilisation : le théorème 3.18 assure que la présentation $L(\mathbb{Z}_2)$ termine, comme Yves Lafont l'avait conjecturé dans [Laf03].

Au cours du **chapitre 4**, nous rappelons les notions de *réseaux de Petri* et de *présentations de monoïdes commutatifs*, puis nous montrons qu'elles sont équivalentes. Enfin, le théorème 4.5 nous dit qu'il s'agit de cas particuliers de présentations d'opérades.

Le **chapitre 5** est dédié à la démonstration du théorème 5.40, qui nous assure que l'on peut plonger, dans un sens qui est défini à la fin du chapitre 1, tout système de réécriture de termes linéaire à gauche dans une présentation d'opérade. Pour ce faire, nous étudions, au cours de ce chapitre, les *opérades cartésiennes* et, plus précisément, diverses présentations de l'opérade cartésienne *initiale* ainsi que de celle qui est *librement engendrée par une signature algébrique*. Nous donnons une présentation *convergente* de chacune d'elles. Enfin, nous discutons des possibilités nouvelles offertes par les présentations d'opérades, relativement aux systèmes de réécriture de termes : par exemple, on peut obtenir des présentations convergentes pour des théories commutatives, comme le prouve le théorème 5.47 avec $L(\mathbb{Z}_2)$.

Le **chapitre 6** contient des rappels concernant différentes pistes explorées dans le but d'obtenir une présentation finie simulant le λ -calcul : la *logique combinatoire*, les *calculs de substitutions explicites*, ainsi que divers calculs graphiques, comme le *calcul de Lamping* et les *réseaux de preuve et d'interaction*. Nous y donnons aussi une limitation théorique forte à l'interprétation du λ -calcul grâce à une présentation d'opérade.

L'**annexe A** est consacrée à la comparaison de différentes structures algébriques servant à abstraire les structures : *opérades classiques*, *PRO*, *PROP*, *théories algébriques*, toutes vues comme des cas particuliers d'*opérades*.

Enfin, l'**annexe B** étudie une présentation du *C-monoïde initial* donnant un *calcul de substitutions explicites* pour le λ -calcul ; nous montrons notamment qu'il ne convient toujours pas au cahier des charges imposé à ce genre de calculs.

Chapitre 1

Relations binaires ou systèmes de réécriture abstraits

Nous allons rappeler ici ce qu'est un *système de réécriture abstrait*. Géométriquement, il s'agit d'un graphe qui, en ce qui nous concerne, est spécifié par un système de réécriture ou une présentation d'objet par générateurs et relations : ses sommets sont les données sur lesquelles le calcul porte et ses flèches, les différentes étapes élémentaires du calcul. On s'intéresse aux propriétés géométriques des chemins de ce graphe, principalement la *terminaison*, qui décrit le fait que tout calcul s'achève, et la *confluence*, qui nous dit si les choix effectués lors du calcul ont une importance ou non.

Il n'y a aucune nouveauté dans ce chapitre qui ne sert qu'à fixer, pour la suite de ce document, le vocabulaire et les notations, qui peuvent varier d'un auteur à l'autre, ainsi que les résultats fondamentaux de la réécriture qui nous seront utiles. Pour de plus amples informations, on pourra se référer à [DJ90], [BN98], [Klo90] ou [Ter03].

Les éléments de théorie des catégories nécessaires à la lecture et non exposés ici peuvent être trouvés dans [ML98], [Sch72] ou [Bor94].

1.1 Définitions

Une *relation binaire* sur un ensemble X est une partie R de $X \times X$. Si un couple (x, y) est dans R , on note souvent xRy . Un *système de réécriture abstrait*, ou *ARS*, est un couple (X, R) où X est un ensemble et R est une relation binaire sur X . Par exemple, l'ensemble \mathbb{N} des entiers naturels muni de l'ordre \leq usuel est un ARS ; de même, tout graphe induit un ARS, formé de l'ensemble des sommets du graphe et de la relation R définie par xRy s'il existe une flèche de x à y dans le graphe.

En réécriture, on note \rightarrow les relations binaires pour insister sur leur caractère d'étapes de calcul : ainsi, dans un ARS (X, \rightarrow) , les éléments de X représentent les états d'un système et les couples (x, y) tels que $x \rightarrow y$ le fait que le système peut passer de x à y en *une* opération élémentaire. On peut, éventuellement, étiqueter ces étapes : on considère alors une relation binaire \rightarrow qui est la réunion de relations \rightarrow_i , où i parcourt l'ensemble des étiquettes ; c'est le cas, en particulier, lorsque l'ARS est issu d'un système de réécriture : les étiquettes sont les règles, ce qui permet de spécifier laquelle est utilisée lors d'un calcul.

À chaque ARS (X, \rightarrow) est associé un graphe dit *de réduction* : ses objets sont les éléments de X et il possède une arête de x à y si et seulement si $x \rightarrow y$. Ce sont les propriétés des chemins de ce graphe qui nous intéressent : en effet, ces chemins sont les *calculs*, c'est-à-dire les enchaînements d'opérations élémentaires menant d'un état à un autre état.

Nous allons définir ces propriétés en termes de relations sur un ensemble et, parallèlement, en termes de chemins du graphe de réduction, afin de donner une intuition géométrique. Avant tout, rappelons :

Définition. Soit X un ensemble. On appelle *diagonale de X* la relation binaire :

$$\Delta_X = \{(x, x), x \in X\}.$$

Si R est une relation binaire sur X , la *relation opposée* à R est :

$$R^o = \{(x, y) \in X^2 : yRx\}.$$

Enfin, si R et S sont deux relations binaires sur X , leur *composée* $S \circ R$ est :

$$S \circ R = \{(x, y) \in X^2 : \exists z \in X, xRz, zSy\}.$$

◆

Note : le symbole ◆ marque la fin d'une définition.

Autrement dit, on a $xR^o y$ si et seulement si yRx . De plus, $x(S \circ R)y$ si et seulement si on a xRz et zSy pour un certain z : en particulier, si $R = S$, on note $R^2 = R \circ R$. Cette opération de composition étant associative et d'unité Δ_X , on note R^n la composée de n copies de R , définie par :

$$R^0 = \Delta_X, \quad R^1 = R, \quad R^{n+1} = R^n \circ R = R \circ R^n.$$

Définition. Une relation binaire R sur X est dite :

- *réflexive* si $\Delta_X \subseteq R$, c'est-à-dire si xRx pour tout $x \in X$;
- *antiréflexive* si $\Delta_X \cap R = \emptyset$, c'est-à-dire s'il n'existe pas de $x \in X$ tel que xRx ;
- *symétrique* si $R^o \subseteq R$, c'est-à-dire si yRx dès que xRy ;
- *antisymétrique* si $R \cap R^o = \Delta_X$, c'est-à-dire si $x = y$ dès que xRy et yRx ;
- *transitive* si $R \circ R \subseteq R$, c'est-à-dire si xRz dès que xRy et yRz .

◆

Exemples. Un *ordre* sur un ensemble X est une relation binaire réflexive, antisymétrique et transitive ; un *ordre strict* est une relation binaire antiréflexive et transitive ; un *préordre* est une relation binaire réflexive et transitive ; une *équivalence* est une relation binaire réflexive, symétrique et transitive.

Définition. Soit (X, R) un ARS. On définit les *clôtures* suivantes :

- la *clôture réflexive* de R est la relation $R^r = R \cup \Delta_X$;
- la *clôture symétrique* de R est la relation $R^s = R \cup R^o$;
- la *clôture transitive* de R est la relation

$$R^t = \bigcup_{n=1}^{+\infty} R^n.$$

◆

Par construction, la clôture réflexive (resp. symétrique, resp. transitive) d'une relation R est la plus petite relation réflexive (resp. symétrique, resp. transitive) contenant R . De plus, les opérations de clôture vérifient :

Lemme 1.1. Soit R une relation binaire sur un ensemble X . On a :

$$(R^r)^s = (R^s)^r, \quad (R^r)^t = (R^t)^r, \quad (R^t)^s \subseteq (R^s)^t.$$

Démonstration. On remarque que, pour deux relations binaires S et T quelconques sur un même ensemble Y , on a :

$$(S \cup T)^{-1} = S^{-1} \cup T^{-1},$$

ainsi que, pour tout ensemble Y :

$$\Delta_Y^{-1} = \Delta_Y.$$

Par suite :

$$\begin{aligned}
 (R^r)^s &= (R \cup \Delta_X) \cup (R \cup \Delta_X)^{-1} \\
 &= R \cup \Delta_X \cup R^{-1} \cup \Delta_X^{-1} \\
 &= R \cup R^{-1} \cup \Delta_X \\
 &= R^s \cup \Delta_X \\
 &= (R^s)^r.
 \end{aligned}$$

Pour toute relation binaire S sur un ensemble Y et pour tout entier n :

$$(S \cup \Delta_Y)^n = \bigcup_{k=0}^n S^k.$$

Par conséquent :

$$\begin{aligned}
 (R^r)^t &= (R \cup \Delta_X)^t \\
 &= \bigcup_{n=1}^{+\infty} (R \cup \Delta_X)^n \\
 &= \bigcup_{n=1}^{+\infty} \bigcup_{k=0}^n R^k \\
 &= \bigcup_{n=0}^{+\infty} R^n \\
 &= (\bigcup_{n=1}^{+\infty} R^n) \cup \Delta_X \\
 &= (R^t)^r.
 \end{aligned}$$

Par définition, on a :

$$(R^t)^s = (\bigcup_{n=1}^{+\infty} R^n) \cup (\bigcup_{n=1}^{+\infty} R^{-n}),$$

en notant R^{-n} la relation $(R^{-1})^n$. Toujours par définition :

$$(R^s)^t = \bigcup_{n=1}^{+\infty} (R \cup R^{-1})^n.$$

Or, pour tout entier n non nul, R^n et R^{-n} sont contenues dans $(R \cup R^{-1})^n$, donc dans $(R^s)^t$. Donc R^t et $(R^{-1})^t$ sont elles aussi contenues dans $(R^s)^t$. Ce qui donne bien, au final :

$$(R^t)^s \subseteq (R^s)^t.$$

◇

Note : les énoncés sont numérotés $m.n$, où m est le numéro du chapitre en cours et n le rang de l'énoncé dans le chapitre ; le symbole ◇ marque la fin d'une démonstration.

On en déduit :

Corollaire 1.2. *Pour toute relation binaire R sur un ensemble X , la relation R^{rst} est la plus petite relation d'équivalence sur X contenant R .*

Par suite, la relation R^{rst} est appelée *équivalence engendrée par R* .

Notation. Si R est notée \rightarrow , on utilise les écritures alternatives et plus imagées : \rightarrow^+ pour \rightarrow^t , \twoheadrightarrow pour \rightarrow^{rt} et \equiv pour \rightarrow^{rst} . On écrit aussi \leftarrow au lieu de $(\rightarrow)^o$, \leftarrow au lieu de $(\twoheadrightarrow)^o$ et \leftarrow^+ pour $(\rightarrow^+)^o$. Enfin, la composée de deux relations \rightarrow_1 et \rightarrow_2 est notée $\rightarrow_1 \rightarrow_2$ au lieu de $\rightarrow_2 \circ \rightarrow_1$.

Si l'on regarde le graphe de réduction associé à un ARS (X, R) , on a :

- $x \rightarrow y$ s'il existe une flèche de x à y ;
- $x \rightarrow^+ y$ s'il existe un chemin (orienté) de longueur non nulle de x à y ;
- $x \twoheadrightarrow y$ s'il existe un chemin (orienté) de x à y ;
- $x \equiv y$ s'il existe une promenade de x à y , c'est-à-dire si l'on peut passer de x à y en parcourant un nombre fini de flèches sans forcément respecter leur orientation.

Venons-en à la première propriété géométrique essentielle d'un ARS :

Définition. On dit qu'un ARS (X, R) *termine* ou qu'il est *noëthérien* s'il n'existe aucune suite $(x_n)_{n \in \mathbb{N}}$ d'éléments de X vérifiant $x_n \rightarrow x_{n+1}$ pour tout n . On dit aussi, indifféremment, que la relation binaire \rightarrow termine ou qu'elle est noëthérienne. \blacklozenge

De manière équivalente, un ARS (X, R) termine si et seulement si le graphe de réduction de (X, \rightarrow) ne contient pas de chemin infini.

Exemples. On remarque aisément que si (X, \rightarrow) est un ARS tel qu'il existe un $x \in X$ avec $x \rightarrow x$, alors il ne termine pas. En particulier, tout ARS dont la relation est réflexive ne termine pas : c'est le cas de (\mathbb{N}, \geq) . En revanche, l'ARS $(\mathbb{N}, >)$ termine.

Remarque. Soit X un ensemble muni d'une relation d'ordre \geq dont on note $>$ la *partie stricte*, donnée par $x > y$ si $x \geq y$ et $x \neq y$. Alors $(X, >)$ termine si et seulement si toute suite décroissante (pour \geq) d'éléments de X est stationnaire. Or, un ordre \geq pour lequel toute suite croissante (resp. décroissante) est stationnaire est dit *noëthérien* (resp. *artinien*). Il y a donc une ambiguïté dans la terminologie : l'ordre \geq est artinien si et seulement si sa partie stricte $>$ est noëthérienne. C'est pour éviter toute confusion que nous employons ici « terminaison » et non « noëthérianité ».

Si un ARS termine, cela signifie qu'il est impossible, partant d'un certain élément, d'effectuer une infinité d'opérations : quel que soit le point de départ, on arrivera, après un nombre fini d'opérations, à un élément sur lequel on ne peut plus agir, c'est-à-dire un élément $x \in X$ tel qu'il n'existe pas de $y \in X$ vérifiant $x \rightarrow y$.

Définition. Soit (X, \rightarrow) un ARS. On appelle *R-forme normale* (ou seulement *forme normale*) tout élément x de X pour lequel il n'existe aucun y dans X vérifiant $x \rightarrow y$. Si x et y sont deux éléments de X , on dit que y est une *(R-)forme normale de x* si y est une *(R-)forme normale* et si $x \twoheadrightarrow y$. ♦

La terminaison implique que tout élément possède *au moins* une forme normale : on dit que (X, R) est *normalisant* ou, indistinctement, que *R normalise*. La normalisation est une propriété plus faible que la terminaison, même dans le cas où la forme normale de chaque élément est unique : considérons un ensemble réduit à deux éléments, notés x et y , que l'on munit de la relation

$$R = \{(x, x), (x, y)\}.$$

Alors y est l'unique forme normale de x et de y ; cependant, comme nous l'avons déjà remarqué, le fait que x vérifie xRx empêche R de terminer.

De plus, il n'y aucune raison pour que l'on ait unicité des formes normales. D'un point de vue opérationnel, cela veut dire que, partant d'une même valeur initiale, il est possible d'arriver à des résultats différents suivant certains choix effectués. Or, les seuls choix que l'on peut faire sont entre deux opérations partant d'un même élément. On arrive ainsi à la notion de branchement :

Définition. Soit (X, \rightarrow) un ARS. Un *branchement* de (X, \rightarrow) est un triplet (x, y, z) d'éléments de X tels que $x \twoheadrightarrow y$ et $x \twoheadrightarrow z$; x est appelé la *source* d'un tel branchement. On dit qu'un branchement (x, y, z) est *local* si $x \rightarrow y$ et $x \rightarrow z$. Un branchement (x, y, z) est dit *confluent* s'il existe un $t \in X$ tel que $y \twoheadrightarrow t$ et $z \twoheadrightarrow t$; on dit d'un tel t qu'il *ferme* le branchement (x, y, z) . ♦

La notion de confluence d'un ARS porte sur celle de ses branchements :

Définition. On dit qu'un ARS (X, \rightarrow) est *confluent* (resp. *localement confluent*) si tous ses branchements (resp. *branchements locaux*) sont confluents. On dit aussi que la relation binaire \rightarrow est (localement) *confluente*. ♦

Alternativement, un tel ARS est confluent si et seulement si

$$\leftarrow \twoheadrightarrow \subseteq \twoheadrightarrow \leftarrow$$

et localement confluent si et seulement si

$$\leftarrow \rightarrow \subseteq \twoheadrightarrow \leftarrow.$$

Ainsi, dans un ARS confluent, les choix effectués n'ont pas d'importance. Cela assure que, partant d'une situation donnée, on ne peut pas arriver à des résultats différents, quels

que soient les chemins de réduction empruntés : tout élément d'un ARS confluent possède *au plus* une forme normale. On comprend alors pourquoi la réécriture accorde autant d'importance aux ARS qui possèdent conjointement les deux propriétés de terminaison et de confluence :

Définition. Un ARS est dit *convergent* ou *gröbnerien* s'il termine et s'il est confluent. On dit aussi que la relation binaire de l'ARS est convergente. \blacklozenge

Remarque. Dans la littérature, on trouve d'autres adjectifs, comme *complet* ou *canonique*, utilisés différemment selon les auteurs : il s'agit, dans certains travaux, de synonymes de *convergent*, alors que, dans d'autres, ils désignent des propriétés plus fortes que la convergence.

On peut aussi définir les notions de terminaison et de confluence en un point : par exemple, si (X, \rightarrow) est un ARS et si $x \in X$, on dit que (X, \rightarrow) *termine en x* s'il ne contient pas de chemin de réduction infini partant de x . On a alors : un ARS (X, \rightarrow) termine si et seulement s'il termine en tout $x \in X$.

1.2 Principaux critères de terminaison et de confluence

Nous allons présenter ici deux critères classiques concernant la terminaison et la confluence des ARS. Avant d'aborder le critère de terminaison, définissons les morphismes d'ARS :

Définition. Soient (X, \rightarrow_X) et (Y, \rightarrow_Y) deux ARS. Un *morphisme d'ARS de X vers Y* est une application $\varphi : X \rightarrow Y$ qui est faiblement compatible avec les relations de réduction, c'est-à-dire telle que $\varphi(\rightarrow_X) \subseteq \rightarrow_Y$, ou encore telle que, pour tous $x, x' \in X$ vérifiant $x \rightarrow_X x'$, on a $\varphi(x) \rightarrow_Y \varphi(x')$. Un tel morphisme est dit :

- *non contractant* si $\varphi(\rightarrow_X) \subseteq \rightarrow_Y^+$, c'est-à-dire si $\varphi(x) \rightarrow_Y^+ \varphi(x')$ dès que $x \rightarrow_X x'$;
- *strict* si $\varphi(\rightarrow_X) \subseteq \rightarrow_Y$, c'est-à-dire si $\varphi(x) \rightarrow_Y \varphi(x')$ dès que $x \rightarrow_X x'$.

\blacklozenge

Le résultat suivant est *essentiel* pour prouver la terminaison d'un ARS :

Théorème 1.3. Soit (X, \rightarrow) un ARS. Les assertions suivantes sont équivalentes :

1. L'ARS (X, \rightarrow) termine.
2. Il existe un ordre strict $>$ sur X tel que $(X, >)$ termine et tel que $x > x'$ dès que $x \rightarrow x'$.
3. Il existe un ARS (Y, \rightarrow_Y) qui termine ainsi qu'un morphisme d'ARS non contractant $f : (X, \rightarrow) \rightarrow (Y, \rightarrow_Y)$.

Démonstration.

1 \Rightarrow 2. On va montrer que \rightarrow^+ est un ordre strict qui termine sur X .

Pour l'antiréflexivité, on suppose qu'il existe $x \in X$ tel que $x \rightarrow^+ x$: par définition, il existe un chemin de longueur non nul de x à x dans (X, \rightarrow) ; en mettant bout à bout une infinité de copies de ce chemin, on obtient un chemin infini dans (X, \rightarrow) , ce qui contredit l'hypothèse.

Pour la transitivité, on suppose que x, y , et z sont trois éléments de X tels que $x \rightarrow^+ y$ et $y \rightarrow^+ z$: il existe donc un chemin de longueur non nulle dans (X, \rightarrow) de x à y et un autre de y à z ; en les recollant, on obtient un chemin de longueur non nulle de x à z dans (X, \rightarrow) , ce qui donne $x \rightarrow^+ z$.

Enfin, pour la terminaison, on suppose qu'il existe une suite $(x_n)_{n \in \mathbb{N}}$ d'éléments de X tels que $x_n \rightarrow^+ x_{n+1}$ pour tout n : il existe donc, pour tout n , un chemin de longueur non nulle de x_n à x_{n+1} dans (X, \rightarrow) ; mis bout à bout, tous ces chemins donnent un chemin infini partant de x_0 dans (X, \rightarrow) , ce qui contredit encore l'hypothèse.

Il ne reste plus qu'à montrer que $x \rightarrow^+ x'$ dès que $x \rightarrow x'$, ce qui est, par définition de la clôture transitive \rightarrow^+ de \rightarrow , le cas.

2 \Rightarrow 3. On prend $Y = X$, $\rightarrow_Y = >$ et $f = \text{id}_X$. Par hypothèse, $(X, >)$ termine et f est un morphisme strict, donc non contractant, de (X, \rightarrow) vers $(X, >)$.

3 \Rightarrow 1. Supposons qu'il existe une suite $(x_n)_{n \in \mathbb{N}}$ d'éléments de X tels que $x_n \rightarrow x_{n+1}$ pour tout n . Alors, le morphisme f nous donne une suite $(f(x_n))_{n \in \mathbb{N}}$ d'éléments de Y tels que $f(x_n) \rightarrow_Y^+ f(x_{n+1})$ pour tout n . Or, comme (Y, \rightarrow) termine, en appliquant 1 \Rightarrow 2, on a la terminaison de (Y, \rightarrow_Y^+) , ce qui contredit l'existence d'une telle suite.

◇

Remarque. On retiendra, en particulier, que, si (X, \rightarrow) termine, alors \rightarrow^+ est un ordre strict qui termine. En pratique, ce résultat est souvent utilisé dans le sens 3 \Rightarrow 1, en prenant $Y = \mathbb{N}$ et \rightarrow_Y la relation d'ordre strict $>$.

Nous avons ainsi un critère de terminaison utilisable. En revanche, en ce qui concerne la confluence, elle est presque invérifiable avec la définition donnée : en effet, dans la plupart des cas, un ARS possède une infinité de branchements. Cependant, lorsqu'un ARS termine, le lemme de Newman simplifie la tâche. Avant de l'énoncer, rappelons la définition du principe de récurrence :

Définition. Soit (X, R) un ARS. On dit que le *principe de récurrence* est vrai dans (X, \rightarrow) si, pour toute propriété P portant sur les éléments de x , on a :

si pour tout $x \in X$, le fait que $P(y)$ soit vraie pour tous les $y \in X$ tels que $x \twoheadrightarrow^+ y$ implique que $P(x)$ est vraie, alors $P(x)$ est vraie pour tout $x \in X$.

◆

Remarque. Dans le cas de $(\mathbb{N}, >)$, il s'agit du principe de récurrence usuel : pour toute propriété P portant sur les entiers, si on a $P(0)$ et $P(k) \Rightarrow P(n+1)$ pour tout n et tout $k \leq n$, alors $P(n)$ est vraie pour tout n .

On a le résultat suivant qui relie ce principe à la terminaison :

Théorème 1.4 (Principe de récurrence). *Un ARS (X, \rightarrow) termine si et seulement si le principe de récurrence est vrai dans (X, \rightarrow) .*

Démonstration. Supposons que (X, \rightarrow) termine mais que le principe de récurrence n'est pas vrai dans (X, \rightarrow) . Alors il existe une propriété P telle que :

- pour tout $x \in X$, le fait que $P(y)$ soit vraie pour tous les $y \in X$ tels que $x \twoheadrightarrow^+ y$ implique que $P(x)$ est vraie ;
- il existe x_0 dans X tel que $P(x_0)$ est fausse.

Alors, il existe un x_1 dans X tel que $x_0 \twoheadrightarrow^+ x_1$ et $P(x_1)$ est fausse : sinon, on aurait $P(x_0)$. On recommence à partir de x_1 : il existe forcément un x_2 dans X tel que $x_1 \twoheadrightarrow^+ x_2$ et $P(x_2)$ est fausse. On peut donc construire un chemin de réduction infini dans $(X, \twoheadrightarrow^+)$ qui ne termine pas, ce qui contredit le fait que (X, \rightarrow) termine.

Réciproquement, supposons que le principe de récurrence est vrai dans (X, \rightarrow) . On note $P(x)$ la forme propositionnelle :

$P(x) = \ll \text{Il n'existe pas de chemin de réduction infini partant de } x \text{ dans } (X, \rightarrow) \gg$.

Soit $x \in X$ et supposons que $P(y)$ est vraie pour tous les $y \in X$ tels que $x \twoheadrightarrow^+ y$: en particulier, il n'existe aucun chemin infini partant d'un y tel que $x \rightarrow y$, ce qui exclut la possibilité d'avoir un chemin infini partant de x . Donc (X, \rightarrow) termine. ◆

On peut à présent démontrer le résultat suivant [New42] :

Théorème 1.5 (« Lemme » de Newman). *Un ARS est convergent si et seulement s'il termine et s'il est localement confluent.*

Démonstration. Supposons que (X, \rightarrow) est un ARS convergent : par définition, il termine et est confluent. Or, il est évident que la confluence implique la confluence locale puisque les branchements locaux sont aussi des branchements.

Réciproquement, supposons que (X, \rightarrow) termine et qu'il est localement confluent. Comme (X, \rightarrow) termine, on peut utiliser le principe de récurrence pour montrer que tout branchement est confluent. Plus précisément, on pose $P(x)$ la forme propositionnelle :

$$P(x) = \llcorner \text{ Tout branchement de source } x \text{ est confluent } \lrcorner.$$

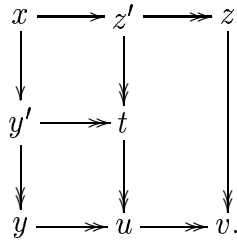
Si x est une forme normale, alors le seul branchement de source x est (x, x, x) qui est toujours confluent : on a $x \twoheadrightarrow x$ pour tout x .

À présent, considérons un x dans X et supposons que $P(y)$ est vraie pour tous les $y \in X$ tels que $x \twoheadrightarrow^+ y$. Soit (x, y, z) un branchement. Distinguons deux cas :

1. Si $x = y$ (ou $x = z$), le branchement est confluent car $y = x \twoheadrightarrow z$ et $z \twoheadrightarrow z$.
2. Sinon, il existe y' et z' dans X tels que $x \rightarrow y' \twoheadrightarrow y$ et $x \rightarrow z' \twoheadrightarrow z$: on a un branchement local (x, y', z') donc, comme (X, \rightarrow) est localement confluent, il existe t tel que $y' \twoheadrightarrow t$ et $z' \twoheadrightarrow t$.

On obtient un branchement (y', y, t) : comme $x \rightarrow y'$, on peut appliquer l'hypothèse de récurrence à y' et en déduire qu'il existe $u \in X$ tel que $y \twoheadrightarrow u$ et $t \twoheadrightarrow u$. Puisque $x \rightarrow z'$, on applique de nouveau l'hypothèse de récurrence à z' pour conclure que le branchement (z', u, z) est confluent, c'est-à-dire qu'il existe $v \in X$ tel que $u \twoheadrightarrow v$ et $z \twoheadrightarrow v$.

On a donc le graphe de réduction suivant :



Le branchement (x, y, z) est donc confluent et $P(x)$ est vérifiée.

◇

1.3 Comparaison de systèmes de réécriture

Les ARS seront utilisés dans la suite pour comparer des systèmes de réécriture. Nous associerons à chaque système de réécriture rencontré un ARS et ce sont ces ARS que nous comparerons. Nous montrerons notamment qu'il existe deux types de liens : le premier, l'isomorphisme, est utilisé pour montrer que deux ARS sont essentiellement identiques.

Définition. Un *isomorphisme entre deux ARS* (A, R) et (B, S) est une application bijective $f : A \longrightarrow B$ telle que f et f^{-1} sont des morphismes stricts d'ARS. \blacklozenge

Pour définir la notion de simulation, nous devons parler de quotient : si X est un ensemble et \simeq une relation d'équivalence sur X , on définit X/\simeq comme l'ensemble des classes d'équivalences d'éléments de X pour la relation \simeq . Par exemple, si $X = \mathbb{Z}$ et si \simeq désigne la relation \equiv_2 de congruence modulo 2, alors \mathbb{Z}/\equiv_2 est l'ensemble $\mathbb{Z}/2\mathbb{Z}$ constitué de deux éléments : l'un est l'ensemble des entiers pairs, noté 0, et l'autre est l'ensemble des entiers impairs, noté 1.

Si X est un ensemble et R une relation binaire, on note X/R le quotient de X par R^{rst} , la relation d'équivalence engendrée par R . Si S est une autre relation binaire, on définit la relation quotient de S par R comme la relation binaire S/R sur X/R ainsi : deux éléments a et b de X/R vérifient $a(S/R)b$ s'il existe $x \in a \subseteq X$ et $y \in b \subseteq X$ tels que xSy . On définit alors :

Définition. Soit (A, R) un ARS. Une *simulation de* (A, R) est une donnée (B, S, Φ) formé d'un ARS (B, S) et d'un morphisme non contractant d'ARS $\Phi : (A, R) \longrightarrow (B, S)$ tel que :

1. le morphisme Φ induit un morphisme strict d'ARS :

$$(A, R) \longrightarrow (B/\Phi(R), S/\Phi(R)) ;$$

2. les éléments de $\Phi(A)$ sont des formes normales pour $S_0 = S^t \setminus \Phi(R)$;
3. l'ARS (B, S_0) est convergent.

On dit qu'une telle simulation est *complète* si, de plus :

4. l'ARS (A, R) termine si et seulement si (B, S) termine ;
5. l'ARS (A, R) est confluent si et seulement si (B, S) est confluent.

\blacklozenge

Le fait qu'il existe une simulation (B, S, Φ) de (A, R) signifie que (B, S) est une version catégorifiée, au sens de [BD98b], de (A, R) . En d'autres termes, les éléments de A sont obtenus par quotient de B par une sous-relation S_0 de S et R est le quotient de S par S_0 . De plus, S_0 est convergente et l'on connaît une section Φ du quotient, qui associe à toute classe d'équivalence $a \in A$ son unique représentant $\Phi(a) \in B$ qui est une S_0 -forme normale.

Ainsi, au lieu de travailler modulo certaines relations dans A (par exemple les relations de gestion des ressources ou de substitution de variables), ce qui oblige à faire des opérations externes au calcul (test d'égalité, « collecte des déchets », α -conversion), on les oriente de manière convergente, ce qui permet de les inclure dans le calcul. De plus, si la simulation est complète, ces nouvelles opérations s'intègrent au calcul sans en changer les propriétés de confluence et de terminaison.

Citons, par exemple, le problème 88 de « Liste de problèmes ouverts », maintenue sur la page de RTA, voir [RTA] : il pose la question de l'existence d'une simulation complète du λ -calcul non typé par un système de réécriture de termes.

Une autre vision de la simulation est que l'ARS A se "plonge" dans l'ARS B et ce, d'un point de vue topologique : B est une somme amalgamée de l'ARS A et d'un ARS correspondant au quotient. Il semble qu'il existe une structure de modèles sur la catégorie des ARS (ou une catégorie qui la contient) telle que les simulations complètes soient des cofibrations (triviales), mais ceci reste à explorer.

1.4 Réécriture abstraite et langage des catégories

Lorsque l'on étudie des systèmes de réécriture plus complexes, comme ceux de mots ou de termes, les ARS semblent à part, comme nous l'avons déjà remarqué : ce ne sont que des objets associés à ces systèmes de réécriture pour définir leurs propriétés géométriques. Pourtant, ils décrivent eux aussi une réécriture dans une certaine structure algébrique. En effet, la relation de réduction d'un ARS est nécessairement compatible avec la structure algébrique des états du système, celle-ci étant triviale.

Il semble ainsi qu'il existe, exprimée dans le langage des catégories, une structure de *système de réécriture*, dans le sens suivant : il paraît envisageable de définir un système de réécriture pour $(\mathcal{C}, \mathcal{D}, \mathcal{L}, \mathcal{U})$ avec \mathcal{C} et \mathcal{D} deux catégories, $(\mathcal{L}, \mathcal{U})$ une adjonction (de type libre-oubli) de \mathcal{C} à \mathcal{D} .

Avec ces données, les $(\mathcal{C}, \mathcal{D}, \mathcal{L}, \mathcal{U})$ -systèmes de réécriture seraient alors :

1. Les systèmes de réécriture abstraits, si $\mathcal{C} = \mathcal{D} = \mathbb{E}\mathbb{N}\mathbb{S}$ (la catégorie des ensembles) et $\mathcal{L} = \mathcal{U} = \text{id}$.
2. Les systèmes de réécriture de mots ou présentations de monoïdes, si $\mathcal{C} = \mathbb{E}\mathbb{N}\mathbb{S}$, $\mathcal{D} = \mathbb{M}\mathbb{O}\mathbb{N}$ (la catégorie des monoïdes), \mathcal{L} le foncteur monoïde libre engendré par un ensemble et \mathcal{U} le foncteur oubli - voir le chapitre 2.
3. Les réseaux de Petri ou présentations de monoïdes commutatifs, si $\mathcal{C} = \mathbb{E}\mathbb{N}\mathbb{S}$, $\mathcal{D} = \mathbb{C}\mathbb{O}\mathbb{M}$ (la catégorie des monoïdes commutatifs), \mathcal{L} le foncteur monoïde commutatif libre engendré par un ensemble et \mathcal{U} le foncteur oubli - voir le chapitre 4.
4. Les présentations d'opérades, si $\mathcal{C} = \mathbb{S}\mathbb{G}\mathbb{N}$ (la catégorie des signatures), $\mathcal{D} = \mathbb{O}\mathbb{P}$ (la catégorie des opérades), \mathcal{L} le foncteur opérade libre engendrée par une signature et \mathcal{U} le foncteur oubli - voir le chapitre 3.

Ceci reste encore à formaliser, mais c'est dans cet esprit que nous étudierons les présentations de monoïdes, de monoïdes commutatifs et d'opérades dans ce qui suit. Nous pourrons ainsi calquer les notions et résultats intervenant dans le chapitre 3 sur celles du chapitre 2, en substituant seulement l'adjonction (monoïde libre - oubli) par l'adjonction (opérade libre - oubli).

Il faut toutefois mentionner qu'il existe d'autres travaux exprimant les notions de la réécriture dans le langage des catégories. Parmi ces études, citons celles-ci :

- Albert Burroni considère, dans [Bur93], la réécriture dans des n -catégories. Une partie du travail qu'il a initié dans cet article est poursuivie ici, dans le chapitre 5 : on y montre qu'un système de réécriture de termes linéaire à gauche peut être simulé complètement par une présentation d'opérade, qui n'est autre qu'un système de réécriture dans une 2-catégorie particulière.
- Marcelo Fiore, Gordon Plotkin et Daniele Turi ont développé, dans [FPT99], un modèle des systèmes de réécriture avec ou sans lieurs, en étudiant la structure de la catégorie des préfaisceaux covariants sur la catégorie \mathbb{F} des ensembles finis.
- Paul-André Melliès a développé, dans une série d'articles, une théorie axiomatique de la réécriture, en extrayant les propriétés vérifiées par les espaces de réduction de nombreux types de systèmes de réécriture. Cette théorie, présentée dans [Mel02], considère des catégories possédant de telles propriétés et il en découle de nombreux résultats concernant, par exemple, la standardisation et la factorisation des chemins de réduction.

Chapitre 2

Présentations de monoïdes ou systèmes de réécriture de mots

Nous allons voir le cas le plus classique de système de réécriture *concret*, celui des mots. Nous donnons une présentation algébrique de la théorie classique de [BO93], en mettant l'accent sur les *structures* mises en jeu ; le choix de la terminologie *présentations de monoïdes* au lieu de *systèmes de réécriture de mots* témoigne de cette volonté. Le but est ici d'exhiber les ingrédients essentiels de tout système de réécriture, vu comme un objet algébrique, et ce, à deux fins : la première, à court terme, est de pouvoir introduire les présentations d'opérades au chapitre 3, en calquant ce qui aura été fait ici ; la seconde, à plus long terme, est de mieux appréhender ce que peut être un système de réécriture en théorie des catégories.

2.1 La catégorie des monoïdes et le foncteur monoïde libre

Commençons par la structure de monoïde :

Définition. Un *monoïde* est une donnée $(M, \cdot, *)$ formée d'un ensemble M muni d'une loi de composition interne \cdot ainsi que d'un élément distingué $*$ de M , le tout soumis aux relations suivantes :

1. La loi \cdot est *associative* : pour tous $x, y, z \in M$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
2. L'élément $*$ est *neutre à gauche* pour \cdot : pour tout $x \in M$, $* \cdot x = x$.
3. L'élément $*$ est *neutre à droite* pour \cdot : pour tout $x \in M$, $x \cdot * = x$.

L'opération \cdot est généralement appelée *produit* du monoïde et l'élément $*$ son *neutre*. L'ensemble M est dit *sous-jacent* au monoïde ; lorsqu'il ne peut y avoir de confusion, on désigne abusivement un monoïde et son ensemble sous-jacent de la même façon. ♦

On peut citer, par exemple, l'ensemble \mathbb{N} des entiers naturels muni de l'addition, avec 0 comme neutre ; ou encore, l'ensemble des nombres complexes de module 1, muni du produit des nombres complexes, avec 1 pour neutre. De même, l'ensemble des matrices 2×2 possède une structure de monoïde pour le produit des matrices, avec l'identité comme neutre.

En général, on omet la notation du produit : ainsi, $x \cdot y$ est souvent noté xy . Comme, pour tous x, y, z , on a $(xy)z = x(yz)$, on note ce double produit xyz ; de même le produit de n éléments x_1, \dots, x_n est noté $x_1 \dots x_n$.

Définition. Soient M et N deux monoïdes. Un *morphisme de monoïdes* de M vers N est une application $\varphi : M \longrightarrow N$ qui vérifie les égalités suivantes :

1. Pour tous $x, y \in M$, $\varphi(xy) = \varphi(x)\varphi(y)$.
2. $\varphi(*) = *$.

Attention, dans la première relation, le produit du membre de gauche est celui de M et celui du membre de droite est celui de N . De même, dans la seconde relation, le neutre du membre de gauche est celui de M et celui du membre de droite est celui de N . Les monoïdes et leurs morphismes s'organisent en une catégorie notée \mathbf{MON} . \blacklozenge

Pour la suite, l'exemple essentiel de monoïde est celui du *monoïde libre engendré par un ensemble*. On note $\mathcal{U} : \mathbf{MON} \longrightarrow \mathbf{ENS}$ le foncteur oubli, c'est-à-dire le foncteur qui associe à tout monoïde son ensemble sous-jacent et à tout morphisme l'application sous-jacente.

Définition. Soit X un ensemble. On appelle *monoïde libre engendré par X* tout couple (M, i) composé d'un monoïde M et d'une application $i : X \longrightarrow \mathcal{U}M$ tels que : pour tout monoïde N et toute application $\varphi : X \longrightarrow \mathcal{U}N$, il existe un unique morphisme de monoïdes $\psi : M \longrightarrow N$ tel que le diagramme

$$\begin{array}{ccc} X & \xrightarrow{i} & \mathcal{U}M \\ & \searrow \varphi & \downarrow \psi \\ & & \mathcal{U}N \end{array} \quad \text{Ⓢ}$$

commute. \blacklozenge

Comme dans tout problème universel, toute solution éventuelle est unique à un unique isomorphisme près : l'abus consistant à la considérer unique n'en est donc pas vraiment un. Nous allons construire une solution et, en conséquence, l'appeler *le* monoïde libre engendré par l'ensemble considéré.

Si l'on fixe un ensemble X , on construit ce monoïde, noté ici $\langle X \rangle$, de la façon suivante : l'ensemble sous-jacent est composé d'un élément noté $*$ et de toutes les familles finies

non vides d'éléments de X , c'est-à-dire de tous les (x_1, \dots, x_n) pour n entier non nul et x_1, \dots, x_n parcourant X . On définit le produit de deux éléments de $\langle X \rangle$ de la manière suivante :

$$\begin{cases} * \cdot * & = * \\ * \cdot (x_1, \dots, x_n) & = (x_1, \dots, x_n) \\ (x_1, \dots, x_n) \cdot * & = (x_1, \dots, x_n) \\ (x_1, \dots, x_n) \cdot (y_1, \dots, y_p) & = (x_1, \dots, x_n, y_1, \dots, y_p). \end{cases}$$

Proposition 2.1. *Le triplet $(\langle X \rangle, \cdot, *)$ est un monoïde. De plus, en notant $i : X \longrightarrow \langle X \rangle$ l'application qui associe à tout élément x de X la famille à un élément formée par x , le couple $(\langle X \rangle, i)$ est solution du problème universel de monoïde libre engendré par X .*

Démonstration. Par construction, $\langle X \rangle$ est un monoïde. Soient M un monoïde et $\varphi : X \longrightarrow M$ une application. On définit $\psi : \langle X \rangle \longrightarrow M$ en posant $\psi(*) = *$ et, si $x_1, \dots, x_n \in X$:

$$\psi(x_1 \dots x_n) = \varphi(x_1) \dots \varphi(x_n).$$

Cette définition nous assure que ψ est un morphisme de monoïdes $\langle X \rangle \longrightarrow M$ qui coïncide avec φ sur les éléments de X . Réciproquement, tout morphisme de monoïdes $\omega : \langle X \rangle \longrightarrow M$ qui coïncide avec φ sur les éléments de X vérifie nécessairement :

$$\omega(*) = * \quad \text{et} \quad \omega(x_1 \dots x_n) = \varphi(x_1) \dots \varphi(x_n).$$

Le morphisme ψ est donc bien l'unique morphisme qui fait commuter le diagramme de l'énoncé. \diamond

On peut formuler ce résultat autrement : l'application $\langle \cdot \rangle : X \longmapsto \langle X \rangle$ s'étend en un foncteur $\mathbf{ENS} \longrightarrow \mathbf{MON}$ qui est adjoint à gauche du foncteur oubli $\mathcal{U} : \mathbf{MON} \longrightarrow \mathbf{ENS}$. Les foncteurs « oubli » permettent de formuler les problèmes universels d'objets libres. Cependant, afin d'alléger les notations et sauf risque de confusion, ils seront parfois omis, une fois l'objet libre construit. De plus, on notera toujours \mathcal{U} les foncteurs libres, mêmes s'ils sont tous distincts.

Définition. On dit qu'un monoïde M est libre s'il existe un ensemble X tel que $M = \langle X \rangle$. Les éléments de $\langle X \rangle$ sont souvent appelés *mots* sur l'*alphabet* X ; le mot $*$ est qualifié de *vide* et le produit de $\langle X \rangle$ appelé *concaténation* ; les éléments de X sont les *lettres* de l'alphabet. \blacklozenge

Exemples. Si $X = \{x\}$, on a $\langle X \rangle = \{x^n | n \in \mathbb{N}\}$. Si $X = \{a, b\}$, les éléments de $\langle X \rangle$ seront $*$ ainsi que toutes les suites finies de a et de b , comme a , ba , $abba$, $bababb$, etc.

2.2 Modules, idéaux et relations de réduction sur un monoïde

Ce paragraphe débute par la définition classique de *relation de réduction sur un monoïde*. Puis nous verrons comment caractériser différemment ces relations, et comment en construire à partir de *règles de réécriture*.

Définition. Soient M un monoïde et R une relation binaire sur M . On dit que R est *compatible avec la structure de monoïde de M* ou que R est une *relation de réduction sur M* si elle vérifie, pour tous x, y, z de M :

$$xRy \implies \begin{cases} (zx)R(zy) \\ (xz)R(yz). \end{cases}$$

◆

Il existe de nombreux exemples de relations de réduction : la relation \leq sur \mathbb{N} est compatible avec l'addition, la relation de divisibilité sur l'ensemble \mathbb{Z}^* des entiers relatifs non nuls est compatible avec le produit, la congruence modulo n est compatible avec l'addition et le produit sur \mathbb{Z} , etc.

En réécriture, on s'intéresse à la *relation de réduction engendrée par une famille de règles de réécriture*. Mais, avant d'aborder cela, nous allons donner une autre interprétation des relations de réduction sur un monoïde, grâce à la notion de module :

Définition. Soit $(M, \cdot, *)$ un monoïde. Un M -module ou *module sur M* est un triplet (X, \cdot_g, \cdot_d) constitué d'un ensemble X et d'applications $\cdot_g : M \times X \longrightarrow X$ et $\cdot_d : X \times M \longrightarrow X$, appelées respectivement *actions à gauche* et *à droite* de M sur X et vérifiant :

1. L'action \cdot_g est *compatible* avec \cdot : $a \cdot_g (b \cdot_g x) = (a \cdot b) \cdot_g x$, pour tous a et b dans M et x dans X .
2. L'action \cdot_d est *compatible* avec \cdot : $(x \cdot_d a) \cdot_d b = x \cdot_d (a \cdot b)$, pour tous a et b dans M et x dans X .
3. Les actions \cdot_g et \cdot_d sont compatibles : $(a \cdot_g x) \cdot_d b = a \cdot_g (x \cdot_d b)$, pour tous a et b dans M et x dans X .
4. L'élément $*$ est *neutre à gauche* pour \cdot_g : $* \cdot_g x = x$, pour tout x dans X .
5. L'élément $*$ est *neutre à droite* pour \cdot_d : $x \cdot_d * = x$, pour tout x dans X .

Comme pour les monoïdes, on identifie le M -module et son ensemble sous-jacent ; les relations nous autorisent à omettre les \cdot_g et \cdot_d , ainsi que les parenthèses. ◆

Exemples. Le M -module le plus simple est (M, \cdot, \cdot) ; les relations sont alors données par l'associativité (les trois premières, ici identiques) et par le fait que $*$ est neutre à gauche et à droite pour le produit (les deux dernières, respectivement).

Un autre exemple, plus important ici, est donné par $M \times M$ muni des *actions diagonales* : on pose $x \cdot_g (y, z) = (x \cdot y, x \cdot z)$ et, similairement, $(x, y) \cdot_d z = (x \cdot z, y \cdot z)$; les cinq relations de la définition de M -module sont bien vérifiées : les trois premières sont données par l'associativité de \cdot et les deux dernières par le fait que $*$ est neutre à gauche et à droite pour $*$. Ce M -module, noté M^2 , est appelé le M -module *diagonal*.

Définition. Soient M un monoïde et X un M -module. Un *sous- M -module* de X est une partie de X stable pour les actions à gauche et à droite de M sur X . Un *idéal* de M est un sous- M -module du M -module diagonal M^2 . \blacklozenge

On remarque que tout sous- M -module, et donc tout idéal de M , est un M -module. On a une nouvelle interprétation des relations de réduction sur un monoïde :

Proposition 2.2. *Soit M un monoïde. Les relations de réductions sur M sont les idéaux de M .*

Démonstration. Soit R une relation de réduction sur M . Montrons que R est un idéal de M , c'est-à-dire que R est une partie de M^2 qui est stable pour les actions diagonales de M sur M^2 . Soient $x, y, z \in M$ tels que yRz : alors $x(y, z) = (xy, xz)$; or R est une relation de réduction sur M , et donc $xyRxz$. De manière similaire, $yxRzx$. Donc R est bien un idéal de M .

Réciproquement, soit I un idéal de M . Comme I est stable par actions diagonales, on a, pour tous $x \in M$ et $(y, z) \in I$, $(xy, xz) = x(y, z) \in I$ et $(yx, zx) = (y, z)x \in I$. Donc I est une relation de réduction sur M . \blacklozenge

Cette équivalence nous permettra de jongler avec les deux notions pour parler tantôt de relation de réduction et tantôt d'idéal. On va voir maintenant que la donnée d'une famille de *relations* ou de *règles de réécriture* sur un monoïde libre $\langle X \rangle$ permet de construire une relation de réduction sur $\langle X \rangle$. Avant tout, une *relation* ou *égalité* ou *règle de réécriture* sur un monoïde M est un élément du M -module diagonal $M \times M$. Pour une telle relation $\alpha = (x, y)$, on appelle x la *source* de α , notée $s(\alpha)$, et y son *but*, noté $t(\alpha)$.

Étant donnée une partie R de M^2 , on peut construire un idéal noté (R) ou \rightarrow_R comme suit : si a et b sont des éléments de M , on a $a \rightarrow_R b$ si et seulement s'il existe $\alpha \in R$ et $u, v \in M$ tels que $(a, b) = u\alpha v$. Par construction, (R) est bien un idéal de M . On a alors :

Proposition 2.3. *Si M est un monoïde et R une partie de M^2 , l'idéal (R) de M^2 est le plus petit idéal de M contenant R .*

Démonstration. Supposons que I est un idéal de M contenant R et que $a \rightarrow_R b$: il existe $u, v \in M$ et $\alpha \in R$ tels que $(a, b) = u\alpha v$; comme $\alpha \in R \subseteq I$ et que I est un idéal, on a bien $(a, b) \in I$. \diamond

Pour une partie R du module diagonal, on appelle (R) l'*idéal de M engendré par l'ensemble R de relations* ou la *relation de réduction engendrée par la famille R de règles de réécriture*.

On peut à présent donner les définitions suivantes :

Définition. Une *présentation de monoïdes* ou *système de réécriture de mots* est un couple (X, R) composé d'un ensemble X et d'une partie R du module diagonal du monoïde libre $\langle X \rangle$ engendré par X (c'est-à-dire que R est une famille de relations sur $\langle X \rangle$). L'ARS associé à (X, R) est $(\langle X \rangle, (R))$ où (R) est l'idéal de $\langle X \rangle$ engendré par R (c'est-à-dire que \rightarrow_R est la relation de réduction sur $\langle X \rangle$ engendrée par R). \blacklozenge

En fait, on devrait plutôt dire que l'ARS associé à un système de réécriture de mots est $(\mathcal{U}\langle X \rangle, \mathcal{U}(R))$: on ne regarde que les ensembles sous-jacents et on *oublie* les structures de monoïde et d'idéal. Pour alléger les notations, on choisira cependant celle de la définition. L'ARS associé permet de rapatrier les notions de terminaison, confluence et convergence :

Définition. On dit qu'un système de réécriture de mots *termine* si son ARS associé termine. On procède de la même façon pour les autres notions définies sur les ARS, y compris les formes normales. Dans le cas où (X, R) est convergent, on note $R(x)$ l'*unique* forme normale de $x \in \langle X \rangle$. \blacklozenge

Remarque. La terminologie employée mérite quelques explications.

1. La notion de module utilisée est plus souvent qualifiée de bimodule, puisque l'on a une opération à gauche et une à droite ; cependant, cette dernière appellation dépend fortement de la structure algébrique étudiée (ici celle de monoïde). Ainsi, dans le chapitre 3, nous étudierons une structure, celle d'opérade, ayant *deux* lois binaires ; ce qui donnerait, pour l'équivalent des *bimodules*, des *quadrmodules*. Nous préférons employer le terme de module pour un objet sur lequel un monoïde ou une opérade (ou n'importe quel autre objet algébrique) agit, de *toutes* les manières possibles et avec *toute* la compatibilité envisageable ; ce choix est préférable dans une optique d'unification en vue de réutiliser, plus loin, les définitions avec un minimum de changements puis, à terme, de dégager une structure commune de système de réécriture.
2. Nous avons parlé d'idéal pour un monoïde. Lorsque l'on parle d'un anneau, un idéal (bilatère) est une partie de l'anneau, alors qu'ici on considère des couples d'éléments du monoïde. Pourtant, la terminologie choisie est cohérente : la première

étape pour s'en apercevoir est de considérer qu'un élément x d'un anneau peut être vu comme un couple $(x, 0)$ et, réciproquement, à un couple (x, y) , on peut associer l'élément $x - y$; si on voit les couples comme des égalités, il est équivalent de dire que $x = y$ ou que $x - y = 0$. Ceci mène à la seconde observation : on veut définir, autant pour un anneau que pour un monoïde, un objet par lequel on peut quotienter celui de départ, tout en conservant sa structure; dans le cas des anneaux, il s'agit d'un idéal (bilatère), ce qui mène à appeler aussi idéal l'objet correspondant pour un monoïde.

3. Nous confondons les termes *égalité*, *relation* et *règle de réécriture*. Les deux premiers, plutôt utilisés en algèbre, désignent des objets de la forme $x = y$, utilisés pour engendrer des relations d'équivalence; le troisième qualifie des objets $x \rightarrow y$, utilisés pour engendrer des relations de réduction. Cependant, du point de vue algébrique, il n'y a aucune différence : ce sont tous des couples (x, y) , qu'on les note $x = y$ ou $x \rightarrow y$. La différence de notation a pour seul but de rappeler que leur utilisation est différente : dans le premier cas, on considère des relations d'équivalence, donc symétriques, ce qui est matérialisé par le fait que $x = y$ et $y = x$ engendrent la même relation. En revanche, en réécriture, on note plutôt $x \rightarrow y$ pour rappeler qu'on s'intéresse à la clôture réflexive-transitive et non symétrique : $x \rightarrow y$ et $y \rightarrow x$ n'engendrent pas la même relation \Rightarrow .

2.3 Contextes sur un monoïde

Les contextes fournissent une autre interprétation des relations de réduction, plus classique en réécriture. De manière informelle, ils sont construits comme les éléments sur lesquels portent la réécriture, mais en remplaçant un générateur par un symbole spécial, en général noté \square et représentant un emplacement libre. Un contexte agit sur un élément en remplaçant \square par l'élément en question.

Notons que cela ressemble à une notion d'application *linéaire*, c'est-à-dire utilisant exactement une copie de son argument. En effet, une application linéaire d'un espace vectoriel dans un autre est de la forme $x \mapsto ax$, où a est un scalaire : elle doit utiliser une fois son argument pour produire le résultat et ne peut pas disposer de plus de copies, contrairement, par exemple, à une application quadratique qui utilise deux fois son argument. De même, l'implication linéaire est une implication logique qui utilise une fois et une seule son hypothèse pour produire sa conclusion, contrairement à l'implication classique qui peut disposer d'une infinité de copies de cette hypothèse.

L'intérêt principal de l'introduction des contextes est d'éliminer encore plus l'utilisation de la structure de monoïde dans les constructions que nous faisons : il sera d'autant plus facile de remplacer l'adjonction (monoïde libre - oubli) par l'adjonction (opérade libre - oubli).

Avant de donner une définition plus formelle des contextes sur un monoïde, voyons ce que sont les morphismes de M -modules :

Définition. Soient M un monoïde ainsi que X et Y deux M -modules. Un *morphisme de M -modules de X vers Y* est une application $\varphi : X \longrightarrow Y$ telle que, pour tous $a \in M$ et $x \in X$, $\varphi(ax) = a\varphi(x)$ et $\varphi(xa) = \varphi(x)a$. Les M -modules et leurs morphismes s'organisent en une catégorie notée $M\text{-}\mathbf{MOD}$. \blacklozenge

Nous avons besoin de la notion de module libre sur un monoïde. On note \mathcal{U} le foncteur oubli qui, à tout M -module, associe son ensemble sous-jacent.

Définition. Soient M un monoïde et X un ensemble. On appelle *M -module libre engendré par X* tout couple (L, i) composé d'un M -module L et d'une application $i : X \longrightarrow \mathcal{U}L$ vérifiant : pour tout M -module A et toute application $f : X \longrightarrow A$, il existe un unique morphisme de M -modules $\bar{f} : L \longrightarrow A$ tel que le diagramme

$$\begin{array}{ccc} X & \xrightarrow{i} & \mathcal{U}L \\ & \searrow f \quad \oplus \quad \downarrow u\bar{f} & \\ & & \mathcal{U}L \end{array}$$

commute. \blacklozenge

Pour tout ensemble X , le module libre qu'il engendre existe ; nous allons en donner une construction.

On définit son ensemble sous-jacent MX comme l'ensemble des triplets (a, x, b) avec $x \in X$ et $a, b \in M$, puis les actions à gauche et à droite par $a(b, x, c) = (ab, x, c)$ et $(a, x, b)c = (a, x, bc)$. Dans le cas où $M = \langle Y \rangle$, on peut aussi interpréter MX comme l'ensemble des éléments de $\langle X \amalg Y \rangle$ contenant dans leur décomposition un et un seul élément de X .

L'application $i : X \longrightarrow \mathcal{U}MX$ est donnée par $i(x) = (*, x, *)$. En général, on enlève les parenthèses, de sorte que (a, x, b) est noté axb et $(*, x, *)$, tout simplement x .

Proposition 2.4. Soient M un monoïde et X un ensemble. Alors le couple (MX, i) est solution du problème de M -module libre engendré par X .

Démonstration. On vérifie que MX est un M -module : les deux premières et deux dernières relations proviennent des relations d'associativité et d'unité de M ; la troisième est vérifiée par les deux actions définies sur MX , puisqu'elles n'agissent pas au même endroit du triplet.

Maintenant, soient A un M -module et $f : X \rightarrow \mathcal{U}A$ une application. On définit $\bar{f} : MX \rightarrow A$ par $\bar{f}(a, x, b) = af(x)b$, ce qui donne bien un morphisme de M -modules. De plus, tout morphisme de M -modules $g : MX \rightarrow A$ doit vérifier $g(a, x, b) = ag(x)b$ car $(a, x, b) = a(*, x, *)b$, il est donc entièrement déterminé par ses valeurs sur les éléments de X , d'où l'unicité de \bar{f} . \diamond

Définition. Soit M un monoïde. Un *contexte sur M* est un élément du M -module libre engendré par $\{\square\}$, un ensemble réduit à un seul élément, noté \square . Le M -module des contextes sur M est noté \mathcal{CM} . \blacklozenge

D'après la construction du module libre engendré par $\{\square\}$, les éléments de \mathcal{CM} sont tous de la forme $x\square y$, avec $x, y \in M$. Les contextes agissent sur les éléments de M de la manière suivante : si $C \in \mathcal{CM}$ et $a \in M$, on note $C[a]$ l'élément xy , si $C = x\square y$.

On peut, de la même façon, définir l'action d'un contexte sur un autre contexte : pour $C, D \in \mathcal{CM}$, on note $C \circ D = xz\square ty$, si $C = x\square y$ et $D = z\square t$. Ainsi, pour tous $C, D \in \mathcal{CM}$ et $a \in M$, on a : $(C \circ D)[a] = C[D[a]]$. De plus, l'opération \circ est associative et admet $\square = *\square*$ comme élément neutre à gauche et à droite - tout cela est donné par la structure de monoïde de M .

Les contextes forment donc un monoïde \mathcal{CM} qui agit à gauche sur l'ensemble \mathcal{UM} sous-jacent à M . Ce monoïde est isomorphe au monoïde $M \times M^{op}$, d'ensemble sous-jacent $M \times M$ et de produit $(x, y).(z, t) = (xz, ty)$.

Remarque. Regardons les choses d'un point de vue un peu plus global. Les contextes sont des éléments de M avec un symbole \square ; on peut imaginer des 2-contextes, avec deux symboles \square , puis des n -contextes pour tout $n \geq 1$. Les éléments de M ont, eux, zéro symbole \square : ce sont des 0-contextes. En remarquant que l'on peut composer un n -contexte avec un m -contexte de n façons différentes (selon le \square du n -contexte que l'on remplace par le m -contexte) et que toutes ces compositions vérifient des propriétés d'associativité et d'unité, on arrive au constat suivant : *la réunion de tous les n -contextes, pour tout $n \in \mathbb{N}$, possède une structure d'opérade classique qui rappelle fortement celle dite des petits cubes*. Cette approche est un des candidats pour décrire l'essence de la réécriture.

Si cette remarque n'a pas encore de conséquence, en revanche, les (1-)contextes donnent une nouvelle interprétation des idéaux de M . Notons que l'action de \mathcal{CM} sur M s'étend à M^2 en une action diagonale : $C[(a, b)] = (C[a], C[b])$.

Proposition 2.5. *Soient M un monoïde et R une partie de M^2 . Les éléments de l'idéal de M engendré par R sont exactement les éléments de M^2 de la forme $C[\alpha]$ pour $\alpha \in R$ et $C \in \mathcal{CM}$.*

Démonstration. Soient $a, b \in M$ tels que $a \rightarrow_R b$. Alors, par définition de \rightarrow_R , il existe $\alpha \in R$ et $u, v \in M$ tels que $(a, b) = u\alpha v$. En posant $C = u\Box v$, on a bien $(a, b) = C[\alpha]$. Réciproquement, soient $\alpha \in R$ et $C \in \mathcal{CM}$. Comme C est un élément du M -module libre engendré par $\{\Box\}$, il existe $u, v \in M$ tels que $C = u\Box v$. Donc $C[\alpha] = u\alpha v$ et c'est donc un élément de l'idéal \rightarrow_R . \diamond

2.4 Présentation d'un monoïde et problème de mots

Nous allons aborder ici l'un des principaux champs d'application de la réécriture de mots. Nous verrons ensuite comment la réécriture fournit une réponse (partielle) à ce problème.

Nous avons vu la notion de monoïdes libres. Cependant, ils ne le sont pas tous : un groupe, même libre, ne l'est pas en tant que monoïde, sauf s'il est trivial. Cependant les monoïdes libres fournissent une manière pratique de décrire tous les autres, en leur adjoignant des *relations*.

On fixe un monoïde libre M et R une famille de relations sur M , c'est-à-dire d'éléments de M^2 . Cette famille induit une *congruence* \equiv_R sur M , qui n'est autre que $(R)^{rst}$. En effet, rappelons qu'une congruence sur M est une relation binaire réflexive, symétrique, transitive et qui est compatible avec la structure de monoïde de M : c'est donc un idéal de M qui est aussi une relation d'équivalence.

Donnons une version explicite de cette congruence. On sait déjà que $(R) = \rightarrow_R$ est l'idéal de M engendré par R . De plus, $(R)^{rt} = \twoheadrightarrow_R$ est la clôture réflexive-transitive de $(R) = \rightarrow_R$. Il faut alors prendre les clôtures symétrique puis transitive de $(R)^{rt} = \twoheadrightarrow_R$ pour obtenir $(R)^{rst} = (R)^{rst} = \equiv_R$. Ainsi, on a $a \equiv_R b$ si et seulement s'il existe $c_1, \dots, c_n \in M$ tels que :

$$a \twoheadrightarrow_R c_1 \leftarrow_R c_2 \twoheadrightarrow_R \dots \leftarrow_R c_n \twoheadrightarrow_R b.$$

Les congruences ont une propriété particulière que l'on peut présenter de manière informelle comme suit : étant donné un objet X possédant une structure algébrique, on peut effectuer son *quotient* par une congruence, sans perdre la structure.

Plus formellement, dans le cas des monoïdes : étant donnés un monoïde M et une congruence \equiv sur M , on peut construire un *monoïde*, appelé *quotient* de M par \equiv , dont

les éléments sont exactement ceux de M modulo la relation \equiv , ou encore les classes de \equiv -équivalence des éléments de M . Par exemple, sur le monoïde \mathbb{N} muni de l'addition, la relation \equiv , donnée par $x \equiv y$ si et seulement si x et y ont même parité, est une congruence ; le quotient de \mathbb{N} par cette relation donne un monoïde comprenant deux éléments, notés 0 et 1 et correspondant respectivement aux entiers pairs et impairs.

Donnons tout de même une définition de monoïde quotient :

Définition. Soient M un monoïde et \equiv une congruence sur M . On appelle *quotient de M par \equiv* tout couple (N, π) composé d'un monoïde N et d'un morphisme de monoïdes $\pi : M \rightarrow N$ vérifiant $\pi(x) = \pi(y)$ pour tous $x, y \in M$ tels que $x \equiv y$ et universels pour cette propriété, c'est-à-dire : pour tout monoïde N' et tout morphisme de monoïdes $\pi' : M \rightarrow N'$ tel que $\pi'(x) = \pi'(y)$ dès que $x \equiv y$, il existe un unique morphisme de monoïdes $\varphi : N \rightarrow N'$ tel que le diagramme

$$\begin{array}{ccc} M & \xrightarrow{\pi} & N \\ & \searrow \pi' & \downarrow \varphi \\ & & N' \end{array} \quad \text{⊙}$$

commute. ◆

On trouve une solution, notée M/\equiv ainsi : comme la relation \equiv est une relation d'équivalence, on peut considérer le quotient de M par \equiv , le tout dans $\mathbb{E}ns$; on note π la surjection canonique.

Le fait que \equiv soit aussi un idéal (c'est-à-dire une relation compatible avec la structure) assure que l'on peut transporter par π à l'ensemble M/\equiv des classes d'équivalence la structure de monoïde de M ; l'application π est alors automatiquement un morphisme de monoïdes.

De plus, tout morphisme de monoïdes $\pi' : M \rightarrow N$ qui identifie deux éléments d'une même classe d'équivalence se factorise de manière unique par π : si, pour tout élément $a \in M/\equiv$, on pose $\varphi(a) = \pi'(x)$, avec x un représentant quelconque de a dans M , on obtient $\pi' = \varphi \circ \pi$; enfin, par construction, l'application φ est un morphisme de monoïdes.

Exemple. Étant donnée une présentation (X, R) de monoïde, on lui associe le monoïde quotient de $\langle X \rangle$ par \equiv_R , noté aussi $\langle X \rangle/R$.

On arrive ainsi à la notion essentielle du paragraphe :

Définition. Un monoïde M admet une présentation (X, R) s'il est isomorphe au monoïde associé à (X, R) :

$$M \simeq \langle X \rangle / R.$$

On dit aussi que (X, R) est une présentation de M . Une présentation (X, R) est *finie* si X et R sont des ensembles finis. Deux présentations de monoïdes (X, R) et (Y, S) sont *équivalentes* si elles présentent le même monoïde, c'est-à-dire si :

$$\langle X \rangle / R \simeq \langle Y \rangle / S.$$



Le résultat suivant est essentiel :

Proposition 2.6. *Tout monoïde admet une présentation.*

Démonstration. Soit M un monoïde; on note $\mathcal{U}M$ son ensemble sous-jacent. Alors M est isomorphe au monoïde admettant la présentation $(\langle \mathcal{U}M \rangle, R)$ où R est l'ensemble des relations :

$$\left\{ \begin{array}{l} (a \cdot b, a \cdot_M b) \quad \text{pour tous } a \text{ et } b \text{ dans } M; \\ (*, *_M). \end{array} \right.$$

On a noté \cdot_M et $*_M$ la multiplication et l'unité de M et \cdot et $*$ celles de $\langle \mathcal{U}M \rangle$. Notons que la première famille de relations est la table de multiplication de M : la partie gauche du couple est le *mot* formé par les *lettres* a et b (donc un mot de deux lettres dans $\langle \mathcal{U}M \rangle$) et la partie droite est le résultat du produit dans M des éléments a et b de M (donc un élément de M vu comme mot de une lettre dans $\langle \mathcal{U}M \rangle$). Pour conclure, il suffit de montrer que M est solution du problème universel de quotient du monoïde $\langle \mathcal{U}M \rangle$ par la congruence engendrée par la partie R de $\langle \mathcal{U}M \rangle^2$, ce qui ne pose aucune difficulté. ◇

Exemple. Soit $\{a, b\}$ un ensemble à deux éléments. On construit un monoïde, noté $[a, b]$, ainsi : ses éléments sont tous les $a^m b^n$ pour m et n entiers; le produit est donné par $(a^m b^n)(a^p b^q) = a^{m+p} b^{n+q}$. On montre aisément que $[a, b]$ admet la présentation finie $\langle a, b \rangle / (ab, ba)$. Attention cependant : dans le cas général, un monoïde admet plusieurs présentations et il n'y a aucune raison pour que l'une d'entre elles soit finie.

Possédant une présentation (X, R) de M , on sait que l'on peut écrire tout élément a de M comme un mot sur l'alphabet X , c'est-à-dire un élément du monoïde libre $\langle X \rangle$. Cependant, une telle écriture n'est pas unique : en effet, avec ce point de vue, les éléments de M sont des classes d'équivalence de mots. Ainsi, en choisissant un mot de $\langle X \rangle$ pour

écrire un élément a de M , on a seulement sélectionné un représentant parmi d'autres de la classe d'équivalence a .

Le problème qui se pose alors est lié à ce choix : il s'agit de *décider* si deux éléments de $\langle X \rangle$ représentent le même élément de M . C'est ce que l'on appelle le *problème de mots* de M . On dit que M a un problème de mots *décidable* s'il existe une présentation (X, R) de M ainsi qu'un algorithme qui dise si deux éléments quelconques de $\langle X \rangle$ représentent ou non le même élément de M .

2.5 Problème de mots et réécriture

La réécriture peut apporter une réponse partielle au problème de mots d'un monoïde : on utilise ici le fait que la réécriture est un calcul de formes normales. En effet, supposons que (X, R) soit une présentation convergente. Alors, pour tout $u \in \langle X \rangle$, u possède une unique forme normale $R(u)$; comme tout enchaînement de réductions partant de u et arrivant à une forme normale aboutit forcément à $R(u)$ en un nombre fini d'étapes, on a un algorithme de calcul de $R(u)$ pour tout u . Il faut cependant ajouter l'hypothèse " R est fini", afin de s'assurer que l'on est arrivé à une forme normale : on passe en revue toutes les règles afin de voir si l'une d'entre elles peut s'appliquer à l'élément considéré. Le résultat suivant nous assure que cet algorithme fonctionne :

Proposition 2.7. *Soient u et v deux éléments d'une présentation (X, R) convergente. Alors $u \equiv_R v$ si et seulement si $R(u) = R(v)$.*

Démonstration. Comme (X, R) est convergente, si $u \rightarrow_R v$, alors $R(u) = R(v)$; on en déduit que, si $u \twoheadrightarrow_R v$, alors $R(u) = R(v)$; puis que, si $u \equiv_R v$, alors $R(u) = R(v)$. Réciproquement, si $R(u) = R(v)$, alors $u \twoheadrightarrow_R R(u) = R(v) \leftarrow_R v$ et donc $u \equiv_R v$. \diamond

Dans le cas d'une présentation finie et convergente, on obtient donc un critère pour décider si $u \equiv_R v$, c'est-à-dire si u et v sont identifiés dans $\langle X \rangle / R$: on calcule les formes normales de u et v et on les compare - la finitude est nécessaire pour vérifier si un mot est une forme normale ou non.

Donc, si M est un monoïde et que l'on peut trouver une présentation convergente finie d'un monoïde, on est sûr de pouvoir résoudre son problème de mots. Cependant, ce n'est pas un critère complet : certains monoïdes ont un problème de mots décidable mais n'admettent pas de présentation convergente finie, comme l'a montré Squier dans [Squ87].

Malgré cela, la recherche d'une présentation convergente pour un monoïde est intéressante : elle donne quand même une condition suffisante à la décidabilité du problème de mots. Parmi les outils permettant d'en trouver, nous allons nous intéresser aux *procédures*

de complétion. Pour simplifier, disons qu'une telle procédure prend, en entrée, une présentation (X, R) et livre une famille R' de relations sur $\langle X \rangle$ de sorte que (X, R) et (X, R') soient équivalentes, c'est-à-dire que $\equiv_R = \equiv_{R'}$, et que (X, R') soit convergente. Ainsi, si l'on connaît une présentation d'un monoïde M , le but d'une procédure de complétion est de produire une présentation *convergente* de ce même monoïde M .

Soit (X, R) une présentation finie. Une procédure de complétion construit progressivement une suite croissante, pour l'inclusion, $(R_n)_{n \in \mathbb{N}}$ de familles de règles de réécriture de telle sorte que \rightarrow_{R_n} termine et que $\equiv_{R_n} = \equiv_R$ pour tout n ; de plus, on veut que cette suite converge vers une limite R' telle que $\rightarrow_{R'}$ soit confluente. Idéalement, on souhaiterait que $(R_n)_{n \in \mathbb{N}}$ soit stationnaire. À la fin, on a donc une présentation convergente du monoïde $\langle X \rangle / \equiv_R$.

On a besoin de plusieurs outils pour faciliter la construction d'une telle procédure. En premier lieu, il est souhaitable de disposer d'une condition suffisante (et vérifiable) pour que $R \cup \{\alpha\}$ termine si R termine : ceci sera fait en vérifiant que la source de α est plus grande que son but, pour une relation d'ordre sur $\langle X \rangle$ ayant des propriétés bien choisies.

Deuxièmement, on ne va pas vérifier que tous les branchements sont joignables : cela conduirait à une infinité d'opérations. En fait, il existe un critère simple pour qu'une présentation noethérienne soit confluente : que toutes les *paires critiques* engendrées par ses règles soient confluentes. Nous y reviendrons, mais disons que les paires critiques sont les branchements locaux *minimaux* et *non triviaux* de la présentation.

2.6 Terminaison et ordres de réduction

Rappelons qu'un *ordre strict* sur un ensemble X est une relation binaire $>$ sur X qui possède les propriétés suivantes :

- antiréflexivité : pour tout $x \in X$, $x \not> x$;
- transitivité : pour tous $x, y, z \in X$, si $x > y$ et $y > z$, alors $x > z$.

L'idée est la suivante : supposons que l'on dispose d'un ordre strict $>$ sur $\langle X \rangle$ qui soit compatible avec la structure de monoïde et tel que, pour toute règle α de R , on ait $s(\alpha) > t(\alpha)$. Si $a \rightarrow_R b$, c'est qu'il existe deux mots c et d ainsi qu'une règle α tels que $(a, b) = c\alpha d$; or $s(\alpha) > t(\alpha)$ et $>$ est compatible avec le produit, donc $a > b$. Dans ce cas, tout chemin de réduction est strictement décroissant pour $>$. Si, de plus, l'ARS $(\langle X \rangle, >)$ termine, on sera assuré que (X, R) termine, en appliquant 1.3.

Définition. Un *ordre de réduction* sur un monoïde M est un idéal $>$ de M qui est aussi un ordre strict sur (l'ensemble sous-jacent à) M et tel que $(M, >)$ termine. \blacklozenge

On a donc, en reformulant le théorème 1.3 :

Corollaire 2.8. *Une présentation (X, R) termine si et seulement s'il existe un ordre de réduction sur $\langle X \rangle$ contenant R .*

Donnons un exemple courant d'ordre de réduction : l'ordre *deglex*. Pour le définir, introduisons d'abord l'ordre *lexicographique*.

On suppose que X est un ensemble muni d'un ordre strict $>$ qui termine ; on l'étend à $\langle X \rangle$ en posant $x_1 \dots x_n >_{\text{lex}} y_1 \dots y_m$ (où les x_i et les y_j sont dans X) si l'on est dans l'un des deux cas suivants :

1. $n > m$ et $x_i = y_i$ pour tout $i \in \{1 \dots m\}$;
2. il existe un $i \in \{1 \dots m\}$ tel que $x_j = y_j$ pour tous les $j \in \{1 \dots i-1\}$ et $x_i > y_i$.

On a donc aussi que $* <_{\text{lex}} u$ pour tout mot u . Si, par exemple, $X = \{x, y\}$, l'ordre lexicographique associé à $x < y$ vérifie :

$$* <_{\text{lex}} x <_{\text{lex}} xx <_{\text{lex}} xxy <_{\text{lex}} xy <_{\text{lex}} y <_{\text{lex}} yx <_{\text{lex}} yy.$$

Notons que cet ordre possède la propriété d'être total si l'ordre sur X est total ; remarquons que c'est celui utilisé dans le dictionnaire pour classer les mots (avec $X = \{a < b < c < \dots < z\}$). Cependant, cet ordre strict ne termine pas en général. En effet, avec le même exemple, on a le chemin de réduction infini suivant :

$$y >_{\text{lex}} xy >_{\text{lex}} x^2y >_{\text{lex}} x^3y >_{\text{lex}} \dots >_{\text{lex}} x^ny >_{\text{lex}} x^{n+1}y >_{\text{lex}} \dots$$

Pour corriger ce défaut, on construit l'ordre *deglex* à partir de l'ordre lexicographique, mais en prenant d'abord en compte la longueur des mots. On commence toujours avec un ordre strict $>$ qui termine sur X . Puis on pose $x_1 \dots x_n >_{\text{deglex}} y_1 \dots y_m$ si $n > m$ ou si $n = m$ et $x_1 \dots x_n >_{\text{lex}} y_1 \dots y_n$. On a alors, avec le même exemple :

$$* <_{\text{deglex}} x <_{\text{deglex}} y <_{\text{deglex}} xx <_{\text{deglex}} xy <_{\text{deglex}} yx <_{\text{deglex}} yy <_{\text{deglex}} xxx <_{\text{deglex}} \dots$$

C'est aussi un ordre total si $>$ l'est sur X . Mais c'est en plus un ordre de réduction sur $\langle X \rangle$. Notons que ces ordres possèdent des duaux : on commence par comparer les dernières lettres puis on remonte : ils sont en général notés $>_{\text{revlex}}$ et $>_{\text{degrevlex}}$.

Proposition 2.9. *Pour tout ensemble X muni d'un ordre strict $>$ qui termine, la relation $>_{\text{deglex}}$ est un ordre de réduction sur $\langle X \rangle$.*

Démonstration. On doit montrer que $>_{\text{deglex}}$ est un ordre strict sur $\langle X \rangle$ et que c'est un idéal de $\langle X \rangle$ qui termine.

1. Idéal de $\langle X \rangle$: soient $a, b \in \langle X \rangle$ tels que $a >_{\text{deglex}} b$ et $u, v \in \langle X \rangle$. Comme $\langle X \rangle$ est libre, on a, en notant $|a|$ la longueur de a :

$$\begin{cases} |uav| = |u| + |a| + |v| \\ |ubv| = |u| + |b| + |v| \end{cases}$$

On a donc $|uav| > |ubv|$ si $|a| > |b|$. Supposons alors que $|a| = |b|$. Alors $|uav| = |ubv|$; comme on a $a >_{\text{lex}} b$, l'inégalité $uav >_{\text{lex}} ubv$ est vérifiée. Dans tous les cas, on a bien $uav >_{\text{deglex}} ubv$.

2. Antiréflexivité : supposons qu'il existe $a \in \langle X \rangle$ tel que $a >_{\text{deglex}} a$. Soient x_1, \dots, x_n les éléments de X tels que $a = x_1 \dots x_n$. On a nécessairement $|a| = |a|$ et donc $a >_{\text{lex}} a$. Ce qui implique qu'il existe un i tel que $x_i > x_i$, ce qui est impossible car $>$ est un ordre strict.

3. Transitivité : soient $a, b, c \in \langle X \rangle$ tels que $a >_{\text{deglex}} b$ et $b >_{\text{deglex}} c$. Quatre cas sont possibles selon que $|a| > |b|$ ou $|a| = |b|$ et que $|b| > |c|$ ou $|b| = |c|$. Si $|a| > |b|$ ou $|b| > |c|$, on a $|a| > |c|$ et donc $a >_{\text{deglex}} c$. Regardons le cas où $|a| = |b| = |c|$: soient $x_1 \dots x_n, y_1 \dots y_n$ et $z_1 \dots z_n$ les décompositions respectives de a, b et c en éléments de X . Il existe un $i \in \{1 \dots n\}$ et un $j \in \{1 \dots n\}$ tels que :

$$\begin{cases} x_1 \dots x_{i-1} = y_1 \dots y_{i-1} & \text{et} & x_i > y_i \\ y_1 \dots y_{j-1} = z_1 \dots z_{j-1} & \text{et} & y_j > z_j \end{cases}$$

En posant $k = \min\{i, j\}$, on a bien $x_1 \dots x_{k-1} = z_1 \dots z_{k-1}$ et $x_k > z_k$ et donc $a >_{\text{lex}} c$.

4. Terminaison : on va montrer, par récurrence sur la longueur, qu'il n'existe pas de suite strictement décroissante pour $>_{\text{deglex}}$ dans $\langle X \rangle$. Soit $a \in \langle X \rangle$ tel que $|a| = 0$: alors $a = *$ qui est le plus petit élément de $\langle X \rangle$. Maintenant, soit $a \in \langle X \rangle$ tel que $|a| > 0$; on suppose que l'on a montré que l'ordre termine en tout b tel que $|b| < |a|$.

Par l'absurde, supposons qu'il existe une suite $(a_n)_{n \in \mathbb{N}}$ d'éléments de $\langle X \rangle$ tels que $a = a_0$ et $a_n >_{\text{deglex}} a_{n+1}$ pour tout n . Par définition, on a une suite décroissante $(|a_n|)_n$ dans \mathbb{N} : elle est donc stationnaire. Pour simplifier, supposons qu'elle est constante. Toujours par définition, il existe donc des suites $(b_n)_n, (c_n)_n$ et $(d_n)_n$ d'éléments de $\langle X \rangle$ tels que, pour tout n , on ait $a_n = b_n c_n$ et $a_{n+1} = b_n d_n$ avec $d_n = *$ ou $c_n = x_n c'_n$ et $d_n = y_n d'_n$ avec $x_n > y_n$.

Si, pour tout n , on a $b_n \neq *$, alors il existe un $x \in X$ et une suite $(a'_n)_n$ tels que $a_n = x a'_n$ pour tout n . Ainsi, la suite $(a'_n)_n$ est un chemin de réduction infini dans

$(\langle X \rangle, >_{\text{deglex}})$ avec $|a'_0| < |a|$, ce qui est impossible par hypothèse de récurrence. Il existe donc un n_0 tel que $a_{n_0} = x'_0 b'_0$ et $a_{n_0+1} = y'_0 c'_0$: on peut recommencer à partir de n_0 afin d'extraire de $(a_n)_n$ une sous-suite $(a_{k_n})_n$ vérifiant, pour tout n :

$$\begin{cases} a_{k_n} = x'_n b'_n \\ a_{k_{n+1}} = y'_n c'_n \\ x'_n > y'_n \end{cases}$$

avec les x'_n et y'_n dans X et les b'_n et c'_n dans $\langle X \rangle$. Or, par liberté de $\langle X \rangle$, on a nécessairement $y'_n = x'_{n+1}$: on a donc obtenu une suite $(x'_n)_n$ d'éléments de X , strictement décroissante pour $>$, ce qui est impossible puisque l'ordre strict de X a été supposé terminant.

◇

Pour terminer sur les ordres, rappelons qu'il existe une généralisation de l'ordre *deglex* : l'ordre *lexicographique pondéré*. On suppose donnés un ordre strict $>$ sur X ainsi qu'une application *poids* $|\cdot| : X \rightarrow \mathbb{N}^*$, associant à chaque lettre un entier non nul. On étend cette application en un morphisme de monoïdes $|\cdot| : \langle X \rangle \rightarrow \mathbb{N}^*$ et on définit l'ordre lexicographique pondéré $>_{\text{lp}}$ engendré par $>$ et $|\cdot|$ sur $\langle X \rangle$ par $a >_{\text{lp}} b$ si l'on est dans l'un des deux cas suivants :

1. $|a| > |b|$;
2. $|a| = |b|$ et $a >_{\text{lex}} b$.

Cet ordre $>_{\text{lp}}$ est aussi un ordre de réduction sur $\langle X \rangle$ dès que $>$ est un ordre qui termine sur X . De plus, c'est aussi un ordre total si $>$ l'est sur X . Enfin, il s'agit bien d'une généralisation de l'ordre *deglex*, puisque ce dernier est un ordre lexicographique pondéré engendré par une fonction poids constante : par exemple, la longueur, qui associe le même entier, 1, à chaque lettre de X .

2.7 Confluence et paires critiques

Comme nous l'avons dit précédemment, les paires critiques correspondent aux branchements locaux, minimaux et non triviaux. C'est au niveau de ces branchements que se décide la confluence locale s'un système de réécriture : c'est ce que dit le *théorème des paires critiques*.

Nous allons, dans un premier temps, donner la vision classique des paires critiques : on étudie toutes les formes possibles des branchements locaux, que l'on peut classer alors en deux familles, dont une correspond aux paires critiques. Puis, nous verrons une approche

algébrique qui, si elle ne donne pas la forme des paires critiques, est en revanche transposable à d'autres types de réécriture où l'étude des formes des branchements locaux est très complexe, voire impossible, comme dans le cas des présentations d'opérades.

2.7.1 La présentation classique

Par définition, on a confluence d'une présentation (X, R) si tous ses branchements sont confluents. On a déjà vu que, grâce au lemme de Newman, on peut se limiter à l'étude des branchements *locaux* dans le cas où (X, R) termine. Cependant, une présentation non triviale possède toujours une infinité de branchements locaux. Il faut essayer de restreindre l'étude à une plus petite classe de branchements locaux.

Pour donner l'intuition, remarquons que, si (a, b, c) est un branchement local, alors, pour tous $u, v \in \langle X \rangle$, le triplet (uav, ubv, ucv) est aussi un branchement local. De plus, si (a, b, c) est confluent alors (uav, ubv, ucv) l'est aussi : si d ferme (a, b, c) , alors (udv) ferme (uav, ubv, ucv) . Ainsi, on a envie de factoriser au maximum les branchements locaux pour en obtenir des minimaux : la confluence locale sera alors équivalente à celle de ces branchements minimaux.

Cependant, ces branchements minimaux sont toujours en nombre infini. Il faut encore restreindre cette famille. C'est en suivant cette idée que l'on distingue deux sortes de branchements locaux, selon la forme du branchement minimal contenu dans chacun d'eux. Une des familles est composée de branchements locaux qui sont toujours confluents. L'autre est celle qui nous intéresse.

Soit (a, b_1, b_2) un branchement local. Par définition, il existe des règles $\alpha_1, \alpha_2 \in R$ et des mots $u_1, v_1, u_2, v_2 \in \langle X \rangle$ tels que :

$$\begin{cases} (a, b_1) = u_1 \alpha_1 v_1 \\ (a, b_2) = u_2 \alpha_2 v_2 \end{cases}$$

Or, $\langle X \rangle$ est le monoïde libre engendré par l'ensemble X . Donc, il existe $x_1, \dots, x_n \in X$ tels que $a = x_1 \dots x_n$; de plus, cette décomposition est unique. On en déduit qu'il existe des entiers $0 \leq i_1 < j_1 \leq n$ et $0 \leq i_2 < j_2 \leq n$ vérifiant :

$$\begin{cases} u_k = x_1 \dots x_{i_k} \\ s(\alpha_k) = x_{i_k+1} \dots x_{j_k} \\ v_k = x_{j_k+1} \dots x_n \end{cases}$$

pour $k \in \{1, 2\}$ et avec la convention $u_k = *$ si $i_k = 0$ et $v_k = *$ si $j_k = n$. Toujours par liberté de $\langle X \rangle$, on a aussi :

$$b_k = x_1 \dots x_{i_k} t(\alpha_k) x_{j_k+1} \dots x_n.$$

On va distinguer des cas selon les positions relatives de i_1, j_1, i_2, j_2 .

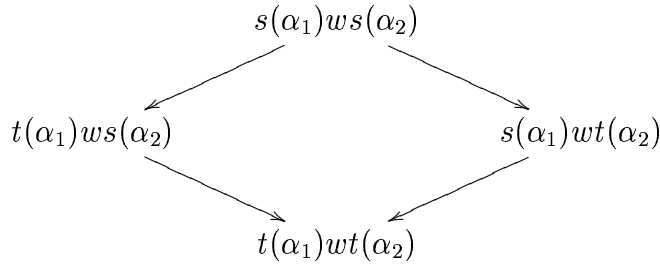
1. Si $i_1 < j_1 \leq i_2 < j_2$: dans ce cas, les $s(\alpha_1)$ et $s(\alpha_2)$ sont séparés dans a . C'est-à-dire :

$$\begin{cases} a = u_1 s(\alpha_1) w s(\alpha_2) v_2 \\ b_1 = u_1 t(\alpha_1) w s(\alpha_2) v_2 \\ b_2 = u_1 s(\alpha_1) w t(\alpha_2) v_2 \end{cases}$$

avec $w = x_{j_1+1} \dots x_{i_2}$ (et $w = *$ si $j_1 = i_2$). Le « cœur » du branchement est le triplet (a', b'_1, b'_2) :

$$\begin{cases} a' = s(\alpha_1) w s(\alpha_2) \\ b'_1 = t(\alpha_1) w s(\alpha_2) \\ b'_2 = s(\alpha_1) t(\alpha_2) \end{cases}$$

Ce branchement est toujours confluent (et (a, b_1, b_2) aussi) :

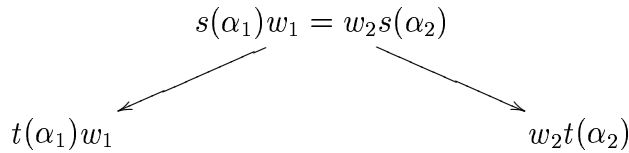


Ainsi, tout branchement de ce type est confluent : on les appelle branchements *triviaux*.

2. Si $i_1 \leq i_2 < j_1 \leq j_2$: on a un chevauchement entre les $s(\alpha_1)$ et $s(\alpha_2)$ dans a . Formellement :

$$\begin{cases} a = u_1 s(\alpha_1) w_1 v_2 = u_1 w_2 s(\alpha_2) v_2 \\ b_1 = u_1 t(\alpha_1) w_1 v_2 \\ b_2 = u_1 w_2 t(\alpha_2) v_2 \end{cases}$$

avec $w_1 = x_{j_1+1} \dots x_{j_2}$ et $w_2 = x_{i_1+1} \dots x_{i_2}$. Alors (a, b_1, b_2) est confluent si le branchement suivant l'est :



La confluence de ce branchement minimal dépend de la forme des règles de R . On dit qu'il est *issu d'une paire critique* ; nous verrons la définition plus loin.

3. Si $i_1 \leq i_2 < j_2 \leq j_1$: on a une inclusion de $s(\alpha_2)$ dans $s(\alpha_1)$. C'est-à-dire :

$$\begin{cases} a = u_1 s(\alpha_1) v_1 = u_1 w s(\alpha_2) w' v_1 \\ b_1 = u_1 t(\alpha_1) v_1 \\ b_2 = u_1 w t(\alpha_2) w' v_1 \end{cases}$$

La confluence de (a, b_1, b_2) dépend donc de celle de :

$$\begin{array}{ccc} & s(\alpha_1) = w s(\alpha_2) w' & \\ \swarrow & & \searrow \\ t(\alpha_1) & & w t(\alpha_2) w' \end{array}$$

Encore une fois, la confluence de ce branchement dépend de la forme des règles de R . Ce branchement est lui aussi *issu d'une paire critique*.

Les autres cas se ramènent aux précédents en regardant le branchement local (a, b_2, b_1) au lieu de (a, b_1, b_2) . Nous avons donc vu que les branchements locaux se rangeaient en deux sortes :

- les branchements triviaux, dans lesquels les deux règles agissent sur deux parties *distinctes* du mot de départ ;
- les branchements issus de paires critiques, dans lesquels les zones d'action des deux règles s'intersectent.

Nous allons à présent définir l'objet d'étude essentiel pour la confluence d'une présentation :

Définition. Une *paire critique* d'une présentation (X, R) est une donnée :

$$(a, (u_1, v_1), \alpha_1, (u_2, v_2), \alpha_2) \in \langle X \rangle \times \langle X \rangle^2 \times R \times \langle X \rangle^2 \times R$$

vérifiant :

1. $a = u_1 s(\alpha_1) v_1 = u_2 s(\alpha_2) v_2$;
2. $u_1 = *$ ou $u_2 = *$;
3. $v_1 = *$ ou $v_2 = *$;
4. il n'existe pas de w dans $\langle X \rangle$ tel que $u_1 = s(\alpha_2)w$ ou $u_2 = s(\alpha_1)w$;
5. $(\alpha_1 \neq \alpha_2)$ ou (l'un des u_1, u_2, v_1, v_2 est différent de $*$).

On dit d'une telle paire critique qu'elle est *engendrée par les règles* (α_1, α_2) et qu'elle est de *source* a . Le *branchement local associé* à une telle paire critique est :

$$(a, u_1 t(\alpha_1) v_1, u_2 t(\alpha_2) v_2).$$

Une paire critique est dite *confluente* si son branchement local associé l'est. Enfin, on note $\text{cp}(X, R)$, ou simplement $\text{cp}(R)$, l'ensemble des paires critiques de (X, R) . \blacklozenge

Remarque. D'après les conditions à vérifier, le branchement engendré par une paire critique possède l'une des formes suivantes :

- $(a, t(\alpha_1), t(\alpha_2))$ avec α_1 et α_2 deux règles distinctes ayant même source ;
- $(a, ut(\alpha_1), t(\alpha_2)v)$ avec $u \neq *, v \neq *, s(\alpha_1) = wv$ et $s(\alpha_2) = uw$ pour un certain $w \in \langle X \rangle$;
- $(a, t(\alpha_1)v, ut(\alpha_2))$ avec $u \neq *, v \neq *, s(\alpha_1) = uw$ et $s(\alpha_2) = wv$ pour un certain $w \in \langle X \rangle$;
- $(a, ut(\alpha_1)v, t(\alpha_2))$ avec u ou v distinct de $*$;
- $(a, t(\alpha_1), ut(\alpha_2)v)$ avec u ou v distinct de $*$.

On remarque aussi que, si $p = (a, (u_1, v_1), \alpha_1, (u_2, v_2), \alpha_2)$ est une paire critique engendrée par (α_1, α_2) , alors $p^{-1} = (a, (u_2, v_2), \alpha_2, (u_1, v_1), \alpha_1)$ est une paire critique engendrée par (α_2, α_1) . On constate qu'une paire critique p est confluente si et seulement si p^{-1} l'est : si le branchement associé à p est fermé par un élément d , alors d convient aussi pour fermer le branchement associé à p^{-1} .

L'étude de cas menée aboutit à :

Lemme 2.10 (des paires critiques). *Si \mathbf{b} est un branchement local d'une présentation (X, R) de monoïde, alors au moins l'une des deux assertions suivantes est vraie :*

1. *le branchement local \mathbf{b} est confluent ;*
2. *il existe un branchement local \mathbf{g} de (X, R) ainsi que $c, d \in \langle X \rangle$ tels que $\mathbf{b} = u\mathbf{g}v$ avec \mathbf{g} le branchement local associé à une paire critique de (X, R) .*

On a utilisé la notation $u(a, b, c)v = (uav, ubv, ucv)$. On en déduit :

Théorème 2.11 (des paires critiques). *Un présentation de monoïde est localement confluente si et seulement si toutes ses paires critiques sont confluentes.*

Démonstration. Soit (X, R) une présentation que l'on suppose localement confluente. Alors, par définition, tous ses branchements locaux sont confluent, y compris ceux qui sont associés à des paires critiques. Réciproquement, si toutes les paires critiques de (X, R) sont confluentes et que \mathbf{b} est un branchement local : d'après le lemme des paires critiques, le seul cas à étudier est celui où $\mathbf{b} = u\mathbf{g}v$ avec \mathbf{g} le branchement local associé à une paire critique p . Comme p est confluente, c'est que, par définition, \mathbf{g} l'est. Or, on a remarqué que si \mathbf{g} était confluent, le branchement $\mathbf{b} = u\mathbf{g}v$ l'était aussi. \blacklozenge

Puis, en utilisant le lemme de Newman :

Corollaire 2.12. *Un présentation est convergente si et seulement si elle termine et si toutes ses paires critiques sont confluentes.*

Remarque. En utilisant les contextes, on peut donner une autre définition (totalement équivalente) de paire critique. Une *paire critique* d'une présentation (X, R) est une donnée

$$(a, C_1, \alpha_1, C_2, \alpha_2) \in \langle X \rangle \times \mathcal{C}\langle X \rangle \times R \times \mathcal{C}\langle X \rangle \times R$$

vérifiant les conditions suivantes :

1. $a = C_1[s(\alpha_1)] = C_2[s(\alpha_2)]$;
2. C_1 ou C_2 est de la forme $u\Box$ avec $u \in \langle X \rangle$;
3. C_1 ou C_2 est de la forme $\Box v$ avec $v \in \langle X \rangle$;
4. il n'existe pas de $w \in \langle X \rangle$ tel que $C_1 = s(\alpha_2)w\Box$ ou $C_2 = s(\alpha_1)w\Box$
5. $\alpha_1 \neq \alpha_2$ ou $C_1 \neq \Box$ ou $C_2 \neq \Box$.

2.7.2 Une approche algébrique des paires critiques

Commençons par examiner la structure algébrique des branchements locaux. On fixe une présentation de monoïde (X, R) .

Définition. On note $\mathcal{B}(X, R)$ l'ensemble des branchements locaux de (X, R) . On dit qu'un branchement local (a, b, c) de (X, R) est *engendré* par le couple de règles (α, β) s'il existe des contextes C et D tels que $(a, b) = C[\alpha]$ et $(a, c) = D[\beta]$. On note $\mathcal{B}(X, \alpha, \beta)$ l'ensemble formés de tels branchements locaux de (X, R) . \blacklozenge

On a vu, dans le paragraphe précédent, que, si \mathbf{b} est un branchement local, alors, pour tout contexte C , $C[\mathbf{b}]$ est un branchement local. De plus, si \mathbf{b} est engendré par (α, β) , alors $C[\mathbf{b}]$ l'est aussi (en étendant diagonalement l'action de C). Autrement dit :

Lemme 2.13. *Pour tout couple (α, β) de règles de R , l'ensemble $\mathcal{B}(X, \alpha, \beta)$ est un sous- $\langle X \rangle$ -module du $\langle X \rangle$ -module $\langle X \rangle^3$, défini comme l'ensemble des triplets d'éléments de $\langle X \rangle$ avec les actions diagonales $u(a, b, c) = (ua, ub, uc)$ et $(a, b, c)u = (au, bu, cu)$. De même, $\mathcal{B}(X, R)$ est un sous- $\langle X \rangle$ -module de $\langle X \rangle^3$.*

On va maintenant montrer que $\mathcal{B}(X, \alpha, \beta)$ est engendré par une famille G de *branchements minimaux*, c'est-à-dire qu'il existe une partie G de $\mathcal{B}(X, \alpha, \beta)$ telle que, pour tout branchement \mathbf{b} engendré par (α, β) , il existe un $\mathbf{g} \in G$ et un $C \in \mathcal{C}\langle X \rangle$ tels que $\mathbf{b} = C[\mathbf{g}]$. On va, en fait, démontrer un résultat plus général :

Proposition 2.14. *Soit $n \geq 1$ un entier ; on note $\langle X \rangle^n$ le $\langle X \rangle$ -module des n -uplets d'éléments de $\langle X \rangle$, muni des actions diagonales de $\langle X \rangle$. Alors tout sous- $\langle X \rangle$ -module A de $\langle X \rangle^n$ possède une unique famille génératrice minimale (c'est-à-dire que, si on lui enlève un élément, la famille obtenue n'est plus génératrice).*

Démonstration. On définit la relation binaire \sqsupset sur A par $a \sqsupset b$ s'il existe un contexte $C \in \mathcal{C}\langle X \rangle$ différent de \square et tel que $a = C[b]$. On va montrer que l'ARS (A, \sqsupset) termine.

On associe à tout élément a de $\langle X \rangle^n$ un entier $|a|$ égal à la longueur de la première composante de a : si $a = (a^1, \dots, a^n)$ avec tous les a^i dans $\langle X \rangle$, on pose $|a|$ la longueur de a^1 , c'est-à-dire le nombre d'éléments de X apparaissant dans son écriture (ce nombre est bien défini car $\langle X \rangle$ est libre).

Alors, si $a, b \in A$ sont tels que $a \sqsupset b$, on a $|a| > |b|$. En effet, par définition de \sqsupset , il existe $C \neq \square$ tel que $a = C[b]$. Comme $C \neq \square$, on a $C = u \square v$ avec $u, v \in \langle X \rangle$, l'un des deux devant être différent de $*$. On en conclut que les premières composantes de a et b sont reliées par $a^1 = ub^1v$ et donc que $|a| > |b|$, toujours parce que $\langle X \rangle$ est libre.

On a donc un morphisme strict d'ARS $|\cdot| : (A, \sqsupset) \longrightarrow (\mathbb{N}, >)$. Or $(\mathbb{N}, >)$ termine et donc (A, \sqsupset) aussi. On pose G l'ensemble des formes normales de (A, \sqsupset) . Comme (A, \sqsupset) termine, tout élément de A possède (au moins) une forme normale pour \sqsupset , donc G est bien une famille génératrice de A .

Supposons que G n'est pas minimale : il existe un $g \in G$ tel que $G \setminus \{g\}$ est génératrice. En particulier, il existe $g' \in G$ tel que $g' \neq g$ et $g = C[g']$ pour un certain contexte C . Comme $g' \neq g$, on a forcément $C \neq \square$ et donc $g \sqsupset g'$, ce qui est impossible puisque g est une forme normale de (A, \sqsupset) .

Il reste à voir que G est unique. Soit H une autre famille génératrice. Alors, H contient forcément les formes normales de (A, \sqsupset) : soit g une telle forme normale ; comme H est génératrice, il existe $h \in H$ et $C \in \mathcal{C}\langle X \rangle$ tels que $g = C[h]$. Comme g est une forme normale de (A, \sqsupset) , on en déduit $C = \square$; par suite, $g = h$ et $g \in H$. \diamond

En appliquant ce résultat à $\mathcal{B}(X, \alpha, \beta)$, on en déduit qu'il existe une unique famille génératrice minimale de $\mathcal{B}(X, \alpha, \beta)$: ses éléments sont appelés les *branchements minimaux de (X, R) engendrés par (α, β)* . On appelle *branchement minimal de (X, R)* tout branchement local qui est un branchement minimal de (X, R) engendré par un certain couple (α, β) de règles. On obtient :

Proposition 2.15. *Une présentation est localement confluyente si et seulement si tous ses branchements minimaux sont confluentes.*

Parmi ceux-ci, il y en a qui n'interviennent pas dans la confluence locale car ils sont toujours confluents. En effet, soient α et β deux éléments de l'idéal de $\langle X \rangle$ engendré par R . On peut construire deux branchements locaux :

$$\begin{array}{ccc} s(\alpha)s(\beta) & \longrightarrow & t(\alpha)s(\beta) \\ \downarrow & & \downarrow \\ s(\alpha)t(\beta) & & t(\alpha)s(\beta) \end{array} \quad \text{et} \quad \begin{array}{ccc} s(\alpha)s(\beta) & \longrightarrow & s(\alpha)t(\beta) \\ \downarrow & & \downarrow \\ t(\alpha)s(\beta) & & t(\alpha)s(\beta) \end{array}$$

Ces deux branchements sont confluents puisque :

$$t(\alpha)s(\beta) \rightarrow t(\alpha)t(\beta) \quad \text{et} \quad s(\alpha)t(\beta) \rightarrow t(\alpha)t(\beta).$$

Or il peut s'agir de branchements minimaux : c'est le cas si $\alpha, \beta \in R$. On peut donc les retirer des branchements minimaux sans conséquence pour l'étude de la confluence locale. On définit alors :

Définition. Un branchement local de (X, R) est dit *trivial* s'il est d'une des formes :

$$(s(\alpha)s(\beta), t(\alpha)s(\beta), s(\alpha)t(\beta)) \quad \text{ou} \quad (s(\alpha)s(\beta), s(\alpha)t(\beta), t(\alpha)s(\beta))$$

avec α et β dans l'idéal de $\langle X \rangle$ engendré par R . Un branchement minimal non trivial de (X, R) est appelé *branchement critique*. \blacklozenge

Par suite :

Proposition 2.16. *Une présentation est localement confluente si et seulement si tous ses branchements critiques sont confluents.*

Reste à faire le lien avec les paires critiques :

Proposition 2.17. *Les paires critiques d'une présentation (X, R) sont les*

$$(a, C, \alpha, D, \beta) \in \langle X \rangle \times \mathcal{C}\langle X \rangle \times R \times \mathcal{C}\langle X \rangle \times R$$

tels que :

- Les trois éléments a , $C[s(\alpha)]$ et $D[s(\beta)]$ sont égaux.
- Le branchement local $(a, C[t(\alpha)], D[t(\beta)])$ est un branchement critique de (X, R) .
- Si $\alpha = \beta$, alors $a \neq s(\alpha)$.

