Déduction et Unification dans les Théories Permutatives

Mnacho Echenim

INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE

N° attribué par la bibliothèque

Thèse

pour obtenir le grade de

DOCTEUR DE L'INPG

Spécialité : "Informatique : Systèmes et Communication"

préparée au Laboratoire Leibniz, dans le cadre de l'Ecole Doctorale "Mathématiques, Sciences et Technologie de l'Information"

présentée et soutenue publiquement par

B. Mnacho Echenim

le 2 Décembre 2005

Deduction et Unification dans les Théories Permutatives

Directeurs de thèse :

Thierry Boy de la Tour et Ricardo Caferra

Jury

Brigitte	Plateau	Présidente
David A.	Plaisted	Rapporteur
Gilles	Dowek	Rapporteur
Ricardo	Caferra	Directeur de thèse
Thierry	Boy de la Tour	Co-encadrant

A Michel et Marie-Madeleine DECREUSE.

Résumé

Il existe de nombreux démonstrateurs automatiques qui effectuent des raisonnements *modulo* une théorie équationnelle, c'est-à-dire en considérant non pas des termes, mais des classes d'équivalence de termes. En général, les travaux accomplis dans ce domaine ont pour but de concevoir des techniques pour faire de la déduction modulo une théorie particulière.

Dans [AP01], Jürgen Avenhaus et David Plaisted ont cherché à déterminer des techniques qui pourraient être employées dans le traitement non plus d'une théorie particulière, mais de toute une classe de théories équationnelles : les *théories permutatives*. Les auteurs ont introduit les notions de *terme stratifié* et d'*ensemble stratifié*, et décrit les procédures qui devraient être implémentées dans un démonstrateur automatique basé sur ces termes stratifiés. Les propriétés de régularité de ces théories font qu'il est possible d'employer des techniques efficaces de *théorie algorithmique des groupes* pour les traiter. Les auteurs espéraient que l'efficacité de ces techniques contrebalancerait le nombre élevé de clauses qui pourraient être générées dans un démonstrateur automatique basé sur ces termes stratifiés. Cependant, les algorithmes proposés pour faire de la déduction avec des termes stratifiés sont basés sur une énumération explicite des éléments des groupes, et sont donc exponentiels.

Dans ce mémoire, nous développons les travaux d'Avenhaus et Plaisted, et modifions leur formalisme pour pouvoir faire l'usage le plus intensif possible des techniques de théorie algorithmique des groupes.

Après avoir rappelé des notions de base de déduction automatique et de réécriture, puis présenté plusieurs résultats de théorie algorithmique des groupes dans la première partie de ce mémoire, nous introduisons dans la deuxième partie les notions de GA-*terme* et de GA-*terme stratifié* sur lesquels une action de groupe simple est définie. Puis nous prouvons que les ensembles stratifiés de [AP01] peuvent être obtenus à partir des orbites par cette action de groupe. Dans la troisième partie, nous démontrons que même les problèmes les plus élémentaires sur les termes stratifiés, comme le test de l'appartenance d'un terme à un ensemble stratifié, sont **NP**-complets. Enfin, dans la quatrième partie, nous présentons certaines restrictions qui peuvent être imposées à une théorie permutative E pour faire de la déduction modulo E, et définissons la notion d'*unif-stabilité*.

Mots clés : déduction automatique, théories équationnelles, réécriture, graphes de termes, symétries, théorie algorithmique des groupes, complexité, E-unification.

Abstract

There exist several theorem provers that perform deduction *modulo* an equational theory, i.e. by considering equivalence classes of terms, instead of ordinary terms. In general, most of the research carried out in this area focuses on determining new techniques to perform deduction modulo one particular theory.

In [AP01], Jürgen Avenhaus and David Plaisted sought for techniques that could be used for the treatment of not one particular theory, but an entire class of equational theories : the so-called *permutative theories*. The authors introduced the notions of *stratified terms*, and *stratified sets*, and described the procedures that should be implemented in a theorem prover based on stratified terms. Permutative theories enjoy several regularity properties that make it possible to use efficient techniques from *computational group theory* to deal with them. The authors hoped that the efficiency of these techniques would counterbalance the high number of clauses that could be generated by a theorem prover based on stratified terms. However, the algorithms they propose to perform deduction on stratified terms are based on an explicit enumeration of the elements of a group, and are therefore exponential.

In this thesis, we develop Avenhaus and Plaisted's work, and adapt their formalism to make a more intensive use of group-theoretic tools.

After having provided several basic definitions from automated deduction and rewriting, and then presented several results from computational group theory in the first part of this thesis, we introduce the notions of GA-*terms* and *stratified* GA-*terms*, on which a simple group action is defined. We then prove that the stratified sets as defined in [AP01] can be obtained from the orbits by this group action. In the third part of this thesis, we prove that even the more basic problems on stratified terms, such as testing the membership of a term to a stratified set are **NP**-complete. Finally, in the fourth part, we present some restrictions that can be imposed to a permutative theory E in order to perform deduction modulo E, and introduce the notion of *unify-stability*.

Keywords : automated deduction, equational theories, term rewriting, term graph rewriting, symmetries, computational group theory, complexity, E-unification.

Remerciements

Je tiens en premier lieu à remercier tous ceux qui m'ont fait l'honneur de siéger à mon jury, et en particulier Brigitte PLATEAU, Professeur à l'Institut National Polytechnique de Grenoble, qui a accepté de le présider. Je remercie Gilles DOWEK, Professeur à l'Ecole Polytechnique, et David A. PLAISTED, Professeur à University of North Carolina at Chapel Hill, qui ont accepté la lourde charge d'être rapporteurs du manuscrit.

Ma gratitude va également à Nicolas BALACHEFF, directeur du Laboratoire LEIBNIZ, ainsi qu'à tous les membres de ce laboratoire, qui m'ont permis d'effectuer mes travaux de recherche dans d'excellentes conditions. Je remercie surtout tous les membres de l'équipe CAPP, et particulièrement Prakash COUNTCHAM et Nicolas PELTIER pour leurs précieux conseils.

Je remercie également toutes les personnes qui ont contribué à faire du laboratoire LEIBNIZ un lieu de travail agréable, notamment Amandine, Béatrice, Benjamin, David, Dimitri, Eric, Julien, Marie, Nadia, Paul, Simon, Sylvain et Vincent.

Je remercie particulièrement ma famille et mes proches, qui m'ont soutenu et supporté au cours de ces trois années. Sophie, merci d'avoir été là jour après jour.

Last but not least, je tiens à remercier mes deux directeurs de thèse. Je tiens à exprimer toute ma reconnaissance à Ricardo CAFERRA qui m'a accueilli en stage dans son équipe il y a six ans, et qui a bien voulu renouveler l'expérience trois ans plus tard. Je le remercie pour ses conseils, ses encouragements, et son engagement personnel dans mon projet. Enfin, je ne saurais par où commencer pour remercier Thierry BOY DE LA TOUR. Merci de m'avoir encadré en stage il y a six ans, puis en DEA il y a quatre ans, et enfin en thèse. Merci d'avoir été un directeur de thèse patient, compréhensif, motivé et motivant. Surtout, merci pour toutes nos conversations, scientifiques, politiques, cinématographiques et littéraires, qui ont été autant de bouffées d'oxygène durant ces trois années.

Table des matières

Table des figures

Chapitre 1

Introduction

Raisonnement automatique

Dans [WOLB92], les principes et objectifs du *Raisonnement Automatique* sont très clairement présentés[1] :

> "Pour comprendre ce qu'est le raisonnement automatique, il faut d'abord comprendre ce que raisonner signifie. Raisonner, c'est le fait de tirer des conclusions à partir de faits. Pour qu'un raisonnement soit juste, ces conclusions doivent systématiquement découler des faits considérés. [...] Les seules conclusions acceptables sont celles qui découlent logiquement des faits en notre possession. Le but du raisonnement automatique est d'écrire des programmes informatiques qui peuvent aider à résoudre des problèmes et à répondre à des questions qui requièrent un raisonnement."

On peut donc voir l'origine de cette notion dans celles de la logique, qui remontent traditionnellement à Aristote. En effet, ce dernier a sans doute effectué la première étude systématique de la science du raisonnement, en créant la notion de *syllogisme*, un ensemble de trois affirmations, deux prémisses et une conclusion. Par exemple, à partir des assertions "tout homme est mortel", et "Socrate est un homme" (les prémices), on conclut que "Socrate est mortel". Les règles de syllogisme peuvent donc être considérées comme les précurseurs des règles d'inférence modernes.

Ce n'est qu'avec les développements mathématiques de la logique, effectués dès la fin du XIX$^{\text{ème}}$ siècle, que sa mécanisation a pu devenir concevable. Cette mécanisation et les fondations des mathématiques sont d'ailleurs intimement liées, comme en témoignent nombre des problèmes ouverts du fameux *programme de Hilbert*, énoncé au début du XX$^{\text{ème}}$ siècle. Pour Hilbert, il n'est en effet possible d'étudier une branche des mathématiques de façon rigoureuse qu'en se servant d'un *système formel*, c'est-à-dire d'un ensemble d'*axiomes* et de *règles d'inférence*. Un tel système formel devait en particulier permettre de développer n'importe quel théorie sans avoir recours à la moindre intuition, et donc de mécaniser cette étude.