Cette approche ne donne pas la forme des paires critiques. En revanche, elle permet d'extraire la structure de monoïde des définitions : elle se prête donc bien à une transposition vers un autre cadre, comme celui des opérades, que nous étudierons au chapitre 3. Il serait intéressant d'étudier si cette approche permet de retrouver la forme explicite des paires critiques, mais cela reste à explorer.

2.8 Procédures de complétion pour les présentation de monoïdes

2.8.1 La procédure basique

Nous allons présenter une première procédure de complétion, dite *basique*. Notons qu'elle possède de nombreuses variantes ainsi que de nombreux raffinements, y compris des transpositions à d'autres cadres comme, par exemple, la procédure de complétion de Huet pour la réécriture de termes, voir [Hue81]. Historiquement, la procédure basique fut exposée dans [KB70] ; on peut aussi la trouver dans [BN98], ainsi que la plupart de ce qui est présenté ici. Mentionnons aussi des évolutions permettant, dans le cas des termes, d'effectuer une complétion modulo certaines équations, c'est-à-dire dans un quotient, comme exposé dans [JK86].

Il est à noter que la procédure suivie est la même que pour l'algorithme de Buchberger, servant à calculer une base de Gröbner pour un idéal dans une algèbre de polynômes : il s'agit aussi d'une procédure de complétion, mais où l'on a remplacé la catégorie des monoïdes par celle des k -algèbres, les paires critiques se nommant alors S -polynômes - voir [Buc79].

La procédure 1 est l'une des formes possibles de la procédure basique. Elle prend, en entrée, une présentation (X, R) finie et munie d'un ordre de réduction $>$ contenant R . Trois comportements sont possibles : 1) L'algorithme termine avec sortie **Échec**. 2) L'algorithme termine avec sortie une famille finie R' de règles de réécriture. 3) L'algorithme ne termine pas.

Cette procédure fonctionne ainsi : à chaque passage dans la boucle, on calcule toutes les paires critiques de la présentation courante. Pour chacune d'entre elles, on détermine des formes normales des deux "côtés" du branchement. Si elles sont distinctes mais comparables pour l'ordre choisi, on rajoute formellement la règle correspondante, de telle sorte que la nouvelle présentation termine toujours et que la paire critique d'origine soit maintenant confluyente.

Remarque. La condition de compatibilité entre l'ordre de réduction et les règles peut être reportée à l'initialisation de la procédure. On commencera alors avec une présentation (X, R) et un ordre de réduction $>$ qui ne contient pas R *a priori*, puis on testera, au début, si chaque règle α de R vérifie : $s(\alpha) > t(\alpha)$ ou $t(\alpha) > s(\alpha)$; dans le premier cas, on laisse α inchangée, dans le second, on lui substitue $\alpha^{-1} = (t(\alpha), s(\alpha))$. Si l'une des règles ne vérifie pas l'une des deux inégalités, on termine sur un échec. Dans le cas contraire, on oriente toutes les règles comme décrit : on obtient une nouvelle famille \tilde{R} de règles telles que $>$ contienne \tilde{R} et que $\equiv_{\tilde{R}} = \equiv_R$.

Procédure 1 La procédure basique de complétion.

$R_0 \leftarrow R$;
 $i \leftarrow 0$;
Répéter
 $R_{i+1} \leftarrow R_i$;
 $P_i \leftarrow \text{cp}(R_i)$;
 Tant que $(P_i \neq \emptyset)$ **faire**
 Choisir $p = (a, C, \alpha, D, \beta)$ dans P_i ;
 $P_i \leftarrow P_i \setminus \{p, p^{-1}\}$;
 Calculer des R_i -formes normales b et c de $C[t(\alpha)]$ et de $D[t(\beta)]$;
 Si $(b \neq c)$ **alors**
 Selon que
 $b > c$: $R_{i+1} \leftarrow R_{i+1} \cup (b, c)$;
 $b < c$: $R_{i+1} \leftarrow R_{i+1} \cup (c, b)$;
 Sinon : **Terminer** avec sortie Échec ;
 Fin Selon que
 $i \leftarrow i + 1$;
 Fin Si
 Fin Tant que
Jusqu'à ce que $(R_i = R_{i-1})$
 $R' \leftarrow R_i$;
Terminer avec sortie R' .

On a le résultat suivant :

Théorème 2.18. *Si la procédure basique de complétion termine et donne une famille finie R' de règles, alors (X, R') est convergente et $\equiv_{R'} = \equiv_R$. Si la procédure ne termine pas, on a une présentation convergente (X, R') telle que $\equiv_{R'} = \equiv_R$, avec :*

$$R' = \bigcup_{i=0}^{+\infty} R_i.$$

Démonstration. Supposons qu'il n'y pas d'échec dans l'exécution. Il est clair qu'à chaque passage de la boucle, on part d'une famille R_i de règles telles que (X, R_i) termine et $\equiv_{R_i} = \equiv_R$; on rajoute à R_i une famille S_i de règles telles que :

- la présentation $(X, R_i \amalg S_i)$ termine ;
- toutes les paires critiques de (X, R_i) sont confluentes dans $(X, R_i \amalg S_i)$;
- on a les égalités $\equiv_{R_i \amalg S_i} = \equiv_{R_i} = \equiv_R$.

Si la procédure termine, c'est qu'il existe un i tel que $S_i = \emptyset$: on a alors (X, R_i) convergente et $\equiv_{R_i} = \equiv_R$.

Si la procédure ne termine pas, la seule difficulté est de vérifier que (X, R') est confluente avec :

$$R' = \bigcup_{i=0}^{+\infty} R_i.$$

Soit p une paire critique de R' engendrée par deux règles α et β de R' . Soient i et j deux indices tels que $\alpha \in R_i$ et $\beta \in R_j$. Comme $(R_k)_{k \in \mathbb{N}}$ est une suite croissante pour l'inclusion, en prenant $n = \max\{i, j\}$, on a $\alpha, \beta \in R_n$. Donc p est confluente dans R_{n+1} et donc dans R' . \diamond

2.8.2 Limitations de la procédure basique

Notons que si l'ordre de réduction choisi est total, alors il n'y a jamais d'échec lors de l'exécution de la procédure : en effet, dans ce cas, pour deux éléments b et c de $\langle X \rangle$ tels que $b \neq c$, on a toujours $b > c$ ou $b < c$. Dans le cas d'un monoïde libre $\langle X \rangle$, il est aisé d'obtenir un ordre de réduction total : par exemple, l'ordre *deglex* engendré par un ordre total $>$ sur X . En revanche, dans des situations plus complexes, comme pour les termes ou les opérades, il n'y a pas de méthode connue pour obtenir un ordre de réduction total dans le cas général. Cependant, ce n'est pas le défaut majeur de cette procédure : nous allons en évoquer deux.

1. Le premier défaut concerne toutes les procédures de complétion : en effet, indépendamment de la procédure, le choix de l'ordre de réduction est très important, car deux ordres différents peuvent produire deux comportements différents d'une même procédure sur une même présentation. Illustrons l'impact du choix de l'ordre de réduction à l'aide d'un exemple bien connu. On considère la présentation (X, R) où :

$$\begin{cases} X = \{a, b, c, d, e\} \\ R = \{(ab, c), (ba, e), (bbbb, d)\} \end{cases}$$

On applique la procédure basique avec l'ordre *deglex* $>$ engendré par $a < b < c < d < e$. On remarque que $>$ contient R . Le premier passage dans la boucle produit, entre autre :

- La règle $ca \rightarrow ae$, issue de la paire critique de sommet aba créée par un conflit entre $ab \rightarrow c$ et $ba \rightarrow e$.
- La règle $cbbb \rightarrow ad$, produite par un conflit entre $ab \rightarrow c$ et $bbbb \rightarrow d$ en $abbbb$.
- La règle $bbbe \rightarrow da$, provenant de la superposition des sources de $ba \rightarrow e$ et $bbbb \rightarrow d$ en $bbba$.
- La règle $dbbb \rightarrow bbba$, qui est créée par la règle $bbbb \rightarrow d$ en $bbbbbb$.

Au second passage dans la boucle, on obtient les deux règles supplémentaires suivantes, parmi d'autres :

- En cbb , les règles $cbbb \rightarrow ad$ et $bbbe \rightarrow da$ produisent $cda \rightarrow ade$.
- En $dbbe$, les règles $dbbb \rightarrow bbbd$ et $bbbe \rightarrow da$ créent $bbbde \rightarrow dda$.

Notons qu'il faut avoir toutes les règles produites par le premier passage pour être sûr que ces deux règles sont bien ajoutées à la présentation par la procédure. On montre ensuite, par récurrence sur $n \geq 1$, que la procédure ajoute, au $(n + 1)^e$ passage dans la boucle, les deux règles suivantes :

- La règle $cd^n a \rightarrow ad^n e$, produite en $cb^3 d^{n-1} e$ par $cb^3 \rightarrow ad$ et $b^3 d^{n-1} e \rightarrow d^n a$.
- La règle $b^3 d^n e \rightarrow d^{n+1} a$, produite en $db^3 d^{n-1} e$ par $db^3 \rightarrow b^3 d$ et $b^3 d^{n-1} e \rightarrow d^n a$.

La procédure ne termine donc pas en (X, R) muni de l'ordre *deglex* engendré par $a < b < c < d < e$.

Cependant, considérons l'ordre lexicographique pondéré $>'$ engendré par $a < b < c < d < e$ et par les poids $|a| = |b| = 1$, $|c| = |e| = 3$ et $|d| = 5$. Alors, R doit être remplacé par R^{-1} pour que $>'$ contienne les règles. Pour (X, R^{-1}) muni de $>'$, la procédure s'arrête dès le premier passage : les règles de R^{-1} ne créent pas de paire critique. On a donc une présentation convergente équivalente à celle de départ : le choix de l'ordre de réduction est donc très important.

2. Le deuxième défaut est, quant à lui, inhérent à la procédure basique. C'est d'ailleurs à cause de lui qu'elle n'est jamais utilisée en pratique. On peut s'en convaincre en la comparant à la même procédure à laquelle on a ajouté une fonction : à l'initialisation et à chaque création de règle, on réduit toutes les règles entre elles. Considérons l'exemple du monoïde libre à deux générateurs, a et b , muni de l'ordre *deglex* engendré par $b > a$ et des trois règles :

$$abb \rightarrow_1 ba, \quad bb \rightarrow_2 b, \quad abba \rightarrow_3 aba.$$

Lors du premier passage dans la boucle de la procédure basique, les règles 1 et 2 forment deux paires critiques : l'une est de sommet abb et engendre la règle $ba \rightarrow_4 ab$. La seconde est de sommet $abbb$ et crée, selon les choix effectués, l'une ou l'autre des règles $bab \rightarrow_5 ba$ et $bab \rightarrow_{5'} ab$. Enfin, les règles 1 et 3 ont un conflit en $abba$, qui engendre $baa \rightarrow_6 aba$. Le deuxième passage vérifie que la présentation à 6 relations ainsi obtenue est convergente.

Cependant, on s'aperçoit que quatre règles sont inutiles, car dérivables à partir des deux autres : ainsi 2 et 4 suffisent. Or, une procédure étendue avec simplification des règles aurait, tout d'abord, éliminé la règle 3 comme conséquence de 2. Puis, elle aurait remplacé 1 par le couple (ab, ba) , réorienté en $ba \rightarrow ab$. Le premier passage de boucle

aurait alors confirmé que cette présentation à deux règles est convergente.

Deux limitations majeures apparaissent donc :

- Sans simplification des règles, on multiplie inutilement leur nombre et donc celui des paires critiques à examiner : c'est un problème d'efficacité.
- Comme nous l'avons vu dans l'exemple, les règles obtenues après complétion dépendent de choix effectués durant l'exécution de la procédure (les règles 5 et 5'). Avec la simplification des règles, ces choix n'ont aucune influence sur le résultat final, dont l'unicité est assurée.

Si la simplification des règles apparaît comme une amélioration indispensable de la procédure de complétion, sa correction est beaucoup plus difficile à prouver : il faut montrer que la nouvelle procédure produit bien des présentations convergentes *équivalentes* à la présentation de départ. Le paragraphe suivant est une courte synthèse des travaux axiomatisant la notion de procédure de complétion et fournissant des outils pour démontrer qu'elles fonctionnent bien.

2.8.3 Procédures de complétion abstraites et preuves

Une description axiomatique des procédures de complétion a été introduite dans [BDH86]. Ce paragraphe rappelle ces travaux ; on pourra aussi se référer à [DJ90] ou à [BN98].

L'idée est de décrire les opérations élémentaires que peut utiliser une procédure de complétion, puis de définir une procédure de complétion comme une composée de telles opérations.

Définition. On fixe un ensemble X ainsi qu'un ordre de réduction $>$ sur $\langle X \rangle$. On définit la relation \vdash sur l'ensemble des couples de parties de $\langle X \rangle^2$ en posant $(E_1, R_1) \vdash (E_2, R_2)$ si l'on peut appliquer l'une des *règles d'inférence* suivantes :

1. Effacer : $(E \amalg \{(s, s)\}, R) \vdash (E, R)$.
2. Composer : $(E, R \amalg \{(s, t)\}) \vdash (E, R \amalg \{(s, u)\})$ si $(t, u) \in (R)$.
3. Simplifier : $(E \amalg \{(s, t)\}, R) \vdash (E \amalg \{(u, v)\}, R)$ si $(s = v \text{ et } (t, u) \in (R))$ ou $(t = v \text{ et } (s, u) \in (R))$.
4. Orienter : $(E \amalg \{(s, t)\}, R) \vdash (E, R \amalg \{(u, v)\})$ si $((s, t) = (u, v) \text{ ou } (s, t) = (v, u) \text{ et } u > v)$.
5. Comprimer : $(E, R \amalg \{(s, t)\}) \vdash (E \amalg \{(u, t)\}, R)$ s'il existe $(l, r) \in R$ tel que $(s, u) = C[(l, r)]$ et $(C \neq \square \text{ ou } t > u)$.
6. Dédire : $(E, R) \vdash (E \amalg \{(s, t)\}, R)$ si R possède un branchement critique de la forme $s \leftarrow_R u \rightarrow_R t$. ◆

L'idée est la suivante : chaque couple (E, R) représente un ensemble E d'égalités à orienter et un ensemble R de règles déjà construites. Chacune des règles d'inférence peut transformer un tel couple (E, R) en produisant (E', R') de telle sorte que le résultat suivant soit vrai :

Lemme 2.19. *Soient X un ensemble, $>$ un ordre de réduction sur $\langle X \rangle$ et E, E', R et R' des parties de $\langle X \rangle^2$ telles que $(E, R) \vdash (E', R')$. Alors :*

- Les congruences $\equiv_{E \amalg R}$ et $\equiv_{E' \amalg R'}$ coïncident sur $\langle X \rangle$.
- Si $>$ contient R , alors il contient aussi R' .

Une preuve de ce résultat peut être trouvée dans [BN98].

Le but d'une procédure de complétion est alors, étant donnée une entrée (E, R) où R termine (éventuellement $R = \emptyset$), de produire une suite $(E_n, R_n)_n$ de telle sorte que $(E_n, R_n) \vdash (E_{n+1}, R_{n+1})$ pour tout $n < N$, la suite étant constante avec $E_n = \emptyset$ et R_n convergent pour $n \geq N$. Ce but n'étant bien sûr pas accessible pour toute entrée, on définit :

Définition. Une *procédure de complétion* (sur X muni d'un ordre de réduction $>$) est une application qui, à tout couple (E, R) formé de deux parties de $\langle X \rangle^2$ avec $>$ contenant R , associe une famille $(E_n, R_n)_{n \in I}$, avec $I = \{0 \dots N\}$ ou $I = \mathbb{N}$, telle que :

- chaque E_n et chaque R_n est une partie de $\langle X \rangle^2$, avec $E_0 = E$ et $R_0 = R$;
- pour tout $n \geq 1$ dans I , $(E_{n-1}, R_{n-1}) \vdash (E_n, R_n)$.

Une telle famille $(E_n, R_n)_n$ s'appelle une *exécution* de la procédure. Étant fixée une telle exécution, on définit ses ensembles E_ω d'*égalités persistantes* et R_ω de *règles persistantes* ainsi :

$$E_\omega = \bigcup_{n \in I} \bigcap_{k \geq n} E_k \quad \text{et} \quad R_\omega = \bigcup_{n \in I} \bigcap_{k \geq n} R_k.$$

On dit d'une exécution (E_n, R_n) qu'elle :

- *réussit* si $E_\omega = \emptyset$ et si (X, R_ω) est convergent et équivalent à $(X, E \amalg R)$;
- *échoue* si $E_\omega \neq \emptyset$;
- est *équitable* si pour tout branchement critique (a, b, c) de R_ω , l'un des E_n , $n \in I$, contient (b, c) ou (c, b) .

Une procédure est *correcte* si toute exécution réussit ou échoue et *équitable* si chacune de ses exécutions l'est. ◆

D'après la définition, ce sont les procédures de complétion correctes qui nous intéressent. Le résultat suivant donne une condition suffisante pour cela :

Théorème 2.20. *Toute procédure de complétion équitable est correcte.*

Pour démontrer ce résultat, nous rappelons les étapes utilisées dans [BN98], sans entrer dans les détails : ceci permet de parler des *preuves d'égalités*. Avant tout, on fixe un ensemble X muni d'un ordre de réduction $>$, une procédure de complétion et son exécution $(E_n, R_n)_{n \in I}$ sur (E, R) avec R contenu dans $>$. On note :

$$E_\infty = \bigcup_{n \in I} E_n \quad \text{et} \quad R_\infty = \bigcup_{n \in I} R_n.$$

On définit alors :

Définition. Soient u et v deux éléments de $\langle X \rangle$. Une *preuve* de $u = v$ dans $E_\infty \cup R_\infty$ est une famille finie (u_0, \dots, u_n) d'éléments de $\langle X \rangle$ tels que $u_0 = u$, $u_n = v$ et, pour tout $k \in \{0 \dots n-1\}$:

$$(u_k, u_{k+1}) \in (E_\infty \amalg R_\infty)^s.$$

Autrement dit, pour tout $k \in \{0 \dots n-1\}$, on est dans l'un des cas $u_k \rightarrow_{E_\infty} u_{k+1}$, $u_k \leftarrow_{E_\infty} u_{k+1}$, $u_k \rightarrow_{R_\infty} u_{k+1}$, $u_k \leftarrow_{R_\infty} u_{k+1}$. Chacun des couples (u_k, u_{k+1}) est appelé *étape de preuve*. Deux preuves d'une même égalité sont dites *équivalentes*. Une preuve est dite *par réécriture dans R_ω* s'il existe un $k \in \{0 \dots n\}$ tel que, pour $l < k$, les étapes sont toutes de la forme $u_l \rightarrow_{R_\omega} u_{l+1}$ et, pour tout $l \geq k$, on a $u_l \leftarrow_{R_\omega} u_{l+1}$.

◆

Le but est de montrer que toute preuve dans $E_\infty \cup R_\infty$ est équivalente à une preuve par réécriture dans R_ω . Pour ce faire, on commence par définir une notion de coût des preuves. Notons que ces définitions nécessitent les notions de monoïde commutatif libre et de multiordre qui seront présentées au chapitre 4.

Définition. Soient s et t deux éléments de $\langle X \rangle$ tels que $(s, t) \in (E_\infty \amalg R_\infty)^s$. On associe au couple (s, t) son *coût*, un triplet (a, u, v) formé d'un élément a du monoïde commutatif $[\langle X \rangle]$ librement engendré par $\langle X \rangle$ et de deux éléments u et v de $\langle X \rangle$, définis ainsi :

1. si $s \rightarrow_{E_\infty} t$ ou si $s \leftarrow_{E_\infty} t$, on pose $c(s, t) = (s + t, *, *)$;
2. si $(s, t) = C[(l, r)]$, $(l, r) \in R_\infty$, on pose $c(s, t) = (s, l, t)$;
3. si $(t, s) = C[(l, r)]$, $(l, r) \in R_\infty$, on pose $c(s, t) = c(t, s) = (t, l, s)$.

Le *coût* d'une preuve $P = (u_0, \dots, u_n)$ dans $E_\infty \cup R_\infty$ est l'élément $c(P)$ du monoïde commutatif libre engendré par $[\langle X \rangle] \times \langle X \rangle^2$ donné par :

$$c(P) = \sum_{k=0}^{n-1} c(u_k, u_{k+1}).$$

◆

Deux remarques s'imposent :

- Le coût des étapes de réduction est bien défini. En effet, il n'y a pas de conflit entre les cas (2) et (3) puisque, pour tout n , on sait que R_n est contenu dans l'ordre de réduction $>$. Donc, chaque règle (l, r) de R_∞ vérifie $l > r$, il est donc impossible d'avoir, à la fois, $s \rightarrow_{R_\infty} t$ et $t \rightarrow_{R_\infty} s$.
- Dans le premier cas, on a fixé $c(s, t) = (s + t, *, *)$, mais on aurait pu remplacer chaque $*$ par n'importe quelle autre élément de $\langle X \rangle$.

Il faut à présent décrire comment comparer deux preuves.

Définition. On définit la relation \succ sur $[\langle X \rangle] \times \langle X \rangle^2$ en posant $(a, u, v) \succ (a', u', v')$ si l'une des conditions suivantes est vérifiée :

1. $a > a'$ où $>$ est le multiordre engendré sur $[\langle X \rangle]$ par l'ordre de réduction fixé sur $\langle X \rangle$;
2. $a = a'$ et $u = C[u']$, $C \neq \square$;
3. $a = a'$, $u = u'$ et $v > v'$, pour l'ordre de réduction sur $\langle X \rangle$.

On étend \succ en son multiordre sur $[[\langle X \rangle] \times \langle X \rangle^2]$, toujours noté \succ , et on pose, pour deux preuves P et P' , $P \succ P'$ si $c(P) \succ c(P')$. ♦

On trouvera, dans [BN98], la preuve du résultat suivant :

Proposition 2.21. *La relation \succ définie sur les preuves est un ordre strict qui termine. De plus, pour toute preuve P dans $E_\infty \cup R_\infty$ qui n'est pas une preuve par réécriture dans R_ω , il existe une preuve équivalente P' dans $E_\infty \cup R_\infty$ telle que $P \succ P'$.*

Cette proposition a les conséquences suivantes :

Corollaire 2.22. *Soit $(E_n, R_n)_{n \in I}$ une exécution équitable et qui n'échoue pas d'une procédure de complétion. Alors :*

1. *Toute preuve dans $E_\infty \cup R_\infty$ est équivalente à une preuve par réécriture dans R_ω .*
2. *Les présentations (X, R_ω) et $(X, E \amalg R)$ sont équivalentes.*
3. *La présentation (X, R_ω) est convergente.*

Le théorème 2.20 est une conséquence de ce dernier résultat.

Chapitre 3

Présentations d'opérades

Cette partie a pour but de définir et d'étudier ce qui peut être vu comme une généralisation de la notion de présentation de monoïde que nous venons de rappeler. Il s'agit des *présentations d'opérades*¹ pour lesquelles nous allons développer exactement la même théorie que dans le cas des monoïdes. En fait, le seul travail consiste à remplacer :

1. La catégorie \mathbf{ENS} des ensembles par la catégorie \mathbf{SGN} des *signatures*.
2. La catégorie \mathbf{MON} des monoïdes par la catégorie \mathbf{OP} des *opérades*.
3. Le foncteur monoïde libre $\mathbf{ENS} \xrightarrow{\langle \cdot \rangle} \mathbf{MON}$ par le foncteur *opérade libre* $\mathbf{SGN} \xrightarrow{\mathcal{L}} \mathbf{OP}$.

Nous verrons que ces présentations généralisent les présentations de monoïdes (systèmes de réécriture de mots) et de monoïdes commutatifs (réseaux de Petri). De plus, elles ont de forts liens avec les systèmes de réécriture de termes : il sera démontré, au chapitre 5, qu'un système de réécriture de termes linéaire à gauche peut être simulé par une présentation d'opérade. Enfin, comme il sera discuté au chapitre 6, on peut espérer qu'un équivalent en dimension supérieure de cette structure pourra simuler des systèmes de réécriture d'ordre supérieur comme, par exemple, le λ -calcul.

Ce travail s'inscrit dans le programme annoncé par Albert Burroni dans [Bur93] : les présentations de monoïdes spécifient des calculs de dimension 2 sur des 1-catégories particulières et les présentations d'opérades, des calculs de dimension 3 sur des 2-catégories particulières ; l'étude des présentations en dimension supérieure peut permettre d'inclure le λ -calcul dans cette classification.

Mais commençons par étudier ce que sont les *opérades* et en quoi les monoïdes en sont des cas particuliers.

¹Comme nous le verrons plus loin, la notion d'opérade introduite ici est une version généralisée des opérades planaires ensemblistes que l'on peut trouver dans la littérature.

3.1 Des mots aux opérateurs

La structure de monoïde peut être vue comme l'archétype des structures associatives et unitaires. Une généralisation naturelle est celle de *(petite) catégorie* : un monoïde est une catégorie avec un seul objet. On pourrait donc envisager de généraliser les présentations de monoïdes par celles de *monoïdes avec plusieurs objets*, c'est-à-dire de petites catégories. Cependant, on va considérer des catégories munies d'une structure supplémentaire, dite *monoïdale* et, plus précisément, celles que l'on appelle *opéades*.

Essayons d'amener la structure. Considérons une présentation de monoïde (X, R) , mais où les éléments qui nous intéressent sont, non pas des mots seuls, mais des familles finies de mots, dans lesquelles on peut, à chaque étape de réduction, réécrire un mot et un seul. On est dans la situation d'une machine qui doit effectuer des opérations de réécriture sur une famille finie de mots, mais qui ne peut en faire qu'une à la fois.

D'un point de vue algébrique, on travaille dans $\langle X \rangle^n$, où n est le nombre de mots. Cet ensemble peut être muni d'une structure de monoïde induite par celle de $\langle X \rangle$: si (a_1, \dots, a_n) et (b_1, \dots, b_n) en sont des éléments, leur produit est effectué composante par composante, ce qui donne $(a_1 b_1, \dots, a_n b_n)$. Le neutre de $\langle X \rangle^n$ est $(*, \dots, *)$.

Alors, on considère comme règles de réécriture les couples $((a_1, \dots, a_n), (b_1, \dots, b_n))$ tels que $a_i = b_i$ pour tous les i sauf pour un j tel que (a_j, b_j) est dans R . Notons que l'on n'a pas pris comme règles tous les éléments de R^n puisque l'on ne peut effectuer qu'une opération à la fois.

Modifions les notations : $a_1 \otimes \dots \otimes a_n$ pour (a_1, \dots, a_n) , $a \circ b$ pour ab si a et b sont des n -uplets de mots, n pour le neutre de $\langle X \rangle^n$. Remarquons que $\langle X \rangle^1 = \langle X \rangle$ et que $\langle X \rangle^0 = \{0\}$, le monoïde trivial. Soit \mathbb{X} la réunion de tous les $\langle X \rangle^n$: examinons la structure dont on peut la munir.

Comme on vient de le voir, on peut multiplier deux éléments de \mathbb{X} pourvu qu'ils soient dans le même $\langle X \rangle^n$; de plus cette multiplication est associative et admet un élément neutre à gauche et à droite : l'élément neutre n de $\langle X \rangle^n$. On pose $\text{Ob } \mathbb{X} = \mathbb{N}$ et, pour tout couple (m, n) d'entiers :

$$\mathbb{X}(m, n) = \begin{cases} \langle X \rangle^n & \text{si } m = n \\ \emptyset & \text{sinon.} \end{cases}$$

On reconnaît en \mathbb{X} une petite catégorie, dont nous rappelons la définition.

Définition. Une *petite catégorie* \mathbb{C} est la donnée :

1. d'un ensemble $\text{Ob } \mathbb{C}$ dont les éléments sont les *objets* de \mathbb{C} ;
2. d'un ensemble $\mathbb{C}(x, y)$, pour tout couple (x, y) d'objets, dont les éléments sont les *flèches* de \mathbb{C} de *source* x et de *but* y ;
3. d'une application $c_{x,y,z} : \mathbb{C}(x, y) \times \mathbb{C}(y, z) \longrightarrow \mathbb{C}(x, z)$, pour tout triplet (x, y, z) d'objets, appelée *composition* ;
4. d'une flèche $1_x \in \mathbb{C}(x, x)$, pour tout objet x , appelée l'*identité* de x .

On demande à la composition d'être associative et d'admettre les identités comme éléments neutres locaux, à gauche et à droite. On utilise indifféremment les notations $f \in \mathbb{C}(x, y)$ et $f : x \longrightarrow y$; pour une telle flèche, on pose $s(f) = x$ et $t(f) = y$: ainsi, en notant $\text{Fl } \mathbb{C}$ pour l'ensemble de toutes les flèches de \mathbb{C} , on obtient deux applications *source* et *but* $s, t : \text{Fl } \mathbb{C} \longrightarrow \text{Ob } \mathbb{C}$. On pratique aussi les abus suivants si aucune confusion n'est possible :

- on note $g \circ f$ au lieu de $c_{x,y,z}(f, g)$;
- les identités sont notées comme leurs objets.

Ainsi, avec ces notations, les relations imposées à la composition et aux identités s'écrivent :

- *Associativité* : pour toutes flèches f, g et h de \mathbb{C} telles que $t(f) = s(g)$ et $t(g) = s(h)$, on a l'égalité $h \circ (g \circ f) = (h \circ g) \circ f$.
- *Unité* : pour toute flèche f de \mathbb{C} , on a $f \circ s(f) = t(f) \circ f = f$.

Dans une catégorie, les flèches ayant mêmes source et but sont aussi appelées des *endomorphismes* de l'objet source et but. Deux flèches d'une catégorie sont dites *parallèles* si elles ont même source et même but. \blacklozenge

Exemples. L'exemple type de petite catégorie est celui des chemins d'un graphe. On peut aussi définir des (grandes) catégories, comme \mathbf{ENS} , \mathbf{MON} ou \mathbf{CAT} , les catégories des ensembles, des monoïdes et des petites catégories.

Dans \mathbb{X} , on peut construire, pour tous m et n , un produit :

$$\begin{aligned} \langle X \rangle^m \times \langle X \rangle^n &\longrightarrow \langle X \rangle^{m+n} \\ (a_1 \otimes \cdots \otimes a_m, b_1 \otimes \cdots \otimes b_n) &\longmapsto a_1 \otimes \cdots \otimes a_m \otimes b_1 \otimes \cdots \otimes b_n \end{aligned}$$

On vérifie que, pour toute flèche a de \mathbb{X} , on a $a \otimes 0 = 0 \otimes a = a$ et que, pour toutes flèches a et b , la relation dite *d'échange* est valide :

$$(t(a) \otimes b) \circ (a \otimes s(b)) = (a \otimes t(b)) \circ (s(a) \otimes b) = a \otimes b.$$

Ainsi, la catégorie \mathbb{X} est munie d'une structure monoïdale (stricte) :

Définition. Une *structure monoïdale stricte* sur une catégorie \mathbb{C} est une donnée (\otimes, I) où $\otimes : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$ est un foncteur et I est un objet de \mathbb{C} , tels que \otimes est associatif et I est neutre à gauche et à droite pour \otimes . Une catégorie munie d'une structure monoïdale (stricte) est une catégorie monoïdale (stricte). Le foncteur \otimes est appelé *produit monoïdal* de \mathbb{C} et l'objet I l'*unité* du produit monoïdal. Si (\mathbb{C}, \otimes, I) est une petite catégorie monoïdale, alors l'ensemble $\text{Ob } \mathbb{C}$ des objets de \mathbb{C} , muni de la restriction du produit monoïdal et de l'unité, est un monoïde, dit *monoïde des objets de \mathbb{C}* . ♦

Remarquons que cette donnée est équivalente à celle d'applications :

$$\text{Ob } \mathbb{C} \times \text{Ob } \mathbb{C} \longrightarrow \text{Ob } \mathbb{C} \quad \text{et} \quad \text{Fl } \mathbb{C} \times \text{Fl } \mathbb{C} \longrightarrow \text{Fl } \mathbb{C},$$

toutes deux notées \otimes , ainsi que d'un objet I , le tout soumis aux relations suivantes :

$$s(f \otimes g) = s(f) \otimes s(g), \quad t(f \otimes g) = t(f) \otimes t(g), \quad I \otimes f = f \otimes I = f,$$

ainsi que la relation d'échange déjà citée :

$$(t(a) \otimes b) \circ (a \otimes s(b)) = (a \otimes t(b)) \circ (s(a) \otimes b) = a \otimes b.$$

Nous allons voir à présent que la catégorie monoïdale \mathbb{X} est engendrée par une signature : celle-ci joue le rôle de l'ensemble des générateurs d'un monoïde.

Définition. Rappelons qu'un graphe G est donné par un ensemble $\text{Ob } G$ d'*objets*, un ensemble $\text{Fl } G$ de *flèches* ainsi que deux applications *source* et *but* $s, t : \text{Fl } G \longrightarrow \text{Ob } G$.

Soit Γ un ensemble. Une *signature Γ -colorée* est un graphe dont les objets sont les éléments du monoïde libre $\langle \Gamma \rangle$. Les éléments de Γ sont appelés *couleurs*.

Dans le cas où $\Gamma = \{*\}$, et donc où $\langle \Gamma \rangle = \mathbb{N}$, le monoïde additif des entiers naturels, on parle de *signatures monochromes* ou même, par abus, de *signatures*. La *valence* d'une flèche est le couple formé par sa source et son but ; quant aux flèches $n \longrightarrow 1$, dans le cas monochrome, on dit qu'elles sont d'*arité* n . ♦

Pour presque toute la suite, on ne s'intéressera qu'au cas monochrome. Pour ce chapitre, on ne traitera donc que ce cas ; cependant, les versions colorées s'en déduisent aisément.

Une signature Σ peut être vue, en première approximation, comme un ensemble d'*opérateurs* abstraits : la source d'une flèche est alors le nombre de ses entrées et son but le nombre de ses sorties ; par exemple, une flèche $0 \longrightarrow 1$ représente une constante, alors qu'une flèche $1 \longrightarrow 0$ est un effaceur. Attention, cette intuition n'est pas forcément juste : dans la suite, on pourra avoir des flèches à deux entrées et zéro sortie qui ne représentent pas forcément l'effacement simultané de deux éléments.

Une manière de se représenter ces opérateurs est de les voir comme des « bouts de circuits » ayant autant de « fils » en entrée que leur source et en sortie que leur but. De manière pratique, on les dessine sous la forme de diagrammes dits de Penrose, couramment utilisés en physique ou en théorie des nœuds ; la figure 3.1 montre des exemples de ces représentations, la convention utilisée étant de placer les entrées en haut et les sorties en bas. Notons que ces diagrammes sont aussi utilisables dans le cas Γ -coloré, en étiquetant chaque fil avec l'élément correspondant de Γ , d'où le terme de couleurs.

Toujours avec cette même image de circuits, on regarde les flèches d'une signature comme des briques élémentaires permettant de construire des circuits plus complexes ; comme avec les n -uplets de mots, on peut faire deux opérations : appliquer un opérateur à n entrées à un opérateur à n sorties (les brancher l'un à l'autre), ainsi que juxtaposer deux opérateurs, l'un de valence (m, n) et l'autre de valence (p, q) pour obtenir un nouvel opérateur de valence $(m + p, n + q)$ (placer deux bouts de circuits l'un à côté de l'autre). La figure 3.1 montre des exemples de ces opérations.

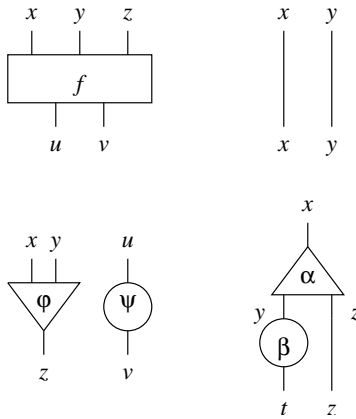


FIG. 3.1 – Exemples de diagrammes associés à des flèches d'une signature et d'opérations sur de telles flèches. De gauche à droite et de haut en bas : une flèche $f : xyz \rightarrow uv$, l'identité de xy , le produit $\varphi \otimes \psi : xyu \rightarrow zv$ de $\varphi : xy \rightarrow z$ et $\psi : u \rightarrow v$, la composée $(\beta \otimes z) \circ \alpha : x \rightarrow tz$ de $\alpha : x \rightarrow yz$ et $(\beta \otimes z) : yz \rightarrow tz$.

Ces deux opérations sont exactement la composition et le produit d'une catégorie monoïdale. Ainsi, on cherche la catégorie monoïdale obtenue en considérant toutes les compositions et juxtapositions des opérateurs de Σ : c'est la *catégorie monoïdale (stricte) librement engendrée par la signature Σ* .

Avant d'en venir à cela, nous allons définir l'objet central de cette étude.

Définition. Étant donné un ensemble Γ , on appelle *opéade* Γ -colorée toute catégorie monoïdale stricte $(\mathbb{C}, \otimes, *)$ dont le monoïde des objets est le monoïde libre $(\langle \Gamma \rangle, \cdot, *)$ engendré par Γ .

Comme pour les signatures, on parle d'*opéades (monochromes)* si $\Gamma = \{*\}$. ◆

Nous verrons toujours les flèches d'une opéade comme des circuits, avec la représentation diagrammatique mentionnée. Il convient de noter qu'il s'agit d'une image fidèle. En effet, les opérations de composition et de produit vérifient certaines propriétés de cohérence que les diagrammes traduisent bien : les flèches correspondent aux classes d'équivalence de circuits *modulo* certaines déformations (appelées isotopies) consistant à pouvoir déplacer des bouts de circuits les uns par rapport aux autres sans créer de croisement de fils ainsi qu'à allonger ou raccourcir des fils (c'est-à-dire toutes les déformations raisonnables de ces diagrammes).

Nous allons à présent ouvrir une parenthèse afin de discuter sur la terminologie choisie. En effet, la notion d'opéade existe déjà ; cependant, ce conflit apparent n'en est pas vraiment un, dans la mesure où la définition donnée ici est une généralisation de l'existante. On pourrait alors parler d'opéades *généralisées*, mais ce n'est pas le choix effectué et nous allons le justifier. Avant cela, donnons certains exemples d'opéades qui nous donnerons quelques arguments.

Le premier exemple d'opéade est donné par $\text{Oper } X$, où X est un ensemble : on l'appelle *opéade des opérations sur X* et elle est définie comme la sous-catégorie pleine de la catégorie \mathbf{Ens} des ensembles dont les objets sont tous les produits X^n de X , y compris le produit vide (le singleton). Plus simplement, $\text{Oper } X(m, n)$ est défini comme l'ensemble des applications de X^m dans X^n . Notons que l'on peut aisément remplacer \mathbf{Ens} par n'importe quelle catégorie monoïdale.

Les *structures algébriques abstraites* constituent la majorité des exemples : étant donnée une structure, celle de monoïde par exemple, l'opéade correspondante, notée Δ , contient toutes les opérations que l'on peut effectuer dans tout monoïde, comme le produit (de source 2 et de but 1), l'unité (source 0, but 1) ou encore des opérations composites comme le produit de trois éléments (source 3, but 1), qui est unique en vertu de la relation d'associativité. Cette opéade est donnée plus loin de manière explicite.

Ajoutons qu'il existe aussi des opéades décrivant des objets géométriques : l'opéade des monoïdes pour les ensembles simpliciaux (augmentés), l'opéade des treillis (booléens) pour les ensembles cubiques (avec connections), mais aussi l'opéade tressée initiale pour les tresses et l'opéade tressée souveraine initiale pour les enchevêtrements (orientés).

Donnons, à présent, quelques exemples formels :

Exemples. 1) L'opérade des permutations \mathfrak{S} . On pose, pour $m, n \in \mathbb{N}$:

$$\mathfrak{S}(m, n) = \begin{cases} \mathfrak{S}_n & \text{si } m = n \\ \emptyset & \text{sinon} \end{cases}$$

où \mathfrak{S}_n est le groupe des permutations d'un ensemble à n éléments avec, comme convention, $\mathfrak{S}_0 = \{0\}$. Le produit est défini de la façon suivante, pour $\sigma \in \mathfrak{S}(m, m)$, $\tau \in \mathfrak{S}(n, n)$ et $i \in \{1 \dots m + n\}$:

$$\sigma \otimes \tau(i) = \begin{cases} \sigma(i) & \text{si } i \in \{1 \dots m\} \\ \tau(i - m) + m & \text{si } i \in \{m + 1 \dots m + n\}. \end{cases}$$

- 2) L'opérade \mathfrak{B} des tresses est construite comme \mathfrak{S} mais en remplaçant les groupes de permutations \mathfrak{S}_n par les groupes de tresses \mathfrak{B}_n .
- 3) L'opérade (co)simpliciale ou des monoïdes Δ . On pose :

$$[n] = \begin{cases} \emptyset & \text{si } n = 0 \\ \{1 \dots n\} & \text{si } n \geq 1 \end{cases}$$

et $\Delta(m, n)$ l'ensemble des applications croissantes de $[m]$ dans $[n]$. Le produit monoïdal est induit par le coproduit de la catégorie des ensembles ; de manière explicite, si $f \in \Delta(m, n)$, $g \in \Delta(p, q)$ et $i \in [m + p]$:

$$f \otimes g(i) = \begin{cases} f(i) & \text{si } i \in [n] \\ g(i - m) + n & \text{si } (i - n) \in [p]. \end{cases}$$

3.1.1 Discussion

Les exemples algébriques donnés précédemment montrent que, outre les opérades usuelles, la notion d'opérade donnée ici rentre aussi en conflit avec les structures classiques de l'algèbre universelle : les théories algébriques, les PRO, les PROP et les 2-monoïdes.

Nous allons examiner une à une les cinq structures conflictuelles, par ordre croissant de généralité, comme le montre le diagramme d'inclusion ci-dessous :

Opérades classiques \subseteq Théories algébriques \subseteq PROP \subseteq PRO \subseteq Opérades \subseteq 2-monoïdes.

Le principal objectif de cette discussion est de justifier que la notion d'opérade utilisée ici n'est pas suffisamment différente de la notion classique pour mériter un nouveau nom et, en outre, que c'est le nom d'opérade qui décrit le mieux la nature profonde ainsi que la raison d'être de ces objets.

Commençons par l'utilisation qui est faite de ces objets. Comme esquissé précédemment, leur but est d'abstraire la structure algébrique d'objets - qu'il s'agisse d'ensembles, d'espaces vectoriels, de modules, de graphes, etc. - pourvus d'opérations qui satisfont certaines équations. Les algèbres associées sont alors exactement les objets dont on a abstrait la structure.

Par exemple, un monoïde est un ensemble muni d'une opération binaire m et d'une constante e qui satisfont trois équations, l'une exprimant le fait que m est associative et les deux autres que e est une unité bilatère pour m . On abstrait ces informations en disant que l'essence de la structure de monoïde est indépendante de l'ensemble sous-jacent et réside dans la donnée d'opérateurs abstraits μ et η , prenant respectivement deux et zéro arguments, rendant tous deux une valeur et satisfaisant les relations d'associativité et d'unité précédemment mentionnées.

Cette démarche permet alors de percevoir des objets aussi divers que les monoïdes, les algèbres associatives et unitaires, les monades, etc. comme étant essentiellement identiques, c'est-à-dire que ce sont tous des algèbres sur l'opérade des monoïdes, la seule différence étant la catégorie dans laquelle elles sont réalisées.

À présent, examinons les différents objets conflictuels avec ce point de vue, c'est-à-dire en regardant quelles structures chacune d'entre elles peut ou ne peut pas abstraire.

Les opérades classiques, introduites par Peter May dans [May72], sont destinées à décrire des structures algébriques ayant des opérations prenant n'importe quel nombre d'arguments mais ne rendant qu'une valeur, et qui satisfont seulement des équations linéaires : il ne peut pas y avoir d'équation où certaines entrées sont supposées égales ou encore où l'un des membres ne contient pas autant d'entrées que l'autre. Ainsi, les opérades classiques fonctionnent très bien en ce qui concerne les monoïdes dans une catégorie monoïdales quelconque (ou les comonoïdes en prenant des algèbres contravariantes), mais échouent dans l'abstraction de structures plus complexes, comme les groupes classiques et les anneaux (qui contiennent des équations non linéaires), ou encore les groupes quantiques et les algèbres de Hopf (qui contiennent des opérations à la fois algébriques et coalgébriques, c'est-à-dire que certaines prennent plusieurs arguments et rendent une valeur, tandis que d'autres font l'inverse).

Puis, nous passons aux théories algébriques, introduites par William Lawvere dans [Law63], qui modifient les opérades classiques de deux façons. La première est une amélioration : leur définition est bien plus simple que celle des opérades classiques, bien que ce ne soit pas vraiment ce qui nous intéresse ici. La seconde est une généralisation : les théories algébriques ne sont pas limitées aux équations linéaires, ce qui permet d'en définir pour les groupes classiques ou les anneaux. Cependant, elles ne peuvent toujours pas décrire les structures de groupe quantique ni d'algèbre de Hopf, ainsi que n'importe quelle autre structure qui n'est pas purement algébrique ou coalgébrique. Avant de continuer, disons qu'une théorie algébrique est une opérade monochrome, comme nous les avons définies, dont le produit monoïdal est en fait cartésien.

En franchissant un nouveau palier de généralité, nous arrivons aux PRO et aux PROP, définis par Saunders MacLane dans [ML65]. Afin de les comparer aux théories algébriques, un PRO est une opérade monochrome et un PROP une opérade monochrome symétrique. S'il l'on ne s'intéresse qu'à l'abstraction de structures algébriques, les PROP - quitte à les colorier - feraient parfaitement l'affaire, puisqu'ils lèvent la dernière restriction sur les opérations : en effet, il existe un PROP pour les groupes quantiques et pour les algèbres de Hopf (notons en passant que c'est le même). Cependant, en généralisant à peine pour arriver au monde non symétrique des PRO, on peut décrire des objets issus de la géométrie : il existe en effet un PRO dont les flèches sont exactement les tresses et un PRO bicolore dont les flèches sont les enchevêtrements orientés.

À ce stade, nous voyons que la notion de PRO (coloré) conviendrait parfaitement puisqu'elle coïncide avec nos opérades. Avant d'en discuter, parlons des 2-monoïdes : ils furent introduits par Albert Burroni dans [Bur93] et sont des petites catégories monoïdales strictes. Ainsi, ils permettent l'abstraction de toute structure avec n'importe quel type d'opération et d'équation, tout en donnant la possibilité supplémentaire d'avoir certaines relations entre les sortes (les couleurs). Cependant, n'ayant pas besoin de cette caractéristique additionnelle pour l'instant, nous resterons un niveau de généralité en retrait.

Il existe une dernière raison pour ne pas considérer des 2-monoïdes ni utiliser le terme PRO : ils ne véhiculent pas l'intuition selon laquelle les opérades sont des structures abstraites. En effet, PRO est une abréviation de « *product category* », ce qui ne décrit que la structure interne de cet objet ; quant au nom de « 2-monoïde », il rappelle seulement qu'il s'agit d'une 2-catégorie avec un seul objet, tout comme les (1-)monoïdes sont des (1-)catégories avec un seul objet. Il nous reste alors « théorie algébrique » ; cependant, comme nous l'avons fait remarquer précédemment, nous sommes arrivés à un niveau de généralité permettant aussi d'abstraire des structures géométriques : cela nous conduirait à abandonner l'adjectif « algébrique », mais appeler « théories » des objets mathématiques serait une trop grande source de confusion.

Nous n'avons évoqué ici que des arguments informels, mais ils motivent l'extension du nom « opérade » à l'usage qui en est fait ici. Soyons pourtant équitables et disons que cette structure est loin d'être parfaite : il manque encore la possibilité d'abstraire des structures possédant des opérations qui ne sont définies que partiellement, comme les corps - l'inverse est défini partout sauf en 0. Pire encore, et bien que cette situation ironique soit fréquente, il n'existe pas d'opérade pour la structure d'opérade, qui possède une opération, la composition, définie seulement en certains points. Nous étudierons ce problème dans un prochain travail, notamment en examinant comment la théorie des opérades prend place dans celle des algèbres graphiques d'Albert Burroni [Bur81]. Mais, pour l'instant, la définition d'opérade (colorée) donnée ici convient.

Enfin, citons d'autres objets dont l'objectif est aussi d'abstraire des structures, parmi lesquels les PACT [ML65], les opétopes [BD98a], les computades [Str76], les structades [Lam] ou encore les catérades [May98]. Il faudrait étudier plus en détails les liens entre les opérades et ces derniers objets, afin d'établir une classification ainsi qu'une harmonisation de la terminologie.

Dans la suite, nous appellerons donc opérades les catégories monoïdales particulières utilisées ici, opérades classiques celles que l'on rencontre dans la littérature, opérades monochromes cartésiennes les théories algébriques, opérades monochromes symétriques les PROP et opérades monochromes les PRO. Les liens entre ces divers types d'opérades sont étudiés dans l'appendice A.

Le paragraphe suivant décrit la construction de l'opérade librement engendrée par une signature, ainsi que le quotient d'une telle catégorie par des relations, pour aboutir à la notion de *présentation d'opérade*. Les constructions effectuées sont parfois techniques et peuvent faire appel à des notions qui ne sont pas détaillées ; cependant, il n'est pas nécessaire d'assimiler les détails pour comprendre la suite.

3.2 Opérades libres et quotients

3.2.1 Présentation d'une petite catégorie par graphe et relations

Notons \mathbb{G}_{PH} la catégorie des graphes et de leurs morphismes. On rappelle que \mathbb{C}_{AT} désigne celle des petites catégories et des foncteurs entre elles. Il existe un foncteur oubli $\mathbb{C}_{\text{AT}} \rightarrow \mathbb{G}_{\text{PH}}$ qui, à toute petite catégorie, associe son graphe sous-jacent, c'est-à-dire le graphe ayant mêmes objets et flèches que la catégorie, mais en oubliant que l'on peut les composer - et donc que certaines sont des identités pour la composition.

Ce foncteur possède un adjoint à gauche $\mathbb{G}_{\text{PH}} \longrightarrow \mathbb{C}_{\text{AT}}$ qui associe à tout graphe G la *catégorie libre qu'il engendre*, appelée aussi catégorie des *chemins dans G* . Les objets de cette catégorie sont ceux de G et ses flèches sont les chemins dans le graphe ; la composition est donnée par la concaténation des chemins et les identités par les chemins vides.

Étant donnée une (petite) catégorie C , on peut effectuer son quotient par une famille R de *règles*, c'est-à-dire de couples de flèches parallèles dans C . On considère \equiv_R la congruence sur C engendrée par R , c'est-à-dire la plus petite relation d'équivalence sur les flèches parallèles de C qui est compatible avec la structure de catégorie, c'est-à-dire avec la composition ; on aurait pu tout aussi bien parler de la clôture réflexive-symétrique-transitive de l'idéal (R) de C engendré par R .

On définit alors le quotient de C par \equiv_R comme la catégorie C/\equiv_R possédant les mêmes objets que C et dont les flèches sont données par $(C/\equiv_R)(x, y) = (C(x, y))/(\equiv_R(x, y))$ où $\equiv_R(x, y)$ est la restriction à $C(x, y)$ de \equiv_R et où le quotient du membre de droite est effectué dans la catégorie \mathbb{E}_{NS} des ensembles. Autrement dit, C/\equiv_R est la catégorie dont les flèches sont les classes d'équivalence des flèches de C pour \equiv_R .

Remarquons que l'on peut transporter la structure de catégorie de C vers le quotient car \equiv_R est compatible avec la structure (c'est un idéal de C).

3.2.2 Opérade librement engendrée par une signature

Un *morphisme d'opérades* est un foncteur monoïdal strict qui induit l'identité sur les objets. Les opérades et les morphismes d'opérades s'organisent en une catégorie notée \mathbb{OP} . De même, un *morphisme de signatures* est un morphisme de graphes qui préserve les objets ; les signatures et leurs morphismes forment une catégorie notée \mathbb{SGN} . Il existe un foncteur oubli $\mathcal{U} : \mathbb{OP} \longrightarrow \mathbb{SGN}$ qui, à toute opérade \mathbb{C} , associe la signature $\text{Fl } \mathbb{C} \rightrightarrows \mathbb{N}$. On va construire un foncteur $\mathcal{L} : \mathbb{SGN} \longrightarrow \mathbb{OP}$, adjoint à gauche du précédent.

Étant fixée une signature Σ , on procède par étapes. Intuitivement, les éléments de $\Sigma(m, n)$ contiennent les opérateurs de base de la catégorie cherchée, celle-ci étant composée de tous les opérateurs que l'on peut obtenir par compositions et juxtapositions finies de ces briques élémentaires. On peut toujours garder à l'esprit la vision diagrammes/circuits et, ainsi, considérer les flèches de Σ comme des composants électroniques, chacun ayant un certain nombre d'entrées et de sorties ; on suppose que l'on dispose d'un stock inépuisable de ces derniers ; les flèches de l'opérade libre sont alors tous les circuits que l'on peut construire avec ces composants élémentaires, dans le plan et sans chevauchement de fil.

Revenons à une approche plus formelle. On commence par associer à Σ la signature $\bar{\Sigma}$ dont les flèches sont tous les triplets (p, φ, q) , où p et q sont des entiers naturels et φ est

une flèche de Σ . Les applications source et but y sont définies par :

$$s(p, \varphi, q) = p + s(\varphi) + q \quad \text{et} \quad t(p, \varphi, q) = p + t(\varphi) + q.$$

On note, plus simplement, $p \otimes \varphi \otimes q$ au lieu de (p, φ, q) avec les conventions $\varphi = 0 \otimes \varphi \otimes 0$, $p \otimes \varphi = p \otimes \varphi \otimes 0$ et $\varphi \otimes q = 0 \otimes \varphi \otimes q$. Cette signature contient tous les diagrammes obtenus en rajoutant des fils verticaux de chaque côté des diagrammes élémentaires de Σ .

Ayant construit cette signature $\bar{\Sigma}$, on pose $\mathcal{L}\Sigma$ la catégorie présentée par le graphe générateur $\bar{\Sigma}$ et soumise aux *relations élémentaires d'échange* :

$$((k + n + i) \otimes \psi \otimes l) \circ (k \otimes \varphi \otimes (i + p + l)) = (k \otimes \varphi \otimes (i + q + l)) \circ ((k + m + i) \otimes \psi \otimes l),$$

pour tous entiers m, n, p, q, k, l, i et toutes flèches $\varphi \in \Sigma(m, n)$ et $\psi \in \Sigma(p, q)$. Cette relation, qui va engendrer celle d'échange, nous permet de déplacer, verticalement et l'un par rapport à l'autre, deux composants élémentaires qui ne sont pas branchés l'un à l'autre : la figure 3.2 montre cette opération, effectuée sur les diagrammes correspondant.

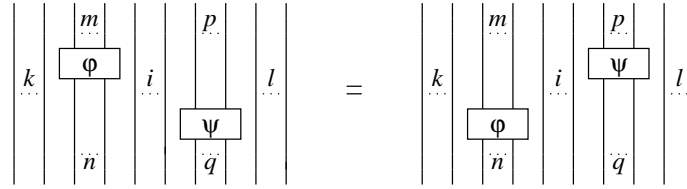


FIG. 3.2 – Relation d'échange, illustrée par des diagrammes.

Il ne reste plus qu'à définir le produit \otimes sur toutes les flèches de $\mathcal{L}\Sigma$. Si $f \in \mathcal{L}\Sigma(m, n)$ telle que

$$f = (p_k \otimes \varphi_k \otimes q_k) \circ \cdots \circ (p_1 \otimes \varphi_1 \otimes q_1)$$

avec les φ_i dans Σ et les p_i et q_i dans \mathbb{N} , alors, pour tous $m, n \in \mathbb{N}$, on pose :

$$\begin{cases} m \otimes f = ((m + p_k) \otimes \varphi_k \otimes q_k) \circ \cdots \circ ((m + p_1) \otimes \varphi_1 \otimes q_1) \\ f \otimes n = (p_k \otimes \varphi_k \otimes (q_k + n)) \circ \cdots \circ (p_1 \otimes \varphi_1 \otimes (q_1 + n)) \end{cases}$$

Alors, pour $f \in \mathcal{L}\Sigma(m, n)$ et $g \in \mathcal{L}\Sigma(p, q)$, on définit $f \otimes g$ comme la flèche de $\mathcal{L}(m + p, n + q)$ donnée par :

$$f \otimes g = (n \otimes g) \circ (f \otimes p).$$

On vérifie la proposition suivante :

Proposition 3.1. *Pour toute signature Σ , $\mathcal{L}\Sigma$ est une opérade et l'application \mathcal{L} s'étend en un foncteur $\mathbf{S}^{\mathbf{GN}} \rightarrow \mathbf{OP}$ qui est adjoint à gauche du foncteur oubli $\mathcal{U} : \mathbf{OP} \rightarrow \mathbf{S}^{\mathbf{GN}}$. De manière équivalente, si i est le monomorphisme de signatures canonique de Σ dans $\mathcal{U}\mathcal{L}\Sigma$, le couple $(\mathcal{L}\Sigma, i)$ est solution du problème universel d'opérade libre engendrée par Σ :*

pour tout couple (\mathbb{C}, F) où \mathbb{C} est une opérade et $F : \Sigma \rightarrow \mathcal{U}\mathbb{C}$ est un morphisme de signatures, il existe un unique morphisme d'opérides $\bar{F} : \mathcal{L}\Sigma \rightarrow \mathbb{C}$ tel que le diagramme

$$\begin{array}{ccc} \Sigma & \xrightarrow{i} & \mathcal{U}\mathcal{L}\Sigma \\ & \searrow F & \downarrow \mathcal{U}\bar{F} \\ & & \mathcal{U}\mathbb{C} \end{array}$$

commute.

Démonstration. Il faut, dans un premier temps, vérifier que $\mathcal{L}\Sigma$ est une opérade. Par construction, il s'agit d'une petite catégorie dont les objets sont les entiers naturels. Il faut vérifier que $m \otimes f \otimes n$ ne dépend pas de la décomposition de f en flèches de $\bar{\Sigma}$, c'est-à-dire que, pour tous entiers $m, n, p, q, k, l, i, r, s$ et toutes flèches $\varphi \in \Sigma(m, n)$ et $\psi \in \Sigma(p, q)$:

$$\begin{aligned} & r \otimes \left(((k + n + i) \otimes \psi \otimes l) \circ (k \otimes \varphi \otimes (i + p + l)) \right) \otimes s \\ &= r \otimes \left((k \otimes \varphi \otimes (i + q + l)) \circ ((k + m + i) \otimes \psi \otimes l) \right) \otimes s. \end{aligned}$$

Cela ne pose aucun problème : on commence par distribuer r et s dans chaque membre de l'égalité à vérifier, qui devient équivalente à la relation élémentaire d'échange, dans laquelle on a remplacé k par $r + k$ et l par $l + s$.

On doit voir que le produit \otimes défini sur les flèches de $\mathcal{L}\Sigma$ est (issu d')un produit monoïdal sur $\mathcal{L}\Sigma$. On étend \otimes aux objets en posant $m \otimes n = m + n$. Alors, si $f \in \mathcal{L}\Sigma(m, n)$ et $g \in \mathcal{L}\Sigma(p, q)$:

$$\begin{aligned} s(f \otimes g) &= s((n \otimes g) \circ (f \otimes p)) \\ &= s(f \otimes p) \\ &= m + p \\ &= s(f) \otimes s(g). \end{aligned}$$

On vérifie de même que $t(f \otimes g) = t(f) \otimes t(g)$. De plus, pour toute flèche f de $\mathcal{L}\Sigma$, $f \otimes 0 = 0 \otimes f = f$.

Il ne reste plus qu'à vérifier la relation d'échange. Prenons deux flèches :

$$\begin{cases} f = (k_i \otimes \varphi_i \otimes l_i) \circ \cdots \circ (k_1 \otimes \varphi_1 \otimes l_1) : m \longrightarrow n \\ g = (r_j \otimes \psi_j \otimes s_j) \circ \cdots \circ (r_1 \otimes \psi_1 \otimes s_1) : p \longrightarrow q \end{cases}$$

On pose, pour tout u , $m_u = k_u + s(\varphi_u) + l_u$ et $q_u = r_u + t(\psi_u) + s_u$. On a, par récurrence sur i et j :

$$\begin{aligned} (n \otimes g) \circ (f \otimes p) &= ((n + r_j) \otimes \psi_j \otimes s_j) \circ \cdots \circ ((n + r_1) \otimes \psi_1 \otimes s_1) \\ &\quad \circ (k_i \otimes \varphi_i \otimes (l_i + p)) \circ \cdots \circ (k_1 \otimes \varphi_1 \otimes (l_1 + p)) \\ &= ((n + r_j) \otimes \psi_j \otimes s_j) \circ \cdots \circ ((n + r_2) \otimes \psi_1 \otimes s_2) \\ &\quad \circ (k_i \otimes \varphi_i \otimes (l_i + q_1)) \circ ((m_i + r_1) \otimes \psi_1 \otimes s_1) \\ &\quad \circ (k_{i-1} \otimes \varphi_{i-1} \otimes (l_{i-1} + p)) \circ \cdots \circ (k_1 \otimes \varphi_1 \otimes (l_1 + p)) \\ &= \dots \\ &= (k_i \otimes \varphi_i \otimes (l_i + q)) \circ \cdots \circ (k_1 \otimes \varphi_1 \otimes (l_1 + q)) \\ &\quad \circ ((m + r_j) \otimes \psi_j \otimes s_j) \circ \cdots \circ ((m + r_1) \otimes \psi_1 \otimes s_1) \\ &= (f \otimes q) \circ (m \otimes g). \end{aligned}$$

Ensuite, on doit construire, pour toute opérade \mathbb{C} et tout morphisme de signatures $F : \Sigma \longrightarrow \mathcal{UC}$, une extension $\bar{F} : \mathcal{L}\Sigma \longrightarrow \mathbb{C}$ qui est un morphisme d'opérades et montrer qu'il est entièrement déterminé par ses valeurs sur les flèches de Σ . Soit f une flèche de $\mathcal{L}\Sigma$ avec $f = f_k \circ \cdots \circ f_1$ une décomposition en flèches de $\bar{\Sigma}$. Si $G : \mathcal{L}\Sigma \longrightarrow \mathbb{C}$ est un morphisme d'opérades, il doit vérifier :

$$G(f) = G(f_k) \circ \cdots \circ G(f_1).$$

Or son comportement sur les flèches de $\bar{\Sigma}$ est lui aussi imposé ; si f est une flèche de $\bar{\Sigma}$ avec $f = p \otimes \varphi \otimes q$, on a nécessairement :

$$G(f) = p \otimes G(\varphi) \otimes q.$$

Donc un tel morphisme G , s'il existe, est entièrement déterminé par ses valeurs sur les flèches de Σ . On étend alors F en $\bar{F} : \mathcal{L}\Sigma \longrightarrow \mathbb{C}$ par étapes. On commence par :

$$\bar{F}(p \otimes \varphi \otimes q) = p \otimes F(\varphi) \otimes q$$

pour toute flèche $p \otimes \varphi \otimes q$ de $\bar{\Sigma}$. Puis, si $f = f_k \circ \cdots \circ f_1$ est une flèche de $\mathcal{L}\Sigma$ décomposée en flèches de $\bar{\Sigma}$, on pose :

$$\bar{F}(f) = \bar{F}(f_k) \circ \cdots \circ \bar{F}(f_1).$$

Il ne reste plus qu'à montrer que \bar{F} est un morphisme d'opérades, ce qui ne pose pas de problème. \diamond

En vertu de ce résultat et pour toute signature Σ , on appelle $\mathcal{L}\Sigma$ l'opérade libre engendrée par Σ .

3.2.3 Limites et colimites dans les catégories des signatures et des opérades

Le but de ce paragraphe est de montrer que $\mathbb{S}_{\mathbb{N}}$ et $\mathbb{O}_{\mathbb{P}}$ sont finiment complètes et cocomplètes, c'est-à-dire qu'elles possèdent toutes les limites et colimites finies. Il s'agit juste de s'assurer que les constructions à venir sont bien définies ; à ce titre, ce paragraphe n'est pas indispensable à la compréhension et ne rappelle pas les notions utilisées : on renvoie à [ML98] pour un complément d'information. Les vérifications sont longues mais ne posent aucun problème et sont donc omises.

On utilise les critères suivants :

Proposition 3.2. *Une catégorie est finiment complète (resp. cocomplète) si et seulement si elle possède tous les produits (resp. coproduits) finis et tous les égalisateurs (resp. coégalisateurs). De plus, une catégorie possède tous les produits (resp. coproduits) finis si et seulement si elle possède un objet terminal (resp. initial) et tous les produits (resp. coproduits) binaires.*

Commençons par la catégorie des signatures. De manière équivalente, on peut la voir comme la catégorie des familles d'ensembles indexées par un couple d'entiers ou comme la catégorie des foncteurs allant de la catégorie discrète $\mathbb{N} \times \mathbb{N}$ vers celle des ensembles. À ce titre, les limites et colimites de la catégorie des signatures sont calculées point par point à partir de celles de la catégorie des ensembles.

On obtient ainsi que l'objet terminal de $\mathbb{S}_{\mathbb{N}}$ est la signature \square possédant une et une seule flèche $m \longrightarrow n$ pour tous $m, n \in \mathbb{N}$. Son objet initial est la signature \emptyset n'ayant aucune flèche.

Le produit dans $\mathbb{S}_{\mathbb{N}}$ est défini comme suit. Soient Σ et Ω deux signatures. Leur produit est la signature $\Sigma \times \Omega$ définie par :

$$\Sigma \times \Omega(m, n) = \Sigma(m, n) \times \Omega(m, n).$$

En d'autres termes, les flèches $m \longrightarrow n$ de $\Sigma \times \Omega$ sont les couples (f, g) où $f \in \Sigma(m, n)$ et $g \in \Omega(m, n)$. Les projections sont les morphismes de signatures donnés par :

$$(f, g) \longmapsto f \quad \text{et} \quad (f, g) \longmapsto g.$$

Le coproduit de deux signatures Σ et Ω est donné par :

$$\Sigma \amalg \Omega(m, n) = \Sigma(m, n) \amalg \Omega(m, n).$$

Les morphismes associés sont les inclusions de chaque ensemble $\Sigma(m, n)$ et $\Omega(m, n)$ dans la réunion disjointe $\Sigma(m, n) \amalg \Omega(m, n)$. Ainsi, une flèche de $\Sigma \amalg \Omega(m, n)$ est soit une

flèche de $\Sigma(m, n)$, soit une flèche de $\Omega(m, n)$.

Soient Σ et Ω deux signatures et $F, G : \Sigma \longrightarrow \Omega$ deux morphismes. L'égalisateur de F et G est le couple (Θ, H) où Θ est la signature donnée par :

$$\Theta(m, n) = \{f \in \Sigma(m, n) : F(f) = G(f)\}$$

et H est induit par les inclusions de chaque $\Theta(m, n)$ dans $\Sigma(m, n)$.

Enfin, avec les mêmes notations, le coégalisateur de F et G est donné comme le couple (Ξ, K) où Ξ est la signature donnée par :

$$\Xi(m, n) = \Omega(m, n) / \simeq (m, n).$$

On a noté $\simeq (m, n)$ la relation d'équivalence sur l'ensemble $\Omega(m, n)$ engendrée par la partie $\{(F(f), G(f)) : f \in \Sigma(m, n)\}$. Le morphisme $H : \Omega \longrightarrow \Xi$ est induit par les projections canoniques de $\Omega(m, n)$ sur $\Xi(m, n)$.

On a ainsi obtenu :

Proposition 3.3. *La catégorie $\mathbf{S}_{\mathbf{GN}}$ des signatures est finiment complète et cocomplète.*

Pour la catégorie des opérades, si les limites sont faciles à construire, les colimites le sont moins.

L'objet terminal de la catégorie des opérades est la signature \square contenant une unique flèche $\square_n^m : m \longrightarrow n$ pour chaque couple (m, n) d'entiers, que l'on munit de la structure suivante :

$$\square_p^n \circ \square_n^m = \square_p^m, \quad \square_n^m \otimes \square_q^p = \square_{n+q}^{m+p}, \quad n = \square_n^n.$$

L'opérade initiale est celle qui ne contient que des identités : il s'agit de $\mathcal{L}\emptyset$, avec \emptyset la signature initiale, c'est-à-dire la signature ne possédant aucune flèche. Il n'y a aucune autre composition possible dans $\mathcal{L}\emptyset$ que celle d'une identité n avec elle-même, qui vérifie nécessairement $n \circ n = n$. Le produit de m et de n , quant à lui, doit être $m \otimes n = m + n$, par définition de la structure d'opérade.

Le produit de deux opérades \mathbb{C} et \mathbb{D} est encore défini composante par composante :

$$\mathbb{C} \times \mathbb{D}(m, n) = \mathbb{C}(m, n) \times \mathbb{D}(m, n).$$

La structure d'opérade de $\mathbb{C} \times \mathbb{D}$ est donnée par :

$$(h, k) \circ (f, g) = (h \circ f, k \circ g), \quad (f, g) \otimes (h, k) = (f \otimes h, g \otimes k), \quad n = (n, n).$$

Enfin, les projections sont $(f, g) \mapsto f$ et $(f, g) \mapsto g$, qui sont, par construction, compatibles avec la structure d'opérade.

Le coproduit de deux opérades \mathbb{C} et \mathbb{D} est plus complexe : on cherche la plus petite opérade qui contienne à la fois \mathbb{C} et \mathbb{D} . Pour l'obtenir, on considère les signatures \mathcal{UC} et \mathcal{UD} sous-jacentes à \mathbb{C} et à \mathbb{D} . On construit le coproduit $\mathcal{UC} \amalg \mathcal{UD}$ de ces deux signatures puis on applique à ce coproduit le foncteur opérade libre. On oublie alors la structure monoïdale de $\mathcal{L}(\mathcal{UC} \amalg \mathcal{UD})$ pour la voir comme une petite catégorie. Sur cette dernière, on construit la congruence \simeq engendré par les familles suivantes de relations, indexées par les couples (h, k) de flèches de $\mathcal{L}(\mathcal{UC} \amalg \mathcal{UD})$:

$$\left\{ \begin{array}{ll} h \otimes (g \circ f) \otimes k \simeq h \otimes (g \circ_{\mathbb{C}} f) \otimes k & \text{pour toutes flèches composables } f \text{ et } g \text{ de } \mathbb{C} ; \\ h \otimes (g \circ f) \otimes k \simeq h \otimes (g \circ_{\mathbb{D}} f) \otimes k & \text{pour toutes flèches composables } f \text{ et } g \text{ de } \mathbb{D} ; \\ h \otimes (f \otimes g) \otimes k \simeq h \otimes (f \otimes_{\mathbb{C}} g) \otimes k & \text{pour toutes flèches } f \text{ et } g \text{ de } \mathbb{C} ; \\ h \otimes (f \otimes g) \otimes k \simeq h \otimes (f \otimes_{\mathbb{D}} g) \otimes k & \text{pour toutes flèches } f \text{ et } g \text{ de } \mathbb{D} ; \\ h \otimes n \otimes k \simeq h \otimes n_{\mathbb{C}} \otimes k \simeq h \otimes n_{\mathbb{D}} \otimes k & \text{pour tout entier } n. \end{array} \right.$$

On a noté $\circ_{\mathbb{C}}$, $\otimes_{\mathbb{C}}$ et $n_{\mathbb{C}}$ les opérations et unités de \mathbb{C} , $\circ_{\mathbb{D}}$, $\otimes_{\mathbb{D}}$ et $n_{\mathbb{D}}$ celles de \mathbb{D} et \circ , \otimes et n celles de $\mathcal{L}(\mathcal{UC} \amalg \mathcal{UD})$. On définit alors la petite catégorie $\mathbb{C} \amalg \mathbb{D}$ comme le quotient suivant, pris dans la catégorie \mathbf{Cat} des petites catégories :

$$\mathbb{C} \amalg \mathbb{D} = \mathcal{L}(\mathcal{UC} \amalg \mathcal{UD}) / \simeq .$$

Il faut encore montrer que le foncteur \otimes obtenu sur $\mathcal{L}(\mathcal{UC} \amalg \mathcal{UD})$ passe au quotient par \simeq , ce qui découle de la construction de cette relation : la catégorie $\mathbb{C} \amalg \mathbb{D}$ est donc une opérade. Il ne reste plus qu'à définir les morphismes associés au coproduit : par construction, chaque flèche de \mathbb{C} et chaque flèche de \mathbb{D} est une flèche de $\mathcal{L}(\mathcal{UC} \amalg \mathcal{UD})$. Le quotient par \simeq nous assure que ces inclusions sont des morphismes d'opérades.

On notera que, dans le cas où $\mathbb{C} = \mathcal{L}\Sigma$ et $\mathbb{D} = \mathcal{L}\Omega$ sont deux opérades libres, leur coproduit est isomorphe à $\mathcal{L}(\Sigma \amalg \Omega)$.

Soient \mathbb{C} et \mathbb{D} des opérades et $F, G : \mathbb{C} \rightarrow \mathbb{D}$ des morphismes d'opérades. On cherche l'égalisateur de F et G . On définit une sous-signature \mathbb{E} de \mathcal{UC} en posant, pour chaque couple (m, n) d'entiers :

$$\mathbb{E}(m, n) = \{f \in \mathbb{C}(m, n) : F(f) = G(f)\}.$$

On veut montrer que \mathbb{E} est une sous-opérade de \mathbb{C} , c'est-à-dire que la signature \mathbb{E} contient les identités de \mathbb{C} et qu'elle est stable par composition et produit. Comme F et G sont des morphismes d'opérades, on a les relations suivantes :

- Pour tout entier n , $F(n) = n = G(n)$.
- Si $f \in \mathbb{E}(m, n)$ et $g \in \mathbb{E}(n, p)$, alors :

$$F(g \circ f) = F(g) \circ F(f) = G(g) \circ G(f) = G(g \circ f).$$

- Si $f \in \mathbb{E}(m, n)$ et $g \in \mathbb{E}(p, q)$, alors :

$$F(f \otimes g) = F(f) \otimes F(g) = G(f) \otimes G(g) = G(f \otimes g).$$

Ainsi, \mathbb{E} est une opérade. On pose alors H l'inclusion de \mathbb{E} dans \mathbb{C} qui est nécessairement un morphisme d'opérades. On peut alors vérifier que le couple (\mathbb{E}, H) est bien l'égalisateur de F et G .

On considère toujours deux opérades \mathbb{C} et \mathbb{D} , ainsi que deux morphismes d'opérades $F, G : \mathbb{C} \longrightarrow \mathbb{D}$. On cherche à présent le coégalisateur de F et G . On commence par oublier la structure monoïdale de l'opérade \mathbb{D} afin de la voir comme une petite catégorie. On définit ensuite, sur les flèches de cette dernière, la congruence \simeq engendrée par la famille suivante de relations, indexée par les couples (h, k) de flèches de \mathbb{D} :

$$h \otimes F(f) \otimes k \simeq h \otimes G(f) \otimes k,$$

pour toute flèche f de \mathbb{C} . On définit la petite catégorie \mathbb{F} comme le quotient dans \mathbb{C}_{AT} de \mathbb{D} par \simeq . On vérifie que, par construction de \simeq , le foncteur \otimes passe au quotient et munit ainsi \mathbb{F} d'une structure d'opérades. De plus, le quotient dans \mathbb{C}_{AT} nous donne un foncteur $K : \mathbb{D} \longrightarrow \mathbb{F}$ qui, toujours par définition de \simeq , est compatible avec le produit monoïdal. Le coégalisateur de F et G est le couple (\mathbb{F}, K) .

On a donc obtenu :

Proposition 3.4. *La catégorie $\mathbb{O}^{\mathbb{P}}$ des opérades est finiment complète et cocomplète.*

3.2.4 Opérade quotient.

Ici, on va décrire le pendant opéradique du quotient d'un monoïde par des relations : on se donne des règles, c'est-à-dire des couples de flèches parallèles, que l'on veut égaliser dans l'opérade choisie. Comme pour les monoïdes, il faut construire la congruence engendrée par ces relations, pour que le quotient ait toujours une structure de catégorie monoïdale.

Soient \mathbb{C} une opérade et \mathcal{R} une famille de couples de flèches parallèles de \mathbb{C} , c'est-à-dire que l'on se donne, pour tout couple (m, n) d'entiers, une partie $\mathcal{R}(m, n)$ de $\mathbb{C}(m, n)^2$: en particulier, \mathcal{R} est une signature.

Les flèches de \mathcal{R} étant des couples de flèches de \mathbb{C} , on a les projections canoniques $\pi_1, \pi_2 : \mathcal{R} \rightarrow \mathcal{UC}$. En utilisant la propriété universelle de l'opérade libre engendrée par la signature \mathcal{R} , on en déduit des morphismes d'opérades, $\bar{\pi}_1, \bar{\pi}_2 : \mathcal{LR} \rightarrow \mathbb{C}$ qui étendent de manière unique π_1 et π_2 à \mathcal{LR} .

On appelle alors *opérade quotient de \mathbb{C} par \mathcal{R}* , et on note $(\mathbb{C}/\mathcal{R}, \pi)$, le coégalisateur de $\bar{\pi}_1$ et $\bar{\pi}_2$.

Dans une formulation plus constructive, l'opérade \mathbb{C}/\mathcal{R} possède comme flèches de m dans n les classes d'équivalence de flèches de $\mathbb{C}(m, n)$ modulo $\equiv_{\mathcal{R}(m, n)} = (\mathcal{R}(m, n))^{rst}$.

On vérifie la proposition suivante :

Proposition 3.5. *Soient \mathbb{C} une opérade et \mathcal{R} un ensemble de relations sur les flèches parallèles de \mathbb{C} . Alors \mathbb{C}/\mathcal{R} est une opérade et, pour tout couple (f, g) de \mathcal{R} , on a $\pi(f) = \pi(g)$; de plus, le couple $(\mathbb{C}/\mathcal{R}, \pi)$ est universel pour ces propriétés, c'est-à-dire que l'on a :*

pour toute opérade \mathbb{D} et tout morphisme d'opérades $\Phi : \mathbb{C} \rightarrow \mathbb{D}$ tel que, pour tout couple (f, g) de \mathcal{R} , on a $\Phi(f) = \Phi(g)$, il existe une unique morphisme d'opérades $\Psi : \mathbb{C}/\mathcal{R} \rightarrow \mathbb{D}$ tel que le diagramme

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\pi} & \mathbb{C}/\mathcal{R} \\ & \searrow \Phi & \downarrow \mathcal{U}\Psi \\ & & \mathbb{D} \end{array}$$

commute.

Donnons quelques exemples de présentations :

Exemples.

1) On a $\Delta \simeq \mathcal{L}\{\mu : 2 \rightarrow 1; \eta : 0 \rightarrow 1\}/R$, où R est composée des trois relations :

$$\begin{cases} \mu \circ (\mu \otimes 1) = \mu \circ (1 \otimes \mu) \\ \mu \circ (\eta \otimes 1) = 1 \\ \mu \circ (1 \otimes \eta) = 1. \end{cases}$$

En effet, on sait que Δ est engendrée, en tant que catégorie, par les familles de faces $\delta_i^n : n \longrightarrow n+1$, $n \geq 0$ et $1 \leq i \leq n+1$, et de dégénérescences $\sigma_i^n : n+1 \longrightarrow n$, $n \geq 1$ et $1 \leq i \leq n$, avec les définitions suivantes :

$$\delta_i^n(j) = \begin{cases} j & \text{si } j < i \\ j+1 & \text{si } j \geq i \end{cases} \quad \text{et} \quad \sigma_i^n(j) = \begin{cases} j & \text{si } j \leq i \\ j-1 & \text{si } j > i. \end{cases}$$

Ces opérations sont soumises aux relations suivantes :

$$\begin{cases} \delta_i^{n+1} \circ \delta_j^n = \delta_{j+1}^{n+1} \circ \delta_i^n & \text{si } i \leq j \\ \sigma_j^n \circ \sigma_i^{n+1} = \sigma_i^n \circ \sigma_{j+1}^{n+1} & \text{si } i \leq j \\ \sigma_j^n \circ \delta_i^n = \delta_i^{n-1} \circ \sigma_{j-1}^{n-1} & \text{si } i < j \\ \sigma_j^n \circ \delta_i^n = n & \text{si } i = j \text{ ou } i = j+1 \\ \sigma_j^n \circ \delta_i^n = \delta_{i-1}^{n-1} \circ \sigma_j^{n-1} & \text{si } i > j+1. \end{cases}$$

Si on pose $\eta = \delta_1^0$ et $\mu = \sigma_1^1$, on vérifie facilement que :

$$\delta_i^n = (i-1) \otimes \eta \otimes (n+1-i) \quad \text{et} \quad \sigma_i^n = (i-1) \otimes \mu \otimes (n-i).$$

Donc Δ est engendrée par $\eta : 0 \longrightarrow 1$ et $\mu : 2 \longrightarrow 1$. Quant aux relations, elles sont presque toutes automatiques, sauf les trois familles suivantes :

$$\begin{cases} \sigma_i^n \circ \sigma_i^{n+1} = \sigma_i^n \circ \sigma_{i+1}^{n+1} \\ \sigma_i^n \circ \delta_i^n = n \\ \sigma_i^n \circ \delta_{i+1}^n = n. \end{cases}$$

Enfin, ces trois familles sont respectivement équivalentes aux trois relations :

$$\begin{cases} \mu \circ (\mu \otimes 1) = \mu \circ (1 \otimes \mu) \\ \mu \circ (\eta \otimes 1) = 1 \\ \mu \circ (1 \otimes \eta) = 1. \end{cases}$$

L'opérade Δ est donc à la fois celle des monoïdes et celle des objets simpliciaux (augmentés) :

- Les Δ -algèbres d'une catégorie monoïdale \mathcal{C} sont les monoïdes de la catégorie \mathcal{C} - comme nous le verrons plus loin, si \mathbb{C} est une opérade, une \mathbb{C} -algèbre dans \mathcal{C} est un foncteur $\mathbb{C} \longrightarrow \mathcal{C}$ qui préserve les produits. Par exemple, les Δ -algèbres de \mathbb{ENS} sont les monoïdes, celles de $k\mathbb{VECT}$ sont les k -algèbres, celles de \mathbb{AB} (la catégorie des groupes abéliens) sont les anneaux.

- Les foncteurs contravariants de Δ dans une catégorie \mathcal{C} sont les objets simpliciaux (augmentés) de \mathcal{C} . En particulier, les *préfaisceaux* de Δ sont les ensembles simpliciaux (augmentés) - un préfaisceau d'une petite catégorie \mathbb{A} est un foncteur $\mathbb{A}^o \longrightarrow \mathbf{ENS}$.

Nous verrons, au chapitre 5 la version symétrique de Δ , à savoir l'opéride \mathbb{F} dont la catégorie duale, \mathbb{F}^o , est souvent appelée opéride *des ensembles finis*.

- 2) On peut effectuer exactement le même traitement avec l'opéride des objets cubiques avec connections, comme définis dans [BH81], pour montrer qu'elle coïncide avec l'opéride des treillis booléens. Ces liens pour le moins surprenant entre objets algébriques et objets cubiques devront être explorés dans des travaux futurs; en particulier, celui entre les objets cubiques et les treillis pourrait permettre un analogue cubique à la construction par Burroni des orientaux de Street par application successive d'une monade particulière (un cône) sur la catégorie des ω -catégorie, en commençant avec le vide : en effet, la structure simpliciale des objets est donnée par la structure de monoïde (dans une catégorie d'endomorphismes) de la monade; on obtiendrait une structure cubique en remplaçant la monade par une "treillade", c'est-à-dire un treillis (booléen) dans la même catégorie d'endomorphismes.
- 3) Toute structure équationnelle, c'est-à-dire toute structure donnée par opérations (définies partout) et relations donne lieu à une présentation d'opéride. Par exemple, l'opéride des groupes quantiques/algèbres de Hopf est présentée par la signature :

$$0 \begin{array}{c} \xrightarrow{\eta} \\ \xleftarrow{\varepsilon} \end{array} 1 \begin{array}{c} \overset{\sigma}{\curvearrowright} \\ \xleftarrow{\mu} \\ \xrightarrow{\delta} \end{array} 2 \begin{array}{c} \curvearrowright \\ \xleftarrow{\tau} \end{array}$$

Et les relations :

- (a) $\mu \circ (\mu \otimes 1) = \mu \circ (1 \otimes \mu)$;
- (b) $\mu \circ (\eta \otimes 1) = 1$;
- (c) $\mu \circ (1 \otimes \eta) = 1$;
- (d) $(\delta \otimes 1) \circ \delta = (1 \otimes \delta) \circ \delta$;
- (e) $(\varepsilon \otimes 1) \circ \delta = 1$;
- (f) $(1 \otimes \varepsilon) \circ \delta = 1$;
- (g) $\delta \circ \mu = (\mu \otimes \mu) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \delta)$;
- (h) $\varepsilon \circ \mu = \varepsilon \otimes \varepsilon$;
- (i) $\delta \circ \eta = \eta \otimes \eta$;
- (j) $\varepsilon \circ \eta = 0$;
- (k) $\mu \circ (\sigma \otimes 1) \circ \delta = \eta \circ \varepsilon$;

- (l) $\mu \circ (1 \otimes \sigma) \circ \delta = \eta \circ \varepsilon$;
- (m) $\tau \circ \tau = 2$;
- (n) $(\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) = (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau)$;
- (o) $\tau \circ (\mu \otimes 1) = (1 \otimes \mu) \circ (\tau \otimes 1) \circ (1 \otimes \tau)$;
- (p) $\tau \circ (\eta \otimes 1) = 1 \otimes \eta$;
- (q) $(\delta \otimes 1) \circ \tau = (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta)$;
- (r) $(\varepsilon \otimes 1) \circ \tau = 1 \otimes \varepsilon$;
- (s) $\tau \circ (\sigma \otimes 1) = (1 \otimes \sigma) \circ \tau$.

Les générateurs s'interprètent comme suit : μ est le produit, η son unité, δ le coproduit, ε sa coïunité, σ l'antipode ou inverse et τ est un opérateur de symétrie. Quant aux relations, elles nous assurent que : (μ, η) est un(e structure de) monoïde (relations a, b et c), (δ, ε) est un comonoïde (d, e et f), μ et η sont des morphismes de comonoïdes et δ et ε des morphismes de monoïdes (g, h, i et j) et σ est un antipode (k et l). Les relations m à s assurent seulement que l'opérade est symétrique, ce qui est nécessaire pour écrire la relation g.

Notons que cette opérade contient le produit de Kronecker (voir [Sch72]) des opérades symétriques Δ et Δ^o ; c'est d'ailleurs de cette construction que proviennent les relations de compatibilité g à j.

- 4) On peut aussi présenter l'opérade symétrique \mathfrak{S} avec un générateur $\tau : 2 \longrightarrow 2$, qui représente la transposition de deux éléments, et deux relations :
 - (a) $\tau \circ \tau = 2$;
 - (b) $(\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) = (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau)$.
- 5) Pour l'opérade \mathfrak{B} des tresses, on prend deux générateurs $\sigma, \sigma^* : 2 \longrightarrow 2$, représentant les deux croisements possibles de deux brins, soumis aux relations :
 - (a) $\sigma^* \circ \sigma = 2$;
 - (b) $\sigma \circ \sigma^* = 2$;
 - (c) $(\sigma \otimes 1) \circ (1 \otimes \sigma) \circ (\sigma \otimes 1) = (1 \otimes \sigma) \circ (\sigma \otimes 1) \circ (1 \otimes \sigma)$;
- 6) On peut aussi décrire des structures algébriques à plusieurs sortes ; pour exemple, l'opérade des actions de monoïdes : ses algèbres dans $\mathbb{E}ns$ sont les couples (M, X) où M est un monoïde et X un ensemble sur lequel M agit à gauche. Cette opérade possède deux couleurs, notées m et x , est engendrée par trois opérateurs :

$$\begin{cases} \mu : m \times m \longrightarrow m \\ \eta : * \longrightarrow m \\ \alpha : m \times x \longrightarrow x. \end{cases}$$

Le produit du monoïde est μ , η son unité et α son action. Le tout est soumis aux relations suivantes, les trois premières exprimant que (μ, η) est un monoïde et les deux autres que α est bien une action compatible avec (μ, η) :

- (a) $\mu \circ (\mu \otimes m) = \mu \circ (m \otimes \mu)$;
- (b) $\mu \circ (\eta \otimes m) = m$;
- (c) $\mu \circ (m \otimes \eta) = m$;
- (d) $\alpha \circ (m \otimes \alpha) = \alpha \circ (\mu \otimes x)$;
- (e) $\alpha \circ (\eta \otimes x) = x$.

Notons que les algèbres sur cette opérades réalisées dans la catégorie des groupes abéliens sont les couples constitués d'un anneau et d'un module sur cet anneau. Notons aussi que cette opérade contient Δ : on a une injection donnée par $1 \mapsto m$ et $\mu \mapsto \mu$, $\eta \mapsto \eta$.

- 7) Terminons avec l'opérade dont les flèches sont exactement les enchevêtrements orientés (monochromes, mais on peut généraliser sans problème). Cette opérade, bicolore de couleurs notées 1 et 1^* , est engendrée par les douze générateurs suivants, où l'on utilise la notation $(1^*)^* = 1$:

$$\begin{cases} \tau_{xy}^1, \tau_{xy}^2 : x \otimes y \longrightarrow y \otimes x & \text{pour tous } x, y \in \{1, 1^*\} \\ \eta_x : x^* \otimes x \longrightarrow 0 & \text{pour tout } x \in \{1, 1^*\} \\ \gamma_x : 0 \longrightarrow x \otimes x^* & \text{pour tout } x \in \{1, 1^*\}. \end{cases}$$

Les relations sont au nombre de 32 :

- (a) $\tau_{yx}^2 \circ \tau_{xy}^1 = x \otimes y$ pour tous $x, y \in \{1, 1^*\}$;
- (b) $\tau_{yx}^1 \circ \tau_{xy}^2 = x \otimes y$ pour tous $x, y \in \{1, 1^*\}$;
- (c) $(z \otimes \tau_{xy}^1) \circ (\tau_{xz}^1 \otimes y) \circ (x \otimes \tau_{yz}^1) = (\tau_{yz}^1 \otimes x) \circ (y \otimes \tau_{xz}^1) \circ (\tau_{xy}^1 \otimes z)$ pour tous $x, y, z \in \{1, 1^*\}$;
- (d) $(x \otimes \eta_x) \circ (\gamma_x \otimes x) = x$ pour tout $x \in \{1, 1^*\}$;
- (e) $(\eta_x \otimes x^*) \circ (x^* \otimes \gamma_x) = x^*$ pour tout $x \in \{1, 1^*\}$;
- (f) $\eta_x \circ \tau_{xx^*}^1 = \eta_{x^*}$ pour tout $x \in \{1, 1^*\}$;
- (g) $\tau_{xx^*}^1 \circ \gamma_x = \gamma_{x^*}$ pour tout $x \in \{1, 1^*\}$;
- (h) $(\eta_x \otimes y) \circ (x \otimes \tau_{yx^*}^1) \circ (\tau_{yx}^1 \otimes x^*) = y \otimes \eta_x$ pour tous $x, y \in \{1, 1^*\}$;
- (i) $(\tau_{xy}^1 \otimes x^*) \circ (x \otimes \tau_{x^*y}^1) \circ (\eta_x \otimes y) = y \otimes \gamma_x$ pour tous $x, y \in \{1, 1^*\}$.

Notons que cette présentation n'est pas minimale : par exemple, les relations (f) et (g) nous assurent que les générateurs η_{1^*} et γ_{1^*} sont superflus. Le paragraphe suivant introduit les notions de la réécriture sur les opérades ; cependant, en imaginant ce

que peut être la convergence d'une telle présentation, une des questions majeures concernant les entrelacs est de résoudre le problème de mots pour de tels objets : en particulier, on ne sait pas s'il existe ou non une présentation convergente de l'opérade des enchevêtrements orientés. On ne sait d'ailleurs pas non plus répondre à la même question concernant l'opérade \mathfrak{B} des tresses, pourtant plus simple.

3.3 Présentations d'opérades

On vient de voir une approche algébrique traditionnelle de ce que peuvent être des relations sur une opérade : on les voit comme des égalités entre flèches sans se préoccuper d'une quelconque orientation des égalités. On va maintenant imiter ce qui a été fait précédemment sur les monoïdes pour définir toutes les notions de la réécriture dans ce cadre.

3.3.1 Modules sur une opérade

Comme dans le cas des monoïdes, on introduit une notion de *modules sur une opérade* permettant de définir ce que sont les relations de réduction sur une opérade. Notons que la structure retenue paraît arbitraire ; cependant il est impossible d'en choisir une autre : un cadre unifié pour la réécriture apportera certainement une explication à ce fait.

Un monoïde est un ensemble muni d'une opération binaire, le produit, vérifiant certaines relations ; on a vu qu'un module sur un monoïde est un ensemble muni d'actions dérivées du produit et vérifiant des relations issues de l'associativité et des neutralités à gauche et à droite. Une opérade est une signature munie de deux opérations, la composition et le produit, toutes deux vérifiant des relations d'associativité et d'unité. Un module sur une telle catégorie sera donc une signature munie d'actions dérivées de ces deux opérations et vérifiant des relations similaires.

Définition. Soit \mathbb{C} une opérade. Un \mathbb{C} -module est une signature Σ munie de quatre familles d'applications :

1. *précompositions* :

$$\begin{aligned} \mathbb{C}(m, n) \times \Sigma(n, p) &\longrightarrow \Sigma(m, p) \\ (f, g) &\longmapsto g \circ f \end{aligned}$$

2. *postcompositions* :

$$\begin{aligned} \Sigma(m, n) \times \mathbb{C}(n, p) &\longrightarrow \Sigma(m, p) \\ (f, g) &\longmapsto g \circ f \end{aligned}$$

3. *produits à gauche* :

$$\begin{aligned}\mathbb{C}(m, n) \times \Sigma(p, q) &\longrightarrow \Sigma(m + p, n + q) \\ (f, g) &\longmapsto f \otimes g\end{aligned}$$

4. *produits à droite* :

$$\begin{aligned}\Sigma(m, n) \times \mathbb{C}(p, q) &\longrightarrow \Sigma(m + p, n + q) \\ (f, g) &\longmapsto f \otimes g\end{aligned}$$

vérifiant les relations suivantes :

- associativité des compositions : $(h \circ g) \circ f = h \circ (g \circ f)$ pour toutes flèches h de Σ et f, g de \mathbb{C} ou g, h de \mathbb{C} et f de Σ et possédant des sources et buts compatibles ;
- unités pour les compositions : $n \circ f = f \circ m = f$ pour toute flèche $f \in \Sigma(m, n)$;
- associativité des produits : $(f \otimes g) \otimes h = f \otimes (g \otimes h)$ pour toutes flèches f, g de \mathbb{C} et h de Σ ou f de Σ et g, h de \mathbb{C} ;
- unités pour les produits : $0 \otimes f = f \otimes 0 = f$ pour toute flèche f de Σ .

Un *morphisme de \mathbb{C} -modules* est un morphisme de signatures qui est compatible avec la structure. Les \mathbb{C} -modules et leurs morphismes forment une catégorie notée $\mathbb{C}\text{-MOD}$. ♦

L'exemple essentiel ici est celui du *\mathbb{C} -module diagonal*, noté \mathbb{C}^2 . Ses flèches sont les couples de flèches parallèles de \mathbb{C} :

$$\mathbb{C}^2(m, n) = \mathbb{C}(m, n) \times \mathbb{C}(m, n).$$

Les quatre actions de \mathbb{C} sur \mathbb{C}^2 sont :

1. *précomposition* : si $f \in \mathbb{C}(m, n)$ et $(g, h) \in \mathbb{C}^2(n, p)$, on pose

$$(g, h) \circ f = (g \circ f, h \circ f) ;$$

2. *postcomposition* : si $(g, h) \in \mathbb{C}^2(m, n)$ et $f \in \mathbb{C}(n, p)$, on pose

$$f \circ (g, h) = (f \circ g, f \circ h) ;$$

3. *produit à gauche* : si $f \in \mathbb{C}(m, n)$ et $(g, h) \in \mathbb{C}^2(p, q)$, on pose

$$f \otimes (g, h) = (f \otimes g, f \otimes h) ;$$

4. *produit à droite* : si $(g, h) \in \mathbb{C}^2(m, n)$ et $f \in \mathbb{C}(p, q)$, on pose

$$(g, h) \otimes f = (g \otimes f, h \otimes f).$$

Ce module diagonal nous permet de définir les notions de relation/règle de réécriture et d'idéal/relation de réduction sur une opérade :

Définition. Soit \mathbb{C} une opérade. Une *relation* ou *règle de réécriture* sur \mathbb{C} est un élément du \mathbb{C} -module diagonal, c'est-à-dire un couple de flèches parallèles de \mathbb{C} . Si \mathbb{M} est un \mathbb{C} -module, un *sous- \mathbb{C} -module de \mathbb{M}* est une sous-signature de la signature (sous-jacente à) \mathbb{M} qui est stable pour les quatre opérations de \mathbb{C} -module de \mathbb{M} . Un sous- \mathbb{C} -module du module diagonal est appelé *idéal de \mathbb{C}* ou *relation de réduction sur \mathbb{C}* . \blacklozenge

3.3.2 Idéal engendré par une famille de relations

Dans une opérade \mathbb{C} , on veut associer un idéal $(R) = \rightarrow_R$ à une famille R de relations. Une première possibilité est de considérer R comme une relation binaire sur les flèches parallèles de \mathbb{C} . On définit alors \rightarrow_R comme la plus petite relation binaire sur \mathbb{C} qui est compatible avec la structure d'opérade, c'est-à-dire avec la composition (des deux côtés) et avec le produit (des deux côtés). Cependant, on préférera, comme pour les monoïdes, construire l'idéal engendré par une sous-signature du \mathbb{C} -module diagonal ; la construction est identique en essence, c'est le point de vue adopté qui diffère.

Soient \mathbb{C} une opérade et \mathcal{R} une sous-signature du \mathbb{C} -module diagonal \mathbb{C}^2 . Intuitivement, l'idéal de \mathbb{C} engendré par \mathcal{R} , noté (\mathcal{R}) ou $\rightarrow_{\mathcal{R}}$ est obtenu ainsi : ses flèches sont toutes celles que l'on peut construire en partant d'une flèche de \mathcal{R} (c'est-à-dire un couple de flèches de \mathbb{C}) et en lui superposant (composition) et juxtaposant (produit) un nombre fini de flèches de \mathbb{C} .

On définit $(\mathcal{R})(m, n)$ comme l'ensemble des couples (f, g) de flèches de $\mathbb{C}(m, n)$ telles qu'il existe $p, q, i, i', j, j' \in \mathbb{N}$, $\alpha \in \mathcal{R}(p, q)$, $h_1 \in \mathbb{C}(m, i + p + j)$, $h_2 \in \mathbb{C}(i' + q + j')$, $k_1 \in \mathbb{C}(i, i')$ et $k_2 \in \mathbb{C}(j, j')$ qui satisfont :

$$(f, g) = h_2 \circ (k_1 \otimes \alpha \otimes k_2) \circ h_1.$$

On vérifie :

Proposition 3.6. *La sous-signature (\mathcal{R}) de \mathbb{C}^2 est le plus petit idéal de \mathbb{C} contenant \mathcal{R} .*

Démonstration. On vérifie d'abord que (\mathcal{R}) est un idéal de \mathbb{C} , c'est-à-dire que (\mathcal{R}) est stable pour les quatre actions diagonales de \mathbb{C} sur \mathbb{C}^2 . Pour les compositions, c'est évident ; pour les produits, par exemple à gauche :

$$k \otimes (h_2 \circ (k_1 \otimes \alpha \otimes k_2) \circ h_1) = (t(k) \otimes h) \circ (k \otimes k_1 \otimes \alpha \otimes k_2) \circ (s(k) \otimes h_1).$$

Supposons que I soit un idéal de \mathbb{C} contenant \mathcal{R} et que $(f, g) \in (\mathcal{R})$. La décomposition de (f, g) donnée par la définition de (\mathcal{R}) dit que (f, g) est obtenu à partir d'une flèche α de \mathcal{R} par produits et compositions avec des flèches de \mathbb{C} . Le fait que I soit un idéal de \mathbb{C} contenant \mathcal{R} nous assure alors que $(f, g) \in I$. \diamond

On appelle $(\mathcal{R}) = \rightarrow_{\mathcal{R}}$ l'idéal de \mathbb{C} engendré par \mathcal{R} ou la relation de réduction sur \mathbb{C} engendrée par \mathcal{R} . On peut alors définir la notion essentielle de ce travail :

Définition. Une *présentation d'opérade* est un couple (Σ, \mathcal{R}) composé d'une signature Σ et d'une sous-signature \mathcal{R} du module diagonal associé à l'opérade libre $\mathcal{L}\Sigma$ engendrée par Σ .

L'ARS associé à une telle présentation est le couple $(\text{Fl } \mathcal{L}\Sigma, \text{Fl}(\mathcal{R}))$ formé de l'ensemble des flèches de $\mathcal{L}\Sigma$ et de la relation binaire sous-jacente à l'idéal de $\mathcal{L}\Sigma$ engendré par \mathcal{R} .

On dit qu'une présentation d'opérade *termine*, qu'elle est *confluente*, etc. si son ARS associé possède la même propriété. Dans le cas où (Σ, \mathcal{R}) est convergente, on note $\mathcal{R}(f)$ l'unique forme normale d'une flèche f de \mathbb{C} . \blacklozenge

3.4 Contextes et construction alternative de l'idéal engendré par des relations

Dans le cas des monoïdes, les contextes sont des éléments du module libre engendré par un singleton. Nous allons calquer cette construction pour définir les contextes sur une opérade. Dans un premier temps, nous allons construire le module libre engendré par une signature, puis nous verrons quelle signature prendre comme génératrice pour les contextes, ainsi que l'interprétation des relations de réduction que l'on peut en déduire.

3.4.1 Module libre engendré par une signature

Soient \mathbb{C} une opérade et Σ une signature. Intuitivement, les flèches du \mathbb{C} -module libre engendré par Σ vont être obtenues en partant d'une flèche de Σ et en rajoutant formellement des flèches de \mathbb{C} par produit et composition. Cependant, les relations de compatibilité que l'on va exiger entre les actions de \mathbb{C} font que l'on peut se contenter de ne faire le produit que par des identités.

On définit $\mathbb{C}\Sigma$ comme la signature suivante :

$$\mathbb{C}\Sigma(m, n) = \left(\coprod_{p, q, i, j \in \mathbb{N}} \mathbb{C}(m, i + p + j) \times \Sigma(p, q) \times \mathbb{C}(i + q + j, n) \right) / \simeq$$

dont un élément (g, f, h) est noté $h \circ (i \otimes f \otimes j) \circ g$ avec les i, j adéquats et où \simeq est la relation d'équivalence engendrée par les *relations élémentaires d'échanges pour les modules* :

$$\begin{aligned} & h \circ (j \otimes f \otimes j') \circ \left((k \otimes p \otimes k') \circ g \right) \\ & \simeq \left(h \circ (k \otimes q \otimes k') \right) \circ (i \otimes f \otimes i') \circ g \end{aligned}$$

pour tous $m, n, p, q, i, i', j, j' \in \mathbb{N}$, $f \in \Sigma(p, q)$, $g \in \mathbb{C}(m, i + p + i')$, $h \in \mathbb{C}(j + q + j')$, $k \in \mathbb{C}(i, j)$ et $k' \in \mathbb{C}(i', j')$. La figure 3.3 illustre l'opération correspondante à l'aide de diagrammes.

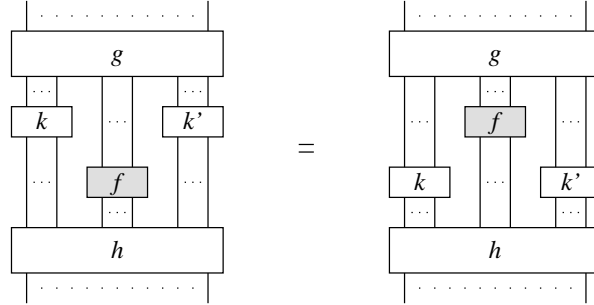


FIG. 3.3 – Relation d'échange pour les modules, illustrée par des diagrammes.

On munit cette signature des opérations désirées :

1. *précomposition* : si $k \in \mathbb{C}(m, n)$ et $(h \circ (i \otimes f \otimes j) \circ g) \in \mathbb{C}\Sigma(n, p)$, on pose

$$(h \circ (i \otimes f \otimes j) \circ g) \circ k = h \circ (i \otimes f \otimes j) \circ (g \circ k);$$

2. *postcomposition* : si $(h \circ (i \otimes f \otimes j) \circ g) \in \mathbb{C}\Sigma(m, n)$ et $k \in \mathbb{C}(n, p)$, on pose

$$k \circ (h \circ (i \otimes f \otimes j) \circ g) = (k \circ h) \circ (i \otimes f \otimes j) \circ g;$$

3. *produit à gauche* : si $k \in \mathbb{C}(m, n)$ et $(h \circ (i \otimes f \otimes j) \circ g) \in \mathbb{C}\Sigma(p, q)$, on pose

$$k \otimes (h \circ (i \otimes f \otimes j) \circ g) = (n \otimes h) \circ ((n + i) \otimes f \otimes j) \circ (k \otimes g);$$

4. *produit à droite* : si $(h \circ (i \otimes f \otimes j) \circ g) \in \mathbb{C}\Sigma(m, n)$ et $k \in \mathbb{C}(p, q)$, on pose

$$(h \circ (i \otimes f \otimes j) \circ g) \otimes k = (h \otimes q) \circ (i \otimes f \otimes (j + q)) \circ (g \otimes k).$$

On doit vérifier que :

Proposition 3.7. *La signature $\mathbb{C}\Sigma$ munie de ces opérations est un \mathbb{C} -module. De plus, l'application $\Sigma \mapsto \mathbb{C}\Sigma$ s'étend en un foncteur $\mathbf{Sgn} \rightarrow \mathbf{C-Mod}$ qui est adjoint à gauche du foncteur oubli $\mathcal{U} : \mathbf{C-Mod} \rightarrow \mathbf{Sgn}$. Autrement dit, pour toute signature Σ , le couple $(\mathbb{C}\Sigma, i)$, où $i : \Sigma \rightarrow \mathcal{U}\mathbb{C}\Sigma$ est l'application qui envoie $f \in \Sigma(m, n)$ sur $n \circ (0 \otimes f \otimes 0) \circ m$, est solution du problème universel suivant :*

pour tout \mathbb{C} -module \mathbb{M} et tout morphisme de signatures $\varphi : \Sigma \rightarrow \mathcal{U}\mathbb{M}$, il existe un unique morphisme de \mathbb{C} -modules $\psi : \mathbb{C}\Sigma \rightarrow \mathbb{M}$ tel que le diagramme

$$\begin{array}{ccc} \Sigma & \xrightarrow{i} & \mathcal{U}\mathbb{C}\Sigma \\ & \searrow \varphi & \downarrow \mathcal{U}\psi \\ & & \mathcal{U}\mathbb{M} \end{array}$$

commute.

Démonstration. Pour vérifier que $\mathbb{C}\Sigma$ est un \mathbb{C} -module, on constate facilement que les quatre actions définies passent au quotient par la relation d'équivalence \simeq utilisée lors de la construction de $\mathbb{C}\Sigma$. Maintenant, soient \mathbb{M} un \mathbb{C} -module et $\varphi : \Sigma \rightarrow \mathcal{U}\mathbb{M}$ un morphisme de signatures. On définit ψ par :

$$\psi(h \circ (i \otimes f \otimes j) \circ g) = h \circ (i \otimes \varphi(f) \otimes j) \circ g.$$

Il est clair que l'on construit ainsi un morphisme de \mathbb{C} -modules $\psi : \mathbb{C}\Sigma \rightarrow \mathbb{M}$ qui étend φ . Or, tout morphisme $\omega : \mathbb{C}\Sigma \rightarrow \mathbb{M}$ est entièrement déterminé par ses valeurs sur les flèches de Σ puisqu'il vérifie forcément :

$$\omega(h \circ (i \otimes f \otimes j) \circ g) = h \circ (i \otimes \omega(f) \otimes j) \circ g.$$

Ceci prouve que ψ est unique. ◇

3.4.2 Contextes sur une opérade

Pour un monoïde M (un ensemble avec structure), nous avons défini les contextes comme les éléments du M -module libre engendré par $\{\square\}$, un ensemble réduit à un élément. Or, un tel ensemble est un *objet terminal* de la catégorie des ensembles, c'est-à-dire que, pour tout ensemble X , il existe une unique application $X \longrightarrow \{\square\}$.

Ceci donne l'intuition pour définir les contextes sur une opérade - une signature avec structure. Tout d'abord, rappelons quel est l'objet terminal de la catégorie des signatures, c'est-à-dire la signature \square telle que, pour toute signature Σ , il existe un unique morphisme de signatures $\Sigma \longrightarrow \square$:

Rappel. On appelle *signature terminale* la signature notée \square et définie par : $\square(m, n)$ est un ensemble à un élément pour tous m et n . Cet élément est noté \square_n^m .

On peut alors définir les contextes :

Définition. Soit \mathbb{C} une opérade. Un *contexte sur \mathbb{C}* est une flèche du \mathbb{C} -module libre engendré par \square . Sa *valence externe* est le couple formé par sa source et son but. On note \mathcal{CC} le \mathbb{C} -module des contextes sur \mathbb{C} . \blacklozenge

En considérant la construction de \mathcal{CC} , on voit que tout contexte est obtenu à partir d'un \square_n^m , unique pour chaque contexte. Pour un contexte obtenu à partir de \square_n^m , on appelle *valence interne* le couple (m, n) . On note $\mathcal{CC}(m, n; p, q)$ l'ensemble des contextes de valence interne (m, n) et de valence externe (p, q) . D'après la construction de \mathcal{CC} , un tel contexte C est de la forme :

$$h \circ (i \times \square_n^m \times j) \circ g,$$

avec $g \in \mathbb{C}(p, i + m + j)$ et $h \in \mathbb{C}(i + n + j, q)$. Notons que les flèches g et h ne sont déterminées qu'aux relations d'échange près.

Ceci étant noté, on peut définir l'action d'un contexte $C \in \mathcal{CC}(m, n; p, q)$ sur les flèches de \mathbb{C} . Cette action n'est toutefois pas définie partout ; on choisit g et h des flèches de \mathbb{C} ainsi que i et j des entiers tels que $C = h \circ (i \times \square_n^m \times j) \circ g$ et on pose :

$$\begin{aligned} C[\cdot] : \mathbb{C}(m, n) &\longrightarrow \mathbb{C}(p, q) \\ f &\longmapsto C[f] = h_2 \circ (i \otimes f \otimes j) \circ h_1. \end{aligned}$$

On doit tout de même vérifier que c'est bien défini, c'est-à-dire que la valeur de $C[f]$ est indépendante des g, h, i, j choisis. Cela revient à constater que :

$$h' \circ (i' \otimes f \otimes j') \circ g' = h \circ (i \otimes f \otimes j) \circ g$$

dès que :

$$h' \circ (i' \otimes \square \otimes j') \circ g' \simeq h \circ (i \otimes \square \otimes j) \circ g.$$

Or, d'après la définition de \simeq , il est équivalent de voir que :

Lemme 3.8. *Pour tous $m, n, p, q, i, i', j, j' \in \mathbb{N}$, $f \in \mathbb{C}(p, q)$, $g \in \mathbb{C}(m, i + p + j)$, $h \in \mathbb{C}(i' + q + j', n)$, $k_1 \in \mathbb{C}(i, i')$ et $k_2 \in \mathbb{C}(j, j')$, on a :*

$$\begin{aligned} & h \circ (i' \otimes f \otimes j') \circ \left((k_1 \otimes p \otimes k_2) \circ g \right) \\ = & \left(h \circ (k_1 \otimes q \otimes k_2) \right) \circ (i \otimes f \otimes j) \circ g. \end{aligned}$$

Démonstration. C'est une conséquence de la relation de compatibilité entre le produit et la composition sur \mathbb{C} :

$$(h \otimes k) \circ (f \otimes g) = (h \circ f) \otimes (k \circ g)$$

pour toutes flèches f, g, h, k de \mathbb{C} vérifiant $t(f) = s(h)$ et $t(g) = s(k)$. \diamond

On garde la même intuition que pour l'action d'un contexte sur un monoïde : on obtient bien $C[f]$ en remplaçant, dans C , le symbole \square_n^m par f . On remarque aussi que les contextes se composent, à condition de vérifier certaines conditions de valence : si C et D sont deux contextes, on peut définir $C \circ D$ si la valence externe de D et la valence interne de C sont égales. Cette composition munit \mathcal{CC} d'une structure de catégorie qui agit à gauche sur la signature sous-jacente à \mathbb{C} .

Remarque. Comme dans le cas des monoïdes, on pourrait définir des n -contextes pour tout n . On s'apercevrait que tous ces contextes s'organisent en une structure qui rappelle encore l'opérade (classique) des petits cubes.

Les \mathbb{C} -contextes fournissent encore une autre interprétation des idéaux de \mathbb{C} , en notant que l'action d'un contexte C de valence interne (m, n) s'étend diagonalement à $\mathbb{C}^2(m, n)$ par $C(\alpha) = (C(s(\alpha)), C(t(\alpha)))$:

Proposition 3.9. *Soient \mathbb{C} une opérade et \mathcal{R} une partie de \mathbb{C}^2 . Les flèches $m \longrightarrow n$ de l'idéal de \mathbb{C} engendré par \mathcal{R} sont exactement les flèches de la forme $C[\alpha]$ où $\alpha \in \mathcal{R}(p, q)$ et $C \in \mathcal{CC}(p, q; m, n)$.*

Démonstration. Soit $(f, g) \in \mathbb{C}(m, n)$ telles que $(f, g) \in (\mathcal{R})$. Par construction de (\mathcal{R}) , il existe des entiers p et q , une règle $\alpha \in \mathcal{R}(p, q)$ et des flèches h_1, h_2, k_1, k_2 de \mathbb{C} telles que :

$$(f, g) = h_2 \circ (k_1 \otimes \alpha \otimes k_2) \circ h_1.$$

Or :

$$h_2 \circ (k_1 \otimes \alpha \otimes k_2) \circ h_1 = h_2 \circ (t(k_1) \otimes \alpha t(k_2)) \circ ((k_1 \otimes p \otimes k_2) \circ h_1).$$

Donc, en posant $C = h_2 \circ (t(k_1) \otimes \square \otimes t(k_2)) \circ ((k_1 \otimes p \otimes k_2) \circ h_1)$, on a bien $(f, g) = C[\alpha]$. L'inclusion réciproque est évidente. \diamond

3.5 Retour aux présentations de monoïdes

À partir d'un ensemble X de lettres, on a construit, au chapitre 2, un monoïde libre $\langle X \rangle$ et défini la relation de réduction \rightarrow_R engendrée par une famille R de règles de réécriture. D'autre part, au début du chapitre 3, on a construit une opérade \mathbb{X} dont les flèches $n \rightarrow n$ sont les n -uplets de mots de $\langle X \rangle$. On se pose la question de savoir si \mathbb{X} est l'opérade librement engendrée par une signature obtenue à partir de X .

Soit $f : n \rightarrow n$ une flèche de \mathbb{X} . Alors $f = a_1 \otimes \cdots \otimes a_n$ où les a_i sont des mots de $\langle X \rangle$; de plus, chaque a_i , en tant qu'élément du monoïde libre engendré par X , s'écrit $a_i = x_{i,1} \circ \cdots \circ x_{i,k_i}$. Ainsi, toute flèche de \mathbb{X} est obtenue par produit de composées d'éléments de X . Réciproquement, tout élément de X étant aussi un mot de $\langle X \rangle$, les composées et les produits de lettres de X sont des flèches de \mathbb{X} . Les éléments de X , vus comme des flèches $1 \rightarrow 1$ sont donc des générateurs des flèches de \mathbb{C} , en tant que catégorie monoïdale.

Ceci conduit à associer à tout ensemble X , la signature Σ_X donnée par :

$$\Sigma_X(m, n) = \begin{cases} X & \text{si } m = n = 1 \\ \emptyset & \text{sinon.} \end{cases}$$

Alors, on vérifie que :

Proposition 3.10. *L'opérade \mathbb{X} est l'opérade librement engendrée par la signature Σ_X .*

Démonstration. On constate que (\mathbb{X}, i) , où i est l'application qui envoie tout élément x de X sur la flèche $x \in \mathbb{X}(1, 1)$, est solution du problème universel d'opérade libre engendrée par Σ_X . Tout morphisme $\varphi : \mathbb{X} \rightarrow \mathbb{C}$, où \mathbb{C} est une opérade quelconque, est entièrement déterminé par ses valeurs sur les éléments de X , puisque toutes les flèches de \mathbb{X} se décomposent comme produit de composées de flèches de Σ_X , c'est-à-dire d'éléments de X . Comme ces valeurs peuvent être choisies librement, on a bien, pour toute

application $f : \Sigma_X \longrightarrow \mathcal{UC}$, une unique extension comme morphisme $\mathbb{X} \longrightarrow \mathbb{C}$. Donc \mathbb{X} et $\mathcal{L}\Sigma_X$ sont toutes deux solutions du problème d'opérade libre engendrée par Σ_X et sont donc, à ce titre, isomorphes à un unique isomorphisme près : on peut donc dire qu'elles sont identiques. \diamond

On a le résultat suivant :

Théorème 3.11. *Soit (X, R) une présentation de monoïde. En voyant R comme une sous-signature \mathcal{R} de $(\mathcal{L}\Sigma_X)^2$ ne contenant que des flèches $1 \longrightarrow 1$, l'ARS $(\text{Fl } \mathcal{L}\Sigma_X, \text{Fl } (\mathcal{R}))$ associé à la présentation (Σ_X, \mathcal{R}) contient l'ARS $(\langle X \rangle, (R))$ associé à (X, R) . Plus précisément, il existe un isomorphisme d'ARS :*

$$(\mathcal{L}\Sigma_X(1, 1), (\mathcal{R})(1, 1)) \simeq (\langle X \rangle, (R)).$$

Démonstration. On constate tout d'abord que les flèches de $\mathcal{L}\Sigma_X(1, 1)$ sont les flèches de $\mathcal{L}\Sigma_X$ de la forme $x_1 \circ \cdots \circ x_n$ avec tous les x_i dans $\Sigma_X(1, 1) = X$. En d'autres termes, $\mathcal{L}\Sigma_X(1, 1) = \langle X \rangle$. Il reste à voir que les deux relations de réductions \rightarrow_R et $\rightarrow_{\mathcal{R}}$ coïncident. Si $a, b \in \langle X \rangle$ sont tels que $a \rightarrow_R b$ alors il existe $\alpha \in R$ et $u, v \in \langle X \rangle$ tels que $(a, b) = u\alpha v$. Si on voit a, b, u, v comme des flèches de $\mathcal{L}\Sigma_X(1, 1)$ et α comme une flèche de $\mathcal{L}\Sigma_X^2(1, 1)$, on a : $(a, b) = u \circ \alpha \circ v$ et donc $a \rightarrow_{\mathcal{R}} b$.

Réciproquement, si f et g sont des flèches de $\mathcal{L}\Sigma_X(1, 1)$ telles que $f \rightarrow_{\mathcal{R}} g$, il existe $\alpha \in \text{Fl } \mathcal{R}$ et $h_1, h_2, k_1, k_2 \in \text{Fl } \mathcal{L}\Sigma_X$ tels que $(f, g) = h_2 \circ (k_1 \otimes \alpha \otimes k_2) \circ h_1$. Or, comme $\text{Fl } \mathcal{R} = \mathcal{R}(1, 1)$ et que $f, g \in \mathcal{L}\Sigma_X(1, 1)$, on a $k_1, k_2 \in \mathcal{L}\Sigma_X(0, 0) = \{0\}$ et donc $(f, g) = h_2 \circ \alpha \circ h_1$ avec $h_1, h_2 \in \mathcal{L}\Sigma_X(1, 1)$. On peut donc voir α comme un élément de R et f, g, h_1, h_2 comme des éléments de $\langle X \rangle$ avec $(f, g) = h_2 \alpha h_1$, d'où on conclut que $f \rightarrow_R g$.

Les deux ARS $(\mathcal{L}\Sigma_X(1, 1), (\mathcal{R})(1, 1))$ et $(\langle X \rangle, (R))$ sont donc isomorphes (ils sont mêmes égaux). \diamond

Il apparaît donc que les présentations d'opérades sont des généralisations des présentations de monoïdes ou systèmes de réécriture de mots. Nous verrons au chapitre 4 qu'elles englobent aussi les présentations de monoïdes commutatifs, c'est-à-dire les réseaux de Petri.

3.6 Présentation d'une opérade et problème de mots

Au chapitre 2, nous avons vu que tout monoïde admet une présentation : pour tout monoïde M , il existe un ensemble X et une partie R de $\langle X \rangle^2$, tels que $M \simeq \langle X \rangle / \equiv_R$, où \equiv_R est la congruence sur $\langle X \rangle$ engendrée par R . On a déjà vu les notions d'opérade libre engendrée par une signature et de quotient d'une opérade par une famille de règles. En combinant les deux, on a :

Définition. Une opéade \mathbb{C} admet une présentation (Σ, \mathcal{R}) si $\mathbb{C} \simeq \mathcal{L}\Sigma/\mathcal{R}$. On dit aussi, dans ce cas, que (Σ, \mathcal{R}) présente \mathbb{C} . On dit qu'une présentation (Σ, \mathcal{R}) est *finie* si $\text{Fl } \Sigma$ et $\text{Fl } \mathcal{R}$ sont finis. Deux présentations sont dites *équivalentes* si elles présentent la même opéade. \blacklozenge

Comme pour les monoïdes, on a :

Proposition 3.12. *Toute opéade admet une présentation.*

Démonstration. Soient \mathbb{C} une opéade et \mathcal{UC} sa signature sous-jacente. Alors \mathbb{C} est isomorphe au quotient de \mathcal{LC} par la congruence engendrée par la réunion des familles suivantes de relations :

$$\left\{ \begin{array}{ll} (g \circ f, g \circ_{\mathbb{C}} f) & \text{pour toutes flèches composables } f \text{ et } g \text{ de } \mathbb{C}; \\ (f \otimes g, f \otimes_{\mathbb{C}} g) & \text{pour toutes flèches } f \text{ et } g \text{ de } \mathbb{C}; \\ (n, n_{\mathbb{C}}) & \text{pour tout entier } n. \end{array} \right.$$

On a noté $\circ_{\mathbb{C}}$, $\otimes_{\mathbb{C}}$ et $n_{\mathbb{C}}$ les opérations et identités de \mathbb{C} et \circ , \otimes et n celles de \mathcal{LC} . \diamond

On a alors un problème de mots (ou d'opérateurs) : étant données une opéade \mathbb{C} et une présentation (Σ, \mathcal{R}) de \mathbb{C} , existe-t-il un algorithme qui décide si deux flèches parallèles f et g de $\mathcal{L}\Sigma$ représentent la même flèche de \mathbb{C} ? Encore une fois, si la présentation est convergente et finie, on a un tel algorithme :

Proposition 3.13. *Soient (Σ, \mathcal{R}) une présentation convergente d'opéade et f et g deux flèches parallèles de $\mathcal{L}\Sigma$. Alors, on a $f \equiv_{\mathcal{R}} g$ si et seulement si $\mathcal{R}(f) = \mathcal{R}(g)$.*

Ceci motive encore une fois la recherche d'une présentation convergente pour une opéade donnée. L'examen des procédures de complétion définies au chapitre 2, concernant les présentations de monoïdes, nous indique que la théorie se transpose immédiatement au cas des présentations d'opéades : en effet, les définitions, résultats et preuves sont indépendants de la structure algébrique.

En revanche, dans le cas des présentations d'opéades, il existe deux obstacles majeurs au fonctionnement de telles procédures de complétion : d'une part, définir et construire des ordres de réduction et, d'autre part, définir et calculer les paires critiques d'une présentation donnée. Nous allons à présent nous intéresser à ces deux problèmes.

3.7 Terminaison d'une présentation d'opéade

Nous allons définir ce qu'est un ordre de réduction, puis développer une technique d'interprétation permettant d'en construire et, éventuellement, de montrer qu'une présentation d'opéade termine.

3.7.1 Ordres de réduction sur une opérade

Les ordres de réduction fournissent, comme pour les monoïdes, un critère de terminaison.

Définition. Soit \mathbb{C} une opérade. Un *ordre de réduction* sur \mathbb{C} est un idéal $>$ de \mathbb{C} tel que chaque $> (m, n)$ est un ordre strict sur l'ensemble $\mathbb{C}(m, n)$ et tel que chaque ARS $(\mathbb{C}(m, n), > (m, n))$ termine. \blacklozenge

Théorème 3.14. Une présentation (Σ, \mathcal{R}) termine si et seulement s'il existe un ordre de réduction sur $\mathcal{L}\Sigma$ contenant \mathcal{R} .

Démonstration. Supposons que (Σ, \mathcal{R}) termine. Alors, la relation $\rightarrow_{\mathcal{R}}^+$ sur $\mathcal{L}\Sigma$ convient. En effet, on sait déjà que $\rightarrow_{\mathcal{R}}^+$ est transitive et que c'est un idéal de $\mathcal{L}\Sigma$ qui contient \mathcal{R} . Le reste vient du fait que (Σ, \mathcal{R}) termine : $\rightarrow_{\mathcal{R}}^+$ est forcément antiréflexive, car sinon on pourrait construire un chemin de réduction infini ; le même argument donne la terminaison de $\rightarrow_{\mathcal{R}}^+$.

Réciproquement, supposons qu'il existe un ordre de réduction $>$ sur $\mathcal{L}\Sigma$ qui contienne les relations \mathcal{R} . Alors, l'identité de $\mathcal{L}\Sigma$ induit un morphisme d'ARS $(\text{Fl } \mathcal{L}\Sigma, \rightarrow_{\mathcal{R}}) \rightarrow (\text{Fl } \mathcal{L}\Sigma, >)$. Comme $>$ termine, l'ARS $(\text{Fl } \mathcal{L}\Sigma, \rightarrow_{\mathcal{R}})$ termine et donc (Σ, \mathcal{R}) aussi. \blacklozenge

Malgré ce résultat, nous n'avons pas encore de technique générale pour prouver qu'une présentation termine. On peut espérer trouver une méthode pour chaque exemple qui nous intéresse, par exemple en généralisant certaines techniques issues de la réécriture de termes. Ceci fonctionne pour des présentations particulières comme celle de l'opérade cartésienne initiale \mathbb{F}^0 que nous rencontrerons plus loin : celle-ci ne possède aucune flèche de source 0 (autre que l'identité 0), ce qui permet d'utiliser une interprétation classique (contravariante), comme l'a fait Yves Lafont dans [Laf03].

Cependant, presque toutes les présentations d'opérades qui nous intéressent ici possèdent à la fois des opérateurs de source 0 et des opérateurs de but 0 (la plupart du temps, il s'agit respectivement d'une constante et de l'effacement). C'est le cas, par exemple, de la présentation de la théorie algébrique libre (que nous étudierons au chapitre 5), dès que la théorie équationnelle correspondante possède une constante. C'est aussi le cas de la présentation de l'opérade des $\mathbb{Z}/2\mathbb{Z}$ -espaces vectoriels donnée dans [Laf03] et rappelée en 3.7.7. Dans ces situations, les techniques issues de la réécriture de termes ne fonctionnent plus, ce qui a empêché, jusqu'alors, de prouver la terminaison des présentations citées. Pour combler ce manque, nous allons développer ici une technique d'interprétation adaptée à la structure algébrique d'opérade et permettant de vérifier la terminaison de nombreuses présentations.

3.7.2 Une technique classique d'interprétation en réécriture de termes

Nous y reviendrons plus loin mais disons, pour l'instant, qu'un système de réécriture de termes est une présentation d'opéride dont la signature ne contient que des flèches de but 1.

L'idée de la technique classique d'interprétation est d'associer à chaque opérateur $f : n \longrightarrow 1$ une application $f_* : \mathbb{N}^n \longrightarrow \mathbb{N}$, de telle sorte que, si $f \rightarrow g$ alors $f_* > g_*$; l'ordre sur les applications est donné point par point par celui de \mathbb{N} . Notons que \mathbb{N} peut-être remplacé par tout autre ensemble muni d'une relation d'ordre qui termine; d'ailleurs, c'est souvent l'ensemble \mathbb{N}^* des entiers naturels non nuls qui est utilisé, pour des raisons de simplicité des expressions.

Supposons que l'on a construit une telle interprétation : on a alors un morphisme d'ARS dont le but termine, ce qui prouve bien la terminaison du système de réécriture d'origine. Une méthode simple pour construire $(\cdot)_*$ est d'associer à chaque opérateur $\varphi : n \longrightarrow 1$ de la signature une application strictement croissante $\varphi_* : \mathbb{N}^n \longrightarrow \mathbb{N}$; on l'étend par propriété universelle à tous les opérateurs de l'opéride libre. On aura alors une interprétation satisfaisante si, pour toute règle α , on a $s(\alpha)_* > t(\alpha)_*$. Le fait que tous les φ_* soient strictement croissants nous permet en effet de conclure que $f_* > g_*$ dès que $f \rightarrow_\alpha g$.

Or, il n'est pas toujours possible d'associer une application strictement croissante à chaque générateur. Par suite, et même si $s(\alpha)_* > t(\alpha)_*$ pour toute règle α , on n'a pas forcément $f_* > g_*$ dès que $f \rightarrow_\alpha g$.

En effet, considérons une présentation (Σ, R) telle que la signature Σ contient à la fois une constante $\gamma : 0 \longrightarrow 1$ et une coconstante $\varepsilon : 1 \longrightarrow 0$. Notons que c'est le cas pour la présentation $L(\mathbb{Z}_2)$, pour la présentation de l'opéride des groupes quantiques/algèbres de Hopf, ainsi que pour la plupart des présentations associées à des systèmes de réécriture de termes (voir chapitre 5).

À présent, supposons que l'on a construit un morphisme d'opérides :

$$(\cdot)_* : \mathcal{L}\Sigma \longrightarrow \text{Oper } \mathbb{N}$$

de telle sorte que, pour toute règle α de $R(m, n)$, on ait $s(\alpha)_* > t(\alpha)_*$. On voudrait alors pouvoir montrer que $f_* > g_*$ dès que $f \rightarrow_\alpha g$. Cependant :

$$(\varepsilon^n \circ s(\alpha) \circ \gamma^m)_* = (\varepsilon^n \circ t(\alpha) \circ \gamma^m)_*,$$

bien que :

$$\varepsilon^n \circ s(\alpha) \circ \gamma^m \rightarrow_R \varepsilon^n \circ t(\alpha) \circ \gamma^m.$$

En effet, ces deux opérateurs sont envoyés par $(\cdot)_*$ sur des applications $\mathbb{N}^0 \longrightarrow \mathbb{N}^0$; or, il n'existe qu'une seule application de ce type, donc les deux images doivent coïncider.

On pourrait construire de nombreux autres contre-exemples, mais celui-ci suffit pour dire que l'on n'a pas forcément $f_* > g_*$ quand $f \rightarrow_\alpha g$, même si $s(\alpha)_* > t(\alpha)_*$; autrement dit, l'ordre $>$ n'est pas compatible avec la structure d'opérade. On ne peut donc pas utiliser cette technique d'interprétation dans un cas général. Notons que le contre-exemple fonctionne aussi pour une interprétation contravariante $(\cdot)^*$ qui associerait $\varphi^* : \mathbb{N}^n \longrightarrow \mathbb{N}^m$ à $\varphi : m \longrightarrow n$.

3.7.3 Un rapide aperçu de la technique améliorée

On vient donc de voir que la comparaison des entrées/sorties d'applications f_*/f^* et g_*/g^* associées à des flèches parallèles ne fonctionnait pas comme on le voudrait ; nous allons donc compléter cette construction.

Notons que le problème provient de la catégorie dans laquelle sont faites les interprétations, celle des ensembles. Cette catégorie étant cartésienne, l'élément neutre du produit est un objet terminal, ce qui confond toutes les applications arrivant en ce point. On pourrait envisager de remplacer $\mathbb{E}NS$ par une catégorie plus appropriée au contexte, c'est-à-dire monoïdale mais pas cartésienne. La première qui vient à l'esprit est celle des espaces vectoriels sur un corps donné k , de caractéristique 0 ; cependant, l'intuition des applications à associer aux générateurs devient difficile, tandis que les calculs explosent. Nous allons donc nous en tenir à la catégorie des ensembles en contournant les difficultés évoquées, mais cette piste reste ouverte.

L'idée que nous allons développer se comprend bien en voyant les flèches d'une opérade comme des circuits, image que nous utilisons déjà pour les représentations diagrammatiques. La technique fonctionne ainsi : on imagine que l'on fait rentrer un courant d'une certaine intensité par chaque entrée et chaque sortie du circuit (la flèche étudiée) ; chaque élément du circuit (générateurs de l'opérade) réagit à ces courants en dégageant de la chaleur : on additionne la chaleur produite par chaque composant pour obtenir celle dégagée par l'ensemble du circuit ; c'est cette valeur que nous retenons pour comparer les flèches. Ainsi, au lieu de lire une variation dans le courant entre les entrées et les sorties d'un circuit (ce qui n'est pas possible s'il n'en possède pas), on considère une valeur qui existe toujours, même si le circuit ne possède ni entrée ni sortie.

Regardons quels sont les ingrédients dont on a besoin. Supposons que f soit une flèche de source m et de but n . On doit connaître trois informations :

1. Étant donnée l'intensité du courant arrivant dans chacune des m entrées de f , on doit pouvoir déterminer la valeur du courant induit dans chacune des n sorties de f ; ceci se traduit par la donnée d'une application $f_* : X^m \longrightarrow X^n$, où X est un ensemble dans lequel sont prises les intensités du courant arrivant dans les entrées.
2. De la même façon, connaissant les intensités des courants arrivant dans les sorties de f , on doit pouvoir calculer celles des courants induits dans les entrées ; on utilise une application $f^* : Y^n \longrightarrow Y^m$ pour cette opération, Y étant l'ensemble des valeurs possibles des courants arrivant dans les sorties.
3. Enfin, si on a des valeurs pour les intensités des courants arrivant dans les entrées et les sorties de f , on veut calculer la chaleur dégagée par f ; ce sera grâce à une application $[f] : X^m \times Y^n \longrightarrow M$, où M est l'ensemble dans lequel vivent les mesures de chaleur.

Ces données doivent vérifier un certain nombre de propriétés, afin d'être utilisables en pratique :

- Les applications f_* , f^* et $[f]$ doivent pouvoir se calculer à partir des φ_* , φ^* et $[\varphi]$ pour chaque générateur φ apparaissant dans f . On demandera alors à $(\cdot)_*$ et $(\cdot)^*$ d'être des foncteurs monoïdaux et on donnera une formule pour calculer $[f]$ à partir des φ_* , φ^* et $[\varphi]$. On a déjà mentionné le fait que les chaleurs vont s'obtenir en ajoutant celles dégagées par les composants élémentaire : on va demander à M d'être un monoïde commutatif.
- On veut aussi que, si on remplace dans f un sous-circuit g par un sous-circuit h , tels que g dégage plus de chaleur que h pour des courants identiques, alors f en dégage aussi plus que le circuit obtenu après remplacement. Nous verrons que c'est le cas si l'on munit X , Y et M de relations d'ordre et que l'on demande à chacune des trois applications dérivées d'un générateur φ d'être croissante.

3.7.4 L'opérade $\mathcal{O}(X, Y, M)$

On considère deux ensembles ordonnés (non vides) X et Y ainsi qu'un monoïde commutatif M muni d'un ordre strict compatible avec sa structure, c'est-à-dire vérifiant $x + z > y + z$ pour tous $x, y, z \in M$ tels que $x > y$.

À partir de ces données, on construit une opérade $\mathcal{O}(X, Y, M)$ qui contient les informations dont nous avons besoin pour interpréter les flèches d'une opérade.

On pose, pour tous m et n entiers :

$$\mathcal{O}(X, Y, M) = \mathbb{O}_{\text{RD}}(X^m, X^n) \times \mathbb{O}_{\text{RD}}(Y^n, Y^m) \times \mathbb{O}_{\text{RD}}(X^m \times Y^n, M).$$

Une flèche $f : m \longrightarrow n$ dans $\mathcal{O}(X, Y, M)$ est donc un triplet $(f_*, f^*, [f])$ d'applications croissantes : on a bien sûr muni X^m , Y^n et $X^m \times Y^n$ des ordres produits induits par ceux de X et Y . Pour l'instant, $\mathcal{O}(X, Y, M)$ n'est qu'une signature (enrichie). Nous allons définir des opérations de produit et de composition qui en feront une opéade.

Pour le produit, supposons que $f : m \longrightarrow n$ et $g : p \longrightarrow q$ sont deux flèches de $\mathcal{O}(X, Y, M)$. On définit $f \otimes g$ comme la flèche $m + p \longrightarrow n + q$ de $\mathcal{O}(X, Y, M)$ définie, composante par composante, par :

- $(f \otimes g)_* = f_* \times g_*$;
- $(f \otimes g)^* = f^* \times g^*$;
- $[f \otimes g]$ est donnée par le diagramme commutatif suivant :

$$\begin{array}{ccc} X^{m+p} \times Y^{n+q} & \xrightarrow{\simeq} & X^m \times Y^n \times X^p \times Y^q \\ [f \otimes g] \downarrow & & \downarrow [f] \times [g] \\ M & \xleftarrow{+} & M \times M \end{array}$$

Autrement dit, pour tous $\vec{x} \in X^m$, $\vec{x}' \in X^p$, $\vec{y} \in Y^n$ et $\vec{y}' \in Y^q$:

$$[f \otimes g](\vec{x}, \vec{x}', \vec{y}, \vec{y}') = [f](\vec{x}, \vec{y}) + [g](\vec{x}', \vec{y}').$$

Pour la composition, supposons que $f : m \longrightarrow n$ et $g : n \longrightarrow p$ sont deux flèches de $\mathcal{O}(X, Y, M)$. On définit $g \circ f$ comme la flèche $m \longrightarrow p$ de $\mathcal{O}(X, Y, M)$ définie, composante par composante, par :

- $(g \circ f)_* = g_* \circ f_*$;
- $(g \circ f)^* = f^* \circ g^*$;
- $[g \circ f]$ est donnée par le diagramme commutatif suivant :

$$\begin{array}{ccc} X^m \times Y^p & \xrightarrow{\delta} & X^m \times Y^p \times X^m \times Y^p \\ [g \circ f] \downarrow & & \downarrow X^m \times g^* \times f_* \times Y^p \\ M & \xleftarrow{+} M \times M & \xleftarrow{[f] \times [g]} X^m \times Y^n \times X^n \times Y^p \end{array}$$

De manière explicite, si $\vec{x} \in X^m$ et $\vec{y} \in Y^p$:

$$[g \circ f](\vec{x}, \vec{y}) = [f](\vec{x}, g^*(\vec{y})) + [g](f_*(\vec{x}), \vec{y}).$$

Pour tout entier n , l'identité de n est le triplet formé de l'identité de X^n , de l'identité de Y^n et de l'application qui envoie tous les éléments de $X^n \times Y^n$ sur 0, l'élément neutre de M . Alors :

Proposition 3.15. *Munie des opérations ainsi définies, la signature $\mathcal{O}(X, Y, M)$ est une opéade.*

Démonstration. Nous devons vérifier les assertions suivantes :

- la composition et le produit sont bien définis, c'est-à-dire que l'on obtient bien des applications croissantes ;
- la composition est associative et admet les identités comme éléments neutres locaux ;
- le produit est associatif et admet l'identité de 0 comme élément neutre bilatère ;
- le produit est fonctoriel, c'est-à-dire qu'il vérifie la relation d'échange relativement à la composition.

Étant donné que les composées et produits d'applications croissantes sont des applications croissantes - c'est-à-dire que \mathbf{ORD} , munie de son produit cartésien est une catégorie monoïdale -, il faut seulement vérifier que $[f \otimes g]$ et, le cas échéant, $[g \circ f]$ sont des applications croissantes dès que f et g sont des flèches de $\mathcal{O}(X, Y, M)$.

On suppose que $f : m \longrightarrow n$ et $g : p \longrightarrow q$ sont des flèches de $\mathcal{O}(X, Y, M)$. On veut montrer que $[f \otimes g]$ est croissante ; soient $\vec{x} \geq \vec{x}' \in X^m$, $\vec{y} \geq \vec{y}' \in Y^n$, $\vec{z} \geq \vec{z}' \in X^p$ et $\vec{t} \geq \vec{t}' \in Y^q$:

$$[f \otimes g](\vec{x}, \vec{z}, \vec{y}, \vec{t}) = [f](\vec{x}, \vec{y}) + [g](\vec{z}, \vec{t}).$$

Comme $[f]$ et $[g]$ sont croissantes, on a :

$$\begin{cases} [f](\vec{x}, \vec{y}) \geq [f](\vec{x}', \vec{y}') \\ [g](\vec{z}, \vec{t}) \geq [g](\vec{z}', \vec{t}'). \end{cases}$$

On conclut alors en utilisant le fait que \geq est compatible avec $+$ sur M .

À présent, supposons que $f : m \longrightarrow n$ et $g : n \longrightarrow p$ sont des flèches de $\mathcal{O}(X, Y, M)$. On va montrer que $[g \circ f]$ est croissante ; soient $\vec{x} \geq \vec{x}' \in X^m$ et $\vec{y} \geq \vec{y}' \in Y^p$:

$$[g \circ f](\vec{x}, \vec{y}) = [f](\vec{x}, g^*(\vec{y})) + [g](f_*(\vec{x}), \vec{y}).$$

Comme $[f]$, $[g]$, f_* et g^* sont croissantes, on a :

$$\begin{cases} [f](\vec{x}, g^*(\vec{y})) \geq [f](\vec{x}', g^*(\vec{y}')) \\ [g](f_*(\vec{x}), \vec{y}) \geq [g](f_*(\vec{x}'), \vec{y}'). \end{cases}$$

On conclut encore en utilisant le fait que \geq est compatible avec $+$ sur M .

Pour l'associativité de la composition, on suppose que $f : m \longrightarrow n$, $g : n \longrightarrow p$ et $h : p \longrightarrow q$ sont trois flèches de $\mathcal{O}(X, Y, M)$ et que $\vec{x} \in X^m$ et $\vec{y} \in Y^q$. En utilisant le fait que la composition dans \mathbf{ENS} est associative, on montre que :

$$(h \circ (g \circ f))_* = ((h \circ g) \circ f)_* \quad \text{et} \quad (h \circ (g \circ f))^* = ((h \circ g) \circ f)^*.$$

Puis :

$$\begin{aligned}
 & [h \circ [g \circ f]](\vec{x}, \vec{y}) \\
 &= [g \circ f](\vec{x}, h^*(\vec{y})) + [h]((g \circ f)_*(\vec{x}), \vec{y}) \\
 &= [f](\vec{x}, g^* \circ h^*(\vec{y})) + [g](f_*(\vec{x}), h^*(\vec{y})) + [h](g_* \circ f_*(\vec{x}), \vec{y}).
 \end{aligned}$$

D'autre part :

$$\begin{aligned}
 & [[h \circ g] \circ f](\vec{x}, \vec{y}) \\
 &= [f](\vec{x}, (h \circ g)^*(\vec{y})) + [h \circ g](f_*(\vec{x}), \vec{y}) \\
 &= [f](\vec{x}, g^* \circ h^*(\vec{y})) + [g](f_*(\vec{x}), h^*(\vec{y})) + [h](g_* \circ f_*(\vec{x}), \vec{y}).
 \end{aligned}$$

Ce qui donne, au final :

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Gardons $f : m \longrightarrow n$. Comme $p_* = \text{id}_{X^p}$ et $p^* = \text{id}_{Y^p}$ pour tout entier p , on a :

$$(f \circ m)_* = (n \circ f)_* = f_* \quad \text{et} \quad (f \circ m)^* = (n \circ f)^* = f^*.$$

En utilisant ces dernières égalités et le fait que, pour tout entier p , l'application $[p]$ est constamment égale à 0, on obtient :

$$[f \circ m] = [n \circ f] = [f].$$

Par suite :

$$f \circ m = n \circ f = f.$$

On a ainsi : $\mathcal{O}(X, Y, M)$ est une catégorie. À présent, regardons le produit : soient $f : m \longrightarrow n$, $g : p \longrightarrow q$ et $h : k \longrightarrow l$ trois flèches de $\mathcal{O}(X, Y, M)$. En utilisant l'associativité du produit cartésien de la catégorie des ensembles, on obtient les égalités suivantes :

$$((f \otimes g) \otimes h)_* = (f \otimes (g \otimes h))_* \quad \text{et} \quad ((f \otimes g) \otimes h)^* = (f \otimes (g \otimes h))^*.$$

Puis, supposons que $\vec{x} \in X^m$, $\vec{x}' \in X^p$, $\vec{x}'' \in X^k$, $\vec{y} \in Y^n$, $\vec{y}' \in Y^q$ et $\vec{y}'' \in Y^l$; alors :

$$\begin{aligned}
 & [(f \otimes g) \otimes h](\vec{x}, \vec{x}', \vec{x}'', \vec{y}, \vec{y}', \vec{y}'') \\
 &= [f \otimes g](\vec{x}, \vec{x}', \vec{y}, \vec{y}') + [h](\vec{x}'', \vec{y}'') \\
 &= [f](\vec{x}, \vec{y}) + [g](\vec{x}', \vec{y}') + [h](\vec{x}'', \vec{y}'') \\
 &= [f](\vec{x}, \vec{y}) + [g \otimes h](\vec{x}', \vec{x}'', \vec{y}' \vec{y}'') \\
 &= [f \otimes (g \otimes h)](\vec{x}, \vec{x}', \vec{x}'', \vec{y}, \vec{y}', \vec{y}'').
 \end{aligned}$$

Et donc :

$$(f \otimes g) \otimes h = f \otimes (g \otimes h).$$

En utilisant le fait que $0_* = 0^*$ est l'unique application, dans \mathbb{E}_{NS} , du singleton dans lui-même, c'est-à-dire l'élément neutre bilatère du produit cartésien de la catégorie des ensembles, on obtient :

$$(f \otimes 0)_* = (0 \otimes f)_* = f_* \quad \text{et} \quad (f \otimes 0)^* = (0 \otimes f)^* = f^*.$$

De plus, puisque $[0]$ est l'application qui envoie l'unique élément du singleton sur 0, l'élément neutre de M , on a :

$$[f \otimes 0] = [0 \otimes f] = [f].$$

D'où :

$$f \otimes 0 = 0 \otimes f = f.$$

Il reste à vérifier la relation d'échange : soient $f : m \longrightarrow n$ et $g : p \longrightarrow q$ deux flèches de $\mathcal{O}(X, Y, M)$. Le fait que

$$((t(f) \otimes g) \circ (f \otimes s(g)))_* = ((f \otimes t(g)) \circ (s(f) \otimes g))_* = (f \otimes g)_*$$

provient du fait que la catégorie \mathbb{E}_{NS} , munie de son produit cartésien, est monoïdale, et de même pour :

$$((t(f) \otimes g) \circ (f \otimes s(g)))^* = ((f \otimes t(g)) \circ (s(f) \otimes g))^* = (f \otimes g)^*.$$

Puis, si $\vec{x} \in X^m$, $\vec{x}' \in X^p$, $\vec{y} \in Y^n$ et $\vec{y}' \in Y^q$:

$$\begin{aligned} & [(t(f) \otimes g) \circ (f \otimes s(g))](\vec{x}, \vec{x}', \vec{y}, \vec{y}') \\ &= [t(f) \otimes g]((f \otimes s(g))_*(\vec{x}, \vec{x}'), \vec{y}, \vec{y}') + [f \otimes s(g)](\vec{x}, \vec{x}', (t(f) \otimes g)^*(\vec{y}, \vec{y}')) \\ &= [t(f)](f_*(\vec{x}), \vec{y}) + [g](s(g)_*(\vec{x}'), \vec{y}') + [f](\vec{x}, t(f)^*(\vec{y})) + [s(g)](\vec{x}', g^*(\vec{y}')) \\ &= [g](\vec{x}', \vec{y}') + [f](\vec{x}, \vec{y}) \\ &= [f](\vec{x}, \vec{y}) + [g](\vec{x}', \vec{y}') \\ &= [f \otimes g](\vec{x}, \vec{x}', \vec{y}, \vec{y}'). \end{aligned}$$

Notons que l'on a utilisé, pour l'avant-dernière égalité, la commutativité de M . La seconde partie de la relation d'échange,

$$[(f \otimes t(g)) \circ (s(f) \otimes g)] = [f \otimes g],$$

est traitée de manière similaire. On a donc le résultat.

◇

3.7.5 Un ordre de réduction sur $\mathcal{O}(X, Y, M)$

Montrons à présent que l'on peut munir $\mathcal{O}(X, Y, M)$ d'un ordre $>$ de réduction. Soient m et n deux entiers ; on définit des relations d'ordre, stricts ou non, sur $\mathbb{ORD}(X^m, X^n)$, $\mathbb{ORD}(Y^n, Y^m)$ et $\mathbb{ORD}(X^m \times Y^n, M)$ en rappatriant, point par point, l'ordre du but, c'est-à-dire, si f et g sont deux éléments de l'un de ces trois ensembles d'applications et si \succ est $>$ ou \geq , en posant $f \succ g$ si :

$$\text{pour tout } \vec{x}, f(\vec{x}) \succ g(\vec{x}).$$

On pose alors, si f et g sont deux flèches parallèles de $\mathcal{O}(X, Y, M)$, $f > g$ si les trois conditions suivantes sont remplies :

$$f_* \geq g_*, \quad f^* \geq g^*, \quad [f] > [g].$$

Alors :

Proposition 3.16. *La relation $>$ ainsi définie sur les flèches parallèles de $\mathcal{O}(X, Y, M)$ est un ordre strict et un idéal de $\mathcal{O}(X, Y, M)$. De plus, si $>$ termine sur M , alors $>$ est un ordre de réduction sur $\mathcal{O}(X, Y, M)$.*

Démonstration. On doit montrer, dans un premier temps, que $>$ est un ordre strict compatible avec la structure de catégorie monoïdale de $\mathcal{O}(X, Y, M)$.

Pour l'antiréflexivité : supposons qu'il existe une flèche $f : m \longrightarrow n$ de $\mathcal{O}(X, Y, M)$ telle que $f > f$. Alors, en particulier, $[f] > [f]$. Si on choisit un élément \vec{x} dans $X^m \times Y^n$, on obtient ainsi un élément $[f](\vec{x})$ de M vérifiant $[f](\vec{x}) > [f](\vec{x})$, situation exclue par l'antiréflexivité de $>$ sur M .

Pour la transitivité : supposons que f, g et h sont trois flèches parallèles de $\mathcal{O}(X, Y, M)$ vérifiant $f > g$ et $g > h$. Alors, pour tous $\vec{x} \in X^m$ et $\vec{y} \in Y^n$, on a :

$$\begin{cases} f_*(\vec{x}) \geq g_*(\vec{x}) \geq h_*(\vec{x}) \\ f^*(\vec{y}) \geq g^*(\vec{y}) \geq h^*(\vec{y}) \\ [f](\vec{x}, \vec{y}) > [g](\vec{x}, \vec{y}) > [h](\vec{x}, \vec{y}). \end{cases}$$

En utilisant la transitivité des relations d'ordre \geq sur X^m et Y^n et de la relation d'ordre strict $>$ sur M , on conclut que $f > h$.

Montrons à présent que $>$ est un idéal de $\mathcal{O}(X, Y, M)$, c'est-à-dire que, pour toute flèche h , les applications de $\text{Fl } \mathcal{O}(X, Y, M)$ dans lui-même $h \otimes \cdot$, $\cdot \otimes h$, $h \circ \cdot$ et $\cdot \circ h$ sont strictement croissantes.

Pour le produit : soient $f, g : m \longrightarrow n$ et $h : p \longrightarrow q$ trois flèches de $\mathcal{O}(X, Y, M)$ ainsi que $\vec{x} \in X^m$, $\vec{y} \in Y^n$, $\vec{z} \in X^p$ et $\vec{t} \in Y^q$. On suppose que $f > g$. Alors :

$$\begin{aligned} (f \otimes h)_*(\vec{x}, \vec{y}) &= (f_*(\vec{x}), h_*(\vec{y})) \\ &\geq (g_*(\vec{x}), h_*(\vec{y})) \\ &= (g \otimes h)_*(\vec{x}, \vec{y}). \end{aligned}$$

De même, on obtient que $(f \otimes h)^* \geq (g \otimes h)^*$. Puis, en utilisant que $>$ est compatible avec $+$ sur M :

$$\begin{aligned} [f \otimes h](\vec{x}, \vec{z}, \vec{y}, \vec{t}) &= [f](\vec{x}, \vec{y}) + [h](\vec{z}, \vec{t}) \\ &> [g](\vec{x}, \vec{y}) + [h](\vec{z}, \vec{t}) \\ &= [g \otimes h](\vec{x}, \vec{z}, \vec{y}, \vec{t}). \end{aligned}$$

D'où $f \otimes h > g \otimes h$. On démontre de même que $h \otimes f > h \otimes g$.

Pour la composition : soient $f, g : m \longrightarrow n$ et $h : n \longrightarrow p$ trois flèches de $\mathcal{O}(X, Y, M)$ et $\vec{x} \in X^m$, $\vec{y} \in Y^p$. On suppose que $f > g$. On a :

$$\begin{aligned} (h \circ f)_*(\vec{x}) &= h_* \circ f_*(\vec{x}) \\ &\geq h_* \circ g_*(\vec{x}) \\ &= (h \circ g)_*(\vec{x}). \end{aligned}$$

Pour l'inégalité, on a utilisé le fait que h_* est croissante. On a aussi :

$$\begin{aligned} (h \circ f)^*(\vec{x}) &= f^* \circ h^*(\vec{x}) \\ &\geq g^* \circ h^*(\vec{x}) \\ &= (h \circ g)^*(\vec{x}). \end{aligned}$$

Cette fois, on n'a pas eu besoin du fait que h^* est croissante. Enfin :

$$[h \circ f](\vec{x}, \vec{y}) = [f](\vec{x}, h^*(\vec{y})) + [h](f_*(\vec{x}), \vec{y}).$$

Comme $[f] > [g]$, par hypothèse, on a :

$$[f](\vec{x}, h^*(\vec{y})) > [g](\vec{x}, h^*(\vec{y})).$$

D'autre part, on a supposé que $f_* \geq g_*$, donc, du fait que $[h]$ est croissante, on a :

$$[h](f_*(\vec{x}), \vec{y}) \geq [h](g_*(\vec{x}), \vec{y}).$$

Il ne reste plus qu'à rappeler que $>$ est compatible avec $+$ sur M (et donc \geq l'est aussi), pour conclure que :

$$[h \circ f] > [h \circ g],$$

et donc que :

$$h \circ f > h \circ g.$$

Avec les mêmes f et g et si $h : p \longrightarrow m$, on montre de façon similaire que :

$$f \circ h > g \circ h,$$

mais en utilisant cette fois que h^* et $[h]$ sont croissantes. On a donc : $>$ est un idéal de $\mathcal{O}(X, Y, M)$.

Supposons à présent que $>$ termine sur M et montrons que $>$ termine sur $\mathcal{O}(X, Y, M)$, ce qui constitue la dernière condition à vérifier pour prouver que $>$ est un ordre de réduction. Supposons qu'il existe une suite strictement décroissante $(f_n)_{n \in \mathbb{N}}$ de flèches $m \longrightarrow n$ de $\mathcal{O}(X, Y, M)$. Alors, en particulier, $([f_n])_{n \in \mathbb{N}}$ est une suite strictement décroissante d'applications de $X^m \times Y^n$ dans M . Si l'on choisit un élément \vec{x} dans $X^m \times Y^n$, on obtient une suite strictement décroissante $([f_n](\vec{x}))_{n \in \mathbb{N}}$ d'éléments de M : cette situation est exclue par l'hypothèse de terminaison de $>$ sur M . Donc $>$ termine sur $\mathcal{O}(X, Y, M)$. \diamond

3.7.6 Le résultat

On peut alors formuler le résultat donnant la technique d'interprétation annoncée :

Théorème 3.17. *Une présentation d'opérade (Σ, R) termine s'il existe deux ensembles X et Y , munis d'ordres qui terminent, un monoïde commutatif M , muni d'un ordre de réduction, ainsi qu'un morphisme d'opérades $F : \mathcal{L}\Sigma \longrightarrow \mathcal{O}(X, Y, M)$ tels que, pour toute règle α de R , on ait $F(s(\alpha)) > F(t(\alpha))$.*

Démonstration. Puisque $>$ termine sur $\mathcal{O}(X, Y, M)$ et d'après le théorème 1.3, il suffit de montrer que F induit un morphisme d'ARS de $(\text{Fl } \mathcal{L}\Sigma, \text{Fl}(R))$ vers $(\text{Fl } \mathcal{O}(X, Y, M), \text{Fl } >)$, c'est-à-dire que $F(f) > F(g)$ dès que $f \rightarrow_R g$.

Supposons donc que f et g sont deux flèches parallèles de $\mathcal{L}\Sigma$ telles que $f \rightarrow_R g$. Par définition de (R) , il existe donc une règle α de R ainsi qu'un contexte C de $\mathcal{L}\Sigma$ tels que :

$$f = C[s(\alpha)] \quad \text{et} \quad g = C[t(\alpha)].$$

De plus, comme C est un contexte de $\mathcal{L}\Sigma$, il existe deux flèches h et k de $\mathcal{L}\Sigma$ ainsi que deux entiers i et j tels que :

$$C = k \circ (i \otimes \square \otimes j) \circ h.$$

D'où :

$$F(f) = F(k) \circ (i \otimes F(s(\alpha)) \otimes j) \circ F(h)$$

puisque F est un morphisme d'opérades. Or, par hypothèse, $F(s(\alpha)) > F(t(\alpha))$ et $>$ est compatible avec les produits et compositions sur $\mathcal{O}(X, Y, M)$, ce qui donne :

$$\begin{aligned} F(f) &> F(k) \circ (i \otimes F(t(\alpha)) \otimes j) \circ F(h) \\ &= F(g). \end{aligned}$$

◇

Voyons comment utiliser ce résultat. Le fait que F soit un morphisme d'opérades, conjugué à la liberté de $\mathcal{L}\Sigma$, impose que F est entièrement déterminé par ses valeurs sur les flèches de Σ . Ainsi, pour appliquer le résultat, il suffit de fixer X , Y et M et d'associer, à chaque générateur φ de Σ , trois applications *croissantes* φ_* , φ^* et $[\varphi]$ de telle sorte que, pour toute règle α de R , on ait $F(s(\alpha)) > F(t(\alpha))$, c'est-à-dire que $s(\alpha)_* \geq t(\alpha)_*$, $s(\alpha)^* \geq t(\alpha)^*$ et $[s(\alpha)] > [t(\alpha)]$.

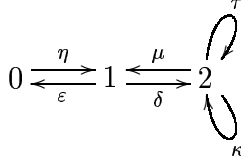
Le paragraphe suivant donne un exemple d'utilisation.

3.7.7 Un premier exemple : la présentation $L(\mathbb{Z}_2)$

Nous allons utiliser la technique décrite précédemment pour démontrer la terminaison de la présentation d'opérades $L(\mathbb{Z}_2)$, donnée par Yves Lafont dans [Laf03]. L'opérade ainsi présentée est celle des $\mathbb{Z}/2\mathbb{Z}$ -espaces vectoriels, c'est-à-dire que ses algèbres dans la catégorie des ensembles sont exactement les $\mathbb{Z}/2\mathbb{Z}$ -espaces vectoriels, ou encore les groupes qui sont isomorphes à des sommes de copies de $\mathbb{Z}/2\mathbb{Z}$, ou encore les groupes dans lesquels tout élément est son propre inverse.

Comme nous le verrons plus loin, la terminaison de $L(\mathbb{Z}_2)$, qui n'était que conjecturée jusqu'alors, en fait le premier exemple de présentation convergente d'opérades pour laquelle il n'existe pas de système de réécriture de termes convergent équivalent.

Avant tout, rappelons la présentation $L(\mathbb{Z}_2)$. Sa signature Σ est constituée de 6 générateurs :



On trouvera des représentations graphiques pour ces six flèches dans la figure 3.4. Donnons, pour l'intuition, ce que représentent ces générateurs : le but est que l'opérade $\mathcal{L}\Sigma/R$ admette, pour algèbres dans la catégorie des ensembles, les $\mathbb{Z}/2\mathbb{Z}$ -espaces vectoriels. Ces objets possèdent les opérations suivantes :

- une addition $\mu(x, y) = x + y$ qui admet un élément neutre η ;
- une duplication $\delta(x) = (x, x)$ admettant une coïunité $\varepsilon(x) = *$ (effaceur), hérités de la structure cartésienne de \mathbb{E}_{NS} ;
- une permutation $\tau(x, y) = (y, x)$, elle aussi héritée de la structure cartésienne de \mathbb{E}_{NS} .

À ces cinq opérations, on en ajoute une sixième, notée κ et correspondant à $\kappa(x, y) = (x + y, x)$. Elle n'est présente qu'à des fins de convergence de la présentation ; elle est, en effet, superflue, car, si x et y sont des éléments d'un $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel :

$$\kappa(x, y) = (\mu \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1)(x, y).$$

Ces opérations vérifient un certain nombre de relations, données ci-après. Nous y trouvons, par exemple, l'associativité et la commutativité de μ , mais aussi le fait que, dans un $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel, chaque élément est son propre inverse, c'est-à-dire que $x + x = 0$, ou encore que $\mu \circ \delta = \eta \circ \varepsilon$. Citons encore, pour finir, la relation donnant la décomposition de κ en fonction de μ , τ et δ . On définit donc l'ensemble R des 67 règles de $L(\mathbb{Z}_2)$, que nous donnons seulement de manière graphique dans la figure 3.5, issue de [Laf03].

Une remarque sur les règles : chaque règle n possède une symétrique haut-bas n^o , obtenue en renversant les diagrammes, avec, éventuellement, $n = n^o$.

On va utiliser la technique d'interprétation que nous avons construite en 3.7 pour démontrer le résultat suivant :

Théorème 3.18. *La présentation $L(\mathbb{Z}_2) = (\Sigma, R)$ termine.*

Démonstration. Nous allons utiliser la technique décrite avec $X = Y = \mathbb{N}^*$, l'ensemble des entiers naturels non nuls, muni de son ordre usuel, et $M = [\mathbb{N}^*]$, le monoïde commutatif libre engendré par \mathbb{N}^* : cette structure sera examinée au chapitre 4 mais, pour l'instant,

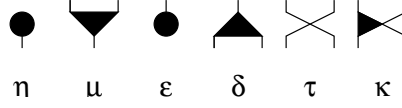


FIG. 3.4 – Les 6 générateurs de la présentation $L(\mathbb{Z}_2)$.

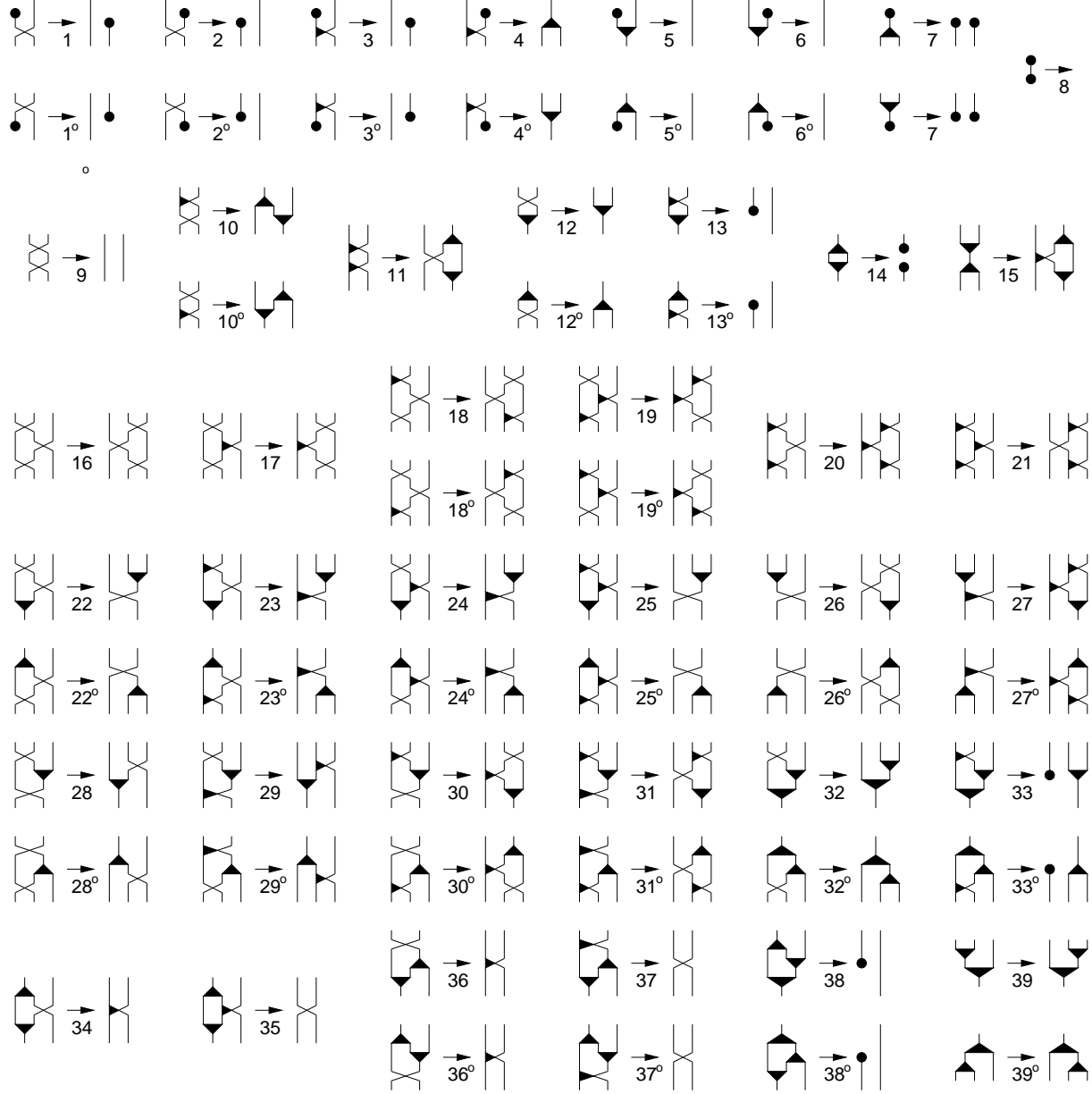


FIG. 3.5 – Les 67 relations de la présentation $L(\mathbb{Z}_2)$.

nous n'avons pas besoin de détails formels ; disons, pour l'instant, que les éléments de $[\mathbb{N}^*]$ sont des sommes finies de la forme :

$$\sum_{i=0}^p k_i \cdot \underline{n_i},$$

où les k_i et les n_i sont des entiers naturels non nuls. On note \underline{n} l'entier n vu comme un générateur de $[\mathbb{N}^*]$ et 0 la somme vide. L'addition est définie en ajoutant les coefficients ; par exemple :

$$(\underline{2} + 2.\underline{5}) + (3.\underline{2} + \underline{3}) = 4.\underline{2} + \underline{3} + 2.\underline{5}.$$

On munit $[\mathbb{N}^*]$ du *multiordre* engendré par $>$ sur \mathbb{N}^* : nous étudierons plus en détail cette construction au chapitre 4 et rappellerons en 4.5 que c'est un ordre de réduction sur $[\mathbb{N}^*]$, car $>$ termine sur \mathbb{N}^* . Disons, pour le moment, qu'il vérifie $a > b$ si l'on est dans un des trois cas suivants :

- $a \neq 0$ et $b = 0$;
- $a = \underline{n}$ et $b = k_1.\underline{n_1} + \dots + k_p.\underline{n_p}$, avec $n > n_i$ pour tout $i \in \{1 \dots p\}$;
- $a = a' + c$ et $b = b' + c$ avec $a' > b'$.

Par exemple, $147.\underline{1} < \underline{2} < 2.\underline{2}$.

Pour simplifier, notons $\mathcal{O}(\mathbb{N}) = \mathcal{O}(\mathbb{N}^*, \mathbb{N}^*, [\mathbb{N}^*])$. Nous allons construire un morphisme d'opérades $F : \mathcal{L}\Sigma \longrightarrow \mathcal{O}(\mathbb{N})$, en commençant par donner ses valeurs sur les flèches de Σ :

- $\mu_*(i, j) = \delta^*(i, j) = i + j$, $\mu^*(i) = \delta_*(i) = (i, i)$ et $[\mu](i, j, k) = [\delta](k, i, j) = \underline{i} + \underline{k}$;
- $\eta_*(*) = \varepsilon^*(*) = 1$, $\eta^*(i) = \varepsilon_*(i) = *$ et $[\eta](i) = [\varepsilon](i) = \underline{i}$;
- $\tau_*(i, j) = \tau^*(i, j) = \kappa_*(i, j) = \kappa^*(i, j) = (i + j, i)$ et $[\tau](i, j, k, l) = [\kappa](i, j, k, l) = \underline{i} + \underline{k}$.

La première constatation est que ces valeurs sont symétriques haut-bas, tout comme les règles, de telle sorte que, si α est une règle de R et α^o sa règle symétrique, on ait $F(s(\alpha)) > F(t(\alpha))$ si et seulement si $F(s(\alpha^o)) > F(t(\alpha^o))$. Ainsi, il ne reste plus que 39 vérifications à effectuer.

Mais on peut aller plus loin : en effet, on a envoyé τ et κ sur la même flèche de $\mathcal{O}(\mathbb{N}^*)$; ainsi, de nombreuses règles se retrouvent identifiées *via* F : les règles 1 et 3 ; 16 à 21 ; 22 à 25 ; 26 et 27 ; 28 et 29 ; 30 et 31 ; 34 et 35 ; 36 et 37. Ainsi, il ne reste que 25 vérifications, au lieu des 67 de départ.

La première chose à vérifier est que les applications φ_* , φ^* et $[\varphi]$ prennent bien leurs valeurs dans les bons ensembles et sont croissantes : ce dernier point est dû au fait qu'il s'agit d'applications polynômiales à coefficients entiers positifs. On peut donc les étendre

en un morphisme d'opérades $F : \mathcal{L}\Sigma \longrightarrow \mathcal{O}(\mathbb{N})$. Puis, pour chacune des règles α restantes, on doit vérifier que $s(\alpha)_* \geq t(\alpha)_*$, $s(\alpha)^* \geq t(\alpha)^*$ et $[s(\alpha)] > [t(\alpha)]$. Notons que si $\alpha^o = \alpha$, on a $s(\alpha)^* \geq t(\alpha)^*$ si et seulement si $s(\alpha)_* \geq t(\alpha)_*$, ce qui simplifie encore les calculs pour les règles 8, 9, 11, 14, 15, 16 et 34.

$$1. \begin{cases} (\tau \circ (\varepsilon \otimes 1))_*(i) = (i+1, 1) > (i, 1) = (1 \otimes \varepsilon)_*(i) \\ (\tau \circ (\varepsilon \otimes 1))^*(i, j) = i = (1 \otimes \varepsilon)^*(i, j) \\ [\tau \circ (\varepsilon \otimes 1)](i, j, k) = \underline{j+k} + \underline{j} + \underline{1} \\ [1 \otimes \varepsilon](i, j, k) = \underline{k}. \end{cases}$$

Comme $j \geq 1$, $j+k > k$ et donc $\underline{j+k} > \underline{k}$; de plus, $\underline{j} + \underline{1} > 0$, ce qui permet de conclure.

$$2. \begin{cases} (\tau \circ (1 \otimes \eta))_*(i) = (i+1, i) > (1, i) = (\eta \otimes 1)_*(i) \\ (\tau \circ (1 \otimes \eta))^*(i, j) = i+j > j = (\eta \otimes 1)^*(i, j) \\ [\tau \circ (1 \otimes \eta)](i, j, k) = \underline{i} + 2.\underline{j} \\ [\eta \otimes 1](i, j, k) = \underline{j}. \end{cases}$$

$$4. \begin{cases} (\kappa \circ (1 \otimes \eta))_*(i) = (i+1, i) > (i, i) = \delta_*(i) \\ (\kappa \circ (1 \otimes \eta))^*(i, j) = i+j = \delta^*(i, j) \\ [\kappa \circ (1 \otimes \eta)](i, j, k) = \underline{i} + 2.\underline{j} \\ [\eta \otimes 1](i, j, k) = \underline{i} + \underline{j}. \end{cases}$$

$$5. \begin{cases} (\mu \circ (\eta \otimes 1))_*(i) = i+1 > i = 1_*(i) \\ (\mu \circ (\eta \otimes 1))^*(i) = i = 1^*(i) \\ [\mu \circ (\eta \otimes 1)](i, j) = 2.\underline{j} + \underline{1} > 0 = [1](i, j). \end{cases}$$

$$6. \begin{cases} (\mu \circ (1 \otimes \eta))_*(i) = i+1 > i = 1_*(i) \\ (\mu \circ (1 \otimes \eta))^*(i) = i = 1^*(i) \\ [\mu \circ (1 \otimes \eta)](i, j) = \underline{i} + 2.\underline{j} > 0 = [1](i, j). \end{cases}$$

$$7. \begin{cases} (\delta \circ \eta)_*(*) = (1, 1) = (\eta \otimes \eta)_*(*) \\ (\delta \circ \eta)^*(i, j) = * = (\eta \otimes \eta)^*(i, j) \\ [\delta \circ \eta](i, j) = \underline{i+j} + \underline{i} + \underline{1} \\ [\eta \otimes \eta](i, j) = \underline{i} + \underline{j}. \end{cases}$$

$$8. \begin{cases} (\varepsilon \circ \eta)_*(*) = * = 0_*(*) \\ [\varepsilon \circ \eta](*) = 2.\underline{1} > 0 = [0](*) \end{cases}$$

$$9. \begin{cases} (\tau \circ \tau)_*(i, j) = (2i + j, i + j) > (i, j) = 2_*(i, j) \\ [\tau \circ \tau](i, j, k, l) = \underline{i + j} + \underline{i} + \underline{k + l} + \underline{k} > 0 = [2](i, j, k, l) \end{cases}$$

$$10. \begin{cases} (\tau \circ \kappa)_*(i, j) = (2i + j, i + j) > (i, i + j) = ((1 \otimes \mu) \circ (\delta \otimes 1))_*(i, j) \\ (\tau \circ \kappa)^*(i, j) = (2i + j, i + j) > (i + j, i) = ((1 \otimes \mu) \circ (\delta \otimes 1))^*(i, j) \\ [\tau \circ \kappa](i, j, k, l) = \underline{i + j} + \underline{i} + \underline{k + l} + \underline{k} \\ [(1 \otimes \mu) \circ (\delta \otimes 1)](i, j, k, l) = 2.\underline{i} + \underline{k} + \underline{l} \end{cases}$$

$$11. \begin{cases} (\kappa \circ \kappa)_*(i, j) = (2i + j, i + j) > (i + j, i + j) = ((1 \otimes \mu) \circ (\tau \otimes 1) \circ (1 \otimes \delta))_*(i, j) \\ [\kappa \circ \kappa](i, j, k, l) = \underline{i + j} + \underline{i} + \underline{k + l} + \underline{k} \\ [(1 \otimes \mu) \circ (\tau \otimes 1) \circ (1 \otimes \delta)](i, j, k, l) = 2.\underline{i} + \underline{j} + 2.\underline{k} + \underline{l} \end{cases}$$

On utilise ici, pour conclure, le fait que $\underline{i + j} > \underline{i} + \underline{j}$, pour tous i et j non nuls.

$$12. \begin{cases} (\mu \circ \tau)_*(i, j) = 2i + j > i + j = \mu_*(i, j) \\ (\mu \circ \tau)^*(i) = (2i, i) > (i, i) = \mu^*(i) \\ [\mu \circ \tau](i, j, k) = \underline{i + j} + \underline{i} + 2.\underline{k} \\ [\mu](i, j, k) = \underline{i} + \underline{k} \end{cases}$$

$$13. \begin{cases} (\mu \circ \kappa)_*(i, j) = 2i + j > j = (\varepsilon \otimes 1)_*(i, j) \\ (\mu \circ \kappa)^*(i) = (2i, i) > (1, i) = (\varepsilon \otimes 1)^*(i) \\ [\mu \circ \kappa](i, j, k) = \underline{i + j} + \underline{i} + 2.\underline{k} \\ [\varepsilon \otimes 1](i, j, k) = \underline{i} \end{cases}$$

$$14. \begin{cases} (\mu \circ \delta)_*(i) = 2i > 1 = (\eta \circ \varepsilon)_*(i) \\ [\mu \circ \delta](i, j) = 2.\underline{i} + 2.\underline{j} \\ [\eta \circ \varepsilon](i, j) = \underline{i} + \underline{j} \end{cases}$$

$$\begin{aligned}
 15. \quad & \begin{cases} (\delta \circ \mu)_*(i, j) = (i + j, i + j) = ((1 \otimes \mu) \circ (\kappa \otimes 1) \circ (1 \otimes \delta))_*(i, j) \\ [\delta \circ \mu](i, j, k, l) = \underline{i + j} + \underline{i} + \underline{k + l} + \underline{k} \\ [(1 \otimes \mu) \circ (\kappa \otimes 1) \circ (1 \otimes \delta)](i, j, k, l) = 2.\underline{i} + \underline{j} + 2.\underline{k} + \underline{l}. \end{cases} \\
 16. \quad & \begin{cases} ((\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1))_*(i, j, k) = (2i + j + k, i + j, i) \\ ((1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau))_*(i, j, k) = (i + j + k, i + j, i) \\ [(\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1)](i, j, k, l, m, n) = \underline{i + j} + 2.\underline{i} + \underline{l + m} + 2.\underline{l} \\ [(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau)](i, j, k, l, m, n) = 2.\underline{i} + \underline{j} + 2.\underline{l} + \underline{m}. \end{cases} \\
 22. \quad & \begin{cases} ((\mu \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1))_*(i, j, k) = (2i + j + k, i) \\ > (i + j + k, i) = (\tau \circ (1 \otimes \mu))_*(i, j, k) \\ ((\mu \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1))^*(i, j) = (2i + j, i, i) \\ > (i + j, i, i) = (\tau \circ (1 \otimes \mu))^*(i, j) \\ [(\mu \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1)](i, j, k, l, m) = \underline{i + j} + 2.\underline{i} + 3.\underline{l} \\ [\tau \circ (1 \otimes \mu)](i, j, k, l, m) = \underline{i} + \underline{j} + 2.\underline{l}. \end{cases} \\
 26. \quad & \begin{cases} (\tau \circ (\mu \otimes 1))_*(i, j, k) = (i + j + k, i + j) = ((1 \otimes \mu) \circ (\tau \otimes 1) \circ (1 \otimes \tau))_*(i, j, k) \\ (\tau \circ (\mu \otimes 1))^*(i, j) = (i + j, i + j, i) = ((1 \otimes \mu) \circ (\tau \otimes 1) \circ (1 \otimes \tau))^*(i, j) \\ [\tau \circ (\mu \otimes 1)](i, j, k, l, m) = \underline{i + j} + \underline{i} + \underline{l + m} + \underline{l} \\ [(1 \otimes \mu) \circ (\tau \otimes 1) \circ (1 \otimes \tau)](i, j, k, l, m) = 2.\underline{i} + \underline{j} + 2.\underline{l} + \underline{m}. \end{cases} \\
 28. \quad & \begin{cases} (\tau \circ (1 \otimes \mu) \circ (\tau \otimes 1))_*(i, j, k) = (2i + j + k, i + j) \\ > (i + j + k, j) = ((\mu \otimes 1) \circ (1 \otimes \tau))_*(i, j, k) \\ (\tau \circ (1 \otimes \mu) \circ (\tau \otimes 1))^*(i, j) = (2i + j, i + j, i) \\ > (i, i + j, i) = ((\mu \otimes 1) \circ (1 \otimes \tau))^*(i, j) \\ [\tau \circ (1 \otimes \mu) \circ (\tau \otimes 1)](i, j, k, l, m) = \underline{i + j} + 2.\underline{i} + \underline{l + m} + 2.\underline{l} \\ [(\mu \otimes 1) \circ (1 \otimes \tau)](i, j, k, l, m) = \underline{i} + \underline{j} + 2.\underline{l}. \end{cases} \\
 30. \quad & \begin{cases} (\tau \circ (1 \otimes \mu) \circ (\kappa \otimes 1))_*(i, j, k) = (2i + j + k, i + j) \\ > (i + j + k, i + j) = ((1 \otimes \mu) \circ (\kappa \otimes 1) \circ (1 \otimes \tau))_*(i, j, k) \\ (\tau \circ (1 \otimes \mu) \circ (\kappa \otimes 1))^*(i, j) = (2i + j, i + j, i) \\ > (i + j, i + j, i) = ((1 \otimes \mu) \circ (\kappa \otimes 1) \circ (1 \otimes \tau))^*(i, j) \\ [\tau \circ (1 \otimes \mu) \circ (\kappa \otimes 1)](i, j, k, l, m) = \underline{i + j} + 2.\underline{i} + \underline{l + m} + 2.\underline{l} \\ [(1 \otimes \mu) \circ (\kappa \otimes 1) \circ (1 \otimes \tau)](i, j, k, l, m) = 2.\underline{i} + \underline{j} + 2.\underline{l} + \underline{m} \end{cases}
 \end{aligned}$$

$$32. \begin{cases} (\mu \circ (1 \otimes \mu) \circ (\tau \otimes 1))_*(i, j, k) = 2i + j + k > i + j + k = (\mu \circ (1 \otimes \mu))_*(i, j, k) \\ (\mu \circ (1 \otimes \mu) \circ (\tau \otimes 1))^*(i) = (2i, i, i) > (i, i, i) = (\mu \circ (1 \otimes \mu))^*(i) \\ [\mu \circ (1 \otimes \mu) \circ (\tau \otimes 1)](i, j, k, l) = \underline{i+j} + 2.\underline{i} + 3.\underline{l} \\ [\mu \circ (1 \otimes \mu)](i, j, k, l) = \underline{i} + \underline{j} + 2.\underline{l}. \end{cases}$$

$$33. \begin{cases} (\mu \circ (1 \otimes \mu) \circ (\kappa \otimes 1))_*(i, j, k) = 2i + j + k > j + k = (\varepsilon \otimes \mu)_*(i, j, k) \\ (\mu \circ (1 \otimes \mu) \circ (\kappa \otimes 1))^*(i) = (2i, i, i) > (1, i, i) = (\varepsilon \otimes \mu)^*(i) \\ [\mu \circ (1 \otimes \mu) \circ (\kappa \otimes 1)](i, j, k, l) = \underline{i+j} + 2.\underline{i} + 3.\underline{l} \\ [\varepsilon \otimes \mu](i, j, k, l) = \underline{i} + \underline{j} + \underline{l}. \end{cases}$$

$$34. \begin{cases} ((\mu \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1))_*(i, j) = (2i + j, i) > (i + j, i) = \kappa_*(i, j) \\ [(\mu \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1)](i, j, k, l) = 3.\underline{i} + 3.\underline{k} \\ [\kappa](i, j, k, l) = \underline{i} + \underline{k}. \end{cases}$$

$$36. \begin{cases} ((\mu \otimes 1) \circ (1 \otimes \delta) \circ \tau)_*(i, j) = (2i + j, i) > (i + j, i) = \kappa_*(i, j) \\ ((\mu \otimes 1) \circ (1 \otimes \delta) \circ \tau)^*(i, j) = (2i + j, i) > (i + j, i) = \kappa^*(i, j) \\ [(\mu \otimes 1) \circ (1 \otimes \delta) \circ \tau](i, j, k, l) = \underline{i+j} + 2.\underline{i} + 3.\underline{k} \\ [\kappa](i, j, k, l) = \underline{i} + \underline{k}. \end{cases}$$

$$38. \begin{cases} (\mu \circ (1 \otimes \mu) \circ (\delta \otimes 1))_*(i, j) = 2i + j > j = (\varepsilon \otimes 1)_*(i, j) \\ (\mu \circ (1 \otimes \mu) \circ (\delta \otimes 1))^*(i) = (2i, i) > (1, i) = (\varepsilon \otimes 1)^*(i, j) \\ [\mu \circ (1 \otimes \mu) \circ (\delta \otimes 1)](i, j, k) = 3.\underline{i} + 3.\underline{k} \\ [\varepsilon \otimes 1](i, j, k) = \underline{i}. \end{cases}$$

$$39. \begin{cases} (\mu \circ (\mu \otimes 1))_*(i, j, k) = i + j + k = (\mu \circ (1 \otimes \mu))_*(i, j, k) \\ (\mu \circ (\mu \otimes 1))^*(i) = (i, i, i) = (\mu \circ (1 \otimes \mu))^*(i) \\ [\mu \circ (\mu \otimes 1)](i, j, k, l) = \underline{i+j} + \underline{i} + 2.\underline{l} \\ [\mu \circ (1 \otimes \mu)](i, j, k, l) = \underline{i} + \underline{j} + 2.\underline{l}. \end{cases}$$

D'où la terminaison de $L(\mathbb{Z}_2)$, en appliquant le théorème 3.17.

◇

3.8 Confluence locale d'une présentation d'opérade

Le but de ce paragraphe est de définir ce que sont les paires critiques d'une présentation d'opérade, de telle sorte que l'on obtienne un résultat nous assurant qu'une présentation d'opérade est confluente si et seulement si toutes ses paires critiques sont joignables. Puis, nous esquisserons une méthode pour les calculer explicitement.

3.8.1 Paires critiques d'une présentation d'opérade

Dans le cas des présentations de monoïdes, nous avons développé deux approches des paires critiques : l'une, directe, consiste à examiner toutes les formes possibles de branchements locaux ; l'autre, non constructive, caractérise les paires critiques selon des propriétés algébriques des branchements qui leur sont associés. Cependant, en raison de la structure algébrique plus complexe des opérades, l'approche directe est presque impossible.

On va donc privilégier la description alternative des paires critiques donnée dans le cas des mots. Soit (Σ, \mathcal{R}) une présentation. Afin d'alléger les notations, on pose $\mathbb{C} = \mathcal{L}\Sigma$.

On note \mathbb{C}^3 le \mathbb{C} -module dont les flèches sont les triplets de flèches parallèles de \mathbb{C} et muni des actions diagonales de \mathbb{C} . On note $\mathcal{B}(\Sigma, \mathcal{R})$ l'ensemble des branchements locaux de (Σ, \mathcal{R}) . Parmi ceux-ci et pour tout couple (α, β) de règles de \mathcal{R} , on note $\mathcal{B}(\Sigma, \alpha, \beta)$ l'ensemble des branchements locaux (f, g, h) pour lesquels il existe des contextes C et D vérifiant $(f, g) = C[\alpha]$ et $(f, h) = D[\beta]$. On a, comme dans le cas des présentations de monoïdes :

Lemme 3.19. *L'ensemble $\mathcal{B}(\Sigma, \mathcal{R})$ est un sous- \mathbb{C} -module de \mathbb{C}^3 . De même, pour chaque couple (α, β) de règles de \mathcal{R} , l'ensemble $\mathcal{B}(\Sigma, \alpha, \beta)$ est un sous- \mathbb{C} -module de \mathbb{C}^3 .*

On va alors prouver que chaque $\mathcal{B}(\Sigma, \alpha, \beta)$ possède une unique famille génératrice minimale, afin de définir les branchements minimaux de (Σ, \mathcal{R}) :

Proposition 3.20. *Soient $n \geq 1$ et A un sous- \mathbb{C} -module de \mathbb{C}^n . Alors A possède une unique famille génératrice minimale.*

Démonstration. La démonstration fonctionne exactement comme dans le cas des monoïdes. On définit une relation binaire \sqsupset sur A (ou plutôt $\text{Fl } A$) en posant $f \sqsupset g$ si l'on a $f = C[g]$ pour un certain contexte $C \neq \square$ sur \mathbb{C} . On montre alors que (A, \sqsupset) termine et tout découle de là.

La seule difficulté pour montrer la terminaison est de construire l'application $|\cdot| : A \longrightarrow \mathbb{N}$. Ici, on ne travaille pas sur des mots mais sur des flèches. Cependant, le fait que \mathbb{C} soit librement engendrée par Σ nous permet de construire une application

qui compte le nombre d'opérateurs de Σ dans une flèche de \mathbb{C} : c'est le pendant, pour les opérateurs, de l'application qui associe sa longueur à un élément d'un monoïde libre.

D'après la construction de \mathbb{C} , toute flèche f de \mathbb{C} s'écrit comme une composée $f_q \circ \dots \circ f_1$ avec chaque f_i qui est un produit $p_i \otimes \varphi_j \otimes q_i$ où φ_i est une flèche de Σ et p_i et q_i sont des entiers. On pose alors $|f| = q$.

Il faut cependant vérifier que c'est bien défini, c'est-à-dire que la valeur de $|f|$ ne dépend pas de la décomposition choisie, ou encore que $|\cdot|$ est compatible avec les relations utilisées pendant la construction de \mathbb{C} . Principalement, on doit vérifier que, pour tous $m, n, p, q \in \mathbb{N}$, $f \in \mathcal{L}\Sigma(m, n)$ et $g \in \mathcal{L}\Sigma(p, q)$:

$$|(n \otimes g) \circ (f \otimes p)| = |(f \otimes q) \circ (m \otimes g)|.$$

On note que les flèches de Σ qui interviennent de part et d'autre de l'égalité sont les mêmes : c'est juste leur place qui change éventuellement. En particulier, le nombre de ces flèches est constant. Donc $|\cdot|$ est bien définie. \diamond

Définition. Pour α et β deux règles fixées, on appelle *branchement minimal* de (Σ, \mathcal{R}) engendré par (α, β) tout élément de la famille génératrice minimale de $\mathcal{B}(\Sigma, \alpha, \beta)$. On appelle *branchement minimal* de (Σ, \mathcal{R}) tout branchement local qui est engendré par un couple (α, β) de règles. \blacklozenge

Pour définir les branchements triviaux, il faut prendre en compte la structure additionnelle des opérateurs par rapport aux monoïdes. Ainsi, si α, β sont des flèches de l'idéal engendré par R , les triplets suivants sont des branchements :

$$\left\{ \begin{array}{l} (s(\alpha) \otimes s(\beta), t(\alpha) \otimes s(\beta), s(\alpha) \otimes t(\beta)) \\ (s(\alpha) \otimes s(\beta), s(\alpha) \otimes t(\beta), t(\alpha) \otimes s(\beta)) \end{array} \right\}$$

ainsi que, dans le cas où $s(\beta)$ est composable avec $s(\alpha)$:

$$\left\{ \begin{array}{l} (s(\alpha) \circ s(\beta), t(\alpha) \circ s(\beta), s(\alpha) \circ t(\beta)) \\ (s(\alpha) \circ s(\beta), s(\alpha) \circ t(\beta), t(\alpha) \circ s(\beta)) \end{array} \right\}$$

Comme les deux premières formes sont des cas particuliers des deux dernières (on le montre grâce aux relations d'échange), on appelle *branchement trivial* de (Σ, \mathcal{R}) tout branchement local de (Σ, \mathcal{R}) qui possède l'une des deux dernières formes décrites, pour un certain α et un certain β dans l'idéal de \mathbb{C} engendré par \mathcal{R} . Un branchement minimal non trivial de (Σ, \mathcal{R}) est appelé *branchement critique*. Enfin, on définit :

Définition. Soit (Σ, \mathcal{R}) une présentation. Une *paire critique* de (Σ, \mathcal{R}) est une donnée (f, C, α, D, β) où α et β sont deux règles de \mathcal{R} , f est une flèche de $\mathcal{L}\Sigma$ et C et D sont deux contextes, le tout vérifiant :

- Les deux notations $C[s(\alpha)]$ et $D[s(\beta)]$ ont un sens et sont toutes deux égales à f .
- Le triplet $(f, C[t(\alpha)], D[t(\beta)])$ est un branchement critique de (Σ, \mathcal{R}) .
- Si $\alpha = \beta$, alors $f \neq s(\alpha)$.

Le branchement local $(f, C[t(\alpha)], D[t(\beta)])$ est appelé *branchement associé* à la paire critique (f, C, α, D, β) . On dit qu'une paire critique est *confluente* si son branchement associé l'est. Une paire critique de la forme (f, C, α, D, β) est dite *engendrée* par le couple de règles (α, β) . L'ensemble des paires critiques de (Σ, \mathcal{R}) est noté $\text{cp}(\Sigma, \mathcal{R})$ ou simplement $\text{cp}(\mathcal{R})$. \blacklozenge

Remarque. Dans la définition, la troisième condition a pour but d'éliminer des paires critiques les éléments de la forme $(s(\alpha), \square, \alpha, \square, \alpha)$. En effet, le branchement associé à un tel élément est $(s(\alpha), t(\alpha), t(\alpha))$: il est donc toujours confluent.

On montre le résultat suivant :

Lemme 3.21 (des paires critiques). *Pour tout branchement local \mathbf{b} de (Σ, \mathcal{R}) , au moins l'une de ces deux assertions est vraie :*

- \mathbf{b} est confluent ;
- \mathbf{b} est de la forme $\mathbf{b} = C[\mathbf{g}]$ avec $C \in \mathcal{CC}$ et \mathbf{g} est le branchement associé à une paire critique de (Σ, \mathcal{R}) .

Démonstration. Soit \mathbf{b} un branchement local de (Σ, \mathcal{R}) . Alors, il existe un branchement minimal \mathbf{g} ainsi qu'un contexte C tels que $\mathbf{b} = C[\mathbf{g}]$. Si \mathbf{g} est trivial, alors \mathbf{g} est confluent et $\mathbf{b} = C[\mathbf{g}]$ aussi. Supposons que \mathbf{g} est un branchement critique. Comme \mathbf{g} est un branchement local, on a $\mathbf{g} = (f, g, h)$ avec $(f, g) = D[\alpha]$ et $(f, h) = E[\beta]$ pour certains $\alpha, \beta \in \mathcal{R}$ et $D, E \in \mathcal{CC}$. La donnée (f, D, α, E, β) vérifie donc $f = D[s(\alpha)] = E[s(\beta)]$ ainsi que $\mathbf{g} = (f, D[t(\alpha)], E[t(\beta)])$ est un branchement critique. C'est donc une paire critique et \mathbf{g} est le branchement qui lui est associé. \blacklozenge

On en déduit :

Théorème 3.22 (des paires critiques). *Une présentation est localement confluente si et seulement si toutes ses paires critiques sont confluentes.*

Démonstration. Soit (Σ, \mathcal{R}) une présentation. Supposons qu'elle est localement confluente. Alors, par définition, tous ses branchements locaux sont confluentes, y compris les branchements critiques ; donc toutes les paires critiques de (Σ, \mathcal{R}) sont confluentes. Réciproquement, supposons que toutes les paires critiques de (Σ, \mathcal{R}) sont confluentes et que \mathbf{b} est un branchement local quelconque : d'après le lemme des paires critiques, \mathbf{b} est confluent ou

il est de la forme $\mathfrak{b} = C[\mathfrak{g}]$ avec $C \in \mathcal{CC}$ et \mathfrak{g} le branchement associé à une paire critique p de (Σ, \mathcal{R}) . Or p est confluente donc, par définition, \mathfrak{g} est confluent et $C[\mathfrak{g}]$ aussi. Dans tous les cas, \mathfrak{b} est confluent et (Σ, \mathcal{R}) est localement confluente. \diamond

D'où, en appliquant le lemme de Newman :

Corollaire 3.23. *Un présentation est convergente si et seulement si elle termine et toutes ses paires critiques sont confluentes.*

3.8.2 Calcul des paires critiques

Nous venons de donner une définition des paires critiques adaptée à la démonstration du lemme et du théorème du même nom. Cependant, nous n'avons pas de caractérisation explicite de ces objets. Nous allons démontrer ici une définition alternative, plus syntaxique, des paires critiques, qui ouvrira une piste vers une méthode pour les calculer. Cependant, cette caractérisation n'est valable que pour certaines présentations, bien que la restriction ne concerne aucune de celles qui seront étudiées par la suite.

Théorème 3.24. *Soient (Σ, \mathcal{R}) une présentation d'opéade et α et β deux règles de \mathcal{R} vérifiant :*

Pour tous contextes C et D applicables à γ ($\gamma \in \{\alpha, \beta\}$), si $C[s(\gamma)] = D[s(\gamma)]$ et $C[t(\gamma)] = D[t(\gamma)]$, alors $C = D$.

Soient f une flèche de $\mathcal{L}\Sigma$ et C et D des contextes tels que $f = C[s(\alpha)] = D[s(\beta)]$. Alors (f, C, α, D, β) est une paire critique de (Σ, \mathcal{R}) si et seulement si les conditions suivantes sont remplies :

- *La flèche f est différente de $s(\alpha)$ dans le cas où $\alpha = \beta$.*
- *Il existe une flèche φ de Σ , ainsi que des contextes C_0 et D_0 vérifiant $C_0[\varphi] = s(\alpha)$ et $D_0[\varphi] = s(\beta)$.*
- *Le couple (C, D) vérifie $C \circ C_0 = D \circ D_0$ et il est minimal pour cette propriété, dans le sens suivant : pour tout couple de contextes (C', D') et tout contexte E vérifiant $C' \circ C_0 = D' \circ D_0$, $C = E \circ C'$ et $D = E \circ D'$, on a $E = \square$.*

Démonstration. Soit (f, C, α, D, β) une paire critique de (Σ, \mathcal{R}) . Comme le branchement $(f, C[t(\alpha)], D[t(\beta)])$ est non trivial, il existe une flèche φ de Σ ainsi que des contextes C_0 et D_0 tels que $C_0[\varphi] = s(\alpha)$ et $D_0[\varphi] = s(\beta)$: sinon, les flèches $s(\alpha)$ et $s(\beta)$ ne peuvent pas se chevaucher dans f . De plus, le φ isolé dans la factorisation $s(\alpha) = C_0[\varphi]$ et celui de $s(\beta) = D_0[\varphi]$ sont les mêmes dans f : ils apparaissent dans le même contexte, ce qui se traduit par $C \circ C_0 = D \circ D_0$.

Maintenant, supposons que C' , D' et E sont trois contextes tels que : $C' \circ C_0 = D' \circ D_0$, $C = E \circ C'$ et $D = E \circ D'$. Alors, le triplet $(f', C'[t(\alpha)], D'[t(\beta)])$ est un branchement local de (Σ, \mathcal{R}) , en posant $f' = C'[s(\alpha)] = D'[s(\beta)]$. De plus, ce branchement vérifie :

$$(f, C[t(\alpha)], D[t(\beta)]) = E[(f', C'[t(\alpha)], D'[t(\beta)])].$$

Or le branchement $(f, C[t(\alpha)], D[t(\beta)])$ a été supposé minimal, donc $E = \square$.

Réciproquement, supposons que l'on a une donnée (f, C, α, D, β) vérifiant les propriétés du théorème 3.24. Le triplet $(f, C[t(\alpha)], D[t(\beta)])$ est un branchement local, puisque $f = C[s(\alpha)] = D[s(\beta)]$, par hypothèse. D'après la condition $C_0[\varphi] = s(\alpha)$ et $D_0[\varphi] = s(\beta)$, pour φ une flèche de Σ , on sait que ce branchement local est non trivial : les sources des deux règles α et β se chevauchent bien dans f .

Enfin, montrons que $(f, C[t(\alpha)], D[t(\beta)])$ est un branchement minimal de (α, β) . À cette fin, supposons qu'il existe un branchement local (f', g', h') de (Σ, \mathcal{R}) ainsi qu'un contexte E tels que :

$$\begin{cases} (f, C[t(\alpha)], D[t(\alpha)]) = E[(f', g', h')] \\ (f', g') = C'[\alpha] \\ (f', h') = D'[\beta]. \end{cases}$$

On en déduit que :

$$\begin{cases} E \circ C'[s(\alpha)] = C[s(\alpha)] \\ E \circ C'[t(\alpha)] = C[t(\alpha)] \\ E \circ D'[s(\beta)] = D[s(\beta)] \\ E \circ D'[t(\beta)] = D[t(\beta)]. \end{cases}$$

Par hypothèse sur les règles α et β , on obtient $E \circ C' = C$ et $E \circ D' = D$. D'autre part, par liberté de $\mathcal{L}\Sigma$, la flèche f' contient le même chevauchement de $s(\alpha)$ et $s(\beta)$ en φ : les contextes C' et D' vérifient l'égalité $C' \circ C_0 = D' \circ D_0$. Par hypothèse de minimalité du couple (C, D) , on a $E = \square$. Donc $(f, C[t(\alpha)], D[t(\beta)])$ est un branchement minimal associé à (α, β) .

◇

Ce critère, plus syntaxique que la définition d'origine, donne une première méthode de calcul de paires critiques. Soit (Σ, \mathcal{R}) une présentation d'opérade vérifiant : pour toute règle α de \mathcal{R} et tous contextes C et D applicables à α , si on a, à la fois, $C[s(\alpha)] = D[s(\alpha)]$ et $C[t(\alpha)] = D[t(\alpha)]$, alors $C = D$.

On fixe deux règles α et β dans \mathcal{R} et on procède comme suit :

1. On détermine tous les triplets (φ, C_0, D_0) composés d'une flèche φ de Σ et de deux contextes C et D , tels que $C_0[\varphi] = s(\alpha)$ et $D_0[\varphi] = s(\beta)$; on exclut, dans le cas où l'on a $\alpha = \beta$, les triplets (φ, C_0, C_0) .
2. Pour chaque triplet (φ, C_0, D_0) ainsi obtenu, on résout l'équation $C \circ C_0 = D \circ D_0$ d'indéterminées C et D .
3. Parmi les solutions de chacune de ces équations, on élimine tous les couples (C, D) pour lesquels il existe une autre solution (C', D') de la même équation, ainsi qu'un contexte E avec $C = E \circ C'$ et $D = E \circ D'$.

Alors, d'après le théorème 3.24, pour chaque triplet (φ, C_0, D_0) et chaque couple solution (C, D) ainsi obtenus, on a une paire critique (f, C, α, D, β) , où f est la flèche $C[s(\alpha)] = D[s(\beta)]$. De plus, on obtient toutes les paires critiques de (Σ, \mathcal{R}) en effectuant ces opérations sur chaque couple (α, β) de règles.

Cette méthode n'est pas encore implantable en l'état, notamment en raison de la seconde opération concernant la résolution d'équations du type $C \circ C_0 = D \circ D_0$: l'automatisation de ces calculs fait partie des prochains travaux envisagés.