[1] traduction personnelle.

Le premier coup porté à ce programme aura été le théorème d'incomplétude de Gödel. Il montre qu'une notion aussi simple que la vérité arithmétique n'admet pas de définition finitaire, et donc que ces vérités ne peuvent pas être énumérées mécaniquement. Ce résultat a été d'autant plus surprenant qu'il suivait de près d'autres résultats plus encourageants, eux, comme l'algorithme de Presburger, permettant de décider de la vérité arithmétique *sans multiplication*, ou même le théorème de complétude de Gödel, permettant l'énumération mécanique des formules valides du premier ordre.

Après que les travaux de Turing et Church ont permis de mieux comprendre la notion de mécanisation (ou calculabilité), ce dernier portait un second coup au programme de Hilbert, en montrant l'indécidabilité de la logique du premier ordre (la validité est énumérable mais non calculable). Ces travaux coïncidaient avec le développement des premiers calculateurs, et n'ont pas pu freiner l'enthousiasme suscité par ces derniers, qui devait donner naissance à l'Intelligence Artificielle. Les premiers démonstrateurs automatiques se révélèrent donc particulièrement inefficaces. Par exemple, le résultat le plus important obtenu par l'implémentation de l'algorithme de Presburger, réalisée en 1954 par Martin Davis, a été la preuve que la somme de deux entiers pairs est paire.

Depuis, de nombreux travaux ont permis d'améliorer considérablement les performances des démonstrateurs automatiques, grâce à la création de concepts célèbres, comme la procédure DPLL ([DLL83]), la règle de résolution de Robinson ([Rob65]), ou la méthode des tableaux ([Smu63, Bet55, Hin55]). Ces travaux ne correspondent plus (ou plus seulement) à cet enthousiasme naïf visant à la mécanisation de l'activité mathématique, abstraite. Des domaines d'application d'une grande importance scientifique et économique sont apparus, comme la *vérification de programme*.

Il est en effet connu que les erreurs logicielles ont un coût gigantesque pour l'économie. Un exemple marquant est celui de l'échec du premier vol de la fusée Ariane 5 en 1996, dont le lanceur a été détruit 40 secondes après le décollage. Aujourd'hui, on sait que cet échec était dû à une défaillance informatique lors de la conversion d'un nombre de 64 bits en un nombre de 16 bits. On se rappellera aussi le fameux bogue des premières puces Pentium.

De telles erreurs pourraient théoriquement être détectées par des humains, mais en pratique ceci est impossible à cause de l'extrême complexité des logiciels mis en œuvre. C'est là où les démonstrateurs automatiques peuvent contribuer à prouver formellement la correction des logiciels ou, de façon similaire, celle des circuits. De plus en plus de grands groupes industriels (IBM, Intel, Motorolla...) se servent de démonstrateurs automatiques dans ce but, en se limitant par nécessité à des applications relativement simples mais "critiques".

Raisonnement équationnel et réécriture

La notion la plus utilisée en mathématiques est incontestablement l'*égalité*. Cette notion est en particulier utilisée pour définir des objets mathématiques. Un groupe peut par exemple être défini par un ensemble d'équations traduisant les propriétés vérifiées par sa loi de composition interne, et les liens entre ses éléments. L'utilisation d'équations pour définir des objets est également très répandue en informatique, notamment en

programmation fonctionnelle.

La simplicité de la notion d'égalité n'est qu'apparente, et s'il est théoriquement possible de simplement traiter l'égalité comme un prédicat binaire satisfaisant certains axiomes, en pratique, l'application explicite de ces axiomes est très laborieuse et inefficace. Néanmoins, l'importance et l'utilité de cette notion font de sa mécanisation un enjeu majeur, et de nouvelles techniques de preuve gérant plus efficacement l'égalité ont rapidement été conçues, comme la règle de *paramodulation* (voir [NR01]), ou les techniques de *réécriture*.

Une façon simple et intuitive d'utiliser un axiome équationnel est en effet de toujours l'utiliser "dans le même sens". C'est ce qui se fait naturellement en arithmétique élémentaire, afin de simplifier des expressions (ou *termes*). Par exemple, l'expression $2 * (3 + 1)$ se simplifie en $2 * 4$, puis en 8. Le fait de toujours utiliser un axiome dans le même sens revient à l'*orienter*, pour obtenir une *règle de réécriture*. Quand tous les axiomes d'une théorie équationnelle ont été orientés, il se pose deux questions principales concernant le *système de réécriture* obtenu :

- Est-il garanti qu'il n'existe aucun terme sur lequel il est possible d'appliquer une séquence infinie de règles de réécriture ? (le système est-il *noethérien* ?)
- Est-il garanti que l'ordre dans lequel les règles de réécriture sont appliquées à un terme est sans importance ? (le système est-il *confluent* ?)

Ces deux problèmes sont indécidables (voir par exemple [BN98] ou [Ohl02]), mais il existe des cas particuliers pour lesquels il est possible de décider si un système de réécriture vérifie ou non ces propriétés.

Si le système de réécriture considéré vérifie ces deux propriétés, on dit qu'il est *convergent*, et il permet de décider si deux termes sont égaux. Il suffit pour cela de réduire ces termes à leurs *formes normales* respectives, c'est-à-dire des termes sur lesquels aucune règle de réécriture ne peut être appliquée, et de tester si ces dernières sont égales. Si le système de réécriture ne vérifie pas ces propriétés, de nouvelles questions se posent. S'il n'est pas noethérien, existe-t-il une autre orientation des axiomes qui permet d'obtenir un système de réécriture noethérien ? S'il n'est pas confluent, est-il possible d'ajouter des règles de réécriture qui le rendent confluent ?

En 1970, dans [KB83], Knuth et Bendix ont présenté un algorithme qui tente de transformer un ensemble d'équations en un système de réécriture convergent. Leur algorithme peut terminer avec un succès, terminer avec un échec, ou ne pas terminer du tout. S'il termine avec un succès, alors le système obtenu permet de décider si deux termes sont égaux. S'il termine avec un échec, cela signifie qu'il n'a pas pu orienter toutes les équations.

Il peut paraître paradoxal que certains axiomes très répandus, et qui simplifient les calculs en algèbre, ne peuvent pas être orientés. C'est le cas par exemple de l'axiome de commutativité, $f(x, y) = f(y, x)$. Une solution classique de ce problème a été proposée par Plotkin en 1972, qui a suggéré dans [Plo72] d'intégrer le raisonnement spécifique lié à ces axiomes dans des mécanismes normalement élémentaires, comme l'*unification*. Plusieurs travaux, d'abord de Slagle ([Sla74]), Lankford et Ballantyne ([LB77a, LB77b]), et Peterson et Stickel ([PS81]), puis de Bachmair et Dershowitz ([BD89]) et Jouannaud

et Kirchner ([JK86]), ont montré qu'une combinaison de règles de réécriture et d'un algorithme d'unification pour une théorie donnée, permettent d'étendre l'algorithme de Knuth et Bendix pour créer des systèmes de réécriture convergents à partir d'ensembles d'équations contenant par exemple les axiomes de commutativité et d'associativité.

Les théories contenant les axiomes de commutativité et d'associativité ont sans doute été les plus étudiées dans ce cadre, et de nombreux outils, souvent très efficaces, ont été conçus pour ces théories, ainsi que leurs extensions. Il demeure néanmoins certaines difficultés incontournables, comme le fait que tout ensemble complet d'unificateurs modulo une théorie associative et commutative est de l'ordre de $O(2^{2^n})$ (voir [Dom92, KN92]).

Théories permutatives

Dans [AP01], Avenhaus et Plaisted se sont intéressés à ce type de démarche non pas pour une théorie équationnelle particulière, mais pour une classe de théories, caractérisées par la forme de leurs axiomes. La classe considérée est la classe des *théories permutatives*, qui sont définies par des ensembles d'*équations permutatives*. Une équation permutative est une équation entres des termes linéaires, telle que le terme de droite est obtenu en permutant les variables du terme de gauche. Il est clair que ces équations permutatives, dont fait partie l'axiome de commutativité, ne peuvent pas être orientées. Le but d'Avenhaus et Plaisted était de développer une méthode uniforme qui pourrait être appliquée à n'importe quelle théorie permutative E, et de traiter des ensembles de termes congrus modulo E, sans pour autant considérer des classes d'équivalence entières de termes. Leur méthode ne s'apparente donc pas aux méthodes classiques de raisonnement modulo une théorie équationnelle, puisque certains axiomes de E doivent être conservés dans le processus de déduction. Ces ensembles de termes congrus sont appelés des *ensembles stratifiés*, et sont représentés par un *terme stratifié*. Les auteurs ont alors montré comment *relever* les règles de réécriture, de paramodulation ou de résolution, pour les appliquer à des termes stratifiés.

Comme l'utilisation d'un axiome de E sur un terme résulte en une permutation de certains de ses sous-termes, l'utilisation de groupes de permutations devient naturelle pour traiter ces ensembles stratifiés, et les auteurs espéraient bénéficier des algorithmes efficaces issus de la *théorie algorithmique des groupes* pour contrebalancer le nombre de clauses et d'équations supplémentaires produites par un démonstrateur basé sur ces termes stratifiés.

Théorie algorithmique des groupes

Bien qu'il soit généralement convenu que les origines de la théorie des groupes remontent aux travaux d'Evariste Galois, la notion de groupe abstrait n'a été formellement définie que vers la fin du dix-neuvième siècle, et a été très rapidement suivie des premières questions algorithmiques sur ces groupes. Les premières questions ont été posées par Dehn ([Deh11]), dont la plus célèbre est sans doute celle concernant le problème du mot pour un *groupe finiment présenté*. La question est la suivante : étant donné un groupe

défini par un ensemble de générateurs X et un ensemble de relations sur ces générateurs R, et étant donné un mot U sur X, U représente-t-il l'identité de G ? Novikov a démontré plus de quarante ans plus tard que ce problème est indécidable dans [Nov55].

Moins d'un siècle plus tard, la théorie algorithmique des groupes est devenue un domaine de recherche à part entière, qui a été appliqué à des sujets aussi variés que la physique, la cristallographie, les réseaux interconnectés ou la cryptographie.

Les groupes de permutation constituent une des branches les plus importantes de la théorie algorithmique des groupes. Cette branche s'est développée à partir des années soixante avec l'introduction par Sims d'outils efficaces pour la manipulation de ces groupes ([Sim70, Sim71]), et la preuve par Luks du lien entre certains problèmes sur les groupes de permutation et le problème d'isomorphisme de graphes ([Luk82]). Ceci explique pourquoi pendant de nombreuses années, il y a eu deux courants de recherche indépendants dans ce domaine, l'un portant sur l'étude de la complexité de ces problèmes ([Hof81]), et l'autre sur la conception d'algorithmes efficaces pour les résoudre (voir [But91]). Puis, au cours de la dernière décennie, ces deux courants ont convergé, et des systèmes de calcul formel comme GAP[2] sont aujourd'hui basés sur des algorithmes dont les temps d'exécution sont optimaux.

Une caractéristique importante des groupes de permutation est qu'ils peuvent être représentés de façon très succincte par des ensembles de générateurs. Ainsi, tout sous-groupe du groupe symétrique $\mathrm{Sym}(n)$ (dont la cardinalité est $n!$), peut être représenté par moins de n générateurs. De plus, de nombreux problèmes, comme le test de l'appartenance d'une permutation à un groupe, ou la détermination de l'ordre du groupe, peuvent être résolus en temps polynomial. D'autres problèmes, comme la détermination d'un ensemble de générateurs pour l'intersection de deux groupes de permutation, sont plus difficiles que le problème d'isomorphisme de graphe. Ces problèmes forment la *classe de complexité de Luks*, qui est considérée comme étant disjointe de la classe des problèmes polynomiaux, et de la classe des problèmes **NP**-complets (à condition que $\mathbf{P} \neq \mathbf{NP}$). [Luk93] contient une liste plus détaillée de problèmes polynomiaux ou dans la classe de Luks.

L'objectif principal de cette thèse a été de développer les travaux de Avenhaus et Plaisted, en exploitant pleinement les bonnes propriétés algorithmiques des groupes. En effet, dans [AP01], les auteurs ne font qu'un usage élémentaire de techniques de la théorie algorithmique des groupes, et il nous est apparu qu'un usage plus intensif pourrait résulter en des algorithmes efficaces pour faire de la déduction avec des théories permutatives. Nous avons commencé par démontrer que les ensembles stratifiés de [AP01] peuvent être obtenus comme des *orbites* sous l'action d'un groupe. Pour cela, nous avons adopté un formalisme proche de celui employé en *réécriture de graphes de termes*, et défini les GA-*termes*, et les GA-*termes stratifiés*, qui sont la traduction dans ce formalisme des termes standard, et des termes stratifiés de [AP01]. Puis, nous avons démontré que même les tâches les plus basiques comme le test de l'appartenance d'un terme à un ensemble stratifié sont **NP**-complètes. Nous avons donc entrepris de rechercher des restrictions qui pourraient être imposées aux théories permutatives considérées afin de pouvoir faire de la déduction modulo de telles théories de façon efficace. Nous avons ainsi défini la notion

[2] http ://www.gap-system.org

d'*unif-stabilité*, qui nous a permis d'exhiber une classe de théories permutatives possédant de bonnes propriétés algorithmiques. Enfin, nous avons prouvé que les théories de cette classe sont de type *finitaire* pour l'unification, ce qui n'est pas le cas pour toutes les théories permutatives.

Plan de la thèse

Après avoir rapidement défini les notions de base de la réécriture, comme les notions de terme, de substitution ou de E-unification, nous rappellerons plusieurs notions de théorie élémentaire des groupes, dont nous nous servirons dans le Chapitre 4 pour présenter plus en détail certains résultats de théorie algorithmique des groupes.

Nous aurons besoin de recourir aux techniques employées dans la réécriture de graphes de termes pour représenter des termes, et nous définirons les notions de GA-*termes* et de GA-*termes* stratifiés dans les chapitres suivants. Les GA-termes stratifiés nous permettront de définir un groupe dont chaque élément correspond à l'application (simultanée) de règles de la réécriture stratifiée définie dans [AP01].

Dans le Chapitre 7, nous définirons une relation d'équivalence sur des GA-termes stratifiés, la relation de *congruence stratifiée*, et nous montrerons que le problème de décider si deux GA-termes stratifiés sont liés par cette relation est dans la classe de Luks.

Dans le chapitre suivant, nous définirons certains problèmes liés à la déduction, et verrons que même en imposant certaines restrictions aux GA-termes stratifiés considérés, ces problèmes sont tous **NP**-complets. C'est pourquoi dans les Chapitres 9 et 10, nous imposerons des restrictions aux théories permutatives à considérer, et définirons les théories permutatives *unif-stables*. Nous étudierons les propriétés de ces théories, et prouverons dans le Chapitre 11 que l'unification modulo une théorie permutative unif-stable est finitaire. Enfin, nous démontrerons que tout problème d'unification possède un ensemble complet d'unificateurs de cardinalité simplement exponentielle. Les démonstrations de certains résultats sont assez longues et ardues, et ont été regroupées en annexe.

Première partie

Notions de base

Chapitre 2

Préliminaires

Dans ce chapitre, nous allons rappeler plusieurs notions standard de réécriture. On pourra trouver une description plus détaillée de ces notions dans [DP01, BN98, BS01, GJ79].

2.1 Relations

Définition 2.1.1 (Listes) Soit A un ensemble, l'ensemble des *listes sur* A (ou *mots sur* A) est noté $A^\star$. Cet ensemble est un monoïde pour l'opération de *concaténation* ".", et son élément neutre, le *mot vide*, est noté ε. Soit $w \in A^\star$, la *longueur* $|w|$ de w est définie inductivement par : si $w = \varepsilon$, alors $|w| = 0$, sinon, $w = a.w'$, et $|w| = 1 + |w'|$.

Soient $a \in A$ et $B \subseteq A^\star$, alors l'ensemble $a.B \subseteq A^\star$ est défini par :

$$a.B \;=\; \{a.b \,|\, b \in B\}.$$

Soit f une fonction de A vers B, on définit $f^\star$ de $A^\star$ vers $B^\star$ par : $f^\star(w_1.\cdots.w_n) = f(w_1).\cdots.f(w_n)$. Par abus de notation, on pourra noter cette fonction f au lieu de $f^\star$.

Soit $w \in A^\star$ un mot non vide, alors pour tout $i \in \{1, \ldots, |w|\}$, on note w_i la $i^{\text{ème}}$ lettre de w. ◇

Définition 2.1.2 (Multiensembles) Etant donné un ensemble A, un *multiensemble* M *sur* A est une fonction $M : A \to \mathbb{N}$. Un multiensemble est dit *fini* si et seulement s'il existe un ensemble fini d'éléments $x \in A$ tels que $M(x) > 0$.

On définit les opérateurs suivants sur les multiensembles :

- Appartenance : $(x \in M) \Leftrightarrow (M(x) > 0)$.
- Inclusion : $(M \subseteq N) \Leftrightarrow (\forall x \in A, M(x) \leq N(x))$.
- Union : $\forall x \in A$, $(M \cup N)(x) := M(x) + N(x)$.
- Différence : $\forall x \in A$, $(M - N)(x) := \max(M(x) - N(x), 0)$. ◇

Définition 2.1.3 (Relations) Etant donné un ensemble A et une relation $R \subseteq A \times A$, on dit que R est :

- *réflexive* si et seulement si $\forall x \in A$, $\langle x, x\rangle \in R$,
- *symétrique* si et seulement si $\forall x, y \in A$, $(\langle x, y\rangle \in R) \Leftrightarrow (\langle y, x\rangle \in R)$,
- *antisymétrique* si et seulement si $\forall x, y \in A$, si $\langle x, y\rangle \in R$ et $\langle y, x\rangle \in R$, alors $x = y$,
- *transitive* si et seulement si $\forall x, y, z \in A$, si $\langle x, y\rangle \in R$ et $\langle y, z\rangle \in R$, alors $\langle x, z\rangle \in R$.