Malgré cela, nous illustrerons son fonctionnement au chapitre 5, lors du calcul des paires critiques de la présentation de l'opérade dite des ensembles finis. En effet, les présentations étudiées dans ce document sont simples : les sources de leurs règles contiennent toutes deux ou trois générateurs. Ainsi, les contextes C_0 et D_0 sont, quant à eux, formés de un ou deux générateurs. Nous verrons que la recherche de solutions minimales pour l'équation $C \circ C_0 = D \circ D_0$ est, dans ce cas, suffisamment simple pour être effectuée à la main.

3.9 Structures de données pour les opérades libres

Ce paragraphe a pour but de présenter des pistes pour combler le fossé existant entre la théorie des opérades et l'implantation de calculs. Si ce qui est décrit ici n'est encore qu'à l'état embryonnaire, il faudra absolument développer, dans un travail ultérieur, des moyens pour calculer effectivement sur les flèches d'une opérade libre.

Deux points sur lesquels il serait souhaitable d'automatiser les calculs sont les suivants : la vérification de la terminaison en utilisant la technique développée en 3.7 et le calcul des paires critiques d'une présentation d'opérade finie, par exemple à l'aide de la méthode de 3.8.2.

La première étape dans ce programme est d'exhiber une structure de donnée dans laquelle on puisse coder les flèches d'une opérade libre. Si l'on a différentes possibilités, on choisira le codage simplifiant le plus les calculs à effectuer. Nous proposons ici deux idées de structures de données : la première est directement issue de la structure algébrique ; la seconde, plus graphique, s'en éloigne mais est certainement plus prometteuse.

3.9.1 Première structure

On utilise ici la structure algébrique d'une opérade libre. Soit Σ une signature ; on va définir un ensemble $L\Sigma$ de termes représentant des flèches formelles. Avant cela, définissons : les *types* sont les $m \longrightarrow n$ pour tout couple (m, n) d'entiers. Puis, l'ensemble $L\Sigma$ des termes est défini de manière inductive par :

- Pour tout entier n , $L\Sigma$ contient un terme n de type $n \longrightarrow n$.
- Si φ est un élément de $\Sigma(m, n)$, alors φ est un terme de type $m \longrightarrow n$.
- Si $f : m \longrightarrow n$ et $g : p \longrightarrow q$ sont deux termes, alors $f \otimes g$ est un terme de type $m + p \longrightarrow p + q$.
- Si $f : m \longrightarrow n$ et $g : n \longrightarrow p$ sont deux termes, alors $g \circ f$ est un terme de type $m \longrightarrow p$.

On définit ensuite une relation \equiv sur $L\Sigma$, toujours de manière inductive :

- Pour tout terme f :

$$f \otimes 0 \equiv 0 \otimes f \equiv f.$$

- Pour tout terme $f : m \longrightarrow n$:

$$n \circ f \equiv f \circ m \equiv f.$$

- Pour tous termes f, g et h :

$$(f \otimes g) \otimes h \equiv f \otimes (g \otimes h).$$

- Pour tous termes $f : m \longrightarrow n, g : n \longrightarrow p$ et $h : p \longrightarrow q$:

$$(h \circ g) \circ f \equiv h \circ (g \circ f).$$

Enfin, on étend \equiv par compatibilité avec la structure :

- Si f, g et h sont des termes tels que $f \equiv g$:

$$f \otimes h \equiv g \otimes h \quad \text{et} \quad h \otimes f \equiv h \otimes g.$$

- Si $f, g : m \longrightarrow n$ et $h : n \longrightarrow p$ sont des termes tels que $f \equiv g$:

$$h \circ f \equiv h \circ g.$$

- Si $f, g : n \longrightarrow p$ et $h : m \longrightarrow n$ sont des termes tels que $f \equiv g$:

$$f \circ h \equiv g \circ h.$$

Remarque. Les termes de type $m \longrightarrow n$ de $L\Sigma$ sont exactement les *graphes décorés* par les éléments de Σ . Sans entrer dans les détails, un *graphe planaire descendant* est un graphe topologique (orienté) G dans le plan \mathbb{R}^2 tel que chacune de ses arêtes est donnée par un chemin $a(t) = (x(t), y(t))$, où $x, y : [0, 1] \longrightarrow \mathbb{R}$ sont des applications continues et y est strictement décroissante, et tel que deux arêtes ne peuvent se couper qu'en un sommet. Pour un tel graphe, chaque sommet possède des *entrées* et des *sorties*, respectivement représentées par les arêtes entrantes et sortantes. Alors, un *graphe décoré* par les éléments de Σ est un graphe planaire descendant muni d'une application associant, à chacun de ses sommets ayant m entrées et n sorties, une flèche $\varphi \in \Sigma(m, n)$. On définit sur ces graphes une relation dite d'*isotopie* consistant à identifier deux graphes qui ne diffèrent que par des déformations continues, sans croisement ni coupure dans les arêtes : cette relation d'isotopie correspond à la relation \equiv définie ci-dessus.

Par construction de $L\Sigma$ et de \equiv , on a :

Proposition 3.25. *Si f et g sont deux termes tels que $f \equiv g$ alors f et g ont même type. De plus, l'ensemble des classes d'équivalence de termes de $L\Sigma$ modulo la relation \equiv est solution du problème d'opérade libre engendrée par Σ .*

Ainsi, on a un langage dans lequel s'expriment les flèches de $\mathcal{L}\Sigma$: chaque flèche de $\mathcal{L}\Sigma$ correspond à une classe d'équivalence de $L\Sigma / \equiv$. Le principal inconvénient de cette représentation est qu'elle impose de calculer *modulo* \equiv , tout comme la réécriture de termes avec un opérateur binaire associatif et commutatif impose de calculer *modulo* les relations dites (AC) d'associativité et de commutativité.

Il est envisageable que, pour certaines présentations (Σ, R) , on puisse catégorifier \equiv pour l'intégrer à R sans changer les propriétés de cette dernière : ainsi, on obtiendrait un calcul avec *isotopies explicites* pour (Σ, R) . Cependant, cette technique risque de ne fonctionner que dans des cas très particuliers.

3.9.2 Deuxième structure

On considère toujours une signature Σ . En s'inspirant de la représentation des flèches de $\mathcal{L}\Sigma$ comme classes d'équivalence de graphes décorés, on peut envisager un autre codage,

moins algébrique mais certainement plus utile. Cependant, il n'est adapté qu'au cas où Σ ne contient aucune flèche $0 \longrightarrow 0$: cela ne fonctionnera donc pas avec les présentations de monoïdes commutatifs (voir le chapitre 4) mais, dans tous les autres cas étudiés ici, on évite ce problème.

On suppose donc que $\Sigma(0, 0)$ est vide. Ainsi, la seule flèche $0 \longrightarrow 0$ de $\mathcal{L}\Sigma(0, 0)$ est 0. Le codage proposé consiste à voir chaque flèche de $\mathcal{L}\Sigma$ comme un tableau indiquant comment les générateurs intervenant dans son écriture sont reliés.

Représentation des diagrammes

Soit $f : m \longrightarrow n$ une flèche de $\mathcal{L}\Sigma$. On associe à f un entier $\#f$ qui est le nombre de générateurs de Σ utilisés pour écrire f : ce nombre est constant, quelle que soit l'écriture choisie, et généralise la longueur des mots. Par construction de $\mathcal{L}\Sigma$, on sait qu'il existe des flèches $f_1, \dots, f_{\#f}$ de Σ ainsi que des entiers $i_1, \dots, i_{\#f}$ et $j_1, \dots, j_{\#f}$ tels que :

$$f = (i_{\#f} \otimes f_{\#f} \otimes j_{\#f}) \circ \dots \circ (i_1 \otimes f_1 \otimes j_1).$$

Ces flèches et entiers ne sont pas uniques, mais définis *modulo* la relation d'échange :

$$(t(g) \otimes h) \circ (g \otimes s(h)) = (g \otimes t(h)) \circ (s(g) \otimes h).$$

On suppose que l'on a effectué un choix parmi toutes les écritures possibles de f . On considère alors un ensemble $X(f)$ dont les éléments sont notés $x_1, \dots, x_{\#f}$ ainsi qu'une application $l_f : X \longrightarrow \text{Fl}\Sigma$ telle que $l_f(x_i) = f_i$, pour tout $i \in [\#f]$. Pour simplifier les notations, on pose $s(x_i) = s(l_f(x_i))$ et $t(x_i) = t(l_f(x_i))$. On a ainsi associé à la flèche f l'ensemble des sommets du diagramme de Penrose qui la représente, ainsi que la décoration de chacun d'entre eux - cette donnée est unique à une permutation des indices des sommets près.

Maintenant, décrivons les arêtes du diagramme. On construit deux ensembles $S(f)$ et $T(f)$, qui contiennent respectivement toutes les entrées et sorties des sommets du diagramme, y compris les sommets libres que sont les entrées et sorties de f , que l'on note respectivement s_1, \dots, s_m et t_1, \dots, t_n . On pose :

$$\begin{cases} S_0(f) = \{(x_i, j) : i \in [\#f], j \in [s(x_i)]\} \\ S(f) = S_0(f) \cup \{t_1, \dots, t_n\}. \end{cases}$$

Et :

$$\begin{cases} T_0(f) = \{(x_i, j) : i \in [\#f], (j - s(x_i)) \in [t(x_i)]\} \\ T(f) = T_0(f) \cup \{s_1, \dots, s_m\}. \end{cases}$$

Notons que les ensembles $S(f)$ et $T(f)$ contiennent nécessairement le même nombre d'éléments :

$$\frac{1}{2} \cdot (m + n + \sum_{i=1}^{\sharp f} (s(x_i) + t(x_i))).$$

La donnée qui manque encore pour décrire les arêtes du diagramme est une correspondance bijective R_f entre $S(f)$ et $T(f)$, telle que :

- Si $(x_i, j) \in T(f)$ et $(x_{i'}, j') \in S(f)$, alors $(x_i, j) R_f (x_{i'}, j')$ si et seulement s'il existe une arête allant de la $(j - s(x_i))^e$ sortie du sommet x_i vers la $(j')^e$ entrée du sommet $x_{i'}$.
- Si $(x_i, j) \in T(f)$ et $k \in [n]$, alors $(x_i, j) R_f t_k$ si et seulement si la j^e sortie du sommet x_i est aussi la k^e sortie de la flèche f .
- Si $k \in [m]$ et $(x_i, j) \in S(f)$, alors $s_k R_f (x_i, j)$ si et seulement si la j^e entrée du sommet x_i est aussi la k^e entrée de la flèche f .
- Si $k \in [m]$ et $l \in [n]$, alors $s_k R_f t_l$ si et seulement si la k^e entrée de f est directement connectée à sa l^e sortie, c'est-à-dire si $f = g \otimes 1 \otimes h$, avec $g : k - 1 \longrightarrow l - 1$ et $h : m - k \longrightarrow n - l$.

On associe donc, à chaque flèche $f : m \longrightarrow n$, une donnée $(X(f), l_f, S(f), T(f), R_f)$, qui est unique aux permutations d'indices des sommets près. Donnons un exemple :

Exemple. On suppose que Σ est composée de deux flèches $\mu : 2 \longrightarrow 1$ et $\eta : 0 \longrightarrow 1$. On considère la flèche $f : 2 \longrightarrow 1$ suivante :

$$f = \mu \circ (1 \otimes \mu) \circ (1 \otimes \eta \otimes 1).$$

On a $\sharp f = 3$. Il n'y a aucun autre choix possible concernant la numérotation des sommets que celle donnée par la décoration :

$$l(x_1) = \eta, \quad l(x_2) = \mu, \quad l(x_3) = \mu.$$

On obtient les ensembles suivants :

$$\begin{cases} S(f) = \{(x_2, 1), (x_2, 2), (x_3, 1), (x_3, 2), t_1\} \\ T(f) = \{(x_1, 1), (x_2, 3), (x_3, 3), s_1, s_2\}. \end{cases}$$

Enfin, la relation R_f est :

$$s_1 R_f (x_3, 1), \quad s_2 R_f (x_2, 2), \quad (x_1, 1) R_f (x_2, 1), \quad (x_2, 3) R_f (x_3, 2), \quad (x_3, 3) R_f t_1.$$

Toutes ces données sont résumées par celle de l sur chaque x_i et par le tableau :

s_1	s_2	$(x_1, 1)$	$(x_2, 3)$	$(x_3, 3)$
$(x_3, 1)$	$(x_2, 2)$	$(x_2, 1)$	$(x_3, 2)$	t_1

Calcul des produits et des composées

Examinons à présent la possibilité de calculer à l'aide de ces représentations. Supposons que $f : m \longrightarrow n$ et $g : p \longrightarrow q$ sont deux flèches de $\mathcal{L}\Sigma$: on peut déterminer la représentation de $f \otimes g$ à partir de celles de f et g . En effet, on peut vérifier que, à la renumérotation des sommets près :

$$\begin{cases} X(f \otimes g) = X(f) \cup X(g)^f \\ l_{f \otimes g}(x_i) = \begin{cases} l_f(x_i) & \text{si } i \in [\#f] \\ l_g(x_{i-\#f}) & \text{si } (i - \#f) \in [\#g] \end{cases} \\ S(f \otimes g) = S(f) \cup S(g)^f \\ T(f \otimes g) = T(f) \cup T(g)^f \\ R_{f \otimes g} = R_f \cup R_g^f \end{cases}$$

où l'action de f est donnée par $x_i^f = x_{i+\#f}$, $s_i^f = s_{i+m}$ et $t_i = t_{i+n}$. Notons que l'on peut aussi calculer directement avec les tableaux : le tableau associé à $(f \otimes g)$ est, à la renumérotation des sommets près, la juxtaposition du tableau associé à f et de celui associé à g dans lequel on a remplacé chaque x_i , s_i et t_i par, respectivement, x_i^f , s_i^f et t_i^f .

Pour la composition, supposons que $f : m \longrightarrow n$ et $g : n \longrightarrow p$ sont deux flèches de $\mathcal{L}\Sigma$. Toujours à renumérotation des variables près, on a :

$$\begin{cases} X(g \circ f) = X(f) \cup X(g)^f \\ l_{g \circ f}(x_i) = \begin{cases} l_f(x_i) & \text{si } i \in [\#f] \\ l_g(x_{i-\#f}) & \text{si } (i - \#f) \in [\#g] \end{cases} \\ S(g \circ f) = S_0(f) \cup S_0(g)^f \cup \{t_1, \dots, t_p\} \\ T(f \otimes g) = T_0(f) \cup T_0(g)^f \cup \{s_1, \dots, s_m\} \\ R_{f \otimes g} = (R_f[t_k := R_g(s_k)]) \cup (R_g^f[s_k := R_f^{-1}(t_k)]) \end{cases}$$

où $R_f[t_k := R_g(s_k)]$ est obtenu à partir de R_f en remplaçant chaque t_k par l'unique élément y de $S(g)$ vérifiant $s_k R_g y$ et $[s_k := R_f^{-1}(t_k)]$ est obtenu à partir de R_g en remplaçant chaque t_f par l'unique élément z de $T(f)$ vérifiant $z R_g s_k$.

Encore une fois, on peut calculer ce résultat directement avec les tableaux. Celui de $g \circ f$ est, à la renumérotation des sommets près, le tableau obtenu à partir de ceux de f et g de la manière suivante :

1. On extrait du tableau de f les colonnes dont la deuxième ligne est un des t_k , $k \in [n]$.
2. On extrait du tableau de g les colonnes dont la première ligne est un des s_k , $k \in [n]$.

3. On concatène les colonnes restant dans chacun des deux tableaux, en faisant opérer $(\cdot)^f$ sur celui de g .
4. On rajoute au résultat les n colonnes obtenues par *composition* deux à deux de celles mises de côté : pour chaque $k \in [n]$, la paire (y_i, t_i) issue du tableau de f et la paire (s_i, z_i) issue de celui de g donnent (y_i, z_i^f) .

Exemple. On considère toujours la même signature Σ contenant deux flèches $\mu : 2 \longrightarrow 1$ et $\eta : 0 \longrightarrow 1$.

1. Commençons par effectuer le produit des deux flèches $f : 3 \longrightarrow 1$ et $g : 1 \longrightarrow 1$ suivantes :

$$f = \mu \circ (1 \otimes \mu) \quad \text{et} \quad g = \mu \circ (\varepsilon \otimes 1).$$

On va utiliser directement les tableaux. Pour f , on a $l_f(x_1) = l_f(x_2) = \mu$ et :

s_1	s_2	s_3	$(x_1, 3)$	$(x_2, 3)$
$(x_2, 1)$	$(x_1, 1)$	$(x_1, 2)$	$(x_2, 2)$	t_1

Pour g , on a $l_g(x_1) = \eta$ et $l_g(x_2) = \mu$, ainsi que :

s_1	$(x_1, 1)$	$(x_2, 3)$
$(x_2, 2)$	$(x_2, 1)$	t_1

On décale tous les indices dans les données de g et on rassemble, ce qui donne $l(x_1) = l(x_2) = l(x_4) = \mu$ et $l(x_3) = \eta$, ainsi que le tableau suivant :

s_1	s_2	s_3	$(x_1, 3)$	$(x_2, 3)$	s_4	$(x_3, 1)$	$(x_4, 3)$
$(x_2, 1)$	$(x_1, 1)$	$(x_1, 2)$	$(x_2, 2)$	t_1	$(x_4, 2)$	$(x_4, 1)$	t_2

On vérifie alors que, au renumérotage des sommets près, ces données sont bien celles associées à $f \otimes g$.

2. Calculons à présent la composée de $f : 2 \longrightarrow 2$ et $g : 2 \longrightarrow 1$, avec :

$$f = \mu \otimes \varepsilon \quad \text{et} \quad g = \mu.$$

Pour f , on a $l_f(x_1) = \mu$, $l_f(x_2) = \eta$ et :

s_1	s_2	$(x_1, 3)$	$(x_2, 1)$
$(x_1, 1)$	$(x_1, 2)$	t_1	t_2

Quant à g , on obtient $l_g(x_1) = \mu$ et :

s_1	s_2	$(x_1, 3)$
$(x_1, 1)$	$(x_1, 2)$	t_1

On procède, comme décrit précédemment, en isolant certaines colonnes, en effectuant les décalages et recollement de colonnes nécessaires, et on obtient $l(x_1) = l(x_3) = \mu$, $l(x_2) = \eta$ et :

s_1	s_2	$(x_3, 3)$	$(x_1, 3)$	$(x_2, 1)$
$(x_1, 1)$	$(x_1, 2)$	t_1	$(x_3, 1)$	$(x_3, 2)$

La double barre sépare les colonnes qui sont restées telles qu'elles ou qui ont éventuellement subi un décalage d'indices (à gauche) des colonnes obtenues par composition (à droite). On vérifie que, à renumérotation des sommets près, on a bien obtenu la décoration et le tableau associés à $g \circ f$.

Flèches associées aux représentations de diagrammes

Nous allons à présent examiner s'il est possible de récupérer une flèche à partir des données que nous venons de définir. Pour tout couple (m, n) d'entiers, définissons $\mathcal{S}\Sigma(m, n)$ comme l'ensemble des triplets (X, l, R) où X est un ensemble fini, dont les éléments sont notés x_1, \dots, x_k , l est une application de X dans $\text{Fl}\Sigma$ et R est une correspondance bijective entre les ensembles S_X et T_X , construits comme $S(f)$ et $T(f)$ précédemment.

On définit le produit et, le cas échéant, la composée de deux éléments de $\mathcal{S}\Sigma$ comme dans le cas où ils sont associés à des flèches de $\mathcal{L}\Sigma$. On peut vérifier que $\mathcal{S}\Sigma$ est une opérade. La question qui se pose est la suivante :

Quels éléments de $\mathcal{S}\Sigma(m, n)$ correspondent à des flèches de $\mathcal{L}\Sigma$?

Tout d'abord, rappelons que si deux éléments de $\mathcal{S}\Sigma$ sont obtenus à partir de flèches de $\mathcal{L}\Sigma$, leur produit et, si elle est définie, leur composée correspondent à une flèche de $\mathcal{L}\Sigma$. Cependant, tous les éléments de $\mathcal{S}\Sigma$ ne vérifient pas cette propriété.

- Exemples.** 1. Le premier exemple est donné par l'élément de $\mathcal{S}\Sigma(2, 2)$ tel que $X = \emptyset$ avec $s_1 R t_2$ et $s_2 R t_1$. Si l'on essaie de tracer le diagramme associé, on se rend compte que l'on est obligé de croiser les arêtes si l'on veut que les deux soient descendantes. Or on l'a interdit lorsque l'on a évoqué les graphes planaires descendants. Nous n'avons pas précisé quelle était la signature Σ utilisée car cet élément est présent dans tous les $\mathcal{S}\Sigma$, quelle que soit Σ .
2. Pour le deuxième exemple, fixons la signature Σ : on la choisit avec une seule flèche, notée σ . Dans $\mathcal{S}\Sigma(0, 0)$, on trouve l'élément suivant : $X = \{x_1\}$, $l(x_1) = \sigma$ et $(x_1, 2) R (x_1, 1)$. Si l'on trace le diagramme associé, on obtient un sommet décoré par σ dont la sortie est reliée à l'entrée : encore une fois, cette situation est prohibée par le fait que les arêtes doivent être descendantes.

Afin d'éviter ces situations, on peut définir des critères caractérisant les éléments de $\mathcal{S}\Sigma$ qui sont des flèches de $\mathcal{L}\Sigma$. Pour l'instant, nous n'avons que des pistes concernant ces critères.

Définition. Soient Σ une signature et (X, l, R) un élément de $\mathcal{S}\Sigma(m, n)$. On note \bar{X} l'ensemble :

$$\bar{X} = X \amalg \{s_1, \dots, s_m\} \amalg \{t_1, \dots, t_n\}.$$

Un *chemin descendant élémentaire* de (X, l, R) est un couple (a, b) d'éléments de \bar{X} vérifiant l'une des conditions suivantes :

- il existe $i \in [m]$ et $j \in [n]$ tels que $a = s_i$, $b = t_j$ et $s_i R t_j$;
- il existe $i \in [m]$, $x \in X$ et $j \in [s(x)]$ tels que $a = s_i$, $b = x$ et $s_i R(x, j)$;
- il existe $x \in X$, $s(x) < i \leq s(x) + t(x)$ et $j \in [n]$ tels que $a = x$, $b = t_j$ et $(x, i) R t_j$;
- il existe $x, y \in X$, $s(x) < i \leq s(x) + t(x)$ et $j \in [s(y)]$ tels que $a = x$, $b = y$ et $(x, i) R(y, j)$.

Un *chemin descendant* de (X, l, R) est une famille (x_1, \dots, x_p) telle que chaque couple (x_q, x_{q+1}) est un chemin descendant élémentaire de (X, l, R) ; un tel chemin est dit *allant de x_1 à x_p* .

On définit sur \bar{X} la relation *est plus à gauche que*, notée \triangleright , en posant $a \triangleright b$ si l'on est dans un des cas suivants :

- il existe $i, j \in [m]$, tels que $i > j$, ainsi que des chemins descendants allant de s_i à a et de s_j à b ;
- il existe $i, j \in [n]$, tels que $i > j$, ainsi que des chemins descendants allant de a à t_i et de b à t_j .

◆

On formule une conjecture. Un élément (X, l, R) de $\mathcal{S}\Sigma(m, n)$ correspond à une flèche de $\mathcal{L}\Sigma(m, n)$ si et seulement si les deux conditions suivantes sont remplies :

1. Il n'y a aucun chemin descendant de longueur non nulle dans (X, l, R) allant d'un sommet $x \in \bar{X}$ vers lui-même.
2. La clôture transitive de \triangleright est un ordre strict sur \bar{X} .

Remarque. La seconde condition a pour but d'interdire les croisements entre les arêtes, la première les rebroussements. Il semble que si l'on n'impose que la première condition, on obtienne une représentation fidèle des flèches de l'opérade symétrique librement engendrée par Σ . Si l'on n'impose aucun des deux critères, $\mathcal{S}\Sigma$ paraît être l'opérade souveraine librement engendrée par Σ .

Comme nous l'avons dit précédemment, cette section devra être développée dans le but d'implanter, en particulier, la méthode de calcul des paires critiques d'une présentation d'opérade de 3.8.2, mais aussi d'automatiser la technique d'interprétation de 3.7.

Chapitre 4

Présentations de monoïdes commutatifs ou réseaux de Petri

Nous allons rappeler le formalisme usuel des réseaux de Petri. Notons que, selon les auteurs, la présentation peut varier ; de plus, il existe de nombreuses généralisations ; on pourra se référer à [Mur89] pour plus de détails.

Après ces rappels, nous verrons qu'un réseau de Petri est équivalent à une présentation de monoïde commutatif ; enfin, nous montrerons comment plonger un tel objet dans une présentation d'opérade.

4.1 Une description succincte des réseaux de Petri

Un *réseau de Petri* est une donnée $\mathcal{R} = (X, T, w)$ où X et T sont des ensembles finis dont les éléments sont respectivement appelés *places* et *transitions*, et w est une application :

$$w : (X \times T) \amalg (T \times X) \longrightarrow \mathbb{N}.$$

Un réseau de Petri est représenté graphiquement de la manière suivante : on associe un sommet à chaque place et à chaque transition, avec des formes différentes (classiquement un cercle pour une place et une double barre pour une transition). Puis, pour chaque couple (x, t) de $X \times T$, on trace une arête de x à t si et seulement si $w(x, t) > 0$ et une de t à x si et seulement si $w(t, x) > 0$. Enfin, chaque arête est étiquetée par l'entier $w(x, t)$ ou $w(t, x)$ selon qu'elle va de x à t ou de t à x .

Exemple. On considère le réseau de Petri $\mathcal{R} = (X, T, w)$ où $X = x_1, x_2, x_3$, $T = t_1, t_2$ et

$$\begin{cases} w(x_1, t_1) = w(t_1, x_2) = w(t_1, x_3) = w(t_2, x_3) = 1 \\ w(x_2, t_2) = 2 \\ w(x, t) = 0 \text{ partout ailleurs.} \end{cases}$$

On peut le représenter comme dans la figure 4.1.

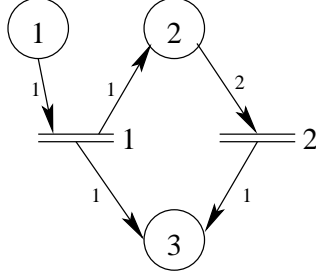


FIG. 4.1 – Un exemple de représentation graphique associée à un réseau de Petri.

Dans toute la suite, on fixe un réseau de Petri $\mathcal{R} = (X, T, w)$. On appelle *marquage* de \mathcal{R} toute application $\mu : X \rightarrow \mathbb{N}$. On note $\mathcal{M}(\mathcal{R})$ l'ensemble des marquages de \mathcal{R} . Un marquage est représenté graphiquement par des *jetons* placés dans les cercles correspondant aux places.

On définit, pour toute transition $t \in T$, une relation binaire \rightarrow_t sur $\mathcal{M}(\mathcal{R})$ de la manière suivante : si μ et ν sont des marquages, on a $\mu \rightarrow_t \nu$ si et seulement si

$$\text{pour tout } x \in X, \begin{cases} \mu(x) \geq w(x, t) \\ \mu(x) + w(t, x) = \nu(x) + w(x, t) \end{cases}$$

La première condition impose qu'il y ait au moins autant de jetons (pour le marquage μ) dans chaque place x que la valeur de $w(x, t)$. Si c'est le cas, on obtient ν ainsi :

1. On ôte $w(x, t)$ jetons de chaque place x .
2. On rajoute $w(t, x)$ jetons dans chaque place x .

Remarquons que, si toutes les inégalités $\mu(x) \geq w(x, t)$, $x \in X$, sont vraies, il y a un et un seul marquage ν tel que $\mu \rightarrow_t \nu$.

On définit alors \rightarrow_T comme la réunion de toutes les relations \rightarrow_t , $t \in T$. L'ARS associé au réseau de Petri $\mathcal{R} = (X, T, w)$ est $(\mathcal{M}(\mathcal{R}), \rightarrow_T)$. Si μ et ν sont des marquages, on dit

que ν est *atteignable* à partir de μ si $\mu \rightarrow_T \nu$.

De nombreux problèmes se posent concernant un réseau de Petri. L'un des plus courant est celui dit d'*atteignabilité*. On peut le décrire ainsi :

Données : un réseau de Petri $\mathcal{R} = (X, T, w)$ et deux marquages μ et ν de \mathcal{R} .

Question : est-ce que ν est atteignable à partir de μ ?

Cela ressemble à un problème de mots : on voudrait exhiber la structure algébrique dans laquelle le formuler. En fait, la résolution du problème de mots ne fournit qu'une procédure de semi-décision pour celui de l'atteignabilité, c'est-à-dire que l'on n'obtient qu'une condition nécessaire pour répondre de manière affirmative à la question. Cette procédure est cependant complète dans le cas des réseaux de Petri réversibles, c'est-à-dire ceux pour lesquels \rightarrow_T et \equiv_T coïncident. Autrement dit, le problème de mots est équivalent au problème suivant :

Données : un réseau de Petri $\mathcal{R} = (X, T, w)$ et deux marquages μ et ν de \mathcal{R} .

Question : est-ce que μ et ν sont égaux *modulo* la relation d'équivalence \equiv_T ?

Comme $\mu \rightarrow_T \nu$ donne $\mu \equiv_T \nu$, on a bien une condition nécessaire pour le problème d'atteignabilité.

Exemple. En reprenant l'exemple précédent, étudions les transitions possibles à partir du marquage $\mu(x_1) = 2$, $\mu(x_2) = 2$ et $\mu(x_3) = 0$. On a représenté les différentes évolutions dans la figure 4.2.

4.2 Un survol des présentations de monoïdes commutatifs

On va imiter ce qui a été fait précédemment pour les monoïdes, mais en ajoutant partout *commutatif* après monoïde. Rappelons tout d'abord ceci :

Définition. Un monoïde M est dit *commutatif* si $xy = yx$ pour tous $x, y \in M$. On note \mathbf{COM} la sous-catégorie pleine de \mathbf{MON} formée par les monoïdes commutatifs. \blacklozenge

On peut écrire un problème universel de monoïde commutatif libre engendré par un ensemble. On va plutôt directement donner sa solution :

Définition. Soit X un ensemble. Le *monoïde commutatif libre engendré par X* est le monoïde noté $[X]$ admettant la présentation (X, E) où E est l'ensemble des couples (xy, yx) pour tous $x, y \in X$. \blacklozenge

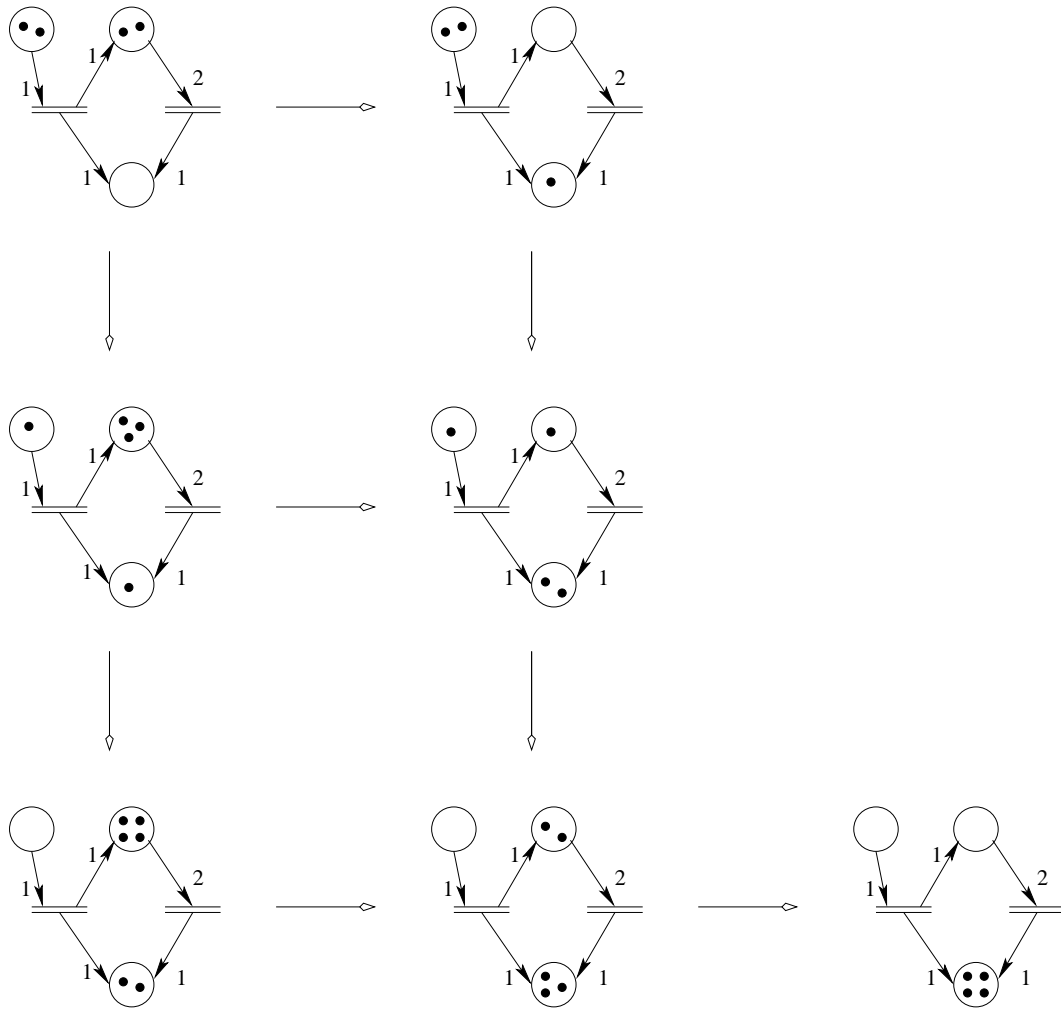


FIG. 4.2 – Évolutions possibles d'un marquage d'un réseau de Petri.

Il se trouve que, si l'on fixe un ordre total sur X , on obtient une présentation convergente de X en remplaçant E par R défini ainsi :

$$R = \{(yx, xy) | x, y \in X, x < y\}.$$

Par suite, tout élément de $[X]$ possède une unique forme normale dans (X, R) . Cela revient à constater qu'un élément de $[X]$ est entièrement déterminé par le nombre d'occurrences de chaque élément de X dans son écriture, nombre qui est nul pour tous les $x \in X$ sauf un nombre fini. On note $\deg(x, a)$ le nombre d'occurrences de $x \in X$ dans $a \in [X]$, aussi appelé *degré de x dans a* .

On obtient ainsi une autre définition équivalente de $[X]$ comme l'ensemble des applications $f : X \rightarrow \mathbb{N}$ telles que $f(x) = 0$ sauf pour un nombre fini d'éléments. Le produit est défini ainsi : $fg(x) = f(x) + g(x)$. Le fait que l'on obtienne un monoïde commutatif provient du fait que \mathbb{N} en est un.

Dans le cas où X est fini, on pose $X = \{x_1, \dots, x_n\}$. Alors, les éléments de $[X]$ sont exactement les $x_1^{i_1} \dots x_n^{i_n}$ pour i_1, \dots, i_n parcourant \mathbb{N} . C'est exactement l'ensemble des formes normales de la présentation de monoïde (X, R) , les règles R étant obtenues comme précédemment avec l'ordre total $x_1 < \dots < x_n$.

Comme $[X]$ est aussi un monoïde, on peut se rattacher à l'étude de cette structure pour définir les notions de $[X]$ -modules et d'idéaux de $[X]$. Un M -module aura exactement la même définition que dans le cas non commutatif. Cependant, la commutativité a certaines conséquences sur le M -module *diagonal*. En effet, M^2 est muni des deux actions diagonales de M , l'une à gauche, l'autre à droite; en utilisant la commutativité du produit de M , on obtient :

$$a(x, y) = (ax, ay) = (xa, ya) = (x, y)a.$$

Ainsi, les deux actions diagonales coïncident. On a quand même les définitions suivantes :

Définition. Soit M un monoïde commutatif. Les éléments de M^2 sont appelés *relations* ou *règles de réécriture sur M* . Un *idéal de M* ou *relation de réduction sur M* est un sous- M -module du module diagonal. ♦

On peut encore donner plusieurs constructions de l'idéal $(R) = \rightarrow_R$ engendré par une partie R de M^2 . La première est directe : les éléments de (R) sont exactement les éléments de M^2 de la forme $x\alpha$ avec $x \in M$ et $\alpha \in R$. La seconde version revient au même mais passe par les contextes :

Définition. Soit M un monoïde commutatif. Un *contexte sur M* est un élément de $\mathcal{C}M$, le M -module libre engendré par le singleton $\{\square\}$. ♦

Les contextes de M sont munis d'une structure de monoïde commutatif (pour la composition), ils sont tous de la forme $x\square$, pour $x \in M$, et agissent sur les éléments de M par $(x\square)[a] = xa$. Ainsi, l'idéal (R) de M engendré par une partie R de M^2 possède la description suivante : les éléments de (R) sont exactement les éléments de M^2 de la forme $C[\alpha]$ pour $C \in \mathcal{CM}$ et $\alpha \in R$. Pour conclure :

Définition. Une *présentation de monoïde commutatif* est un couple (X, R) constitué d'un ensemble X et d'une partie R de $[X]^2$. L'ARS associé à (X, R) est $([X], (R))$. ♦

4.3 Les réseaux de Petri sont des présentations de monoïdes commutatifs

On considère toujours un réseau de Petri $\mathcal{R} = (X, T, w)$. On va montrer que l'on peut construire une présentation de monoïde commutatif dont l'ARS est isomorphe à celui de \mathcal{R} . L'idée sous-jacente est qu'un réseau de Petri spécifie les lettres de l'alphabet ainsi que les règles de réécriture, les marquages de ce réseau étant les termes de la réécriture.

L'ensemble $\mathcal{M}(\mathcal{R})$ des marquages de \mathcal{R} possède une structure de monoïde commutatif, donnée par l'addition des jetons dans chaque place. De plus, ce monoïde est isomorphe à $[X]$, comme nous allons le voir.

On se donne un marquage μ de \mathcal{R} ; on lui associe un élément $\varphi(\mu)$ de $[X]$ de la façon suivante :

$$\varphi(\mu) = \prod_{x \in X} x^{\mu(x)}.$$

Réciproquement, si $a \in [X]$, on définit un marquage $\psi(a)$ ainsi sur un élément $x \in X$:

$$\psi(a)(x) = \deg(x, a).$$

Ces deux applications sont des morphismes de monoïdes (commutatifs) et inverses l'une de l'autre.

Pour les transitions, on commence par associer à chaque $t \in T$ un couple $(g(t), d(t))$ de marquages en posant :

$$g(t) = w(\cdot, t) \quad \text{et} \quad d(t) = w(t, \cdot).$$

On étend alors $\varphi : \mathcal{M}(\mathcal{R}) \longrightarrow [X]$ en $\varphi : T \longrightarrow [X]^2$ en posant :

$$\varphi(t) = (\varphi(g(t)), \varphi(d(t))).$$

On a donc $\varphi(T)$ une partie de $[X]^2$ et on note $(\varphi(T)) \Rightarrow_{\varphi(T)}$ l'idéal de $[X]$ qu'elle engendre.

Lemme 4.1. *Soient μ et ν deux marquages et t une transition. Alors $\mu \rightarrow_t \nu$ si et seulement s'il existe un élément q de $[X]$ tel que :*

$$(\varphi(\mu), \varphi(\nu)) = q \cdot \varphi(t).$$

Démonstration. Supposons que $\mu \rightarrow_t \nu$. On a alors, pour tout x dans X :

$$\mu(x) \geq w(x, t).$$

Donc $\varphi(g(t))$ divise $\varphi(\mu)$ et, par suite, il existe q vérifiant :

$$\varphi(\mu) = q \cdot \varphi(g(t)).$$

Il s'agit de :

$$q = \prod_{x \in X} x^{\mu(x) - w(x, t)}.$$

De plus, pour tout x dans X :

$$\mu(x) + w(t, x) = \nu(x) + w(x, t).$$

Donc :

$$\varphi(\mu) \cdot \varphi(d(t)) = \varphi(\nu) \cdot \varphi(g(t)).$$

Par suite et puisque $[X]$ est libre :

$$q \cdot \varphi(g(t)) \cdot \varphi(d(t)) = \varphi(\nu) \cdot \varphi(g(t)) \quad \text{et} \quad \varphi(\nu) = q \cdot \varphi(d(t)).$$

Enfin :

$$(\varphi(\mu), \varphi(\nu)) = q \cdot \varphi(t).$$

Réciproquement, supposons qu'il existe q tel que $(\varphi(\mu), \varphi(\nu)) = q \cdot \varphi(t)$. On a, d'une part, pour tout x dans X :

$$\mu(x) \geq w(x, t).$$

Et d'autre part, pour tout x de X :

$$\mu(x) = w(x, t) + \deg(x, q) \quad \text{et} \quad \nu(x) = w(t, x) + \deg(x, q).$$

Ce qui donne, pour tout x dans X :

$$\mu(x) + w(t, x) = \nu(x) + w(x, t).$$

On en conclut que $\mu \rightarrow_t \nu$.

◇

Corollaire 4.2. *Soient μ et ν deux marquages de \mathcal{R} . Alors $\mu \rightarrow_T \nu$ si et seulement si $\varphi(\mu) \rightarrow_{\varphi(T)} \varphi(\nu)$. En d'autres termes, les ARS $(\mathcal{M}(\mathcal{R}), \rightarrow_T)$ et $([X], \rightarrow_{\varphi(T)})$ sont isomorphes.*

4.4 Présentation d'opérade associée à une présentation de monoïde commutatif

Comme pour les présentations de monoïdes, on cherche une opérade interprétant le cadre commutatif. Soit X un ensemble ; la première idée est de prendre la même signature Σ_X que pour les mots : tous les éléments de X sont vus comme des flèches $1 \longrightarrow 1$. Puis on quotiente l'opérade $\mathcal{L}\Sigma_X$ par l'idéal engendré par l'ensemble E des couples $(x \circ y, y \circ x)$, pour tous les $x, y \in X$. Ainsi, on reproduit, au niveau des catégories, la présentation par générateurs et relations du monoïde $[X]$.

Dans ce cas, les éléments de $[X]$ seront exactement les flèches $1 \longrightarrow 1$ de $\mathcal{L}\Sigma_X/E$. Étant donnée une famille R de règles sur $[X]$, on a alors un choix à faire. La première possibilité est de travailler *modulo* E . C'est-à-dire que les éléments sur lesquels portent la réécriture sont des classes d'équivalence de flèches de $\mathcal{L}\Sigma$: on rentre ici dans le domaine périlleux de la réécriture *modulo* (ici modulo commutativité).

La seconde piste est de rajouter les règles de E à celles de R : on reste ainsi dans le monde de la réécriture de mots (classiques), en espérant que l'ajout de règles ne modifie pas les propriétés de terminaison et de confluence de \rightarrow_R . Cependant, ce n'est pas toujours le cas ; pire, il est possible que le monoïde $\langle X \rangle / \equiv_R$ possède une présentation convergente mais que $\langle X \rangle / \equiv_{R \cup E}$ n'en ait pas.

Ce problème se posera de nouveau pour la réécriture de termes. Nous y reviendrons alors. Ici, les opérades fournissent une troisième voie pour éviter ces questions.

En effet, du point de vue des opérades, les structures de monoïdes et de monoïdes commutatifs sont *essentiellement* différentes. Dans une telle catégorie \mathbb{C} , comme dans toutes les autres, tout ensemble d'endomorphismes $\mathbb{C}(n, n)$ hérite de \mathbb{C} d'une structure de monoïde : ainsi, pour $\mathcal{L}\Sigma_X(1, 1)$, on retrouve le monoïde libre $\langle X \rangle$. Cependant, la structure monoïdale d'une opérade a un effet étonnant sur l'un de ces monoïdes : il est *naturellement* commutatif. Il s'agit de l'ensemble des scalaires de \mathbb{C} , $\mathbb{C}(0, 0)$.

Cet ensemble d'endomorphismes possède *deux* structures de monoïde avec des relations entre elles. Or, un résultat d'algèbre générale nous indique que :

Proposition 4.3. *Soit M un ensemble muni de deux lois de composition interne \cdot et $*$ vérifiant la relation suivante :*

$$(x \cdot y) * (z \cdot t) = (x * z) \cdot (y * t)$$

et admettant chacune un élément neutre à gauche et à droite. Alors ces deux lois coïncident et sont commutatives.

Démonstration. On note e l'élément neutre de \cdot et ε celui de $*$. On va commencer par montrer que $e = \varepsilon$. On applique la relation avec $x = t = e$ et $y = z = \varepsilon$. D'une part :

$$(e \cdot \varepsilon) * (\varepsilon \cdot e) = \varepsilon * \varepsilon = \varepsilon.$$

La première égalité est donnée en appliquant la neutralité à gauche et à droite de e pour \cdot ; la seconde en appliquant la neutralité à gauche ou à droite de ε pour $*$. D'autre part, on a :

$$(e * \varepsilon) \cdot (\varepsilon * e) = e \cdot e = e.$$

Or la relation entre \cdot et $*$ nous dit que :

$$(e \cdot \varepsilon) * (\varepsilon \cdot e) = (e * \varepsilon) \cdot (\varepsilon * e)$$

et donc que $e = \varepsilon$. Maintenant, si x et y sont deux éléments de M quelconques, on a :

$$x * y = (x \cdot e) * (e \cdot y) = (x * e) \cdot (e * y) = x \cdot y.$$

Par suite, les deux opérations coïncident. Pour finir :

$$x * y = (e \cdot x) * (y \cdot e) = (e * y) \cdot (x * e) = y \cdot x.$$

Puisque les deux opérations coïncident, elles sont de plus commutatives. \diamond

On l'applique à $\mathbb{C}(0, 0)$ en prenant $\cdot = \circ$ et $*$ = \otimes :

Corollaire 4.4. *Dans toute opérade \mathbb{C} , les restrictions à $\mathbb{C}(0, 0)$ de la composition et du produit coïncident et sont commutatives.*

Ainsi, l'ensemble $\mathbb{C}(0, 0)$ des scalaires de \mathbb{C} , muni de la composition (ou du produit), est un monoïde commutatif. Si l'on veut retrouver les éléments de $[X]$ comme flèches d'une opérade, on définit la signature Σ_X^{ab} en posant :

$$\Sigma_X^{ab}(m, n) = \begin{cases} X & \text{si } m = n = 0 \\ \emptyset & \text{sinon.} \end{cases}$$

Une partie R de $[X]^2$ est vue comme une partie \mathcal{R} de $(\mathcal{L}\Sigma_X^{ab})^2$, avec seulement des flèches $0 \longrightarrow 0$. On obtient le résultat suivant :

Théorème 4.5. *Soit (X, R) une présentation de monoïde commutatif. Alors, l'ARS associé à la présentation d'opérade $(\mathcal{L}\Sigma_X^{ab}, (\mathcal{R}))$ contient l'ARS $([X], (R))$ associé à (X, R) . Plus précisément, on a un isomorphisme d'ARS :*

$$([X], (R)) \simeq (\mathcal{L}\Sigma_X^{ab}(0, 0), (\mathcal{R})(0, 0)).$$

La preuve est la même que pour le théorème 3.11 concernant les monoïdes.

4.5 Un ordre de réduction particulier

Avant de passer à la réécriture de termes, nous allons définir un ordre de réduction particulier sur les monoïdes commutatifs libres : le *multiordre*. Nous l'avons déjà utilisé au chapitre 3, pour démontrer la terminaison de la présentation $L(\mathbb{Z}_2)$, comme exemple d'utilisation du théorème 3.17.

On fixe un ensemble X que l'on suppose muni d'un ordre strict $>$ qui termine. On veut étendre cet ordre au monoïde commutatif libre $[X]$ afin d'obtenir un ordre de réduction. Remarquons que nous n'avons pas défini cette notion pour les monoïdes commutatifs; cependant, comme précédemment, il suffit de reprendre celle des monoïdes et de l'adapter : un ordre de réduction sur un monoïde commutatif M est à la fois un ordre strict qui termine et un idéal de M .

Donnons l'intuition de la construction. Un élément de $[X]$ s'écrit comme une somme formelle d'éléments de X : c'est d'ailleurs pour cela qu'on appelle parfois *multiensembles sur X* les éléments de $[X]$. L'ordre que nous allons construire est aussi connu sous le nom *ordre des multiensembles sur X associé à $>$* et noté $>_{\text{mul}}$; nous l'appellerons le *multiordre engendré par $>$* et nous le noterons encore $>$. De manière informelle, on dira qu'un élément a de $[X]$ est plus grand qu'un autre élément b si tout élément de X intervenant dans l'écriture de b est majoré par un élément de X intervenant dans l'écriture de a .

Précisons maintenant la construction. On commence par étendre l'ordre $>$ de X en une partie de $X \times [X]$, toujours notée $>$: si $x \in X$ et $a \in [X]$ on pose que $x > a$ si $a = 0$ ou si tout élément y de X intervenant dans l'écriture de a vérifie $x > y$. Puis, on étend cette relation en une relation binaire $>$ sur $[X]$ par clôture relativement aux opérations :

Définition. Soit X un ensemble muni d'un ordre strict noté $>$. On appelle *multiordre engendré par $>$* la relation binaire sur $[X]$ donnée par $a > b$ s'il existe a' , b' et c dans $[X]$ vérifiant les conditions suivantes :

$$\begin{cases} a = a' + c \\ b = b' + c \\ a' = x_1 + \cdots + x_m, & m > 0, x_1, \dots, x_m \in X \\ b' = y_1 + \cdots + y_n, & n \geq 0, y_1, \dots, y_n \in X \\ \text{pour tout } j \in [n], \text{ il existe un } i \in [m], \text{ tel que } x_i > y_j. \end{cases}$$

On a le résultat suivant :

Proposition 4.6. *Si $>$ est un ordre strict qui termine sur un ensemble X , alors le multiordre $>$ engendré est un ordre de réduction sur $[X]$.*

On trouvera une preuve de ce résultat dans [BN98]. Comme nous l'avons déjà fait pour $L(\mathbb{Z}_2)$, nous utiliserons à plusieurs reprises le multiordre engendré sur $[\mathbb{N}]$ (ou $[\mathbb{N}^*]$) par l'ordre usuel de \mathbb{N} (ou \mathbb{N}^*) afin de prouver la terminaison de diverses présentations d'opérades en utilisant 3.17.

Chapitre 5

Réécriture de termes et présentations d'opérades

Le but de cette partie est de prouver que l'on peut associer, à tout système de réécriture de termes linéaire à gauche, une présentation d'opérade qui le simule complètement.

Après avoir rappelé les notions essentielles de la réécriture de termes, nous verrons que l'ensemble des termes construits à partir d'une signature algébrique Σ est une partie de l'opérade cartésienne libre engendrée par Σ . Puis, nous donnerons une présentation convergente de cette opérade cartésienne. Enfin, nous démontrerons le théorème 5.40 qui nous dit que, dans le cas linéaire à gauche, la présentation obtenue, munie d'une interprétation des règles R du système de réécriture de termes, simule complètement (Σ, R) .

5.1 Systèmes de réécriture de termes

La réécriture de termes s'intéresse aux calculs effectués dans des algèbres quelconques : un tel objet est un ensemble muni d'opérations de différentes arités qui vérifient un certain nombre de relations. Cette approche générale des structures algébriques permet de décrire aussi bien des structures classiques comme des monoïdes ou des groupes que des structures complètement exotiques. Ici, la réécriture opère sur des *termes* qui représentent les opérateurs abstraits de la structure considérée ; les règles de réécriture sont des versions orientées des relations, dont le but est de permettre le calcul de formes normales pour les opérateurs abstraits de la structure.

5.1.1 Termes et règles de réécriture

Soit Σ une signature *algébrique*, c'est-à-dire une signature dont toutes les flèches ont 1 pour but. On fixe un ensemble dénombrable V , dont les éléments sont appelés *variables*.

Par opposition, les flèches de $\Sigma(0, 1)$ sont appelées *constantes*. L'ensemble $T_\Sigma(V)$ des termes associés à Σ est construit par induction à partir des éléments de V de la manière suivante. On pose $T_\Sigma(V)_0 = V \amalg \Sigma(0, 1)$. Puis, si $T_\Sigma(V)_n$ est construit, on définit $T_\Sigma(V)_{n+1}$ ainsi :

$$T_\Sigma(V)_{n+1} = \coprod_{k \in \mathbb{N}^*} \Sigma(k, 1) \times T_\Sigma(V)_n^{(k)}$$

où $T_\Sigma(V)_n^{(k)}$ est l'ensemble des (t_1, \dots, t_k) tels que, pour tout i , t_i est dans $T_\Sigma(V)_{p_i}$ avec $p_i \leq n$ pour tout i et $p_i = n$ pour au moins un i . Enfin, on prend pour $T_\Sigma(V)$ la réunion disjointe de tous les $T_\Sigma(V)_n$.

Un élément $(\varphi, t_1, \dots, t_k)$ de $T_\Sigma(V)_n$ est noté $\varphi(t_1, \dots, t_k)$; on dit qu'il est de *degré* n . Pour un terme t , on définit l'ensemble $V(t)$ des *variables de* t , toujours par induction : pour commencer, on pose $V(x) = \{x\}$ si $x \in V$ et $V(\gamma) = \emptyset$ si $\gamma \in \Sigma(0, 1)$. Puis, si $t = \varphi(t_1, \dots, t_k)$ est un terme de degré $n + 1$, on pose $V(t) = V(t_1) \cup \dots \cup V(t_k)$. Ceci permet de définir la notion de *règle de réécriture* sur $T_\Sigma(V)$:

Définition. Une *règle de réécriture* sur $T_\Sigma(V)$ est un couple (u, v) de termes tels que $u \notin V$ et $V(v) \subseteq V(u)$. ♦

On verra dans la suite que, d'un point de vue théorique limité aux termes, la première condition n'est pas obligatoire ; cependant, une règle de réécriture dont le premier membre est une variable donnerait obligatoirement une relation de réduction qui ne termine pas. De plus, nous aurons besoin de cette condition pour démontrer le théorème 5.40.

Définition. Un *système de réécriture de termes* est un couple (Σ, R) composé d'une signature algébrique et d'une famille de règles de réécriture sur $T_\Sigma(V)$. ♦

Notons que l'ensemble des variables n'est pas donné dans le système de réécriture : on peut le remplacer par n'importe quel autre ensemble dénombrable. En effet, si V' est un autre ensemble dénombrable, il existe une bijection $\sigma : V \rightarrow V'$. On envoie chaque terme de $T_\Sigma(V)$ sur un terme de $T_\Sigma(V')$ en remplaçant toutes ses variables par leur image par σ . On opère de même sur les règles. Il est évident que l'on obtient un système de réécriture « équivalent ». Le fait que l'on puisse remplacer V par tout autre ensemble dénombrable sera expliqué lorsque nous aurons vu que l'utilisation des variables correspond à celle des opérateurs de l'opérade cartésienne initiale : on peut donc remplacer les variables par toute autre version de cette opérade comme, par exemple, un autre ensemble de variables.

5.1.2 Contextes, substitutions et relations de réduction

Avant de définir la notion de relation de réduction associée à une famille de règles de réécriture, on doit définir celles de contextes et de substitutions. De manière informelle,

un contexte est un terme avec exactement un emplacement de libre. Plus formellement, on construit l'ensemble $C_\Sigma(V)$ des *contextes sur* Σ par induction : on commence par $C_\Sigma(V)_0 = \{\square\}$, un ensemble réduit à un élément noté \square ; puis, si l'on a construit $C_\Sigma(V)_n$, on définit $C_\Sigma(V)_{n+1}$ comme :

$$C_\Sigma(V)_{n+1} = \coprod_{k \in \mathbb{N}^*, i \in [k]} \Sigma(k, 1) \times (T_\Sigma(V))^{i-1} \times C_\Sigma(V)_n \times (T_\Sigma(V))^{k-i}.$$

On pose enfin $C_\Sigma(V)$ la réunion disjointe des $C_\Sigma(V)_n$. Un contexte est donc un terme dans lequel on a remplacé exactement une variable par le symbole \square .

Comme pour les termes, on note $\varphi(t_1, \dots, C, \dots, t_k)$ un élément $(\varphi, t_1, \dots, C, \dots, t_k)$ de $C_\Sigma(V)_n$. Tout contexte C définit une application $C[\cdot] : T_\Sigma(V) \longrightarrow T_\Sigma(V)$ en posant $\square[t] = t$ et, si $C = \varphi(t_1, \dots, D, \dots, t_k)$, $C[u] = \varphi(t_1, \dots, D[u], \dots, t_k)$: l'application de C à u revient à remplacer, dans C , le symbole \square par u .

Les substitutions sont les applications $T_\Sigma(V) \longrightarrow T_\Sigma(V)$ qui remplacent les variables des termes par d'autres termes. On définit l'ensemble $S_\Sigma(V)$ des *substitutions sur* Σ comme l'ensemble des applications $\sigma : T_\Sigma(V) \longrightarrow T_\Sigma(V)$ vérifiant :

$$\sigma(\varphi(t_1, \dots, t_k)) = \varphi(\sigma(t_1), \dots, \sigma(t_k))$$

pour tout $\varphi \in \Sigma(k, 1)$ et tous t_1, \dots, t_k dans $T_\Sigma(V)$. On voit qu'une substitution est entièrement déterminée par ses valeurs sur les variables : les substitutions sont en correspondance bijective avec les applications $V \longrightarrow T_\Sigma(V)$.

La composition des applications munit $S_\Sigma(V)$ d'une structure de monoïde qui, de plus, agit à droite sur l'ensemble $T_\Sigma(V)$ des termes, c'est-à-dire que pour tout terme t et toutes substitutions σ et σ' :

$$\begin{cases} (t \cdot \sigma) \cdot \sigma' = t \cdot (\sigma \circ \sigma') \\ t \cdot 1_V = t \end{cases}$$

On note $[x := t]$ la substitution qui envoie x sur t et laisse inchangées les autres variables. L'action d'une substitution σ sur un terme t est notée $t \cdot \sigma$ ou $t[x := t']$ si $\sigma = [x := t']$. On montre que :

Lemme 5.1. *Pour tout terme t et toute substitution σ , il existe des variables x_1, \dots, x_n et des termes t_1, \dots, t_n tels que :*

$$t \cdot \sigma = t[x_1 := t_1][x_2 := t_2] \dots [x_n := t_n].$$

Cette décomposition n'est pas unique et dépend a priori du terme t .

Démonstration. On note y_1, \dots, y_p les variables de t et, pour chaque $i \in [p]$, $y_{i,1}, \dots, y_{i,p_i}$ celles de $\sigma(y_i)$. Pour chaque couple (i, j) , avec $i \in [k-1]$ et $j \in [p_i]$, on choisit une variable $z_{i,j}$ de telle sorte que :

- les $z_{i,j}$ sont deux à deux distincts ;
- aucun $z_{i,j}$ n'est égal à un y_k ni à un $y_{k,l}$.

On a alors :

$$t \cdot \sigma = t \cdot ([y_1 := \sigma(y_1)] \circ \rho_1 \circ [y_2 := \sigma(y_2)] \circ \rho_2 \circ \dots \circ \rho_{p-1} \circ [y_p := \sigma(y_p)] \circ \rho'_{p-1} \circ \dots \circ \rho'_1),$$

où, pour $i \in [p-1]$, ρ_i et ρ'_i sont les substitutions suivantes :

$$\begin{cases} \rho_i = [y_{i,1} := z_{i,1}] \circ \dots \circ [y_{i,k_i} := z_{i,k_i}] \\ \rho'_i = [z_{i,1} := y_{i,1}] \circ \dots \circ [z_{i,k_i} := y_{i,k_i}]. \end{cases}$$

On conclut en rappelant que $S_\Sigma(V)$ est un monoïde qui agit à droite sur $T_\Sigma(V)$, de sorte que, en renommant toutes les substitutions obtenues, on ait bien :

$$t \cdot \sigma = t[x_1 := t_1][x_2 := t_2] \dots [x_n := t_n].$$

◇

On peut maintenant définir la notion de *relation de réduction associée à une famille R de règles de réécriture*. On pose $t \rightarrow_R t'$ s'il existe une règle (u, v) de R ainsi qu'un contexte C et une substitution σ tels que $t = C[u \cdot \sigma]$ et $t' = C[v \cdot \sigma]$.

Comme pour les présentations vues précédemment, on définit :

Définition. L'ARS associé à un système de réécriture de termes (Σ, R) est le couple $(T_\Sigma(V), \rightarrow_R)$. On définit les notions de *terminaison*, *confluence* et *convergence* d'un système de réécriture de termes à partir de celles de l'ARS associé. ◆

5.1.3 Ordres de réduction sur un ensemble de termes

Comme pour les autres systèmes de réécriture rencontrés, un moyen pratique de montrer la terminaison d'un système de réécriture de termes est d'exhiber un ordre de réduction qui contienne les règles.

Définition. Soit Σ une signature algébrique. Un *ordre de réduction* sur $T_\Sigma(V)$ est un ordre strict $>$ qui termine et qui est compatible avec la structure, c'est-à-dire qui vérifie, pour tout couple (t, u) de termes tels que $t > u$:

- $C[t] > C[u]$ pour tout contexte C ;
- $t \cdot \sigma > u \cdot \sigma$ pour toute substitution σ .



On a, comme précédemment, le résultat suivant :

Proposition 5.2. *Un système de réécriture de termes (Σ, R) termine si et seulement s'il existe un ordre de réduction $>$ sur $T_\Sigma(V)$ qui contient R .*

Il existe plusieurs façons de construire des ordres de réduction, notamment à partir d'un ordre strict donné sur $\text{Fl } \Sigma$. Nous allons détailler l'exemple de l'*ordre lexicographique des chemins* ou ordre *lpo*.

Supposons que l'on s'est donné un ordre strict $>$ sur $\text{Fl } \Sigma$. On définit la relation $>_{\text{lpo}}$ sur $T_\Sigma(V)$ en posant que $t >_{\text{lpo}} u$ si l'on est dans une des situations suivantes :

1. $u \in \mathcal{V}(t)$ et $t \notin V$;
2. $t = \varphi(t_1, \dots, t_n)$ et il existe $i \in \{1 \dots n\}$ tel que $t_i \geq_{\text{lpo}} u$;
3. $t = \varphi(t_1, \dots, t_m)$, $u = \psi(u_1, \dots, u_n)$ avec $\varphi > \psi$ et $t > u_i$ pour tout $i \in \{1 \dots n\}$;
4. $t = \varphi(t_1, \dots, t_n)$, $u = \varphi(u_1, \dots, u_n)$ et il existe un $i \in \{1 \dots n\}$ tel que :

$$\begin{cases} t_j = u_j & \text{pour } 1 \leq j \leq i-1 \\ t_i >_{\text{lpo}} u_i \\ t >_{\text{lpo}} u_j & \text{pour } i+1 \leq j \leq n \end{cases}$$

On a le résultat suivant, dont [BN98] contient une démonstration :

Proposition 5.3. *La relation $>_{\text{lpo}}$ ainsi construite à partir d'un ordre strict $>$ sur $\text{Fl } \Sigma$ est un ordre de réduction sur $T_\Sigma(V)$.*

5.2 Interprétation algébrique des termes

Nous allons, dans un premier temps, interpréter l'ensemble des termes comme l'algèbre libre sur Σ engendrée par V . Cela permettra de définir facilement bien que rigoureusement les notions de linéarité à gauche et de terme normalisé.

5.2.1 Algèbre sur une opérade

De la même façon que l'on définit des algèbres sur une opérade classique ou une opérade cartésienne, on peut introduire cette notion pour les opérades. Cette dernière définition englobe d'ailleurs les précédentes, puisque les opérades classiques et cartésiennes sont des cas particuliers d'opérades. Afin de définir ces algèbres, donnons un nouvel exemple d'opérades :

Exemple. Soit X un ensemble. En notant $\text{Oper } X(m, n)$ l'ensemble des applications de X^m dans X^n , on définit une opérade, dite des *opérations sur X* et notée $\text{Oper } X$. On ne se servira que de telles algèbres, mais on peut poser la même définition en remplaçant la catégorie des ensembles par une autre catégorie monoïdale comme, par exemple, la catégorie des espaces vectoriels sur un corps k .

Remarque. En fait, $\text{Oper } X$ est un peu plus qu'une opérade : c'est une opérade cartésienne. En effet, le produit cartésien de la catégorie $\mathbb{E}\text{NS}$ des ensembles fournit des opérations $\varepsilon : X \longrightarrow \{*\}$, $\delta : X \longrightarrow X^2$ et $\tau : X^2 \longrightarrow X^2$ définies par :

$$\varepsilon(x) = * \quad \delta(x) = (x, x) \quad \tau(x, y) = (y, x).$$

Ces opérations vérifient les relations qui font de $\text{Oper } X$ une opérade cartésienne. Nous les verrons plus loin.

Cette opérade $\text{Oper } X$ nous permet de donner une définition d'algèbre sur une opérade :

Définition. Soit \mathbb{C} une opérade. Une *algèbre sur \mathbb{C}* ou *\mathbb{C} -algèbre* est un couple (X, F) où X est un ensemble et $F : \mathbb{C} \longrightarrow \text{Oper } X$ est un morphisme d'opérades. Parfois, on omet le foncteur et on dit simplement que X est une \mathbb{C} -algèbre.

Si (X, F) et (Y, G) sont des \mathbb{C} -algèbres, un *morphisme de \mathbb{C} -algèbres de X vers Y* est une famille d'applications $(\alpha_n : X^n \longrightarrow Y^n)_{n \in \mathbb{N}}$ telles que, pour tout $\varphi \in \mathbb{C}(m, n)$, le diagramme

$$\begin{array}{ccc} X^m & \xrightarrow{F(\varphi)} & X^n \\ \alpha_m \downarrow & \text{\textcircled{C}} & \downarrow \alpha_n \\ Y^m & \xrightarrow{G(\varphi)} & Y^n \end{array}$$

commute. On note $\mathbb{C}\text{-ALG}$ la catégorie des \mathbb{C} -algèbres. ♦

En fait, il existe une caractérisation équivalente des \mathbb{C} -algèbres :

Proposition 5.4. *Il existe une équivalence de catégories entre les catégories $\mathbb{C}\text{-ALG}$ des \mathbb{C} -algèbres et $[\mathbb{C}, \mathbb{E}\text{NS}]_{\otimes}$ des foncteurs monoïdaux stricts de \mathbb{C} vers $\mathbb{E}\text{NS}$ - munie du produit cartésien.*

Démonstration. Soit (X, F) une \mathbb{C} -algèbre. On définit un foncteur monoïdal strict $F_X : \mathbb{C} \longrightarrow \mathbb{E}\text{NS}$ en posant $F_X(n) = X^n$ et $F_X(f) = F(f)$.

Réciproquement, si $G : \mathbb{C} \longrightarrow \mathbb{E}\text{NS}$ est un foncteur monoïdal strict, on lui associe la \mathbb{C} -algèbre $(G(1), F)$ où F est la restriction de G à la sous-catégorie pleine $\text{Oper } G(1)$ de $\mathbb{E}\text{NS}$.

On vérifie que cette correspondance est bijective. On remarque aussi que les morphismes de \mathbb{C} -algèbres et les transformations naturelles entre foncteurs monoïdaux stricts de \mathbb{C} dans \mathbf{Ens} sont en correspondance bijective. Enfin, la bijection

$$\mathbb{C}\text{-}\mathbf{ALG}(X, F; Y, G) \simeq [\mathbb{C}, \mathbf{ENS}]_{\otimes}(F_X, G_Y)$$

est fonctorielle en chacun de ses arguments. \diamond

À l'avenir, nous utiliserons celle des deux notions qui est la plus adaptée au cas traité.

Il existe une notion de \mathbb{C} -algèbre libre engendrée par un ensemble. Pour la donner, remarquons l'existence d'un foncteur oubli $\mathcal{U} : \mathbb{C}\text{-}\mathbf{ALG} \rightarrow \mathbf{ENS}$ qui associe à toute \mathbb{C} -algèbre son ensemble sous-jacent : $\mathcal{U}(X, F) = X$ ou $\mathcal{U}(X) = X(1)$ selon la forme choisie.

Définition. Soit X un ensemble. On appelle *\mathbb{C} -algèbre libre engendrée par X* tout couple (A, i) formé d'une \mathbb{C} -algèbre A et d'une application $i : X \rightarrow \mathcal{U}A = A(1)$ telles que :

pour toute \mathbb{C} -algèbre B et toute application $f : X \rightarrow B(1)$, il existe un unique morphisme $F : A \rightarrow B$ de \mathbb{C} -algèbres tel que le diagramme

$$\begin{array}{ccc} X & \xrightarrow{i} & A(1) \\ & \searrow f & \downarrow F(1) \\ & & B(1) \end{array} \quad \text{avec } \textcircled{\text{C}}$$

commute. \diamond

L'algèbre libre engendrée par un ensemble donné n'existe pas toujours. Cependant, dans le cas qui nous intéresse - celui d'une opérade libre engendrée par une signature algébrique -, l'algèbre libre existe et sa construction est particulièrement simple. Soient Σ une signature algébrique, \mathbb{C} l'opérade libre qu'elle engendre et X un ensemble. On définit l'ensemble sous-jacent à l'algèbre cherchée par :

$$\mathbb{C}X = \coprod_{n \in \mathbb{N}} \mathbb{C}(n, 1) \times X^n.$$

Un élément $(\varphi, x_1, \dots, x_n)$ dans la composante d'indice n du coproduit est noté :

$$\varphi(x_1, \dots, x_n).$$

Le foncteur, encore noté $\mathbb{C}X$, est alors défini par $\mathbb{C}X(n) = (\mathbb{C}X)^n$ et, si $\varphi \in \mathbb{C}(m, n)$:

$$\begin{aligned} \mathbb{C}X(\varphi) & \left((\varphi_1, x_{1,1}, \dots, x_{1,k_1}), \dots, (\varphi_m, x_{m,1}, \dots, x_{m,k_m}) \right) \\ &= (\varphi \circ (\varphi_1 \otimes \dots \otimes \varphi_m))(x_{1,1}, \dots, x_{m,k_m}). \end{aligned}$$

On note i l'application $X \longrightarrow \mathcal{U}\mathbb{C}X$ qui envoie chaque $x \in X$ sur $x = 1(x) = (1, x)$. On vérifie que :

Proposition 5.5. *Soient $\mathbb{C} = \mathcal{L}\Sigma$ avec Σ une signature algébrique et X un ensemble. Alors le couple $(\mathbb{C}X, i)$ est solution du problème de \mathbb{C} -algèbre libre engendrée par X .*

Démonstration. Par construction, $\mathbb{C}X$ est une \mathbb{C} -algèbre. Soient A une \mathbb{C} -algèbre et $f : X \longrightarrow \mathcal{U}A(1)$ une application. On définit $F : \mathbb{C}X \longrightarrow A$ par :

$$F(\varphi, x_1, \dots, x_n) = A(\varphi)(f(x_1), \dots, f(x_n)).$$

Ainsi défini, F est un morphisme de \mathbb{C} -algèbres. De plus, si $G : \mathbb{C}X \longrightarrow A$ est un morphisme, il vérifie :

$$G(\varphi, x_1, \dots, x_n) = A(\varphi)(G(x_1), \dots, G(x_n))$$

puisque $(\varphi, x_1, \dots, x_n) = \varphi(n, x_1, \dots, x_n)$. Ainsi, G est entièrement déterminé par ses valeurs sur les éléments de X , ce qui prouve que F est unique. \diamond

Pour la suite, ce que nous retiendrons de ce paragraphe est :

Corollaire 5.6. *Si Σ est une signature algébrique et X est un ensemble, alors tout élément a de $\mathcal{L}\Sigma X$ est de la forme $a = \varphi(x_1, \dots, x_n)$ avec $\varphi \in \mathcal{L}\Sigma(n, 1)$ et $x_1, \dots, x_n \in X$ déterminés de manière unique.*

5.2.2 L'ensemble des termes vu comme une algèbre

Revenons à la réécriture de termes ou, tout du moins, à la structure des termes. On a vu comment construire l'ensemble $T_\Sigma(V)$ des termes, pour Σ une signature algébrique et V un ensemble dénombrable. On peut aussi associer à Σ une opérade libre $\mathcal{L}\Sigma$. La notion d'algèbre permet de faire la jonction entre ces deux constructions; le résultat suivant est une conséquence directe du corollaire 5.6 :

Proposition 5.7. *L'ensemble $T_\Sigma(V)$ des termes est l'ensemble sous-jacent à la $\mathcal{L}\Sigma$ -algèbre libre engendrée par V .*

Démonstration. Il suffit en effet de vérifier que $T_\Sigma(V)$, muni des opérations suivantes, est solution du problème universel de $\mathcal{L}\Sigma$ -algèbre libre engendrée par V . Pour toute flèche $\varphi \in \Sigma(n, 1)$, on définit l'application :

$$\begin{aligned}\varphi_T : T_\Sigma(V)^n &\longrightarrow T_\Sigma(V) \\ (u_1, \dots, u_n) &\longmapsto \varphi(u_1, \dots, u_n).\end{aligned}$$

On étend ensuite cette définition à toutes les flèches de $\mathcal{L}\Sigma$ en utilisant leur décomposition en flèches de Σ . \diamond

Ainsi, l'ensemble des termes est isomorphe, à un unique isomorphisme près, à $\mathcal{L}\Sigma V$: comme précédemment, on commet l'abus minime de les identifier.

Corollaire 5.8. *Pour tout terme $t \in T_\Sigma(V)$, il existe un unique entier n , une unique flèche $t_\Sigma \in \mathcal{L}\Sigma(n, 1)$ et une unique famille $t_V = (x_1, \dots, x_n)$ de variables de V tels que $t = t_\Sigma(t_V)$.*

On a ainsi une décomposition bien utile des termes; cependant, ce n'est pas encore suffisant. On cherche maintenant à décomposer les éléments de V^n . Avant cela, donnons encore un peu de vocabulaire.

5.2.3 Règles linéaires à gauche et uniformisation

Nous avons déjà défini la notion de substitution sur l'ensemble $T_\Sigma(V)$ des termes associés à une signature algébrique et vu que l'ensemble $S_\Sigma(V)$ était en correspondance bijective avec l'ensemble des applications $V \longrightarrow T_\Sigma(V)$. Ainsi, on peut distinguer, parmi les substitutions :

Définition. Soit Σ une signature algébrique. Un *renommage* des termes de $T_\Sigma(V)$ est une substitution $\sigma \in S_\Sigma(V)$ qui, vue en tant qu'application $V \longrightarrow T_\Sigma(V)$, induit une bijection sur V . \blacklozenge

Autrement dit, l'ensemble des renommages de $T_\Sigma(V)$ est l'ensemble \mathfrak{S}_V des permutations de l'ensemble V . Les renommages possèdent la propriété suivante :

Lemme 5.9. *Soit Σ une signature algébrique et α une règle de réécriture sur $T_\Sigma(V)$. Alors, pour tout renommage $\rho \in \mathfrak{S}_V$ et tous termes $u, v \in T_\Sigma(V)$, on a $f \rightarrow_\alpha g$ si et seulement si $f \rightarrow_{\alpha \cdot \rho} g$, où ρ agit diagonalement sur α , c'est-à-dire par $\alpha \cdot \rho = (s(\alpha) \cdot \rho, t(\alpha) \cdot \rho)$.*

Démonstration. Supposons que $f \rightarrow_\alpha g$. Par définition, il existe un contexte C ainsi qu'une substitution σ tels que $f = C[s(\alpha) \cdot \sigma]$ et $g = C[t(\alpha) \cdot \sigma]$. Comme ρ est bijective, on a aussi :

$$\begin{aligned}f &= C[s(\alpha) \cdot (\rho \circ \rho^{-1} \circ \sigma)] \\ &= C[s(\alpha \cdot \rho) \cdot (\rho^{-1} \circ \sigma)].\end{aligned}$$

De même, $g = C[t(\alpha \cdot \rho) \cdot (\rho^{-1} \circ \sigma)]$ et donc $f \rightarrow_{\alpha \cdot \rho} g$. Réciproquement, si $f \rightarrow_{\alpha \cdot \rho} g$, alors il existe un contexte C ainsi qu'une substitution σ vérifiant $f = C[s(\alpha \cdot \rho) \cdot \sigma]$ et $g = C[t(\alpha \cdot \rho) \cdot \sigma]$. D'où $f = C[s(\alpha) \cdot (\rho \circ \sigma)]$, $g = C[t(\alpha) \cdot (\rho \circ \sigma)]$ et $f \rightarrow_{\alpha} g$. \diamond

Rappelons que l'ensemble V est supposé dénombrable, c'est-à-dire qu'il existe une bijection entre V et \mathbb{N} . On suppose désormais que l'on choisit systématiquement une telle bijection, ce qui revient à numéroter les variables x_1, x_2, x_3 , etc.

Comme nous venons de le voir dans le paragraphe précédent, le corollaire 5.8 nous dit que tout terme u admet une unique écriture $u = f(y_1, \dots, y_p)$ avec $f \in \mathcal{L}\Sigma(p, 1)$ et $y_1, \dots, y_p \in V$. En particulier, si α est une règle de réécriture sur $T_{\Sigma}(V)$, sa source admet une telle décomposition, ce qui nous conduit à :

Définition. Une règle de réécriture α sur $T_{\Sigma}(V)$ est dite *uniformisée* si sa source s'écrit $s(\alpha) = f(y_1, \dots, y_p)$ avec les y_i vérifiant la condition suivante : pour tout $i \in \{1 \dots p\}$, si $y_i = x_j$ alors $\{y_1, \dots, y_{i-1}\} = \{x_1, \dots, x_{j-1}\}$ ou $\{x_1, \dots, x_j\}$. On dit qu'un renommage ρ *uniformise* une règle α si $\alpha \cdot \rho$ est uniformisée. Un système de réécriture de termes (Σ, R) est dit *uniformisé* si toutes ses règles le sont. \blacklozenge

Proposition 5.10. *Toute règle de réécriture α sur $T_{\Sigma}(V)$ admet un renommage qui l'uniformise.*

Démonstration. Soit $f(y_1, \dots, y_p)$ la décomposition de $s(\alpha)$. On utilise l'algorithme suivant pour construire un renommage ρ : on commence par poser $\rho(y_1) = x_1$ et on initialise un compteur k à 1. Pour i variant de 2 à p , on teste si $y_i \in \{y_1, \dots, y_{i-1}\}$: si c'est le cas, on a déjà défini ρ sur y_i , sinon on pose $\rho(y_i) = x_{k+1}$ et on incrémente k de 1. Il suffit ensuite de compléter ρ en posant, par exemple, pour chaque x_k tel que $\rho(y_i) = x_k$, $\rho(x_k) = y_i$ et, pour tous les autres x_l , $\rho(x_l) = x_l$. Il est alors clair que l'on a bien défini un renommage ρ qui uniformise α . \diamond

Certaines règles de réécriture sont plus faciles à manipuler que d'autres, comme nous le verrons par la suite :

Définition. Une règle de réécriture α sur $T_{\Sigma}(V)$ est dite *linéaire à gauche* si sa source s'écrit $s(\alpha) = f(y_1, \dots, y_p)$ avec les y_i deux à deux distincts. Un système de réécriture de termes (Σ, R) est dit *linéaire à gauche* si toutes ses règles le sont. \blacklozenge

Proposition 5.11. *Une règle de réécriture α est à la fois linéaire à gauche et uniformisée si et seulement si sa source s'écrit $s(\alpha) = f(x_1, \dots, x_m)$. De plus, si α est linéaire à gauche et que ρ est un renommage qui uniformise α , alors $\alpha \cdot \rho$ est linéaire à gauche.*

En réunissant tous les résultats de ce paragraphe, on obtient :

Corollaire 5.12. *Pour tout système de réécriture (Σ, R) , il existe une famille R' de règles uniformisées sur $T_\Sigma(V)$, en correspondance bijective avec celles de R telles que $(R) = (R')$. De plus, si α est une règle de R linéaire à gauche, la règle α' qui lui correspond dans R' est linéaire à gauche ; par conséquent, si (Σ, R) est linéaire à gauche, alors (Σ, R') l'est aussi.*

Le but de la suite de ce chapitre est de prouver qu'étant donnée une signature algébrique Σ , l'ensemble des termes $T_\Sigma(V)$ est une partie des flèches de l'*opérade cartésienne libre engendrée par Σ* et que, si R est une famille de règles de réécriture linéaires à gauche sur T_Σ , on peut construire une présentation (Σ^c, R^c) qui simule complètement (Σ, R) .

5.3 Opérades cartésiennes et signatures algébriques

5.3.1 Opérades cartésiennes : définition et exemple fondamental

Soit \mathcal{C} une catégorie ; on note \mathcal{C}^2 le produit de deux copies de \mathcal{C} et $*$ la catégorie avec un seul objet et une seule flèche. Alors, on peut définir deux foncteurs $\delta_{\mathcal{C}} : \mathcal{C} \rightarrow \mathcal{C}^2$ et $\varepsilon_{\mathcal{C}} : \mathcal{C} \rightarrow \{*\}$ en posant $\delta_{\mathcal{C}}(x) = (x, x)$ et $\varepsilon_{\mathcal{C}}(x) = *$, l'unique élément de $*$.

Rappelons qu'une structure monoïdale stricte sur \mathcal{C} est la donnée de foncteurs $\otimes : \mathcal{C}^2 \rightarrow \mathcal{C}$ et $*$: $*$ $\rightarrow \mathcal{C}$ vérifiant des relations d'associativité et de neutralité, ainsi que nous l'avons vu au chapitre 3.

Si ces quatre foncteurs satisfont certaines propriétés supplémentaires :

Définition. Une catégorie monoïdale stricte $(\mathcal{C}, \otimes, *)$ est dite *cartésienne* si les deux conditions suivantes sont remplies :

1. le foncteur $\otimes : \mathcal{C}^2 \rightarrow \mathcal{C}$ est adjoint à droite du foncteur $\delta_{\mathcal{C}} : \mathcal{C} \rightarrow \mathcal{C}^2$;
2. le foncteur $*$: $*$ $\rightarrow \mathcal{C}$ est adjoint à droite du foncteur $\varepsilon_{\mathcal{C}} : \mathcal{C} \rightarrow *$.

Une opérade est dite *cartésienne* si elle l'est en tant que catégorie monoïdale stricte. \blacklozenge

Cette définition n'est cependant pas constructive ; pour remédier à ce défaut, nous avons, grâce aux travaux d'Albert Burroni, la caractérisation équationnelle suivante :

Théorème 5.13 ([Bur93]). *Une catégorie monoïdale stricte $(\mathcal{C}, \otimes, *)$ est cartésienne si et seulement si elle contient deux familles de flèches*

$$(\delta_x : x \rightarrow x \otimes x)_{x \in \text{Obj } \mathcal{C}} \quad \text{et} \quad (\varepsilon_x : x \rightarrow *)_{x \in \text{Obj } \mathcal{C}}$$

vérifiant les relations suivantes, pour tous objets x et y et toute flèche $f \in \mathcal{C}(x, y)$:

1. $\varepsilon_* = *$;

2. $(x \otimes \varepsilon_y \otimes \varepsilon_x \otimes y) \circ \delta_{x \otimes y} = x \otimes y$;
3. $\varepsilon_y \circ f = \varepsilon_x$;
4. $\delta_y \circ f = (f \otimes f) \circ \delta_x$.

Ainsi, plutôt que de caractériser la présence de produits cartésiens par des problèmes universels ou des adjonctions, on préfère vérifier la présence de certaines flèches satisfaisant certaines équations, ce qui, nous le verrons plus loin, est bien plus pratique pour construire des opérades cartésiennes libres. En attendant, dans le cas des opérades cartésiennes, on peut encore franchir un palier.

Corollaire 5.14. *Une opérade Γ -colorée $(\mathbb{C}, \otimes, *)$ est cartésienne si et seulement si elle contient trois familles de flèches :*

$$(\tau_{x,y} : x \otimes y \longrightarrow y \otimes x)_{x,y \in \Gamma}, \quad (\delta_x : x \longrightarrow x \otimes x)_{x \in \Gamma}, \quad (\varepsilon_x : x \longrightarrow *)_{x \in \Gamma},$$

satisfaisant les équations suivantes, pour tous x, y et z éléments de Γ et toute flèche $f \in \mathcal{C}(x, y)$:

- 1_x. $(x \otimes \delta_x) \circ \delta_x = (\delta_x \otimes x) \circ \delta_x$;
- 2_x. $(\varepsilon_x \otimes x) \circ \delta_x = x$;
- 4_x. $\tau_x \circ \delta_x = \delta_x$;
- 5_{xy}. $\tau_{y,x} \circ \tau_{x,y} = x \otimes y$;
- 6_{xyz}. $(z \otimes \tau_{x,y}) \circ (\tau_{x,z} \otimes y) \circ (x \otimes \tau_{y,z}) = (\tau_{y,z} \otimes x) \circ (y \otimes \tau_{x,z}) \circ (\tau_{x,y} \otimes z)$;
- 7_{xy}. $(y \otimes \delta_x) \circ \tau_{x,y} = (\tau_{x,y} \otimes x) \circ (x \otimes \tau_{x,y}) \circ (\delta_x \otimes y)$;
- 9_{xy}. $(y \otimes \varepsilon_x) \circ \tau_{x,y} = \varepsilon_x \otimes y$;
- $f\varepsilon$. $\varepsilon_y \circ f = \varepsilon_x$;
- $f\delta$. $\delta_y \circ f = (f \otimes f) \circ \delta_x$;
- $f\tau 1_z$. $\tau_{y,z} \circ (f \otimes z) = (z \otimes f) \circ \tau_{x,z}$.

Ainsi, dans le cas d'une opérade, les familles de flèches ne sont plus indexées par tous les objets mais seulement par les couleurs. Alors, si Γ est fini de cardinal n , on aura $n^2 + 2n$ flèches pour la structure ; la numérotation des relations laisse la place pour des relations complémentaires que nous définirons plus loin.

Lorsque Γ est réduit à un élément, c'est-à-dire dans le cas des opérades monochromes, le critère se simplifie encore en :

Corollaire 5.15. *Une opérade monochrome \mathbb{C} est cartésienne si et seulement si elle contient trois flèches*

$$\tau : 2 \longrightarrow 2, \quad \delta : 1 \longrightarrow 2, \quad \varepsilon : 1 \longrightarrow 0$$

qui vérifient les équations suivantes :

1. $(1 \otimes \delta) \circ \delta = (\delta \otimes 1) \circ \delta ;$
2. $(\varepsilon \otimes 1) \circ \delta = 1 ;$
4. $\tau \circ \delta = \delta ;$
5. $\tau \circ \tau = 2 ;$
6. $(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) = (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) ;$
7. $(1 \otimes \delta) \circ \tau = (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) ;$
9. $(1 \otimes \varepsilon) \circ \tau = \varepsilon \otimes 1 ;$

ainsi que, pour tout $n \in \mathbb{N}$ et toute flèche $f \in \mathbb{C}(n, 1) :$

$$f\delta. \delta \circ f = (f \otimes f) \circ \delta_n ;$$

$$f\varepsilon. \varepsilon \circ f = \varepsilon^n ;$$

$$f\tau 1. \tau \circ (f \otimes 1) = (1 \otimes f) \circ \tau_{n,1}.$$

On a utilisé les notations suivantes :

- $\rho_n : 2n \longrightarrow 2n$ est la flèche définie par récurrence sur n par $\rho_0 = 0$, puis par :

$$\rho_{n+1} = (1 \otimes \rho_n \otimes 1) \circ (1 \otimes \tau^n \otimes 1) ;$$

- $\delta_n : n \longrightarrow 2n$ est donnée par $\rho_n \circ \delta^n ;$

- pour $\tau_{n,1} : n+1 \longrightarrow n+1$ et $\tau_{1,n} : n+1 \longrightarrow n+1$, on procède de nouveau par récurrence sur $n : \tau_{0,1} = \tau_{1,0} = 1$ puis

$$\begin{cases} \tau_{n+1,1} = (\tau \otimes n) \circ (1 \otimes \tau_{n,1}) \\ \tau_{1,n+1} = (n \otimes \tau) \circ (\tau_{1,n} \otimes 1) \end{cases}$$

On trouvera, dans l'annexe A, plus de détails sur tous ces résultats.

Examinons à présent l'exemple fondamental d'opérade monochrome cartésienne : la catégorie \mathbb{F}° . Le moyen le plus simple de la définir, en tant que catégorie, est de dire que \mathbb{F} est la sous-catégorie pleine de \mathbb{E}^{NS} dont les objets sont les ensembles $[n] = \{1 \dots n\}$, pour tout $n \in \mathbb{N}$, avec la convention $[0] = \emptyset$. Alors :

Proposition 5.16. *La catégorie \mathbb{F}° est une opérade cartésienne.*

Démonstration. Montrons, pour commencer, que \mathbb{F}° est une opérade. On note que ses objets sont (indexés par) les entiers naturels et on pose $[n] \otimes [m] = [n+m]$. Définissons le produit sur les flèches ; par commodité, on travaille sur les flèches de \mathbb{F} : si $f : m \longrightarrow n$ est une flèche de \mathbb{F}° , on note $f^* : n \longrightarrow m$ la flèche de \mathbb{F} qui lui correspond et, réciproquement, si $f : m \longrightarrow n$ est une flèche de \mathbb{F} , on note $f^* : n \longrightarrow m$ la flèche de \mathbb{F}° qui lui correspond.

Soient $f : m \longrightarrow n$ et $g : p \longrightarrow q$ deux flèches de \mathbb{F}° . Alors, leur produit $f \otimes g : m + p \longrightarrow n + q$ est donné par $(f^* \otimes g^*)^*$, où $f^* \otimes g^* : n + q \longrightarrow m + p$ est la flèche de \mathbb{F} définie par :

$$f^* \otimes g^*(i) = \begin{cases} f^*(i) & \text{si } i \in [n] \\ g^*(i - n) + m & \text{si } (i - n) \in [q] \end{cases}$$

On vérifie que \otimes admet 0 comme unité à gauche et à droite et satisfait la relation d'échange :

$$(t(f) \otimes g) \circ (f \otimes s(g)) = (f \otimes t(g)) \circ (s(f) \otimes g) = f \otimes g$$

pour toutes flèches f et g de \mathbb{F}° . Ainsi, \mathbb{F}° est une opérade monochrome (et \mathbb{F} aussi).

Vérifions à présent que \mathbb{F}° contient bien les trois flèches τ , δ et ε et que celles-ci satisfont aux relations de 5.15. On note $\tau^* : [2] \longrightarrow [2]$ l'application qui envoie 1 sur 2 et 2 sur 1, $\delta^* : [2] \longrightarrow [1]$ celle qui envoie 1 et 2 sur 1, $\varepsilon^* : [0] \longrightarrow [1]$ l'unique application de \emptyset vers $\{1\}$.

À présent, vérifions les relations (ou plutôt les relations duales, obtenues en remplaçant les flèches par leurs versions étoilées et en renversant le sens des compositions). Pour plus de commodité, on note $f^* : m \longrightarrow n$ sous la forme du m -uplet $(f^*(1), \dots, f^*(m))$ d'éléments de $[n]$. Ainsi, si $f^* : m \longrightarrow n$ et $g^* : n \longrightarrow p$:

$$g^* \circ f^* = g^* \circ (f^*(1), \dots, f^*(m)) = (g^* \circ f^*(1), \dots, g^* \circ f^*(m)),$$

et, si $f^* : m \longrightarrow n$ et $g^* : p \longrightarrow q$:

$$f^* \otimes g^* = (f^*(1), \dots, f^*(m), g^*(1) + n, \dots, g^*(p) + n).$$

Alors :

1. Détaillons, pour cette première relation :

$$\begin{aligned} \delta^* \circ (1 \otimes \delta^*) &= \delta^* \circ (1, \delta^*(1) + 1, \delta^*(2) + 1) \\ &= \delta^* \circ (1, 2, 2) \\ &= (1, 1, 1). \end{aligned}$$

D'autre part :

$$\begin{aligned} \delta^* \circ (\delta^* \otimes 1) &= \delta^* \circ (\delta^*(1), \delta^*(2), 1 + 1) \\ &= \delta^* \circ (1, 1, 2) \\ &= (1, 1, 1). \end{aligned}$$

$$2. \delta^* \circ (\varepsilon^* \otimes 1) = \delta^* \circ (2) = (1) = 1.$$

$$4. \delta^* \circ \tau^* = \delta^* \circ (2, 1) = (1, 1) = \delta^*.$$

$$5. \tau^* \circ \tau^* = \tau^* \circ (2, 1) = (1, 2) = 2.$$

6. On a :

$$\begin{aligned} (1 \otimes \tau^*) \circ (\tau^* \otimes 1) \circ (1 \otimes \tau^*) &= (1 \otimes \tau^*) \circ (\tau^* \otimes 1) \circ (1, 3, 2) \\ &= (1 \otimes \tau^*) \circ (2, 3, 1) \\ &= (3, 2, 1). \end{aligned}$$

Et :

$$\begin{aligned} (\tau^* \otimes 1) \circ (1 \otimes \tau^*) \circ (\tau^* \otimes 1) &= (\tau^* \otimes 1) \circ (1 \otimes \tau^*) \circ (2, 1, 3) \\ &= (\tau^* \otimes 1) \circ (3, 1, 2) \\ &= (3, 2, 1). \end{aligned}$$

7. On a :

$$\begin{aligned} \tau^* \circ (1 \otimes \delta^*) &= \tau^* \circ (1, 2, 2) \\ &= (2, 1, 1). \end{aligned}$$

Et :

$$\begin{aligned} (\delta^* \otimes 1) \circ (1 \otimes \tau^*) \circ (\tau^* \otimes 1) &= (\delta^* \otimes 1) \circ (1 \otimes \tau^*) \circ (2, 1, 3) \\ &= (\delta^* \otimes 1) \circ (3, 1, 2) \\ &= (2, 1, 1) \end{aligned}$$

$$9. \tau^* \circ (1 \otimes \varepsilon^*) = \tau^* \circ (1) = (2) = \varepsilon^* \otimes 1.$$

$f\delta$. Soient $n \in \mathbb{N}$ et $f \in \mathbb{C}(n, 1)$. Alors :

$$\begin{aligned} f^* \circ \delta^* &= f^* \circ (1, 1) \\ &= (f^*(1), f^*(1)). \end{aligned}$$

Et :

$$\begin{aligned} \delta_n^* \circ (f^* \otimes f^*) &= \delta_n^* \circ (f^*(1), f^*(1) + n) \\ &= (f^*(1), f^*(1)). \end{aligned}$$

On utilise la relation $\delta^n = (1, \dots, n, 1, \dots, n)$ que l'on démontre en rappelant que $\delta_n^* = (\delta^n)^* \circ \rho_n^*$ et en vérifiant, par récurrence sur n , que :

$$\rho_n^* = (1, n+1, 2, n+2, \dots, n, 2n).$$

$f\varepsilon$. Soient $n \in \mathbb{N}$ et $f \in \mathbb{C}(n, 1)$. Alors $f^* \circ \varepsilon^*$ et $(\varepsilon^n)^*$ sont deux applications de $[0] = \emptyset$ vers $[n]$, or il n'existe qu'une telle application, donc $f^* \circ \varepsilon^* = (\varepsilon^n)^*$.

$f\tau 1$. Soient $n \in \mathbb{N}$ et $f \in \mathbb{C}(n, 1)$.

$$\begin{aligned} (f^* \otimes 1) \circ \tau^* &= (f^* \otimes 1) \circ (2, 1) \\ &= (n+1, f^*(1)). \end{aligned}$$

Et :

$$\begin{aligned} \tau_{n,1}^* \circ (1 \otimes f^*) &= \tau_{n,1}^* \circ (1, f^*(1) + 1) \\ &= (n+1, f^*(1)). \end{aligned}$$

En utilisant $\tau_{n,1}^* = (n+1, 1, 2, \dots, n)$ que l'on démontre par récurrence sur n .

◇

Remarque. En fait, on a démontré que \mathbb{F} est une opérade cocartésienne, ce qui se définit en dualisant : les adjoints à droite deviennent des adjoints à gauche, les flèches et les relations sont renversées.

On va à présent montrer que cette opérade cartésienne \mathbb{F}° possède une propriété particulière relativement aux autres opérades cartésiennes ; mais avant cela :

Notation. On note Δ la signature comprenant trois flèches :

$$0 \xleftarrow{\varepsilon} 1 \xrightarrow{\delta} 2 \bigcirc_{\tau}$$

On note E_Δ la signature composée des relations 1, 2, 4, 5, 6, 7, 9. On peut représenter ces flèches et ces relations de manière graphique comme dans les figures 5.1 et 5.2.

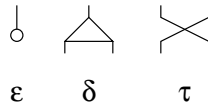
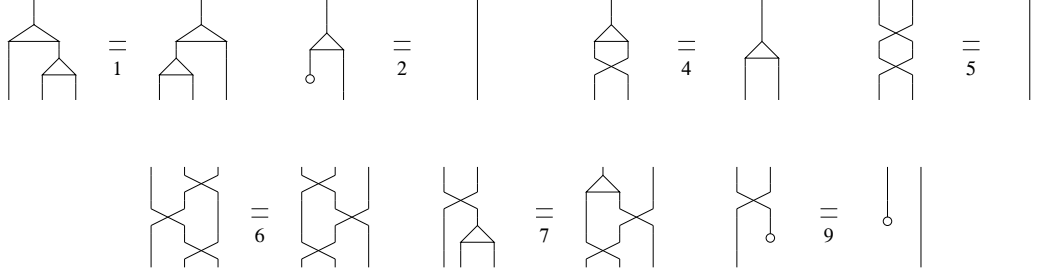


FIG. 5.1 – La signature Δ .

Rappelons le résultat suivant, dont la formulation duale est due à Albert Burroni :

Proposition 5.17 ([Bur93]). *L'opérade \mathbb{F}° admet la présentation (Δ, E_Δ) .*

On trouvera deux preuves différentes, l'une dans [Bur93], l'autre dans [Laf95]. L'idée générale est de montrer que toute flèche de \mathbb{F}° se décompose en produits et composées des trois flèches τ , δ et ε puis que deux telles décompositions d'une même flèche sont égales modulo E_Δ .


 FIG. 5.2 – Les relations de E_Δ .

Définition. Soient \mathbb{C} et \mathbb{D} deux opérades cartésiennes (monochromes). Un *morphisme d'opérades cartésiennes* de \mathbb{C} vers \mathbb{D} est un morphisme d'opérades $F : \mathbb{C} \longrightarrow \mathbb{D}$ qui préserve les produits cartésiens, c'est-à-dire qui envoie les trois flèches τ , δ et ε de \mathbb{C} sur leurs homologues de \mathbb{D} . Les opérades cartésiennes et leurs morphismes s'organisent en une sous-catégorie \mathbb{OP}^\times de \mathbb{OP} . \blacklozenge

En vertu de ce qui précède, on a :

Proposition 5.18. *La catégorie \mathbb{F}° est l'opérade cartésienne initiale. Autrement dit : pour toute opérade cartésienne \mathbb{C} , il existe un unique morphisme d'opérades cartésiennes de \mathbb{F}° dans \mathbb{C} .*

5.3.2 Opérade cartésienne libre engendrée par une signature algébrique

Rappelons qu'une *signature algébrique* est une signature dont toutes les flèches sont de but 1. On note $\mathbb{S}_{\mathbb{GN}}^\times$ la sous-catégorie pleine de $\mathbb{S}_{\mathbb{GN}}$ dont les objets sont les signatures algébriques. En remarquant qu'il existe un foncteur oubli \mathcal{U} de la catégorie des opérades cartésiennes vers les signatures algébriques, défini en ne considérant que les flèches de but 1 et en oubliant la structure, on définit :

Définition. Soit Σ une signature algébrique. On appelle *opérade cartésienne libre engendrée par Σ* tout couple (\mathbb{C}, i) où \mathbb{C} est une opérade cartésienne et $i : \Sigma \longrightarrow \mathcal{U}\mathbb{C}$ est un morphisme de signatures vérifiant :

pour toute opérade cartésienne \mathbb{D} et tout morphisme de signatures F de Σ dans $\mathcal{U}\mathbb{D}$, il existe un unique morphisme d'opérades cartésiennes $\bar{F} : \mathbb{C} \longrightarrow \mathbb{D}$ qui fait commuter le diagramme

$$\begin{array}{ccc} \Sigma & \xrightarrow{i} & \mathcal{U}\mathbb{C} \\ & \searrow F & \downarrow \bar{F} \\ & & \mathcal{U}\mathbb{D}. \end{array}$$

\blacklozenge

Nous allons voir comment construire un tel objet. Soit Σ une signature algébrique ; on note Σ^c la signature obtenue comme coproduit de Σ et de la signature Δ . Puis on pose $E_{\Sigma/\Delta}$ la signature formée des relations suivantes, données pour chaque $\varphi \in \Sigma(n, 1)$:

$$\varphi\varepsilon. \varepsilon \circ \varphi = \varepsilon^n ;$$

$$\varphi\delta. \delta \circ \varphi = (\varphi \otimes \varphi) \circ \delta_n ;$$

$$\varphi\tau 1. \tau \circ (\varphi \otimes 1) = (1 \otimes \varphi) \circ \tau_{n,1}.$$

On peut aussi utiliser des représentations graphiques, comme dans les figures 5.3, 5.4 et 5.5. Enfin, on pose $E_{\Delta,\Sigma}$ la réunion de E_{Δ} et de $E_{\Sigma/\Delta}$.

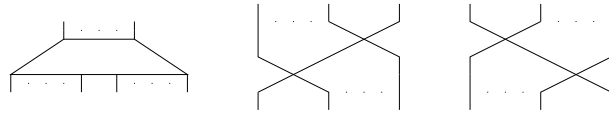


FIG. 5.3 – Les flèches δ_n , $\tau_{n,1}$ et $\tau_{1,n}$ de $\mathcal{L}\Delta$.