La *fermeture transitive de* R, notée $R^\star$, est la plus petite relation transitive contenant R, au sens de l'inclusion.

Il est standard de noter xRy au lieu de $\langle x, y\rangle \in R$. On dit que R est un *préordre* si R est réflexive, et transitive, si R est un préordre symétrique, on dira que R est une *relation d'équivalence*, et si R est un préordre antisymétrique, on dira que R est un *ordre*, qu'on notera en général $\leq$. Enfin, on dira que $\leq$ est un ordre *total* si pour tout $x, y \in A$, on a $x \leq y$, ou $y \leq x$.

Si R est une relation antisymétrique et transitive et pour tout $x \in A$, $\langle x, x\rangle \notin R$, on dira que R est un *ordre strict*, ce qu'on notera en général $<$ ou $\lneq$. Un ordre strict $<$ est dit *bien fondé* s'il n'existe pas de séquence infinie $(x_i)_{i\in\mathbb{N}}$ telle que pour tout $i \in \mathbb{N}$, $u_{i+1} < u_i$. ◇

Nous allons maintenant définir deux ordres induits : l'*ordre lexicographique induit*, et l'*ordre induit sur les multiensembles* (voir [DM79], ou [BN98, p. 21]).

Définition 2.1.4 (Ordre lexicographique) Soient des ensembles $A_1, \ldots, A_n$ des ensembles, respectivement munis des ordres stricts $<_i, i = 1, \ldots, n$. L'*ordre lexicographique induit par les ordres stricts* $<_i$, ou l'*extension lexicographique des ordres stricts* $<_i$, est la relation d'ordre $\prec$ définie sur $A_1 \times \ldots \times A_n$ par :

$$((a_1, \ldots, a_n) \prec (b_1, \ldots, b_n)) \Leftrightarrow (\exists i \in \{1, \ldots, n\}, (\forall j < i,\ a_j = b_j) \wedge (a_i <_i b_i)). \qquad \diamond$$

Théorème 2.1.5 *L'ordre* $\prec$ *est bien défini, et si pour tout* $i = 1, \ldots, n$, $<_i$ *est bien fondé, alors* $\prec$ *est bien fondé.*

Définition 2.1.6 (Ordre sur les multiensembles) Etant donnés un ensemble A et un ordre strict $<$ sur A, on définit l'ordre induit par $<$ sur les multiensembles de A, noté $\lessdot$, de la façon suivante :

$$M \lessdot N \Leftrightarrow \exists X, Y : \begin{cases} \emptyset \neq X \subseteq M, \\ N = (M - X) \cup Y, \\ \forall y \in Y,\ \exists x \in X,\ y < x. \end{cases} \qquad \diamond$$

Théorème 2.1.7 *L'ordre* $\lessdot$ *est bien défini, et si* $<$ *est bien fondé, alors* $\lessdot$ *l'est aussi.*

2.2 Théories équationnelles

Définition 2.2.1 (Signature) Une *signature* est un ensemble de symboles Σ, auquel est associé une fonction d'*arité*, arité : $\Sigma \to \mathbb{N}$. Un symbole $f \in \Sigma$ est un *symbole de fonction* si et seulement si arité$(f) > 0$, sinon, f est un *symbole de constante*. ◇

Définition 2.2.2 Soient une signature Σ, et un ensemble $\mathcal{V}$ de *variables* tel que $\Sigma \cap \mathcal{V} = \emptyset$. L'ensemble de Σ-*termes sur* $\mathcal{V}$, noté $\mathcal{T}(\Sigma, \mathcal{V})$, est défini inductivement par :

- $\mathcal{V} \subseteq \mathcal{T}(\Sigma, \mathcal{V})$ (toute variable est un Σ-terme),
- pour tout $n \geq 0$, pour tout $t_1, \ldots, t_n \in \mathcal{T}(\Sigma, \mathcal{V})$, si f est un symbole de Σ d'arité n, alors $f(t_1, \ldots, t_n) \in \mathcal{T}(\Sigma, \mathcal{V})$.

Par convention, si a est un symbole de constante de Σ, alors on notera $a \in \mathcal{T}(\Sigma, \mathcal{V})$ au lieu de $a() \in \mathcal{T}(\Sigma, \mathcal{V})$.

L'ensemble des variables d'un terme $t \in \mathcal{T}(\Sigma, \mathcal{V})$ est noté $\mathrm{Var}(t)$. Si cet ensemble est vide, on dit que le terme est *clos*. Si toute variable de $\mathcal{V}$ apparaît au plus une fois dans t, on dit que t est *linéaire*.

Enfin, on étend la définition de la fonction Var aux ensembles de termes en posant, pour tout ensemble S de termes, $\mathrm{Var}(S) = \bigcup_{t \in S} \mathrm{Var}(t)$. $\diamond$

Définition 2.2.3 Soit $t \in \mathcal{T}(\Sigma, \mathcal{V})$. L'ensemble des *positions* de t est l'ensemble $\mathrm{Pos}(t) \subseteq \mathbb{N}^\star$ défini inductivement par :

- si $t \in \mathcal{V}$, alors $\mathrm{Pos}(t) = \{\varepsilon\}$,
- sinon, posons $t = f(t_1, \ldots, t_n)$, alors

$$\mathrm{Pos}(t) \;=\; \{\varepsilon\} \cup \bigcup_{j=1}^{n} \{j.p \mid p \in \mathrm{Pos}(t_j)\}.$$

La *taille* de t est alors définie par : $|t| = |\mathrm{Pos}(t)|$.

Etant donné un mot $p \in \mathrm{Pos}(t)$, le *sous-terme à la position* p *de* t, noté $t|_p$, est défini inductivement par :

$$\begin{aligned} t|_\varepsilon &= t, \\ f(t_1, \ldots, t_n)|_{j.q} &= t_j|_q. \end{aligned}$$

On dit qu'un terme t est de *profondeur* k si et seulement si $k = \max\{|p| \mid p \in \mathrm{Pos}(t)\}$. $\diamond$

Exemple 2.2.4 Soit $\Sigma = \{e, i, f\}$, où e est une constante, i est une fonction d'arité 1, et f une fonction d'arité 2, et soit le Σ-terme $t = f(e, f(x, i(x)))$, où $x \in \mathcal{V}$. Alors on a $\mathrm{Pos}(t) = \{\varepsilon, 1, 2, 2.1, 2.2, 2.2.1\}$, d'où $|t| = 6$, et par exemple, $t|_{2.2} = i(x)$.

Définition 2.2.5 Soient Σ une signature et $\mathcal{V}$ un ensemble infini de variables. Une $\mathcal{T}(\Sigma, \mathcal{V})$-*substitution* est une fonction $\sigma : \mathcal{V} \to \mathcal{T}(\Sigma, \mathcal{V})$, telle que l'ensemble

$$\mathrm{Dom}(\sigma) \;=\; \{x \in \mathcal{V} \mid \sigma(x) \neq x\}$$

est fini. L'ensemble $\mathrm{Dom}(\sigma)$ est appelé le *domaine* de σ, et l'ensemble $\mathrm{Ran}(\sigma) = \{\sigma(x) \mid x \in \mathrm{Dom}(\sigma)\}$, le *codomaine* de σ. Si aucune confusion n'est possible, nous dirons simplement que σ est une substitution.

Si σ est une substitution de domaine $\{x_1, \ldots, x_n\}$, nous noterons en général $\sigma = \{x_1 \leftarrow \sigma(x_1), \ldots, x_n \leftarrow \sigma(x_n)\}$.

On étend naturellement une substitution σ à une fonction $\hat{\sigma}$ de $\mathcal{T}(\Sigma, \mathcal{V})$ vers $\mathcal{T}(\Sigma, \mathcal{V})$, en définissant :

$$\begin{aligned} \forall x \in \mathcal{V},\ \hat{\sigma}(x) &= \sigma(x), \\ \forall t = f(t_1, \ldots, t_n),\ \hat{\sigma}(t) &= f(\hat{\sigma}(t_1), \ldots, \hat{\sigma}(t_n)). \end{aligned}$$

Par abus de notation, nous noterons σ au lieu de $\hat{\sigma}$, et par convention, pour tout $t \in \mathcal{T}(\Sigma, \mathcal{V})$, nous noterons $t\sigma$ au lieu de $\sigma(t)$; la composition de σ et de μ est donc notée $\sigma\mu$ au lieu de $\mu \circ \sigma$.

Une substitution σ est dite *idempotente* si et seulement si $\sigma\sigma = \sigma$, et si $\mathrm{Dom}(\sigma) = \mathrm{Ran}(\sigma)$, on dit que σ est un *renommage*.

Soient $t, t' \in \mathcal{T}(\Sigma, \mathcal{V})$, on dit que t' est une *instance* de t si et seulement s'il existe une substitution telle que $t' = t\sigma$. ◇

On a la propriété standard suivante :

Propriété 2.2.6 *Soit σ une substitution, alors σ est idempotente si et seulement si* $\mathrm{Dom}(\sigma) \cap \mathrm{Var}(\mathrm{Ran}(\sigma)) = \emptyset$.

Définition 2.2.7 (Théorie équationnelle) Soit A un ensemble d'équations, c'est-à-dire un ensemble d'éléments de la forme $t \rightleftharpoons t'$, où $t, t' \in \mathcal{T}(\Sigma, \mathcal{P})$. On appelle *théorie équationnelle définie par A* la plus petite relation de congruence (voir [BN98]) contenant A. Si E est la théorie équationnelle définie par A, alors on notera $t =_E t'$ si t et t' sont congrus modulo E, et on dira que t' *est dans la classe de congruence de t modulo E.*

Une théorie équationnelle définie par un ensemble d'axiomes A est dite *permutative* si et seulement si pour tout $s \rightleftharpoons t \in A$, s et t sont des termes linéaires, et sont des instances l'un de l'autre. ◇

Exemple 2.2.8 Les théories de la commutativité et de l'associativité-commutativité sont des théories permutatives, puisqu'elles sont respectivement définies par les ensembles d'axiomes suivants :

$$A_C = \{f(x, y) \rightleftharpoons f(y, x)\},\ \text{et}\ A_{AC} = A_C \cup \{f(f(x, y), z) \rightleftharpoons f(f(y, z), x)\}.$$

Définition 2.2.9 (Problème du mot généralisé) Le *problème du mot généralisé* est le problème suivant :

> **Problème**: Problème du mot généralisé
> **Entrée**: Un ensemble d'axiomes définissant une théorie permutative E, et deux Σ-termes s et t
> **Question**: s et t sont-ils congrus modulo E ?

2.3 Unification équationnelle

Définition 2.3.1 (*E*-unification) Etant donnée une théorie équationnelle E et une signature Σ contenant tous les symboles apparaissant dans E, un *problème de E-unification sur Σ* est un ensemble fini d'équations

$$S \;=\; \{s_1 =^?_E t_1, \ldots, s_n =^?_E t_n\},$$

où les s_i et les t_i sont des Σ-termes. Un *E-unificateur de S*, ou *solution de S* est une substitution σ telle que pour tout $i = 1, \ldots, n$, $s_i\sigma =_E t_i\sigma$. L'ensemble des solutions de S est noté $\mathcal{U}_E(S)$, et si cet ensemble est non vide, on dit que S est *E-unifiable*. Si tous les symboles de Σ apparaissent dans E, on dit que S est un *problème de E-unification élémentaire*.

Si $E = \emptyset$, on dit que S est un *problème d'unification syntaxique*, et on notera

$$S \;=\; \{s_1 =^? t_1, \ldots, s_n =^? t_n\}. \qquad \diamond$$

Exemple 2.3.2 Soit C la théorie de la commutativité, définie par l'axiome $f(x, y) \rightleftharpoons f(y, x)$. Alors le problème de C-unification $S = \{f(x, a) =^?_C f(y, b)\}$ est C-unifiable, et la substitution $\{x \leftarrow b, y \leftarrow a\}$ est une solution de S. Par contre, le problème d'unification syntaxique correspondant n'admet aucune solution.

Définition 2.3.3 Soient E une théorie équationnelle, $\mathcal{X}$ un ensemble de variables, et σ et μ deux substitutions. On dit que *σ est plus générale que μ sur $\mathcal{X}$ modulo E* si et seulement s'il existe une substitution θ telle que pour tout $x \in \mathcal{X}$, $x\mu =_E x\sigma\theta$. On écrit alors $\sigma \lesssim^{\mathcal{X}}_E \mu$, ou $\mu \gtrsim^{\mathcal{X}}_E \sigma$, et on dit que μ est une *E-instance de σ sur $\mathcal{X}$*. $\diamond$

Propriété 2.3.4 *La relation $\lesssim^{\mathcal{X}}_E$ est un préordre.*

Théorème 2.3.5 *Etant donnée une théorie E, soient t et s deux termes, x une variable, et γ une substitution telle que $x\gamma =_E s\gamma$. Alors $t\gamma =_E t\{x \leftarrow s\}\gamma$.*

PREUVE. On démontre le résultat par induction sur la profondeur p de t. Si $p = 0$, il y a deux cas à considérer. Si $t \neq x$, alors $t\{x \leftarrow s\} = t$, et le résultat est immédiat, et si $t = x$, alors on a $t\gamma = x\gamma =_E s\gamma = t\{x \leftarrow s\}\gamma$. Supposons maintenant que le résultat est vrai pour tout terme de profondeur inférieure ou égale à $k-1$, et que t est de profondeur k. Alors on a $t = f(t_1, \ldots, t_n)$, et si pour $i = 1, \ldots, n$, on pose $t'_i = t_i\{x \leftarrow s\}$, alors par hypothèse d'induction, on a $t_i\gamma =_E t'_i\gamma$ pour tout $i = 1, \ldots, n$. On en déduit que

$$t\gamma \;=\; f(t_1\gamma, \ldots, t_n\gamma) \;=_E\; f(t'_1\gamma, \ldots, t'_n\gamma) \;=\; t\{x \leftarrow s\}\gamma. \qquad \blacksquare$$

Corollaire 2.3.6 *Soient t, t' et s des termes, x une variable, et γ une substitution. Alors on a*

$$(x\gamma =_E s\gamma \text{ et } t\gamma =_E t'\gamma) \;\Leftrightarrow\; (x\gamma =_E s\gamma \text{ et } t\{x \leftarrow s\}\gamma =_E t'\{x \leftarrow s\}\gamma).$$

Définition 2.3.7 Soient S un problème de E-unification, $\mathcal{X} = \mathrm{Var}(S)$, et soit $C \subseteq \mathcal{U}_E(S)$. On dit que C est un *ensemble complet d'unificateurs* (ou CSU pour *complete set of unifiers*), si et seulement si

$$\forall \mu \in \mathcal{U}_E(S),\ \exists \sigma \in C,\ \sigma \lesssim_E^{\mathcal{X}} \mu.$$

Si de plus, C vérifie la propriété suivante :

$$\forall \sigma, \mu \in C,\ (\sigma \lesssim_E^{\mathcal{X}} \mu)\ \Rightarrow\ (\sigma = \mu),$$

alors on dit que C est un *CSU minimal*. En particulier, si S ne possède aucune solution, alors $\emptyset$ est un CSU minimal pour S. Si C est un singleton, alors l'élément de C est appelé l'*unificateur le plus général*, ou mgu (pour *most general unifier*) de S. ◇

Lemme 2.3.8 (Lemme 10.1.6 de [BN98]) *Etant donné un problème de E-unification S, si C_1 et C_2 sont des CSU minimaux de S, alors C_1 et C_2 ont la même cardinalité.*

Définition 2.3.9 Soit E une théorie équationnelle, on dit que E est de type

- *unitaire* si et seulement si pour tout problème de E-unification S, il existe un CSU minimal pour S, et ce CSU est de cardinalité au plus 1,
- *finitaire* si et seulement si pour tout problème de E-unification S, il existe un CSU minimal pour S, et ce CSU est de cardinalité finie,
- *infinitaire* si et seulement si pour tout problème de E-unification S, il existe un CSU minimal pour S, et il existe un problème pour lequel ce CSU est de cardinalité infinie,
- *de type zéro* si et seulement s'il existe un problème de E-unification S qui ne possède pas de CSU minimal. ◇

Exemple 2.3.10 Voici les types de quelques théories équationnelles :

- La théorie vide est unitaire, puisque pour tout problème d'unification syntaxique S, soit S n'a aucune solution, soit S possède un mgu.
- Les théories de la commutativité et de l'associativité-commutativité sont toutes deux finitaires (voir [Sie79, Sti81, Fag84]).
- La théorie de l'associativité est de type infinitaire.
- Le premier exemple de théorie équationnelle de type zéro a été exhibé dans [FH86]. Il a ensuite été démontré simultanément dans [Baa87] et [SS87] que la théorie E définie par l'ensemble d'axiomes

$$A\ =\ \{f(x, f(y, z)) \rightleftharpoons f(f(x, y), z),\ f(x, x) \rightleftharpoons x\}$$

est de type zéro.

Les théories permutatives ne sont pas de type zéro

Nous allons maintenant prouver que les théories permutatives ne peuvent pas être de type zéro. Pour démontrer ce résultat, nous nous servirons du théorème suivant :

Théorème 2.3.11 (Théorème 3.1 de [Baa89]) *Soient une théorie équationnelle E, un ensemble de variables $\mathcal{X}$, et l'ensemble U des solutions d'un problème S d'unification modulo E. Si S n'admet pas de CSU minimal, alors il existe une chaîne descendante $u_1 \gtrsim_E^{\mathcal{X}} u_2 \gtrsim_E^{\mathcal{X}} \ldots$ dans U sans borne inférieure dans U.*

Dans ce qui suit, nous allons montrer que cette condition ne peut pas être remplie par un problème d'unification modulo une théorie permutative.