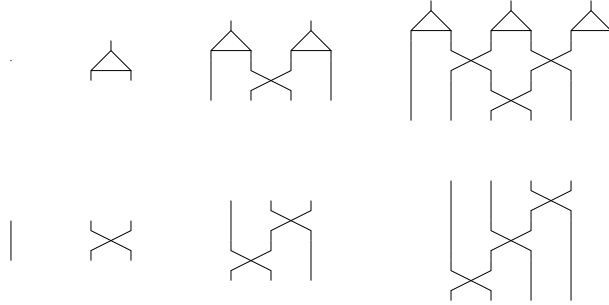


FIG. 5.4 – De gauche à droite et de haut en bas, diagrammes représentant : δ_0 à δ_3 et $\tau_{0,1}$ à $\tau_{3,1}$.

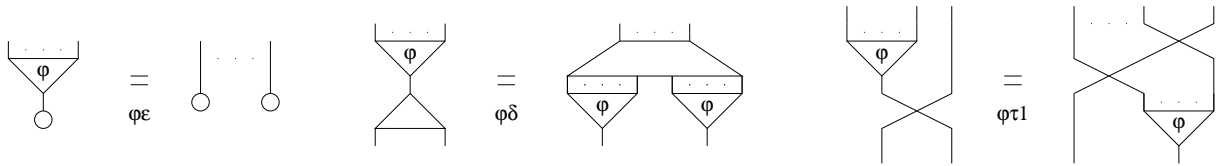


FIG. 5.5 – Les relations $\varphi\varepsilon$, $\varphi\delta$ et $\varphi\tau 1$ de $E_{\Sigma/\Delta}$ pour un $\varphi \in \Sigma(n, 1)$.

Alors, on vérifie que :

Proposition 5.19. *L'opérade quotient $\mathcal{L}\Sigma^c/E_{\Delta,\Sigma}$ est solution du problème d'opérade cartésienne libre engendrée par Σ .*

Démonstration. La première étape est de vérifier que $\mathcal{L}\Sigma^c/E_{\Delta,\Sigma}$ est une opérade cartésienne. D'après 5.15, il suffit de vérifier que $\mathcal{L}\Sigma^c/E_{\Delta,\Sigma}$ contient trois flèches τ , δ et ε (ce qui est le cas puisque Σ^c contient Δ) qui vérifient les relations de E_{Δ} (ce qui est le cas puisque $E_{\Delta,\Sigma}$ contient E_{Δ}) ainsi que les trois (familles de) relations, indexées par $n \in \mathbb{N}$ et $f \in \mathcal{L}\Sigma^c(n, 1)$:

$$f\delta. \delta \circ f = (f \otimes f) \circ \delta_n;$$

$$f\varepsilon. \varepsilon \circ f = \varepsilon^n;$$

$$f\tau 1. \tau \circ (f \otimes 1) = (1 \otimes f) \circ \tau_{n,1}.$$

On sait déjà que ces relations sont vraies pour les flèches de Σ . On en déduit, par récurrence sur la taille des flèches de $\mathcal{L}\Sigma$, qu'elles sont aussi vraies pour toute flèche de $\mathcal{L}\Sigma$. Ainsi, on sait que toute flèche $f \in (\mathcal{L}\Sigma^c/E_{\Delta,\Sigma})(m, 1)$ se factorise en :

$$f = f_{\Sigma} \circ f_{\Delta}$$

avec $f_{\Sigma} \in \mathcal{L}\Sigma^c(n, 1)$ et $f_{\Delta} \in \mathbb{F}^o(m, n)$. Il ne reste donc plus qu'à vérifier que, pour toute flèche $f \in \mathbb{F}^o(m, n)$, on a :

$$\begin{cases} \delta_n \circ f = (f \otimes f) \circ \delta_m \\ \varepsilon^n \circ f = \varepsilon^m \\ \tau_{n,1} \circ (f \otimes 1) = (1 \otimes f) \circ \tau_{m,1} \end{cases}$$

Cela provient du fait que \mathbb{F}^o est cartésienne. Pour s'en convaincre :

$f\delta$. En reprenant les notations déjà utilisées pour les flèches de \mathbb{F} :

$$\begin{aligned} f^* \circ \delta_n^* &= f^* \circ (1, \dots, n, 1, \dots, n) \\ &= (f^*(1), \dots, f^*(n), f^*(1), \dots, f^*(n)). \end{aligned}$$

Et :

$$\begin{aligned} \delta_m^* \circ (f^* \otimes f^*) &= \delta_m^* \circ (f^*(1), \dots, f^*(n), f^*(1) + m, \dots, f^*(n) + m) \\ &= (f^*(1), \dots, f^*(n), f^*(1), \dots, f^*(n)). \end{aligned}$$

$f\varepsilon$. Les applications $f^* \circ (\varepsilon^n)^*$ et $(\varepsilon^m)^*$ sont forcément égales puisqu'il n'existe qu'une seule application de $[0] = \emptyset$ vers $[m]$.

$f\tau 1$. On a :

$$\begin{aligned}(f^* \otimes 1) \circ \tau_{n,1}^* &= (f^* \otimes 1) \circ (n+1, 1, \dots, n) \\ &= (m+1, f^*(1), \dots, f^*(n)).\end{aligned}$$

Et :

$$\begin{aligned}\tau_{m,1}^* \circ (1 \otimes f^*) &= \tau_{m,1}^* \circ (1, f^*(1) + 1, \dots, f^*(n) + 1) \\ &= (m+1, f^*(1), \dots, f^*(n)).\end{aligned}$$

Supposons à présent que \mathbb{C} est une opérade cartésienne et que $F : \Sigma \longrightarrow \mathcal{UC}$ est un morphisme de signatures : on veut prouver qu'il existe un unique morphisme d'opérades cartésiennes $\bar{F} : \mathcal{L}\Sigma^c/E_{\Delta,\Sigma} \longrightarrow \mathbb{C}$ tel que $F = \mathcal{U}\bar{F} \circ i$ où i est l'injection évidente de Σ dans $\mathcal{L}\Sigma^c/E_{\Delta,\Sigma}$.

Comme \mathbb{C} est cartésienne, elle contient Δ et ses flèches satisfont, en particulier, les relations de $E_{\Delta,\Sigma}$. On définit donc \bar{F} en donnant ses valeurs sur les flèches de Σ^c : $\bar{F}(\tau) = \tau$, $\bar{F}(\delta) = \delta$, $\bar{F}(\varepsilon) = \varepsilon$ et, pour toute flèche φ de Σ , $\bar{F}(\varphi) = F(\varphi)$.

Le foncteur induit sur $\mathcal{L}\Sigma^c$ passe bien au quotient par $E_{\Delta,\Sigma}$ puisque \mathbb{C} est cartésienne et c'est bien un morphisme d'opérades cartésiennes puisqu'il envoie Δ sur Δ .

De plus, il factorise F via $\mathcal{L}\Sigma^c/E_{\Delta,\Sigma}$ et il est l'unique morphisme à le faire puisqu'il est entièrement déterminé par ses valeurs sur les flèches de Σ .

◇

5.3.3 Une présentation convergente de l'opérade cartésienne libre

On remarque assez facilement que la présentation $(\Sigma^c, E_{\Delta,\Sigma})$ n'est pas confluente. On complète alors les relations E_{Δ} en R_{Δ} et $E_{\Sigma/\Delta}$ en $R_{\Sigma/\Delta}$, afin d'obtenir une nouvelle présentation $(\Sigma^c, R_{\Delta,\Sigma})$. Ainsi, E_{Δ} est remplacé par R_{Δ} :

1. $(1 \otimes \delta) \circ \delta \rightarrow (\delta \otimes 1) \circ \delta$;
2. $(\varepsilon \otimes 1) \circ \delta \rightarrow 1$;
3. $(1 \otimes \varepsilon) \circ \delta \rightarrow 1$;
4. $\tau \circ \delta \rightarrow \delta$;
5. $\tau \circ \tau \rightarrow 2$;
6. $(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \rightarrow (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1)$;
7. $(1 \otimes \delta) \circ \tau \rightarrow (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1)$;
8. $(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \rightarrow (\delta \otimes 1) \circ \tau$;

9. $(1 \otimes \varepsilon) \circ \tau \rightarrow \varepsilon \otimes 1$;
10. $(\varepsilon \otimes 1) \circ \tau \rightarrow 1 \otimes \varepsilon$;
11. $(1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \rightarrow (\delta \otimes 1) \circ \delta$;
12. $(1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \rightarrow (\tau \otimes 1) \circ (1 \otimes \delta)$.

Et $R_{\Sigma/\Delta}$ remplace $E_{\Sigma/\Delta}$, comprenant quatre règles pour chaque $\varphi \in \Sigma(n, 1)$:

- $\varphi\varepsilon$. $\varepsilon \circ \varphi \rightarrow \varepsilon^n$;
- $\varphi\delta$. $\delta \circ \varphi \rightarrow (\varphi \otimes \varphi) \circ \delta_n$;
- $\varphi\tau 1$. $\tau \circ (\varphi \otimes 1) \rightarrow (1 \otimes \varphi) \circ \tau_{n,1}$;
- $\varphi\tau 2$. $\tau \circ (1 \otimes \varphi) \rightarrow (\varphi \otimes 1) \circ \tau_{1,n}$.

Les figures 5.6 et 5.7 montrent ces nouvelles relations représentées graphiquement.

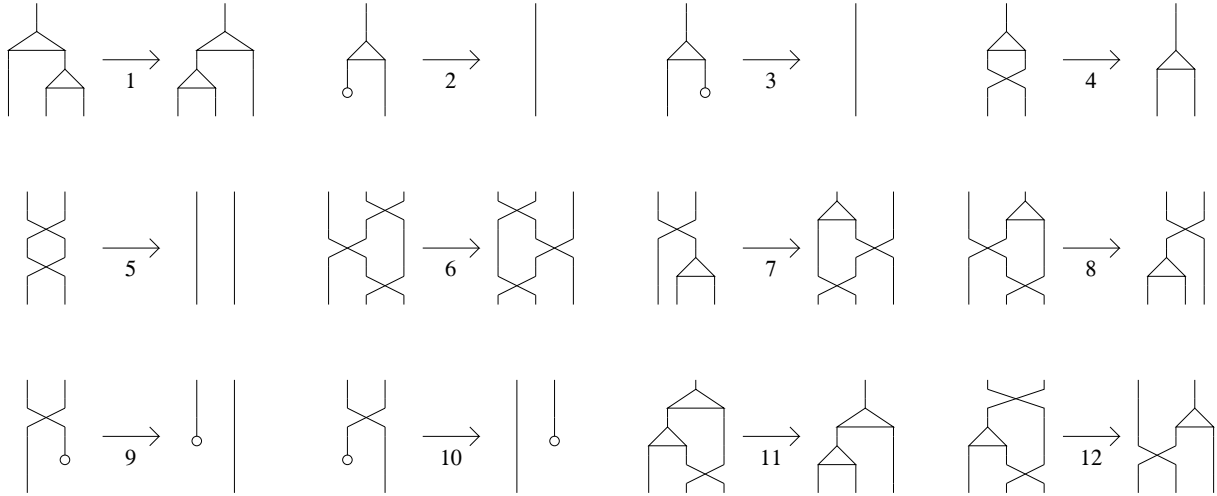


FIG. 5.6 – Les douze règles de R_{Δ} .

Enfin, on pose $R_{\Delta, \Sigma}$ la réunion de R_{Δ} et de $R_{\Sigma/\Delta}$. On vérifie que :

Lemme 5.20. *Le couple $(\Sigma^c, R_{\Delta, \Sigma})$ est une présentation de l'opérade $\mathcal{L}\Sigma^c/E_{\Delta, \Sigma}$.*

Démonstration. Il suffit de s'assurer que les relations $\equiv_{R_{\Delta, \Sigma}}$ et $\equiv_{E_{\Delta, \Sigma}}$. Comme on a les inclusions $E_{\Delta} \subseteq R_{\Delta}$ et $E_{\Sigma/\Delta} \subseteq R_{\Sigma/\Delta}$, il suffit de vérifier que les règles que l'on a rajoutées sont dérivables à partir des relations de départ.

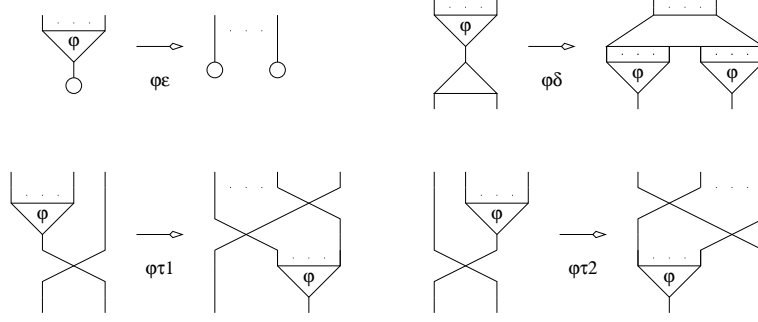


FIG. 5.7 – Les quatre familles de règles de $R_{\Sigma/\Delta}$.

Pour 3 :

$$\begin{aligned} (1 \otimes \varepsilon) \circ \delta &\leftarrow_4 (1 \otimes \varepsilon) \circ \tau \circ \delta \\ &\rightarrow_9 (\varepsilon \otimes 1) \circ \delta \\ &\rightarrow_2 1. \end{aligned}$$

Pour 8 :

$$\begin{aligned} (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) &\leftarrow_5 (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \circ \tau \circ \tau \\ &\rightarrow_7 (1 \otimes \tau) \circ (\tau \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\ &\rightarrow_5 (1 \otimes \tau) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\ &\rightarrow_5 (\delta \otimes 1) \circ \tau. \end{aligned}$$

Pour 10 :

$$\begin{aligned} (\varepsilon \otimes 1) \circ \tau &\leftarrow_9 (1 \otimes \varepsilon) \circ \tau \circ \tau \\ &\rightarrow_5 1 \otimes \varepsilon. \end{aligned}$$

Pour 11 :

$$\begin{aligned} (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta &\leftarrow_1 (1 \otimes \tau) \circ (1 \otimes \delta) \circ \delta \\ &\rightarrow_4 (1 \otimes \delta) \circ \delta \\ &\rightarrow_1 (\delta \otimes 1) \circ \delta. \end{aligned}$$

Pour 12 :

$$\begin{aligned} (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau &\leftarrow_5 (\tau \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\ &\leftarrow_7 (\tau \otimes 1) \circ (1 \otimes \delta) \circ \tau \circ \tau \\ &\rightarrow_5 (\tau \otimes 1) \circ (1 \otimes \delta). \end{aligned}$$

Enfin, pour $\varphi\tau 2$, après avoir remarqué que, pour tout n , $\tau_{n,1} \circ \tau_{1,n} \rightarrow_s 1 \otimes n$:

$$\begin{aligned} \tau \circ (1 \otimes \varphi) &\leftarrow_s \tau \circ (1 \otimes \varphi) \circ \tau_{n,1} \circ \tau_{1,n} \\ &\leftarrow_{\varphi\tau 1} \tau \circ \tau \circ (\varphi \otimes 1) \circ \tau_{1,n} \\ &\rightarrow_s (\varphi \otimes 1) \circ \tau_{1,n}. \end{aligned}$$

◇

Le reste du paragraphe a pour finalité de prouver que $(\Sigma^c, R_{\Delta, \Sigma})$ est une présentation convergente.

5.3.4 Terminaison de $(\Sigma^c, R_{\Delta, \Sigma})$

Nous allons utiliser la technique décrite en 3.7. Cela va consister, ici, en la construction d'un morphisme d'opérades F de $\mathcal{L}\Sigma^c$ dans $\mathcal{O}(\mathbb{N}^*, \mathbb{N}^*, [\mathbb{N}^*])$, noté $\mathcal{O}(\mathbb{N})$, tel que, pour toute règle α de $R_{\Delta, \Sigma}$, on ait $F(s(\alpha)) > F(t(\alpha))$. En fait, il y a deux étapes : dans un premier temps, on montre que la terminaison de $R_{\Delta, \Sigma}$ est équivalente à celle de $\{6\}$; puis, on vérifie que $\{6\}$ termine.

Remarque. Au vu des règles de $R_{\Delta, \Sigma}$, on constate que celles de R_{Δ} agissent en « déplaçant » des flèches ε , δ et τ de la gauche vers la droite. En revanche, les règles de $R_{\Sigma/\Delta}$ déplacent les flèches de Σ vers le bas et celles de Δ vers le haut.

Il n'est donc pas très surprenant que la technique d'interprétation, qui utilise fortement le fait que ce type de « déplacement » se fait toujours dans la même direction, peine à montrer en une fois la terminaison de $R_{\Delta, \Sigma}$ tout entier.

Si nous avons choisi, ici, de réduire au maximum le nombre de règles restant à la fin de la première interprétation, notons, cependant, qu'il est tout à fait possible qu'une interprétation mieux pensée fonctionne en une fois.

Enfin, disons qu'il aurait certainement été possible et, peut-être, plus simple, de montrer dans un premier temps, que la terminaison de $R_{\Delta, \Sigma}$ est équivalente à celle de R_{Δ} , puis de montrer que cette dernière termine, grâce à une nouvelle interprétation inspirée de celle utilisée dans [Laf03].

On définit un premier morphisme d'opérades F en donnant ses valeurs sur les flèches de Σ^c :

- $\varepsilon_*(i) = *$, $\varepsilon^*(*) = 1$ et $[\varepsilon](i) = 0$;
- $\delta_*(i) = (i, i)$, $\delta^*(i, j) = i + j + 1$ et $[\delta](i, j, k) = \underline{i} + \underline{k}$;
- $\tau_*(i, j) = (j, i)$, $\tau^*(i, j) = (j, i)$ et $[\tau](i, j, k, l) = ij.\underline{l} + l.\underline{(i + j)}$;
- $\gamma_*(*) = 1$, $\gamma^*(i) = *$ et $[\gamma](i) = \underline{i}$ pour toute constante $\gamma \in \Sigma(0, 1)$;
- $\varphi_*(i_1, \dots, i_n) = i_1 + \dots + i_n + 1$, $\varphi^*(i) = (i, \dots, i)$ et $[\varphi](i_1, \dots, i_n, j) = \underline{j}$ pour tout opérateur non constant $\varphi \in \Sigma(n, 1)$, $n \geq 1$.

Afin d'être sûr que ces données s'étendent bien en un morphisme d'opérades F de $\mathcal{L}\Sigma^c$ vers $\mathcal{O}(\mathbb{N})$, la seule chose à vérifier est que chaque générateur est bien envoyé sur des applications croissantes, ce qui ne pose aucun problème. Alors :

Proposition 5.21. *Le morphisme d'opérades $F : \mathcal{L}\Sigma^c \longrightarrow \mathcal{O}(\mathbb{N})$ vérifie, pour toute règle α de $R_{\Delta, \Sigma}$, $s(\alpha)_* \geq t(\alpha)_*$, $s(\alpha)^* \geq t(\alpha)^*$ et $[s(\alpha)] > [t(\alpha)]$, sauf pour $\alpha = 6$, où l'on a égalité entre $[s(\alpha)]$ et $[t(\alpha)]$.*

Démonstration.

1. On a trois vérifications à faire : $s(1)_* \geq t(1)_*$, $s(1)^* \geq t(1)^*$ et $[s(1)] > [t(1)]$. Pour les deux premières inégalités :

$$\begin{cases} ((1 \otimes \delta) \circ \delta)_*(i) = (1 \otimes \delta)_*(i, i) = (i, i, i) \\ ((\delta \otimes 1) \circ \delta)_*(i) = (\delta \otimes 1)_*(i, i) = (i, i, i). \end{cases}$$

$$\begin{cases} ((1 \otimes \delta) \circ \delta)^*(i, j, k) = (\delta)^*(i, j + k + 1) = i + j + k + 2 \\ ((\delta \otimes 1) \circ \delta)^*(i, j, k) = (\delta)^*(i + j + 1, k) = i + j + k + 2. \end{cases}$$

Pour $[\cdot]$:

$$\begin{cases} [(1 \otimes \delta) \circ \delta](i, j, k, l) = [\delta](i, j, k + l + 2) + [\delta](i, k, l) = 2.\underline{i} + \underline{(k + l + 1)} + \underline{l} \\ [(\delta \otimes 1) \circ \delta](i, j, k, l) = [\delta](i, j + k + 1, l) + [\delta](i, j, k) = 2.\underline{i} + \underline{k} + \underline{l}. \end{cases}$$

On conclut en remarquant que $\underline{k + l + 1} \geq \underline{k + 1} > \underline{k}$. Pour les règles suivantes, nous irons plus vite.

2.

$$\begin{cases} ((\varepsilon \otimes 1) \circ \delta)_*(i) = 1 = 1_*(i) \\ ((\varepsilon \otimes 1) \circ \delta)^*(i) = i + 2 > i = 1^*(i) \\ [(\varepsilon \otimes 1) \circ \delta](i, j) = \underline{i} + \underline{j} > 0 = [1](i, j). \end{cases}$$

3.

$$\begin{cases} ((1 \otimes \varepsilon) \circ \delta)_*(i) = 1 = 1_*(i) \\ ((1 \otimes \varepsilon) \circ \delta)^*i = i + 2 > i = 1^*(i) \\ [(1 \otimes \varepsilon) \circ \delta](i, j) = \underline{i} + \underline{1} > 0 = [1](i, j). \end{cases}$$

4.

$$\begin{cases} (\tau \circ \delta)_*(i) = (i, i) = \delta_*(i) \\ (\tau \circ \delta)^*(i, j) = i + j + 1 = \delta^*(i, j). \end{cases}$$

Et :

$$\begin{cases} [\tau \circ \delta](i, j, k) = \underline{i} + \underline{j} + i^2.\underline{k} + k.2\underline{i} \\ [\delta](i, j, k) = \underline{i} + \underline{k}. \end{cases}$$

Comme $i^2 \geq 1$, on a $i^2.\underline{k} \geq \underline{k}$. Le fait que $\underline{j} > 0$ permet alors de conclure.

5.

$$\begin{cases} (\tau \circ \tau)_*(i, j) = (i, j) = 2_*(i, j) \\ (\tau \circ \tau)^*(i, j) = (i, j) = 2^*(i, j) \\ [\tau \circ \tau](i, j, k, l) = ij.(\underline{k} + \underline{l}) + (k + l).\underline{i + j} > 0 = [2](i, j, k, l). \end{cases}$$

6.

$$\begin{cases} ((1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau))_*(i, j, k) \\ = (k, j, i) = ((\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1))_*(i, j, k) \\ ((1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau))^*(i, j, k) \\ = (k, j, i) = ((\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1))^*(i, j, k). \end{cases}$$

Et :

$$\begin{aligned} & [(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau)](i, j, k, l, m, n) \\ &= jk.\underline{m} + m.\underline{j + k} + i(j + k).\underline{n} + n.(\underline{i + j} + \underline{i + k}) \\ &= [(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau)](i, j, k, l, m, n). \end{aligned}$$

Comme annoncé, on a seulement $[s(6)] = [t(6)]$.

7.

$$\begin{cases} ((1 \otimes \delta) \circ \tau)_*(i, j) = (j, i, i) = ((\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1))_*(i, j) \\ ((1 \otimes \delta) \circ \tau)^*(i, j, k) = (j + k + 1, i) = ((\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1))^*(i, j, k). \end{cases}$$

Et :

$$\begin{cases} [(1 \otimes \delta) \circ \tau](i, j, k, l, m) = \underline{i} + \underline{m} + (l + m).\underline{i + j} + ij.\underline{l + m + 1} \\ [(\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1)](i, j, k, l, m) = \underline{i} + \underline{m} + (l + m).\underline{i + j} + ij.(\underline{l + m}). \end{cases}$$

Comme $ij \geq 1$, on a $ij.\underline{l + m + 1} \geq ij.\underline{l + 1} > ij.\underline{l}$ et, de même, $ij.\underline{l + m + 1} > ij.\underline{m}$, d'où :

$$ij.\underline{l + m + 1} > ij.(\underline{l + m}),$$

ce qui permet de conclure.

8.

$$\begin{cases} ((1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta))_*(i, j) = (j, j, i) = ((\delta \otimes 1) \circ \tau)_*(i, j) \\ ((1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta))^*(i, j, k) = (k, i + j + 1) = ((\delta \otimes 1) \circ \tau)^*(i, j, k). \end{cases}$$

Et :

$$\begin{cases} [(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta)](i, j, k, l, m) = \underline{j} + \underline{l} + 2ij.\underline{m} + 2m.\underline{i} + \underline{j} \\ [(\delta \otimes 1) \circ \tau](i, j, k, l, m) = \underline{j} + \underline{l} + ij.\underline{m} + m.\underline{i} + \underline{j}. \end{cases}$$

 Comme $ij > 0$ et $m > 0$, on a bien $2ij.\underline{m} > ij.\underline{m}$ et $2m.\underline{i} + \underline{j} > m.\underline{i} + \underline{j}$.

9.

$$\begin{cases} ((1 \otimes \varepsilon) \circ \tau)_*(i, j) = j = (\varepsilon \otimes 1)_*(i, j) \\ ((1 \otimes \varepsilon) \circ \tau)^*(i) = (1, i) = (\varepsilon \otimes 1)^*(i) \\ [(1 \otimes \varepsilon) \circ \tau](i, j, k) = ij.\underline{1} + \underline{i} + \underline{j} > 0 = [\varepsilon \otimes 1](i, j, k). \end{cases}$$

10.

$$\begin{cases} ((\varepsilon \otimes 1) \circ \tau)_*(i, j) = i = (1 \otimes \varepsilon)_*(i, j) \\ ((\varepsilon \otimes 1) \circ \tau)^*(i) = (i, 1) = (1 \otimes \varepsilon)^*(i) \\ [(\varepsilon \otimes 1) \circ \tau](i, j, k) = ij.\underline{k} + k.\underline{i} + \underline{j} > 0 = [1 \otimes \varepsilon](i, j, k). \end{cases}$$

11.

$$\begin{cases} ((1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta)_*(i) = (i, i, i) = ((\delta \otimes 1) \circ \delta)_*(i) \\ ((1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta)^*(i, j, k) = i + j + k + 2 = ((\delta \otimes 1) \circ \delta)^*(i, j, k). \end{cases}$$

Et :

$$\begin{cases} [(1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta](i, j, k, l) = 2.\underline{i} + \underline{k} + \underline{l} + i^2.\underline{l} + l.\underline{2i} \\ [(\delta \otimes 1) \circ \delta](i, j, k, l) = 2.\underline{i} + \underline{k} + \underline{l}. \end{cases}$$

 On conclut en notant que $i^2 > 0$ et $l > 0$ et donc $i^2.\underline{l} + l.\underline{2i} > 0$.

12.

$$\begin{cases} ((1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau)_*(i, j) = (j, i, j) = ((\tau \otimes 1) \circ (1 \otimes \delta))_*(i, j) \\ ((1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau)^*(i, j, k) = (j, i + k + 1) = ((\tau \otimes 1) \circ (1 \otimes \delta))^*(i, j, k). \end{cases}$$

Et :

$$\begin{cases} [(1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau](i, j, k, l, m) = \underline{j} + \underline{m} + ij.(\underline{l} + \underline{m}) + (l + m).\underline{i} + \underline{j} \\ [(\tau \otimes 1) \circ (1 \otimes \delta)](i, j, k, l, m) = \underline{j} + \underline{m} + ij.\underline{l} + l.\underline{i} + \underline{j}. \end{cases}$$

 Comme $ij > 0$ et $m > 0$, on a bien $ij.\underline{m} + m.\underline{i} + \underline{j} > 0$.

On va à présent regarder les règles $\gamma\varepsilon$, $\gamma\delta$, $\gamma\tau 1$ et $\gamma\tau 2$ pour une constante γ de Σ (si Σ ne contient pas de constante, ces quatre règles n'apparaissent pas dans $R_{\Sigma/\Delta}$).

$\gamma\varepsilon$.

$$\begin{cases} (\varepsilon \circ \gamma)_*(*) = * = 0_*(*) \\ (\varepsilon \circ \gamma)^*(*) = * = 0^*(*) \\ [\varepsilon \circ \gamma](*) = \underline{1} > 0 = [0](*). \end{cases}$$

$\gamma\delta$.

$$\begin{cases} (\delta \circ \gamma)_*(*) = (1, 1) = (\gamma \otimes \gamma)_*(*) \\ (\delta \circ \gamma)^*(i, j) = * = (\gamma \otimes \gamma)^*(i, j). \end{cases}$$

Et :

$$\begin{cases} [\delta \circ \gamma](i, j) = \underline{i + j + 1} + \underline{j} + \underline{1} \\ [\gamma \otimes \gamma](i, j) = \underline{i} + \underline{j}. \end{cases}$$

On conclut en notant que $\underline{i + j + 1} + \underline{1} > \underline{i}$.

$\gamma\tau 1$.

$$\begin{cases} (\tau \circ (\gamma \otimes 1))_*(i) = (i, 1) = (1 \otimes \gamma)_*(i) \\ (\tau \circ (\gamma \otimes 1))^*(i, j) = i = (1 \otimes \gamma)^*(i, j). \end{cases}$$

Et :

$$\begin{cases} [\tau \circ (\gamma \otimes 1)](i, j, k) = (i + 1). \underline{k} + k. \underline{i + 1} \\ [1 \otimes \gamma](i, j, k) = \underline{k}. \end{cases}$$

Pour conclure : $(i + 1). \underline{k} \geq 2. \underline{k} > \underline{k}$.

$\gamma\tau 2$.

$$\begin{cases} (\tau \circ (1 \otimes \gamma))_*(i) = (1, i) = (\gamma \otimes 1)_*(i) \\ (\tau \circ (1 \otimes \gamma))^*(i, j) = j = (\gamma \otimes 1)^*(i, j). \end{cases}$$

Et :

$$\begin{cases} [\tau \circ (1 \otimes \gamma)](i, j, k) = \underline{j} + i. \underline{k} + k. \underline{i + 1} \\ [\gamma \otimes 1](i, j, k) = \underline{j}. \end{cases}$$

On conclut avec : $i. \underline{k} + k. \underline{i + 1} \geq \underline{k} + \underline{i + 1} > 0$.

Avant d'étudier les dernières relations, on doit calculer les valeurs de F en δ_n , $\tau_{n,1}$ et $\tau_{1,n}$. On montre, par récurrence sur n , que, pour tout $n \geq 1$, on a :

- pour δ_n :

$$\begin{cases} (\delta_n)_*(i_1, \dots, i_n) = (i_1, \dots, i_n, i_1, \dots, i_n) \\ \delta_n^*(i_1, \dots, i_n, j_1, \dots, j_n) = (i_1 + j_1 + 1, \dots, i_n + j_n + 1) \\ [\delta_n](i_1, \dots, i_n, j_1, \dots, j_n, k_1, \dots, k_n) \\ \quad = \sum_{1 \leq u \leq n} (\underline{i_u} + \underline{k_u}) + \sum_{1 \leq u < v \leq n} (i_u i_v \cdot \underline{k_u} + k_u \cdot \underline{i_u} + i_v). \end{cases}$$

- pour $\tau_{n,1}$:

$$\begin{cases} (\tau_{n,1})_*(i_1, \dots, i_n, j) = (j, i_1, \dots, i_n) \\ \tau_{n,1}^*(i, j_1, \dots, j_n) = (j_1, \dots, j_n, i) \\ [\tau_{n,1}](i_1, \dots, i_n, j, k, l_1, \dots, l_n) = \sum_{1 \leq u \leq n} (i_u j \cdot \underline{l_u} + l_u \cdot \underline{i_u} + j). \end{cases}$$

- pour $\tau_{1,n}$:

$$\begin{cases} (\tau_{1,n})_*(i, j_1, \dots, j_n) = (j_1, \dots, j_n, i) \\ \tau_{1,n}^*(i_1, \dots, i_n, j) = (j, i_1, \dots, i_n) \\ [\tau_{1,n}](i, j_1, \dots, j_n, k_1, \dots, k_n, l) = \sum_{1 \leq u \leq n} (i j_u \cdot \underline{l} + l \cdot \underline{i} + j_u). \end{cases}$$

On peut alors étudier les règles $\varphi\varepsilon$, $\varphi\delta$, $\varphi\tau 1$ et $\varphi\tau 2$ pour une flèche $\varphi \in \Sigma(n, 1)$ fixée.

$\varphi\varepsilon$.

$$\begin{cases} (\varepsilon \circ \varphi)_*(i_1, \dots, i_n) = * = \varepsilon_*^n(i_1, \dots, i_n) \\ (\varepsilon \circ \varphi)^*(*) = (1, \dots, 1) = (\varepsilon^n)^*(*) \\ [\varepsilon \circ \varphi](i_1, \dots, i_n) = \underline{1} > 0 = [\varepsilon^n](i_1, \dots, i_n). \end{cases}$$

$\varphi\delta$.

$$\begin{cases} (\delta \circ \varphi)_*(i_1, \dots, i_n) = (i_1 + \dots + i_n + 1, i_1 + \dots + i_n + 1) = ((\varphi \otimes \varphi) \circ \delta_n)_* \\ (\delta \circ \varphi)^*(i, j) = (i + j + 1, \dots, i + j + 1) = ((\varphi \otimes \varphi) \circ \delta_n)^*. \end{cases}$$

Et pour $[\cdot]$:

$$\begin{cases} [\delta \circ \varphi](i_1, \dots, i_n, j, k) \\ \quad = \underline{j + k + 1} + \underline{i_1 + \dots + i_n + 1} + \underline{k} \\ [(\varphi \otimes \varphi) \circ \delta_n](i_1, \dots, i_n, j, k) \\ \quad = \underline{j} + (n + 1 + \sum_{1 \leq u < v \leq n} i_u i_v) \cdot \underline{k} + \sum_{1 \leq u \leq n} \underline{i_u} + k \cdot \sum_{1 \leq u < v \leq n} \underline{i_u} + \underline{i_v}. \end{cases}$$

On conclut en notant les inégalités suivantes :

$$\begin{cases} \underline{j+k+1} > \underline{j+1} > \underline{j} \\ \underline{j+k+1} > \underline{k+1} > \underline{k} \\ \underline{i_1 + \dots + i_n + 1} \geq \underline{i_u + 1} > \underline{i_u} & \text{pour tout } u \in \{1 \dots n\} \\ \underline{i_1 + \dots + i_n + 1} \geq \underline{i_u + i_v + 1} > \underline{i_u + i_v} & \text{pour tous } u, v \in \{1 \dots n\}, u \neq v. \end{cases}$$

$\varphi\tau 1.$

$$\begin{cases} (\tau \circ (\varphi \otimes 1))_*(i_1, \dots, i_n, j) = (j, i_1 + \dots + i_n + 1) = ((1 \otimes \varphi) \circ \tau_{n,1})_* \\ (\tau \circ (\varphi \otimes 1))^*(i, j) = (j, \dots, j, i) = ((1 \otimes \varphi) \circ \tau_{n,1})^*. \end{cases}$$

Et pour $[\cdot]$:

$$\begin{cases} [\tau \circ (\varphi \otimes 1)](i_1, \dots, i_n, j, k, l) \\ = \underline{l} + (i_1 + \dots + i_n + 1)j.\underline{l} + l.\underline{i_1 + \dots + i_n + j + 1} \\ [(1 \otimes \varphi) \circ \tau_{n,1}](i_1, \dots, i_n, j, k, l) \\ = \underline{l} + (i_1 + \dots + i_n)j.\underline{l} + l.(\underline{i_1 + j} + \dots + \underline{i_n + j}). \end{cases}$$

Comme $j > 0$, on a $j.\underline{l} > 0$ et, comme $l > 0$, on a, pour tout u :

$$l.\underline{i_1 + \dots + i_n + j + 1} > l.\underline{i_u + j}.$$

$\varphi\tau 2.$

$$\begin{cases} (\tau \circ (1 \otimes \varphi))_*(i, j_1, \dots, j_n) = (j_1 + \dots + j_n + 1, i) = ((\varphi \otimes 1) \circ \tau_{1,n})_* \\ (\tau \circ (1 \otimes \varphi))^*(i, j) = (j, i, \dots, i) = ((\varphi \otimes 1) \circ \tau_{1,n})^*. \end{cases}$$

Et pour $[\cdot]$:

$$\begin{cases} [\tau \circ (1 \otimes \varphi)](i, j_1, \dots, j_n, k_1, \dots, k_n, l) \\ = \underline{k} + i(j_1 + \dots + j_n + 1).\underline{l} + l.\underline{i + j_1 + \dots + j_n + 1} \\ [(\varphi \otimes 1) \circ \tau_{1,n}](i, j_1, \dots, j_n, k_1, \dots, k_n, l) \\ = \underline{k} + i(j_1 + \dots + j_n).\underline{l} + l.(\underline{i + j_1} + \dots + \underline{i + j_n}). \end{cases}$$

Comme pour $\varphi\tau 1$, on note que $i.\underline{l} > 0$ et que $l.\underline{i + j_1 + \dots + j_n + 1} > l.\underline{i + j_u}$ pour tout u .

On a donc vu que, pour toute règle $\alpha \in R_{\Delta, \Sigma}$, on a $s(\alpha)_* \geq t(\alpha)_*$, $s(\alpha)^* \geq t(\alpha)^*$ et $[s(\alpha)] > [t(\alpha)]$, sauf si $\alpha = 6$, auquel cas $[s(6)] = [t(6)]$.

◇

On en déduit :

Corollaire 5.22. *La présentation $(\Sigma^c, R_{\Delta, \Sigma})$ termine si et seulement si $(\Sigma^c, 6)$ termine.*

Démonstration. L'implication gauche-droite est évidente. Pour la réciproque, supposons que $(\Sigma^c, R_{\Delta, \Sigma})$ ne termine pas. Il existe donc un chemin de réduction infini $(f_n)_n$ dans $(\Sigma^c, R_{\Delta, \Sigma})$. On en déduit donc une suite $([f_n])_n$ décroissante dans $([\mathbb{N}^*], >)$: ce dernier ARS termine, donc $([f_n])_n$ est stationnaire, c'est-à-dire qu'à partir d'un certain rang N , tous les $[f_n]$ sont égaux. D'après le résultat précédent, on en déduit qu'à partir du rang N , toutes les réductions effectuées sont issues de la règle 6. On a donc un chemin de réduction infini dans $(\Sigma^c, 6)$, qui ne termine donc pas. ◇

Il ne reste plus qu'à montrer que 6 termine. On va donc construire un nouveau morphisme d'opérades $G : \mathcal{L}\Sigma^c \longrightarrow \mathcal{O}(\mathbb{N}, \mathbb{N}, \mathbb{N})$:

- $\tau_*(i, j) = (j, i + 1)$, $\tau^*(i, j) = (j, i)$, $[\tau](i, j, k, l) = i + j$;
- $\delta_*(i) = (i, i)$, $\delta^*(i, j) = i + j$, $[\delta](i, j, k) = 0$;
- $\varepsilon_*(i) = *$, $\varepsilon^*(*) = 1$, $[\varepsilon](i) = 0$;
- $\gamma_*(*) = 1$, $\gamma^*(i) = *$, $[\gamma](i) = 0$;
- $\varphi_*(i_1, \dots, i_n) = i_1 + \dots + i_n$, $\varphi^*(i) = (i, \dots, i)$, $[\varphi](i_1, \dots, i_n, j) = 0$.

On vérifie que cela fonctionne pour 6 :

$$((1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau))_*(i, j, k) = (k, j + 1, i + 2) = ((\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1))_*(i, j, k).$$

Et :

$$((1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau))^*(i, j, k) = (k, j, i) = G((\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1))(i, j, k).$$

Puis, pour $[\cdot]$:

$$\begin{cases} [(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau)](i, j, k, l, m, n) = 2i + 2j + 2k + 2 \\ [(\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1)](i, j, k, l, m, n) = 2i + 2j + 2k + 1. \end{cases}$$

On a bien $[s(6)] > [t(6)]$, ce qui permet de conclure que :

Proposition 5.23. *La présentation d'opérade $(\Sigma^c, R_{\Delta, \Sigma})$ termine.*

Remarque. En particulier, la présentation (Δ, R_{Δ}) , qui n'est autre que celle de \mathbb{F}^o donnée par Yves Lafont dans [Laf03], termine, ce qui était déjà prouvé mais grâce à une interprétation classique qui ne peut pas s'étendre à $(\Sigma^c, R_{\Delta, \Sigma})$ dès que Σ contient une constante.

5.3.5 Confluence de $(\Sigma^c, R_{\Delta, \Sigma})$

Comme on a déjà prouvé que cette présentation termine, il ne reste plus, d'après le lemme de Newmann, qu'à vérifier sa confluence locale, et donc, d'après le théorème des paires critiques, que toutes ses paires critiques sont confluentes. Cependant, on touche ici une nouvelle difficulté inhérente aux présentations d'opérides et à leur nature 2-dimensionnelle : en effet, bien qu'ayant un nombre fini de relations, la présentation étudiée possède une infinité de paires critiques. Pourtant, il suffit d'en étudier un nombre fini, comme c'était déjà le cas dans [Laf03] au sujet de (Δ, R_Δ) .

Nous allons commencer par examiner les paires critiques de (Δ, R_Δ) .

Confluence de (Δ, R_Δ)

Nous utilisons la méthode décrite en 3.8.2 pour produire la liste des paires critiques de cette présentation. Nous n'allons détailler que certains cas, montrant qu'il existe deux types de paires critiques : la présentation (Δ, R_Δ) possède cinquante paires critiques que nous pourrions qualifier de régulières ; mais on trouve aussi six familles infinies de paires critiques, chacune étant produite par un couple donné de règles : $(1, 8)$, $(6, 6)$, $(6, 8)$, $(6, 11)$, $(6, 12)$ et $(7, 8)$.

Il faut commencer par vérifier que la présentation (Δ, R_Δ) est bien conforme aux hypothèse du théorème 3.24, c'est-à-dire que pour toute règle α de R_Δ et pour tous contextes C et D applicables à α , on a $C = D$ dès que $C[\alpha] = D[\alpha]$. Nous allons, par exemple, traiter le cas où α est la règle numéro 1 :

$$(1 \otimes \delta) \circ \delta \rightarrow_1 (\delta \otimes 1) \circ \delta.$$

Supposons que C et D sont deux contextes tels que :

$$C[(1 \otimes \delta) \circ \delta] = D[(1 \otimes \delta) \circ \delta].$$

Alors trois cas sont possibles :

- a. Les occurrences de $s(1)$ mises en valeur dans chaque membre de l'égalité sont les mêmes. Dans ce cas, les deux contextes C et D sont égaux.
- b. Les deux occurrences de $s(1)$ se chevauchent mais sont distinctes. Alors, il existe un contexte E tel que, quitte à échanger C et D :

$$\begin{cases} C = E[(1 \otimes \square_3^1) \circ \delta] \\ D = E[(2 \otimes \delta) \circ \square_3^1]. \end{cases}$$

- c. Les deux occurrences de $s(1)$ sont disjointes. Alors, il existe deux contextes E et F tels que, quitte encore à échanger C et D :

$$\begin{cases} C = E[\cdot] \circ F[(1 \otimes \delta) \circ \delta] \\ D = E[(1 \otimes \delta) \circ \delta] \circ F[\cdot]. \end{cases}$$

À présent, supposons que C et D vérifient aussi :

$$C[(\delta \otimes 1) \circ \delta] = D[(\delta \otimes 1) \circ \delta].$$

Alors, si l'on est dans le cas (b) :

$$E[(1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \circ \delta] = E[(\delta \otimes \delta) \circ \delta],$$

ce qui est impossible. Si l'on est dans le cas (c) :

$$E[(\delta \otimes 1) \circ \delta] \circ F[(1 \otimes \delta) \circ \delta] = E[(1 \otimes \delta) \circ \delta] \circ F[(\delta \otimes 1) \circ \delta],$$

ce qui est aussi exclu. On est donc bien dans le cas (a), c'est-à-dire que $C = D$. Le reste des vérifications, pour les onze autres règles, se fait de manière similaire avec, éventuellement, plus de cas à distinguer. On arrive ainsi à :

Lemme 5.24. *Pour toute règle α de R_Δ et tous contextes C et D tels que $C[\alpha] = D[\alpha]$, on a : $C = D$.*

Ainsi, la méthode de 3.8.2 est applicable ici. Nous allons en détailler l'application dans quatre cas, pour les couples de règles $(1, 1)$, $(1, 2)$, $(2, 4)$ et $(6, 6)$.

Paires critiques de $(1, 1)$. Il faut, dans un premier temps, déterminer tous les triplets (φ, C_0, D_0) formés d'une flèche φ de Σ et de deux contextes C_0 et D_0 applicables à φ et tels que $C_0[\varphi] = D_0[\varphi] = s(1)$. En constatant que δ est l'unique flèche de Σ qui apparaît dans $s(1)$, on obtient les quatre triplets suivants :

$$\begin{cases} (\delta, (1 \otimes \delta) \circ \square_2^1, (1 \otimes \delta) \circ \square_2^1) \\ (\delta, (1 \otimes \square_2^1) \circ \delta, (1 \otimes \delta) \circ \square_2^1) \\ (\delta, (1 \otimes \delta) \circ \square_2^1, (1 \otimes \square_2^1) \circ \delta) \\ (\delta, (1 \otimes \square_2^1) \circ \delta, (1 \otimes \square_2^1) \circ \delta). \end{cases}$$

Comme on est dans le cas $\alpha = \beta$, on enlève les premier et dernier triplets. De plus, toute paire critique éventuellement calculée à partir du troisième triplet sera de la forme p^{-1} avec p une paire critique calculée à partir du deuxième triplet. Il ne reste donc plus qu'à considérer le cas où :

$$\varphi = \delta, \quad C_0 = (1 \otimes \square_2^1) \circ \delta, \quad D_0 = (1 \otimes \delta) \circ \square_2^1.$$

À présent, supposons que C et D sont deux contextes vérifiant $C \circ C_0 = D \circ D_0$. On commence par écrire C et D sous la forme :

$$C = g \circ (i \otimes \square_3^1 \otimes j) \circ f \quad \text{et} \quad D = g' \circ (i' \otimes \square_3^1 \otimes j') \circ f',$$

avec i, j, i' et j' des entiers et f, g, f' et g' des flèches de $\mathcal{L}\Delta$. On a, par hypothèse :

$$g \circ (i \otimes 1 \otimes \square_2^1 \otimes j) \circ (i \otimes \delta \otimes j) \circ f = g' \circ (i' \otimes 1 \otimes \delta \otimes j') \circ (i' \otimes \square_2^1 \otimes j') \circ f'.$$

Si, de plus, le couple (C, D) est une solution minimale, on doit avoir $i = j = j' = 0$, $i' = i + 1 = 1$, $g' = 4$, $g = g' \circ (2 \otimes \delta) = 2 \otimes \delta$, $f = 1$ et $f' = \delta \circ f = \delta$. C'est-à-dire :

$$C = (2 \otimes \delta) \circ \square_3^1 \quad \text{et} \quad D = (1 \otimes \square_3^1) \circ \delta.$$

Réciproquement, on vérifie que ce couple (C, D) est bien solution de $C \circ C_0 = D \circ D_0$, ce qui est bien le cas puisque :

$$C \circ C_0 = D \circ D_0 = (2 \otimes \delta) \circ (1 \otimes \square_2^1) \circ \delta.$$

On en déduit ainsi l'unique paire critique (à inversion près) formée par la règle 1 avec elle-même :

$$\left((2 \otimes \delta) \circ (1 \otimes \delta) \circ \delta, (2 \otimes \delta) \circ \square_3^1, (1), (1 \otimes \square_3^1) \circ \delta, (1) \right).$$

Le branchement associé à cette paire critique est donné par les deux réductions suivantes :

$$\begin{cases} (2 \otimes \delta) \circ (1 \otimes \delta) \circ \delta \rightarrow_1 (\delta \otimes \delta) \circ \delta \\ (2 \otimes \delta) \circ (1 \otimes \delta) \circ \delta \rightarrow_1 (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \circ \delta. \end{cases}$$

Paires critiques de $(1, 2)$. Pour ces deux règles, la seule flèche de Σ apparaissant dans les deux sources est δ . On en déduit deux triplets (δ, C_0, D_0) tels que $C_0[\delta] = s(1)$ et $D_0[\delta] = s(2)$:

$$\begin{cases} (\delta, (1 \otimes \delta) \circ \square_2^1, (\varepsilon \otimes 1) \circ \square_2^1) \\ (\delta, (1 \otimes \square_2^1) \circ \delta, (\varepsilon \otimes 1) \circ \square_2^1). \end{cases}$$

La résolution de $C \circ C_0 = D \circ D_0$ est immédiate dans les deux cas. On obtient, pour le premier triplet, la solution minimale suivante :

$$C = (\varepsilon \otimes 2) \circ \square_3^1 \quad \text{et} \quad D = \delta \circ \square_1^1.$$

Quant au deuxième triplet, il donne :

$$C = (1 \otimes \varepsilon \otimes 1) \circ \square_3^1 \quad \text{et} \quad D = (1 \otimes \square_1^1) \circ \delta.$$

Les deux règles 1 et 2 créent donc, à inversion près, deux paires critiques :

$$\left((\varepsilon \otimes \delta) \circ \delta, (\varepsilon \otimes 2) \circ \square_3^1, (1), \delta \circ \square_1^1, (2) \right)$$

et :

$$\left((1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \delta) \circ \delta, (1 \otimes \varepsilon \otimes 1) \circ \square_3^1, (1), (1 \otimes \square_1^1) \circ \delta, (2) \right).$$

Paires critiques de (2, 4). Encore une fois, la seule flèche de Σ qui apparaît à la fois dans $s(2)$ et $s(4)$ est δ . On obtient un seul triplet (δ, C_0, D_0) tel que $C_0[\delta] = D_0[\delta]$:

$$(\delta, (\varepsilon \otimes 1) \circ \square_2^1, \tau \circ \square_2^1).$$

Supposons à présent que C et D sont deux contextes qui sont des solutions minimales de l'équation $C \circ C_0 = D \circ D_0$. On écrit :

$$C = g \circ (i \otimes \square_1^1 \otimes j) \circ f \quad \text{et} \quad D = g' \circ (i' \otimes \square_2^1 \otimes j') \circ f'.$$

Par hypothèse, on a :

$$g \circ (i \otimes \varepsilon \otimes 1 \otimes j) \circ (i \otimes \square_2^1 \otimes j) \circ f = g' \circ (i' \otimes \tau \otimes j') \circ (i' \otimes \square_2^1 \otimes j') \circ f'.$$

Comme (C, D) est une solution minimale, on a $i = i' = j = j' = 0$, $f = f' = 1$ et :

$$g \circ (\varepsilon \otimes 1) = g' \circ \tau.$$

Or, cette dernière équation ne possède aucune solution, puisque $\mathcal{L}\Delta$ est libre. Donc les règles 2 et 4 ne forment aucune paire critique.

Paires critiques de (6, 6). Ici, τ est l'unique flèche de $\mathcal{L}\Delta$ qui apparaît dans $s(6)$. On calcule les triplets (τ, C_0, D_0) tels que $C_0[\tau] = D_0[\tau] = s(6)$, on retire ceux qui vérifient $C_0 = D_0$ (car $\alpha = \beta$ ici), ainsi que tous les autres qui sont symétriques en C_0 et D_0 (il produiraient seulement des paires critiques inverses de celles qui auront été calculées). Il en reste alors trois :

$$\left\{ \begin{array}{l} (\tau, (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \square_2^2), (1 \otimes \tau) \circ (\square_2^2 \otimes 1) \circ (1 \otimes \tau)) \\ (\tau, (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \square_2^2), (1 \otimes \square_2^2) \circ (\tau \otimes 1) \circ (1 \otimes \tau)) \\ (\tau, (1 \otimes \tau) \circ (\square_2^2 \otimes 1) \circ (1 \otimes \tau), (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \square_2^2)). \end{array} \right.$$

Or, à partir d'une symétrie haut-bas, on peut récupérer les paires critiques associées au troisième triplet à partir de celles qui sont associées au premier. Il ne reste donc plus que les deux premiers triplets à étudier.

En ce qui concerne le premier, la résolution de l'équation $C \circ C_0 = D \circ D_0$ aboutit, en particulier, à celle de :

$$g \circ (1 \otimes \tau) \circ (\tau \otimes 1) = g' \circ (1 \otimes \tau).$$

Or cette dernière équation n'admet pas de solution dans une opérade libre. Le premier triplet ne crée donc pas de paire critique (et donc le troisième non plus).

Regardons à présent le cas du deuxième. Supposons que C et D sont des contextes qui sont des solutions minimales de l'équation $C \circ C_0 = D \circ D_0$. On écrit :

$$C = g \circ (i \otimes \square_3^3 \otimes j) \circ f \quad \text{et} \quad D = g' \circ (i' \otimes \square_3^3 \otimes j') \circ f'.$$

Alors :

$$\begin{aligned} & g \circ (i \otimes 1 \otimes \tau \otimes j) \circ (i \otimes \tau \otimes 1 \otimes j) \circ (i \otimes 1 \otimes \square_2^2 \otimes j) \circ f \\ &= g' \circ (i' \otimes 1 \otimes \square_2^2 \otimes j') \circ (i' \otimes \tau \otimes 1 \otimes j') \circ (i' \otimes 1 \otimes \tau \otimes j') \circ f'. \end{aligned}$$

On écrit maintenant $f = (h \otimes 2 \otimes j) \circ h'$, ce qui est toujours possible, quitte à prendre $h' = f$ et $h = i + 1$. Ainsi :

$$\begin{aligned} & g \circ (i \otimes 1 \otimes \tau \otimes j) \circ (i \otimes \tau \otimes 1 \otimes j) \circ (h \otimes \square_2^2 \otimes j) \circ h' \\ &= g' \circ (i' \otimes 1 \otimes \square_2^2 \otimes j') \circ (i' \otimes \tau \otimes 1 \otimes j') \circ (i' \otimes 1 \otimes \tau \otimes j') \circ f'. \end{aligned}$$

Comme C et D sont des solutions minimales, on doit avoir $j = j' = 0$, $f' = i' + 3$, $g = i + 3$ et :

$$\begin{cases} h' = (i' \otimes \tau \otimes 1) \circ (i' \otimes 1 \otimes \tau) \\ g' = (i \otimes 1 \otimes \tau) \circ (i \otimes \tau \otimes 1) \circ (h \otimes 2). \end{cases}$$

Ainsi :

$$\begin{cases} C_h = (i \otimes \square_3^3) \circ (h \otimes 2) \circ (i' \otimes \tau \otimes 1) \circ (i' \otimes 1 \otimes \tau) \\ D_h = (i \otimes 1 \otimes \tau) \circ (i \otimes \tau \otimes 1) \circ (h \otimes 2) \circ (i' \otimes \square_3^3). \end{cases}$$

De plus, pour avoir (C_h, D_h) solution minimale, on doit imposer que la flèche h ne se factorise d'aucune des façons suivantes :

- en $h = h_1 \otimes h_2$, avec $h_2 : m + 1 \longrightarrow n + 1$ et $h_1 \neq 0$;
- en $h = h_2 \circ (h_1 \otimes 1)$, avec h_1 différente d'une identité;
- en $h = (h_1 \otimes 1) \circ h_2$, avec h_1 différente d'une identité.

On note, temporairement, H l'ensemble des flèches $h : p + 1 \longrightarrow q + 1$ qui n'admettent aucune de ces factorisations. On vérifie alors que, pour toute flèche h de H , le couple (C_h, D_h) est une solution minimale de l'équation $C \circ C_0 = D \circ D_0$.

Ainsi, la règle 6 crée, avec elle-même, une infinité de paires critiques p_h , indexées par les flèches h de H . Cependant, nous allons rappeler à présent comment Yves Lafont a montré, dans [Laf03], que la confluence de toutes ces paires critiques p_h , h dans H , est équivalente à celle de quatre d'entre elles.

Le premier ingrédient utilisé est la terminaison de la présentation : elle nous permet de démontrer, par récurrence, que la confluence des paires critiques d'une famille donnée est équivalente à celle de sa sous-famille indexée seulement sur les flèches irréductibles de $\mathcal{L}\Delta$. En effet, comme R_Δ termine, on peut appliquer le principe de récurrence pour montrer, comme dans la figure 5.8, que l'on peut se limiter aux cas où la paire critique considérée est indexée par une flèche en R_Δ -forme normale.

Ainsi :

Lemme 5.25. *Les assertions suivantes sont équivalentes :*

- i. *Pour toute flèche h dans H , la paire critique p_h est confluente.*
- ii. *Pour toute flèche h dans H en R_Δ -forme normale, la paire critique p_h est confluente.*

Le second ingrédient est l'examen de toutes les formes que peuvent avoir les flèches $h : m + 1 \longrightarrow n + 1$ irréductibles pour R_Δ . Yves Lafont a montré, toujours dans [Laf03] :

Lemme 5.26. *Si $h : m + 1 \longrightarrow n + 1$ est une R_Δ -forme normale, alors h possède l'une des formes suivantes :*

- *il existe une flèche h' telle que $h = h' \otimes 1$;*
- *il existe une flèche h' telle que $h = (h' \otimes 1) \circ (m \otimes \delta)$;*
- *il existe une flèche h' telle que $h = h' \otimes \varepsilon$;*
- *il existe un entier p ainsi que deux flèches h_1 et h_2 tels que :*

$$h = (h_2 \otimes 1) \circ (p \otimes \tau) \circ (h_1 \otimes 1).$$

On en déduit que :

Corollaire 5.27. *Les seules flèches de H qui sont des R_Δ -formes normales sont 1 , δ , τ et $1 \otimes \varepsilon$. Par suite, les assertions suivantes sont équivalentes :*

- i. *Pour toute flèche h dans H , la paire critique p_h est confluente.*
- ii. *Les quatre paires critiques p_1 , p_δ , p_τ et $p_{1 \otimes \varepsilon}$ sont confluentes.*

Ainsi, il ne reste plus que quatre paires critiques engendrées par $(6, 6)$ à étudier.

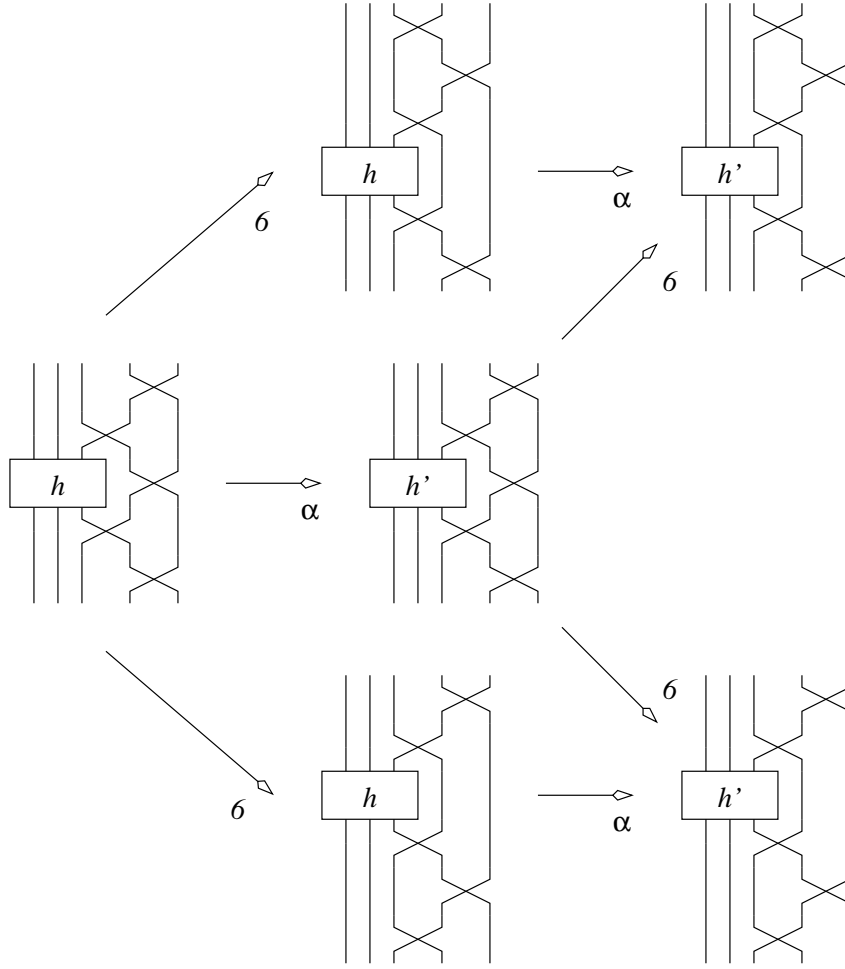


FIG. 5.8 – Réduction de la paire critique entre 6 et 6 indexée par h en la paire critique entre 6 et 6 indexée par h' dans le cas où $h \rightarrow_\alpha h'$.

Confluence des paires critiques de (Δ, R_Δ) . Avec la même démarche, on calcule toutes les paires critiques engendrées par les autres couples de règles. La plupart en produisent un nombre fini. Seuls les couples $(1, 8)$, $(6, 8)$, $(6, 11)$, $(6, 12)$ et $(7, 8)$ se comportent comme $(6, 6)$ en créant des familles infinies de paires critiques $(p_h)_{h \in H}$. On montre, exactement de la même façon, qu'il suffit de considérer les p_h où h est une R_Δ -forme normale : par suite, il suffit de considérer les paires critiques indexées par 1 , δ , τ et $1 \otimes \varepsilon$.

On conclut donc que la confluence locale de (Δ, R_Δ) est équivalente à la confluence des soixante-quatorze paires critiques que nous allons examiner maintenant. Pour la première, nous donnons, en plus du calcul littéral, une version en diagrammes de Penrose du graphe de réduction.

$\text{cp}(1, 1)$. On peut appliquer 1 à deux endroits différents dans $(2 \otimes \delta) \circ (1 \otimes \delta) \circ \delta$:

$$\begin{aligned} (2 \otimes \delta) \circ (1 \otimes \delta) \circ \delta &\rightarrow_1 (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \circ \delta \\ &\rightarrow_1 (1 \otimes \delta \otimes 1) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_1 (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta ; \end{aligned}$$

$$\begin{aligned} (2 \otimes \delta) \circ (1 \otimes \delta) \circ \delta &\rightarrow_1 (\delta \otimes \delta) \circ \delta \\ &\rightarrow_1 (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta. \end{aligned}$$

La figure 5.9 donne une version diagrammatique de ces réductions.

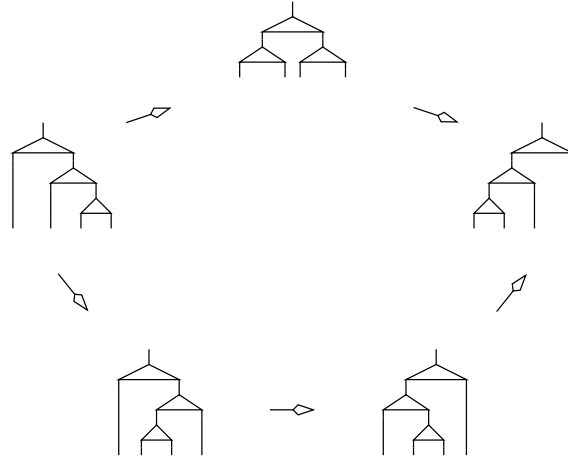


FIG. 5.9 – Graphe de réduction montrant la confluence du branchement associé à la paire critique créée par $(1, 1)$.

cp(1,2). Il y a deux paires critiques, l'une de source $(\varepsilon \otimes \delta) \circ \delta$ et l'autre de source $(1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \delta) \circ \delta$.

$$\begin{aligned} (\varepsilon \otimes \delta) \circ \delta &\rightarrow_1 (\varepsilon \otimes 2) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_2 \delta ; \end{aligned}$$

$$(\varepsilon \otimes \delta) \circ \delta \rightarrow_2 \delta.$$

$$\begin{aligned} (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \delta) \circ \delta &\rightarrow_1 (1 \otimes \varepsilon \otimes 1) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_3 \delta ; \end{aligned}$$

$$(1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \delta) \circ \delta \rightarrow_2 \delta.$$

cp(1,3). Une paire critique qui commence en $(2 \otimes \varepsilon) \circ (1 \otimes \delta) \circ \delta$:

$$\begin{aligned} (2 \otimes \varepsilon) \circ (1 \otimes \delta) \circ \delta &\rightarrow_1 (\delta \otimes \varepsilon) \circ \delta \\ &\rightarrow_3 \delta ; \end{aligned}$$

$$(2 \otimes \varepsilon) \circ (1 \otimes \delta) \circ \delta \rightarrow_3 \delta.$$

cp(1,4). Une paire critique en $(1 \otimes \tau) \circ (1 \otimes \delta) \circ \delta$:

$$\begin{aligned} (1 \otimes \tau) \circ (1 \otimes \delta) \circ \delta &\rightarrow_1 (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_{11} (\delta \otimes 1) \circ \delta ; \end{aligned}$$

$$\begin{aligned} (1 \otimes \tau) \circ (1 \otimes \delta) \circ \delta &\rightarrow_4 (1 \otimes \delta) \circ \delta \\ &\rightarrow_1 (\delta \otimes 1) \circ \delta. \end{aligned}$$

cp(1,7). Une paire critique en $(2 \otimes \delta) \circ (1 \otimes \delta) \circ \tau$:

$$\begin{aligned} (2 \otimes \delta) \circ (1 \otimes \delta) \circ \tau &\rightarrow_1 (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \circ \tau \\ &\rightarrow_7 (1 \otimes \delta \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\ &\rightarrow_7 (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\delta \otimes 1) ; \end{aligned}$$

$$\begin{aligned} (2 \otimes \delta) \circ (1 \otimes \delta) \circ \tau &\rightarrow_7 (\tau \otimes \delta) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\ &\rightarrow_7 (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (\delta \otimes 1) \\ &\rightarrow_1 (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\delta \otimes 1). \end{aligned}$$

cp(1, 8). Quatre paires critiques :

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \circ \delta \\
 \rightarrow_1 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (\delta \otimes 1) \circ \delta \\
 \rightarrow_4 & (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\
 \rightarrow_{11} & (\delta \otimes 1) \circ \delta ;
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \circ \delta \\
 \rightarrow_8 & (\delta \otimes 1) \circ \tau \circ \delta \\
 \rightarrow_4 & (\delta \otimes 1) \circ \delta.
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \delta) \circ \delta \\
 \rightarrow_1 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta \\
 \rightarrow_{11} & (\delta \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\
 \rightarrow_{11} & (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta ;
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \delta) \circ \delta \\
 \rightarrow_8 & (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\
 \rightarrow_{11} & (1 \otimes \delta \otimes 1) \circ (\delta \otimes 1) \circ \delta \\
 \rightarrow_1 & (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta.
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \delta) \circ (1 \otimes \delta) \\
 \rightarrow_1 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_8 & (\delta \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_8 & (\delta \otimes 2) \circ (\delta \otimes 1) \circ \tau ;
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \delta) \circ (1 \otimes \delta) \\
 \rightarrow_8 & (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_8 & (1 \otimes \delta \otimes 1) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_1 & (\delta \otimes 2) \circ (\delta \otimes 1) \circ \tau.
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes \delta) \circ (1 \otimes \delta) \\
 & \rightarrow_1 (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \\
 & \rightarrow_2 (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 & \rightarrow_8 (\delta \otimes 1) \circ \tau ;
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes \delta) \circ (1 \otimes \delta) \\
 & \rightarrow_8 (\delta \otimes 1) \circ \tau \circ (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \delta) \\
 & \rightarrow_2 (\delta \otimes 1) \circ \tau.
 \end{aligned}$$

cp(1, 11). Une paire critique en $(2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \circ \delta$:

$$\begin{aligned}
 (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \circ \delta & \rightarrow_1 (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (\delta \otimes 1) \circ \delta \\
 & \rightarrow_1 (\delta \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\
 & \rightarrow_{11} (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta ;
 \end{aligned}$$

$$\begin{aligned}
 (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \circ \delta & \rightarrow_{11} (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \circ \delta \\
 & \rightarrow_1 (1 \otimes \delta \otimes 1) \circ (\delta \otimes 1) \circ \delta \\
 & \rightarrow_1 (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta.
 \end{aligned}$$

cp(2, 3). Une paire critique en $(\varepsilon \otimes \varepsilon) \circ \delta$. Que l'on applique 2 ou 3, on arrive à ε .

cp(2, 7). Une paire critique en $(1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \delta) \circ \tau$:

$$(1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \delta) \circ \tau \rightarrow_2 \tau ;$$

$$\begin{aligned}
 (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \delta) \circ \tau & \rightarrow_7 (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\
 & \rightarrow_9 (\varepsilon \otimes \tau) \circ (\delta \otimes 1) \\
 & \rightarrow_2 \tau.
 \end{aligned}$$

cp(2, 11). Une paire critique en $(\varepsilon \otimes \tau) \circ (\delta \otimes 1) \circ \delta$:

$$\begin{aligned}
 (\varepsilon \otimes \tau) \circ (\delta \otimes 1) \circ \delta & \rightarrow_2 \tau \circ \delta \\
 & \rightarrow_4 \delta ;
 \end{aligned}$$

$$\begin{aligned}
 (\varepsilon \otimes \tau) \circ (\delta \otimes 1) \circ \delta & \rightarrow_{11} (\varepsilon \otimes 2) \circ (\delta \otimes 1) \circ \delta \\
 & \rightarrow_2 \delta.
 \end{aligned}$$

cp(2, 12). Une paire critique en $(\varepsilon \otimes 2) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau$:

$$\begin{aligned} (\varepsilon \otimes 2) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau &\rightarrow_2 \tau \circ \tau \\ &\rightarrow_5 2; \end{aligned}$$

$$\begin{aligned} (\varepsilon \otimes 2) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau &\rightarrow_{12} (\varepsilon \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\ &\rightarrow_{10} (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \delta) \\ &\rightarrow_2 2. \end{aligned}$$

cp(3, 7). Une paire critique en $(2 \otimes \varepsilon) \circ (1 \otimes \delta) \circ \tau$:

$$(2 \otimes \varepsilon) \circ (1 \otimes \delta) \circ \tau \rightarrow_3 \tau;$$

$$\begin{aligned} (2 \otimes \varepsilon) \circ (1 \otimes \delta) \circ \tau &\rightarrow_7 (\tau \otimes \varepsilon) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\ &\rightarrow_9 \tau \circ (1 \otimes \varepsilon \otimes 1) \circ (\delta \otimes 1) \\ &\rightarrow_3 \tau. \end{aligned}$$

cp(4, 5). Une paire critique en $\tau \circ \tau \circ \delta$:

$$\begin{aligned} \tau \circ \tau \circ \delta &\rightarrow_4 \tau \circ \delta \\ &\rightarrow_4 \delta; \end{aligned}$$

$$\tau \circ \tau \circ \delta \rightarrow_5 \delta.$$

cp(4, 6). Une paire critique en $(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (1 \otimes \delta)$:

$$\begin{aligned} (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (1 \otimes \delta) &\rightarrow_4 (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\ &\rightarrow_8 (\delta \otimes 1) \circ \tau; \end{aligned}$$

$$\begin{aligned} (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (1 \otimes \delta) &\rightarrow_6 (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\ &\rightarrow_8 (\tau \otimes 1) \circ (\delta \otimes 1) \circ \tau \\ &\rightarrow_4 (\delta \otimes 1) \circ \tau. \end{aligned}$$

cp(4, 7). Deux paires critiques :

$$\begin{aligned} (1 \otimes \delta) \circ \tau \circ \delta &\rightarrow_4 (1 \otimes \delta) \circ \delta \\ &\rightarrow_1 (\delta \otimes 1) \circ \delta; \end{aligned}$$

$$\begin{aligned} (1 \otimes \delta) \circ \tau \circ \delta &\rightarrow_7 (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_{11} (\tau \otimes 1) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_4 (\delta \otimes 1) \circ \delta. \end{aligned}$$

$$\begin{aligned} (1 \otimes \tau) \circ (1 \otimes \delta) \circ \tau &\rightarrow_4 (1 \otimes \delta) \circ \tau \\ &\rightarrow_7 (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1); \end{aligned}$$

$$\begin{aligned} (1 \otimes \tau) \circ (1 \otimes \delta) \circ \tau &\rightarrow_7 (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\ &\rightarrow_6 (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (\delta \otimes 1) \\ &\rightarrow_4 (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1). \end{aligned}$$

cp(4, 9). Une paire critique en $(1 \otimes \varepsilon) \circ \tau \circ \delta$:

$$\begin{aligned} (1 \otimes \varepsilon) \circ \tau \circ \delta &\rightarrow_4 (1 \otimes \varepsilon) \circ \delta \\ &\rightarrow_3 1; \end{aligned}$$

$$\begin{aligned} (1 \otimes \varepsilon) \circ \tau \circ \delta &\rightarrow_9 (\varepsilon \otimes 1) \circ \delta \\ &\rightarrow_2 1. \end{aligned}$$

cp(4, 10). Une paire critique en $(\varepsilon \otimes 1) \circ \tau \circ \delta$:

$$\begin{aligned} (\varepsilon \otimes 1) \circ \tau \circ \delta &\rightarrow_4 (\varepsilon \otimes 1) \circ \delta \\ &\rightarrow_2 1; \end{aligned}$$

$$\begin{aligned} (\varepsilon \otimes 1) \circ \tau \circ \delta &\rightarrow_{10} (1 \otimes \varepsilon) \circ \delta \\ &\rightarrow_3 1. \end{aligned}$$

cp(4, 12). Une paire critique en $(1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \circ \delta$:

$$\begin{aligned} (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \circ \delta &\rightarrow_4 (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_{11} (\delta \otimes 1) \circ \delta; \end{aligned}$$

$$\begin{aligned} (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \circ \delta &\rightarrow_{12} (\tau \otimes 1) \circ (1 \otimes \delta) \circ \delta \\ &\rightarrow_1 (\tau \otimes 1) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_4 (\delta \otimes 1) \circ \delta. \end{aligned}$$

cp(5, 5). On peut appliquer la règle 5 à deux endroits différents de $\tau \circ \tau \circ \tau$ mais les deux réductions donnent τ .

cp(5,6). Ces deux règles forment deux paires critiques :

$$(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (1 \otimes \tau) \rightarrow_5 (1 \otimes \tau) \circ (\tau \otimes 1) ;$$

$$\begin{aligned} (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (1 \otimes \tau) &\rightarrow_6 (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\ &\rightarrow_6 (\tau \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\ &\rightarrow_5 (1 \otimes \tau) \circ (\tau \otimes 1). \end{aligned}$$

$$(1 \otimes \tau) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \rightarrow_5 (\tau \otimes 1) \circ (1 \otimes \tau) ;$$

$$\begin{aligned} (1 \otimes \tau) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) &\rightarrow_6 (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\ &\rightarrow_6 (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (\tau \otimes 1) \\ &\rightarrow_5 (\tau \otimes 1) \circ (1 \otimes \tau). \end{aligned}$$

cp(5,7). Une paire critique en $(1 \otimes \delta) \circ \tau \circ \tau$:

$$(1 \otimes \delta) \circ \tau \circ \tau \rightarrow_5 1 \otimes \delta ;$$

$$\begin{aligned} (1 \otimes \delta) \circ \tau \circ \tau &\rightarrow_7 (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\ &\rightarrow_{12} (\tau \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\ &\rightarrow_5 1 \otimes \delta. \end{aligned}$$

cp(5,8). Une paire critique en $(1 \otimes \tau) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta)$:

$$(1 \otimes \tau) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \rightarrow_5 (\tau \otimes 1) \circ (1 \otimes \delta) ;$$

$$\begin{aligned} (1 \otimes \tau) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) &\rightarrow_8 (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\ &\rightarrow_{12} (\tau \otimes 1) \circ (1 \otimes \delta). \end{aligned}$$

cp(5,9). Une paire critique en $(1 \otimes \varepsilon) \circ \tau \circ \tau$:

$$(1 \otimes \varepsilon) \circ \tau \circ \tau \rightarrow_5 1 \otimes \varepsilon ;$$

$$\begin{aligned} (1 \otimes \varepsilon) \circ \tau \circ \tau &\rightarrow_9 (\varepsilon \otimes 1) \circ \tau \\ &\rightarrow_{10} 1 \otimes \varepsilon. \end{aligned}$$

cp(5, 10). Une paire critique en $(\varepsilon \otimes 1) \circ \tau \circ \tau$:

$$(\varepsilon \otimes 1) \circ \tau \circ \tau \rightarrow_5 \varepsilon \otimes 1 ;$$

$$\begin{aligned} (\varepsilon \otimes 1) \circ \tau \circ \tau &\rightarrow_{10} (1 \otimes \varepsilon) \circ \tau \\ &\rightarrow_9 \varepsilon \otimes 1. \end{aligned}$$

cp(5, 11). Une paire critique en $(1 \otimes \tau) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta$:

$$(1 \otimes \tau) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \rightarrow_5 (\delta \otimes 1) \circ \delta ;$$

$$\begin{aligned} (1 \otimes \tau) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta &\rightarrow_{11} (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_{11} (\delta \otimes 1) \circ \delta. \end{aligned}$$

cp(5, 12). Deux paires critiques :

$$(1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \circ \tau \rightarrow_5 (1 \otimes \tau) \circ (\delta \otimes 1) ;$$

$$\begin{aligned} (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \circ \tau &\rightarrow_{12} (\tau \otimes 1) \circ (1 \otimes \delta) \circ \tau \\ &\rightarrow_7 (\tau \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\ &\rightarrow_5 (1 \otimes \tau) \circ (\delta \otimes 1). \end{aligned}$$

$$(1 \otimes \tau) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \rightarrow_5 (\delta \otimes 1) \circ \tau ;$$

$$\begin{aligned} (1 \otimes \tau) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau &\rightarrow_{12} (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\ &\rightarrow_8 (\delta \otimes 1) \circ \tau. \end{aligned}$$

cp(6, 6). Quatre paires critiques :

$$\begin{aligned} &(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\ &\rightarrow_6 (1 \otimes \tau) \circ (\tau \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\ &\rightarrow_5 (1 \otimes \tau) \circ \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\ &\rightarrow_5 \tau \otimes 1 ; \end{aligned}$$

$$\begin{aligned} &(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\ &\rightarrow_6 (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\ &\rightarrow_5 (\tau \otimes 1) \circ (1 \otimes \tau) \circ (1 \otimes \tau) \\ &\rightarrow_5 \tau \otimes 1. \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_6 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\
 \rightarrow_{12} & (\tau \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\
 \rightarrow_{12} & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \delta) ;
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_6 & (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_{12} & (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_{12} & (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \delta) \\
 \rightarrow_6 & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \delta).
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \\
 \rightarrow_6 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \\
 \rightarrow_6 & (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \\
 \rightarrow_6 & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \\
 \rightarrow_6 & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) ;
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \\
 \rightarrow_6 & (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \\
 \rightarrow_6 & (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \\
 \rightarrow_6 & (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \\
 \rightarrow_6 & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2).
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \\
 \rightarrow_6 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \\
 \rightarrow_{10} & (1 \otimes \tau) \circ (\tau \otimes \varepsilon \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \\
 \rightarrow_{10} & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau \otimes \varepsilon) \\
 \rightarrow_6 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1 \otimes \varepsilon) ;
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \\
 \rightarrow_6 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \\
 \rightarrow_{10} & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes \varepsilon \otimes 1) \circ (2 \otimes \tau) \\
 \rightarrow_{10} & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1 \otimes \varepsilon).
 \end{aligned}$$

cp(6, 7). Une paire critique en $(2 \otimes \delta) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau)$:

$$\begin{aligned}
 & (2 \otimes \delta) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_6 & (2 \otimes \delta) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\
 \rightarrow_7 & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (\tau \otimes 1) \\
 \rightarrow_7 & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) ;
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \delta) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_7 & (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_7 & (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \\
 \rightarrow_6 & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2).
 \end{aligned}$$

cp(6, 8). Quatre paires critiques :

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_6 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_5 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (1 \otimes \delta) \\
 \rightarrow_4 & (\tau \otimes 1) \circ (1 \otimes \delta) ;
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_8 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_4 & (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_{12} & (\tau \otimes 1) \circ (1 \otimes \delta).
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_6 & (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_{12} & (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_{11} & (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_8 & (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \delta) ;
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_8 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_{11} & (\delta \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_{12} & (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \delta).
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \delta) \\
 \rightarrow_6 & (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \delta) \\
 \rightarrow_6 & (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \delta) \\
 \rightarrow_8 & (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\
 \rightarrow_8 & (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) ;
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \delta) \\
 \rightarrow_8 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_8 & (\delta \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_6 & (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1).
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \delta) \\
 \rightarrow_6 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \delta) \\
 \rightarrow_{10} & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes \varepsilon \otimes 1) \circ (2 \otimes \delta) \\
 \rightarrow_2 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) ;
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \delta) \\
 \rightarrow_8 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_2 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_6 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1).
 \end{aligned}$$

cp(6, 9). Une paire critique en $(2 \otimes \varepsilon) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau)$:

$$\begin{aligned} (2 \otimes \varepsilon) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) &\rightarrow_6 (2 \otimes \varepsilon) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\ &\rightarrow_9 \tau \circ (1 \otimes \varepsilon \otimes 1) \circ (\tau \otimes 1) \\ &\rightarrow_9 \varepsilon \otimes \tau ; \end{aligned}$$

$$\begin{aligned} (2 \otimes \varepsilon) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) &\rightarrow_9 (1 \otimes \varepsilon \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\ &\rightarrow_9 \varepsilon \otimes \tau. \end{aligned}$$

cp(6, 10). Deux paires critiques :

$$\begin{aligned} (\varepsilon \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) &\rightarrow_6 (\varepsilon \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\ &\rightarrow_{10} (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\ &\rightarrow_{10} \tau \otimes \varepsilon ; \end{aligned}$$

$$\begin{aligned} (\varepsilon \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) &\rightarrow_{10} \tau \circ (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \\ &\rightarrow_{10} \tau \otimes \varepsilon. \end{aligned}$$

$$\begin{aligned} (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) &\rightarrow_6 (1 \otimes \varepsilon \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\ &\rightarrow_9 (\varepsilon \otimes 2) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\ &\rightarrow_{10} \tau \circ (1 \otimes \varepsilon \otimes 1) ; \end{aligned}$$

$$\begin{aligned} (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) &\rightarrow_{10} (2 \otimes \varepsilon) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\ &\rightarrow_9 \tau \circ (1 \otimes \varepsilon \otimes 1). \end{aligned}$$

cp(6, 11). Quatre paires critiques :

$$\begin{aligned} (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta &\rightarrow_6 (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_4 (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_{11} (\tau \otimes 1) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_4 (\delta \otimes 1) \circ \delta ; \end{aligned}$$

$$\begin{aligned} (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta &\rightarrow_{11} (1 \otimes \tau) \circ (\tau \otimes 1) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_4 (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_{11} (\delta \otimes 1) \circ \delta. \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\
 \rightarrow_6 & (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta \\
 \rightarrow_{11} & (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta \\
 \rightarrow_{11} & (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta \\
 \rightarrow_{11} & (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta ;
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\
 \rightarrow_{11} & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta \\
 \rightarrow_{11} & (\delta \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\
 \rightarrow_{11} & (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta.
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_6 & (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_8 & (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_8 & (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_{11} & (\delta \otimes 2) \circ (\delta \otimes 1) \circ \tau ;
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_{11} & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_8 & (\delta \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_8 & (\delta \otimes 2) \circ (\delta \otimes 1) \circ \tau.
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_6 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_2 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_8 & (\tau \otimes 1) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_4 & (\delta \otimes 1) \circ \tau ;
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_{11} & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_2 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_8 & (\delta \otimes 1) \circ \tau.
 \end{aligned}$$

$\text{cp}(6, 12)$. Cinq paires critiques :

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_6 & (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\
 \rightarrow_7 & (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\tau \otimes 1) \\
 \rightarrow_6 & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\tau \otimes 1) \\
 \rightarrow_{12} & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \delta \otimes 1) ;
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_{12} & (1 \otimes \tau \otimes 1) \circ (2 \otimes \delta) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_7 & (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \\
 \rightarrow_6 & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \delta \otimes 1).
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_6 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_4 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_{12} & (\tau \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_5 & 1 \otimes \delta ;
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_{12} & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_5 & (1 \otimes \tau) \circ (1 \otimes \delta) \\
 \rightarrow_4 & 1 \otimes \delta.
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_6 & (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_{11} & (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (\delta \otimes 2) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_{12} & (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_{12} & (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) ;
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_{12} & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_{12} & (\tau \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_{11} & (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta).
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_6 & (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_8 & (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_6 & (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\
 \rightarrow_{12} & (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) ;
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_{12} & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \delta) \\
 \rightarrow_6 & (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \delta) \\
 \rightarrow_8 & (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1).
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_6 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_2 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_6 & (\tau \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\
 \rightarrow_5 & (1 \otimes \tau) \circ (\tau \otimes 1) ;
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_{12} & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \delta) \\
 \rightarrow_{10} & (1 \otimes \tau) \circ (\tau \otimes \varepsilon \otimes 1) \circ (2 \otimes \delta) \\
 \rightarrow_2 & (1 \otimes \tau) \circ (\tau \otimes 1).
 \end{aligned}$$

cp(7, 8). Cinq paires critiques :

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \circ \tau \\
 \rightarrow_7 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\
 \rightarrow_5 & (1 \otimes \tau) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\
 \rightarrow_5 & \delta \otimes 1 ;
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \circ \tau \\
 \rightarrow_8 & (\delta \otimes 1) \circ \tau \circ \tau \\
 \rightarrow_5 & \delta \otimes 1.
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \delta) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_{\tau} & (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_{\tau} & (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \delta) \\
 \rightarrow_8 & (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\
 \rightarrow_8 & (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1);
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \delta) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_8 & (\delta \otimes \delta) \circ \tau \\
 \rightarrow_{\tau} & (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1).
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \delta) \circ \tau \\
 \rightarrow_{\tau} & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\
 \rightarrow_{12} & (\tau \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\
 \rightarrow_{12} & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \delta);
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \delta) \circ \tau \\
 \rightarrow_8 & (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\
 \rightarrow_{12} & (1 \otimes \delta \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 \rightarrow_{\tau} & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \delta).
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \delta) \circ (1 \otimes \tau) \\
 \rightarrow_{\tau} & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \\
 \rightarrow_6 & (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \tau) \circ (1 \otimes \delta \otimes 1) \\
 \rightarrow_6 & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \\
 \rightarrow_8 & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\tau \otimes 1);
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\tau \otimes \delta) \circ (1 \otimes \tau) \\
 \rightarrow_8 & (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \\
 \rightarrow_6 & (1 \otimes \delta \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \\
 \rightarrow_{\tau} & (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\tau \otimes 1).
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes \delta) \circ (1 \otimes \tau) \\
 & \rightarrow_7 (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \\
 & \rightarrow_{10} (1 \otimes \tau) \circ (\tau \otimes \varepsilon \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \\
 & \rightarrow_{10} (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta \otimes \varepsilon) \\
 & \rightarrow_8 (\delta \otimes 1) \circ (\tau \otimes \varepsilon) ;
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \varepsilon \otimes \delta) \circ (1 \otimes \tau) \\
 & \rightarrow_8 (\delta \otimes 1) \circ \tau \circ (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \\
 & \rightarrow_{10} (\delta \otimes 1) \circ (\tau \otimes \varepsilon).
 \end{aligned}$$

cp(7, 10). Une paire critique en $(\varepsilon \otimes \delta) \circ \tau$:

$$\begin{aligned}
 (\varepsilon \otimes \delta) \circ \tau & \rightarrow_7 (\varepsilon \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\
 & \rightarrow_{10} (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\
 & \rightarrow_{10} \delta \otimes \varepsilon ;
 \end{aligned}$$

$$(\varepsilon \otimes \delta) \circ \tau \rightarrow_{10} \delta \otimes \varepsilon.$$

cp(7, 11). Deux paires critiques :

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \circ \tau \\
 & \rightarrow_7 (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\
 & \rightarrow_7 (\tau \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (\delta \otimes \tau) \circ (\delta \otimes 1) \\
 & \rightarrow_6 (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\delta \otimes 1) \\
 & \rightarrow_{11} (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\delta \otimes 1) ;
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \circ \tau \\
 & \rightarrow_{11} (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \circ \tau \\
 & \rightarrow_7 (1 \otimes \delta \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\
 & \rightarrow_7 (\tau \otimes 2) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\delta \otimes 1).
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \delta) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\
 & \rightarrow_{\tau} (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (\delta \otimes 1) \circ \delta \\
 & \rightarrow_1 (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\
 & \rightarrow_{11} (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta \\
 & \rightarrow_{11} (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta ;
 \end{aligned}$$

$$\begin{aligned}
 & (2 \otimes \delta) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\
 & \rightarrow_{11} (\delta \otimes \delta) \circ \delta \\
 & \rightarrow_1 (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta.
 \end{aligned}$$

cp(7, 12). Une paire critique en $(2 \otimes \delta) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau$:

$$\begin{aligned}
 (2 \otimes \delta) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau & \rightarrow_{\tau} (1 \otimes \tau \otimes 1) \circ (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (\delta \otimes 1) \circ \tau \\
 & \rightarrow_1 (1 \otimes \tau \otimes 1) \circ (\delta \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\
 & \rightarrow_{12} (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 & \rightarrow_{12} (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) ;
 \end{aligned}$$

$$\begin{aligned}
 (2 \otimes \delta) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau & \rightarrow_{12} (\tau \otimes \delta) \circ (1 \otimes \delta) \\
 & \rightarrow_1 (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta).
 \end{aligned}$$

cp(8, 9). Une paire critique en $(2 \otimes \varepsilon) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta)$:

$$\begin{aligned}
 (2 \otimes \varepsilon) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) & \rightarrow_8 (\delta \otimes \varepsilon) \circ \tau \\
 & \rightarrow_9 \varepsilon \otimes \delta ;
 \end{aligned}$$

$$\begin{aligned}
 (2 \otimes \varepsilon) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) & \rightarrow_9 (1 \otimes \varepsilon \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\
 & \rightarrow_9 \varepsilon \otimes \delta.
 \end{aligned}$$

cp(8, 10). Deux paires critiques :

$$\begin{aligned}
 (\varepsilon \otimes 2) \circ (1 \otimes \tau) \circ (1 \otimes \delta) & \rightarrow_8 (\varepsilon \otimes 2) \circ (\delta \otimes 1) \circ \tau \\
 & \rightarrow_2 \tau ;
 \end{aligned}$$

$$\begin{aligned}
 (\varepsilon \otimes 2) \circ (1 \otimes \tau) \circ (1 \otimes \delta) & \rightarrow_{10} \tau \circ (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \delta) \\
 & \rightarrow_2 \tau.
 \end{aligned}$$

$$(1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \rightarrow_8 (1 \otimes \varepsilon \otimes 1) \circ (\delta \otimes 1) \circ \tau \\ \rightarrow_3 \tau ;$$

$$(1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \rightarrow_{10} (\tau \otimes \varepsilon) \circ (1 \otimes \delta) \\ \rightarrow_3 \tau.$$

cp(8, 12). Une paire critique en $(2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta)$:

$$(2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\ \rightarrow_8 (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (\delta \otimes 1) \circ \tau \\ \rightarrow_1 (\delta \otimes \tau) \circ (\delta \otimes 1) \circ \tau \\ \rightarrow_{12} (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \delta) ;$$

$$(2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\ \rightarrow_{12} (1 \otimes \tau \otimes 1) \circ (\tau \otimes \delta) \circ (1 \otimes \delta) \\ \rightarrow_1 (1 \otimes \tau \otimes 1) \circ (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \delta) \\ \rightarrow_8 (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \delta).$$

cp(9, 10). On peut appliquer les deux règles 9 et 10 en $(\varepsilon \otimes \varepsilon) \circ \tau$ pour obtenir, dans les deux cas, $\varepsilon \otimes \varepsilon$.

cp(9, 11). Une paire critique en $(2 \otimes \varepsilon) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta$:

$$(2 \otimes \varepsilon) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \rightarrow_9 (1 \otimes \varepsilon \otimes 1) \circ (\delta \otimes 1) \circ \delta \\ \rightarrow_3 \delta ;$$

$$(2 \otimes \varepsilon) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \rightarrow_{11} (2 \otimes \varepsilon) \circ (\delta \otimes 1) \circ \delta \\ \rightarrow_3 \delta.$$

cp(9, 12). Une paire critique en $(2 \otimes \varepsilon) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau$:

$$(2 \otimes \varepsilon) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \rightarrow_9 (1 \otimes \varepsilon \otimes 1) \circ (\delta \otimes 1) \circ \tau \\ \rightarrow_3 \tau ;$$

$$(2 \otimes \varepsilon) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \rightarrow_{12} (\tau \otimes \varepsilon) \circ (1 \otimes \delta) \\ \rightarrow_3 \tau.$$

cp(10, 11). Une paire critique en $(1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta$:

$$\begin{aligned} (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta &\rightarrow_{10} (\delta \otimes \varepsilon) \circ \delta \\ &\rightarrow_3 \delta ; \end{aligned}$$

$$\begin{aligned} (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta &\rightarrow_{11} (1 \otimes \varepsilon \otimes 1) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_3 \delta . \end{aligned}$$

cp(10, 12). Une paire critique en $(1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau$:

$$\begin{aligned} (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau &\rightarrow_{10} (\delta \otimes \varepsilon) \circ \tau \\ &\rightarrow_9 \varepsilon \otimes \delta ; \end{aligned}$$

$$\begin{aligned} (1 \otimes \varepsilon \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau &\rightarrow_{12} (1 \otimes \varepsilon \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\ &\rightarrow_9 \varepsilon \otimes \delta . \end{aligned}$$

cp(11, 12). Une paire critique en $(2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta$:

$$\begin{aligned} (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta &\rightarrow_{11} (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_1 (\delta \otimes \tau) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_{11} (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta ; \end{aligned}$$

$$\begin{aligned} (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta &\rightarrow_{12} (1 \otimes \tau \otimes 1) \circ (\delta \otimes \delta) \circ \delta \\ &\rightarrow_1 (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta \\ &\rightarrow_{11} (\delta \otimes 2) \circ (\delta \otimes 1) \circ \delta . \end{aligned}$$

cp(12, 12). Une paire critique en $(2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau$:

$$\begin{aligned} (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau &\rightarrow_{12} (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \\ &\rightarrow_7 (\tau \otimes \tau) \circ (1 \otimes \tau \otimes 1) \circ (\delta \otimes \delta) \\ &\rightarrow_8 (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) ; \end{aligned}$$

$$\begin{aligned} (2 \otimes \tau) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau &\rightarrow_{12} (1 \otimes \tau \otimes 1) \circ (\delta \otimes \delta) \circ \tau \\ &\rightarrow_7 (1 \otimes \tau \otimes 1) \circ (\delta \otimes 2) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \\ &\rightarrow_{12} (\tau \otimes 2) \circ (1 \otimes \delta \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) . \end{aligned}$$

On a donc la confluence locale de (Δ, R_Δ) et, à l'aide du lemme de Newman, le résultat :

Proposition 5.28. *La présentation (Δ, R_Δ) est convergente.*

L'opérade \mathbb{F}^o et ses algèbres

Nous allons faire une digression sur la présentation (Δ, R_Δ) , qui nous sera utile pour prouver la confluence de $(\Sigma^c, R_{\Delta, \Sigma})$. Il s'agit de rappeler le résultat suivant, démontré par Albert Burroni dans [Bur93] :

Proposition 5.29. *Le couple (Δ, R_Δ) est une présentation de l'opérade \mathbb{F}^o dite des ensembles et définie par :*

$$\mathbb{F}(m, n) = \mathbb{E}_{\text{NS}}([m], [n]).$$

Son nom est dû au résultat suivant :

Proposition 5.30. *Tout ensemble X est une \mathbb{F}^o -algèbre libre.*

Démonstration. Il s'agit de vérifier que l'on peut bien associer à ε , δ et τ des opérations sur X qui vérifient les relations de R_Δ . Les images nous sont données par le produit cartésien de \mathbb{E}_{NS} . En effet, il induit des applications $\varepsilon_X : X \longrightarrow \{*\}$, $\delta_X : X \longrightarrow X^2$ et $\tau_X : X^2 \longrightarrow X^2$ définies par :

$$\varepsilon_X(x) = * \quad \delta_X(x) = (x, x) \quad \tau_X(x, y) = (y, x).$$

En envoyant chacune des trois flèches de Δ sur la flèche correspondante ci-dessus et en appliquant la propriété universelle d'opérade libre engendrée par Δ , on obtient un morphisme d'opérades $\mathcal{L}\Delta \longrightarrow \text{Oper } X$, c'est-à-dire une structure de $\mathcal{L}\Delta$ -algèbre sur X . Il faut alors vérifier que ce morphisme passe au quotient par R_Δ , ce qui ne pose aucune difficulté. Il est tout aussi aisé de se convaincre que ce morphisme est la \mathbb{F}^o -algèbre libre engendrée par X . \diamond

Ainsi, on en conclut que :

Corollaire 5.31. *Deux flèches $f, g \in \mathcal{L}\Delta(m, n)$ vérifient $f \equiv_{R_\Delta} g$ si et seulement si, pour tout ensemble X possédant au moins m éléments et pour tous $x_1, \dots, x_m \in X$, on a : $f(x_1, \dots, x_m) = g(x_1, \dots, x_m)$.*

Confluence de $(\Sigma^c, R_{\Delta, \Sigma})$

On doit maintenant examiner les paires critiques de $(\Sigma^c, R_{\Delta, \Sigma})$. Elles sont de trois types : celles associées à deux règles de $R_{\Sigma/\Delta}$, celles associées à une règle de R_Σ et une règle de $R_{\Sigma/\Delta}$ et celles associées à deux règles de R_Δ . Parmi ces dernières, nous en avons déjà exploré une grande partie ; cependant, la présence de nouveaux générateurs fait que les six familles infinies déjà mentionnées grossissent encore ; mais, comme précédemment, on peut conclure que la confluence de ces nouvelles paires critiques est équivalente à celle de paires critiques déjà examinées.

En effet, comme $(\Sigma^c, R_{\Delta, \Sigma})$ termine, on peut démontrer, en appliquant le principe de récurrence, que l'on peut se limiter, pour chacune des six familles, aux paires critiques indexées par une forme normale de $R_{\Delta, \Sigma}$. Si ces dernières sont toujours en quantité infinie, il est toutefois possible de réduire encore le nombre de paires critiques à étudier. Il est aisé de se convaincre que toutes les formes normales f de $R_{\Delta, \Sigma}$ sont de la forme :

$$f = (h_1 \otimes \cdots \otimes h_m) \circ g,$$

où chaque $h_i \in \mathcal{L}\Sigma(n_i, 1)$ et $g \in \mathcal{L}\Delta(p, n_1 + \cdots + n_m)$ est une R_{Δ} -forme normale. La figure 5.10 montre comment on peut ne considérer que le cas où f est elle-même une R_{Δ} -forme normale de $\mathcal{L}\Delta$.

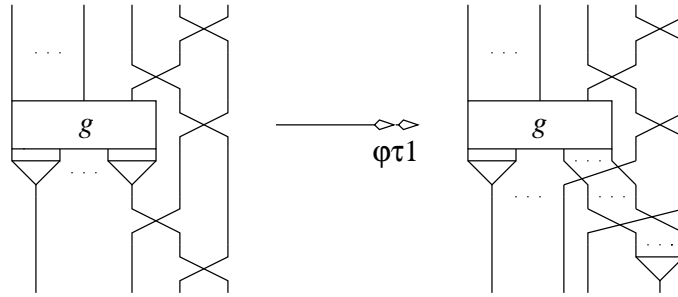


FIG. 5.10 – Réduction d'une paire critique indexée par une $R_{\Delta, \Sigma}$ -forme normale f à une qui est indexée par une R_{Δ} -forme normale g de $\mathcal{L}\Delta$.

Ainsi, on se ramène aux quatre cas déjà étudiés pour chaque famille : les paires critiques indexées par 1 , δ , τ et $1 \otimes \varepsilon$.

Nous allons, dans un premier temps, regarder les paires critiques du deuxième type, les paires *mixtes*. On fixe un entier n et une flèche $f \in \Sigma(n, 1)$. Remarquons que les preuves seront faites dans le cas où n est strictement positif; cependant, on peut aisément les transposer au cas $n = 0$, pour lequel nous rappelons que :

$$\varepsilon^0 = 0, \quad \delta_0 = 0, \quad \tau_{1,0} = \tau_{0,1} = 1.$$

On applique de nouveau la méthode de 3.8.2, qui donne la liste des paires critiques *mixtes* : il y en a vingt pour chaque flèche de Σ .

$\text{cp}(f\delta, 1)$. Une paire critique de sommet $(1 \otimes \delta) \circ \delta \circ f$:

$$\begin{aligned} (1 \otimes \delta) \circ \delta \circ f &\rightarrow_{f\delta} (1 \otimes \delta) \circ (f \otimes f) \circ \delta_n \\ &\rightarrow_{f\delta} (f \otimes f \otimes f) \circ (n \otimes \delta_n) \circ \delta_n ; \end{aligned}$$

$$\begin{aligned} (1 \otimes \delta) \circ \delta \circ f &\rightarrow_1 (\delta \otimes 1) \circ \delta \circ f \\ &\rightarrow_{f\delta} (\delta \otimes 1) \circ (f \otimes f) \circ \delta_n \\ &\rightarrow_{f\delta} (f \otimes f \otimes f) \circ (\delta_n \otimes n) \circ \delta_n . \end{aligned}$$

Ici, deux choix s'offrent à nous : la première possibilité est de démontrer, par récurrence sur n , que $(n \otimes \delta_n) \circ \delta_n$ et $(\delta_n \otimes n) \circ \delta_n$ se réduisent, selon les règles de R_Δ , en une même flèche. Cependant, on a montré que deux flèches parallèles φ et ψ de $\mathcal{L}\Delta$ vérifiaient $\varphi \equiv_{R_\Delta} \psi$ si et seulement si leurs réalisations en tant que flèches de $\text{Oper } X$ coïncidaient, pour un ensemble X assez grand ; à cette fin, on fixera pour la suite de l'étude un ensemble X dénombrable. Ainsi, si on montre que, pour tous x_1, \dots, x_n de X , on a :

$$(n \otimes \delta_n) \circ \delta_n(x_1, \dots, x_n) = (\delta_n \otimes n) \circ \delta_n(x_1, \dots, x_n)$$

on pourra en conclure que $(n \otimes \delta_n) \circ \delta_n \equiv_{R_\Delta} (\delta_n \otimes n) \circ \delta_n$. En utilisant le fait que la présentation (Δ, R_Δ) est convergente, on aura l'existence d'une flèche φ de $\mathcal{L}\Delta(n, 3n)$ telle que :

$$\begin{cases} (n \otimes \delta_n) \circ \delta_n \twoheadrightarrow_{R_\Delta} \varphi \\ (\delta_n \otimes n) \circ \delta_n \twoheadrightarrow_{R_\Delta} \varphi . \end{cases}$$

Et donc :

$$\begin{cases} (f \otimes f \otimes f) \circ (n \otimes \delta_n) \circ \delta_n \twoheadrightarrow_{R_\Delta} (f \otimes f \otimes f) \circ \varphi \\ (f \otimes f \otimes f) \circ (\delta_n \otimes n) \circ \delta_n \twoheadrightarrow_{R_\Delta} (f \otimes f \otimes f) \circ \varphi . \end{cases}$$

Ainsi, on aura prouvé que la paire critique étudiée est confluente. Regardons donc :

$$\begin{aligned} (n \otimes \delta_n) \circ \delta_n(x_1, \dots, x_n) &= (n \otimes \delta_n)(x_1, \dots, x_n, x_1, \dots, x_n) \\ &= (x_1, \dots, x_n, x_1, \dots, x_n, x_1, \dots, x_n) ; \end{aligned}$$

$$\begin{aligned} (\delta_n \otimes n) \circ \delta_n(x_1, \dots, x_n) &= (\delta_n \otimes n)(x_1, \dots, x_n, x_1, \dots, x_n) \\ &= (x_1, \dots, x_n, x_1, \dots, x_n, x_1, \dots, x_n) . \end{aligned}$$

Cette technique va être utilisée dans la plupart des autres cas étudiés, sans justification supplémentaire.

$\text{cp}(f\delta, 2)$. Une paire critique de sommet $(\varepsilon \otimes 1) \circ \delta \circ f$:

$$\begin{aligned} (\varepsilon \otimes 1) \circ \delta \circ f &\rightarrow_{f\delta} (\varepsilon \otimes 1) \circ (f \otimes f) \circ \delta_n \\ &\rightarrow_{f\varepsilon} (\varepsilon^n \otimes f) \circ \delta_n ; \end{aligned}$$

$$(\varepsilon \otimes 1) \circ \delta \circ f \rightarrow_2 f.$$

$$\begin{aligned} (\varepsilon^n \otimes n) \circ \delta_n(x_1, \dots, x_n) &= (\varepsilon^n \otimes n)(x_1, \dots, x_n, x_1, \dots, x_n) \\ &= (x_1, \dots, x_n) \\ &= n(x_1, \dots, x_n). \end{aligned}$$

$\text{cp}(f\delta, 3)$. Une paire critique de sommet $(1 \otimes \varepsilon) \circ \delta \circ f$:

$$\begin{aligned} (1 \otimes \varepsilon) \circ \delta \circ f &\rightarrow_{f\delta} (1 \otimes \varepsilon) \circ (f \otimes f) \circ \delta_n \\ &\rightarrow_{f\varepsilon} (f \otimes \varepsilon^n) \circ \delta_n ; \end{aligned}$$

$$(1 \otimes \varepsilon) \circ \delta \circ f \rightarrow_3 f.$$

$$\begin{aligned} (n \otimes \varepsilon^n) \circ \delta_n(x_1, \dots, x_n) &= (n \otimes \varepsilon^n)(x_1, \dots, x_n, x_1, \dots, x_n) \\ &= (x_1, \dots, x_n) \\ &= n(x_1, \dots, x_n). \end{aligned}$$

$\text{cp}(f\delta, 4)$. Une paire critique en $\tau \circ \delta \circ f$. Cependant, avant de l'étudier, on montre, par récurrence sur un entier m que l'on a :

$$\tau_{m,1} \circ (m \otimes f) \rightarrow_{f\tau_2} (f \otimes m) \circ \tau_{m,n}.$$

En effet, si $m = 0$, on doit vérifier que $f \rightarrow_{f\tau_2} f$, ce qui est toujours vrai. Puis, si on suppose que c'est vrai pour un entier m fixé, on a :

$$\begin{aligned} \tau_{m+1,1} \circ ((m+1) \otimes f) &= (\tau \otimes m) \circ (1 \otimes \tau_{m,1}) \circ (1 \otimes m \otimes f) \\ &\rightarrow_{f\tau_2} (\tau \otimes m) \circ (1 \otimes f \otimes m) \circ (1 \otimes \tau_{m,n}) \\ &\rightarrow_{f\tau_2} (f \otimes 1 \otimes m) \circ (\tau_{1,n} \otimes m) \circ (1 \otimes \tau_{m,n}) \\ &= (f \otimes (m+1)) \circ \tau_{m+1,n}. \end{aligned}$$

Regardons à présent le branchement critique :

$$\begin{aligned}\tau \circ \delta \circ f &\rightarrow_{f\delta} \tau \circ (f \otimes f) \circ \delta_n \\ &\rightarrow_{f\tau 1} (1 \otimes f) \circ \tau_{n,1} \circ (n \otimes f) \circ \delta_n \\ &\rightarrow_{f\tau 2} (f \otimes f) \circ \tau_{n,n} \circ \delta_n ;\end{aligned}$$

$$\begin{aligned}\tau \circ \delta \circ f &\rightarrow_4 \delta \circ f \\ &\rightarrow_{f\delta} (f \otimes f) \circ \delta_n.\end{aligned}$$

$$\begin{aligned}\tau_{n,n} \circ \delta_n(x_1, \dots, x_n) &= \tau_{n,n}(x_1, \dots, x_n, x_1, \dots, x_n) \\ &= (x_1, \dots, x_n, x_1, \dots, x_n) \\ &= \delta_n(x_1, \dots, x_n).\end{aligned}$$

$\text{cp}(f\delta, 8)$. Une paire critique de sommet $(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \circ (1 \otimes f)$:

$$\begin{aligned}&(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \circ (1 \otimes f) \\ &\rightarrow_{f\delta} (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes f \otimes f) \circ (1 \otimes \delta_n) \\ &\rightarrow_{f\tau 2} (f \otimes \tau) \circ (\tau_{1,n} \otimes f) \circ (1 \otimes \delta_n) \\ &\rightarrow_{f\tau 2} (f \otimes f \otimes 1) \circ (n \otimes \tau_{1,n}) \circ (\tau_{1,n} \otimes n) \circ (1 \otimes \delta_n) ;\end{aligned}$$

$$\begin{aligned}&(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \delta) \circ (1 \otimes f) \\ &\rightarrow_8 (\delta \otimes 1) \circ \tau \circ (1 \otimes f) \\ &\rightarrow_{f\tau 2} (\delta \otimes 1) \circ (f \otimes 1) \circ \tau_{1,n} \\ &\rightarrow_{f\delta} (f \otimes f \otimes 1) \circ (\delta_n \otimes 1) \circ \tau_{1,n}.\end{aligned}$$

$$\begin{aligned}&(n \otimes \tau_{1,n}) \circ (\tau_{1,n} \otimes n) \circ (1 \otimes \delta_n)(y, x_1, \dots, x_n) \\ &= (n \otimes \tau_{1,n}) \circ (\tau_{1,n} \otimes n)(y, x_1, \dots, x_n, x_1, \dots, x_n) \\ &= (n \otimes \tau_{1,n})(x_1, \dots, x_n, y, x_1, \dots, x_n) \\ &= (x_1, \dots, x_n, x_1, \dots, x_n, y) ;\end{aligned}$$

$$\begin{aligned}&(\delta_n \otimes 1) \circ \tau_{1,n}(y, x_1, \dots, x_n) \\ &= (\delta_n \otimes 1)(x_1, \dots, x_n, y) \\ &= (x_1, \dots, x_n, x_1, \dots, x_n, y).\end{aligned}$$

$\text{cp}(f\delta, 11)$. Une paire critique de sommet $(1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \circ f$:

$$\begin{aligned} (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \circ f &\rightarrow_{f\delta} (1 \otimes \tau) \circ (\delta \otimes 1) \circ (f \otimes f) \circ \delta_n \\ &\rightarrow_{f\delta} (f \otimes \tau) \circ (n \otimes f \otimes 1) \circ (\delta_n \otimes f) \circ \delta_n \\ &\rightarrow_{f\tau_1} (f \otimes 1 \otimes f) \circ (n \otimes \tau_{n,1}) \circ (\delta_n \otimes f) \circ \delta_n \\ &\rightarrow_{f\tau_2} (f \otimes f \otimes f) \circ (n \otimes \tau_{n,n}) \circ (\delta_n \otimes n) \circ \delta_n ; \end{aligned}$$

$$\begin{aligned} (1 \otimes \tau) \circ (\delta \otimes 1) \circ \delta \circ f &\rightarrow_{11} (\delta \otimes 1) \circ \delta \circ f \\ &\rightarrow_{f\delta} (\delta \otimes 1) \circ (f \otimes f) \circ \delta_n \\ &\rightarrow_{f\delta} (f \otimes f \otimes f) \circ (\delta_n \otimes n) \circ \delta_n. \end{aligned}$$

$$\begin{aligned} (n \otimes \tau_{n,n}) \circ (\delta_n \otimes n) \circ \delta_n(x_1 \dots, x_n) &= (n \otimes \tau_{n,n}) \circ (\delta_n \otimes n)(x_1 \dots, x_n, x_1 \dots, x_n) \\ &= (n \otimes \tau_{n,n})(x_1 \dots, x_n, x_1 \dots, x_n, x_1 \dots, x_n) \\ &= (x_1 \dots, x_n, x_1 \dots, x_n, x_1 \dots, x_n) ; \end{aligned}$$

$$\begin{aligned} (\delta_n \otimes n) \circ \delta_n(x_1 \dots, x_n) &= (\delta_n \otimes n)(x_1 \dots, x_n, x_1 \dots, x_n) \\ &= (x_1 \dots, x_n, x_1 \dots, x_n, x_1 \dots, x_n). \end{aligned}$$

$\text{cp}(f\tau 1, 5)$. Une paire critique de sommet $\tau \otimes \tau \otimes (f \otimes 1)$:

$$\begin{aligned} \tau \circ \tau \circ (f \otimes 1) &\rightarrow_{f\tau_1} \tau \circ (1 \otimes f) \circ \tau_{n,1} \\ &\rightarrow_{f\tau_2} (f \otimes 1) \circ \tau_{1,n} \circ \tau_{n,1} ; \end{aligned}$$

$$\tau \circ \tau \circ (f \otimes 1) \rightarrow_5 f \otimes 1.$$

$$\begin{aligned} \tau_{1,n} \circ \tau_{n,1}(x_1, \dots, x_n, y) &= \tau_{1,n}(y, x_1, \dots, x_n) \\ &= (x_1, \dots, x_n, y) \\ &= (n+1)(x_1, \dots, x_n, y). \end{aligned}$$

$\text{cp}(f\tau 1, 6)$. Deux paires critiques. La première est de sommet $(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (1 \otimes f \otimes 1)$:

$$\begin{aligned} & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (1 \otimes f \otimes 1) \\ \rightarrow_{f\tau 1} & (1 \otimes \tau) \circ (\tau \otimes f) \circ (1 \otimes \tau_{n,1}) \\ \rightarrow_{f\tau 2} & (1 \otimes f \otimes 1) \circ (1 \otimes \tau_{1,n}) \circ (\tau \otimes n) \circ (1 \otimes \tau_{n,1}) ; \end{aligned}$$

$$\begin{aligned} & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (1 \otimes f \otimes 1) \\ \rightarrow_6 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes f \otimes 1) \\ \rightarrow_{f\tau 2} & (\tau \otimes 1) \circ (f \otimes \tau) \circ (\tau_{1,n} \otimes 1) \\ \rightarrow_{f\tau 1} & (1 \otimes f \otimes 1) \circ (\tau_{n,1} \otimes 1) \circ (n \otimes \tau) \circ (\tau_{1,n} \otimes 1). \end{aligned}$$

$$\begin{aligned} & (1 \otimes \tau_{1,n}) \circ (\tau \otimes n) \circ (1 \otimes \tau_{n,1})(y, x_1, \dots, x_n, z) \\ = & (1 \otimes \tau_{1,n}) \circ (\tau \otimes n)(y, z, x_1, \dots, x_n) \\ = & (1 \otimes \tau_{1,n})(z, y, x_1, \dots, x_n) \\ = & (z, x_1, \dots, x_n, y) ; \end{aligned}$$

$$\begin{aligned} & (\tau_{n,1} \otimes 1) \circ (n \otimes \tau) \circ (\tau_{1,n} \otimes 1)(y, x_1, \dots, x_n, z) \\ = & (\tau_{n,1} \otimes 1) \circ (n \otimes \tau)(x_1, \dots, x_n, y, z) \\ = & (\tau_{n,1} \otimes 1)(x_1, \dots, x_n, z, y) \\ = & (z, x_1, \dots, x_n, y). \end{aligned}$$

La seconde paire critique a pour sommet $(1 \otimes \tau) \circ (\tau \otimes 1) \circ (f \otimes \tau)$:

$$\begin{aligned} & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (f \otimes \tau) \\ \rightarrow_{f\tau 1} & (1 \otimes \tau) \circ (1 \otimes f \otimes 1) \circ (\tau_{n,1} \otimes 1) \circ (n \otimes \tau) \\ \rightarrow_{f\tau 1} & (2 \otimes f) \circ (1 \otimes \tau_{n,1}) \circ (\tau_{n,1} \otimes 1) \circ (n \otimes \tau) ; \end{aligned}$$

$$\begin{aligned} & (1 \otimes \tau) \circ (\tau \otimes 1) \circ (f \otimes \tau) \\ \rightarrow_6 & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) \circ (f \otimes 2) \\ \rightarrow_{f\tau 1} & (\tau \otimes 1) \circ (1 \otimes \tau) \circ (1 \otimes f \otimes 1) \circ (\tau_{n,1} \otimes 1) \\ \rightarrow_{f\tau 1} & (\tau \otimes f) \circ (1 \otimes \tau_{n,1}) \circ (\tau_{n,1} \otimes 1). \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \tau_{n,1}) \circ (\tau_{n,1} \otimes 1) \circ (n \otimes \tau)(x_1, \dots, x_n, y, z) \\
 &= (1 \otimes \tau_{n,1}) \circ (\tau_{n,1} \otimes 1)(x_1, \dots, x_n, z, y) \\
 &= (1 \otimes \tau_{n,1})(z, x_1, \dots, x_n, y) \\
 &= (z, y, x_1, \dots, x_n);
 \end{aligned}$$

$$\begin{aligned}
 & (\tau \otimes n) \circ (1 \otimes \tau_{n,1}) \circ (\tau_{n,1} \otimes 1)(x_1, \dots, x_n, y, z) \\
 &= (\tau \otimes n) \circ (1 \otimes \tau_{n,1})(y, x_1, \dots, x_n, z) \\
 &= (\tau \otimes n)(y, z, x_1, \dots, x_n) \\
 &= (z, y, x_1, \dots, x_n).
 \end{aligned}$$

$\text{cp}(f\tau 1, 7)$. Une paire critique de sommet $(1 \otimes \delta) \circ \tau \circ (f \otimes 1)$:

$$\begin{aligned}
 & (1 \otimes \delta) \circ \tau \circ (f \otimes 1) \\
 & \rightarrow_{f\tau 1} (1 \otimes \delta) \circ (1 \otimes f) \circ \tau n, 1 \\
 & \rightarrow_{f\delta} (1 \otimes f \otimes f) \circ (1 \otimes \delta_n) \circ \tau_{n,1};
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \delta) \circ \tau \circ (f \otimes 1) \\
 & \rightarrow_{\tau} (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) \circ (f \otimes 1) \\
 & \rightarrow_{f\delta} (\tau \otimes 1) \circ (1 \otimes \tau) \circ (f \otimes f \otimes 1) \circ (\delta_n \otimes 1) \\
 & \rightarrow_{f\tau 1} (\tau \otimes f) \circ (f \otimes \tau_{n,1}) \circ (\delta_n \otimes 1) \\
 & \rightarrow_{f\tau 1} (1 \otimes f \otimes f) \circ (\tau_{n,1} \otimes n) \circ (n \otimes \tau_{n,1}) \circ (\delta_n \otimes 1).
 \end{aligned}$$

$$\begin{aligned}
 & (1 \otimes \delta_n) \circ \tau_{n,1}(x_1, \dots, x_n, y) \\
 &= (1 \otimes \delta_n)(y, x_1, \dots, x_n) \\
 &= (y, x_1, \dots, x_n, x_1, \dots, x_n);
 \end{aligned}$$

$$\begin{aligned}
 & (\tau_{n,1} \otimes n) \circ (n \otimes \tau_{n,1}) \circ (\delta_n \otimes 1)(x_1, \dots, x_n, y) \\
 &= (\tau_{n,1} \otimes n) \circ (n \otimes \tau_{n,1})(x_1, \dots, x_n, x_1, \dots, x_n, y) \\
 &= (\tau_{n,1} \otimes n)(x_1, \dots, x_n, y, x_1, \dots, x_n) \\
 &= (y, x_1, \dots, x_n, x_1, \dots, x_n).
 \end{aligned}$$

$\text{cp}(f\tau 1, 8)$. Une paire critique de sommet $(1 \otimes \tau) \circ (\tau \otimes 1) \circ (f \otimes \delta)$:

$$\begin{aligned} (1 \otimes \tau) \circ (\tau \otimes 1) \circ (f \otimes \delta) &\rightarrow_{f\tau 1} (1 \otimes \tau) \circ (1 \otimes f \otimes 1) \circ (\tau_{n,1} \otimes 1) \circ (n \otimes \delta) \\ &\rightarrow_{f\tau 1} (2 \otimes f) \circ (1 \otimes \tau_{n,1}) \circ (\tau_{n,1} \otimes 1) \circ (n \otimes \delta) ; \end{aligned}$$

$$\begin{aligned} (1 \otimes \tau) \circ (\tau \otimes 1) \circ (f \otimes \delta) &\rightarrow_8 (\delta \otimes 1) \circ \tau \circ (f \otimes 1) \\ &\rightarrow_{f\tau 1} (\delta \otimes f) \circ \tau_{n,1}. \end{aligned}$$

$$\begin{aligned} &(1 \otimes \tau_{n,1}) \circ (\tau_{n,1} \otimes 1) \circ (n \otimes \delta)(x_1, \dots, x_n, y) \\ &= (1 \otimes \tau_{n,1}) \circ (\tau_{n,1} \otimes 1)(x_1, \dots, x_n, y, y) \\ &= (1 \otimes \tau_{n,1})(y, x_1, \dots, x_n, y) \\ &= (y, y, x_1, \dots, x_n) ; \end{aligned}$$

$$\begin{aligned} (\delta \otimes n) \circ \tau_{n,1}(x_1, \dots, x_n, y) &= (\delta \otimes n)(y, x_1, \dots, x_n) \\ &= (y, y, x_1, \dots, x_n). \end{aligned}$$

$\text{cp}(f\tau 1, 9)$. Une paire critique de sommet $(1 \otimes \varepsilon) \circ \tau \circ (f \otimes 1)$:

$$\begin{aligned} (1 \otimes \varepsilon) \circ \tau \circ (f \otimes 1) &\rightarrow_{f\tau 1} (1 \otimes \varepsilon) \circ (1 \otimes f) \circ \tau_{n,1} \\ &\rightarrow_{f\varepsilon} (1 \otimes \varepsilon^n) \circ \tau_{n,1} ; \end{aligned}$$

$$\begin{aligned} (1 \otimes \varepsilon) \circ \tau \circ (f \otimes 1) &\rightarrow_9 (\varepsilon \otimes 1) \circ (f \otimes 1) \\ &\rightarrow_{f\varepsilon} \varepsilon^n \otimes 1. \end{aligned}$$

$$\begin{aligned} (1 \otimes \varepsilon^n) \circ \tau_{n,1}(x_1, \dots, x_n, y) &= (1 \otimes \varepsilon^n)(y, x_1, \dots, x_n) \\ &= y \\ &= (\varepsilon^n \otimes 1)(x_1, \dots, x_n, y). \end{aligned}$$

$\text{cp}(f\tau 1, 10)$. Une paire critique de sommet $(\varepsilon \otimes 1) \circ \tau \circ (f \otimes 1)$:

$$(\varepsilon \otimes 1) \circ \tau \circ (f \otimes 1) \rightarrow_{f\tau 1} (\varepsilon \otimes f) \circ \tau_{n,1} ;$$

$$(\varepsilon \otimes 1) \circ \tau \circ (f \otimes 1) \rightarrow_{10} f \otimes \varepsilon.$$

$$\begin{aligned} (\varepsilon \otimes n) \circ \tau_{n,1}(x_1, \dots, x_n, y) &= (\varepsilon \otimes n)(y, x_1, \dots, x_n) \\ &= (x_1, \dots, x_n) \\ &= (n \otimes \varepsilon)(x_1, \dots, x_n, y). \end{aligned}$$

$\text{cp}(f\tau 1, 12)$. Une paire critique de sommet $(1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \circ (f \otimes 1)$:

$$\begin{aligned} (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \circ (f \otimes 1) &\rightarrow_{f\tau 1} (1 \otimes \tau) \circ (\delta \otimes f) \circ \tau_{n,1} \\ &\rightarrow_{f\tau 2} (1 \otimes f \otimes 1) \circ (1 \otimes \tau_{1,n}) \circ (\delta \otimes n) \circ \tau_{n,1} ; \end{aligned}$$

$$\begin{aligned} (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \circ (f \otimes 1) &\rightarrow_{12} (\tau \otimes 1) \circ (f \otimes \delta) \\ &\rightarrow_{f\tau 1} (1 \otimes f \otimes 1) \circ (\tau_{n,1} \otimes 1) \circ (n \otimes \delta). \end{aligned}$$

$$\begin{aligned} (1 \otimes \tau_{1,n}) \circ (\delta \otimes n) \circ \tau_{n,1}(x_1, \dots, x_n, y) &= (1 \otimes \tau_{1,n}) \circ (\delta \otimes n)(y, x_1, \dots, x_n) \\ &= (1 \otimes \tau_{1,n})(y, y, x_1, \dots, x_n) \\ &= (y, x_1, \dots, x_n, y) ; \end{aligned}$$

$$\begin{aligned} (\tau_{n,1} \otimes 1) \circ (n \otimes \delta)(x_1, \dots, x_n, y) &= (\tau_{n,1} \otimes 1)(x_1, \dots, x_n, y, y) \\ &= (y, x_1, \dots, x_n, y). \end{aligned}$$

$\text{cp}(f\tau 2, 5)$. Une paire critique de sommet $\tau \circ \tau \circ (1 \otimes f)$:

$$\begin{aligned} \tau \circ \tau \circ (1 \otimes f) &\rightarrow_{f\tau 2} \tau \circ (f \otimes 1) \circ \tau_{1,n} \\ &\rightarrow_{f\tau 1} (1 \otimes f) \circ \tau_{n,1} \circ \tau_{1,n} ; \end{aligned}$$

$$\tau \circ \tau \circ (1 \otimes f) \rightarrow_5 1 \otimes f.$$

$$\begin{aligned}
 \tau_{n,1} \circ \tau_{1,n}(y, x_1, \dots, x_n) &= \tau_{n,1}(x_1, \dots, x_n, y) \\
 &= (y, x_1, \dots, x_n) \\
 &= (n+1)(y, x_1, \dots, x_n).
 \end{aligned}$$

cp($f\tau 2, 6$). Une paire critique de sommet $(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (2 \otimes f)$:

$$\begin{aligned}
 &(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (2 \otimes f) \\
 &\rightarrow_{f\tau 2} (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes f \otimes 1) \circ (1 \otimes \tau_{1,n}) \\
 &\rightarrow_{f\tau 2} (f \otimes \tau) \circ (\tau_{1,n} \otimes 1) \circ (1 \otimes \tau_{1,n}) ;
 \end{aligned}$$

$$\begin{aligned}
 &(1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) \circ (2 \otimes f) \\
 &\rightarrow_6 (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes f) \\
 &\rightarrow_{f\tau 2} (\tau \otimes 1) \circ (1 \otimes f \otimes 1) \circ (1 \otimes \tau_{1,n}) \circ (\tau \otimes n) \\
 &\rightarrow_{f\tau 2} (f \otimes 2) \circ (\tau_{1,n} \otimes 1) \circ (1 \otimes \tau_{1,n}) \circ (\tau \otimes n).
 \end{aligned}$$

$$\begin{aligned}
 &(n \otimes \tau) \circ (\tau_{1,n} \otimes 1) \circ (1 \otimes \tau_{1,n})(y, z, x_1, \dots, x_n) \\
 &= (n \otimes \tau) \circ (\tau_{1,n} \otimes 1)(y, x_1, \dots, x_n, z) \\
 &= (n \otimes \tau)(x_1, \dots, x_n, y, z) \\
 &= (x_1, \dots, x_n, z, y) ;
 \end{aligned}$$

$$\begin{aligned}
 &(\tau_{1,n} \otimes 1) \circ (1 \otimes \tau_{1,n}) \circ (\tau \otimes n)(y, z, x_1, \dots, x_n) \\
 &= (\tau_{1,n} \otimes 1) \circ (1 \otimes \tau_{1,n})(z, y, x_1, \dots, x_n) \\
 &= (\tau_{1,n} \otimes 1)(z, x_1, \dots, x_n, y) \\
 &= (x_1, \dots, x_n, z, y).
 \end{aligned}$$

cp($f\tau 2, 7$). Une paire critique de sommet $(1 \otimes \delta) \circ \tau \circ (1 \otimes f)$:

$$(1 \otimes \delta) \circ \tau \circ (1 \otimes f) \rightarrow_{f\tau 2} (f \otimes \delta) \circ \tau_{1,n} ;$$

$$\begin{aligned}
 (1 \otimes \delta) \circ \tau \circ (1 \otimes f) &\rightarrow_{\tau} (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes f) \\
 &\rightarrow_{f\tau 2} (\tau \otimes 1) \circ (1 \otimes f \otimes 1) \circ (1 \otimes \tau_{1,n}) \circ (\delta \otimes n) \\
 &\rightarrow_{f\tau 2} (f \otimes 2) \circ (\tau_{1,n} \otimes 1) \circ (1 \otimes \tau_{1,n}) \circ (\delta \otimes n).
 \end{aligned}$$

$$\begin{aligned}(n \otimes \delta) \circ \tau_{1,n}(y, x_1, \dots, x_n) &= (n \otimes \delta)(x_1, \dots, x_n, y) \\ &= (x_1, \dots, x_n, y, y); \end{aligned}$$

$$\begin{aligned} &(\tau_{1,n} \otimes 1) \circ (1 \otimes \tau_{1,n}) \circ (\delta \otimes n)(y, x_1, \dots, x_n) \\ &= (\tau_{1,n} \otimes 1) \circ (1 \otimes \tau_{1,n})(y, y, x_1, \dots, x_n) \\ &= (\tau_{1,n} \otimes 1)(y, x_1, \dots, x_n, y) \\ &= (x_1, \dots, x_n, y, y). \end{aligned}$$

cp($f\tau 2, 9$). Une paire critique de sommet $(1 \otimes \varepsilon) \circ \tau \circ (1 \otimes f)$:

$$(1 \otimes \varepsilon) \circ \tau \circ (1 \otimes f) \rightarrow_{f\tau 2} (f \otimes \varepsilon) \circ \tau_{1,n};$$

$$(1 \otimes \varepsilon) \circ \tau \circ (1 \otimes f) \rightarrow_9 \varepsilon \otimes f.$$

$$\begin{aligned}(n \otimes \varepsilon) \circ \tau_{1,n}(y, x_1, \dots, x_n) &= (n \otimes \varepsilon)(x_1, \dots, x_n, y) \\ &= (x_1, \dots, x_n) \\ &= (\varepsilon \otimes n)(y, x_1, \dots, x_n). \end{aligned}$$

cp($f\tau 2, 10$). Une paire critique de sommet $(\varepsilon \otimes 1) \circ \tau \circ (1 \otimes f)$:

$$\begin{aligned}(\varepsilon \otimes 1) \circ \tau \circ (1 \otimes f) &\rightarrow_{f\tau 2} (\varepsilon \otimes 1) \circ (f \otimes 1) \circ \tau_{1,n} \\ &\rightarrow_{f\varepsilon} (\varepsilon^n \otimes 1) \circ \tau_{1,n} \end{aligned}$$

$$\begin{aligned}(\varepsilon \otimes 1) \circ \tau \circ (1 \otimes f) &\rightarrow_{10} (1 \otimes \varepsilon) \circ (1 \otimes f) \\ &\rightarrow_{f\varepsilon} 1 \otimes \varepsilon^n. \end{aligned}$$

$$\begin{aligned}(\varepsilon^n \otimes 1) \circ \tau_{1,n}(y, x_1, \dots, x_n) &= (\varepsilon^n \otimes 1)(x_1, \dots, x_n, y) \\ &= y \\ &= (1 \otimes \varepsilon^n)(y, x_1, \dots, x_n). \end{aligned}$$

$\text{cp}(f\tau 2, 12)$. Une paire critique de sommet $(1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \circ (1 \otimes f)$:

$$\begin{aligned} (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \circ (1 \otimes f) &\rightarrow_{f\tau 2} (1 \otimes \tau) \circ (\delta \otimes 1) \circ (f \otimes 1) \circ \tau_{1,n} \\ &\rightarrow_{f\delta} (f \otimes \tau) \circ (n \otimes f \otimes 1) \circ (\delta_n \otimes 1) \circ \tau_{1,n} \\ &\rightarrow_{f\tau 1} (f \otimes 1 \otimes f) \circ (n \otimes \tau_{n,1}) \circ (\delta_n \otimes 1) \circ \tau_{1,n} ; \end{aligned}$$

$$\begin{aligned} (1 \otimes \tau) \circ (\delta \otimes 1) \circ \tau \circ (1 \otimes f) &\rightarrow_{12} (\tau \otimes 1) \circ (1 \otimes \delta) \circ (1 \otimes f) \\ &\rightarrow_{f\delta} (\tau \otimes f) \circ (1 \otimes f \otimes n) \circ (1 \otimes \delta_n) \\ &\rightarrow_{f\tau 2} (f \otimes 1 \otimes f) \circ (\tau_{1,n} \otimes n) \circ (1 \otimes \delta_n). \end{aligned}$$

$$\begin{aligned} (n \otimes \tau_{n,1}) \circ (\delta_n \otimes 1) \circ \tau_{1,n}(y, x_1, \dots, x_n) &= (n \otimes \tau_{n,1}) \circ (\delta_n \otimes 1)(x_1, \dots, x_n, y) \\ &= (n \otimes \tau_{n,1})(x_1, \dots, x_n, x_1, \dots, x_n, y) \\ &= (x_1, \dots, x_n, y, x_1, \dots, x_n) ; \end{aligned}$$

$$\begin{aligned} (\tau_{1,n} \otimes n) \circ (1 \otimes \delta_n)(y, x_1, \dots, x_n) &= (\tau_{1,n} \otimes n)(y, x_1, \dots, x_n, x_1, \dots, x_n) \\ &= (x_1, \dots, x_n, y, x_1, \dots, x_n). \end{aligned}$$

Toutes les paires critiques mixtes, c'est-à-dire engendrées par une règle de R_Δ et une règle de $R_{\Sigma/\Delta}$, sont donc confluentes. Il ne reste plus qu'à regarder celles qui sont engendrées par deux règles de $R_{\Sigma/\Delta}$: il y en a autant que le carré du nombre de flèches de Σ . En effet, on a une paire critique pour chaque couple (f, g) de flèches de Σ entre les règles $f\tau 1$ et $g\tau 2$. Supposons que $f \in \Sigma(m, 1)$ et que $g \in \Sigma(n, 1)$ pour m et n entiers. Alors :

$\text{cp}(f\tau 1, g\tau 2)$. Une paire critique de sommet $\tau \circ (f \otimes g)$. Rappelons que l'on a montré que :

$$\tau_{m,1} \circ (m \otimes g) \twoheadrightarrow_{g\tau 2} (g \otimes m) \circ \tau_{m,n}.$$

Une démonstration similaire aboutit à :

$$\tau_{1,n} \circ (f \otimes n) \twoheadrightarrow_{f\tau 1} (n \otimes f) \circ \tau_{m,n}.$$

Étudions à présent le branchement critique :

$$\begin{aligned} \tau \circ (f \otimes g) &\rightarrow_{f\tau 1} (1 \otimes f) \circ \tau_{m,1} \circ (m \otimes g) \\ &\twoheadrightarrow_{g\tau 2} (g \otimes f) \circ \tau_{m,n} ; \end{aligned}$$

$$\begin{aligned} \tau \circ (f \otimes g) &\rightarrow_{g\tau 2} (g \otimes 1) \circ \tau_{1,n} \circ (f \otimes n) \\ &\twoheadrightarrow_{f\tau 1} (g \otimes f) \circ \tau_{m,n}. \end{aligned}$$

On a donc montré que :

Proposition 5.32. *La présentation $(\Sigma^c, R_{\Delta, \Sigma})$ est localement confluente.*

On en déduit, à l'aide du lemme de Newman :

Corollaire 5.33. *Le couple $(\Sigma^c, R_{\Delta, \Sigma})$ est une présentation convergente de l'opérade cartésienne libre engendrée par la signature algébrique Σ .*

5.4 Une autre version de l'opérade cartésienne libre engendrée par une signature algébrique

Notre but, ici, est de construire, à partir de l'ensemble $T_\Sigma(V)$ des termes une opérade cartésienne $\mathbb{T}\Sigma$ qui est aussi une opérade cartésienne libre engendrée par Σ . On aura alors un isomorphisme d'opérades cartésiennes entre $\mathbb{T}\Sigma$ et $\mathcal{L}\Sigma^c/R_{\Delta, \Sigma}$ qui, comme $R_{\Delta, \Sigma}$ est convergent, se relève en un morphisme d'opérades de $\mathbb{T}\Sigma$ vers $\mathcal{L}\Sigma^c$. Nous verrons que les termes de $T_\Sigma(V)$ se plongent dans les flèches de $\mathbb{T}\Sigma$, ce qui permettra d'associer à chaque terme une flèche de $\mathcal{L}\Sigma^c$ en $R_{\Delta, \Sigma}$ -forme normale. Nous verrons que l'on peut aussi traduire des règles de réécriture de telle sorte que, si ces dernières sont linéaires à gauche et uniformisées, la présentation d'opérade obtenue simule complètement le système de réécriture de termes de départ.

5.4.1 Construction de $\mathbb{T}\Sigma$

Commençons par définir $\mathbb{T}\Sigma$; cette construction avait déjà été signalée dans [Laf95]. Avant tout, précisons quelques notations qui nous seront utiles par la suite :

Notation. On suppose désormais que l'on a fixé une bijection entre les ensembles V des variables et \mathbb{N}^* des entiers naturels non nuls, ce qui est toujours possible puisque l'on a supposé V dénombrable : cela revient à numéroter les variables x_1, x_2, x_3 , etc. Pour tout terme u de $T_\Sigma(V)$, on note $\sharp u$ le plus petit des entiers n vérifiant $V(u) \subseteq \{x_1, \dots, x_n\}$.

On note, pour tous $m \in \mathbb{N}$ et $n \in \mathbb{N}^*$, $\mathbb{T}(m, n)$ l'ensemble des n -uplets (u_1, \dots, u_n) d'éléments de $T_\Sigma(V)$ tels que, pour tout $i \in [n]$, on ait $\sharp u_i \leq m$. Dans le cas où $n = 0$, on note, pour tout $m \in \mathbb{N}$, $\mathbb{T}(m, 0)$ l'ensemble réduit à la famille vide vue comme terme en les variables x_1, \dots, x_m et notée $*(m)$.

Ainsi, une flèche $f : m \longrightarrow n$ de $\mathbb{T}\Sigma$ est un n -uplet de termes dont les variables sont contenues dans $\{x_1, \dots, x_m\}$. De plus, $\mathbb{T}(m, 1)$ est l'ensemble des termes u tels que $\sharp u \leq m$; ainsi, tout terme u peut être vu comme une flèche de $\mathbb{T}(m, 1)$ pour tout $m \geq \sharp u$.

Nous devons encore définir la composition et le produit dans $\mathbb{T}\Sigma$. Supposons que $f = (u_1, \dots, u_n) : m \longrightarrow n$ et que $g = (v_1, \dots, v_p) : n \longrightarrow p$ soient deux flèches de $\mathbb{T}\Sigma$; leur composée $g \circ f : m \longrightarrow p$ est donnée par $g \circ f = (w_1, \dots, w_p)$ où chaque w_i est défini par :

$$w_i = v_i[x_1 := u_1, \dots, x_n := u_n].$$

L'identité de n est (x_1, \dots, x_n) . Quant au produit, si $f = (u_1, \dots, u_n) : m \longrightarrow n$ et que $g = (v_1, \dots, v_q) : p \longrightarrow q$ sont deux flèches de $\mathbb{T}\Sigma$, on définit $f \otimes g = (w_1, \dots, w_{n+q})$ en posant :

$$w_i = \begin{cases} u_i & \text{si } i \in \{1 \dots m\} \\ v_{i-n}[x_1 := x_{m+1}, \dots, x_p := x_{m+p}] & \text{si } i \in \{m+1, \dots, m+p\}. \end{cases}$$

Le neutre pour le produit, qui est aussi l'identité de 0, est donc la famille vide $* = *(0)$ vue comme une constante. On vérifie alors que :

Proposition 5.34. *Munie de la composition, du produit et des identités ainsi définis, la catégorie $\mathbb{T}\Sigma$ est une opérade.*

Démonstration. On doit vérifier que :

- la composition est associative et admet les identités comme éléments neutres locaux ;
- le produit est associatif et admet 0 comme élément neutre à gauche et à droite ;
- le produit et la composition vérifient la relation d'échange.

Pour la composition : soient $f = (u_1, \dots, u_n) : m \longrightarrow n$, $g = (v_1, \dots, v_p) : n \longrightarrow p$ et $h = (w_1, \dots, w_q) : p \longrightarrow q$ trois flèches de $\mathbb{T}\Sigma$. On définit les substitutions suivantes :

$$\sigma(x_i) = \begin{cases} u_i & \text{si } i \in [n] \\ x_i & \text{sinon} \end{cases} \quad \text{et} \quad \tau(x_i) = \begin{cases} v_i & \text{si } i \in [p] \\ x_i & \text{sinon} \end{cases}$$

Alors, d'une part :

$$h \circ (g \circ f) = (w_1 \cdot (\sigma \circ \tau), \dots, w_q \cdot (\sigma \circ \tau))$$

et, d'autre part :

$$(h \circ g) \circ f = ((w_1 \cdot \tau) \cdot \sigma, \dots, (w_q \cdot \tau) \cdot \sigma).$$

On conclut en remarquant que, pour tout $i \in [p]$, $(x_i \cdot \tau) \cdot \sigma = v_i \cdot \sigma = x_i \cdot (\sigma \circ \tau)$. De plus :

$$\begin{aligned} f \circ s(f) &= (u_1, \dots, u_n) \circ (x_1, \dots, x_n) \\ &= (u_1 \cdot \text{id}, \dots, u_n \cdot \text{id}) \\ &= (u_1, \dots, u_n) \\ &= f. \end{aligned}$$

Et aussi :

$$\begin{aligned} t(f) \circ f &= (x_1, \dots, x_n) \circ (u_1, \dots, u_n) \\ &= (x_1 \cdot \sigma, \dots, x_n \cdot \sigma) \\ &= (u_1, \dots, u_n) \\ &= f. \end{aligned}$$

Pour le produit, supposons que $f = (u_1, \dots, u_n) : m \longrightarrow n$, $g = (v_1, \dots, v_q) : p \longrightarrow q$ et $h = (w_1, \dots, w_s) : r \longrightarrow s$ sont trois flèches de $\mathbb{T}\Sigma$. On note, pour tout entier $k \in \mathbb{N}$, τ_k la substitution qui envoie chaque x_i sur x_{i+k} . Alors :

$$\begin{aligned} (f \otimes g) \otimes h &= (u_1, \dots, u_n, v_1 \cdot \tau_m, \dots, v_q \cdot \tau_m) \otimes h \\ &= (u_1, \dots, u_n, v_1 \cdot \tau_m, \dots, v_q \cdot \tau_m, w_1 \cdot \tau_{m+p}, \dots, w_s \cdot \tau_{m+p}) \end{aligned}$$

Et :

$$\begin{aligned} f \otimes (g \otimes h) &= f \otimes (v_1, \dots, v_q, w_1 \cdot \tau_p, \dots, w_s \cdot \tau_p) \\ &= (u_1, \dots, u_n, v_1 \cdot \tau_m, \dots, v_q \cdot \tau_m, (w_1 \cdot \tau_p) \cdot \tau_m, \dots, (w_s \cdot \tau_p) \cdot \tau_m) \end{aligned}$$

On conclut en remarquant que $\tau_{m+p}(x_i) = x_{i+m+p} = \tau_p \circ \tau_m(x_i)$. On a :

$$f \otimes 0 = f = 0 \otimes f,$$

la première égalité étant donnée par construction et la seconde provenant du fait que $\tau_0 = \text{id}$.

Enfin, pour la relation d'échange, conservons les mêmes flèches f et g ; on définit la substitution suivante :

$$\sigma'(x_i) = \begin{cases} u_i & \text{si } i \in [n] \\ x_{i-n+m} & \text{sinon} \end{cases}$$

de telle sorte que $\sigma' \circ \tau_n = \tau_m$. Alors :

$$\begin{aligned} &(t(f) \otimes g) \circ (f \otimes s(g)) \\ &= (x_1, \dots, x_n, v_1 \cdot \tau_n, \dots, v_q \cdot \tau_n) \circ (u_1, \dots, u_n, x_{m+1}, \dots, x_{m+p}) \\ &= (x_1 \cdot \sigma', \dots, x_n \cdot \sigma', (v_1 \cdot \tau_n) \cdot \sigma', \dots, (v_q \cdot \tau_n) \cdot \sigma') \\ &= (u_1, \dots, u_n, v_1 \cdot \tau_m, \dots, v_q \cdot \tau_m) \\ &= f \otimes g. \end{aligned}$$

Enfin :

$$\begin{aligned}
 & (f \otimes t(g)) \circ (s(f) \otimes g) \\
 &= (u_1, \dots, u_n, x_{m+1}, \dots, x_{m+q}) \circ (x_1, \dots, x_m, v_1 \cdot \tau_m, \dots, v_q \cdot \tau_m) \\
 &= (u_1, \dots, u_n, v_1 \cdot \tau_m, \dots, v_q \cdot \tau_m) \\
 &= f \otimes g.
 \end{aligned}$$

◇

En fait, $\mathbb{T}\Sigma$ est même cartésienne mais, avant de prouver cela, nous allons montrer que $\mathbb{T}\Sigma$ contient (une copie de) \mathbb{F}^o . Définissons \mathbb{V} , la sous-opérade *des variables* de $\mathbb{T}\Sigma$, en posant, pour $m \in \mathbb{N}$ et $n \in \mathbb{N}^*$, $\mathbb{V}(m, n)$ l'ensemble des n -uplets (y_1, \dots, y_n) de variables vérifiant, pour tout $i \in [n]$, $\#y_i \leq m$. Dans le cas $n = 0$ et pour tout entier m , on pose $\mathbb{V}(m, 0) = \{*(m)\}$.

Pour résumer en d'autres termes, $\mathbb{V}(m, n)$ est l'ensemble des familles à n éléments pris dans $\{x_1, \dots, x_m\}$. Alors :

Proposition 5.35. *L'opérade des variables \mathbb{V} est isomorphe à l'opérade \mathbb{F}^o des ensembles.*

Démonstration. Pour construire un morphisme $F : \mathbb{V} \longrightarrow \mathbb{F}^o$, on commence par remarquer que, pour tout n -uplet $\varphi = (y_1, \dots, y_n)$ de variables prises dans $\{x_1, \dots, x_m\}$, il existe une *unique* application $f \in \mathbb{F}(n, m)$ vérifiant $y_i = x_{f(i)}$. On pose alors $F(\varphi) = f^*$. On doit vérifier que F est un morphisme d'opérades.

Soient $\varphi = (x_{f(1)}, \dots, x_{f(n)}) : m \longrightarrow n$ et $\psi = (x_{g(1)}, \dots, x_{g(p)}) : n \longrightarrow p$ deux flèches de \mathbb{V} . On a donc $F(\varphi) = f^* \in \mathbb{F}(m, n)$ et $F(\psi) = g^* \in \mathbb{F}(p, q)$. Alors :

$$\begin{aligned}
 \psi \circ \varphi &= (x_{g(1)}, \dots, x_{g(p)}) \circ (x_{f(1)}, \dots, x_{f(n)}) \\
 &= (x_{f \circ g(1)}, \dots, x_{f \circ g(p)}).
 \end{aligned}$$

Ainsi, par définition de F , on a $F(\psi \circ \varphi) = (f \circ g)^* = g^* \circ f^* = F(\psi) \circ F(\varphi)$. De plus, on a $n = (x_1, \dots, x_n)$ et donc $F(n) = n$. Donc F est un foncteur.

Soient $\varphi = (x_{f(1)}, \dots, x_{f(n)}) : m \longrightarrow n$ et $\psi = (x_{g(1)}, \dots, x_{g(q)}) : p \longrightarrow q$ deux flèches de \mathbb{V} :

$$\begin{aligned}
 \varphi \otimes \psi &= (x_{f(1)}, \dots, x_{f(n)}) \otimes (x_{g(1)}, \dots, x_{g(q)}) \\
 &= (x_{f(1)}, \dots, x_{f(n)}, x_{g(1)+m}, \dots, x_{g(q)+m}) \\
 &= (x_{f \otimes g(1)}, \dots, x_{f \otimes g(n+q)}).
 \end{aligned}$$

Alors $F(\varphi \otimes \psi) = (f \otimes g)^* = f^* \otimes g^* = F(\varphi) \otimes F(\psi)$. Comme on a, par construction, l'égalité $F(0) = 0$, on en déduit que F est bien un morphisme d'opérades de \mathbb{V} vers \mathbb{F}^o . De plus, la restriction de F aux flèches est bijective, ce qui fait de F un isomorphisme. ◇

On en déduit que :

Proposition 5.36. *L'opérade $\mathbb{T}\Sigma$ est cartésienne.*

Démonstration. Il suffit d'exhiber des flèches $\varepsilon : 1 \longrightarrow 0$, $\delta : 1 \longrightarrow 2$ et $\tau : 2 \longrightarrow 2$ qui vérifient les relations de $E_{\Delta, \Sigma}$. Or, l'isomorphisme entre \mathbb{V} et \mathbb{F}^o nous donne les candidats suivants :

$$\begin{cases} \varepsilon = *(1) \\ \delta = (x_1, x_1) = (x_{\delta^*(1)}, x_{\delta^*(2)}) \\ \tau = (x_2, x_1) = (x_{\tau^*(1)}, x_{\tau^*(2)}) \end{cases}$$

Ce même isomorphisme nous assure de plus que ces flèches vérifient bien les relations de E_{Δ} . il ne nous reste plus qu'à vérifier les relations de $E_{\Sigma/\Delta}$. Soit $u \in \mathbb{T}\Sigma(n, 1)$. Alors :

$u\delta$. On a, d'une part :

$$\begin{aligned} \delta \circ u &= (x_1, x_1) \circ u \\ &= (x_1[x_1 := u], x_1[x_1 := u]) \\ &= (u, u). \end{aligned}$$

On note τ_{-n} la substitution qui envoie x_{n+i} sur x_i pour tout $i \geq 1$ et laisse inchangés les x_1, \dots, x_n ; de plus, on a :

$$\delta_n = (x_{\delta_n^*(1)}, \dots, x_{\delta_n^*(2n)}) = (x_1, \dots, x_n, x_1, \dots, x_n).$$

Ce qui donne :

$$\begin{aligned} (u \otimes u) \circ \delta_n &= (u, u \cdot \tau_n) \circ (x_1, \dots, x_n, x_1, \dots, x_n) \\ &= (u \cdot \tau_{-n}, (u \cdot \tau_n) \cdot \tau_{-n}) \\ &= (u, u). \end{aligned}$$

$u\varepsilon$. On a : $\varepsilon \circ u = *(1) \circ u = *(n) = \varepsilon^n$.

$u\tau 1$. On a : $\tau \circ (u \otimes 1) = (x_2, x_1) \circ (u, x_{n+1}) = (x_{n+1}, u)$. Or :

$$\tau_{n,1} = (x_{\tau_{n,1}^*(1)}, \dots, x_{\tau_{n,1}^*(n+1)}) = (x_{n+1}, x_1, \dots, x_n).$$

Ainsi :

$$\begin{aligned} (1 \otimes u) \circ \tau_{n,1} &= (x_1, u \cdot \tau_1) \circ (x_{n+1}, x_1, \dots, x_n) \\ &= (x_{n+1}, (u \cdot \tau_1) \cdot \tau_{-1}) \\ &= (x_{n+1}, u). \end{aligned}$$

◇

Par conséquent, on a une opérade cartésienne $\mathbb{T}\Sigma$ contenant Σ et rappelant très fortement l'opérade cartésienne libre engendrée par Σ déjà construite. Nous allons montrer que ce sont, en réalité, les mêmes.

5.4.2 L'opérade cartésienne $\mathbb{T}\Sigma$ est librement engendrée par Σ

Montrons que :

Proposition 5.37. *Les opérades cartésiennes $\mathbb{T}\Sigma$ et $\mathcal{L}\Sigma^c/R_{\Delta,\Sigma}$ sont isomorphes.*

Démonstration. Puisque $\mathbb{T}\Sigma$ est une opérade cartésienne contenant Σ , on sait qu'il existe un unique morphisme d'opérades cartésiennes

$$F : \mathcal{L}\Sigma^c/R_{\Delta,\Sigma} \longrightarrow \mathbb{T}\Sigma.$$

Ce morphisme est l'identité sur les flèches de $\mathcal{L}\Sigma$ et associe à toute $f \in \mathbb{F}^o(m, n)$ la flèche $(x_{f^*(1)}, \dots, x_{f^*(n)})$ de $\mathbb{V}(m, n)$.

Si l'on fixe une flèche $f = (u_1, \dots, u_n) \in \mathbb{T}\Sigma(m, n)$, on a déjà vu que chaque u_i s'écrit de manière unique sous la forme $f_i(y_1^i, \dots, y_{k_i}^i)$ avec f_i dans $\mathcal{L}\Sigma(k_i, 1)$, pour un certain entier k_i , et les y_j^i dans $\{x_1, \dots, x_m\}$. D'où la décomposition *unique* de f :

$$f = f_\Sigma \circ f_\Delta$$

avec $f_\Sigma = f_1 \otimes \dots \otimes f_n$ dans $\mathcal{L}\Sigma(k, 1)$ et f_Δ dans $\mathbb{V}(m, k)$, en notant k la somme de tous les k_i , $i \in [n]$. Le fait que cette décomposition soit unique nous assure que F est un isomorphisme. \diamond

On a donc, comme corollaire :

Corollaire 5.38. *L'opérade $\mathbb{T}\Sigma$ admet la présentation convergente $(\Sigma^c, R_{\Delta,\Sigma})$.*

Le fait que cette présentation soit convergente nous assure que :

Corollaire 5.39. *Il existe un morphisme d'opérades $\Phi : \mathbb{T}\Sigma \longrightarrow \mathcal{L}\Sigma^c$ tel que, pour toute flèche f de $\mathbb{T}\Sigma$, $\Phi(f)$ soit une $R_{\Delta,\Sigma}$ -forme normale et qui fait commuter le diagramme suivant :*

$$\begin{array}{ccc} \mathbb{T}\Sigma & \xrightarrow{\Phi} & \mathcal{L}\Sigma^c \\ & \searrow \textcircled{\simeq} & \downarrow \pi \\ & & \mathcal{L}\Sigma^c/R_{\Delta,\Sigma} \end{array}$$

où π désigne le morphisme canonique associé au quotient.

Notation. Soit u un terme de $T_\Sigma(V)$. Pour tout $n \geq \sharp u$, on peut voir u comme une flèche u_n de $\mathbb{T}\Sigma(n, 1)$ et on pose $\Phi^n(u) = \Phi(u_n)$; en particulier, on note $\Phi(u) = \Phi^{\sharp u}(u)$. De même, si α est une règle de réécriture de termes uniformisée, on pose :

$$\Phi(\alpha) = (\Phi(s(\alpha)), \Phi^{\sharp s(\alpha)}(t(\alpha))).$$

Pour tout terme u de $T_\Sigma(V)$ et tout $n \geq \sharp u$, la flèche $\Phi^n(u)$ de $\mathcal{L}\Sigma^c$ est une $R_{\Delta, \Sigma}$ -forme normale; en particulier, $\Phi(u)$ est une $R_{\Delta, \Sigma}$ -forme normale.

De même, pour toute règle de réécriture α , le couple $\Phi(\alpha)$ est formé de deux flèches parallèles : c'est ici que sert l'hypothèse $V(t(\alpha)) \subseteq V(s(\alpha))$. De plus, comme nous l'avons déjà vu, si α est linéaire à gauche et uniformisée, $\Phi(s(\alpha))$ est une flèche de $\mathcal{L}\Sigma$ et ne contient donc pas de τ , δ ou ε .

Exemples. On suppose que Σ contient deux générateurs, l'un, μ , d'arité 2 et l'autre, η , d'arité 0. Déterminons $\Phi(u)$ pour :

$$u = \mu(\mu(x_3, x_1), \mu(x_1, \eta)).$$

On cherche donc une flèche $\Phi(u) : 3 \longrightarrow 1$ de $\mathcal{L}\Sigma^c$ qui soit une $R_{\Delta, \Sigma}$ -forme normale et vérifie $\Phi(u) \circ (x_1, x_2, x_3) = u$. Par exemple, on peut procéder ainsi :

$$\begin{aligned} \Phi(u) &= \mu(\mu(x_3, x_1), \mu(x_1, \eta)) \\ &= \mu \circ (\mu(x_3, x_1), \mu(x_1, \eta)) \\ &= \mu \circ (\mu \otimes \mu) \circ (x_3, x_1, x_1, \eta) \\ &= \mu \circ (\mu \otimes \mu) \circ (1 \otimes \delta \otimes \eta) \circ (x_3, x_1) \\ &= \mu \circ (\mu \otimes \mu) \circ (1 \otimes \delta \otimes \eta) \circ \tau \circ (x_1, x_3) \\ &= \mu \circ (\mu \otimes \mu) \circ (1 \otimes \delta \otimes \eta) \circ \tau \circ (1 \otimes \varepsilon \otimes 1) \circ (x_1, x_2, x_3). \end{aligned}$$

On a donc obtenu une décomposition de u en générateurs de $\mathcal{L}\Sigma^c$; cependant, les égalités écrites ne sont vraies que lorsque l'on quotiente par $R_{\Delta, \Sigma}$. Pour obtenir $\Phi(u)$, il faut encore mettre cette flèche de $\mathcal{L}\Sigma^c$ en $R_{\Delta, \Sigma}$ -forme normale, ce qui revient à mettre la flèche

$$(1 \otimes \delta) \circ \tau \circ (1 \otimes \varepsilon \otimes 1)$$

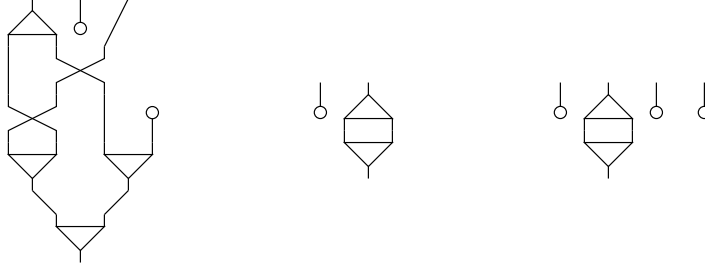
en R_{Δ} -forme normale, ce qui donne, au final :

$$\Phi(u) = \mu \circ (\mu \otimes \mu) \circ (\tau \otimes 1 \otimes \eta) \circ (1 \otimes \tau) \circ (\delta \otimes \varepsilon \otimes 1).$$

La figure 5.11 montre cette même flèche, ainsi que les exemples suivants, sous forme graphique.

De la même façon, on obtiendrait, si $v = \mu(x_2, x_2)$:

$$\Phi(v) = \mu \circ (\varepsilon \otimes \delta).$$


 FIG. 5.11 – Les traductions $\Phi(u)$, $\Phi(v)$ et $\Phi^4(v)$.

Mais :

$$\Phi^4(v) = \mu \circ (\varepsilon \otimes \delta \otimes \varepsilon \otimes \varepsilon).$$

Donnons aussi des exemples de traduction de règles avec la logique combinatoire. Ce système de réécriture possède quatre constructeurs, un d'arité 2 noté μ et trois d'arité 0 notés I , K et S , ainsi que trois règles :

$$\begin{aligned} \mu(I, x) &\rightarrow_I x \\ \mu(\mu(K, x), y) &\rightarrow_K x \\ \mu(\mu(\mu(S, x), y), z) &\rightarrow_S \mu(\mu(x, z), \mu(y, z)). \end{aligned}$$

Ces règles sont ainsi traduites (on les suppose uniformisées avec $x = x_1$, $y = x_2$ et $z = x_3$) :

$$\begin{aligned} \mu \circ (I \otimes 1) &\rightarrow_{\Phi(I)} 1 \\ \mu \circ (\mu \otimes 1) \circ (K \otimes 2) &\rightarrow_{\Phi(K)} 1 \otimes \varepsilon \\ \mu \circ (\mu \otimes 1) \circ (\mu \otimes 2) &\rightarrow_{\Phi(S)} \mu \circ (\mu \otimes \mu) \circ (1 \otimes \tau \otimes 1) \circ (2 \otimes \delta). \end{aligned}$$

La figure 5.12 montre ces règles sous forme graphique.

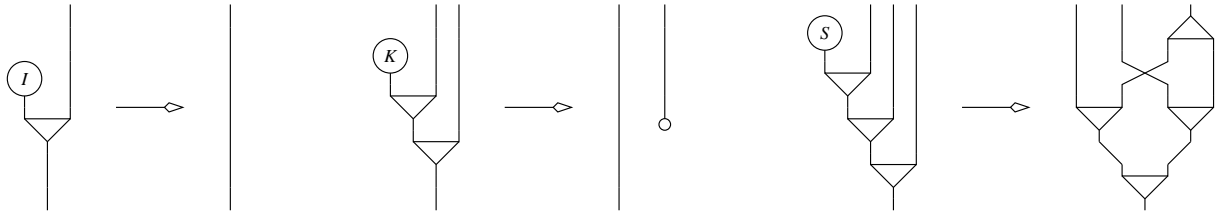


FIG. 5.12 – Les règles de la logique combinatoire sous forme opéradique.

Définition. Si (Σ, R) est un système de réécriture de termes, on note $R^c = \Phi(R) \amalg R_{\Delta, \Sigma}$ et on appelle (Σ^c, R^c) la *présentation d'opérades associée* à (Σ, R) . \blacklozenge

5.5 Liens entre un système de réécriture de termes et sa présentation associée

Le but de ce paragraphe est de prouver le résultat suivant :

Théorème 5.40. *Soit (Σ, R) un système de réécriture de termes (uniformisé). Alors, si (Σ, R) termine en un terme u , sa présentation associée (Σ^c, R^c) termine en toute flèche f vérifiant $f \equiv_{R_{\Delta, \Sigma}} \Phi^n(u)$, pour tout $n \geq \#u$. De plus, si (Σ, R) est linéaire à gauche, alors la présentation $(\Sigma^c, R^c; \Phi)$ est une simulation complète de (Σ, R) .*

On sait déjà que Φ envoie tout terme u sur une $R_{\Delta, \Sigma}$ -forme normale qui est aussi une $R_{\Delta, \Sigma}^t$ -forme normale. De plus, on a déjà vu que $(\Sigma^c, R_{\Delta, \Sigma})$, et donc $(\Sigma^c, R_{\Delta, \Sigma}^t)$ est convergent. Il reste les autres points à vérifier.

5.5.1 Simulation des étapes de réduction

On va démontrer ici que Φ induit un morphisme strict allant de $(T_\Sigma(V), \rightarrow_R)$ vers $(F\mathcal{L}\Sigma, \rightarrow_{\Phi(R)})$. Étant donné que, pour tout u , $\Phi(u)$ est une $R_{\Delta, \Sigma}$ -forme normale, cela revient à montrer que :

Proposition 5.41. *Si α est une règle linéaire à gauche de R , alors on a l'inclusion :*

$$\Phi((\alpha)) \subseteq (R_{\Delta, \Sigma})^{rt} \circ (\Phi(\alpha)),$$

où (α) désigne la relation de réduction sur $T_\Sigma(V)$ engendrée par la règle α . Autrement dit, si u et v sont deux termes tels que $u \rightarrow_\alpha v$, alors il existe une flèche f de $\mathcal{L}\Sigma^c$ telle que :

$$\Phi(u) \rightarrow_{\Phi(\alpha)} f \rightarrow_{R_{\Delta, \Sigma}} \Phi^{\#u}(v).$$

Supposons que u et v sont deux termes de $T_\Sigma(V)$ et que α est une règle uniformisée et linéaire à gauche de R , le tout tel que $u \rightarrow_\alpha v$. Par définition, il existe un contexte C et une substitution σ tels que $u = C[s(\alpha) \cdot \sigma]$ et $v = C[t(\alpha) \cdot \sigma]$. On a besoin de définir un certain nombre de notations.

- La règle α est uniformisée et linéaire à gauche, c'est-à-dire qu'il existe un n tel que :

$$\begin{cases} s(\alpha) = \varphi_\Sigma(s(\alpha)) \circ (x_1, \dots, x_n) \\ \Phi(s(\alpha)) = s(\alpha)_\Sigma \in \mathcal{L}\Sigma(n, 1). \end{cases}$$

- Puisque α est une règle de réécriture sur $T_\Sigma(V)$, on a $V(t(\alpha)) \subseteq V(s(\alpha))$. D'où :

$$\begin{cases} t(\alpha) = t(\alpha)_\Sigma \circ (x_{f^*(1)}, \dots, x_{f^*(n)}) \\ \Phi(t(\alpha)) = t(\alpha)_\Sigma \circ t(\alpha)_\Delta \end{cases}$$

avec $t(\alpha)_\Delta^* = f$.

- On peut aussi associer au contexte C une décomposition similaire, où les y_k sont des variables :

$$C = C_\Sigma \circ (y_1, \dots, y_i, \square, y_i + 1, \dots, y_{i+j}).$$

Ainsi, pour tout terme $t = t_\Sigma \circ (a_1, \dots, a_l)$, on a :

$$C[t] = C_\Sigma \circ (i \otimes t_\Sigma \otimes j) \circ (y_1, \dots, y_i, a_1, \dots, a_l, y_i + 1, \dots, y_{i+j}).$$

- La substitution σ est entièrement déterminée par ses valeurs sur V et, pour ce qui nous intéresse ici, sur les x_1, \dots, x_n . On note alors :

$$\sigma^q = (x_q \cdot \sigma)_\Sigma \quad \text{et} \quad (x_1^q, \dots, x_{k_q}^q) = (x_q \cdot \sigma)_\Delta,$$

ce qui donne :

$$x_q \cdot \sigma = \sigma^q \circ (x_1^q, \dots, x_{k_q}^q)$$

- On obtient donc $\Phi(u) = u_\Sigma \circ u_\Delta$ où :

$$u_\Sigma = C_\Sigma \circ (i \otimes s(\alpha)_\Sigma \otimes j) \circ (i \otimes \sigma^1 \otimes \dots \otimes \sigma^n \otimes j)$$

et $u_\Delta = (z_1, \dots, z_p)$ est la R_Δ -forme normale des flèches de \mathbb{F}° ayant pour flèche duale dans \mathbb{F} l'application $g : [i + k_1 + \dots + k_n + j] \longrightarrow [p]$ telle que

$$\begin{aligned} & (z_{g(1)}, \dots, z_{g(i+k_1+\dots+k_n+j)}) \\ = & (z_1, \dots, z_p) \\ = & (y_1, \dots, y_i, x_1^1, \dots, x_{k_1}^1, \dots, x_1^n, \dots, x_{k_n}^n, y_{i+1}, \dots, y_{i+j}). \end{aligned}$$

- De même, $\Phi^{\sharp u}(v) = v_\Sigma \circ v_\Delta^{\sharp u}$ où :

$$v_\Sigma = C_\Sigma \circ (i \otimes t(\alpha)_\Sigma \otimes j) \circ (i \otimes \sigma^{f(1)} \otimes \dots \otimes \sigma^{f(m)} \otimes j)$$

et $v_\Delta^{\sharp u}$ est la R_Δ -forme normale des flèches de \mathbb{F}° ayant pour flèche duale dans \mathbb{F} l'application $h : [i + k_{f(1)} + \dots + k_{f(m)} + j] \longrightarrow [p]$ vérifiant :

$$\begin{aligned} & (z_{h(1)}, \dots, z_{h(i+k_{f(1)}+\dots+k_{f(m)}+j)}) \\ = & v_\Delta^{\sharp u} \\ = & (y_1, \dots, y_i, x_1^{f(1)}, \dots, x_{k_1}^{f(1)}, \dots, x_1^{f(m)}, \dots, x_{k_{f(m)}}^{f(m)}, y_{i+1}, \dots, y_{i+j}). \end{aligned}$$

Une fois traduite via Φ , la règle α devient :

$$s(\alpha)_\Sigma \longrightarrow_{\Phi(\alpha)} t(\alpha)_\Sigma \circ t(\alpha)_\Delta.$$

D'où :

$$\Phi(u) \rightarrow_{\Phi(\alpha)} C_\Sigma \circ (i \otimes t(\alpha)_\Sigma \otimes j) \circ (i \otimes t(\alpha)_\Delta \otimes j) \circ (i \otimes \sigma^1 \otimes \dots \otimes \sigma^n \otimes j) \circ u_\Delta.$$

Il reste à voir que cette dernière flèche se réduit en un nombre quelconque d'étapes de $R_{\Delta, \Sigma}$ en $\Phi^{\#u}(v)$. Comme cette dernière flèche est une $R_{\Delta, \Sigma}$ -forme normale, il suffit de voir que ces deux flèches sont $R_{\Delta, \Sigma}$ -équivalentes, c'est-à-dire que leurs images dans \mathbb{V} coïncident.

$$\begin{aligned} & (i \otimes \varphi \otimes j) \circ (i \otimes \sigma^1 \otimes \dots \otimes \sigma^n \otimes j) \circ u_\Delta \\ = & (i \otimes \varphi \otimes j) \circ (i \otimes \sigma^1 \otimes \dots \otimes \sigma^n \otimes j) \circ (x_{g(1)}, \dots, x_{g(i+k_1+\dots+k_n+j)}). \end{aligned}$$

On pose alors :

$$(b_1, \dots, b_i, c_1^1, \dots, c_{k(1)}^1, \dots, c_1^n, \dots, c_{k(n)}^n, b_{i+1}, \dots, b_{i+j}) = (x_{g(1)}, \dots, x_{g(i+k_1+\dots+k_n+j)}).$$

D'où :

$$\begin{aligned} & (i \otimes \varphi \otimes j) \circ (i \otimes \sigma^1 \otimes \dots \otimes \sigma^n \otimes j) \circ u_\Delta \\ = & (i \otimes \varphi \otimes j) \circ (b_1, \dots, b_i, \sigma^1 \circ (c_1^1, \dots, c_{k(1)}^1), \dots, \sigma^n \circ (c_1^n, \dots, c_{k(n)}^n), b_{i+1}, \dots, b_{i+j}). \end{aligned}$$

On pose à présent :

$$t_q = \sigma^q \circ (c_1^q, \dots, c_{k(q)}^q).$$

Ainsi :

$$\begin{aligned} & (i \otimes \varphi \otimes j) \circ (i \otimes \sigma^1 \otimes \dots \otimes \sigma^n \otimes j) \circ u_\Delta \\ = & (i \otimes \varphi \otimes j) \circ (b_1, \dots, b_i, t_1, \dots, t_n, b_{i+1}, \dots, b_{i+j}) \\ = & (b_1, \dots, b_i, t_{f(1)}, \dots, t_{f(m)}, b_{i+1}, \dots, b_{i+j}). \end{aligned}$$

D'autre part :

$$\begin{aligned} & (i \otimes \sigma^{f(1)} \otimes \dots \otimes \sigma^{f(m)} \otimes j) \circ v_\Delta^{\#u} \\ = & (i \otimes \sigma^{f(1)} \otimes \dots \otimes \sigma^{f(m)} \otimes j) \circ (x_{h(1)}, \dots, x_{i+k_{f(1)}+\dots+k_{f(m)}+j}) \end{aligned}$$

En regardant de plus près les définitions de g et h , on constate que :

$$\begin{aligned} & (x_{h(1)}, \dots, x_{i+k_{f(1)}+\dots+k_{f(m)}+j}) \\ = & (b_1, \dots, b_i, c_1^{f(1)}, \dots, c_{k_{f(1)}}^{f(1)}, \dots, c_1^{f(n)}, \dots, c_{k_{f(n)}}^{f(n)}, b_{i+1}, \dots, b_{i+j}). \end{aligned}$$

D'où :

$$\begin{aligned} & (i \otimes \sigma^{f(1)} \otimes \dots \otimes \sigma^{f(m)} \otimes j) \circ v_{\Delta}^{\sharp u} \\ = & (i \otimes \sigma^{f(1)} \otimes \dots \otimes \sigma^{f(m)} \otimes j) \\ & \circ (b_1, \dots, b_i, c_1^{f(1)}, \dots, c_{k_{f(1)}}^{f(1)}, \dots, c_1^{f(n)}, \dots, c_{k_{f(n)}}^{f(n)}, b_{i+1}, \dots, b_{i+j}) \\ = & (b_1, \dots, b_i, t_{f(1)}, \dots, t_{f(m)}, b_{i+1}, \dots, b_{i+j}). \end{aligned}$$

On a donc bien le résultat : il existe une flèche γ de $\mathbb{T}\Sigma$ telle que

$$\Phi(u) \rightarrow_{\Phi(\alpha)} \gamma \rightarrow_{R_{\Delta, \Sigma}} \Phi^{\sharp u}(v).$$

En fait, il est aisé de se convaincre que la même démonstration permet de montrer que, pour toute règle α linéaire à gauche et uniformisée, pour tous termes u et v tels que $u \rightarrow_{\alpha} v$ et tout entier $n \geq \sharp u$, il existe une flèche γ de $\mathbb{T}\Sigma$ telle que :

$$\Phi^n(u) \rightarrow_{\Phi(\alpha)} \gamma \rightarrow_{R_{\Delta, \Sigma}} \Phi^n(v).$$

5.5.2 Terminaison

On va ici prouver le point 2 du théorème 5.40. On veut d'abord montrer que, si (Σ, R) est un système de réécriture de termes qui termine, alors (Σ^c, R^c) termine. On va utiliser la technique d'interprétation développée en 3.7, mais avec d'autres valeurs que seulement des entiers. En effet, ne connaissant pas les règles R , il est impossible de fixer des valeurs comme nous l'avons fait jusqu'à présent.

On va plutôt construire un morphisme d'opérades $\mathcal{L}\Sigma^c \longrightarrow \mathcal{O}(T \times \mathbb{N}^*, \{*\}, [\mathbb{N}^*])$. Afin d'alléger les notations, on a noté T l'ensemble des termes. Pour les mêmes raisons, on note \mathcal{O} l'opérade $\mathcal{O}(T \times \mathbb{N}^*, \{*\}, [\mathbb{N}^*])$.

Notons que, pour l'instant, cette dernière notation n'a aucun sens dans la mesure où l'on n'a pas défini les ordres que nous allons utiliser. Pour $[\mathbb{N}^*]$, ce sera le multiordre engendré par l'ordre usuel des entiers. Il faut encore définir une relation d'ordre sur $T \times \mathbb{N}^*$.

On utilise le résultat classique suivant :

Théorème 5.42. *Un système de réécriture de termes (Σ, R) termine si et seulement s'il existe une application $|\cdot| : X \longrightarrow \mathbb{N}$ telle que $|u| > |v|$ dès que $u \rightarrow_R v$. Si tel est le cas, on peut de plus choisir $|\cdot|$ de telle sorte que $|u| \geq |v|$ si v est un sous-terme de u . On peut aussi choisir $|\cdot|$ à valeurs dans tout ensemble dénombrable.*

Démonstration. Si R termine, on pose $|u|$ la longueur du plus long chemin de réduction partant de u ; cela donne bien une application ayant les propriétés recherchées. Réciproquement, si une telle application existe, alors R termine. De plus, si l'on dispose d'une telle application, il suffit de la composer avec un isomorphisme pour l'avoir à valeurs dans un autre ensemble dénombrable, par exemple avec $n \longrightarrow n + 1$ pour arriver dans \mathbb{N}^* . \diamond

Considérons une telle application $|\cdot| : T \longrightarrow \mathbb{N}^*$ telle que :

- $|u| > |v|$ dès que $u \rightarrow_R v$;
- $u \geq v$ si v est un sous-terme de u .

On se sert de cette application pour définir la relation suivante sur T : on pose $u > v$ si, pour tout contexte c , on a $|c[u]| > |c[v]|$. Alors :

Lemme 5.43. *La relation $>$ ainsi définie sur T est un ordre strict qui termine.*

Démonstration. La relation $>$ est un ordre strict sur T , car $>$ en est un sur \mathbb{N}^* . Quant à la terminaison : si $>$ ne terminait pas, il existerait une suite $(u_n)_{n \in \mathbb{N}}$ de termes tels que $u_n > u_{n+1}$ pour tout n et donc, en particulier, une suite $(|u_n|)_{n \in \mathbb{N}}$ d'entiers tels que $|u_n| > |u_{n+1}|$ ce qui est impossible puisque $>$ termine sur \mathbb{N} . \diamond

Puis, on prend comme ordre sur $T \times \mathbb{N}^*$ un ordre lexicographique produit : on pose $(u, i) \geq (v, j)$ si $u > v$ ou si $u = v$ et $i \geq j$. Alors :

Lemme 5.44. *La relation \geq ainsi définie sur $T \times \mathbb{N}^*$ est une relation d'ordre. De plus, l'ordre strict $>$ qui lui est associé termine.*

Démonstration. La réflexivité est évidente. Pour l'antisymétrie, supposons que (u, i) et (v, j) vérifient à la fois $(u, i) \geq (v, j)$ et $(v, j) \geq (u, i)$. Il est impossible d'avoir $u > v$ ou $v > u$; donc $u = v$ et $i \geq j$ et $j \geq i$, ce qui donne bien $(u, i) = (v, j)$. Pour la transitivité, on se donne trois couples (u, i) , (v, j) et (w, k) tels que $(u, i) \geq (v, j)$ et $(v, j) \geq (w, k)$. Alors, quatre situations sont possibles :

- $u > v$ et $v > w$: alors $u > w$ par transitivité de $>$ sur T ;
- $u > v$, $v = w$ et $j \geq k$: alors $u > w$;
- $u = v$, $i \geq j$ et $v > w$: alors $u > w$;
- $u = v$, $v = w$, $i \geq j$ et $j \geq k$: alors, $u = w$ et $i \geq k$.

Dans tous les cas, on a bien $(u, i) \geq (w, k)$. Pour la terminaison, on suppose qu'il existe une suite $(u_n, i_n)_{n \in \mathbb{N}}$ strictement décroissante. Tout d'abord, il existe une suite $(k_n)_{n \in \mathbb{N}}$ strictement croissante d'entiers tels que, pour tout n , $u_{k_n} > u_{k_{n+1}}$; en effet, si ce n'est pas le cas, à partir d'un certain rang n_0 , tous les u_n sont égaux. On en déduit que la suite $(i_{k_{n+1}})_{n \geq n_0}$ d'entiers est strictement décroissante, ce qui est impossible. On a donc une suite $(u_{k_n})_{n \in \mathbb{N}}$ strictement décroissante de termes : le fait que l'ordre que l'on a construit sur T termine nie cette éventualité. \diamond

On considère donc l'opérade \mathcal{O} avec les relations d'ordre ainsi définies. On construit maintenant le foncteur $F : \mathcal{L}\Sigma^c \rightarrow \mathcal{O}$ en donnant ses valeurs sur les flèches de Σ^c ; notons que les applications f^* sont toutes triviales. Pour des raisons de clarté, on notera parfois $(u_1, \dots, u_n; i_1, \dots, i_n)$ l'élément $((u_1, i_1), \dots, (u_n, i_n))$ de $(T \times \mathbb{N}^*)^n$ en utilisant l'isomorphisme canonique :

$$(T \times \mathbb{N}^*)^n \longrightarrow T^n \times (\mathbb{N}^*)^n.$$

On pose :

- $\delta_*(u, i) = (u, u; i, i)$ et $[\delta](u, i) = i.\underline{u}$;
- $\varepsilon_*(u, i) = *$ et $[\varepsilon](u, i) = 0$;
- $\tau_*(u, v; i, j) = (v, u; j, i)$ et $[\tau](u, v; i, j) = 0$;
- si $\gamma \in \Sigma(0, 1)$, $\gamma_*(*) = (\gamma, 1)$ et $[\gamma](*) = \underline{|\gamma|}$;
- si $\varphi \in \Sigma(n, 1)$, $n \geq 1$ alors :

$$\begin{cases} \varphi_*(u_1, \dots, u_n; i_1, \dots, i_n) = (\varphi(u_1, \dots, u_n), 2.(i_1 + \dots + i_n)) \\ [\varphi](u_1, \dots, u_n; i_1, \dots, i_n) = (i_1 + \dots + i_n). \underline{|\varphi(u_1, \dots, u_n)|}. \end{cases}$$

On doit vérifier, dans un premier temps, que toutes ces applications sont croissantes. Regardons les cas de φ_* et de $[\varphi]$, pour une flèche $\varphi \in \Sigma(n, 1)$ fixée, $n \in \mathbb{N}$.

Supposons que u_1, \dots, u_n et v_1, \dots, v_n sont des termes et i_1, \dots, i_n et j_1, \dots, j_n des entiers non nuls tels que $(u_k, i_k) \geq (v_k, j_k)$ pour tout k . On veut montrer que :

$$\varphi(u_1, \dots, u_n) > \varphi(v_1, \dots, v_n) \quad \text{ou} \quad i_1 + \dots + i_n \geq j_1 + \dots + j_n.$$

Soit c un contexte ; puisque $u_k \geq v_k$ et que $c \circ \varphi(v_1, \dots, v_{k-1}, \square, u_k, \dots, u_n)$ est un contexte pour tout k :

$$\begin{aligned} |c[\varphi(u_1, \dots, u_n)]| &\geq |c[\varphi(v_1, u_2, \dots, u_n)]| \\ &\geq \dots \\ &\geq |c[\varphi(v_1, \dots, v_{k-1}, u_k, \dots, u_n)]| \\ &\geq |c[\varphi(v_1, \dots, v_k, u_{k+1}, \dots, u_n)]| \\ &\geq |c[\varphi(v_1, \dots, v_n)]|. \end{aligned}$$

De plus, si $u_k > v_k$ pour au moins un k , au moins l'une de ces inégalités est stricte et donc $\varphi(u_1, \dots, u_n) > \varphi(v_1, \dots, v_n)$. Sinon, on a $\varphi(u_1, \dots, u_n) = \varphi(v_1, \dots, v_n)$ et $i_k \geq j_k$ pour chaque k , ce qui donne $i_1 + \dots + i_n \geq j_1 + \dots + j_n$. Dans tous les cas, on a donc :

$$(\varphi(u_1, \dots, u_n), 2 \cdot (i_1 + \dots + i_n)) \geq (\varphi(v_1, \dots, v_n), 2 \cdot (j_1 + \dots + j_n)).$$

On en conclut que φ_* est croissante. Pour $[\varphi]$, on procède par récurrence sur un compteur $k \in [n]$, en distinguant à chaque fois deux cas. Pour $k = 1$:

- Si $u_1 > v_1$, alors, comme $\varphi(\square, u_2, \dots, u_n)$ est un contexte, on a :

$$|\varphi(u_1, \dots, u_n)| > |\varphi(v_1, u_2, \dots, u_n)|.$$

D'où :

$$(i_1 + \dots + i_n) \cdot \underline{|\varphi(u_1, \dots, u_n)|} > (j_1 + i_2 + \dots + i_n) \cdot \underline{|\varphi(v_1, u_2, \dots, u_n)|}.$$

- Sinon, $u_1 = v_1$ et $i_1 \geq j_1$, ce qui donne :

$$(i_1 + \dots + i_n) \cdot \underline{|\varphi(u_1, \dots, u_n)|} \geq (j_1 + i_2 + \dots + i_n) \cdot \underline{|\varphi(v_1, u_2, \dots, u_n)|}.$$

On répète l'opération pour k quelconque, pour obtenir, dans tous les cas :

$$(i_1 + \dots + i_n) \cdot \underline{|\varphi(u_1, \dots, u_n)|} \geq (j_1 + \dots + j_n) \cdot \underline{|\varphi(v_1, \dots, v_n)|}.$$

Ainsi :

$$[\varphi](u_1, \dots, u_n; i_1, \dots, i_n) \geq [\varphi](v_1, \dots, v_n; j_1, \dots, j_n).$$

Par suite, $[\varphi]$ est croissante.

On va, à présent, montrer que, pour toute règle α de $R_{\Delta, \Sigma}$, on a $F(s(\alpha)) \geq F(t(\alpha))$ et que, pour toute règle α de $\Phi(R)$, on a $F(s(\alpha)) > F(t(\alpha))$.

Pour les règles de R_{Δ} , on a égalité entre $F(s(\alpha))$ et $F(t(\alpha))$, sauf pour les règles 2 et 3, où $[s(\alpha)] > [t(\alpha)]$; regardons, par exemple, la règle 2, l'autre étant similaire :

$$\begin{cases} [(\varepsilon \otimes 1) \circ \delta](u, i) = i \cdot \underline{u} \\ 1^*(u, i) = 0. \end{cases}$$

Pour les règles de $R_{\Sigma/\Delta}$, on fixe une constante $\gamma \in \Sigma(0, 1)$ et une flèche $\varphi \in \Sigma(n, 1)$, avec $n \geq 1$. Avant tout, on vérifie, par récurrence sur $n \geq 1$ que :

- $\varepsilon_*^n(\vec{u}; \vec{i}) = *$;
- $(\delta_n)_*(\vec{u}; \vec{i}) = (\vec{u}, \vec{u}; \vec{i}, \vec{i})$ et $[\delta_n](\vec{u}; \vec{i}) = i_1.\underline{u_1} + \cdots + i_n.\underline{u_n}$;
- $(\tau_{n,1})_*(\vec{u}, v; \vec{i}, j) = (v, \vec{u}; j, \vec{i})$;
- $(\tau_{1,n})_*(u, \vec{v}; i, \vec{j}) = (\vec{v}, u; \vec{j}, i)$.

Puis :

$\gamma\varepsilon$. On a nécessairement :

$$(\varepsilon \circ \gamma)_*(*) = 0_*(*) = *.$$

Puis :

$$\begin{aligned} [\varepsilon \circ \gamma](*) &= [\varepsilon](\gamma, 1) + [\gamma](*) \\ &= \underline{|\gamma|} \\ &> 0 \\ &= [0](*). \end{aligned}$$

$\gamma\delta$. D'une part :

$$(\delta \circ \gamma)_*(*) = (\gamma, \gamma; 1, 1) = (\gamma \otimes \gamma)_*(*) .$$

Puis :

$$\begin{aligned} [\delta \circ \gamma](*) &= [\delta](\gamma, 1) + [\gamma](*) \\ &= 2.\underline{|\gamma|} \\ &= [\gamma \otimes \gamma](*). \end{aligned}$$

$\gamma\tau 1$.

$$(\tau \circ (\gamma \otimes 1))_*(u, i) = (u, \gamma; i, 1) = (1 \otimes \gamma)_*(u, i).$$

$$[\tau \circ (\gamma \otimes 1)](u, i) = \underline{|\gamma|} = [1 \otimes \gamma](u, i).$$

$\gamma\tau 2$. Similaire à $\gamma\tau 1$.

$\varphi\varepsilon$. On a :

$$(\varepsilon \circ \varphi)_*(\vec{u}, \vec{i}) = * = \varepsilon_*^n(\vec{u}, \vec{i}).$$

Puis :

$$\begin{aligned} [\varepsilon \circ \varphi](\vec{u}, \vec{i}) &= [\varphi](\vec{u}, \vec{i}) \\ &= (i_1 + \dots + i_n) \cdot \underline{|\varphi(\vec{u})|} \\ &> 0 \\ &= [\varepsilon^n](\vec{u}, \vec{i}). \end{aligned}$$

$\varphi\delta$. Pour commencer :

$$\begin{aligned} (\delta \circ \varphi)_*(\vec{u}, \vec{i}) &= (\varphi(\vec{u}), \varphi(\vec{u}); 2.(i_1 + \dots + i_n), 2.(i_1 + \dots + i_n)) \\ &= ((\varphi \otimes \varphi) \circ \delta_n)_*(\vec{u}, \vec{i}). \end{aligned}$$

Et :

$$\begin{aligned} &[\delta \circ \varphi](\vec{u}, \vec{i}) \\ &= [\delta](\varphi(\vec{u}), 2.(i_1 + \dots + i_n)) + [\varphi](\vec{u}, \vec{i}) \\ &= 3.(i_1 + \dots + i_n) \cdot \underline{|\varphi(\vec{u})|}. \end{aligned}$$

Or :

$$\begin{aligned} &[(\varphi \otimes \varphi) \circ \delta_n](\vec{u}, \vec{i}) \\ &= 2.[\varphi](\vec{u}, \vec{i}) + [\delta_n](\vec{u}, \vec{i}) \\ &= 2.(i_1 + \dots + i_n) \cdot \underline{|\varphi(\vec{u})|} + i_1 \cdot \underline{u_1} + \dots + i_n \cdot \underline{u_n}. \end{aligned}$$

Comme u_i est un sous-terme de $\varphi(\vec{u})$ pour tout i et par hypothèse sur $|\cdot|$, on a l'inégalité $|\varphi(\vec{u})| \geq |u_i|$ pour tout i . On en conclut donc que :

$$[\delta \circ \varphi](\vec{u}, \vec{i}) \geq [(\varphi \otimes \varphi) \circ \delta_n](\vec{u}, \vec{i}).$$

$\varphi\tau 1$. En premier lieu :

$$\begin{aligned} &(\tau \circ (\varphi \otimes 1))_*(\vec{u}, v; \vec{i}, j) \\ &= (v, \varphi(\vec{u}); j, 2.(i_1 + \dots + i_n)) \\ &= ((1 \otimes \varphi) \circ \tau_{n,1})_*(\vec{u}, v; \vec{i}, j). \end{aligned}$$

Et :

$$\begin{aligned}
 [\tau \circ (\varphi \otimes 1)](\vec{u}, v, \vec{i}, j) &= [\varphi](\vec{u}, \vec{i}) \\
 &= (i_1 + \dots + i_n) \cdot |\varphi(\vec{u})| \\
 &= [1 \otimes \varphi](v, \vec{u}, j, \vec{i}) \\
 &= [(1 \otimes \varphi) \circ \tau_{n,1}](\vec{u}, v, \vec{i}, j).
 \end{aligned}$$

$\varphi\tau 2$. On procède de manière similaire à $\varphi\tau 1$.

Il reste à voir le cas des règles de $\Phi(R)$. Supposons que α est une règle de R et montrons que $F(s(\Phi(\alpha))) > F(t(\Phi(\alpha)))$.

On commence par montrer, par récurrence sur le degré des termes de T :

Lemme 5.45. *Pour tout terme u de T , tout entier n vérifiant $n \geq \sharp u$, tout $\vec{v} \in T^n$ et tout $\vec{i} \in (\mathbb{N}^*)^n$, on a, en notant σ la substitution définie par $\sigma(x_k) = v_k$ si $k \in [n]$ et x_k sinon :*

1. $(\Phi^n(u))_*(\vec{v}, \vec{i}) = (u \cdot \sigma, l)$ pour un certain $l \in \mathbb{N}^*$;
2. $[\Phi^n(u)](\vec{v}, \vec{i}) < \underline{|u \cdot \sigma| + 1}$;
3. si, de plus, u n'est pas une variable, $[\Phi^n(u)](\vec{v}, \vec{i}) \geq \underline{|u \cdot \sigma|}$.

Rappelons que $s(\Phi(\alpha)) = \Phi^{\sharp s}(s(\alpha))$ et que $t(\Phi(\alpha)) = \Phi^{\sharp s}(s(\alpha))$. D'où, si u_1, \dots, u_n sont des termes et i_1, \dots, i_n sont des entiers :

$$s(\Phi(\alpha))_*(u_1, \dots, u_n; i_1, \dots, i_n) = (s(\alpha) \cdot \sigma, k),$$

où σ est la substitution définie par $\sigma(x_i) = u_i$ pour tout $i \in \{1 \dots n\}$ et $\sigma(x_j) = x_j$ si $j > i$ et où k est un entier. De même :

$$t(\Phi(\alpha))_*(u_1, \dots, u_n; i_1, \dots, i_n) = (t(\alpha) \cdot \sigma, k'),$$

avec k' un entier. Maintenant, soit c un contexte. Par définition de la relation de réduction \rightarrow_α , on a :

$$c[s(\alpha) \cdot \sigma] \rightarrow_\alpha c[t(\alpha) \cdot \sigma].$$

Ce qui donne :

$$|c[s(\alpha) \cdot \sigma]| > |c[t(\alpha) \cdot \sigma]|.$$

Ce qui prouve bien que $s(\alpha)_* \geq t(\alpha)_*$.

Pour $[\cdot]$: comme α est une règle de réécriture, $s(\alpha)$ n'est pas une variable et donc :

$$[s(\Phi(\alpha))](\vec{u}; \vec{i}) \geq |s(\alpha) \cdot \sigma|.$$

D'autre part :

$$[t(\Phi(\alpha))](\vec{u}; \vec{i}) < |t(\alpha) \cdot \sigma| + 1.$$

Or, par hypothèse sur $|\cdot|$:

$$|s(\alpha) \cdot \sigma| > |t(\alpha) \cdot \sigma|.$$

Donc :

$$[s(\Phi(\alpha))] > [t(\Phi(\alpha))].$$

On vient donc de montrer que (Σ^c, R^c) termine si et seulement si $(\Sigma^c, R_{\Delta, \Sigma})$ termine, ce que l'on sait déjà.

Maintenant, supposons que (Σ, R) est linéaire à gauche et que (Σ^c, R^c) termine. S'il existait une suite $(u_n)_{n \in \mathbb{N}}$ de termes tels que $u_n \rightarrow_R u_{n+1}$ pour tout n alors, d'après la proposition 5.41, on aurait une suite

$$\Phi(u_0) \twoheadrightarrow_{R^c}^+ \Phi^{\sharp u_0}(u_1) \twoheadrightarrow_{R^c}^+ \cdots \twoheadrightarrow_{R^c}^+ \Phi^{\sharp u_0}(u_n) \twoheadrightarrow_{R^c}^+ \Phi^{\sharp u_0}(u_{n+1}) \twoheadrightarrow_{R^c}^+ \cdots$$

dans $\text{Fl } \mathcal{L}\Sigma^c$, ce qui est impossible par hypothèse; donc (Σ, R) termine.

5.5.3 Confluence

On note π le foncteur associé au quotient de $\mathcal{L}\Sigma^c$ par $R_{\Delta, \Sigma}$: ainsi $\pi : \mathcal{L}\Sigma^c \longrightarrow \mathbb{T}\Sigma$ associe à toute flèche $f \in \mathcal{L}\Sigma^c$ un n -uplet $\pi(f) = (f_1, \dots, f_n)$. Il est aisé de se convaincre de :

Lemme 5.46. *Si f et g sont deux flèches parallèles de $\mathcal{L}\Sigma^c$ telles que $f \rightarrow_{R_{\Delta, \Sigma}} g$ alors $\pi(f) = \pi(g)$. Si f et g sont deux flèches parallèles de but n de $\mathcal{L}\Sigma^c$ telles que $f \rightarrow_{\Phi(R)} g$, alors, pour tout $i \in [n]$, $f_i \twoheadrightarrow_R g_i$. Dans tous les cas, si $f \rightarrow_{R^c} g$ alors $f_i \twoheadrightarrow_R g_i$ pour tout i .*

Nous allons à présent démontrer le troisième point du théorème 5.40 : on suppose donc que (Σ, R) est un système de réécriture de termes linéaire à gauche et uniformisé.

Dans un premier temps, supposons que (Σ, R) est confluent et que l'on a un branchement (f, g, h) dans (Σ^c, R^c) : f , g et h sont trois flèches de $\mathcal{L}\Sigma^c(m, n)$ et vérifient $f \twoheadrightarrow_{R^c} g$ et $f \twoheadrightarrow_{R^c} h$. On en déduit trois n -uplets de termes $\pi(f)$, $\pi(g)$ et $\pi(h)$. D'après le lemme précédent, l'hypothèse (f, g, h) est un branchement nous donne que, pour tout i , (f_i, g_i, h_i)

est un branchement de (Σ, R) ; comme ce dernier est confluent, on définit $k = (k_1, \dots, k_n)$ de telle sorte que chaque k_i ferme le branchement (f_i, g_i, h_i) . Comme (Σ, R) est linéaire à gauche, d'après le point 1 du théorème, la flèche $\Phi^m(k)$ ferme bien le branchement (f, g, h) .

Réciproquement, supposons que (Σ^c, R^c) est confluent et que (u, v, w) est un branchement dans (Σ, R) . Comme ce dernier est linéaire à gauche, ce triplet se relève en un branchement $(\Phi(u), \Phi^{\sharp u}(v), \Phi^{\sharp u}(w))$ de (Σ^c, R^c) , lequel est confluent. On choisit alors une flèche t de $\mathcal{L}\Sigma^c$ qui ferme ce dernier branchement ; de plus, t a pour but 1 : alors, $\pi(t)$ est un terme qui ferme le branchement (u, v, w) de départ.

5.6 Et les systèmes non linéaires à gauche ?

Dans le cas d'un système de réécriture de termes linéaire à gauche, on peut donc simuler la réécriture dans une opérade libre. Sinon, on est obligé de travailler dans un quotient, et donc modulo des relations : il faut explorer des classes d'équivalence. On retrouve donc à ce niveau toutes les difficultés provenant des systèmes de réécriture non linéaires à gauche comme, par exemple, les tests d'égalité pour vérifier si on peut appliquer une règle ayant une variable doublée dans son membre de gauche (cela correspond à explorer une classe d'équivalence).

Le théorème précédent semble prouver que le relèvement des systèmes de réécriture de termes dans une opérade crée des problèmes là où il n'y en avait pas. On peut cependant voir les choses autrement et même montrer que l'on peut résoudre des difficultés.

Pour commencer, le fait que les opérations de gestion des variables soient extérieures au calcul renvoie les problèmes qu'elles créent à l'implantation : par exemple, la présence d'une règle non linéaire à gauche oblige le calculateur à effectuer des tests d'égalité pour vérifier si cette règle est applicable à un terme donné. Le fait d'inclure les opérations de gestion des variables dans le système de réécriture permet de ramener dans la théorie ces difficultés pratiques et permet donc de mieux les étudier.

Nous allons évoquer à présent deux voies à explorer prouvant, pour l'une, que la réécriture en dimension supérieure peut réussir là où la réécriture de termes échoue et laissant espérer, pour l'autre, que la limitation aux règles linéaires à gauche pourrait être contournée.

5.6.1 Réécriture de termes modulo commutativité

La réécriture de termes est très sérieusement limitée dans l'étude de la plupart des structures algébriques. C'est en particulier le cas pour des algèbres possédant des opéra-

teurs commutatifs. La plus simple d'entre elle, celle des magmas commutatifs, ne termine jamais : on a seulement un opérateur μ d'arité 2 et l'équation $\mu(x, y) = \mu(y, x)$. Il est clair que l'on a un chemin de réduction infini :

$$\mu(x, y) \rightarrow_{\mu}(y, x) \rightarrow_{\mu}(x, y) \rightarrow_{\mu}(y, x) \rightarrow \dots$$

Cependant, le fait que les opérateurs cartésiens soient explicites permet de construire une présentation convergente de l'opérade des magmas commutatifs. Comme cette structure algébrique n'est pas véritablement intéressante, on en regarde une autre qui la contient - la terminaison de la plus grande donnera celle de la plus petite.

On considère l'opérade des espaces vectoriels sur le corps $\mathbb{Z}/2\mathbb{Z}$. La présentation de cette opérade, issue de [Laf03], a déjà été donnée en 3.7.7. Nous y avons montré sa terminaison. Comme la confluence locale était déjà connue, on obtient :

Théorème 5.47. *Le couple (Σ, R) est une présentation convergente de l'opérade des espaces vectoriels sur $\mathbb{Z}/2\mathbb{Z}$.*

Analysons ce résultat. La première des choses que l'on constate est que la traduction n'est pas celle qui a été décrite précédemment. En effet, on aurait :

$$\Phi(\mu(x, y) \rightarrow_{\mu}(y, x)) = \mu \rightarrow_{\mu} \tau$$

qui donnerait évidemment un système qui ne termine pas. Il est clair que cette relation doit être prise dans l'autre sens. Ceci provoque alors l'apparition d'une règle non linéaire à gauche. Il faut réaménager les règles de $R_{\Sigma/\Delta}$ pour conserver la confluence. Cependant, le fait que μ soit exactement le symétrique de δ , tant au niveau des sources et buts que du comportement, permet de réutiliser les relations de Δ en les renversant.

Ainsi, on est en présence d'un exemple justifiant à lui seul l'étude de la réécriture en dimension supérieure et, plus particulièrement, des présentations d'opérades : en effet, la structure de $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel ne peut pas être décrite par un système de réécriture de termes (en une dimension) convergent à cause de la relation de commutativité. Cependant, il existe une présentation convergente de l'opérade dont les algèbres dans la catégorie des ensembles sont ces mêmes $\mathbb{Z}/2\mathbb{Z}$ -espaces vectoriels. De plus, on a ainsi un premier exemple de présentation convergente malgré la présence de règles non-linéaires à gauche dans le système de réécriture de termes correspondant.

Cet exemple devrait être suivi par bien d'autres, inaccessibles aux termes : on peut espérer obtenir, prochainement, une présentation convergente de l'opérade des groupes quantiques/algèbres de Hopf ; cette voie de recherche possède de forts liens avec la théorie

des circuits classiques et quantiques, comme évoqué dans [Laf03].

D'autre part, la possibilité de décrire les enchevêtrements, ce qui est tout autant inaccessible aux théories équationnelles, est intéressante : elle ouvre la voie à l'étude de présentations d'objets utilisés dans la théorie tanakienne, reliant, d'une part, des structures sur les groupes quantiques et les algèbres de Hopf et, d'autres part, des structures tressées et en rubans sur les catégories monoïdales.

5.6.2 Le cas des systèmes non linéaires

Nous allons rapidement discuter du cas laissé de côté, celui des règles non linéaires à gauche. Nous venons de voir qu'il existait au moins un cas de présentation d'opérades convergente malgré la présence de règles non linéaires à gauche dans le système de réécriture de termes correspondant. Ceci justifie que l'on explore un peu plus la possibilité de traduire de manière automatique un système de réécriture non linéaire.

Avec la traduction Φ utilisée pour le théorème 5.40, on crée des défauts de confluence pour toute règle non linéaire à gauche. Par exemple, fixons une signature Σ contenant un opérateur binaire φ ainsi qu'un opérateur unaire ψ . Nous allons utiliser la représentation graphique de la figure 5.13.



FIG. 5.13 – Représentation graphique des deux flèches de la signature Σ .

Fixons aussi une règle α :

$$\varphi(x, x) \rightarrow_{\alpha} \psi(x).$$

Cette règle donne $\Phi(\alpha)$ sur $\mathcal{L}\Sigma^c$:

$$\varphi \circ \delta \rightarrow_{\Phi(\alpha)} \psi.$$

La figure 5.14 montre la représentation graphique de $\Phi(\alpha)$.

En rajoutant $\Phi(\alpha)$ à la famille $R_{\Delta, \Sigma}$, on obtient, entre autres, la paire critique montrée par la figure 5.15. Cette paire critique, engendrée par les règles $\Phi(\alpha)$ et $\varphi\delta$, est non confluente, car les deux réductions possibles aboutissent à des R^c -formes normales, clairement distinctes.

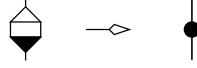
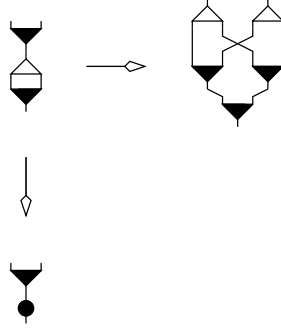

 FIG. 5.14 – Représentation graphique de la règle $\Phi(\alpha)$.


FIG. 5.15 – Un exemple de paire critique créée par une règle non linéaire à gauche.

On montre aisément que le système de réécriture de termes (Σ, R) est convergent : pour la terminaison, l'ordre $>_{\text{Ipo}}$ engendré par $\varphi > \psi$ fonctionne très bien, tandis que la confluence locale est donnée par le fait que α ne crée pas de paire critique avec elle-même (le système de réécriture est *orthogonal*). Cependant, sa traduction (Σ^c, R^c) n'est même pas confluente. On se demande alors s'il existe une présentation convergente (Σ^c, R') , ou éventuellement (Σ', R') , équivalente à (Σ^c, R^c) .

La première piste consiste à appliquer un algorithme de complétion à la présentation (Σ^c, R^c) ; ici, on obtiendra aisément une présentation convergente en renversant $\Phi(\alpha)$. Dans le cas de $L(\mathbb{Z}_2)$, cela fonctionne aussi, quitte à introduire un nouvel opérateur dans la signature. Cependant, la réussite de la complétion semble très dépendante de la présentation étudiée.