Propriété 2.3.12 *Soient θ et θ' deux substitutions telles que $\theta \lesssim_E^{\mathcal{X}} \theta'$, alors pour tout $x \in \mathcal{X}$, $|x\theta| \leq |x\theta'|$.*

PREUVE. Soit $x \in \mathcal{X}$, alors, comme $\theta \lesssim_E^{\mathcal{X}} \theta'$, il existe une substitution τ telle que $x\theta' =_E x\theta\tau$. Comme E est une théorie permutative, si deux termes sont égaux modulo E, alors ils sont de même taille, d'où

$$|x\theta'| \;=\; |x\theta\tau| \;\geq\; |x\theta|.$$

■

Définition 2.3.13 Soient un ensemble fini et ordonné de variables $\mathcal{X} = \{x_1, \ldots, x_n\}$ et une substitution θ dont le domaine est inclus dans $\mathcal{X}$, on définit la taille de θ par :

$$|\theta| \;=\; \langle |x_1\theta|, \ldots, |x_n\theta| \rangle.$$

Les tailles des substitutions sont ordonnées par l'extension lexicographique $\preceq$ de $\leq$. ◇

Corollaire 2.3.14 *Si $\theta \lesssim_E^{\mathcal{X}} \theta'$, alors $|\theta| \preceq |\theta'|$*

PREUVE. Ceci est une conséquence immédiate de la Propriété 2.3.12. ■

Lemme 2.3.15 *Il n'existe aucune chaîne infinie descendante de la forme $\theta_1 \gtrsim_E^{\mathcal{X}} \theta_2 \gtrsim_E^{\mathcal{X}} \ldots$ quand E est une théorie permutative.*

PREUVE. Supposons qu'une telle chaîne existe, alors, comme pour tout $i \in \mathbb{N}$, $|\theta_{i+1}| \preceq |\theta_i|$ d'après le Corollaire 2.3.14, il existe nécessairement un entier $n_0 \in \mathbb{N}$ tel que

$$i \geq n_0 \;\Rightarrow\; |\theta_{i+1}| = |\theta_i|.$$

Soient $i \geq n_0$, et μ_i la substitution telle que pour tout $x \in \mathcal{X}$, $x\theta_i =_E x\theta_{i+1}\mu_i$. Comme $|x\theta_i| = |x\theta_{i+1}|$, nécessairement, pour tout $y \in \mathrm{Var}(\mathrm{Ran}(\theta_{i+1}))$, l'image par μ_i de y est soit une variable, soit une constante.

Il est clair que μ_i ne peut pas être un renommage, sinon on aurait $\theta_i \lesssim_E^{\mathcal{X}} \theta_{i+1}$, il y a donc deux cas possibles : soit l'image par μ_i d'une des variables de $\mathrm{Var}(\mathrm{Ran}(\theta_{i+1}))$ est

une constante, soit deux variables distinctes de $\mathrm{Var}(\mathrm{Ran}(\theta_{i+1}))$ ont la même image par μ_i. Dans les deux cas, on a donc $|\mathrm{Var}(\mathrm{Ran}(\theta_{i+1}))| > |\mathrm{Var}(\mathrm{Ran}(\theta_i))|$, et comme

$$\forall i \geq n_0,\ |\mathrm{Var}(\mathrm{Ran}(\theta_i))| \ < \ \sum_{x\in\mathcal{X}} |x\theta_i| \ < \ \sum_{x\in\mathcal{X}} |x\theta_{n_0}|,$$

il ne peut pas exister de chaîne infinie descendante. ∎

Théorème 2.3.16 *Tout problème d'unification modulo une théorie équationnelle permutative admet un CSU minimal.*

PREUVE. D'après le Lemme 2.3.15, comme il n'existe aucune chaîne infinie descendante de la forme $\theta_1 \gtrsim_E^{\mathcal{X}} \theta_2 \gtrsim_E^{\mathcal{X}} \ldots$, toute chaîne descendante dans l'ensemble des solutions d'un problème d'unification modulo une théorie permutative est nécessairement finie, et admet donc un minimum qui est une borne inférieure dans cet ensemble de solutions. D'après le Théorème 2.3.11, on a le résultat. ∎

Corollaire 2.3.17 *Si E est une théorie équationnelle permutative, alors E est au plus de type infinitaire.*

2.4 Le problème SAT

Le problème SAT est le problème de décision suivant : étant donnée une formule booléenne F sous forme normale conjonctive, existe-t-il une interprétation I des variables de F qui satisfait F ? Il est bien connu que ce problème est **NP**-complet ([Coo71]), tout comme sa restriction 3-SAT, aux formules dont toutes les clauses sont de taille 3 (voir [GJ79]). Ces problèmes sont des cas particuliers des *problèmes de satisfaisabilité généralisés* (voir [Sch78]), et dans [Sch78], Schaefer a démontré un résultat de dichotomie sur ces derniers :

Théorème 2.4.1 (Théorème 2.1, p.217 de [Sch78]) *Tout problème de satisfaisabilité généralisé est soit dans* **P**, *soit* **NP**-*complet (à condition que* **P** $\neq$ **NP**). *De plus, on peut décider de la complexité d'un problème de satisfaisabilité généralisé en temps polynomial.*

Considérons maintenant le problème suivant :

> **Problème**: 1SURk+SAT
> **Entrée**: Un ensemble S de clauses positives, toutes de taille k, sur un ensemble fini de variables V
> **Question**: Existe-t-il une interprétation I de V qui 1-satisfait S, c'est-à-dire telle que pour tout $C \in S$, I satisfait exactement une variable dans C ?

Ce problème peut être modélisé comme un problème de satisfaisabilité généralisé, et le résultat de Schaefer permet de démontrer le résultat suivant :

Théorème 2.4.2 *Pour tout $k \geq 3$, le problème* 1SURk+SAT *est* **NP**-*complet.*

Chapitre 3

Théorie des groupes

Dans ce chapitre, nous allons formellement définir plusieurs notions de la théorie des groupes. Nous commencerons par définir des notions et prouver des propriétés générales sur les groupes, puis nous nous intéresserons particulièrement aux *groupes symétriques*. L'essentiel des résultats de ce chapitre sont standard, et sont développés dans tous les livres d'introduction à la théorie des groupes, comme [Sco64] ou [DF03]. Pour un résumé succinct voir [Tau97].

3.1 Groupes

Définition 3.1.1 (Groupe) Un *groupe* est un ensemble G muni d'une loi de composition interne $\star : G \times G \to G$, qui vérifie les propriétés suivantes :

1. *associativité :* pour tout $x, y, z \in G$, $(x \star y) \star z = x \star (y \star z)$,
2. existence d'un *élément neutre* $e_G \in G$ tel que $\forall x \in G$, $x \star e_G = e_G \star x = x$,
3. existence d'*inverses* : pour tout $x \in G$, il existe un $y \in G$ tel que $x \star y = y \star x = e_G$.

On note alors le groupe $(G, \star)$, ou simplement G s'il n'y a pas d'ambiguïté sur la loi de composition considérée.

Un groupe $(G, \star)$ est dit *abélien* si et seulement si pour tout $x, y \in G$, $x \star y = y \star x$, et *fini* si et seulement si l'ensemble G est fini. Si $(G, \star)$ est fini, alors on définit *l'ordre* ou *la cardinalité* de $(G, \star)$ comme étant la cardinalité de l'ensemble G. ◇

Remarque. Un groupe contient toujours un élément neutre, et est donc nécessairement non vide.

Exemple 3.1.2 Voici quelques exemples de groupes :

- Soit l'ensemble $\{e_G\}$, muni de la seule loi de composition possible : $e_G \star e_G = e_G$, alors $(\{e_G\}, \star)$ est un groupe, dont l'élément neutre est e_G. Ce groupe est nommé le *groupe trivial*, et est noté I.
- $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ sont des groupes abéliens, dont l'élément neutre est 0. Posons $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, alors $(\mathbb{Q}^*, \times)$ est également un groupe, mais pas $(\mathbb{Q}, \times)$, puisque l'élément 0 n'a pas d'inverse.

- Considérons $\mathrm{GL}_2(\mathbb{R})$, l'ensemble des matrices carrées de taille 2 inversibles, alors $(\mathrm{GL}_2(\mathbb{R}), \times)$ est un groupe.
- Soit A un ensemble, et notons $\mathrm{Sym}(A)$ l'ensemble des permutations de A, alors $(\mathrm{Sym}(A), \circ)$ est un groupe, appelé le *groupe symétrique* de A. Si $A = \{1, \ldots, n\}$, on pourra noter $\mathrm{Sym}(n)$ au lieu de $\mathrm{Sym}(A)$.

Propriété 3.1.3 *Soit G un groupe, et e un élément neutre de G, alors :*

1. *e est l'unique élément neutre de G,*
2. *pour tout $x \in G$, l'inverse de x est unique, on le note x^{-1},*
3. *pour tout $x, y, z \in G$, si $x \star z = y \star z$ (resp. $z \star x = z \star y$), alors $x = y$.*

Remarque. Si G est un groupe et s'il n'y a aucune confusion possible, on notera sa loi de composition "." ou "+". Dans le premier cas, on dira que G est "noté multiplicativement", et son neutre sera noté 1, et dans le deuxième, que G est "noté additivement", et son neutre sera noté 0. De plus, quand G est noté multiplicativement, on notera xy au lieu de $x.y$, et l'élément x^n représentera $x.x \cdots .x$ (où x apparaît n fois).

On se servira plus fréquemment de la notation multiplicative d'un groupe, la notation additive étant réservée aux groupes abéliens.

Etant donné un ensemble A, nous adopterons une notation particulière pour le groupe $\mathrm{Sym}(A)$.

Définition 3.1.4 Etant donné un ensemble A, nous noterons la loi de composition des fonctions inversement et multiplicativement pour les éléments de $\mathrm{Sym}(A)$, ce qui signifie que nous noterons $\sigma\sigma'$ au lieu de $\sigma' \circ \sigma$. Pour $a \in A$ et $\sigma \in \mathrm{Sym}(A)$, l'image de a par σ sera notée a^σ au lieu de $\sigma(a)$, avec notre convention, on a donc $a^{\sigma\sigma'} = (a^\sigma)^{\sigma'}$. ◇

3.2 Morphismes et actions de groupes

Nous allons maintenant présenter les notions de morphismes de groupes et d'action d'un groupe sur un ensemble, et étudier le lien entre ces deux notions.

Morphismes de groupes

Définition 3.2.1 (Morphisme de groupes) Soient $(G, \star)$ et $(H, \diamond)$ des groupes. Une fonction $\phi : G \to H$ est appelée un *morphisme de groupes* si et seulement si

$$\forall x, y \in G,\ \phi(x \star y) \ = \ \phi(x) \diamond \phi(y).$$

Si ϕ est une fonction bijective, on dira que ϕ est un *isomorphisme*, et on dira que $(G, \star)$ et $(H, \diamond)$ sont *isomorphes*, ce qu'on notera $G \simeq H$.

Si $(G, \star)$ et $(H, \diamond)$ sont identiques, on dira que ϕ est un *endomorphisme*. ◇

Exemple 3.2.2 Voici quelques exemples de morphismes de groupes :

- Il existe toujours au moins un morphisme de groupes entre deux groupes G et H : la fonction qui associe à chaque élément de G l'élément neutre de H. Ce morphisme est appelé le *morphisme trivial*.
- Pour tout groupe G, l'identité est un endomorphisme de G. Ce n'est cependant pas nécessairement le seul endomorphisme de G. Ainsi, soit $x \in G$, et considérons la fonction $c_x : G \to G$ qui à $g \in G$ associe xgx^{-1}. Pour g, h des éléments de G, on a

$$c_x(gh) = x(gh)x^{-1} = xg(x^{-1}x)hx^{-1} = (xgx^{-1})(xhx^{-1}) = c_x(g)c_x(h),$$

  c_x est donc également un endomorphisme de G, appelé *conjugaison par* x.
- La fonction logarithme est un isomorphisme de $(\mathbb{R}_+^*, \times)$ vers $(\mathbb{R}, +)$, mais ce n'est pas un endomorphisme.

On a les propriétés suivantes :

Théorème 3.2.3 *Soient G et H deux groupes, et ϕ un morphisme de G vers H, alors :*

1. $\phi(e_G) = e_H$,
2. $\forall x \in G$, $\phi(x^{-1}) = \phi(x)^{-1}$,
3. *si ϕ est un isomorphisme, alors ϕ^{-1} est également un isomorphisme,*
4. *si ψ est un morphisme de H vers K, alors $\psi \circ \phi$ est un morphisme de G vers K.*

PREUVE. 1. On a $\phi(e_G e_G) = \phi(e_G)\phi(e_G)$ par définition, et e_G étant l'élément neutre de G, on a $e_G e_G = e_G$, d'où $\phi(e_G)\phi(e_G) = \phi(e_G)$. D'après la Propriété 3.1.3, on en déduit que $\phi(e_G) = e_H$.
2. Soit $x \in G$, alors on a $\phi(xx^{-1}) = \phi(e_G)$, on en déduit donc que $\phi(x)\phi(x^{-1}) = e_H$, et comme l'inverse de $\phi(x)$ est unique, on a le résultat.
3. Posons $\psi = \phi^{-1}$, et montrons que ψ est un morphisme de groupes. Soient y et y' deux éléments de H, il s'agit de prouver que $\psi(yy') = \psi(y)\psi(y')$. Comme $\psi(y)$ et $\psi(y')$ sont des éléments de G, on a

$$\phi[\psi(y)\psi(y')] \;=\; \phi[\psi(y)]\phi[\psi(y')] \;=\; yy',$$

d'où $\psi \circ \phi[\psi(y)\psi(y')] = \psi(y)\psi(y') = \psi(yy')$.
4. Soient x et x' deux éléments de G, alors on a :

$$\psi(\phi(xx')) \;=\; \psi(\phi(x)\phi(x')) \;=\; \psi(\phi(x))\psi(\phi(x')),$$

d'où le résultat. ∎

Action d'un groupe sur un ensemble

Définition 3.2.4 (Action de groupe) Soit G un groupe et A un ensemble. Une *action de G sur A* est une fonction

$$\begin{cases} G \times A & \to A \\ (g, a) & \mapsto a.g \end{cases}$$

qui vérifie les propriétés suivantes :

- pour tout $g, g' \in G$ et pour tout $a \in A$, $(a.g).g' = a.(g.g')$,
- pour tout $a \in A$, $a.1 = a$. ◇

Exemple 3.2.5 Voici quelques exemples d'actions :
- Pour tout groupe G et tout ensemble A, la fonction qui à (g, a) associe a pour tout $g \in G$ et pour tout $a \in A$ est une action, appelée l'action *triviale*.
- Tout groupe G agit sur lui-même par *conjugaison*, en définissant la fonction $(x, g) \mapsto x^{-1}gx = c_x(g)$.
- Tout groupe G agit également sur lui-même par *translation à droite* (resp. *translation à gauche*), en définissant la fonction $(g, x) \mapsto xg$ (resp. $(g, x) \mapsto gx$).
- Pour tout ensemble A, le groupe $\mathrm{Sym}(A)$ agit de façon "naturelle" sur A, en définissant $(\sigma, a) \mapsto a^\sigma$.

On a le théorème suivant :

Théorème 3.2.6 *Soit G un groupe qui agit sur un ensemble A, et définissons la fonction*

$$\Psi : \begin{cases} G & \to \mathrm{Sym}(A) \\ g & \mapsto (a \mapsto a.g). \end{cases}$$

Alors Ψ est un morphisme de groupes.

Réciproquement, si ϕ est un morphisme de G vers $\mathrm{Sym}(A)$*, alors ϕ induit l'action $(g, a) \mapsto a^{\phi(g)}$.*

PREUVE. Pour un $g \in G$ donné, il est clair que la fonction $a \mapsto a.g$ est une bijection, et sa réciproque est la fonction $a \mapsto a.g^{-1}$, puisque $(a.g).g^{-1} = a.(g.g^{-1}) = a$, et de même, $(a.g^{-1}).g = a$. La fonction Ψ est donc bien définie.

Soient g, g' deux éléments de G, et notons respectivement σ et σ' leurs images par Ψ. Alors pour tout $a \in A$, on a

$$a^{\Psi(gg')} = (a.g).g' = (a^\sigma).g' = (a^\sigma)^{\sigma'} = a^{\sigma\sigma'} = a^{\Psi(g)\Psi(g')}.$$

Donc, Ψ est bien un morphisme de groupes.

Réciproquement, il est aisé de vérifier que pour tout morphisme ϕ de G vers $\mathrm{Sym}(A)$, la fonction $(g, a) \mapsto a^{\phi(g)}$ est une action de G sur A. ■

Ainsi, étant donnés un groupe G et un ensemble A, il est équivalent de définir une action de G sur A, ou un morphisme de G vers $\mathrm{Sym}(A)$. Par la suite, nous privilégierons la deuxième formulation, et définirons la plupart du temps les actions comme des morphismes.

Définition 3.2.7 Si G est un groupe agissant sur un ensemble A, et ϕ est le morphisme de G vers $\mathrm{Sym}(A)$ correspondant à cette action, on dira que ϕ est *morphisme associé à l'action de G sur A*, ou que *G agit par ϕ sur A*. ◇

Lemme 3.2.8 *Soient G un groupe, et A et A' deux ensembles tels que G agit sur A et sur A'. Alors G agit naturellement sur les ensembles 2^A et $A \times A'$. De plus, si A et A' sont disjoints, alors G agit naturellement sur $A \uplus A'$.*

PREUVE. Notons ϕ le morphisme de G vers $\mathrm{Sym}(A)$, et ψ le morphisme de G vers $\mathrm{Sym}(A')$. On définit les fonctions $\Psi_1 : G \to \mathrm{Sym}(2^A)$ et $\Psi_2 : G \to \mathrm{Sym}(A \times A')$ par :

$$\begin{array}{lll} \forall g \in G, \forall A_1 \subseteq A, & A_1^{\Psi_1(g)} & = \{a^{\phi(g)} \mid a \in A_1\}, \\ \forall g \in G, \forall \langle a, a' \rangle \in A \times A', & \langle a, a' \rangle^{\Psi_2(g)} & = \langle a^{\phi(g)}, a'^{\psi(g)} \rangle. \end{array}$$

Il est aisé de vérifier que Ψ_1 et Ψ_2 sont des morphismes de groupes.