Pour les cas où la complétion échoue, on cherche une solution de remplacement : la seconde piste est alors d'implanter dans le calcul les opérations qui manquent pour savoir si une règle non linéaire est applicable ou non à une flèche ; il s'agit, principalement, de coder les tests d'égalité. Cela pourrait se faire, par exemple, en introduisant un nouvel opérateur $\delta^o : 2 \longrightarrow 1$, ainsi que des règles T du type :

$$\begin{aligned} \delta^o \circ (\varphi \otimes \varphi) &\rightarrow_{T_\varphi} \varphi \circ \delta_n^o \\ \delta^o \circ \tau &\rightarrow_{T_\tau} \delta^o \\ \delta^o \circ \delta &\rightarrow_{T_\delta} 1. \end{aligned}$$

La première relation est en fait une famille indexée par les flèches φ de Σ et δ_n^o est défini par récurrence de manière duale à δ_n . Notons qu'il faut aussi ajouter à T des règles de cohérence, comme $T5$ et $T6$, qui sont exactement les mêmes que les règles 5 et 6 de R_Δ .

On pose $\Sigma^t = \Sigma^c \amalg \{\delta^o\}$. Deux flèches $f, g \in \mathcal{L}\Sigma^c(n, 1)$ sont alors égales modulo $R_{\Delta, \Sigma}$ si et seulement si la forme normale de $\delta^o \circ (f \otimes g)$ est une flèche de $\mathcal{L}\Sigma^c$; dans ce cas, la forme normale obtenue est d'ailleurs $f = g$.

Ainsi, une règle du type $\varphi(x, x) \rightarrow \psi(x)$ pourrait être traduite sous la forme d'une règle conditionnelle $\Phi'(\alpha)$ engendrant la relation :

$$\varphi \circ (f \otimes g) \rightarrow_{\Phi'(\alpha)} \psi(h) \quad \text{si } h = T(\delta^o \circ (f \otimes g)) \in \text{Fl}\mathcal{L}\Sigma^c.$$

L'étude de telles règles nécessite cependant de définir un cadre pour la réécriture conditionnelle d'ordre supérieur. Cela mérite d'être exploré, puisque la paire critique de la figure 5.15 est à présent confluente, grâce à une application conditionnée de la règle $\Phi'(\alpha)$, comme la montre la figure 5.16.

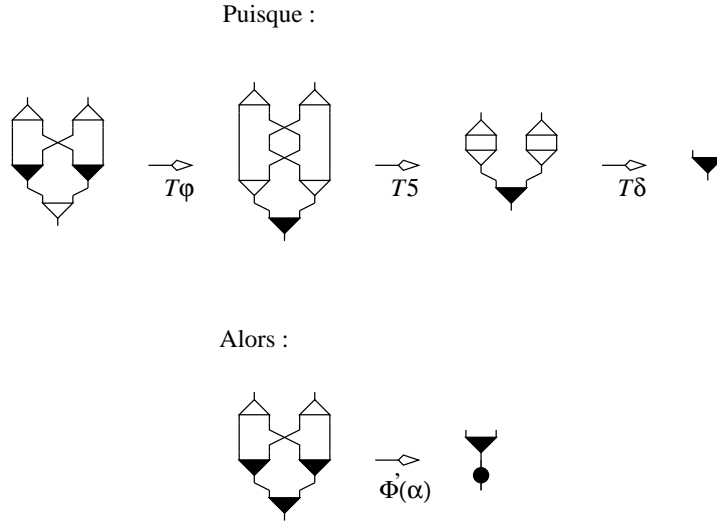


FIG. 5.16 – Exemple d'application conditionnée de la règle $\Phi'(\alpha)$.

Chapitre 6

Vers une présentation diagrammatique du λ -calcul ?

Ce chapitre a pour objet d'examiner les diverses possibilités qui s'offrent à nous, dans le but d'obtenir une présentation *finie* simulant le λ -calcul. De nombreuses pistes ont déjà été explorées, mais aucune n'est, à ce jour, totalement satisfaisante.

Avant tout, rappelons ce qu'est le λ -calcul (non typé et avec β et η réductions), dont on trouvera une description bien plus complète dans [Bar84].

6.1 Le λ -calcul

6.1.1 Ensemble des λ -termes formels

On commence par construire l'ensemble $\bar{\Lambda}$ des λ -termes formels, c'est-à-dire l'ensemble des termes du λ -calcul non typé *avant* quotient par la relation d' α -conversion.

On fixe un ensemble V dénombrable, dont les éléments sont appelés *variables*. Cet ensemble sera supposé fixé dans toute la suite. On construit alors l'ensemble $\bar{\Lambda}$ de la façon suivante :

1. on pose $\bar{\Lambda}^0 = V$;
2. supposons que l'on a construit $\bar{\Lambda}^k$ pour $0 \leq k \leq n$ où n est un entier fixé ; on pose alors :

$$\bar{\Lambda}_\lambda^{n+1} = V \times \bar{\Lambda}^n,$$

dont un élément (x, f) est noté $\lambda x.f$, ainsi que :

$$\bar{\Lambda}_\mu^{n+1} = \coprod_{0 \leq k \leq n} \left(\bar{\Lambda}^k \times \bar{\Lambda}^n \right) \coprod \left(\bar{\Lambda}^n \times \bar{\Lambda}^k \right),$$

dont un élément (f, g) est noté $\mu(f, g)$. Alors, on définit :

$$\bar{\Lambda}^{n+1} = \bar{\Lambda}_\lambda^{n+1} \coprod \bar{\Lambda}_\mu^{n+1}.$$

Enfin, on pose $\bar{\Lambda} = \coprod_{n \in \mathbb{N}} \bar{\Lambda}^n$.

Exemples. Si x, y, z sont des variables, alors x , $\lambda x.\mu(x, y)$, $\lambda x.\mu(\lambda z.x, \lambda y.y)$ et $\mu(z, x)$ sont des λ -termes formels.

Cette construction, plus technique qu'à l'accoutumée, a pour but de définir un *degré* pour les λ -termes formels : pour $f \in \bar{\Lambda}$, on appelle *degré de f* et on note $|f|$ l'entier n tel que $f \in \bar{\Lambda}^n$.

Exemples. $|x| = 0$, $|\lambda x.\mu(x, y)| = 2$, $|\lambda x.\mu(\lambda z.x, \lambda y.\mu(y, y))| = 4$ et $|\mu(z, x)| = 1$.

Enfin, on définit l'ensemble des variables libres d'un λ -terme formel f , noté $\mathcal{V}(f)$ ainsi :

1. si $f \in V$ alors $\mathcal{V}(f) = \{f\}$;
2. si $f = \lambda x.g$ alors $\mathcal{V}(f) = \mathcal{V}(g) \setminus \{x\}$;
3. si $f = \mu(g, h)$ alors $\mathcal{V}(f) = \mathcal{V}(g) \cup \mathcal{V}(h)$.

Exemples.

$$\begin{aligned} \mathcal{V}(x) &= \{x\}, \\ \mathcal{V}(\lambda x.\mu(x, y)) &= \{y\}, \\ \mathcal{V}(\lambda x.\mu(\lambda z.x, \lambda y.\mu(y, y))) &= \emptyset, \\ \mathcal{V}(\mu(z, x)) &= \{x, z\}. \end{aligned}$$

On peut aussi avoir besoin de la notion de λ -termes formels *enrichis de constantes*, comme dans l'appendice B. Soit Γ un ensemble dont les éléments sont appelés *constantes*. On définit l'ensemble $\bar{\Lambda}_\Gamma$ des λ -termes formels avec constantes dans Γ , ou λ_Γ -termes, de la même façon que $\bar{\Lambda}$ mais en posant $\bar{\Lambda}_\Gamma^0 = V \amalg \Gamma$ au lieu de V .

Attention, on ne remplace V par $V \amalg \Gamma$ que pour le degré 0 : si $c \in \Gamma$ et $f \in \bar{\Lambda}_\Gamma$ alors l'expression $\lambda c.f$ n'est pas un λ_Γ -terme formel.

On définit exactement comme pour $\bar{\Lambda}$ les notions de degré et de variables libres d'un λ_Γ -terme.

Exemple. Dans l'appendice B, nous rencontrerons le cas où $\Gamma = \mathbb{N}^*$, l'ensemble des entiers naturels non nuls. Par exemple, si x et y sont des variables, $\lambda x.\mu(y, 4)$ est dans $\bar{\Lambda}_{\mathbb{N}^*}$.

Remarque. L'ensemble $\bar{\Lambda}$ est donc égal à $\bar{\Lambda}_\emptyset$. Pour tout ensemble Γ , il existe donc une inclusion naturelle : $\bar{\Lambda} \hookrightarrow \bar{\Lambda}_\Gamma$. On la note i dans le cas où $\Gamma = \mathbb{N}^*$.

6.1.2 Ensemble des λ -contextes

On poursuit en définissant la notion de contextes sur les λ -termes formels. Ce sont des applications "linéaires" de $\bar{\Lambda}$ sur lui-même. On construit l'ensemble $\mathcal{C}(\bar{\Lambda})$ des λ -contextes de la façon suivante :

1. on pose $\mathcal{C}(\bar{\Lambda})^0 = \{\square\}$ un ensemble réduit à un élément, noté \square et appelé *contexte vide* ;
2. on suppose que l'on a construit $\mathcal{C}(\bar{\Lambda})^k$ pour $0 \leq k \leq n$ où n est un entier fixé ; on définit :
 - $\mathcal{C}(\bar{\Lambda})_{\lambda}^{n+1} = V \times \mathcal{C}(\bar{\Lambda})^n$, dont un élément (x, C) est noté $\lambda x.C$;
 - $\mathcal{C}(\bar{\Lambda})_{\mu_1}^{n+1} = \mathcal{C}(\bar{\Lambda})^n \times \bar{\Lambda}$, dont un élément (C, f) est noté $\mu(C, f)$;
 - $\mathcal{C}(\bar{\Lambda})_{\mu_2}^{n+1} = \bar{\Lambda} \times \mathcal{C}(\bar{\Lambda})^n$, dont un élément (f, C) est noté $\mu(f, C)$;

on pose alors :

$$\mathcal{C}(\bar{\Lambda})^{n+1} = \mathcal{C}(\bar{\Lambda})_{\lambda}^{n+1} \coprod \mathcal{C}(\bar{\Lambda})_{\mu_1}^{n+1} \coprod \mathcal{C}(\bar{\Lambda})_{\mu_2}^{n+1}.$$

Enfin :

$$\mathcal{C}(\bar{\Lambda}) = \coprod_{n \in \mathbb{N}} \mathcal{C}(\bar{\Lambda})^n.$$

En d'autres termes, un λ -contexte est un λ -terme formel contenant, à la place d'une et une seule variable, un caractère spécial noté \square .

Exemples. Par exemple, si x et y sont des variables, $\lambda x.\square$, $\mu(\lambda y.\square, \mu(y, x))$ et $\mu(x, \square)$ sont des λ -contextes.

Si Γ est un ensemble de constantes, on définit de même l'ensemble $\mathcal{C}(\bar{\Lambda}_{\Gamma})$ des contextes sur les λ_{Γ} -termes formels en remplaçant partout $\bar{\Lambda}$ par $\bar{\Lambda}_{\Gamma}$. Les constructions qui suivent se généralisent de la même façon.

Tout comme pour les λ -termes formels, on définit une notion de *degré* pour les λ -contextes : si C est un λ -contexte, alors on pose $|C| = n$ avec n tel que $C \in \mathcal{C}(\bar{\Lambda})^n$. On définit aussi un ensemble de *variables libres* noté $\mathcal{V}(C)$ en fixant $\mathcal{V}(\square) = \emptyset$.

Exemples. Avec les mêmes exemples que précédemment :

$$|\lambda x.\square| = 1, \quad |\mu(\lambda y.\square, \mu(y, x))| = 2, \quad |\mu(x, \square)| = 1.$$

Tout λ -contexte définit une application $\bar{\Lambda} \longrightarrow \bar{\Lambda}$. Si f est un λ -terme formel et C est un λ -contexte, on note $C[f]$ l'image de f par cette application, que l'on définit par récurrence sur le degré du contexte C - le λ -terme formel f est supposé fixé :

1. si $C = \square$, on pose $C[f] = f$;
2. si $C = \lambda x.D$, on pose $C[f] = \lambda x.D[f]$;
3. si $C = \mu(D, g)$, on pose $C[f] = \mu(D[f], g)$;
4. si $C = \mu(g, D)$, on pose $C[f] = \mu(g, D[f])$.

Autrement dit, $C[f]$ est le λ -terme formel obtenu en remplaçant dans C le caractère spécial \square par f . De manière assez évidente, on peut définir l'action d'un λ -contexte C sur un λ -contexte D , notée $C \circ D$, comme le contexte obtenu en remplaçant le symbole \square de C par D . La notation \circ est due au fait que, pour tout λ -terme formel f , $(C \circ D)[f]$ est exactement $C[D[f]]$.

Pour tout λ -contexte C , on définit des notions de *degré sur λ* , noté $|C|_\lambda$, et d'*ensemble de variables liées*, noté $\mathcal{L}(C)$, de la façon suivante :

1. $|\square|_\lambda = 0$ et $\mathcal{L}(\square) = \emptyset$;
2. $|\mu(C, f)|_\lambda = |\mu(f, C)|_\lambda = |C|_\lambda$ et $\mathcal{L}(\mu(C, f)) = \mathcal{L}(\mu(f, C)) = \mathcal{L}(C)$;
3. $|\lambda x.C|_\lambda = |C|_\lambda + 1$ et $\mathcal{L}(\lambda x.C) = \mathcal{L}(C) \cup \{x\}$.

Si f et g sont deux λ -termes formels, on dit que g est un *sous-terme* de f s'il existe un λ -contexte C tel que $f = C[g]$. Si x est une variable, on appelle *occurrence* de x dans f tout sous-terme x de f . Par exemple, le terme x est une occurrence de la variable x dans $\lambda y.x$, mais pas dans $\lambda x.y$. Une occurrence de x dans f (avec $f = C[x]$) est dite *liée* s'il existe des λ -contextes D et E tels que $C = D \circ (\lambda x.E)$; elle est dite *libre* sinon. Par exemple, x possède une occurrence libre dans $\mu(x, y)$, liée dans $\lambda x.x$ et une occurrence de chaque type dans $\mu(\lambda x.x, x)$. On notera qu'une variable x possède une occurrence libre dans un terme f si et seulement si $x \in \mathcal{V}(f)$.

6.1.3 Relation d' α -conversion et λ -termes

L'étape suivante consiste à définir la relation dite d' *α -conversion* sur les λ -termes formels. En λ -calcul, on ne travaille que modulo cette règle. Son sens est le suivant : l'application du λ -contexte $\lambda x.\square$ à un terme f renvoie une *fonction de x* . D'un point de vue mathématique, x devient une variable *muette* (ou *liée*) dans $\lambda x.f$, c'est-à-dire que x peut être remplacé par une autre variable sans changer ce que représente $\lambda x.f$. Cependant, cette transformation ne doit pas changer le statut libre ou lié de chaque occurrence de variable. Il suffit de choisir la nouvelle variable dans le complémentaire de $\mathcal{V}(f)$; c'est d'ailleurs en partie pour que ce soit toujours possible que V a été supposé dénombrable.

On va donc définir, pour tous x et y dans V , une application notée $[x := y]$, associant, à tout λ -terme formel f , le λ -terme formel noté $f[x := y]$, obtenu en remplaçant toutes les occurrences *libres* de x par y , le tout sans provoquer de conflit de nom de variables comme évoqué précédemment.

Dernière remarque. Si on cherche à définir $[x := y]$ de la manière classique sur les λ -termes formels, on va avoir un problème de choix de variable ; pour l'instant, on suppose que l'on a fixé, pour tout terme f et toute variable x , une variable notée $\nu(f, x)$ qui n'est pas dans $\mathcal{V}(f) \cup \{x\}$. Nous verrons par la suite que, sur les λ -termes, un autre choix de $\nu(f, x)$ ne change rien.

Soient x et y deux variables et f un λ -terme formel. On définit $f[x := y]$ par récurrence sur le degré de f :

1. si $f = x$, alors $f[x := y] = y$;
2. si $f \in V$ et $f \neq x$, alors $f[x := y] = f$;
3. si $f = \mu(g, h)$, alors $f[x := y] = \mu(g[x := y], h[x := y])$;
4. si $f = \lambda x.g$ alors $f[x := y] = f$;
5. si $f = \lambda y.g$ et $x \neq y$, alors $f[x := y] = \lambda \nu.((g[y := \nu])[x := y])$ avec $\nu = \nu(g, y)$;
6. si $f = \lambda z.g$ avec $z \notin \{x, y\}$, alors $f[x := y] = \lambda z.(g[x := y])$.

Remarque. Cette définition s'étend aux λ_Γ -termes en posant $c[x := y] = c$ pour toute constante $c \in \Gamma$. On peut aussi définir l'action de $[x := y]$ sur les λ -contextes en posant $\square[x := y] = \square$.

Les résultats suivants sont immédiats :

Lemme 6.1. 1. Pour tout $x \in V$, l'application $[x := x]$ est l'identité.

2. Pour tous $x, y \in V$ et $f \in \bar{\Lambda}$, on a $\mathcal{V}(f[x := y]) = (\mathcal{V}(f) \setminus \{x\}) \cup \{y\}$.

3. Pour tous $x, y \in V$, $C \in \mathcal{C}(\bar{\Lambda})$ et $f \in \bar{\Lambda}$, on a :

$$(C[f])[x := y] = \begin{cases} (C[x := y])[f] & \text{si } x \in \mathcal{L}(C) \\ (C[x := y])[f[x := y]] & \text{sinon.} \end{cases}$$

4. Pour tous $x, y \in V$, $C \in \mathcal{C}(\bar{\Lambda})$ et $f \in \bar{\Lambda}$ tels que $y \notin \mathcal{V}(f)$ et $y \notin \mathcal{V}(C)$, on a :

$$f[x := y][y := x] = f \quad \text{et} \quad C[x := y][y := x] = C.$$

Exemple. On peut calculer $(\lambda y.\mu(x, y))[x := z]$ qui donne $\lambda y.\mu(z, y)$. Par contre $[y := z]$ appliqué au même terme ne change rien puisque celui-ci ne contient pas de y libre.

On peut maintenant définir la *relation d' α -réduction* comme la relation binaire \rightarrow_α sur $\bar{\Lambda}$ suivante : pour tous f et g dans $\bar{\Lambda}$, $f \rightarrow_\alpha g$ si il existe un λ -contexte C , un λ -terme formel h et deux variables x et y vérifiant $f = C[\lambda x.h]$ et $g = C[\lambda y.(h[x := y])]$.

On remarque que \rightarrow_α est réflexive ; ainsi, on peut définir la *relation d' α -conversion* (ou α -équivalence), notée \equiv_α comme la clôture symétrique et transitive de \rightarrow_α . En d'autres termes, deux λ -termes formels f et g vérifient $f \equiv_\alpha g$ si et seulement si il existe des λ -termes formels f_1, \dots, f_k vérifiant :

$$f \rightarrow_\alpha f_1 \leftarrow_\alpha f_2 \rightarrow_\alpha \dots \rightarrow_\alpha f_k \leftarrow_\alpha g.$$

On définit un λ -terme comme une classe d' α -équivalence de λ -termes formels. L'ensemble des λ -termes est noté Λ .

Remarques.

1. Modulo α -conversion, le choix de $\nu(f, x)$ précédemment fait n'a plus d'importance. De plus, pour toutes variables x et y , l'application $[x := y]$ passe au quotient. On a donc une application *canonique* de substitution de variables sur les λ -termes.
2. La classe d'équivalence d'une variable x est $\{x\}$, car il n'existe pas de contexte C tel que x soit de la forme $C[\lambda y.f]$.
3. Il est assez évident que l' α -conversion ne change pas le degré des λ -termes formels. Ainsi, on pourra parler du *degré* d'un λ -terme. De plus, par définition, l' α -conversion est compatible avec la structure des λ -termes formels ; par exemple, si $f \equiv_\alpha g$, alors, pour tout $x \in V$, $\lambda x.f \equiv_\alpha \lambda x.g$. On a donc : les λ -termes de degré 0 sont les ensembles $\{x\}$ pour $x \in V$, et les λ -termes f de degré $n + 1$ sont d'une des formes suivantes :
 - f est la classe de $\lambda x.g$ avec g un λ -terme formel de degré n ;
 - f est la classe de $\mu(g, h)$ avec g et h deux λ -termes formels, g de degré n et h de degré $\leq n$ ou inversement.
4. Dans la suite, on va commettre l'abus suivant : on notera $f = g$ pour f est la classe de g ou g est un représentant de f .

6.1.4 Les deux règles de réécriture du λ -calcul

Relation de β -réduction

La relation de β -réduction permet de calculer avec les λ -termes. On doit d'abord définir le *remplacement d'une variable x par un λ -terme g dans un λ -terme f* , opération que l'on note $[x := g]$ et dont le résultat est écrit $f[x := g]$.

On définit, toujours par récurrence sur le degré de f :

1. si $f = x$, alors $f[x := g] = g$;
2. si $f \in V$ et $f \neq x$, alors $f[x := g] = f$;
3. si $f = \mu(h, k)$, alors $f[x := g] = \mu(h[x := g], k[x := g])$;
4. si $f = \lambda x.h$, alors $f[x := g] = f$;
5. si $f = \lambda y.h$ avec $y \in V$ choisi tel que $y \neq x$ et $y \notin \mathcal{V}(g)$, alors :

$$f[x := g] = \lambda y.(h[x := g]).$$

On définit alors la relation \rightarrow_β de β -réduction comme la relation binaire sur Λ suivante : si f et g sont deux λ -termes, alors $f \rightarrow_\beta g$ si il existe un λ -contexte C , deux λ -termes h et k et une variable x vérifiant $f = C[\mu(\lambda x.h, k)]$ et $g = C[h[x := k]]$.

On appelle λ_β -calcul (*non typé*) le couple $(\Lambda, \rightarrow_\beta)$.

Relation d' η -réduction

La relation d' η -réduction est une égalité fonctionnelle : si un λ -terme f évalué - *via* β -réduction - en chaque terme a donne toujours $\mu(g, a)$, où g est un terme indépendant de a , alors f et g devraient être identifiés. C'est le rôle de l' η -réduction.

On définit la relation d' η -réduction \rightarrow_η comme la relation binaire sur Λ donnée par $f \rightarrow_\eta g$ s'il existe un λ -contexte C , une variable x et un terme h tels que :

$$\begin{cases} x \notin \mathcal{V}(h) \\ f = C[\lambda x.\mu(h, x)] \\ g = C[h] \end{cases}$$

On définit alors sur Λ la relation $\rightarrow_{\beta\eta} = \rightarrow_\beta \cup \rightarrow_\eta$ et on appelle $\lambda_{\beta\eta}$ -calcul (*non typé*) le couple $(\Lambda, \rightarrow_{\beta\eta})$.

6.2 Le premier modèle : la logique combinatoire

La logique combinatoire est un système de réécriture de termes, au sens classique, c'est-à-dire comme défini au chapitre 5. Elle est définie par la signature Σ possédant une flèche $\mu : 2 \rightarrow 1$ et trois constantes $S, K, I : 0 \rightarrow 1$, ainsi que par l'ensemble R de trois règles :

$$\begin{aligned} \mu(I, x) &\rightarrow_I x \\ \mu(\mu(K, x), y) &\rightarrow_K x \\ \mu(\mu(S, x), y), z) &\rightarrow_S \mu(\mu(x, z), \mu(y, z)). \end{aligned}$$

Intuitivement, il s'agit, comme le λ -calcul, de décrire comment une fonction explicite s'applique à un argument : I est l'identité, K est un effaceur et S un duplicateur. On a une traduction Ψ des termes de la logique linéaire vers les λ -termes donnée par :

- $\Psi(x) = x$;
- $\Psi(\mu(u, v)) = \mu(\Psi(u), \Psi(v))$;
- $\Psi(I) = \lambda x.x$;
- $\Psi(K) = \lambda xy.x$;
- $\Psi(S) = \lambda xyz.\mu(\mu(x, z), \mu(y, z))$.

On a aussi une traduction Φ dans l'autre sens. On doit d'abord définir, pour tout $x \in V$, une application $\varphi_x : T_\Sigma(V) \longrightarrow T_\Sigma(V)$, ce que l'on fait par récurrence sur le degré des termes :

- $\varphi_x(x) = I$;
- $\varphi_x(u) = \mu(K, u)$ si $x \notin V(u)$;
- $\varphi_x(\mu(u, v)) = \mu(\mu(S, \varphi_x(u)), \varphi_x(v))$ sinon.

Notons que, si u est un terme tel que $u \neq x$ et $x \in V(u)$, alors u est forcément de degré au moins 1, ce qui nous assure que, dans le troisième cas, u est bien de la forme $\mu(v, w)$. On définit Φ :

- $\Phi(x) = x$;
- $\Phi(\mu(f, g)) = \mu(\Phi(f), \Phi(g))$;
- $\Phi(\lambda x.f) = \varphi_x(\Phi(f))$.

Cependant, ces traductions de termes n'induisent pas des morphismes d'ARS. Par exemple, si l'on considère le λ -terme représenté par $f = \lambda x.\mu(\lambda y.y, x)$, sa traduction en logique combinatoire est :

$$\begin{aligned}
 \Phi(\lambda x.\mu(\lambda y.y, x)) &= \varphi_x \Phi(\mu(\lambda y.y, x)) \\
 &= \varphi_x \mu(\Phi(\lambda y.y), \Phi(x)) \\
 &= \mu(\mu(S, \varphi_x \varphi_y \Phi(y)), \varphi_x(x)) \\
 &= \mu(\mu(S, \varphi_x \varphi_y(y)), I) \\
 &= \mu(\mu(S, \varphi_x(I)), I) \\
 &= \mu(\mu(S, \mu(K, I)), I).
 \end{aligned}$$

Or ce dernier terme est une R -forme normale, alors que f se β -réduit en $\lambda x.x$, dont l'image par Φ est I . On a donc deux λ -termes f et g tels que $f \rightarrow_{\beta\eta} g$ mais on n'a pas $\Phi(f) \rightarrow_R \Phi(g)$.

Dans la littérature, ce problème est connu sous le nom de *non préservation de la règle ξ* , c'est-à-dire Φ ne vérifie pas :

$$\Phi(f) \equiv_r \Phi(g) \implies \Phi(\lambda x.f) \equiv_r \Phi(\lambda x.g).$$

Pour une étude plus approfondie, on pourra se référer à [Sel02].

Donnons un autre inconvénient de cette traduction : elle apparaît plus comme un accident lié à la nature du λ -calcul que comme une manière profonde d'interpréter les termes. Ainsi, il est loin d'être évident de trouver une traduction du même type pour d'autres systèmes de réécriture d'ordre supérieur, tels que le π -calcul [MPW92] ou le calcul des Ambients [CG00].

6.3 D'autres termes : les calculs de substitutions explicites

L'objectif de cette piste, très active, peut être résumé par le problème 88 de la liste RTA de problèmes ouverts, voir [RTA] : est-ce qu'il existe une simulation complète du λ -calcul par un système de réécriture de termes de présentation finie qui inclut, dans ses règles, des opérations simulant la substitution du λ -calcul.

En effet, cette opération est *externe* au calcul. Pourtant, afin d'implanter le mécanisme de β -réduction, on doit être capable de décrire explicitement son fonctionnement : il faut pouvoir calculer le terme $f[x := g]$ pour toute variable x et tous termes f et g , afin d'obtenir le résultat de la β -réduction appliquée à $(\lambda x.f)g$.

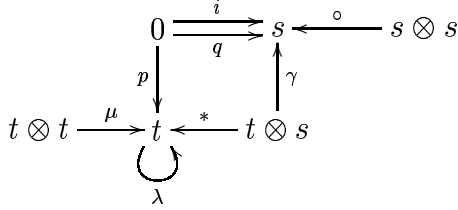
Les calculs de substitutions explicites décrivent plus fidèlement de telles implantations : ils étendent la signature du calcul de telle sorte que $f[x := g]$ corresponde à un terme du calcul et non plus au résultat de l'évaluation ; puis, à la règle de β -réduction ainsi affaiblie, est adjoint un calcul convergent dont le but est de faire disparaître les substitutions introduites. Ainsi, l'évaluation a été catégorifiée, en remplaçant les λ -termes par des composantes connexes d'un ARS plus grand. C'est cette même idée qui a déjà été utilisée au chapitre 5 pour expliciter les opérations de gestion des ressources d'un système de réécriture de termes linéaire à gauche.

Il existe à présent de nombreux calculs de substitutions explicites, divers, dont nous allons citer les plus connus.

Le premier calcul de substitutions explicites est dû à Nicolaas de Bruijn, [dB78], et est directement lié à son travail sur les indices, dans [dB72]. En effet, en développant une

alternative à l'utilisation des variables dans le λ -calcul, les *indices de de Bruijn*, cet auteur a obtenu des relations algébriques vérifiées par les substitutions. C'est en orientant ces relations qu'il a obtenu le calcul appelé $C\lambda\xi\varphi$.

Puis, en 1991, vint le $\lambda\sigma$ -calcul de Martin Abadi, Luca Cardelli, Pierre-Louis Curien et Jean-Jacques Lévy [ACCL91]. Il s'agit d'un système de réécriture de termes avec deux sortes t et s , la première correspondant aux termes et la seconde aux substitutions. Il est donné par la signature Σ à deux couleurs, t et s :



Les notations utilisées ne sont pas les mêmes que celles de [ACCL91], mais permettront de passer plus rapidement à celles de l'appendice B. Les règles de ce calcul sont au nombre de 11 (a et b sont des variables de type t et s_1 et s_2 de type s) :

$$\begin{aligned}
 \mu(\lambda a, b) &\rightarrow a * \gamma(b, i) \\
 p * i &\rightarrow p \\
 p * \gamma(a, s_1) &\rightarrow a \\
 \mu(a, b) * s_1 &\rightarrow \mu(a * s, b * s_1) \\
 \lambda a * s_1 &\rightarrow \lambda(a * \gamma(p, s_1 \circ q)) \\
 (a * s_1) * s_2 &\rightarrow a * (s_1 \circ s_2) \\
 i \circ s_1 &\rightarrow s_1 \\
 q \circ i &\rightarrow q \\
 q \circ \gamma(a, s_1) &\rightarrow s_1 \\
 \gamma(a, s_1) \circ s_2 &\rightarrow \gamma(a * s_2, s_1 \circ s_2) \\
 (s_1 \circ s_2) \circ s_3 &\rightarrow s_1 \circ (s_2 \circ s_3).
 \end{aligned}$$

Les λ -termes sont traduits en termes du $\lambda\sigma$ -calcul de la même façon que pour $C\lambda\xi\varphi$, c'est-à-dire en remplaçant les variables par les indices de de Bruijn. Avec cette traduction, le sous-ensemble des $\lambda\sigma$ -termes clos, c'est-à-dire des termes sans variable, simule complètement le λ -calcul. Cependant, l'utilisation des λ -termes comme modèles pour les preuves nécessite d'avoir aussi cette propriété pour les termes non clos, qui représentent les preuves partielles. Or, le $\lambda\sigma$ -calcul ne possède pas cette propriété : il n'est pas confluent sur les termes ouverts et, comme l'a montré Paul-André Melliès [Mel95], il peut ne pas terminer sur des λ -termes où la β -réduction termine, y compris des termes typables.

Une variante du $\lambda\sigma$ -calcul, le $\lambda\sigma_{\text{ff}}$ -calcul de Pierre-Louis Curien, Thérèse Hardin et Jean-Jacques Lévy [CHL96], corrige l'un de ces défauts en obtenant la confluence sur les termes ouverts.

Un autre calcul, $\lambda\nu$, dû à Pierre Lescanne [Les94], possède, quant à lui, la propriété de préserver la terminaison, c'est-à-dire qu'il termine sur tout élément correspondant à un λ -terme sur lequel la β -réduction termine. Ce calcul est étudié en détails par Zine-El-Abidine Benaïssa, Daniel Briaud, Pierre Lescanne et Jocelyne Rouyer-Degli [BBLR96]. Notons que ce même article contient une version modernisée du calcul $C\lambda\xi\varphi$ de Nicolaas de Bruijn, ainsi qu'une variante, le $\lambda\xi\varphi$ -calcul, elle aussi due à Pierre Lescanne.

D'autres calculs ont aussi vu le jour en essayant de concilier ces deux propriétés ainsi que celle de préserver les étapes de β -réduction. Citons λxgc de Roel Bloo et Kristoffer Rose [BR95], λs de Fairouz Kamareddine et Alejandro Ríos [KR95], $\lambda\zeta$ de César Muñoz [Mun96] et λws de René David et Bruno Guillaume [DG01]. Notons que, contrairement aux trois derniers qui utilisent, eux aussi, des indices de de Bruijn, le premier contient des variables. Parmi les calculs qui n'utilisent pas non plus les indices, citons aussi $\lambda\chi$ de Pierre Lescanne et Jocelyne Rouyer-Degli [LR95], qui est construit à l'aide des *niveaux* de de Bruijn.

Enfin, citons des avancées récentes dans le domaine des substitutions explicites. Dans [KL], Delia Kesner et Stéphane Lengrand introduisent λlxr et développent un lien avec les réseaux de preuve, dont nous parlerons plus loin. Dans [Kes00], Delia Kesner commence une axiomatisation de la notion de calcul de substitutions explicites, permettant d'initier un rapprochement entre différents calculs existant. Enfin, dans [LLDDB04], Stéphane Lengrand, Pierre Lescanne, Dan Dougherty, Mariangiola Dezani-Ciancaglini et Steffen van Bakel décrivent un système de types d'intersection pour un calcul de substitutions explicites, caractérisant les termes sur lesquels le calcul termine.

Malgré de nombreuses tentatives, il n'existe pas, à ce jour, de système de réécriture de termes de présentation finie (c'est-à-dire avec un nombre fini de sortes, de générateurs et de règles) simulant complètement la β -réduction du λ -calcul. On pourra consulter [Bon01] pour une synthèse bien plus complète concernant certains des calculs mentionnés ici.

Avant de passer au paragraphe suivant, mentionnons l'appendice B : on y montre que, si l'on part de la signature du $\lambda\sigma$ -calcul et que l'on quotiente par $t = s$ (on identifie les sortes) et $* = \circ$ (on identifie l'application et la composition), la traduction en indices de de Bruijn donne une injection de $\Lambda / \equiv_{\beta\eta}$ dans le C -monoïde initial. Cette structure contient en effet tout le nécessaire pour construire des calculs de substitutions explicites : trouver une simulation complète du λ -calcul à l'aide de cette structure consiste alors à trouver une présentation convergente de la structure du C -monoïde initial (ou au moins

d'une partie de celle-ci). On trouvera, toujours dans l'appendice B, une étude de l'une de ces présentations, finie, qui est une simulation (non complète) du λ -calcul muni seulement de la β -réduction.

6.4 Troisième voie : divers calculs graphiques

Ce paragraphe présente succinctement trois modèles graphiques, en dimension 2, du λ -calcul.

6.4.1 Le calcul de Lamping

Ce modèle graphique du λ -calcul a pour but d'optimiser la réduction, grâce à une notion de partage. La référence initiale est [Lam90], mais on trouvera une version plus lisible et plus détaillée dans [AG98].

Pour faire le lien avec les présentations d'opérades, disons que les termes sont traduits comme des flèches d'une opérade, mais qui n'est pas libre. Cette opérade possède, comme signature, des flèches λ et μ correspondant aux opérateurs du λ -calcul, plus des opérateurs ressemblant fortement à ceux d'une opérade souveraine, en particulier une évaluation et une coévaluation ; nous reviendrons sur cette notion d'opérade souveraine plus loin. On ajoute encore des opérateurs ressemblant aux flèches de Δ , qui vont permettre la gestion des ressources, mais dans des versions numérotées.

Le tout est quotienté par un certain nombre de relations, ressemblant à celles de l'opérade des enchevêtrements et correspondant à des isotopies en trois dimension des circuits représentant les flèches, c'est-à-dire que l'on peut faire se croiser les fils et que l'on considère l'évaluation et la coévaluation comme des fils et non comme des flèches.

Le problème de ce calcul est qu'il nécessite une quantité infinie de générateurs et de relations. Nous verrons pourquoi, si l'on essaye de se restreindre à une présentation finie, le calcul s'effondre.

6.4.2 Les réseaux d'interaction

Les réseaux d'interaction sont des systèmes de calcul 2-dimensionnels et intrinsèquement parallèles créés par Yves Lafont, voir [Laf90]. À ce titre, ils ressemblent très fortement à des quotients de présentations d'opérades, avec des conditions imposées sur les règles.

Frédéric Lang a étudié, dans sa thèse [Lan98], une implantation de la β -réduction dans des réseaux d'interaction, inspirée du calcul de Lamping, mais en éliminant des com-

plications nécessaires à l'optimalité. Il obtient ainsi un algorithme, appelé *RINO* pour Réseau d'Interaction Non Optimal, qui permet d'effectuer des β -réductions dans des réseaux d'interaction. Le même problème que pour l'algorithme de Lamping apparaît alors : il est nécessaire d'avoir un nombre infini de générateurs.

Sylvain Lippi a proposé, dans [Lip02], une traduction du λ -calcul en termes de réseaux d'interaction. En fait, il s'agit plutôt de deux traductions, chacune simulant un type de stratégies de réduction sur les λ -termes. Ainsi, on est obligé d'utiliser des opérateurs annexes, l'encodage et le décodage, ainsi que des règles décrivant leur comportement vis-à-vis des autres opérateurs, pour passer d'une traduction à l'autre. On n'a donc pas de simulation, puisque l'on n'est pas sûr de pouvoir obtenir $\Phi(f) \rightarrow \Phi(g)$ dès que $f \rightarrow_{\beta} g$. Cependant, ce calcul est de présentation finie et l'idée sous-jacente paraît décrire plus la nature des variables liées et des substitutions que le λ -calcul lui-même, ce qui est intéressant en vue de l'utiliser pour traduire d'autres systèmes de réécriture d'ordre supérieur.

6.4.3 Les réseaux de preuves

Les réseaux de preuves associés au fragment multiplicatif exponentiel de la logique linéaire (MELL) fournissent un autre moyen de traduire le λ -calcul sous forme graphique, assez similaire aux deux précédentes traductions. Nous n'allons pas nous étendre sur le sujet, très vaste et complexe, de la logique linéaire.

L'intérêt principal de cette traduction est qu'elle fournit une simulation complète du λ -calcul. Pourtant, elle possède plusieurs inconvénients.

Le premier est qu'elle nécessite encore de la structure externe au calcul : la boîte. Il s'agit d'une opération agissant formellement sur les réseaux, de sorte que, pour chaque réseau π , on a autre réseau $\Box\pi$ qui est différent du précédent. On n'a donc pas une structure décrite de manière équationnelle, similaire à celle de Burroni pour les opérades cartésiennes.

Le deuxième inconvénient provient de la forme des règles : la boîte est utilisée pour en définir certaines, comme celle donnant l'action de la contraction (qui correspond à un duplicateur). Ainsi, on a une quantité infinie de règles, dont certaines sont, qui plus est, globales, c'est-à-dire qu'elles ne sont pas définies seulement sur une partie limitée du réseau mais sur tout le réseau. C'est le cas de la règle de duplication, ce qui oblige à avoir une opération de duplication globale des réseaux, comme dans le cas de la réécriture de termes. Ce dernier problème est un frein conséquent à l'utilisation du parallélisme dans la réduction des réseaux de preuves.

Un moyen de remédier à cela consiste à réutiliser le calcul de Lamping pour supprimer les boîtes. Ceci a été fait dans [AGL92]. Cependant, on en revient à une présentation ayant une infinité de générateurs et de relations.

Une piste intéressante est celle du calcul des structures, développé par Alessio Guglielmi, voir [GS01]. Son principal intérêt est que l'on peut décomposer des règles non locales de MELL en règles atomiques. Ceci, combiné à la définition de réseaux de preuves pour le calcul des structures, pourrait permettre de se restreindre à une présentation finie, sans boîte.

6.5 Une présentation d'opérades associée au λ -calcul ?

Nous allons évaluer ici la possibilité de simuler complètement le λ -calcul à l'aide une présentation d'opérade. On veut expliciter deux types d'opérations externes au calcul : la gestion des ressources et la substitution.

6.5.1 Une opérade souveraine pour le λ -calcul linéaire

Regardons, dans un premier temps, le cas du λ -calcul linéaire : ces termes n'ont pas besoin de gestion des ressources pour être réduits, ce qui permet de se concentrer sur les opérations de substitution.

Commençons par définir ce qu'est le λ -calcul linéaire. On limite l'ensemble des λ -termes à ceux qui sont dits linéaires et définis comme suit :

Définition. Un λ -terme f est dit *linéaire* si les deux conditions suivantes sont remplies :

1. pour tout sous-terme de f de la forme $\mu(g, h)$, les variables libres de g et de h sont distinctes ;
2. pour tout sous-terme de f de la forme $\lambda x.g$, le terme g contient une et une seule occurrence libre de la variable x .

On note Λ_I l'ensemble des termes linéaires du λ -calcul. ◆

On démontre aisément que :

Lemme 6.2. *Si f est un λ -terme linéaire et que g est un λ -terme tel que $f \rightarrow_{\beta\eta} g$, alors g est linéaire.*

Notre but est alors de simuler l'ARS $(\Lambda_I, \rightarrow_{\beta\eta})$ à l'aide d'une présentation d'opérade (Λ, R) . Comme l'ont montré les travaux de Burroni et de Lafont dans d'autres cas, la première étape de cette démarche est de trouver une présentation équationnelle du λ -calcul linéaire, c'est-à-dire une présentation d'opérade (Λ, R) ainsi qu'une injection de $\Lambda_I / \equiv_{\beta\eta}$

dans $\mathcal{L}\Lambda / \equiv_R$. L'étape suivante consistera à essayer de trouver une présentation convergente de $\mathcal{L}\Lambda / \equiv_R$.

Pour l'instant, nous allons nous contenter de proposer un candidat pour (Λ, R) et de discuter de la possibilité de lui trouver une présentation convergente.

Dans le λ -calcul, on a deux opérations : l'application μ et l'abstraction λ . L'application semble se comporter comme un opérateur classique de la réécriture de termes : par exemple, les substitutions se propagent dans ses sous-termes sans être modifiées ; on va lui associer un opérateur $\mu : 2 \longrightarrow 1$ classique.

En revanche, l'abstraction est essentiellement différente : d'une part, une de ses entrées reçoit uniquement des variables ; d'autre part, les substitutions ne se propagent pas normalement à travers une abstraction. Pour le premier problème, on va *colorier* avec des couleurs différentes l'entrée "termes" et l'entrée "variables" de l'abstraction. Pour le second, on va propager les substitutions par un autre chemin, *via* des opérateurs non algébriques spéciaux : l'évaluation et la coévaluation, données par une structure souveraine.

Pour une étude très complète des catégories munies de structures similaires, on pourra se référer à [Mal95]. Pour la suite, il nous suffit cependant de donner la définition suivante :

Définition. Une catégorie monoïdale stricte $(\mathcal{C}, \otimes, *)$ est dite *souveraine (stricte)* si, pour tout objet x de \mathcal{C} , il existe un objet x^o dans \mathcal{C} , appelé le *dual* de x , ainsi que deux flèches $\eta_x : x^o \otimes x \longrightarrow *$ et $\gamma_x : * \longrightarrow x \otimes x^o$, vérifiant :

- $(x^o)^o = x$;
- $*^o = *$ et $\eta_* = \gamma_* = *$;
- $(x \otimes \eta_x) \circ (\gamma_x \otimes x) = x$;
- $(\eta_x \otimes x^o) \circ (x^o \otimes \gamma_x) = x^o$.

◆

On propose alors comme candidat l'opérade symétrique souveraine librement engendrée par la signature réduite à deux flèches $\mu : t \otimes t \longrightarrow t$ et $\lambda : t \otimes l \longrightarrow t$, avec la dualité engendrée par $t^o = l$. Cette opérade admet une présentation (Λ, R) que nous allons donner. La signature Λ est constituée de douze flèches :

$$\begin{array}{c} \tau_{tt} \left(t \otimes t \xrightarrow{\mu} t \xleftarrow{\lambda} t \otimes l \xleftarrow{\lambda^o} l \xrightarrow{\mu^o} l \otimes l \right) \tau_{ll} \\ \begin{array}{c} \uparrow \eta_l \\ \downarrow \gamma_t \end{array} \begin{array}{c} \nearrow \tau_{tl} \\ \searrow \tau_{lt} \end{array} \\ \begin{array}{c} 0 \xrightarrow{\gamma_l} l \otimes t \\ \xleftarrow{\eta_t} \end{array} \end{array}$$

Les deux opérateurs λ et μ correspondent aux constructeurs de l'ensemble des λ -termes (formels) : μ à l'application et λ à l'abstraction. Notons que les deux arguments de λ sont ici inversés et ce pour des raisons de simplification de la relation correspondant à la β -réduction. Les opérateurs η_x et γ_x jouent respectivement le rôle d'une évaluation et d'une coévaluation. Les flèches duales λ^o et μ^o peuvent être vues comme des termes en cours d'évaluation. La figure 6.1 donne une représentation graphique des flèches de la signature Λ .

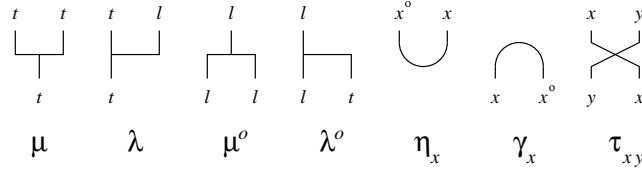


FIG. 6.1 – Représentations graphiques des douze flèches de la signature Λ .

Les relations ressemblent à celles de l'opérade des enchevêtrements orientés, bien qu'en nombre inférieur étant donné que l'on ne considère qu'un type de croisement entre deux brins donnés. On définit R comme l'ensemble des 35 relations :

$$B. \mu \circ (\lambda \otimes l) = t \otimes \eta_t;$$

$$E. \lambda \circ (\mu \otimes l) \circ (t \otimes \gamma_t) = t;$$

$$\gamma_l \eta_t. \eta_t \circ \gamma_l = 0;$$

$$\gamma_x \eta_x. (x \otimes \eta_x) \circ (\gamma_x \otimes x) = x \text{ pour tout } x \in \{t, l\};$$

$$\eta_x \gamma_x. (\eta_x \otimes x^o) \circ (x^o \otimes \eta_x) = x^o \text{ pour tout } x \in \{t, l\};$$

$$\tau \eta_t. \eta_t \circ \tau_t = \eta_l;$$

$$\gamma_t \tau. \tau_{tl} \circ \gamma_t = \gamma_l;$$

$$5xy. \tau_{yx} \circ \tau_{xy} = x \otimes y \text{ pour tous } x, y \in \{t, l\};$$

$$6xyz. (z \otimes \tau_{xy}) \circ (\tau_{xz} \otimes y) \circ (x \otimes \tau_{yz}) = (\tau_{yz} \otimes x) \circ (y \otimes \tau_{xz}) \circ (\tau_{xy} \otimes z) \text{ pour tous } x, y, z \in \{t, l\};$$

$$\mu x. \tau_{tx} \circ (\mu \otimes x) = (x \otimes \mu) \circ (\tau_{tx} \otimes t) \circ (t \otimes \tau_{tx}) \text{ pour tout } x \in \{t, l\};$$

$$\lambda x. \tau_{tx} \circ (\lambda \otimes x) = (x \otimes \lambda) \circ (\tau_{tx} \otimes t) \circ (t \otimes \tau_{tx}) \text{ pour tout } x \in \{t, l\};$$

$$\mu \eta. \eta_t \circ (l \otimes \mu) = \eta_t \circ (l \otimes \eta_t \otimes t) \circ (\mu^o \otimes t \otimes t);$$

$$\lambda \eta. \eta_t \circ (l \otimes \lambda) = \eta_t \circ (l \otimes \eta_l \otimes t) \circ (\lambda^o \otimes l \otimes t);$$

$$\eta_x y. (\eta_x \otimes y) \circ (x^o \otimes \tau_{yx}) = (y \otimes \eta_x) \circ (\tau_{x^o y} \otimes x) \text{ pour tous } x, y \in \{t, l\};$$

$$\gamma_x y. (x \otimes \tau_{x^o y}) \circ (\gamma_x \otimes y) = (\tau_{yx} \otimes x^o) \circ (y \otimes \gamma_x) \text{ pour tous } x, y \in \{t, l\}.$$

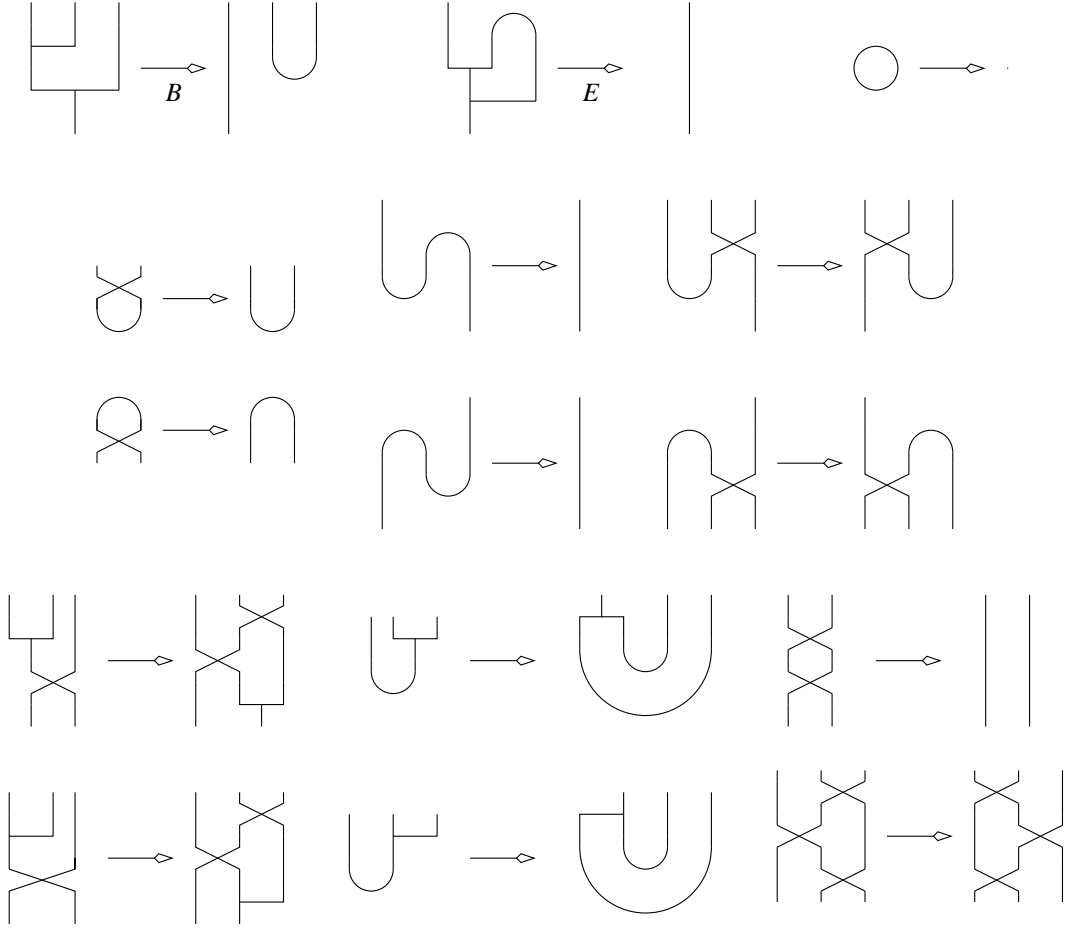


FIG. 6.2 – Les 35 relations de R sont obtenus en coloriant de toutes les manières possibles ces diagrammes.

La figure 6.2 montre une version graphique de ces relations. Notons que la présentation n'est pas minimale puisque, par exemple, μ^o est définissable à partir des autres générateurs.

Il semble possible de traduire les λ -termes comme des flèches de $\mathcal{L}\Lambda$. La figure 6.3 montre des exemples de traductions et la figure 6.4 comment l'équivalence

$$(\lambda xy.xy)(\lambda z.z) \equiv_{\beta_\eta} \lambda x.x$$

se traduit sous forme d'égalité entre des flèches parallèles de $\mathcal{L}\Lambda/R$. Cependant, avant de chercher une présentation convergente de cette opérade, ou même de formaliser ces traductions, nous allons discuter de deux problèmes majeurs qui seront rencontrés.

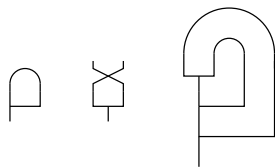


FIG. 6.3 – Exemples de traduction de $\lambda x.x$, à gauche, $\mu(x_2, x_1)$, au milieu, et $\lambda xy.yx$, à droite.

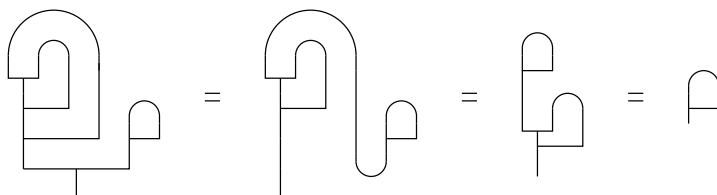


FIG. 6.4 – Exemple de traduction d'une $\beta\eta$ -équivalence dans $\mathcal{L}\Lambda/R$.

6.5.2 Un premier problème : les flèches inutiles

Le premier inconvénient d'une telle traduction est la quantité de flèches de $\mathcal{L}\Lambda/R$ qui ne correspondent pas à des λ -termes linéaires. Il y avait déjà de nombreuses flèches, dans l'opérade présentée par (Σ^c, R^c) , où (Σ, R) est un système de réécriture de termes, qui ne correspondaient pas à des termes mais à des familles de termes : pour toute flèche f dans $\mathcal{L}\Sigma^c(m, n)$, son image dans $\mathbb{T}\Sigma$ est un n -uplet de termes :

$$(f_1(x_1, \dots, x_m), \dots, f_n(x_1, \dots, x_m)).$$

Cependant, ici, la situation est bien pire, puisque l'on obtient des flèches qui n'ont aucune interprétation possible relativement aux λ -termes. La figure 6.5 montre deux telles flèches, parmi celles qui sont les moins éloignées de λ -termes.

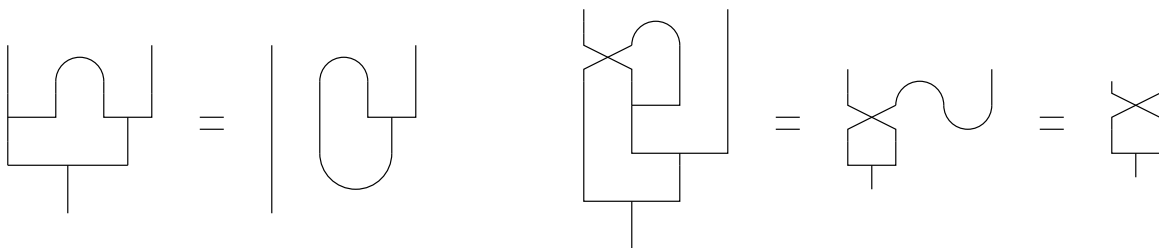


FIG. 6.5 – Deux flèches de $\mathcal{L}\Lambda$ qui ne sont pas des λ -termes.

La première flèche semble correspondre au λ -terme $(\lambda x.x_1)(xx_2)$; par contre, au lieu de se réduire en x_1 , on obtient une flèche que l'on peut difficilement interpréter : en effet, le λ lie le x présent dans l'argument, ce qui fait que l'application de $\lambda x.x_1$ à xx_2 donne $(xx_2)[x := xx_2]$.

La seconde flèche est un peu moins étonnante, dans le sens où elle est plus proche d'un λ -terme, bien que l'on retrouve le même phénomène : elle semble correspondre à $x((\lambda x.x_1)x_2)$ mais où, encore une fois, le λ lie la variable x qui est à l'extérieur du terme. Cette fois, il n'y a plus d'application en boucle, et on obtient, après réduction, l'expression x_2x_1 (et non pas xx_1 comme aurait dû se réduire le λ -terme de départ).

On peut considérer que l'on obtient une extension du λ -calcul linéaire, c'est-à-dire une version 2-dimensionnelle pouvant décrire des termes que le λ -calcul ne peut appréhender. Cependant, dans le but d'obtenir une représentation fidèle du λ -calcul, où l'on peut comprendre sa nature algébrique, ce n'est pas satisfaisant.

6.5.3 Le problème majeur : l'extension au λ -calcul

L'autre problème que nous soulevons est bien plus grave que celui du paragraphe précédent. En effet, si l'on décrit la substitution à l'aide d'une structure souveraine, on va vouloir, pour obtenir le λ -calcul tout entier, la mélanger avec les opérateurs de gestion des ressources que nous avons déjà étudié.

On s'achemine donc vers la recherche d'une présentation convergente d'une opéade cartésienne souveraine :

Définition. Une opéade est dite *cartésienne souveraine* si elle possède à la fois une structure souveraine et une structure cartésienne. \blacklozenge

Cependant, on arrive rapidement à :

Proposition 6.3. *La seule opéade cartésienne et souveraine est l'opéade terminale, qui possède exactement une flèche entre chaque couple d'objets.*

Démonstration. Soit \mathbb{C} une opéade Γ -colorée cartésienne souveraine. Soit f une flèche de x vers y , avec $x, y \in \langle \Gamma \rangle$. Alors :

$$f = (y \otimes \eta_y) \circ (\gamma_y \otimes f).$$

Or η_y est une flèche de $y^\circ \otimes y$ vers 0. Cependant, comme \mathbb{C} est cartésienne, il n'existe qu'une telle flèche : $\varepsilon_{y^\circ} \otimes \varepsilon_y$. On obtient donc :

$$\begin{aligned} f &= (y \otimes \eta_y) \circ (\gamma_y \otimes f) \\ &= (y \otimes \varepsilon_{y^\circ} \otimes \varepsilon_y) \circ (\gamma_y \otimes f) \\ &= \varepsilon_y^\circ \otimes \varepsilon_x. \end{aligned}$$

Donc toutes les flèches $x \longrightarrow y$ sont égales. \diamond

Ainsi, toute interprétation des λ -termes dans une telle opérade les identifierait tous.

Il est cependant certainement possible de trouver une présentation qui n'est pas une simulation complète, pour la raison que nous venons de donner, mais dans laquelle on peut traduire les termes et les réduire à l'aide d'une stratégie bien choisie, qui évite les écueils liés à des problèmes de confluence. Par exemple, les figures 6.6 et 6.7 donnent un candidat.

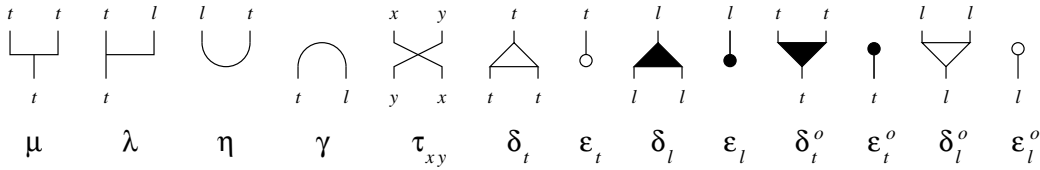


FIG. 6.6 – Une signature à 16 générateurs.

Cette présentation possède des défauts de confluence, comme celui qui est décrit par la figure 6.8.

Ce défaut n'a pas été choisi au hasard : il s'agit du problème, déjà noté par Lamping, de savoir si deux dupicateurs se correspondent ou non. Si l'on complète la présentation pour faire disparaître ce défaut, toutes les flèches parallèles deviendront alors équivalentes. Donc deux λ -termes ayant les mêmes variables libres seront identifiés par la traduction.

Dans les calculs déjà mentionnés, ce problème est résolu par divers moyens :

- dans le calcul de Lamping, les dupicateurs sont indexés, mais l'on crée ainsi une infinité de générateurs et de règles ;
- dans les réseaux de preuves, on introduit la boîte et on duplique chaque boîte d'un coup, mais on n'a plus de règle de duplication atomique ;
- dans les réseaux d'interaction, on code ou on décode les termes pour éviter ce problème, mais on perd la possibilité de simuler toutes les réductions possibles.

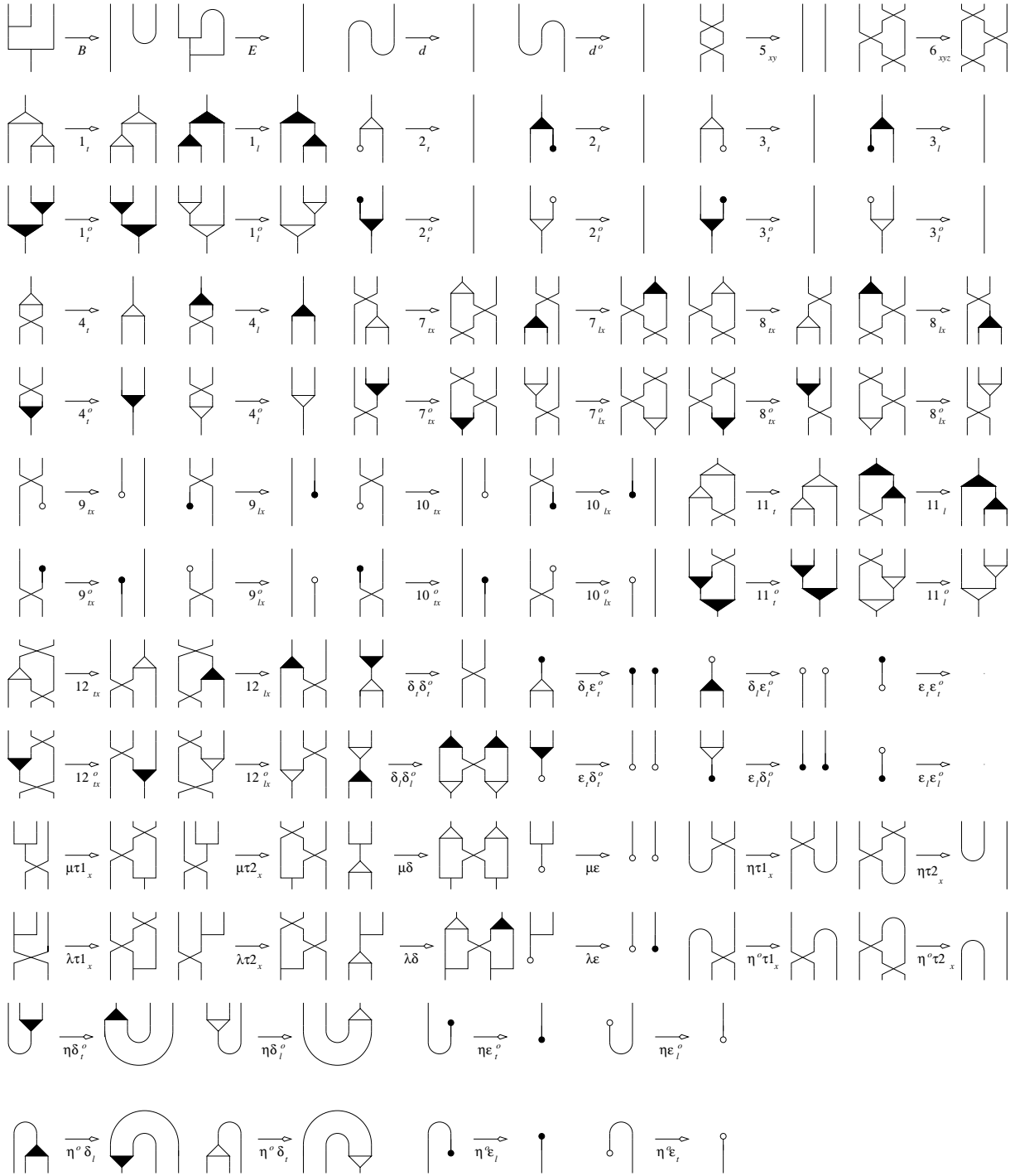


FIG. 6.7 – Une famille de 92 règles.

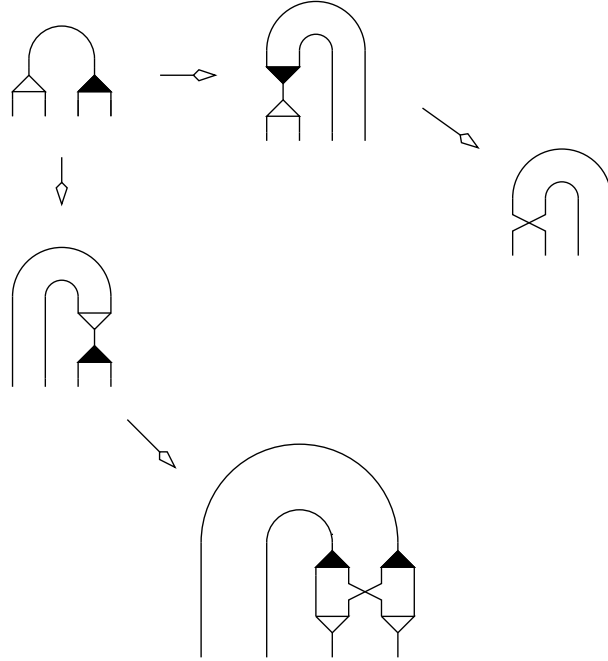


FIG. 6.8 – Le défaut de confluence majeur de la présentation.

Proposons ici aussi un palliatif. On peut séparer les règles en deux groupes que l'on fait agir l'un après l'autre : l'un s'occupe des duplications, l'autre de la normalisation des termes. Les deux règles qui créent le problème de confluence sont alors séparées, de sorte que l'on ne peut jamais appliquer les deux au même moment. Notons ici l'intérêt d'être dans une catégorie monoïdale et non dans un graphe : les opérateurs δ et δ^o sont distincts, de sorte qu'ils peuvent réagir à des règles différentes.

Nous avons déjà remarqué que cette solution est peu satisfaisante dans le but de fournir un modèle algébrique pour le λ -calcul. Il faut ajouter à cela que, même si l'on résout les problèmes de confluence en conditionnant l'application des règles, la terminaison est loin d'être évidente à prouver. Par exemple, les règles impliquant les opérateurs η et γ rendent, pour la plupart, impossible l'utilisation de la technique élaborée en 3.7.

6.6 Vers une dimension supérieure

Il semble que l'interprétation du λ -calcul à l'aide d'une présentation d'opérades, c'est-à-dire avec des termes de dimension 2 et des relations de dimension 3, soit vouée à l'échec. On peut cependant se poser la même question en dimension supérieure.

À ce jour, l'interprétation la plus fidèle du λ -calcul reste celle de Lambek et Scott, que l'on trouve dans [LS86]. Il y est montré une équivalence entre les λ -calculs typés (avec structure additionnelle) et les catégories cartésiennes fermées, structure qui traduit parfaitement l'application et l'abstraction du λ -calcul. Dans le cas non typé, le λ -calcul (avec structure additionnelle) s'identifie au C -monoïde initial. Notons que ce n'est pas la même interprétation que celle utilisée pour les calculs de substitutions explicites, notamment celui de l'annexe B.

Cependant, comme dans le cas d'une catégorie cartésienne, il est loin d'être évident d'obtenir une représentation graphique des flèches d'une catégorie cartésienne fermée. Ainsi, un programme de recherche intéressant consiste à obtenir un résultat similaire à celui de [Bur93] pour les catégories cartésiennes fermées, c'est-à-dire une caractérisation équationnelle de la structure. Ce serait en effet le premier pas vers une présentation convergente de la structure de catégorie cartésienne fermée. Il reste à déterminer quel type d'objets ces présentations définiraient.

On peut donner un début de réponse en faisant une constatation. Les problèmes que nous avons rencontrés sont liés au fait que l'opérateur λ était interprété comme un opérateur du même type que les autres : de dimension 2, à 2 entrées - éventuellement colorées - et 1 sortie. Or, il serait certainement plus fidèle de le considérer comme un opérateur prenant une 2-flèche avec une entrée et une sortie et en rendant une avec 0 entrée et 1 sortie. Ainsi, ce nouvel opérateur λ ne vivrait plus en dimension 2 mais 3.

Cette constatation n'est cependant que le début d'une longue piste à explorer. ★

Annexe A

Opérades et autres structures de l'algèbre universelle

A.1 Opérades et opérades classiques

Nous allons examiner plus précisément en quoi les opérades généralisent les opérades classiques. Commençons par rappeler la définition de ces dernières, telle que donnée par Peter May dans [May72].

Définition. Une *opérade (ensembliste unitaire) classique* \mathcal{P} est la donnée :

- 1) d'une famille $(\mathcal{P}_n)_{n \in \mathbb{N}^*}$ d'ensembles ;
- 2) pour tout $n \in \mathbb{N}^*$, d'une action à droite de \mathfrak{S}_n sur \mathcal{P}_n ;
- 3) pour tout $n \in \mathbb{N}^*$ et tous $i_1 \dots i_n \in \mathbb{N}^*$, d'une application

$$c : \mathcal{P}_n \times \mathcal{P}_{i_1} \times \dots \times \mathcal{P}_{i_n} \longrightarrow \mathcal{P}_{i_1 + \dots + i_n} ;$$

qui vérifient les axiomes suivants :

Associativité : pour tous $n, i_1 \dots i_n, j_{1,1} \dots j_{1,i_1} \dots j_{n,1} \dots j_{n,i_n}$ dans \mathbb{N}^* , le diagramme suivant commute :

$$\begin{array}{ccc}
 \mathcal{P}_1 \times \mathcal{P}_{i_1} \times \dots \times \mathcal{P}_{i_n} \times \mathcal{P}_{j_{1,1}} \times \dots \times \mathcal{P}_{j_{n,i_n}} & \xrightarrow{c \times id} & \mathcal{P}_{i_1 + \dots + i_n} \times \mathcal{P}_{j_{1,1}} \times \dots \times \mathcal{P}_{j_{n,i_n}} \\
 \downarrow id \times c^n & \text{\textcircled{C}} & \downarrow c \\
 \mathcal{P}_n \times \mathcal{P}_{j_{1,1} + \dots + j_{1,i_1}} \times \dots \times \mathcal{P}_{j_{n,1} + \dots + j_{n,i_n}} & \xrightarrow{c} & \mathcal{P}_{j_{1,1} + \dots + j_{n,i_n}} ;
 \end{array}$$

Identité : il existe un élément $1 \in \mathcal{P}_1$ tel que, pour tout $f \in \mathcal{P}_n$, on a :

$$1 \circ f = f \circ (\underbrace{1, \dots, 1}_{n \text{ fois}}) = f;$$

Équivariance : pour tous $f \in \mathcal{P}_n$, $g_1 \in \mathcal{P}_{i_1} \dots g_n \in \mathcal{P}_{i_n}$, on a :

- pour $\sigma \in \mathfrak{S}_n$, $f^\sigma \circ (g_{\sigma(1)}, \dots, g_{\sigma(n)}) = f \circ (g_1, \dots, g_n)^{\sigma^*}$, où $\sigma^* \in \mathfrak{S}_{i_1 + \dots + i_n}$ agit par permutation des blocs;
- pour $\sigma_1 \in \mathfrak{S}_{i_1} \dots \sigma_n \in \mathfrak{S}_{i_n}$, $f \circ (g^{\sigma_1}, \dots, g^{\sigma_n}) = f \circ (g_1, \dots, g_n)^{\sigma_1 \dots \sigma_n}$, où $\sigma_1 \dots \sigma_n$ est l'élément de $\mathfrak{S}_{i_1 + \dots + i_n}$ obtenu par juxtaposition des permutations $\sigma_1, \dots, \sigma_n$.

Les opérades classiques et leurs morphismes, définis de façon évidente, forment une catégorie notée \mathbb{O} . Nous allons montrer qu'il s'agit d'une sous-catégorie pleine de la catégorie \mathbb{P} des PROP, elle-même étant une sous-catégorie de celle des opérades, comme nous le verrons plus loin .



Proposition A.1. *La catégorie \mathbb{O} est isomorphe à une sous-catégorie pleine de \mathbb{P} . Plus précisément, il existe des foncteurs $\mathcal{L} : \mathbb{O} \longrightarrow \mathbb{P}$ et $\mathcal{U} : \mathbb{P} \longrightarrow \mathbb{O}$ tels que $\mathcal{U} \circ \mathcal{L} = id_{\mathbb{O}}$.*

Cette proposition signifie que les PROP, et par conséquent les opérades, sont bien une généralisation des opérades classiques. On peut s'en persuader ainsi : une opérade classique ne contient que des opérateurs de valence $(n, 1)$, alors que ceux des PROP et des opérades peuvent avoir n'importe quelle valence (m, n) .

Démonstration. Soit \mathcal{P} une opérade classique. On pose $\mathcal{LP}(n, 1) = \mathcal{P}_n$ et :

$$\mathcal{LP}(n, m) = \left(\coprod_{n_1 + \dots + n_m = n} (\mathcal{P}_{n_1} \times \dots \times \mathcal{P}_{n_m}) \right) \times \mathfrak{S}_m.$$

On définit la composition dans \mathcal{LP} ainsi : si $f_1 \in \mathcal{P}_{n_1}, \dots, f_m \in \mathcal{P}_{n_m}$, $g_1 \in \mathcal{P}_{m_1}, \dots, g_p \in \mathcal{P}_{m_p}$, $\sigma \in \mathfrak{S}_m$, $\tau \in \mathfrak{S}_p$,

$$\begin{aligned} & (g_1 \dots g_p; \tau) \circ (f_1 \dots f_m; \sigma) \\ &= \left(g_1 \circ (f_{\sigma^{-1}(1)} \dots f_{\sigma^{-1}(m_1)}) \dots g_p \circ (f_{\sigma^{-1}(m-m_p+1)} \dots f_{\sigma^{-1}(m)}) ; \tau \right). \end{aligned}$$

Le produit de \mathcal{LP} est donné par : pour $(f_1 \dots f_m; \sigma)$ dans $\mathcal{LP}(n, m)$ et $(g_1 \dots g_q; \tau)$ dans $\mathcal{LP}(p, q)$,

$$(f_1 \dots f_m; \sigma) \otimes (g_1 \dots g_q; \tau) = (f_1 \dots f_m, g_1 \dots g_q; \sigma\tau).$$

Enfin, l'identité de n est $(\underbrace{1 \dots 1}_{n \text{ fois}}; id_{\mathfrak{S}_n})$.

Réciproquement, soit \mathbb{C} un PROP. On pose $\mathcal{UC}_n = \mathbb{C}(n, 1)$. L'unité de l'opérade classique est id_1 . Ensuite, la composition est donnée par : si $f \in \mathcal{UC}_n$, $g_1 \in \mathcal{UC}_{i_1}$, \dots , $g_n \in \mathcal{UC}_{i_n}$ alors :

$$f \circ (g_1 \dots g_n) = f \circ (g_1 \otimes \dots \otimes g_n).$$

L'action de \mathfrak{S}_n est donnée par : $f^\sigma = f \circ \Sigma_{\mathbb{C}}(\sigma)$. \diamond

A.2 Opérades, PRO et PROP

Nous allons examiner ici des critères caractérisant les opérades qui sont des PRO ou des PROP. Rappelons la définition de [ML65] :

Définition. Un *PRO* est une petite catégorie monoïdale dont les objets sont les entiers naturels et telle que la restriction aux objets du produit monoidal coïncide avec l'addition des entiers. Un *PROP* est un PRO qui est symétrique en tant que catégorie monoïdale. \blacklozenge

On déduit de la définition :

Proposition A.2. *Les PRO sont les opérades monochromes et les PROP sont les opérades monochromes symétriques.*

Il n'y a donc pas besoin de critère pour les PRO. En ce qui concerne les PROP, on les caractérise de manière équationnelle. On note, pour toute catégorie \mathcal{C} , $\sigma_{\mathcal{C}}$ l'endofoncteur de symétrie $\mathcal{C}^2 \rightarrow \mathcal{C}^2$ associé au produit cartésien des catégories, c'est-à-dire qui est défini par $\sigma_{\mathcal{C}}(x, y) = (y, x)$. Si, de plus, \mathcal{C} est monoïdale, on note \otimes^{op} la composée du produit tensoriel avec $\sigma_{\mathcal{C}}$, c'est-à-dire que $x \otimes^{op} y = y \otimes x$.

On démontre le résultat général suivant :

Proposition A.3. *Soit \mathcal{C} une catégorie monoïdale stricte. Les assertions suivantes sont équivalentes :*

- 1) *La catégorie \mathcal{C} est symétrique.*
- 2) *Il existe un morphisme fonctoriel $\tau : \otimes \rightarrow \otimes^{op}$ dont les composantes vérifient :*
 - $\tau_{y,x} \circ \tau_{x,y} = x \otimes y$, pour tous x et y objets de \mathcal{C} ;
 - $(\tau_{y,z} \otimes x) \circ (y \otimes \tau_{x,z}) \circ (\tau_{x,y} \otimes z) = (z \otimes \tau_{x,y}) \circ (\tau_{x,z} \otimes y) \circ (x \otimes \tau_{y,z})$, pour tous x , y et z objets de \mathcal{C} ;
- 3) *La catégorie \mathcal{C} contient une flèche*

$$\tau_{xy} : x \otimes y \rightarrow y \otimes x$$

pour tous x et y objets de \mathcal{C} , de telle sorte que les relations suivantes soient satisfaites :

- $\tau_{y,x} \circ \tau_{x,y} = x \otimes y$, pour tous x et y objets de \mathcal{C} ;
- $(\tau_{y,z} \otimes x) \circ (y \otimes \tau_{x,z}) \circ (\tau_{x,y} \otimes z) = (z \otimes \tau_{x,y}) \circ (\tau_{x,z} \otimes y) \circ (x \otimes \tau_{y,z})$, pour tous x , y et z objets de \mathcal{C} ;
- $\tau_{y,z} \circ (f \otimes z) = (z \otimes f) \circ \tau_{x,z}$, pour tous x , y et z objets de \mathcal{C} et toute flèche $f \in \mathcal{C}(x, y)$.

Démonstration. L'équivalence entre les deux premières assertions est donnée par la définition d'une symétrie. L'équivalence entre les deux dernières est donnée par la définition d'un morphisme fonctoriel. \diamond

D'où :

Corollaire A.4. *Une opérade monochrome \mathbb{C} est symétrique si et seulement si elle contient une flèche $\tau : 2 \longrightarrow 2$ vérifiant les relations suivantes :*

$$5. \tau \circ \tau = 2 ;$$

$$6. (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) = (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) ;$$

ainsi que, pour tous entiers m et n et toute flèche $f \in \mathbb{C}(m, n)$:

$$f\tau 1. \tau_{n,1} \circ (f \otimes 1) = (1 \otimes f) \circ (\tau_{m,1}).$$

Les flèches $\tau_{n,1}$ sont définies par récurrence sur n , en posant $\tau_{0,1} = 1$ et $\tau_{1,1} = \tau$ puis :

$$\tau_{n+1,1} = (\tau_{n,1} \otimes 1) \circ (n \otimes \tau).$$

Démonstration. Si \mathbb{C} est symétrique, on obtient, en utilisant le 3 de la proposition A.3, une flèche

$$\tau_{m,n} : m \otimes n \longrightarrow n \otimes m,$$

pour tous entiers m et n . On vérifie alors que l'on a bien $\tau_{0,1} = 1$ et, qu'en posant $\tau = \tau_{1,1}$, on obtient, par récurrence sur n :

$$\tau_{n+1,1} = (\tau_{n,1} \otimes 1) \circ (n \otimes \tau).$$

Les relations 5, 6 ainsi que les $f\tau 1$, pour f flèche de \mathbb{C} , sont des cas particuliers de celles données dans le point 3 de la proposition A.3.

Réciproquement, si \mathbb{C} contient une flèche τ vérifiant les relations 5, 6 et $f\tau 1$ pour toute flèche f de \mathbb{C} , on définit les flèches $\tau_{m,n}$ par récurrence sur m et n . On commence par $\tau_{0,0} = 0$, puis $\tau_{1,0} = \tau_{0,1} = 1$, $\tau_{1,1} = \tau$, puis :

$$\begin{cases} \tau_{m+1,n} = (\tau_{m,n} \otimes 1) \circ (m \otimes \tau_{1,n}) \\ \tau_{m,n+1} = (1 \otimes \tau_{m,n}) \circ (\tau_{m,1} \otimes n). \end{cases}$$

La vérification des relations du point 3 de la proposition A.3 se fait ainsi :

- pour $\tau_{n,m} \circ \tau_{m,n} = m \otimes n$: par récurrence sur m et n ;
- pour $(\tau_{n,p} \otimes m) \circ (n \otimes \tau_{m,p}) \circ (\tau_{m,n} \otimes p) = (p \otimes \tau_{m,n}) \circ (\tau_{m,p} \otimes n) \circ (m \otimes \tau_{n,p})$: par récurrence sur m , n et p ;
- pour $\tau_{n,p} \circ (f \otimes p) = (p \otimes f) \circ \tau_{m,p}$: par récurrence sur m , n et p .

◇

A.3 Opérades et théories algébriques

Ici, nous allons rappeler un résultat de [Bur93]. Commençons par la définition suivante, issue de [Law63] :

Définition. Une *théorie algébrique* est une petite catégorie cartésienne dont les objets sont les entiers naturels et telle que la restriction aux objets de la partie fonctorielle du produit cartésien coïncide avec l'addition des entiers. ◆

On en déduit immédiatement que :

Proposition A.5. *Les théories algébriques sont les opérades monochromes cartésiennes.*

On note, pour toute catégorie monoïdale \mathcal{C} , $\Delta_{\mathcal{C}} : \mathcal{C} \longrightarrow \mathcal{C}$ la composante en \mathcal{C} de la diagonale associée au produit cartésien de catégories, composée avec le produit de \mathcal{C} , c'est-à-dire que $\Delta_{\mathcal{C}}$ est défini par $\Delta_{\mathcal{C}}(x) = x \otimes x$. On pose aussi $*_{\mathcal{C}} : \mathcal{C} \longrightarrow \mathcal{C}$ la flèche terminale $\mathcal{C} \longrightarrow *$, où $*$ est la catégorie avec un seul objet et une seule flèche, composée avec l'unité de \mathcal{C} , c'est-à-dire que $*_{\mathcal{C}}$ est défini par $*_{\mathcal{C}}(x) = *$, où $*$ est l'unité de \mathcal{C} . Nous avons le résultat général suivant :

Proposition A.6. *Soit \mathcal{C} une catégorie monoïdale stricte. Les assertions suivantes sont équivalentes :*

- 1) *La catégorie \mathcal{C} est cartésienne.*
- 2) *Il existe des morphismes fonctoriels $\delta : id_{\mathcal{C}} \longrightarrow \Delta_{\mathcal{C}}$ et $\varepsilon : id_{\mathcal{C}} \longrightarrow *_{\mathcal{C}}$ dont les composantes vérifient les équations suivantes :*
 - $\varepsilon_* = *$;
 - $(x \otimes \varepsilon_y \otimes \varepsilon_x \otimes y) \circ \delta_{x \otimes y} = x \otimes y$, pour tous x et y objets de \mathcal{C} .
- 3) *La catégorie \mathcal{C} contient des flèches δ_x et ε_x pour chaque objet x de \mathcal{C} , de telle sorte que les équations suivantes soient vérifiées :*
 - $\varepsilon_* = *$;
 - $(x \otimes \varepsilon_y \otimes \varepsilon_x \otimes y) \circ \delta_{x \otimes y} = x \otimes y$, pour tous x et y objets de \mathcal{C} ;
 - $(y \otimes \delta_x) \circ \tau_{x,y} = (\tau_{x,y} \otimes x) \circ (x \otimes \tau_{x,y}) \circ (\delta_x \otimes y)$, pour tous x et y objets de \mathcal{C} ;
 - $(y \otimes \varepsilon_x) \circ \tau_{x,y} = \varepsilon_x \otimes y$, pour tous x et y objets de \mathcal{C} .

- 4) Il existe des morphismes fonctoriels $\tau : \otimes \longrightarrow \otimes^{op}$, $\delta : id_{\mathcal{C}} \longrightarrow \Delta_{\mathcal{C}}$ et $\varepsilon : id_{\mathcal{C}} \longrightarrow *_C$ dont les composantes vérifient les équations suivantes :
- $(\delta_x \otimes x) \circ (\delta_x) = (x \otimes \delta_x) \circ \delta_x$, pour tout objet x de \mathcal{C} ;
 - $(\varepsilon_x \otimes x) \circ \delta_x = x$, pour tout objet x de \mathcal{C} ;
 - $\tau_x \circ \delta_x = \delta_x$, pour tout objet x de \mathcal{C} ;
 - $\tau_{y,x} \circ \tau_{x,y} = x \otimes y$, pour tous x et y objets de \mathcal{C} ;
 - $(\tau_{y,z} \otimes x) \circ (y \otimes \tau_{x,z}) \circ (\tau_{x,y} \otimes z) = (z \otimes \tau_{x,y}) \circ (\tau_{x,z} \otimes y) \circ (x \otimes \tau_{y,z})$, pour tous x , y et z objets de \mathcal{C} ;
 - $(y \otimes \delta_x) \circ \tau_{x,y} = (\tau_{x,y} \otimes x) \circ (x \otimes \tau_{x,y}) \circ (\delta_x \otimes y)$, pour tous x et y objets de \mathcal{C} ;
 - $(y \otimes \varepsilon_x) \circ \tau_{x,y} = \varepsilon_x \otimes y$, pour tous x et y objets de \mathcal{C} .
- 5) La catégorie \mathcal{C} contient des flèches $\tau_{x,y}$, pour tous x et y objets de \mathcal{C} , et (δ_x) et (ε_x) , pour tout objet x de \mathcal{C} , de telle sorte que les équations suivantes soient satisfaites :
- $(\delta_x \otimes x) \circ (\delta_x) = (x \otimes \delta_x) \circ \delta_x$, pour tout objet x de \mathcal{C} ;
 - $(\varepsilon_x \otimes x) \circ \delta_x = x$, pour tout objet x de \mathcal{C} ;
 - $\tau_x \circ \delta_x = \delta_x$, pour tout objet x de \mathcal{C} ;
 - $\tau_{y,x} \circ \tau_{x,y} = x \otimes y$, pour tous x et y objets de \mathcal{C} ;
 - $(\tau_{y,z} \otimes x) \circ (y \otimes \tau_{x,z}) \circ (\tau_{x,y} \otimes z) = (z \otimes \tau_{x,y}) \circ (\tau_{x,z} \otimes y) \circ (x \otimes \tau_{y,z})$, pour tous x , y et z objets de \mathcal{C} ;
 - $(y \otimes \delta_x) \circ \tau_{x,y} = (\tau_{x,y} \otimes x) \circ (x \otimes \tau_{x,y}) \circ (\delta_x \otimes y)$, pour tous x et y objets de \mathcal{C} ;
 - $(y \otimes \varepsilon_x) \circ \tau_{x,y} = \varepsilon_x \otimes y$, pour tous x et y objets de \mathcal{C} ;
 - $\varepsilon_y \circ f = \varepsilon_x$, pour tous x et y objets de \mathcal{C} et toute flèche $f \in \mathcal{C}(x, y)$;
 - $\delta_y \circ f = (f \otimes f) \circ \delta_x$, pour tous x et y objets de \mathcal{C} et toute flèche $f \in \mathcal{C}(x, y)$;
 - $\tau_{y,z} \circ (f \otimes z) = (z \otimes f) \circ \tau_{x,z}$, pour tous x , y et z objets de \mathcal{C} et toute flèche $f \in \mathcal{C}(x, y)$.

Remarque. Dans [Bur93], Albert Burroni avait déjà montré l'équivalence entre les assertions 1, 2 et 3.

Démonstration. L'équivalence entre les assertions 1 et 2 est donnée par la définition de catégorie monoïdale cartésienne : il suffit d'expliciter les morphismes fonctoriels correspondant aux adjonctions entre le produit et le foncteur diagonal, d'une part, et l'unité et le foncteur terminal, d'autre part. L'équivalence entre 2 et 3 est, par suite, donnée par les diagrammes associés à ces morphismes fonctoriels.

Puis, on montre l'équivalence entre 2 et 4 : dans le sens 2 implique 4, on définit le morphisme τ en donnant ses composantes :

$$\tau_{x,y} = (\varepsilon_x \otimes y \otimes x \otimes y) \circ \delta_{x \otimes y}.$$

Le fait ces flèches soient les composantes d'un morphisme fonctoriel découle de cette définition, de même que les relations à vérifier. Réciproquement, on obtient les relations de 2 en manipulant celles de 4. Enfin, l'équivalence entre 4 et 5 est donnée par la définition de morphisme fonctoriel. \diamond

On déduit de ce résultat :

Corollaire A.7. *Une opérade monochrome \mathbb{C} est cartésienne si et seulement si elle contient trois flèches $\tau : 2 \longrightarrow 2$, $\delta : 1 \longrightarrow 2$ et $\varepsilon : 1 \longrightarrow 0$ qui vérifient les équations suivantes :*

1. $(\delta \otimes 1) \circ \delta = (1 \otimes \delta) \circ \delta ;$
2. $(\varepsilon \otimes 1) \circ \delta = 1 ;$
4. $\tau \circ \delta = \delta ;$
5. $\tau \circ \tau = 2 ;$
6. $(\tau \otimes 1) \circ (1 \otimes \tau) \circ (\tau \otimes 1) = (1 \otimes \tau) \circ (\tau \otimes 1) \circ (1 \otimes \tau) ;$
7. $(1 \otimes \delta) \circ \tau = (\tau \otimes 1) \circ (1 \otimes \tau) \circ (\delta \otimes 1) ;$
9. $(1 \otimes \varepsilon) \circ \tau = \varepsilon \otimes 1 ;$

ainsi que, pour tout entier n et toute flèche $f \in \mathbb{C}(n, 1)$:

- $f\delta. \delta \circ f = (f \otimes f) \circ \delta_n ;$
- $f\varepsilon. \varepsilon \circ f = \varepsilon^n ;$
- $f\tau 1. \tau \circ (f \otimes 1) \rightarrow (1 \otimes f) \circ \tau_{n,1}.$

On a utilisé les notations suivantes :

- $\rho_n : 2n \longrightarrow 2n$ est la flèche définie, par récurrence sur n , par $\rho_0 = 0$, puis

$$\rho_{n+1} = (1 \otimes \rho_n \otimes 1) \circ (1 \otimes \tau^n \otimes 1) ;$$

- $\delta_n : n \longrightarrow 2n$ est la flèche $\rho_n \circ \delta^n ;$
- pour $\tau_{n,1} : n + 1 \longrightarrow n + 1$, on procède de nouveau par récurrence sur n : $\tau_{0,1} = 1$ puis

$$\tau_{n+1,1} = (\tau \otimes n) \circ (1 \otimes \tau_{n,1})$$

Démonstration. Si \mathbb{C} est cartésienne, on utilise le point 5 de la proposition A.6, spécialisé dans le cas d'une opérade monochrome. On définit les trois flèches par :

$$\tau = \tau_{1,1}, \quad \delta = \delta_1, \quad \varepsilon = \varepsilon_1.$$

On vérifie que $\delta_0 = 0$, $\tau_{0,0} = 0$ et $\tau_{1,0} = 1$ puis, par récurrence sur n , que :

$$\begin{cases} \delta_n = \rho_n \circ \delta^n \\ \tau_{n+1,1} = (\tau \otimes n) \circ (1 \otimes \tau_{n,1}). \end{cases}$$

Les relations du corollaire sont alors des cas particuliers de celles du point 5 de la proposition A.6.

Réciproquement, on construit les trois familles de flèches du point 5 de la proposition A.6. On pose, pour tout n , $\varepsilon_n = \varepsilon^n$, ainsi que :

$$\delta_0 = 0, \quad \delta_1 = \delta, \quad \tau_{0,0} = 0, \quad \tau_{1,0} = \tau_{0,1} = 1, \quad \tau_{1,1} = \tau.$$

Puis, on définit δ_n et $\tau_{n,1}$, par récurrence sur n , comme dans l'énoncé du corollaire A.7. Toujours par récurrence sur n , on pose :

$$\tau_{1,n+1} = (n \otimes \tau) \circ (\tau_{1,n} \otimes 1).$$

Enfin, par récurrence sur m et n :

$$\begin{cases} \tau_{m+1,n} = (\tau_{m,n} \otimes 1) \circ (m \otimes \tau_{1,n}) \\ \tau_{m,n+1} = (1 \otimes \tau_{m,n}) \circ (\tau_{m,1} \otimes n). \end{cases}$$

Les relations du point 5 de la proposition A.6 s'obtiennent par des récurrences sur les entiers apparaissant en indice des flèches $\tau_{m,n}$, δ_n et ε_n utilisées dans l'écriture de chaque équation.

◇

Annexe B

Présentation du C -monoïde initial et λ -calcul avec substitutions explicites

L'objectif de cette voie est d'associer au λ -calcul un système de réécriture de termes, éventuellement avec plusieurs sortes, qui explicite, au niveau du calcul, les substitutions. Il existe de nombreux systèmes de réécriture construits dans ce but ; citons principalement le tout premier d'entre eux : le $\lambda\sigma$ -calcul.

En général, les termes de ces systèmes de réécriture sont les λ -termes en *notations de de Bruijn* : on remplace les variables par des entiers - nous verrons comment dans la suite. L'intérêt principal est que chaque *classe d' α -équivalence* possède une seule écriture en notations de de Bruijn : on évite ainsi tous les problèmes provenant de la notion de variable liée.

Mais cette notation possède un autre avantage : grâce à elle, on peut exprimer les substitutions (d'une variable par un terme) de manière simple. Ainsi, le $\lambda\sigma$ -calcul a proposé d'inclure les substitutions dans le calcul : elles deviennent ainsi des termes du calcul et leur propagation dans les λ -termes est décrite par des règles de réécriture, adjointes à la β -réduction.

Dans ces calculs, les substitutions apparaissent clairement et leur action n'est plus décrite de manière externe au calcul, d'où le nom générique de *calculs de substitutions explicites*. Nous allons voir que le $\lambda_{\beta\eta}$ -calcul est un fragment du C -monoïde initial, proposer un système de réécriture de termes (avec une sorte) pour (une partie de) la structure de C -monoïde et montrer que ce calcul ne possède malheureusement pas toutes les propriétés que l'on souhaite.

B.1 La structure de C -monoïde

L'ensemble $\Lambda / \equiv_{\beta\eta}$ des λ -termes modulo la congruence engendrée par les relations de β et d' η -conversion possède une transcription algébrique : il est inclus dans le C -monoïde initial.

Définition. Un C -monoïde est un ensemble M avec trois éléments distingués p, q, i , muni d'applications $\lambda : M \longrightarrow M$ et $*, \gamma, \mu : M^2 \longrightarrow M$ vérifiant les égalités suivantes, pour tous $x, y, z \in M$:

- A. $*$ est associative : $(x * y) * z = x * (y * z)$;
- I. i neutre à gauche pour $*$: $i * x = x$;
- J. i neutre à droite pour $*$: $x * i = x$;
- P. p est la première projection pour γ : $p * \gamma(x, y) = x$;
- Q. q est la seconde projection pour γ : $q * \gamma(x, y) = y$;
- G. cohérence de γ avec les projections p et q : $\gamma(p, q) = i$;
- D. $*$ est distributive à droite relativement à γ : $\gamma(x, y) * z = \gamma(x * z, y * z)$;
- M. $*$ est distributive à droite relativement à μ : $\mu(x, y) * z = \mu(x * z, y * z)$;
- L. règle de commutation de λ et $*$: $\lambda(x) * y = \lambda(x * \gamma(p, y * q))$;
- B. β -conversion : $\mu(\lambda(x), y) = x * \gamma(y, i)$;
- E. η -conversion : $\lambda(\mu(x * q, p)) = x$.

◆

Il existe une notion de C -monoïde librement engendré par un ensemble X . Dans le cas où $X = \emptyset$, il existe une injection de l'ensemble $\Lambda / \equiv_{\beta\eta}$ dans le C -monoïde initial ; ce sera évident plus loin. Cependant, l'existence d'une présentation par signature et règles de réécriture, possédant les mêmes propriétés que le λ -calcul, de ce C -monoïde initial reste une question ouverte ; en fait, il est conjecturé qu'il n'en existe pas. On ne peut donc pas trop espérer de cette voie pour associer une présentation d'opérade au λ -calcul.

B.2 Le système de réécriture \mathbb{K}

B.2.1 Signature et règles de réécriture de \mathbb{K}

La signature Σ de \mathbb{K} contient sept éléments : trois en degré 0, $\Sigma(0, 1) = \{p, q, i\}$, un en degré 1, $\Sigma(1, 1) = \{\lambda\}$, et trois en degré 2, $\Sigma(2, 1) = \{*, \gamma, \mu\}$.

On construit l'ensemble T des termes de manière classique :

1. On commence avec $T^0 = V \amalg \{p, q, i\}$.
2. Si tous les T^k , $k \leq n$, sont construits, on pose :
 - $T_\lambda^{n+1} = T^n$, dont les éléments sont notés $\lambda(a)$ ou juste λa .
 - $T_*^{n+1} = \left(\amalg_{0 \leq k \leq n} T^n \amalg T^k \right) \amalg \left(\amalg_{0 \leq k \leq n} T^k \amalg T^n \right)$, dont les éléments sont notés $a * b$.
 - $T_\gamma^{n+1} = \left(\amalg_{0 \leq k \leq n} T^n \amalg T^k \right) \amalg \left(\amalg_{0 \leq k \leq n} T^k \amalg T^n \right)$, dont les éléments sont notés $\gamma(a, b)$.
 - $T_\mu^{n+1} = \left(\amalg_{0 \leq k \leq n} T^n \amalg T^k \right) \amalg \left(\amalg_{0 \leq k \leq n} T^k \amalg T^n \right)$, dont les éléments sont notés $\mu(a, b)$.

Puis : $T^{n+1} = T_\lambda^{n+1} \amalg T_*^{n+1} \amalg T_\gamma^{n+1} \amalg T_\mu^{n+1}$.

3. On pose $T = \amalg_{n \in \mathbb{N}} T^n$.

On définit le degré d'un élément, les contextes, les substitutions, etc. comme habituellement en réécriture de termes.

Les règles de réécriture sont données ainsi, avec a, b, c des variables arbitrairement choisies (deux à deux distinctes cependant) :

$$\begin{aligned}
 (a * b) * c &\longrightarrow_A a * (b * c) \\
 i * a &\longrightarrow_I a \\
 a * i &\longrightarrow_J a \\
 p * \gamma(a, b) &\longrightarrow_P a \\
 q * \gamma(a, b) &\longrightarrow_Q b \\
 \gamma(p, q) &\longrightarrow_G i \\
 \gamma(p * a, q * a) &\longrightarrow_X a \\
 \gamma(a, b) * c &\longrightarrow_D \gamma(a * c, b * c) \\
 \mu(a, b) * c &\longrightarrow_M \mu(a * c, b * c) \\
 \lambda(a) * b &\longrightarrow_L \lambda(a * \gamma(p, b * q)) \\
 \mu(\lambda(a), b) &\longrightarrow_B a * \gamma(b, i)
 \end{aligned}$$

Cette présentation est obtenue à partir de celle du $\lambda\sigma$ -calcul, en identifiant les deux sortes, $t = s$, et deux opérateurs, $*$ = o. Pour référence ultérieure, on notera K_0 la réunion de toutes ces relations à l'exclusion de L et B , $K = K_0 \cup \{L\}$ et $KB = K \cup \{B\}$. On note $\mathbb{K} = (\Sigma, KB)$. On va montrer que K termine et que KB est confluente.

Cependant, ces règles ne permettent pas l'application des méthodes usuelles :

- la règle L empêche d'utiliser un ordre lexicographique ou une interprétation polynômiale pour prouver que K termine ; on va donc montrer que K_0 termine avec un ordre lexicographique, puis utiliser une variante de la technique des couples de dépendance pour obtenir la terminaison de K ;
- la réunion KB ne termine pas : il n'est donc pas possible de prouver sa confluence grâce à la confluence locale et au lemme de Newman ; on ne peut pas non plus utiliser directement la technique d'interprétation de Hardin, voir [Har89], ni le lemme de [HY90], à cause de la règle X , non linéaire à gauche ; on va procéder ainsi : montrer que K termine et est localement confluente (et donc convergente via le lemme de Newman) puis prouver une technique d'interprétation légèrement modifiée applicable ici et en conclure que KB est confluente.

B.2.2 La relation K_0 termine

On va munir \mathbb{K} d'un *ordre lexicographique* et montrer que les règles de K_0 sont strictement décroissantes pour cet ordre. On utilisera les résultats suivants - que l'on peut retrouver, par exemple, dans [BN98] - pour conclure :

- un ordre lexicographique est un ordre de simplification ;
- un ordre de simplification sur les termes associés à une signature *finie* est un ordre de réduction ;
- un système de réécriture de termes termine si et seulement si on peut le munir d'un ordre de réduction pour lequel toute règle de réécriture est strictement décroissante.

On munit la signature Σ de \mathbb{K} de l'ordre strict $>$ donné par $* > \mu$, $* > \gamma$ et $p > i$. L'ordre lexicographique des chemins induit sur T , toujours noté $>$, est alors donné par récurrence sur le degré des termes. Pour deux éléments a et b de T , on a $a > b$ si et seulement si l'une de ces conditions est remplie :

1. a contient un sous-terme strict c tel que $c \geq b$;
2. $a = p$ et $b = i$;
3. $a = a_1 * a_2$, $b = \varphi(b_1, b_2)$ avec $\varphi \in \{\mu, \gamma\}$, $a > b_1$ et $a > b_2$;
4. $a = \varphi(a_1, a_2)$ et $b = \varphi(b_1, b_2)$ avec $\varphi \in \{*, \gamma, \mu\}$, $a > b_2$ et $a_1 > b_1$;
5. $a = \varphi(a_1, a_2)$ et $b = \varphi(b_1, b_2)$ avec $\varphi \in \{*, \gamma, \mu\}$, $a_1 = b_1$ et $a_2 > b_2$.

On vérifie :

Proposition B.1. *Pour toute règle (l, r) de K_0 , on a : $l > r$.*

Démonstration.

- A. $(a * b) * c > a * (b * c)$ d'après le cas 4. D'une part, $(a * b) * c > b * c$ d'après 4 : $(a * b) * c > c$ (1) et $a * b > b$ (1). D'autre part, $a * b > a$ (1).
- I. $i * a > a$ par 1.
- J. $a * i > a$ par 1.
- P. $p * \gamma(a, b) > a$ par 1.
- Q. $q * \gamma(a, b) > b$ par 1.
- G. $\gamma(p, q) > i$ par 1 avec $p > i$ (2).
- X. $\gamma(p * a, q * a) > a$ par 1.
- D. $\gamma(a, b) * c > \gamma(a * c, b * c)$ par 3. En effet, $\gamma(a, b) * c > a * c$ avec 4, en notant que $\gamma(a, b) * c > c$ (1) et que $\gamma(a, b) > a$ (1). Pour les mêmes raisons, $\gamma(a, b) * c > b * c$.
- M. $\mu(a, b) * c * > \mu(a * c, b * c)$ par 3. En effet, $\mu(a, b) * c > a * c$ par 4 avec $\mu(a, b) * c > c$ (1) et $\mu(a, b) > a$ (1). De même, $\mu(a, b) * c > b * c$.

◇

On conclut donc :

Proposition B.2. *La relation K_0 termine sur T .*

B.2.3 La relation K termine

On va utiliser les méthodes fournies par la notion de *couples de dépendance*, introduite dans [AG00]. Rappelons quelques notions et résultats.

Définition. Soit (Σ, R) un système de réécriture de termes. On appelle *racine* d'un terme a l'élément φ de Σ tel que $a = \varphi(a_1, \dots, a_n)$. Un élément de Σ est appelé *symbole défini* s'il est la racine d'au moins une règle de R .

Un *couple de dépendance* (associé à une règle (s, t)) de R est un couple (s, u) tel qu'il existe un contexte C vérifiant $t = C[u]$ et tel que la racine de u est un symbole défini.

Une *R -chaîne* est une famille $(s_i, t_i)_{i \in I}$, où $I = \{1 \dots n\}$ ou $I = \mathbb{N}$, telle qu'il existe une substitution $f \in \mathcal{S}_\Sigma$ avec $f(t_i) \rightarrow_R f(s_{i+1})$ pour tout i .

◆

Toujours dans [AG00] :

Théorème B.3. *Un système de réécriture (Σ, R) termine si et seulement si il n'existe pas de R -chaîne infinie.*

Après ces rappels, nous allons démontrer une variante d'un résultat de [AG00] :

Proposition B.4. *Soient (Σ, R) un système de réécriture de termes qui termine et (a, b) une règle de réécriture supplémentaire. On note $(a, b_1), \dots, (a, b_k)$ les couples de dépendance associés à (a, b) et $\bar{R} = R \cup \{(a, b)\}$. Supposons qu'il existe une application $|\cdot| : T_\Sigma \longrightarrow \mathbb{N}$ vérifiant :*

- pour toute règle ou paire de dépendance (s, t) de R et toute substitution $f \in \mathcal{S}_\Sigma$, on a $|f(s)| \geq |f(t)|$;
- pour toute substitution $f \in \mathcal{S}_\Sigma$, on a $|f(a)| \geq |f(b)|$;
- pour tout $i \in \{1 \dots k\}$ et toute substitution $f \in \mathcal{S}_\Sigma$, on a $|f(a)| > |f(b_i)|$;
- pour tout contexte $C \in \mathcal{C}_\Sigma$ et tous $a, b \in \mathcal{T}_\Sigma$ tels que $|a| \geq |b|$, on a $|C[a]| \geq |C[b]|$.

Alors \bar{R} termine.

Démonstration. On va montrer qu'il n'existe pas de \bar{R} -chaîne infinie. Remarquons tout d'abord que, comme les contextes et les substitutions préservent l'ordre, on a, pour tous a et b dans \mathcal{T}_Σ :

$$a \twoheadrightarrow_{\bar{R}} b \implies |a| \geq |b|.$$

Maintenant supposons qu'il existe une \bar{R} -chaîne infinie $(s_n, t_n)_{n \in \mathbb{N}}$: les (s_n, t_n) sont des couples de dépendance de \bar{R} et il existe une substitution f telle que $f(t_n) \twoheadrightarrow_{\bar{R}} f(s_{n+1})$ pour tout n .

En particulier, $|f(s_n)| \geq |f(t_n)|$ par hypothèse et $|f(t_n)| \geq |f(s_{n+1})|$ d'après la remarque précédente. Comme R termine, il n'existe pas de R -chaîne infinie.

Il existe donc une sous-suite $(s_{k_n}, t_{k_n})_{n \in \mathbb{N}}$ de $(s_n, t_n)_{n \in \mathbb{N}}$ telle que $s_{k_n} = a$ et $t_{k_n} = b_{i_n}$. On a donc :

$$|s_{k_n}| = |a| > |b_{i_n}| = |t_{k_n}| \geq \dots \geq |s_{k_{n+1}}| = |a|.$$

C'est impossible : il n'existe donc pas de \bar{R} -chaîne infinie, ce qui implique que \bar{R} termine. ◇

On va appliquer ce résultat avec $R = K_0$ et $(a, b) = L$. Reste à construire l'application $|\cdot| : T \longrightarrow \mathbb{N}$. Intuitivement, $|a|$ est le nombre de symboles λ potentiels dans a .

On commence par définir une application auxiliaire $m : T \longrightarrow \mathbb{N}$ par récurrence sur le degré des termes :

- $m(p) = m(q) = m(i) = m(x) = 1$;
- $m(\lambda(a)) = m(a)$;
- $m(\mu(a, b)) = m(a) + m(b)$;
- $m(\gamma(a, b)) = \max(m(a), m(b))$;
- $m(a * b) = m(a) \times m(b)$.

La valeur de $m(a)$ est un multiplicateur du nombre de λ potentiels dans un terme b placé dans le contexte $a * \square$. Pour $|\cdot|$:

- $|p| = |q| = |i| = |x| = 0$;
- $|\lambda(a)| = |a| + 1$;
- $|\mu(a, b)| = |a| + |b|$;
- $|\gamma(a, b)| = \max(|a|, |b|)$;
- $|a * b| = |a| + m(a) \cdot |b|$.

On remarque immédiatement que m et $|\cdot|$ sont des applications à valeurs dans \mathbb{N} et que $m(a) \geq 1$ pour tout a de T . De plus, il est évident que, si $|a| \geq |b|$ et $m(a) \geq m(b)$, alors, pour tout contexte C , $|C[a]| \geq |C[b]|$. Enfin, si C est un contexte, alors, pour tout terme a , $|C[a]| \geq |a|$ et $m(C[a]) \geq m(a)$.

Les symboles définis de K sont γ (règles G et X) et $*$ (toutes les autres). Déterminons les couples de dépendance de K :

A. $(a * b) * c$ avec $a * (b * c)$ et $b * c$.

I, J, P, Q, G, X. Aucune, les membres de droite de ces règles ne contenant pas de symbole $*$ ni γ .

D. $\gamma(a, b) * c$ avec $\gamma(a * c, b * c)$, $a * c$ et $b * c$.

M. $\mu(a, b) * c$ avec $a * c$, $b * c$.

L. $\lambda(a) * b$ avec $a * \gamma(p, b * q)$, $\gamma(p, b * q)$ et $b * q$.

En vertu des remarques faites précédemment, il suffit maintenant de prouver que, pour toute substitution f , les inégalités suivantes sont satisfaites :

- $m(f(a)) \geq m(f(b))$ et $|f(a)| \geq |f(b)|$ pour toute règle (a, b) de K_0 ;
- $m(f(\lambda(a) * b)) \geq m(f(\lambda(a * \gamma(p, b * q))))$ et $|f(\lambda(a) * b)| \geq |f(\lambda(a * \gamma(p, b * q)))|$;
- $|f(\lambda(a) * b)| > |f(a * \gamma(p, b * q))|$.

Lemme B.5. *Pour toute règle (a, b) de K et toute substitution f , on a :*

$$m(f(a)) \geq m(f(b)).$$

Démonstration. Remarquons, tout d'abord, que montrer le résultat pour (A) revient à montrer que $m((a * b) * \gamma(c, d)) \geq m(a * (b * \gamma(c, d)))$ pour tous $a, b, c, d \in T$, de même pour les autres règles et pour les futures preuves.

- A. $m((a * b) * c) = m(a).m(b).m(c) = m(a * (b * c))$.
- I. $m(i * a) = m(a)$.
- J. $m(a * i) = m(a)$.
- P. $m(p * \gamma(a, b)) = \max(m(a), m(b)) \geq m(a)$.
- Q. $m(q * \gamma(a, b)) = \max(m(a), m(b)) \geq m(b)$.
- G. $m(\gamma(p, q)) = 1 = m(i)$.
- X. $m(\gamma(p * a, q * a)) = m(a)$.
- D. $m(\gamma(a, b) * c) = \max(m(a), m(b)).m(c) = m(\gamma(a * c, b * c))$.
- M. $m(\mu(a, b) * c) = (m(a) + m(b)).m(c) = m(\mu(a * c, b * c))$.
- L. $m(\lambda(a) * b) = m(a).m(b) = m(\lambda(a * \gamma(p, b * q)))$.

◇

Il ne reste plus qu'à montrer :

Proposition B.6. *Pour toute règle (a, b) dans K et toute substitution f , on a :*

$$|f(a)| \geq |f(b)|.$$

De plus, pour tous termes a, b et c et pour toute substitution f , on a :

$$|f(\lambda(a) * \gamma(b, c))| > |f(a * \gamma(p, \gamma(b * q)))|.$$

Démonstration. On fixe $a, b, c \in T$.

- A. $|(a * b) * c| = |a| + m(a).|b| + m(a).m(b).|c| = |a * (b * c)|$.
- I. $|i * a| = |a|$.
- J. $|a * i| = |a|$.
- P. $|p * \gamma(a, b)| = \max(|a|, |b|) \geq |a|$.
- Q. $|q * \gamma(a, b)| = \max(|a|, |b|) \geq |b|$.
- G. $|\gamma(p, q)| = 0 = |i|$.
- X. $|\gamma(p * a, q * a)| = |a|$.
- D. $\begin{cases} |\gamma(a, b) * c| = \max(|a|, |b|) + \max(m(a), m(b)).|c| \\ |\gamma(a * c, b * c)| = \max(|a| + m(a).|c|, |b| + m(b).|c|) \end{cases}$
D'où $|\gamma(a, b) * c| \geq |\gamma(a * c, b * c)|$.

$$\text{M. } |\mu(a, b) * c| = |a| + |b| + (m(a) + m(b)).|c| = |\mu(a * c, b * c)|.$$

$$\text{L. } \begin{cases} |\lambda(a) * b| = 1 + |a| + m(a).|b| = |\lambda(a * \gamma(p, b * q))| \\ |a * \gamma(p, b * q)| = |a| + m(a).|b| \end{cases}$$

$$\text{D'où } |\lambda(a) * b| - |a * \gamma(p, b * q)| = 1 > 0.$$

◇

On en conclut donc :

Théorème B.7. *La relation K termine sur T .*

B.2.4 La relation K est confluente

Puisque la relation K termine et, en vertu du lemme de Newman, il suffit de montrer que K est localement confluente. C'est le cas si toutes les paires critiques de K peuvent être fermées, c'est-à-dire que, pour tout branchement critique $b \leftarrow_K a \rightarrow_K c$ dans T , il existe $d \in T$ tel que $b \rightarrow_K d \leftarrow_K c$.

La relation K possède vingt-deux paires critiques ; nous allons voir qu'elles sont toutes confluentes.

A/A. D'une part :

$$\begin{aligned} ((a * b) * c) * d &\rightarrow_A (a * b) * (c * d) \\ &\rightarrow_A a * (b * (c * d)). \end{aligned}$$

D'autre part :

$$\begin{aligned} ((a * b) * c) * d &\rightarrow_A (a * (b * c)) * d \\ &\rightarrow_A a * ((b * c) * d) \\ &\rightarrow_A a * (b * (c * d)). \end{aligned}$$

A/I. On a :

$$\begin{aligned} (i * a) * b &\rightarrow_A i * (a * b) \\ &\rightarrow_I a * b. \end{aligned}$$

Et :

$$(i * a) * b \rightarrow_I a * b.$$

A/J-1. On a :

$$\begin{aligned} (a * i) * b &\rightarrow_A a * (i * b) \\ &\rightarrow_I a * b. \end{aligned}$$

Et :

$$(a * i) * b \rightarrow_J a * b.$$

A/J-2. On a :

$$\begin{aligned} (a * b) * i &\rightarrow_A a * (b * i) \\ &\rightarrow_J a * b. \end{aligned}$$

Et :

$$(a * b) * i \rightarrow_J a * b.$$

A/P. On a :

$$\begin{aligned} (p * \gamma(a, b)) * c &\rightarrow_{AP} p * (\gamma(a, b) * c) \\ &\rightarrow_{DP} p * \gamma(a * c, b * c) \\ &\rightarrow_P a * c. \end{aligned}$$

Et :

$$(p * \gamma(a, b)) * c \rightarrow_P a * c.$$

A/Q. On a :

$$\begin{aligned} (q * \gamma(a, b)) * c &\rightarrow_A q * (\gamma(a, b) * c) \\ &\rightarrow_{DQ} q * \gamma(a * c, b * c) \\ &\rightarrow_Q b * c. \end{aligned}$$

Et :

$$(q * \gamma(a, b)) * c \rightarrow_Q b * c.$$

A/D. On a :

$$\begin{aligned} (\gamma(a, b) * c) * d &\rightarrow_A \gamma(a, b) * (c * d) \\ &\rightarrow_D \gamma(a * (c * d), b * (c * d)). \end{aligned}$$

Et :

$$\begin{aligned} (\gamma(a, b) * c) * d &\rightarrow_D \gamma(a * c, b * c) * d \\ &\rightarrow_D \gamma((a * c) * d, (b * c) * d) \\ &\rightarrow_A \gamma(a * (c * d), b * (c * d)). \end{aligned}$$

A/M. On a :

$$\begin{aligned} (\mu(a, b) * c) * d &\rightarrow_A \mu(a, b) * (c * d) \\ &\rightarrow_M \mu(a * (c * d), b * (c * d)). \end{aligned}$$

Et :

$$\begin{aligned} (\mu(a, b) * c) * d &\rightarrow_M \mu(a * c, b * c) * d \\ &\rightarrow_M \mu((a * c) * d, (b * c) * d) \\ &\rightarrow_A \mu(a * (c * d), b * (c * d)). \end{aligned}$$

A/L. On a :

$$\begin{aligned} (\lambda(a) * b) * c &\rightarrow_A \lambda(a) * (b * c) \\ &\rightarrow_L \lambda(a * \gamma(p, (b * c) * q)) \\ &\rightarrow_A \lambda(a * \gamma(p, b * (c * q))). \end{aligned}$$

Et :

$$\begin{aligned} (\lambda(a) * b) * c &\rightarrow_L \lambda(a * \gamma(p, b * q)) * c \\ &\rightarrow_L \lambda((a * \gamma(p, b * q)) * \gamma(p, c * q)) \\ &\rightarrow_A \lambda(a * (\gamma(p, b * q) * \gamma(p, c * q))) \\ &\rightarrow_D \lambda(a * \gamma(p * \gamma(p, c * q), (b * q) * \gamma(p, c * q))) \\ &\rightarrow_P \lambda(a * \gamma(p, (b * q) * \gamma(p, c * q))) \\ &\rightarrow_A \lambda(a * \gamma(p, b * (q * \gamma(p, c * q)))) \\ &\rightarrow_Q \lambda(a * \gamma(p, b * (c * q))). \end{aligned}$$

I/J. On a : $i \leftarrow_I i * i \rightarrow_J i$.

J/X. On a :

$$\begin{aligned} \gamma(p * i, q * i) &\rightarrow_J \gamma(p, q) \\ &\rightarrow_G i. \end{aligned}$$

Et :

$$\gamma(p * i, q * i) \rightarrow_X i.$$

J/D. On a :

$$\begin{aligned} \gamma(a, b) * i &\rightarrow_D \gamma(a * i, b * i) \\ &\rightarrow_J \gamma(a, b). \end{aligned}$$

Et :

$$\gamma(a, b) * i \rightarrow_J \gamma(a, b).$$

J/M. On a :

$$\begin{aligned}\mu(a, b) * i &\rightarrow_D \mu(a * i, b * i) \\ &\rightarrow_J \mu(a, b).\end{aligned}$$

Et :

$$\mu(a, b) * i \rightarrow_J \mu(a, b).$$

J/L. On a :

$$\begin{aligned}\lambda(a) * i &\rightarrow_L \lambda(a * \gamma(p, i * q)) \\ &\rightarrow_I \lambda(a * \gamma(p, q)) \\ &\rightarrow_G \lambda(a * i) \\ &\rightarrow_J \lambda(a).\end{aligned}$$

Et :

$$\lambda(a) * i \rightarrow_J \lambda(a).$$

P/G. On a :

$$\begin{aligned}p * \gamma(p, q) &\rightarrow_G p * i \\ &\rightarrow_J p.\end{aligned}$$

Et :

$$p * \gamma(p, q) \rightarrow_P p.$$

P/X-1. $p * a \leftarrow_P p * \gamma(p * a, q * a) \rightarrow_X p * a.$

P/X-2. On a :

$$\begin{aligned}\gamma(p * \gamma(a, b), q * \gamma(a, b)) &\rightarrow_P \gamma(a, q * \gamma(a, b)) \\ &\rightarrow_Q \gamma(a, b).\end{aligned}$$

Et :

$$\gamma(p * \gamma(a, b), q * \gamma(a, b)) \rightarrow_X \gamma(a, b).$$

Q/G. On a :

$$\begin{aligned}q * \gamma(p, q) &\rightarrow_G q * i \\ &\rightarrow_J q.\end{aligned}$$

Et :

$$q * \gamma(p, q) \rightarrow_Q q.$$

Q/X-1. $q * a \leftarrow_Q q * \gamma(p * a, q * a) \rightarrow_X q * a.$

Q/X-2. On a :

$$\begin{aligned} \gamma(p * \gamma(a, b), q * \gamma(a, b)) &\rightarrow_Q \gamma(p * \gamma(a, b), b) \\ &\rightarrow_P \gamma(a, b). \end{aligned}$$

Et :

$$\gamma(p * \gamma(a, b), q * \gamma(a, b)) \rightarrow_X \gamma(a, b).$$

G/D. On a :

$$\begin{aligned} \gamma(p, q) * a &\rightarrow_G i * a \\ &\rightarrow_I a. \end{aligned}$$

Et :

$$\begin{aligned} \gamma(p, q) * a &\rightarrow_D \gamma(p * a, q * a) \\ &\rightarrow_X a. \end{aligned}$$

X/D. On a :

$$\begin{aligned} \gamma(p * a, q * a) * b &\rightarrow_D \gamma((p * a) * b, (q * a) * b) \\ &\rightarrow_A \gamma(p * (a * b), q * (a * b)) \\ &\rightarrow_X a * b. \end{aligned}$$

Et :

$$\gamma(p * a, q * a) * b \rightarrow_X a * b.$$

M/B. Il n'est pas nécessaire d'étudier cette paire critique pour la confluence de K , mais on en aura besoin plus tard. On a :

$$\begin{aligned} \mu(\lambda(a), b) * c &\rightarrow_M \mu(\lambda(a) * c, b * c) \\ &\rightarrow_L \mu(\lambda(a * \gamma(p, c * q)), b * c) \\ &\rightarrow_B (a * \gamma(p, c * q)) * \gamma(b * c, i) \\ &\rightarrow_A a * (\gamma(p, c * q) * \gamma(b * c, i)) \\ &\rightarrow_D a * \gamma(p * \gamma(b * c, i), (c * q) * \gamma(b * c, i)) \\ &\rightarrow_P a * \gamma(b * c, (c * q) * \gamma(b * c, i)) \\ &\rightarrow_A a * \gamma(b * c, c * (q * \gamma(b * c, i))) \\ &\rightarrow_Q a * \gamma(b * c, c * i) \\ &\rightarrow_J a * \gamma(b * c, c). \end{aligned}$$

Et :

$$\begin{aligned}
 \mu(\lambda(a), b) * c &\rightarrow_B (a * \gamma(b, i)) * c \\
 &\rightarrow_A a * (\gamma(b, i) * c) \\
 &\rightarrow_D a * \gamma(b * c, i * c) \\
 &\rightarrow_I a * \gamma(b * c, c).
 \end{aligned}$$

Puisque K termine, on en conclut :

Proposition B.8. *La relation K est confluente sur T .*

B.2.5 La relation KB est confluente

On commence par :

Lemme B.9. *La relation B est convergente sur T .*

Démonstration. Pour la confluence, il suffit de noter que B est linéaire à gauche et ne crée pas de paire critique avec elle-même. C'est donc une relation *orthogonale* et, en particulier, confluente.

Pour la terminaison, on munit Σ de l'ordre strict $\mu >_\Sigma *$, $\mu >_\Sigma \gamma$ et $\mu >_\Sigma i$, puis on construit $>$ l'ordre lexicographique sur T associé à $>_\Sigma$. On a alors $\mu(\lambda(a), b) > a * \gamma(b, i)$. En effet, comme $\mu >_\Sigma *$, il suffit de vérifier que $\mu(\lambda(a), b) > a$ et $\mu(\lambda(a), b) > \gamma(b, i)$. La première inégalité est donnée par le fait que a est un sous-terme strict de $\mu(\lambda(a), b)$ et la seconde par $\mu >_\Sigma \gamma$, $\mu(\lambda(a), b) > b$ (car b sous-terme strict de $\mu(\lambda(a), b)$) et $\mu(\lambda(a), b) > i$ (car $\mu >_\Sigma i$). \diamond

On a donc deux relations convergentes K et B sur T . Tout élément a de T a donc une unique forme normale $K(a)$ pour K et une unique forme normale $B(a)$ pour B . On note $K(T)$ l'ensemble des K -formes normales de T . Rappelons quelques notions et résultats :

Rappels. Soient X un ensemble et R, S deux relations binaires sur X . On dit que S est un *raffinement* de R si $R \subseteq S^*$ et que ce raffinement est *compatible* si :

$$\text{pour tous } a, b, c \in X, \text{ si } a \rightarrow_S b \rightarrow_R c \text{ alors il existe un } d \in X, \text{ tel que } a \rightarrow_R d \leftarrow_R c.$$

Si S est un raffinement compatible de R alors : R est confluente si et seulement si S est confluente.

On va montrer :

Lemme B.10. *La relation KB est confluente sur $K(T)$.*

Démonstration. On définit les relations K^∞ et B^∞ par $a \rightarrow_{K^\infty} b$ (resp. $a \rightarrow_{B^\infty} b$) si $b = K(a)$ (resp. $b = B(a)$). De plus, on définit $B^\infty \cdot K^\infty$ comme la composée de ces deux relations, c'est-à-dire que $a \rightarrow_{B^\infty \cdot K^\infty} b$ si il existe $c \in T$ vérifiant $a \rightarrow_{B^\infty} c \rightarrow_{K^\infty} b$: en d'autres termes, $c = B(a)$ et $b = K(c) = K(B(a))$.

On va montrer que KB est un raffinement compatible de $B^\infty \cdot K^\infty$ sur $K(T)$ et que cette relation est confluente. On a : $B^\infty \subseteq B^*$ et $K^\infty \subseteq K^*$ donc $B^\infty \cdot K^\infty \subseteq (KB)^*$ et donc KB est un raffinement de $B^\infty \cdot K^\infty$. Soient $a, b, c \in K(T)$ vérifiant :

$$a \rightarrow_{KB} b \rightarrow_{B^\infty \cdot K^\infty} c.$$

Il est impossible que $a \rightarrow_K b$ car $a \in K(T)$ donc $a \rightarrow_B b$. Si $b = c$, on a $a \rightarrow_B c$ donc $B(a) = B(c)$ et donc $K(B(a)) = K(B(c))$. On a donc bien, en posant $d = K(B(a))$:

$$a \twoheadrightarrow_{B^\infty \cdot K^\infty} d \leftarrow_{B^\infty \cdot K^\infty} c.$$

Si $b \neq c$ alors la réduction de b à c commence par au moins un B^∞ et donc $B(b) = B(a)$, d'où $a \twoheadrightarrow_{B^\infty \cdot K^\infty} c$ et donc $d = c$ convient. On a donc montré que KB est un raffinement compatible de $B^\infty \cdot K^\infty$ sur $K(T)$. Il reste à voir que $B^\infty \cdot K^\infty$ est confluente.

Soient $a, b, c \in T$ tels que $a \twoheadrightarrow_{B^\infty \cdot K^\infty} b$ et $a \twoheadrightarrow_{B^\infty \cdot K^\infty} c$. Alors il existe $m, n \in \mathbb{N}$ tels que $b = (K \circ B)^m(a)$ et $c = (K \circ B)^n(a)$. Si $m = n$ alors $b = c$. Sinon, on suppose que l'on a $m > n$: alors $b = (K \circ B)^{m-n}(c)$. Dans les deux cas $b \rightarrow_{B^\infty \cdot K^\infty} c$ (si $n > m$, la réduction est dans l'autre sens).

On en conclut que $B^\infty \cdot K^\infty$ est confluente et donc que KB est confluente sur $K(T)$. \diamond

On définit à présent une relation \tilde{B} dérivée de B . Cette réduction agit comme B , sauf qu'elle réduit tous les B -redexes identiques d'un terme ; pour des raisons techniques, on va aussi demander à \tilde{B} d'être réflexive. Formellement, $a \rightarrow_{\tilde{B}} b$ si $a = b$ ou si il existe $n \geq 1$ et $a_0, \dots, a_n, c, d \in T$ tels que $a = a_0$ et $b = b_n$ ainsi que des contextes C_0, \dots, C_n vérifiant :

- pour tout $k \in \{0, \dots, n-1\}$, $a_k = C_k[\mu(\lambda(c), d)]$ et $a_{k+1} = C_{k+1}[c * \gamma(d, i)]$;
- il n'existe pas de contexte D tel que $b = D[\mu(\lambda(c), d)]$.

Par exemple :

$$\gamma(p * \mu(\lambda(c), d), q * \mu(\lambda(c), d)) \rightarrow_{\tilde{B}} \gamma(p * (c * \gamma(d, i)), q * (c * \gamma(d, i))).$$

La relation \tilde{B} est une composée particulière de B -réductions. Cependant, il est clair que, B étant orthogonale, l'ordre dans lequel on effectue les B -réductions n'a pas d'importance.

On vérifie :

Lemme B.11. *On a les inclusions : $\tilde{B} \subseteq B^t$ et $B^\infty \subseteq \tilde{B}^t$.*

Le lemme suivant précise la forme des diagrammes de commutation entre \tilde{B} et K .

Lemme B.12. *Si a, b, c sont des éléments de T tels que $a \rightarrow_{\tilde{B}} b$ et $a \rightarrow_K c$ alors il existe d_1, d_2 , et d_3 dans T tels que :*

$$\begin{array}{ccccc} a & \xrightarrow{\tilde{B}} & b & & \\ K \downarrow & & \downarrow K & & \\ c & \xrightarrow{K} d_1 & \xrightarrow{\tilde{B}} d_2 & \xrightarrow{K} & d_3 \end{array}$$

Démonstration. Si $a = b$, on prend $d_1 = d_2 = d_3 = c$. On suppose donc que $a \neq b$.

Soit $x = \mu(\lambda(y), z)$ le B -redex réduit lors de $a \rightarrow_{\tilde{B}} b$. On va procéder en examinant quelle règle intervient lors de $a \rightarrow_K c$ et la position du K -redex par rapport aux positions de c dans a .

Tout d'abord, on observe que seule la règle M induit une paire critique avec B : toutes les autres lui sont orthogonales. De plus, parmi les autres règles, D et X sont les seules à ne pas être linéaires et P et Q sont les seules à ne pas avoir les mêmes variables à gauche et à droite. Cependant, tout B -redex x de a est soit préservé, soit dupliqué, soit effacé.

L'application de la règle \tilde{B} (contractant le redex x) à c est donc possible, et on obtient un diagramme :

$$\begin{array}{ccc} a & \xrightarrow{\tilde{B}} & b \\ K \downarrow & & \downarrow K \\ c & \xrightarrow{\tilde{B}} & d \end{array}$$

Remarquons que, même si le B -redex x n'est plus dans c , on a $c \rightarrow_{\tilde{B}} c$.

Il reste à traiter le cas où $a \rightarrow_M c$. Si le redex réduit par M ne celui réduit par B , on est dans le cas précédent (comme avec D). Sinon, il existe exactement un redex x dans a tel que $a = C[x * t]$. On a déjà vu que, dans un tel cas, si on note $a' = C[(y * \gamma(z, i)) * t]$, il existe e_1, e_2 et e_3 tels que :

$$\begin{array}{ccccc} a & \xrightarrow{B} & a' & & \\ M \downarrow & & \downarrow K & & \\ c & \xrightarrow{K} e_1 & \xrightarrow{B} e_2 & \xrightarrow{K} & e_3 \end{array}$$

De plus, la règle M n'apparaît pas dans les $a' \rightarrow_K e_3$, $c \rightarrow_K e_1$, $e_2 \rightarrow_K e_3$. Ainsi, toute autre B -réduction effectuée sur a commute avec toutes ces K -réductions. Ainsi, on obtient bien un diagramme :

$$\begin{array}{ccccc} a & \xrightarrow{\tilde{B}} & b & & \\ \downarrow K & & \downarrow K & & \\ c & \xrightarrow{K} d_1 \xrightarrow{\tilde{B}} d_2 \xrightarrow{K} d_3 & & & \end{array}$$

◇

Lemme B.13. *Pour tous a, b dans T tels que $a \rightarrow_{\tilde{B}} b$, on a $K(a) \rightarrow_{KB} K(b)$:*

$$\begin{array}{ccc} a & \xrightarrow{\tilde{B}} & b \\ \downarrow K & & \downarrow K \\ K(a) & \xrightarrow{KB} & K(b) \end{array}$$

Démonstration. Comme K termine on peut appliquer le principe de récurrence pour démontrer le résultat. Soit $a \in T$. Si $a \in K(T)$, alors $K(a) = a$, donc $K(a) \rightarrow_B b$ et donc $K(a) \rightarrow_{KB} K(b)$. Maintenant, supposons que $a \notin K(T)$ et que, pour tout c dans T tel que $a \rightarrow_K^+ c$, on a $P(c)$. Comme $a \notin K(T)$, il existe $c \in T$ tel que $a \rightarrow_K c \rightarrow_K K(a)$. D'après le lemme précédent, il existe d_1, d_2, d_3 tels que :

$$\begin{array}{ccccc} a & \xrightarrow{\tilde{B}} & b & & \\ \downarrow K & & \downarrow K & & \\ c & \xrightarrow{K} d_1 \xrightarrow{\tilde{B}} d_2 \xrightarrow{K} d_3 & & & \end{array}$$

Comme $a \rightarrow_K c \rightarrow_K d_1$, on a $a \rightarrow_K^+ d_1$. On peut donc appliquer l'hypothèse de récurrence à $d_1 \rightarrow_{\tilde{B}} d_2$:

$$\begin{array}{ccccccc} a & \xrightarrow{\tilde{B}} & b & & & & \\ \downarrow K & & \downarrow K & & & & \\ c & \xrightarrow{K} d_1 \xrightarrow{\tilde{B}} d_2 \xrightarrow{K} d_3 & & & & & \\ \downarrow K & \downarrow K & \downarrow K & & \downarrow K & & \\ K(a) & K(d_1) \xrightarrow{KB} K(d_2) & & & K(b) & & \end{array}$$

Comme $a \rightarrow_K d_1$ et que K est convergente, on a $K(a) = K(d_1)$. De même, $b \rightarrow_K d_3$ et $d_2 \rightarrow_K d_3$, donc $K(d_2) = K(d_3) = K(b)$ d'où :

$$\begin{array}{ccccc}
 a & \xrightarrow{\tilde{B}} & & & b \\
 \downarrow K & & & & \downarrow K \\
 c & \xrightarrow{K} & d_1 & \xrightarrow{\tilde{B}} & d_2 & \xrightarrow{K} & d_3 \\
 \downarrow K & \swarrow K & & \searrow K & & & \downarrow K \\
 K(a) = K(d_1) & \xrightarrow{KB} & & & K(d_2) = K(b)
 \end{array}$$

On a donc prouvé le lemme. \diamond

Lemme B.14. *Pour tout a de T , on a $K(a) \rightarrow_{KB} K(B(a))$:*

$$\begin{array}{ccc}
 a & \xrightarrow{B} & B(a) \\
 \downarrow K & & \downarrow K \\
 K(a) & \xrightarrow{KB} & K(B(a))
 \end{array}$$

Démonstration. On va procéder par récurrence, en utilisant cette fois le fait que B est convergente. Si $a = B(a)$, alors $K(a) = K(B(a))$. Maintenant, supposons que $a \neq B(a)$. On a vu que $B^\infty \subseteq \tilde{B}^*$. Comme $a \rightarrow_{B^\infty} B(a)$, il existe a_1, \dots, a_n tels que $a \rightarrow_{\tilde{B}} a_1$, $a_n \rightarrow_{\tilde{B}} B(a)$ et, pour tout i , $a_i \rightarrow_{\tilde{B}} a_{i+1}$; de plus, il y a au moins un i tel que $a_i \neq a_{i+1}$ car sinon $a = B(a)$. On peut supposer que $a \neq a_1$ puisque l'ordre des réductions est indifférent (B est orthogonale). On applique alors le lemme précédent pour obtenir :

$$\begin{array}{ccccc}
 a & \xrightarrow{\tilde{B}} & a_1 & \xrightarrow{B} & B(a) \\
 \downarrow K & & \downarrow K & & \downarrow K \\
 K(a) & \xrightarrow{KB} & K(a_1) & & K(B(a))
 \end{array}$$

Comme $a \rightarrow_{\tilde{B}} a_1$ et que $\tilde{B} \subseteq B^t$, on a $B(a) = B(a_1)$; de plus, $a \neq a_1$, donc on peut appliquer l'hypothèse de récurrence à a_1 ce qui donne :

$$\begin{array}{ccccc}
 a & \xrightarrow{\tilde{B}} & a_1 & \xrightarrow{B} & B(a) \\
 \downarrow K & & \downarrow K & & \downarrow K \\
 K(a) & \xrightarrow{KB} & K(a_1) & \xrightarrow{KB} & K(B(a))
 \end{array}$$

Ce qui conclut la preuve. \diamond

Corollaire B.15. *Pour tous $a, b \in T$ tels que $a \rightarrow_B b$, il existe $c \in K(T)$ tel que :*

$$K(a) \rightarrow_{KB} c \leftarrow_{KB} K(b).$$

Démonstration. On commence par appliquer le lemme précédent à a et b . On en déduit que $K(a) \rightarrow_{KB} K(B(a))$ et $K(b) \rightarrow_{KB} K(B(b))$. Or $a \rightarrow_B b$ et donc, comme B est convergente, $B(a) = B(b)$. D'où $K(a) \rightarrow_{KB} c \leftarrow_{KB} K(b)$ avec $c = K(B(a)) = K(B(b)) \in K(T)$. \diamond

On va maintenant démontrer une variante de la technique d'interprétation de Hardin qui permettra de conclure.

Proposition B.16. *Soit X un ensemble muni de deux relations binaires R et S avec R convergente. On note $R(x)$ la R -forme normale d'un élément x de X et $R(X)$ l'ensemble des R -formes normales de X . Supposons qu'il existe $U \subseteq (R \cup S)^t_{R(X)}$ vérifiant la condition suivante :*

Pour tous x et y dans X tels que $x \rightarrow_S y$, il existe un $z \in R(X)$, vérifiant

$$R(x) \rightarrow_U z \leftarrow_U R(y).$$

Alors, la confluence de U entraîne celle de $R \cup S$.

Démonstration. On va montrer que $R \cup S$ est semi-confluente, ce qui suffit à prouver sa confluence. Tout d'abord, notons que $x \rightarrow_{R \cup S} y$ si et seulement si il existe x_1, \dots, x_n tels que :

$$x \rightarrow_R x_1 \rightarrow_S x_2 \rightarrow_R x_3 \rightarrow_S \dots \rightarrow_S x_n \rightarrow_R y.$$

Soient x et y tels que $x \rightarrow_{R \cup S} y$. Deux cas sont possibles : $x \rightarrow_R y$ et $x \rightarrow_S y$. Supposons que l'on est dans le premier cas. Maintenant soient x_1, \dots, x_n tels que :

$$x \rightarrow_R x_1 \rightarrow_S x_2 \rightarrow_R x_3 \rightarrow_S \dots \rightarrow_R x_n.$$

On va montrer par récurrence que, pour tout $i \in \{1, \dots, n\}$, il existe $y_i \in R(X)$ tel que $R(y) \rightarrow_U y_i \leftarrow_U R(x_i)$. Pour $i = 1$, on a $x \rightarrow_R x_1$ et $x \rightarrow_R y$; donc, par convergence de R , $R(y) = R(x_1)$ et donc $y_1 = R(y)$ convient. Supposons que l'on a construit un tel y_i pour $i \in \{1, \dots, n-1\}$ fixé. Construisons y_{i+1} selon la parité de i . Si i est pair, on a :

$$\begin{array}{ccc} x_i & \xrightarrow{R} & x_{i+1} \\ R \downarrow & & \downarrow R \\ R(x_i) & & R(x_{i+1}) \\ U \downarrow & & \\ R(y) & \xrightarrow{U} & y_i \end{array}$$

Comme R est convergente et que $x_i \twoheadrightarrow_R x_{i+1}$, on a $R(x_i) = R(x_{i+1})$ et donc $y_{i+1} = y_i$ convient.

Maintenant, supposons que i est impair :

$$\begin{array}{ccc}
 x_i & \xrightarrow{S} & x_{i+1} \\
 R \downarrow & & \downarrow R \\
 R(x_i) & & R(x_{i+1}) \\
 U \downarrow & & \\
 R(y) \xrightarrow{U} y_i & &
 \end{array}$$

Par hypothèse, il existe $z \in R(X)$, tel que :

$$R(x_i) \twoheadrightarrow_U z \leftarrow_U R(x_{i+1}).$$

On a donc $R(x_i) \twoheadrightarrow_U z$ et $R(x_i) \twoheadrightarrow_U y_i$. Comme on a supposé U confluente, il existe $y_{i+1} \in R(X)$ tel que :

$$y \twoheadrightarrow_U y_i \twoheadrightarrow_U y_{i+1} \quad \text{et} \quad R(x_{i+1}) \twoheadrightarrow_U z \twoheadrightarrow_U y_{i+1}.$$

On a donc construit une famille (y_1, \dots, y_n) . En particulier, y_n vérifie :

$$\begin{array}{ccc}
 x & \xrightarrow{R \cup S} & x_n \\
 R \downarrow & & \downarrow U \\
 y \xrightarrow{R} R(y) \xrightarrow{U} y_n & &
 \end{array}$$

On conclut en rappelant que $U \subseteq (R \cup S)^t_{|R(X)}$.

Examinons à présent le cas $x \rightarrow_S y$. Soient x_1, \dots, x_n tels que :

$$x \twoheadrightarrow_R x_1 \rightarrow_S x_2 \twoheadrightarrow_R x_3 \rightarrow_S \dots \twoheadrightarrow_R x_n.$$

On va montrer par récurrence que, pour tout $i \in \{1, \dots, n\}$, il existe $y_i \in R(X)$ tel que $R(y) \twoheadrightarrow_U y_i \leftarrow_U R(x_i)$. Pour $i = 1$: par hypothèse, il existe $y_1 \in R(X)$ tel que $R(y) \twoheadrightarrow_U y_1 \leftarrow_U R(x)$. Or R est convergente et $x \twoheadrightarrow_R x_1$ donc $R(x) = R(x_1)$. La suite de la récurrence est identique au cas précédent.

◇

On applique alors ce résultat avec $X = T$, $R = K$, $S = B$ et $U = (KB)^t_{|K(T)}$ pour obtenir :

Théorème B.17. *La relation KB est confluente sur T .*

B.3 Définition du déliement

B.3.1 Définition du déliement sur les λ -termes formels

On définit ici l'application $\Phi : \bar{\Lambda} \longrightarrow T$, qui n'est rien d'autre que la transcription des λ -termes en notation de de Bruijn, telle qu'elle est définie dans [dB72], composée avec l'application $n \longmapsto p * q^n$.

Pour commencer, on définit, pour tout $x \in V$ et tout $n \in \mathbb{N}^*$, une application σ_x^n de $\bar{\Lambda}_{\mathbb{N}^*}$ dans lui-même, qui remplace chaque occurrence de x par $n + k$ où k est le nombre de λ rencontrés jusqu'à elle. Plus formellement, si f est un $\lambda_{\mathbb{N}^*}$ -terme formel, et toujours par récurrence sur son degré :

1. si $f = x$, alors $\sigma_x^n(f) = n$;
2. si $f \in V$ et $f \neq x$, alors $\sigma_x^n(f) = f$;
3. si $f \in \mathbb{N}^*$, alors $\sigma_x^n(f) = f$;
4. si $f = \mu(g, h)$, alors $\sigma_x^n(f) = \mu(\sigma_x^n(g), \sigma_x^n(h))$;
5. si $f = \lambda x.g$, alors $\sigma_x^n(f) = f$;
6. si $f = \lambda y.g$ avec $y \neq x$, alors $\sigma_x^n(f) = \lambda y.(\sigma_x^{n+1}(g))$.

On commence par démontrer :

Lemme B.18. *Pour tous $n \in \mathbb{N}^*$, $x \in V$ et $f \in \bar{\Lambda}_{\mathbb{N}^*}$ tels que $x \notin \mathcal{V}(f)$, on a $\sigma_x^n(f) = f$.*

Démonstration. Par récurrence sur le degré de f . Si $f \in V$, alors on a forcément $f \neq x$ puisque $x \notin \mathcal{V}(f)$ et donc $\sigma_x^n(f) = f$, par définition de σ_x^n ; de même pour $f \in \mathbb{N}^*$.

Maintenant, supposons que la propriété est vraie pour les termes de degré au plus $k \in \mathbb{N}^*$ fixé et que $|f| = k + 1$. On distingue les cas suivants.

- Si $f = \mu(g, h)$ avec g et h de degré au plus k . On a $\mathcal{V}(f) = \mathcal{V}(g) \cup \mathcal{V}(h)$, donc $y \notin \mathcal{V}(g)$ et $y \notin \mathcal{V}(h)$. Alors :

$$\begin{aligned}
 \sigma_x^n(f) &= \sigma_x^n(\mu(g, h)) \\
 &= \mu(\sigma_x^n(g), \sigma_x^n(h)) \\
 &= \mu(g, h) \\
 &= f.
 \end{aligned}
 \tag{HR}$$

- Si $f = \lambda x.g$: la définition de σ_x^n donne directement le résultat.

- Si $f = \lambda y.g$ avec $y \neq g$ et $|g| \leq k$. On a $\mathcal{V}(f) = \mathcal{V}(g) \setminus \{y\}$ donc $x \notin \mathcal{V}(g)$. Alors :

$$\begin{aligned} \sigma_x^n(f) &= \sigma_x^n(\lambda y.g) \\ &= \lambda y.(\sigma_x^{n+1}(g)) \\ &= \lambda y.g \\ &= f. \end{aligned} \tag{HR}$$

◇

On vérifie :

Lemme B.19. 1. Pour tous $n \in \mathbb{N}^*$, $x \in V$ et $f \in \bar{\Lambda}_{\mathbb{N}^*}$, on a $\mathcal{V}(\sigma_x^n(f)) = \mathcal{V}(f) \setminus \{x\}$.

2. Pour tous $n, m \in \mathbb{N}^*$, $x, y \in V$ tels que $x \neq y$ on a $\sigma_x^n \circ \sigma_y^m = \sigma_y^m \circ \sigma_x^n$.

3. Pour tous $n \in \mathbb{N}^*$, $x, y, z \in V$ tels que $z \notin \{x, y\}$, on a $\sigma_z^n \circ [x := y] = [x := y] \circ \sigma_z^n$.

Fixons maintenant deux notations. L'ensemble V des variables est dénombrable ; on choisit une bijection $\chi : V \longrightarrow \mathbb{N}^*$. De plus, pour tout $n \in \mathbb{N}^*$, on pose $q^{n+1} = q * q^n$, avec $q^1 = q$.

Maintenant, on peut définir, pour tout $n \in \mathbb{N}$, une application $\Phi^n : \bar{\Lambda}_{\mathbb{N}^*} \longrightarrow T$ comme suit. Si f est un $\lambda_{\mathbb{N}^*}$ -terme formel, et toujours par récurrence sur son degré :

1. si $f \in V$, alors $\Phi^n(f) = \begin{cases} p & \text{si } n = 0 \text{ et } \chi(f) = 1 ; \\ p * q^{\chi(f)+n-1} & \text{sinon ;} \end{cases}$
2. si $f \in \mathbb{N}^*$, alors $\Phi^n(f) = \begin{cases} p & \text{si } f = 1 ; \\ p * q^{f-1} & \text{sinon ;} \end{cases}$
3. si $f = \mu(g, h)$, alors $\Phi^n(f) = \mu(\Phi^n(g), \Phi^n(h))$;
4. si $f = \lambda x.g$, alors $\Phi^n(f) = \lambda(\Phi^{n+1}(\sigma_x^1(g)))$.

Enfin, on appelle *déliement* l'application $\Phi : \bar{\Lambda} \longrightarrow T$ obtenue par composition de $i : \bar{\Lambda} \longrightarrow \bar{\Lambda}_{\mathbb{N}^*}$ avec $\Phi^0 : \bar{\Lambda}_{\mathbb{N}^*} \longrightarrow T$.

Remarque. Cette application donne, comme nous le verrons plus loin, une injection de l'ensemble des classes des λ -termes *modulo* $\alpha\beta\eta$ -équivalence dans le C -monoïde initial. Ce n'est pas la même construction que celle de [LS86] qui établit une équivalence de catégories entre celle des λ -calculs non typés avec couplage surjectif et celle des C -monoïdes.

Exemples. 1. On suppose que x, y, z, t sont des variables deux à deux distinctes et que $\chi(t) = 1$. Alors :

$$\begin{aligned}
 & \Phi(\lambda x. \lambda y. \mu(\lambda z. \mu(z, t), \mu(x, y))) \\
 &= \Phi^0(\lambda x. \lambda y. \mu(\lambda z. \mu(z, t), \mu(x, y))) \\
 &= \lambda(\Phi^1(\sigma_x^1(\lambda y. \mu(\lambda z. \mu(z, t), \mu(x, y)))) \\
 &= \lambda(\Phi^1(\lambda y. \sigma_x^2(\mu(\lambda z. \mu(z, t), \mu(x, y)))) \\
 &= \lambda\lambda(\Phi^2(\sigma_y^1(\mu(\sigma_x^2(\lambda z. \mu(z, t), \sigma_x^2(\mu(x, y)))))) \\
 &= \lambda\lambda(\Phi^2(\mu(\sigma_y^1(\lambda z. \sigma_x^3(\mu(z, t), \sigma_y^1(\mu(\sigma_x^2(x), \sigma_x^2(y))))))) \\
 &= \lambda\lambda\mu(\Phi^2(\lambda z. \sigma_y^2(\mu(\sigma_x^3(z), \sigma_x^3(t))), \Phi^2(\mu(\sigma_y^1(2), \sigma_y^1(y)))) \\
 &= \lambda\lambda\mu(\lambda(\Phi^3(\sigma_z^1(\mu(\sigma_y^2(z), \sigma_y^2(t))))), \mu(\Phi^2(2), \Phi^2(1))) \\
 &= \lambda\lambda\mu(\lambda(\Phi^3(\mu(\sigma_z^1(z), \sigma_z^1(t))))), \mu(p * q, p)) \\
 &= \lambda\lambda\mu(\lambda\mu(\Phi^3(1), \Phi^3(t)), \mu(p * q, p)) \\
 &= \lambda\lambda\mu(\lambda\mu(p, p * q^3), \mu(p * q, p)).
 \end{aligned}$$

2. Si $x \neq y$ et en allant plus vite :

$$\Phi(\lambda x. \lambda y. \mu(\lambda x. y, x)) = \lambda\lambda\mu(\lambda(p * q), p * q).$$

B.3.2 Définition du déliement sur les λ -contextes

On va étendre les définitions précédentes aux λ -contextes. Ainsi, on va définir :

- Pour tous $x \in V$, $n \in \mathbb{N}^*$, $C \in \mathcal{C}(\bar{\Lambda})$, une application $\sigma_x^n(C) : \bar{\Lambda}_{\mathbb{N}^*} \longrightarrow \bar{\Lambda}_{\mathbb{N}^*}$ vérifiant, pour tout $f \in \bar{\Lambda}_{\mathbb{N}^*}$, $\sigma_x^n(C[f]) = \sigma_x^n(C)(f)$.
- Pour tous $n \in \mathbb{N}^*$ et $C \in \mathcal{C}(\bar{\Lambda})$, une application $\Phi^n(C) : \bar{\Lambda}_{\mathbb{N}^*} \longrightarrow K$ vérifiant, pour tout $f \in \bar{\Lambda}_{\mathbb{N}^*}$, $\Phi^n(C[f]) = \Phi^n(C)(f)$.

On fixe $x \in V$, $n \in \mathbb{N}^*$ et $C \in \mathcal{C}(\bar{\Lambda})$. On définit $\sigma_x^n(C)$ par récurrence sur le degré de C :

1. si $C = \square$, alors $\sigma_x^n(C) = \sigma_x^n$;
2. si $C = \mu(D, f)$, alors $\sigma_x^n(C) = \mu(\sigma_x^n(D), \sigma_x^n(f))$;
3. si $C = \mu(f, D)$, alors $\sigma_x^n(C) = \mu(\sigma_x^n(f), \sigma_x^n(D))$;
4. si $C = \lambda x. D$, alors $\sigma_x^n(C) = C$;
5. si $C = \lambda y. D$ avec $y \neq x$, alors $\sigma_x^n(C) = \lambda y. (\sigma_x^{n+1}(D))$.

L'action de $\sigma_x^n(C)$ sur un λ -terme formel f est définie par récurrence sur le degré de C de manière similaire. Par exemple, si $C = \mu(D, g)$, on pose :

$$\sigma_x^n(C)(f) = \mu(\sigma_x^n(D)(f), \sigma_x^n(g)).$$

Pour des besoins techniques, on définit, à partir de σ_x^n , une application τ_x^n de $\mathcal{C}(\bar{\Lambda})$ vers lui-même. En fait, on ne modifie la définition de σ_x^n que pour \square , en posant : $\tau_x^n(\square) = \square$.

Exemple. On a :

$$\tau_x^n(\lambda y. \mu(x, \square)) = \lambda y. (\mu(n+1, \square))$$

alors que :

$$\sigma_x^n(\lambda y. \mu(x, \square)) = \lambda y. (\mu(n+1, \sigma_x^{n+1})).$$

Pour tout λ -contexte C , $\tau_x^n(C)$ est un λ -contexte vérifiant les égalités :

$$|\tau_x^n(C)| = |C|, \quad |\tau_x^n(C)|_\lambda = |C|_\lambda, \quad \mathcal{L}(\tau_x^n(C)) = \mathcal{L}(C).$$

De plus, les applications σ et τ sont reliées par le résultat suivant :

Lemme B.20. Soient $n \in \mathbb{N}^*$, $x \in V$ et $C \in \mathcal{C}(\bar{\Lambda})$. Alors :

$$\sigma_x^n(C) = \begin{cases} \tau_x^n(C) & \text{si } x \in \mathcal{L}(C) \\ \tau_x^n(C) \circ \sigma_x^{n+k} & \text{si } x \notin \mathcal{L}(C) \text{ et si } |C|_\lambda = k. \end{cases}$$

Si n est un entier et C un contexte, on définit $\Phi^n(C)$ ainsi :

1. si $C = \square$, alors $\Phi^n(C) = \Phi^n$;
2. si $C = \mu(D, f)$, alors $\Phi^n(C) = \mu(\Phi^n(D), \Phi^n(f))$;
3. si $C = \mu(f, D)$, alors $\Phi^n(C) = \mu(\Phi^n(f), \Phi^n(D))$;
4. si $C = \lambda x. D$, alors $\Phi^n(C) = \lambda(\Phi^{n+1}(\sigma_x^1(D)))$.

On va maintenant vérifier que l'on a bien ce que l'on voulait.

Proposition B.21. Soient $n \in \mathbb{N}^*$, $C \in \mathcal{C}(\bar{\Lambda})$ et $f \in \bar{\Lambda}$. Alors :

1. Pour tout $x \in V$, on a $\sigma_x^n(C[f]) = \sigma_x^n(C)(f)$;
2. On a $\Phi^n(C[f]) = \Phi^n(C)(f)$.

Démonstration. Dans les deux cas, on va procéder par récurrence sur le degré du λ -contexte.

1. Soient $n \in \mathbb{N}^*$, $x \in V$ et $f \in \bar{\Lambda}$. Alors :

$$\begin{aligned} \sigma_x^n(\square[f]) &= \sigma_x^n(f) \\ &= \sigma_x^n(\square)(f). \end{aligned}$$

Maintenant, supposons que l'on a démontré le résultat pour tout contexte de degré $k \in \mathbb{N}$ fixé. Soit C un contexte de degré $k+1$. Alors, on a quatre cas possibles.

- Si $C = \mu(D, g)$ avec $|D| = k$, alors :

$$\begin{aligned}
 \sigma_x^n(C[f]) &= \sigma_x^n(\mu(D[f], g)) \\
 &= \mu(\sigma_x^n(D[f]), \sigma_x^n(g)) \\
 &= \mu(\sigma_x^n(D)(f), \sigma_x^n(g)) \\
 &= \mu(\sigma_x^n(D), \sigma_x^n(g))(f) \\
 &= \sigma_x^n(\mu(D, g))(f) \\
 &= \sigma_x^n(C)(f).
 \end{aligned}$$

- Si $C = \mu(g, D)$ avec $|D| = k$, on procède de même.
- Si $C = \lambda x.D$ avec $|D| = k$, alors :

$$\begin{aligned}
 \sigma_x^n(C[f]) &= \sigma_x^n(\lambda x.D[f]) \\
 &= \lambda x.D[f] \\
 &= (\lambda x.D)(f) \\
 &= \sigma_x^n(\lambda x.D)(f) \\
 &= \sigma_x^n(C)(f).
 \end{aligned}$$

- Si $C = \lambda y.D$ avec $|D| = k$ et $y \neq x$, alors :

$$\begin{aligned}
 \sigma_x^n(C[f]) &= \sigma_x^n(\lambda y.D[f]) \\
 &= \lambda y.(\sigma_x^{n+1}(D[f])) \\
 &= \lambda y.(\sigma_x^{n+1}(D)(f)) \\
 &= \lambda y.(\sigma_x^{n+1}(D))(f) \\
 &= \sigma_x^n(\lambda y.D)(f) \\
 &= \sigma_x^n(C)(f).
 \end{aligned}$$

Dans tous les cas, on a bien $\sigma_x^n(C[f]) = \sigma_x^n(C)(f)$.

2. On procède exactement comme pour σ . En distinguant les cas $C = \square$, pour initier la récurrence, puis $C = \mu(D, g)$, $C = \mu(g, D)$ et $C = \lambda x.D$. Les trois premiers cas se traitent aisément. Pour le cas $C = \lambda x.D$, on a :

$$\begin{aligned}
 \Phi^n(C[f]) &= \Phi^n(\lambda x.D[f]) \\
 &= \lambda x.(\Phi^{n+1}(\sigma_x^1(D[f]))) \\
 &= \lambda x.(\Phi^{n+1}(\sigma_x^1(D)(f))) && \text{d'après le 1} \\
 &= \lambda x.(\Phi^{n+1}(\sigma_x^1(D))(f)) && \text{(HR)} \\
 &= (\lambda x.(\Phi^{n+1}(\sigma_x^1(D))))(f) \\
 &= \Phi^n(\lambda x.D)(f) \\
 &= \Phi^n(C)(f).
 \end{aligned}$$

◇

B.4 Le système de réécriture \mathbb{K} ne simule pas complètement le λ -calcul

On montre ici que (\mathbb{K}, Φ) est une simulation de $(\Lambda, \rightarrow_\beta)$, mais que \mathbb{K} ne termine pas en certains termes de la forme $\Phi(f)$ où f est un λ -terme sur lequel β termine.

B.4.1 Le déliement est compatible avec l' α -conversion

On va donc démontrer, dans ce paragraphe, que si f et g sont deux λ -termes formels qui sont dans la même classe d' α -équivalence, alors $\Phi(f) = \Phi(g)$. Or, deux termes f et g sont α -équivalents si et seulement si on peut trouver une famille finie de λ -termes formels f_1, \dots, f_k tels que :

$$f \rightarrow_\alpha f_1 \leftarrow_\alpha f_2 \rightarrow_\alpha \dots \rightarrow_\alpha f_k \leftarrow_\alpha g.$$

Ainsi, pour montrer le résultat annoncé, il suffit de démontrer la proposition suivante.

Proposition B.22. *Soient f et g deux λ -termes formels tels que $f \rightarrow_\alpha g$, alors $\Phi(f) = \Phi(g)$.*

On va démontrer la proposition en plusieurs temps.

Lemme B.23. *Pour tous $m \in \mathbb{N}$, $n \in \mathbb{N}^*$, $x, y \in V$ et $f \in \bar{\Lambda}_{\mathbb{N}^*}$ tels que $y \notin \mathcal{V}(f)$, on a :*

$$\Phi^m(\sigma_x^n(f)) = \Phi^m(\sigma_y^n(f[x := y])).$$

Démonstration. On suppose que $y \neq x$, le cas d'égalité étant trivial. On procède encore par récurrence sur le degré de f . Tout d'abord, supposons que $|f| = 0$. Alors deux cas sont possibles.

- Si $f = x$, alors $\sigma_x^n(f) = n$ et $\sigma_y^n(f[x := y]) = \sigma_y^n(y) = n$.
- Si $f \neq x$, alors $\sigma_x^n(f) = f$ et $\sigma_y^n(f[x := y]) = \sigma_y^n(f) = f$; en effet, on a forcément $f \neq y$ puisqu'on a supposé que $y \notin \mathcal{V}(f)$.

Supposons maintenant que l'on a démontré le résultat pour tous les λ -termes formels de degré au plus k , où k est un entier fixé. Soit f un terme de degré $k + 1$. On a quatre cas possibles.

- Si $f = \mu(g, h)$ avec g et h deux λ -termes formels de degré au plus k , l'un des deux étant de degré k . Remarquons tout d'abord que $\mathcal{V}(f) = \mathcal{V}(g) \cup \mathcal{V}(h)$ et donc que $y \notin \mathcal{V}(g)$ et $y \notin \mathcal{V}(h)$. On a donc :

$$\begin{aligned}
 \Phi^m(\sigma_x^n(f)) &= \Phi^m(\sigma_x^n(\mu(g, h))) \\
 &= \mu(\Phi^m(\sigma_x^n(g)), \Phi^m(\sigma_x^n(h))) \\
 &= \mu(\Phi^m(\sigma_y^n(g[x := y])), \Phi^m(\sigma_y^n(h[x := y]))) \quad (\text{HR}) \\
 &= \Phi^m(\sigma_y^n(\mu(g[x := y], h[x := y]))) \\
 &= \Phi^m(\sigma_y^n((\mu(g, h))[x := y])) \\
 &= \Phi^m(\sigma_y^n(f[x := y])).
 \end{aligned}$$

- Si $f = \lambda x.g$ avec g un λ -terme formel de degré k . On a $\mathcal{V}(f) = \mathcal{V}(g) \setminus \{x\}$, d'où $y \notin \mathcal{V}(g)$ (on a supposé $y \neq x$). Alors :

$$\begin{aligned}
 \Phi^m(\sigma_x^n(f)) &= \Phi^m(\sigma_x^n(\lambda x.g)) \\
 &= \Phi^m(\lambda x.g).
 \end{aligned}$$

D'autre part :

$$\begin{aligned}
 \Phi^m(\sigma_y^n(f[x := y])) &= \Phi^m(\sigma_y^n((\lambda x.g)[x := y])) \\
 &= \Phi^m(\sigma_y^n(\lambda x.g)) \\
 &= \Phi^m(\lambda x.(\sigma_y^{n+1}(g))) \\
 &= \Phi^m(\lambda x.g) \quad \text{car } y \notin \mathcal{V}(g).
 \end{aligned}$$

- Si $f = \lambda y.g$ avec $|g| = k$. Alors :

$$\begin{aligned}
 \Phi^m(\sigma_x^n(f)) &= \Phi^m(\sigma_x^n(\lambda y.g)) \\
 &= \Phi^m(\lambda y.(\sigma_x^{n+1}(g))) \quad \text{puisque } y \neq x \\
 &= \lambda(\Phi^{m+1}(\sigma_y^1(\sigma_x^{n+1}(g))))
 \end{aligned}$$

D'autre part,

$$\begin{aligned}
 \Phi^m(\sigma_y^n(f[x := y])) &= \Phi^m(\sigma_y^n((\lambda y.g)[x := y])) \\
 &= \Phi^m(\sigma_y^n((\lambda \nu.(g[y := \nu][x := y])))) \quad \text{en posant } \nu = \nu(g, y) \\
 &= \Phi^m(\lambda \nu.(\sigma_y^{n+1}(g[y := \nu][x := y]))) \quad \text{puisque } \nu \neq y \\
 &= \Phi^m(\lambda \nu.(\sigma_x^{n+1}(g[y := \nu]))) \quad (\text{HR}) \\
 &= \lambda(\Phi^{m+1}(\sigma_\nu^1(\sigma_x^{n+1}(g[y := \nu])))) \\
 &= \lambda(\Phi^{m+1}(\sigma_\nu^1((\sigma_x^{n+1}(g))[y := \nu]))) \\
 &= \lambda(\Phi^{m+1}(\sigma_y^1(\sigma_x^{n+1}(g)))) \quad (\text{HR}).
 \end{aligned}$$

- Si $f = \lambda z.g$ avec $|g| = k$ et $z \notin \{x, y\}$. Alors :

$$\begin{aligned}
 \Phi^m(\sigma_x^n(f)) &= \Phi^m(\sigma_x^n(\lambda z.g)) \\
 &= \Phi^m(\lambda z.(\sigma_x^{n+1}(g))) && \text{puisque } z \neq x \\
 &= \Phi^m(\lambda z.(\sigma_y^{n+1}(g[x := y]))) && \text{(HR)} \\
 &= \Phi^m(\sigma_y^n(\lambda z.(g[x := y]))) && \text{puisque } z \neq x \\
 &= \Phi^m(\sigma_y^n((\lambda z.g)[x := y])) && \text{puisque } z \neq x \\
 &= \Phi^m(\sigma_y^n(f[x := y])).
 \end{aligned}$$

◇

Remarque. La présence de Φ^m n'est utile que pour l'avant-dernier cas, celui où $f = \lambda y.g$. Sans application de Φ^m , c'est faux. Par exemple, si $g = y$, on a $\sigma_x^n(\lambda y.y) = \lambda y.y$ mais, comme $(\lambda y.y)[x := y] = \lambda \nu.\nu$, avec $\nu = \nu(y, y)$ (et donc $\nu \neq y$), on a $\sigma_y^n(\lambda \nu.\nu) = \lambda \nu.\nu$.

Corollaire B.24. Pour tous $n \in \mathbb{N}$, $x, y \in V$ et $f \in \bar{\Lambda}_{\mathbb{N}^*}$ tels que $y \notin \mathcal{V}(f)$, on a :

$$\Phi^n(\lambda x.f) = \Phi^n(\lambda y.(f[x := y])).$$

Démonstration. On a :

$$\begin{aligned}
 \Phi^n(\lambda x.f) &= \lambda(\Phi^{n+1}(\sigma_x^1(f))) \\
 &= \lambda(\Phi^{n+1}(\sigma_y^1(f[x := y]))) && \text{d'après le résultat précédent} \\
 &= \Phi^n(\lambda y.(f[x := y])).
 \end{aligned}$$

◇

Lemme B.25. Soient $C \in \mathcal{C}(\bar{\Lambda}_{\mathbb{N}^*})$, $n \in \mathbb{N}$, $x, y \in V$ et $f \in \bar{\Lambda}_{\mathbb{N}^*}$ tels que $y \notin \mathcal{V}(f)$. Alors :

$$\Phi^n(C)(\lambda x.f) = \Phi^n(C)(\lambda y.(f[x := y])).$$

Démonstration. On va procéder par récurrence sur le degré de C et toujours dans le cas où $y \neq x$. Pour $C = \square$, c'est le résultat précédent. Maintenant, supposons que la proposition est vraie pour tout contexte de degré k et que $|C| = k+1$. Trois cas sont possibles. Les deux premiers cas, $C = \mu(D, g)$ et $C = \mu(g, D)$, se traitent sans difficulté. Le troisième cas est $C = \lambda z.D$:

$$\begin{aligned}
 \Phi^n(C)(\lambda x.f) &= \Phi^n(\lambda z.D)(\lambda x.f) \\
 &= \Phi^n(\lambda z.D[\lambda x.f]) \\
 &= \lambda(\Phi^n(\sigma_z^1(D[\lambda x.f])))
 \end{aligned}$$

On doit distinguer deux sous-cas, selon que $z \in \mathcal{L}(D)$ ou non. Si $z \in \mathcal{L}(D)$:

$$\begin{aligned}
 \Phi^n(C)(\lambda x.f) &= \lambda(\Phi^{n+1}(\tau_z^1(D)(\lambda x.f))) \\
 &= \lambda(\Phi^{n+1}(\tau_z^1(D))(\lambda x.f)) \\
 &= \lambda(\Phi^{n+1}(\tau_z^1(D))(\lambda y.(f[x := y]))) & \text{(HR)} \\
 &= \lambda(\Phi^{n+1}(\sigma_z^1(D[\lambda y.(f[x := y])])) \\
 &= \Phi^n(\lambda z.D[\lambda y.(f[x := y])]) \\
 &= \Phi^n(C)(\lambda y.(f[x := y])).
 \end{aligned}$$

Si $z \notin \mathcal{L}(D)$, on pose $l = |D|_\lambda$. Alors : $\Phi^n(C)(\lambda x.f) = \lambda(\Phi^{n+1}(\tau_z^1(D)(\sigma_z^{l+1}(\lambda x.f))))$.
Maintenant, si $z = x$:

$$\begin{aligned}
 \Phi^n(C)(\lambda x.f) &= \lambda(\Phi^{n+1}(\tau_x^1(D)(\lambda x.f))) \\
 &= \lambda(\Phi^{n+1}(\tau_x^1(D))(\lambda y.(f[x := y]))) & \text{(HR)} \\
 &= \lambda(\Phi^{n+1}(\tau_x^1(D))(\sigma_x^{l+1}(\lambda y.(f[x := y])))) & \text{puisque } x \notin \mathcal{V}(\lambda y.(f[x := y])) \\
 &= \lambda(\Phi^{n+1}(\sigma_x^1(D[\lambda y.(f[x := y])])) \\
 &= \Phi^n(C)(\lambda y.(f[x := y])).
 \end{aligned}$$

Si $z \notin \{x, y\}$:

$$\begin{aligned}
 \Phi^n(C)(\lambda x.f) &= \lambda(\Phi^{n+1}(\tau_z^1(D)(\lambda x.\sigma_z^{l+2}(f)))) \\
 &= \lambda(\Phi^{n+1}(\tau_z^1(D))(\lambda y.(\sigma_z^{l+2}(f))[x := y]))) \\
 &= \lambda(\Phi^{n+1}(\tau_z^1(D))(\sigma_z^{l+1}(\lambda y.f[x := y]))) & \text{puisque } z \notin \{x, y\} \\
 &= \lambda(\Phi^{n+1}(\sigma_z^1(D[\lambda y.f[x := y])])) \\
 &= \Phi^n(C)(\lambda y.f[x := y])).
 \end{aligned}$$

Enfin, si $z = y$; on choisit $t \in V$ tel que $t \notin \mathcal{V}(D[f]) \cup \{x, y\}$ et on se ramène au cas précédent :

$$\begin{aligned}
 &\Phi^n(C)(\lambda x.f) \\
 &= \Phi^n(\lambda y.D[\lambda x.f]) \\
 &= \Phi^n(\lambda t.(D[\lambda x.f])[y := t]) \\
 &= \Phi^n(\lambda t.(D[y := t])(\lambda x.f[y := t])) & \text{puisque } y \notin \mathcal{L}(D) \\
 &= \Phi^n(\lambda t.(D[y := t])(\lambda x.f)) & \text{puisque } y \notin \mathcal{V}(f) \\
 &= \Phi^n(\lambda t.(D[y := t])(\lambda y.(f[x := y]))) & \text{en appliquant ce qui précède} \\
 &= \Phi^n(\lambda t.(D[y := t])(\lambda y.(f[x := y])[y := t])) & \text{puisque } y \notin \mathcal{V}(\lambda y.(f[x := y])) \\
 &= \Phi^n(\lambda y.(D)(\lambda y.(f[x := y]))) \\
 &= \Phi^n(C)(\lambda y.(f[x := y])).
 \end{aligned}$$

◇

On a donc démontré la proposition annoncée, d'où le théorème :

Théorème B.26. *L'application Φ induit une application $\Phi : \Lambda \longrightarrow T$, c'est-à-dire que pour tous λ -termes formels f et g tels que $f \equiv_\alpha g$, on a $\Phi(f) = \Phi(g)$.*

B.4.2 Le déliement préserve les étapes de β -réduction

On va montrer le résultat suivant :

Théorème B.27. *Soient f et g deux λ -termes. Si $f \rightarrow_\beta g$, alors $\Phi(f) \rightarrow_{KB} \Phi(g)$.*

On va commencer par poser quelques notations, permises par le theoreme B.26. Tout d'abord, on définit une variante de Φ , $\Psi : \mathcal{C}(\Lambda) \longrightarrow \mathcal{C}(T)$. On procède comme pour Φ , mis à part $\Psi(\square) = \square$.

Pour alléger les calculs ultérieurs, on va poser, si $n \in \mathbb{N}^*$ et si x_1, \dots, x_n sont des variables deux à deux distinctes :

$$\Phi_{x_1, \dots, x_n} = \Phi^n \circ \sigma_{x_1}^1 \circ \dots \circ \sigma_{x_n}^n.$$

En particulier, on a, pour $x \in V$:

$$\Phi_{x_1, \dots, x_n}(x) = \begin{cases} p & \text{si } x = x_1 \\ p * q^{i-1} & \text{si } x = x_i, i \geq 2 \\ p * q^{\chi(x)+n-1} & \text{sinon.} \end{cases}$$

Le théorème B.26 nous assure que, pour un λ -terme f fixé : pour tout λ -contexte C , on peut supposer que $\#\mathcal{L}(C) = |C|_\lambda$ pour calculer $\Phi(C[f])$. En effet, si ce n'est pas le cas, il existe une variable x et trois λ -contextes D , E et F tels que :

$$C = D \circ (\lambda x. \square) \circ E \circ (\lambda x. \square) \circ F.$$

Or, si on choisit une variable y qui n'est ni dans $\mathcal{V}(C)$, ni dans $\mathcal{L}(C)$, ni dans $\mathcal{V}(f)$ on a :

$$\Phi(C[f]) = \Phi(D \circ (\lambda y. \square) \circ (E[x := y]) \circ (\lambda x. \square) \circ F[f]).$$

De plus, $\mathcal{L}(C)$ est totalement ordonnable avec "l'ordre dans lequel on rencontre les λx en partant de \square "; sans rentrer dans les détails, dans le cas précédent, on aura $x < y$. Tout ceci permet d'obtenir le résultat suivant :

Proposition B.28. *Soient C un λ -contexte et f un λ -terme. On suppose que $\mathcal{L}(C)$ est l'ensemble totalement ordonné $\{x_1 < \dots < x_n\}$ avec $n = |C|_\lambda$. Alors :*

$$\Phi(C[f]) = \Psi(C)[\Phi_{x_1, \dots, x_n}(f)].$$

Enfin, on va utiliser les notations suivantes dans T . On pose $q^1 = q$ et $q^{n+1} = q * q^n$. On définit le contexte $Q = q * \square$, avec Q^n l'itéré n fois de Q ; en particulier, $Q^n[i] \rightarrow_J q^n$, $Q^{n-1}[q] = q^n$ et $Q^n[\gamma(a, b)] \rightarrow_Q Q^{n-1}[b]$ pour tout $n \in \mathbb{N}^*$. Enfin, on définit le contexte $\Delta \in \mathcal{C}(K)$ comme $\Delta = \gamma(p, \square * q)$. Enfin, si C est un contexte, on note $C^0 = \square$, $C^1 = C$ et $C^{n+1} = C^n \circ C = C \circ C^n$.

Lemme B.29. *Soient n et m deux entiers naturels et $a \in K$. Alors :*

$$p * Q^n[\Delta^m[a]] \rightarrow_K \begin{cases} p & \text{si } m > n = 0 \\ p * q^n & \text{si } m > n \geq 1 \\ p * Q^n[a] & \text{si } m = 0 \\ p * Q^{n-m}[a * q^m] & \text{si } n \geq m \geq 1. \end{cases}$$

Démonstration. Par récurrence sur m . Si $m = 0$, c'est évident. Supposons que la propriété est vraie pour un m fixé. Alors :

$$p * Q^n[\Delta^{m+1}[a]] = p * Q^n[\Delta^m[\Delta[a]]] \rightarrow_K \begin{cases} p & \text{si } m > n = 0 \\ p * q^n & \text{si } m > n \geq 1. \\ p * Q^n[\Delta[a]] & \text{si } m = 0 \\ p * Q^{n-m}[\Delta[a] * q^m] & \text{si } n \geq m \geq 1. \end{cases}$$

Dans le cas $m = 0$, on a deux possibilités. Si $n = 0$:

$$p * \Delta[a] = p * \gamma(p, a * q) \rightarrow_P p.$$

Si $n \geq 1$:

$$p * Q^n[\Delta[a]] = p * Q^{n-1}[q * \gamma(p, a * q)] \rightarrow_Q p * Q^{n-1}[a * q].$$

Maintenant, si $n = m \geq 1$:

$$\begin{aligned} p * (\Delta[a] * q^n) &= p * (\gamma(p, a * q) * q^n) \\ &\rightarrow_D p * \gamma(p * q^n, (a * q) * q^n) \\ &\rightarrow_P p * q^n. \end{aligned}$$

Enfin, si $n > m \geq 1$:

$$\begin{aligned} p * Q^{n-m}[\Delta[a] * q^m] &= p * Q^{n-(m+1)}[q * (\Delta[a] * q^m)] \\ &\rightarrow_D p * Q^{n-(m+1)}[q * \gamma(p * q^m, (a * q) * q^m)] \\ &\rightarrow_Q p * Q^{n-(m+1)}[(a * q) * q^m] \\ &\rightarrow_A p * Q^{n-(m+1)}[a * q^{m+1}]. \end{aligned}$$

◇

Corollaire B.30. *Soient i, j, m des entiers naturels. Alors :*

$$p * Q^j[\Delta^i[q^m]] \rightarrow_K \begin{cases} p & \text{si } i > j = 0 \\ p * q^j & \text{si } i > j \geq 1 \\ p * q^{m+j} & \text{si } j \geq i. \end{cases}$$

Proposition B.31. *Soient $m, n \in \mathbb{N}^*$, $i \in \{0, \dots, n\}$, $x_1, \dots, x_n, y_1, \dots, y_m$ des variables deux à deux distinctes et $f \in \Lambda$, avec $y_1, \dots, y_m \notin \mathcal{V}(f)$. Alors :*

$$\Phi_{x_1, \dots, x_n}(f) * \Delta^i[q^m] \rightarrow_K \Phi_{x_1, \dots, x_i, y_1, \dots, y_m, x_{i+1}, \dots, x_n}(f).$$

Démonstration. Par récurrence sur le degré de f .

- Si $f = x_1$:

$$\Phi_{x_1, \dots, x_n}(x_1) * \Delta^i[q^m] = p * \Delta^i[q^m] \rightarrow_K \begin{cases} p * q^m & \text{si } i = 0 \\ p & \text{si } i \geq 1. \end{cases}$$

D'autre part :

$$\Phi_{x_1, \dots, x_i, y_1, \dots, y_m, x_{i+1}, \dots, x_n}(x_1) = \begin{cases} p * q^m & \text{si } i = 0 \\ p & \text{si } i \geq 1. \end{cases}$$

- Si $f = x_j$, $j \in \{2, \dots, n\}$:

$$\begin{aligned} \Phi_{x_1, \dots, x_n}(x_j) * \Delta^i[q^m] &= (p * q^{j-1}) * \Delta^i[q^m] \\ &\rightarrow_A p * Q^{j-1}[\Delta^i[q^m]] \\ &\rightarrow_K \begin{cases} p * q^{j-1} & \text{si } i \geq j \\ p * q^{m+j-1} & \text{si } j > i. \end{cases} \end{aligned}$$

D'autre part :

$$\Phi_{x_1, \dots, x_i, y_1, \dots, y_m, x_{i+1}, \dots, x_n}(x_j) = \begin{cases} p * q^{j-1} & \text{si } j \leq i \\ p * q^{m+j-1} & \text{si } j > i. \end{cases}$$

- Si $f = x \in V \setminus \{x_1, \dots, x_n, y_1, \dots, y_m\}$:

$$\begin{aligned} \Phi_{x_1, \dots, x_n}(x) * \Delta^i[q^m] &= (p * q^{\chi(x)+n-1}) * \Delta^i[q^m] \\ &\rightarrow_A p * Q^{\chi(x)+n-1}[\Delta^i[q^m]] \\ &\rightarrow_K p * q^{\chi(x)+n+m-1} \\ &= \Phi_{x_1, \dots, x_i, y_1, \dots, y_m, x_{i+1}, \dots, x_n}(x). \end{aligned}$$

- Si $f = \mu(g, h)$:

$$\begin{aligned}
 & \Phi_{x_1, \dots, x_n}(f) * \Delta^i[q^m] \\
 &= \Phi_{x_1, \dots, x_n}(\mu(g, h)) * \Delta^i[q^m] \\
 &= \mu(\Phi_{x_1, \dots, x_n}(g), \Phi_{x_1, \dots, x_n}(h)) * \Delta^i[q^m] \\
 &\rightarrow_M \mu(\Phi_{x_1, \dots, x_n}(g) * \Delta^i[q^m], \Phi_{x_1, \dots, x_n}(h) * \Delta^i[q^m]) \\
 &\rightarrow_K \mu(\Phi_{x_1, \dots, x_i, y_1, \dots, y_m, x_{i+1}, \dots, x_n}(g), \Phi_{x_1, \dots, x_i, y_1, \dots, y_m, x_{i+1}, \dots, x_n}(h)) \\
 &= \Phi_{x_1, \dots, x_i, y_1, \dots, y_m, x_{i+1}, \dots, x_n}(\mu(g, h)) \\
 &= \Phi_{x_1, \dots, x_i, y_1, \dots, y_m, x_{i+1}, \dots, x_n}(f)
 \end{aligned} \tag{HR}$$

- Si $f = \lambda z.g$, où on suppose $z \notin \{x_1, \dots, x_n, y\}$:

$$\begin{aligned}
 & \Phi_{x_1, \dots, x_n}(f) * \Delta^i[q^m] \\
 &= \Phi_{x_1, \dots, x_n}(\lambda z.g) * \Delta^i[q^m] \\
 &= \lambda(\Phi_{z, x_1, \dots, x_n}(g)) * \Delta^i[q^m] \\
 &\rightarrow_L \lambda(\Phi_{z, x_1, \dots, x_n}(g) * \Delta^{i+1}[q^m]) \\
 &\rightarrow_K \lambda(\Phi_{z, x_1, \dots, x_i, y_1, \dots, y_m, x_{i+1}, \dots, x_n}(g)) \\
 &= \Phi_{x_1, \dots, x_i, y_1, \dots, y_m, x_{i+1}, \dots, x_n}(\lambda z.g) \\
 &= \Phi_{x_1, \dots, x_i, y_1, \dots, y_m, x_{i+1}, \dots, x_n}(f).
 \end{aligned} \tag{HR}$$

◇

On démontre de la même façon :

Proposition B.32. Soient $m \in \mathbb{N}^*$, $y_1, \dots, y_m \in V$ et $f \in \Lambda$ avec $y_1, \dots, y_m \notin \mathcal{V}(f)$. Alors :

$$\Phi(f) * q^m \rightarrow_K \Phi_{y_1, \dots, y_m}(f).$$

Proposition B.33. Soient $n \in \mathbb{N}^*$, $i \in \{1, \dots, n\}$, x_1, \dots, x_n des variables deux à deux distinctes et $f, g \in \Lambda$, avec $x_1, \dots, x_{i-1} \notin \mathcal{V}(g)$. Alors :

$$\Phi_{x_1, \dots, x_n}(f) * \Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)] \rightarrow_K \Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(f[x_i := g]).$$

Démonstration. Par récurrence sur le degré de f .

- Si $f = x_1$:

$$\begin{aligned}
 & \Phi_{x_1, \dots, x_n}(x_1) * \Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)] \\
 &= p * \Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)] \\
 &\rightarrow_K \begin{cases} p * \gamma(\Phi_{x_2, \dots, x_n}(g), i) \rightarrow_P \Phi_{x_2, \dots, x_n}(g) & \text{si } i = 1 \\ p & \text{si } i \geq 2. \end{cases}
 \end{aligned}$$

D'autre part :

$$\Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(x_1[x_i := g]) = \begin{cases} \Phi_{x_2, \dots, x_n}(g) & \text{si } i = 1 \\ \Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(x_1) = p & \text{si } i \geq 2. \end{cases}$$

- Si $f = x_j$, $j \in \{2, \dots, n\}$:

$$\begin{aligned} & \Phi_{x_1, \dots, x_n}(x_j) * \Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)] \\ &= (p * q^{j-1}) * \Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)] \\ &\rightarrow_A p * Q^{j-1}[\Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)]] \\ &\rightarrow_K \begin{cases} p * Q[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)] \rightarrow_Q p * i \rightarrow_J p & \text{si } j = 2 \text{ et } i = 1 \\ p * Q^{j-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)] \rightarrow_Q p * Q^{j-2}[i] \rightarrow_J p * q^{j-2} & \text{si } i = 1 \text{ et } j > 2 \\ p * q^{j-1} & \text{si } i > j \\ p * (\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i) * q^{i-1}) \rightarrow_K \Phi_{x_{i+1}, \dots, x_n}(g) * q^{i-1} & \text{si } i = j \\ p * Q^{j-i}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i) * q^{i-1}] \rightarrow_K p * q^{j-2} & \text{si } j \geq i \geq 2. \end{cases} \end{aligned}$$

D'autre part :

$$\begin{aligned} & \Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(x_j[x_i := g]) \\ &= \begin{cases} \Phi_{x_2, \dots, x_n}(x_2) = p & \text{si } i = 1 \text{ et } j = 2 \\ \Phi_{x_2, \dots, x_n}(x_j) = p * q^{j-2} & \text{si } i = 1 \text{ et } j > 2 \\ \Phi_{x_1, \dots, x_j, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(x_j) = p * q^{j-1} & \text{si } i > j \\ \Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(g) & \text{si } i = j \\ \Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_j, \dots, x_n}(x_j) = p * q^{j-2} & \text{si } j \geq i \geq 2. \end{cases} \end{aligned}$$

Il reste à voir que, si $i \geq 2$:

$$\Phi_{x_{i+1}, \dots, x_n}(g) * q^{i-1} \rightarrow_K \Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(g).$$

Ce qui découle la proposition précédente.

- Si $f = x \in V \setminus \{x_1, \dots, x_n\}$:

$$\begin{aligned} \Phi_{x_1, \dots, x_n}(x) * \Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)] &= (p * q^{\chi(x)+n-1}) * \Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)] \\ &\rightarrow_A p * Q^{\chi(x)+n-1}[\Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)]] \\ &\rightarrow_K p * Q^{\chi(x)+n-i}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i) * q^{i-1}] \\ &\rightarrow_K p * q^{\chi(x)+n-2} \\ &= \Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(x) \\ &= \Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(x[x_i := g]). \end{aligned}$$

- Si $f = \mu(h, k)$:

$$\begin{aligned}
 & \Phi_{x_1, \dots, x_n}(\mu(h, k)) * \Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)] \\
 &= \mu(\Phi_{x_1, \dots, x_n}(h), \Phi_{x_1, \dots, x_n}(k)) * \Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)] \\
 &\rightarrow_M \mu(\Phi_{x_1, \dots, x_n}(h) * \Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)], \Phi_{x_1, \dots, x_n}(k) * \Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)]) \\
 &\rightarrow_K \mu(\Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(h[x_i := g]), \Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(k[x_i := g])) \quad (\text{HR}) \\
 &= \Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(\mu(h[x_i := g], k[x_i := g])) \\
 &= \Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}((\mu(h, k)[x_i := g])) \\
 &= \Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(f[x_i := g]).
 \end{aligned}$$

- Si $f = \lambda y.h$ avec $y \notin \mathcal{V}(g) \cup \{x_1, \dots, x_n\}$:

$$\begin{aligned}
 & \Phi_{x_1, \dots, x_n}(\lambda y.h) * \Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)] \\
 &= \lambda(\Phi_{y, x_1, \dots, x_n}(h)) * \Delta^{i-1}[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)] \\
 &\rightarrow_L \lambda(\Phi_{y, x_1, \dots, x_n}(h) * \Delta^i[\gamma(\Phi_{x_{i+1}, \dots, x_n}(g), i)]) \\
 &\rightarrow_K \lambda(\Phi_{y, x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(h[x_i := g])) \quad (\text{HR}) \\
 &= \Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}(\lambda y.(h[x_i := g])) \\
 &= \Phi_{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n}((\lambda y.h)[x_i := g]) \quad \text{puisque } y \notin \mathcal{V}(g) \cup \{x_i\}.
 \end{aligned}$$

◇

Corollaire B.34. Soient n un entier, x, x_1, \dots, x_n des variables deux à deux distinctes et f et g deux λ -termes. Alors :

$$\Phi_{x, x_1, \dots, x_n}(f) * \gamma(\Phi_{x_1, \dots, x_n}(g), i) \rightarrow_K \Phi_{x, x_1, \dots, x_n}(f[x := g]).$$

Remarque. On démontre exactement de la même façon que, si x est une variable et f et g deux λ -termes, alors :

$$\Phi_x(f) * \gamma(\Phi(g), i) \rightarrow_K \Phi(f[x := g]).$$

On peut à présent démontrer le théorème B.27.

Démonstration du théorème B.27. Soient f et g deux λ -termes tels que $f \rightarrow_\beta g$. Alors, par définition de la β -réduction, il existe un λ -contexte C , deux λ -termes h et k et une variable x tels que :

$$f = C[\mu(\lambda x.h, k)] \text{ et } g = C[h[x := k]].$$

On note $\mathcal{L}(C) = \{x_1 < \dots < x_n\}$ (dans le cas $\mathcal{L}(C) = \emptyset$, c'est pareil). Alors :

$$\begin{aligned}
 \Phi(f) &= \Phi(C[\mu(\lambda x.h, k)]) \\
 &= \Psi(C)[\Phi_{x_1, \dots, x_n}(\mu(\lambda x.h, k))] \\
 &= \Psi(C)[\mu(\lambda(\Phi_{x_1, \dots, x_n}(h), \Phi_{x_1, \dots, x_n}(k)))] \\
 &\rightarrow_B \Psi(C)[\Phi_{x_1, \dots, x_n}(h) * \gamma(\Phi_{x_1, \dots, x_n}(k), i)] \\
 &\rightarrow_K \Psi(C)[\Phi_{x_1, \dots, x_n}(h[x := k])] && \text{d'après le corollaire précédent} \\
 &= \Phi(C[h[x := k]]) \\
 &= \Phi(g).
 \end{aligned}$$

◇

B.4.3 Le déliement préserve seulement la β -normalisation

On commence par montrer :

Proposition B.35. *Soit f un λ -terme possédant une β -forme normale. Alors $\Phi(f)$ possède une KB -forme normale.*

Démonstration. Notons $\beta(f)$ l'unique β -forme normale de f .

Alors $\Phi(\beta(f))$ ne contient que des opérateurs p , q , λ , et μ par construction de Φ . C'est donc une K -forme normale.

De plus, $\beta(f)$ ne contient pas de β -redex : $\Phi(\beta(f))$ ne peut donc pas contenir de B -redex, c'est donc aussi une B -forme normale et donc une KB -forme normale.

Comme $f \rightarrow_\beta \beta(f)$, on a bien $\Phi(f) \rightarrow_{KB} \Phi(\beta(f))$, ce qui prouve que $\Phi(\beta(f))$ est une KB -forme normale de $\Phi(f)$. ◇

Cependant, on a le résultat négatif suivant :

Proposition B.36. *Le déliement ne préserve pas la β -terminaison. Autrement dit, il existe un λ -terme f tel que β termine en f mais KB ne termine pas en $\Phi(f)$.*

Démonstration. Il suffit de traduire le contre-exemple de Melliès [Mel95] dans \mathbb{K} , ce qui donne :

$$m = \mu(\lambda\mu(\lambda p, \mu(\lambda p, p)), \mu(\lambda p, p)).$$

On vérifie alors que KB ne termine pas en m de la même façon que dans [Mel95]. ◇

En revanche, on a le résultat opérationnel suivant :

Proposition B.37. *La stratégie S définie par $a \rightarrow_S b$ si $a \rightarrow_B c$ et $b = K(c)$ termine en tout $\Phi(f)$ pour un λ -terme f possédant une β -forme normale.*

Démonstration. Supposons qu'il existe une suite infinie de S -réductions issue de $\Phi(f)$. Alors on peut l'écrire :

$$\Phi(f) \rightarrow_B a_1 \rightarrow_K K(a_1) \rightarrow_B a_2 \rightarrow_K K(a_2) \rightarrow_B \dots$$

Le B -redex réduit lors de $\Phi(f) \rightarrow_B a_1$ correspond à un β -redex de f . On en déduit que, si f_1 est le λ -terme obtenu à partir de f par contraction de ce β -redex, on a $K(a_1) = \Phi(f_1)$.

Par récurrence, on construit alors une suite infinie de β -réductions issue de f , ce qui contredit le fait que β termine en f .

◇

Bibliographie

- [ACCL91] Martín Abadi, Luca Cardelli, Pierre-Louis Curien, Jean-Jacques Lévy, *Explicit substitutions*. Journal of Functional Programming 1/4, pages 375-416, 1991.
- [AGL92] Martín Abadi, Georges Gonthier, Jean-Jacques Lévy, *Linear logic without boxes*. Logic in computer science, actes, pages 223-234, 1992.
- [Ada94] Colin Conrad Adams, *The knot book. An elementary introduction to the mathematical theory of knots*. W.H. Freeman and Company, 1994.
- [All89] Alphonse Allais, *Deux et deux font cinq* (1896). Œuvres anthumes, Robert Laffont, 1989.
- [AG00] Thomas Arts et Jürgen Giesl, *Termination of term rewriting using dependency pairs*. Trees in algebra and programming, actes, pages 133-178. Theoretical Computer Science 236/1-2, 2000.
- [AG98] Andrea Asperti et Stefano Guerrini, *The optimal implementation of functional programming languages*. Cambridge tracts in theoretical computer science, Cambridge University Press, 1998.
- [BN98] Franz Baader et Tobias Nipkow, *Term rewriting and all that*. Cambridge University Press, 1998.
- [BDH86] Leo Bachmair, Nachum Dershowitz et Jieh Hsiang, *Orderings for equational proofs*. Logic in computer science, actes, pages 346-357, 1986.
- [BD98a] John Carlos Baez et James Dolan, *Higher-dimensional algebra 3 : n-categories and the algebra of opetopes*. Advances in Mathematics 135/2, pages 145-206, 1998.
- [BD98b] John Carlos Baez et James Dolan, *Categorification*. Prépublication, arXiv math.QA/9802029, 1998. arxiv.org/abs/math.QA/9802029.
- [Bar84] Hendrik Pieter Barendregt, *The λ -calculus, its syntax and semantics*. North-Holland, 1984.

- [BBLR96] Zine-El-Abidine Benaïssa, Daniel Briaud, Pierre Lescanne et Jocelyne Rouyer-Degli, λ_v , *a calculus of explicit substitutions which preserves strong normalisation*. Journal of Functional Programming 6/5, pages 699-722, 1996.
- [BR95] Roel Bloo et Kristoffer Høgsbro Rose, *Preservation of strong normalisation in named λ -calculi with explicit substitution and garbage collection*. Computer Science in Netherlands, actes, 1995.
- [Bon01] Eduardo Augusto Bonelli, *Substitutions explicites et réécriture de termes*. Thèse de doctorat, Université Paris-Sud. Orsay, 2001.
- [BO93] Ronald Vernon Book et Friedrich Otto, *String-rewriting systems*. Texts and Monographs in Computer Science, Springer, 1993.
- [Bor94] Francis Borceux, *Handbook of categorical algebra*. Encyclopedia of mathematics and its applications 50-51-52. Cambridge University Press, 1994.
- [Bou39] Nicolas Bourbaki, *Éléments de mathématique. Livre 1 : Théorie des ensembles*. Hermann & Cie, 1939.
- [BH81] Ronald Brown et Philip J. Higgins, *On the algebra of cubes*. Journal of Pure and Applied Algebra 21, pages 233-260, 1981.
- [Buc79] Bruno Buchberger, *A theoretical basis for the reduction of polynomials to canonical forms*. ACM SIGSAM Bulletin 10/3, pages 19-29, 1976.
- [Bur81] Albert Burroni, *Algèbres graphiques (sur un concept de dimension dans les langages formels)*. Cahiers de Topologie et de Géométrie Différentielle Catégoriques 22/3, pages 249-265, 1981.
- [Bur93] Albert Burroni, *Higher-dimensional word problems with applications to equational logic*. Theoretical Computer Science 115/1, pages 46-62, 1993.
- [CG00] Luca Cardelli et Andrew Gordon, *Mobile ambients*. Theoretical Computer Science 240/1, pages 177-213, 2000.
- [Chu41] Alonzo Church, *The calculi of λ -conversion*. Annals of Mathematics Studies 6. Princeton University Press, 1941.
- [CHL96] Pierre-Louis Curien, Thérèse Hardin et Jean-Jacques Lévy, *Confluence properties of weak and strong calculi of explicit substitutions*. Journal of the Association for Computing Machinery 43/2, pages 362-397, 1996.
- [DG01] René David et Bruno Guillaume, *a λ -calculus with explicit weakening and explicit substitution*. Mathematical Structures in Computer Science 11/1, pages 169-206, 2001.
- [dB72] Nicolaas Govert de Bruijn, *Lambda calculus notation with nameless dummies, a tool for automatic formula manipulation, with application to the Church-Rosser theorem*. Koninklijke Nederlandse Akademie van Wetenschappen. Indagationes Mathematicae 34, pages 381-392, 1972.

- [dB78] Nicolaas Govert de Bruijn, *A namefree λ -calculus with facilities for internal definition of expressions and segments*. TH-Report 78-WSK-03. Technological University, Eindhoven, Netherlands, 1978.
- [DJ90] Nachum Dershowitz et Jean-Pierre Jouannaud, *Rewrite systems*. Handbook of theoretical computer science volume B : formal methods and semantics, chapitre 6, pages 243-320. North Holland, Amsterdam, 1990.
- [Eul98] Houston Euler, *The history of $2 + 2 = 5$* . www.kfunigraz.ac.at/imawww/pages/humor/twoandtwo.html.
- [FPT99] Marcelo Fiore, Gordon Plotkin et Daniele Turi, *Abstract syntax and variable binding*. Logic in Computer Science, actes, pages 193-202, 1999.
- [GS01] Alessio Guglielmi et Lutz Strassburger, *Non-commutativity and MELL in the calculus of structures*. Computer science logic, actes, pages 54-68. Lecture notes in computer science 2142, Springer, 2001.
- [Har89] Thérèse Hardin, *Confluence results for the pure strong categorical logic CCL. λ -calculi as subsystems of CCL*. Theoretical Computer Science 65/3, pages 291-342, 1989.
- [HY90] Teruo Hikita et Hirofumi Yokouchi, *A rewriting system for categorical combinators with multiple arguments*. SIAM Journal of Computing 19/1, pages 78-97, 1990.
- [Hue81] Gérard Huet, *A complete proof of correctness of the Knuth-Bendix completion algorithm*. Journal of Computer and System Sciences 23/1, pages 11-21, 1981.
- [JK86] Jean-Pierre Jouannaud et Hélène Kirchner, *Completion of a set of rules modulo a set of equations*. SIAM Journal on Computing 15/4, pages 1155-1194, 1986.
- [KR95] Fairouz Kamareddine et Alejandro Ríos, *λ -calculus à la de Bruijn with explicit substitutions*. Programming Languages : Implementations, Logics and Programs, actes. Lecture notes in computer science 982, pages 45-62. Springer, 1995.
- [Kes00] Delia Kesner, *Confluence of extensional and non-extensional λ -calculi with explicit substitutions*. Theoretical Computer Science 238/1-2, pages 183-220, 2000.
- [KL] Delia Kesner et Stéphane Lengrand, *Broadening the horizon of the explicit substitution paradigm via a logical model*. Prépublication.
- [Klo90] Jan Willem Klop, *Term rewriting systems*. Rapport CS-R9073, Centrum voor Wiskunde en Informatica, Amsterdam, 1990.
- [KB70] Donald Ervin Knuth et Peter B. Bendix, *Simple word problems in universal algebras*. Computational Problems in Abstract Algebra, actes, pages 263-297, 1970.

- [Laf90] Yves Lafont, *Interaction nets*. Principles of Programming Languages, actes, pages 95-108. ACM Press, 1990.
- [Laf95] Yves Lafont, *Equational reasoning with 2-dimensional diagrams*. Term Rewriting, Lecture Notes in Computer Science 909, pages 170-195. Springer, 1995.
- [Laf03] Yves Lafont, *Towards an algebraic theory of boolean circuits*. Journal of Pure and Applied Algebra 184, pages 257-310, 2003.
- [Lam] François Lamarche, *On the algebra of structural contexts*. Mathematical Structures in Computer Science, à paraître.
- [LS86] Joachim Lambek et Philip J. Scott, *Introduction to higher order categorical logic*. Cambridge studies in advanced mathematics 7, Cambridge University Press, 1986.
- [Lam90] John Lamping, *An algorithm for optimal λ -calculus reduction*. Principles of Programming Languages, actes, pages 16-30. ACM Press, 1990.
- [Lan98] Frédéric Lang, *Modèles de la β -réduction pour les implantations*. Thèse de doctorat, École Normale Supérieure. Lyon, 1998.
- [Law63] Francis William Lawvere, *Functorial semantics of algebraic theories*. Proceedings of the National Academy of Science 50/5, pages 869-872, Novembre 1963.
- [LLDDB04] Stéphane Lengrand, Pierre Lescanne, Dan Dougherty, Mariangiola Dezani-Ciancaglini et Steffen van Bakel, *Intersection types for explicit substitutions*. Information and Computation 189/1, pages 17-42, 2004.
- [Les94] Pierre Lescanne, *From $\lambda\sigma$ to $\lambda\nu$, a journey through calculi of explicit substitutions*. Principles of Programming Languages, actes, pages 60-69, 1994.
- [LR95] Pierre Lescanne et Jocelyne Rouyer-Degli, *Explicit substitutions with de Bruijn's levels*. Rewriting Techniques and Applications, actes. Lecture Notes in Computer Science 914, pages 294-308. Springer, 1995.
- [Lip02] Sylvain Lippi, *Encoding left reduction in the λ -calculus with interaction nets*. Mathematical structures in computer science 12/6, pages 797-822, 2002.
- [ML65] Saunders MacLane, *Categorical algebra*. Bulletin of the American Mathematical Society 71, pages 40-106, 1965.
- [ML98] Saunders MacLane, *Categories for the working mathematician*, deuxième édition. Springer, 1998.
- [Mal95] Georges Maltsiniotis, *Traces dans les catégories monoïdales, dualité et catégories monoïdales fibrées*. Cahiers de Topologie et de Géométrie Différentielle Catégoriques 36/3, pages 195-288, 1995.

-
- [May72] Jon Peter May, *The geometry of iterated loop spaces*. Lectures Notes in Mathematics 271. Springer, 1972.
- [May98] Jon Peter May, *Caterads*. Prépublication, 2003.
www.math.uchicago.edu/~may/PAPERS/Caterads.pdf.
- [Mel95] Paul-André Melliès, *Typed λ -calculi with explicit substitutions may not terminate*. Typed lambda calculi and applications, actes, pages 328-334. Lecture Notes in Computer Science 902, Springer, 1995.
- [Mel02] Paul-André Melliès, *Axiomatic rewriting theory I : a diagrammatic standardization theorem*. Prépublication de l'équipe Preuve, Programmes et Systèmes, numéro 13, décembre 2002.
- [MPW92] Robin Milner, Joachim Parrow et David Walker, *A calculus of mobile processes I-II*. Information and Computation, 100/1, pages 1-77, 1992.
- [Mun96] César Muñoz, *Confluence and preservation of strong normalisation in an explicit substitutions calculus*. Logic in Computer Science, actes, 1996.
- [Mur89] Tadao Murata, *Petri nets : properties, analysis and applications*. Proceedings of the Institute of Electrical and Electronics Engineers 77/4, pages 541-580, 1989.
- [New42] Maxwell Herman Alexander Newman, *On theories with a combinatorial definition of "equivalence"*. Annals of Mathematics 43/2, pages 223-243, 1942.
- [RTA] Rewriting homepage, *Problème ouvert numéro 88*.
www.lsv.ens-cachan.fr/rtaloop/problems/88.html.
- [Sch72] Horst Schubert, *Categories*. Springer, 1972.
- [Sel02] Peter Selinger, *The λ -calculus is algebraic*. Journal of Functional Programming 12/6, pages 549-566, 2002.
- [Squ87] Craig C. Squier, *Word problems and a homological finiteness condition for monoids*. Journal of Pure and Applied Algebra 49, pages 201-217, 1987.
- [Str76] Ross Street, *Limits indexed by category-valued 2-functors*. Journal of Pure and Applied Algebra 8/2, pages 149-181, 1976.
- [Ter03] Terese, *Term rewriting systems*. Cambridge tracts in theoretical computer science 55, Cambridge University Press, 2003.