Supposons maintenant que A et A' sont disjoints, alors on définit la fonction $\phi\psi$ de G vers $\mathrm{Sym}(A \uplus A')$ par : $\forall g \in G$, $\phi\psi(g) = \phi(g)\psi(g)$. Comme $A \cap A' = \emptyset$, on a $\phi(g)\psi(g) = \phi(g) \uplus \psi(g)$, d'où $\phi\psi = \psi\phi$. De plus, pour tout $g, h \in G$, on a :

$$\begin{array}{rcl} (\phi\psi)(gh) & = & \phi(gh)\psi(gh) \\ & = & \phi(g)\phi(h)\psi(g)\psi(h) \\ & = & \phi(g)\psi(g)\phi(h)\psi(h) \\ & = & \phi(gh)\psi(gh). \end{array}$$

Donc, $\phi\psi$ est bien un morphisme de groupes, d'où le résultat. ∎

Définition 3.2.9 (Orbite) Soit G un groupe agissant sur un ensemble A, et $a \in A$. On appelle *orbite* de a par G l'ensemble

$$a^G = \{a.g \mid g \in G\}.$$

On dit que l'action de G sur A est *transitive* si et seulement s'il existe un élément $a \in A$ tel que $a^G = A$. ◇

Définition 3.2.10 (Régularité, semi-régularité) Soit G un groupe d'élément neutre e_G, agissant sur un ensemble A. On dit que l'action de G sur A est :

- *semi-régulière* si et seulement si pour tout $a \in A$, $a.g = a \Rightarrow g = e_G$,
- *régulière* si et seulement si elle est semi-régulière et transitive. ◇

Exemple 3.2.11 Reprenons les actions de l'Exemple 3.2.5, alors on a :

- L'orbite de tout élément $a \in A$ par l'action triviale est égale à $\{a\}$.
- Supposons que G agit sur lui-même par conjugaison, et soit $h \in G$. L'orbite de h est nommée sa *classe de conjugaison*, c'est l'ensemble des éléments h' tels qu'il existe un élément $g \in G$ tel que $gh = h'g$.
- Soient h et h' deux éléments de G, où on suppose que G agit sur lui-même par translation à droite, alors on a $h' = h(h^{-1}h')$, ce qui prouve que $h' \in h^G$, et donc $h^G = G$. La translation à droite de G sur G est une action transitive. De plus, si $hh' = h$, alors nécessairement $h' = e_G$, et la translation à droite est donc une action régulière.

– Considérons le groupe $\mathrm{Sym}(A)$ et son action naturelle sur A, alors, pour tout $a' \in A$, il est clair qu'il existe une permutation de A qui associe a' à a, et donc, $a^{\mathrm{Sym}(A)} = A$.

On a les propriétés suivantes :

Théorème 3.2.12 *Soit G un groupe agissant sur un ensemble A, alors on a :*

1. *l'ensemble des orbites de A sous l'action de G forme une partition de A,*
2. *pour tout $a \in A$, l'action de G sur A induit une action transitive de G sur a^G.*

PREUVE. Nous commençons par prouver que pour tout $a' \in a^G$, on a $a'^G = a^G$. Soit $a' \in a^G$, alors il existe $g \in G$ tel que $a' = a.g$. On en déduit que pour tout $h \in G$, on a $a'.h = (a.g).h = a.(gh) \in a^G$, d'où $a'^G \subseteq a^G$. Comme $a' = a.g$, on a $a = a'.g^{-1}$, et $a \in a'^G$, par symétrie, on en déduit donc que $a'^G = a^G$.
1. Soient a et a' deux éléments de A, il s'agit de prouver que soit $a^G \cap a'^G = \emptyset$, soit $a^G = a'^G$. Supposons que $a^G \cap a'^G \neq \emptyset$, alors il existe $a'' \in a^G \cap a'^G$, et d'après ce qui précède, on a $a^G = a''^G = a'^G$, d'où le résultat.
2. Tous les axiomes de l'action de groupe sont vérifiés sur les éléments de a^G, puisqu'ils le sont sur A, et d'après ce qui précède, on a $a'.g \in a^G$, pour tout $g \in G$ et pour tout $a' \in a^G$. Il est alors évident que l'action induite est transitive, d'après la définition de l'orbite de a. ∎

Comme l'ensemble des orbites de A forme une partition de A, on en déduit que

Corollaire 3.2.13 *L'action de G sur A est transitive si et seulement si $a^G = A$ pour tout $a \in A$.*

3.3 Sous-groupes

Définition 3.3.1 (Sous-groupe) Soit G un groupe, et H un sous-ensemble non vide de G. On dit que H est un *sous-groupe* de G, ce qu'on note $H \leq G$, si et seulement si H est stable par multiplication et par inverse, c'est-à-dire que pour tout $x, y \in H$, $x^{-1} \in H$ et $xy \in H$. ◇

Exemple 3.3.2 Voici quelques exemples de sous-groupes :
– Tout groupe G possède deux sous-groupes : le groupe trivial, et G lui-même.
– On a $(\mathbb{Q}, +) \leq (\mathbb{R}, +)$, $(\mathbb{Q}^*, \times) \leq (\mathbb{R}^*, \times)$ et $(\mathbb{Q}_+^*, \times) \leq (\mathbb{R}_+^*, \times)$. Par contre, $(\mathbb{Q}, +) \not\leq (\mathbb{R}^*, \times)$, et $(\mathbb{Q}^*, \times) \not\leq (\mathbb{R}_+^*, \times)$.

Les critères suivants permettent de s'assurer qu'un ensemble est un sous-groupe :

Propriété 3.3.3 *Soient G un groupe et $H \subseteq G$, alors H est un sous-groupe de G si et seulement si H est non vide et, pour tout $x, y \in H$, $xy^{-1} \in H$.*

De plus, si H est fini, alors H est un sous-groupe de G si et seulement si H est non vide et pour tout $x, y \in H$, $xy \in H$.

Nous pouvons naturellement définir des actions de H sur G :

Exemple 3.3.4 Tout sous-groupe H de G agit sur G par translation à droite et par translation à gauche.

Nous donnons maintenant d'autres exemples de sous-groupes d'un groupe quelconque.

Définition 3.3.5 (Ker(ϕ) et $\phi(G)$) Soient G et H deux groupes, et ϕ un morphisme de G vers H. On définit les ensembles suivants :

$$\mathrm{Ker}(\phi) \;=\; \{g \in G \,|\, \phi(g) = e_H\}, \text{ et } \phi(G) \;=\; \{\phi(g) \,|\, g \in G\}. \qquad \diamond$$

Théorème 3.3.6 *Soit ϕ un morphisme de groupes de G vers H. Alors :*

1. $\mathrm{Ker}(\phi)$ *est un sous-groupe de G, et $\phi(G)$ est un sous-groupe de H.*
2. *Si G est un groupe abélien, alors $\phi(G)$ est un groupe abélien.*

PREUVE. 1. Comme $\phi(e_G) = e_H$, $\mathrm{Ker}(\phi)$ est non vide. Soient x et y deux éléments de $\mathrm{Ker}(\phi)$, on a donc $\phi(x) = \phi(y) = e_H$. On en déduit que $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} = e_H$, d'où $xy^{-1} \in \mathrm{Ker}(\phi)$.

De même, $\phi(G)$ est non vide, puisque $e_H = \phi(e_G) \in \phi(G)$. Soient $h, h' \in \phi(G)$, il existe donc des éléments g et g' dans G tels que $h = \phi(g)$ et $h' = \phi(g')$. On a donc $hh^{-1} = \phi(g)\phi(g')^{-1} = \phi(gg'^{-1})$, d'où $hh^{-1} \in \phi(G)$.

2. Supposons que G est abélien, et soient $\phi(g)$ et $\phi(g')$ deux éléments de $\phi(G)$, alors on a

$$\phi(g)\phi(g') \;=\; \phi(gg') \;=\; \phi(g'g) \;=\; \phi(g')\phi(g), \qquad \blacksquare$$

d'où le résultat.

Le sous-groupe $\mathrm{Ker}(\phi)$ peut jouer un rôle important lors de l'étude des propriétés de ϕ, on a en effet la propriété suivante :

Propriété 3.3.7 *Soit ϕ un morphisme de groupes de G vers H, alors ϕ est injectif si et seulement si* $\mathrm{Ker}(\phi) = \{e_G\}$.

PREUVE. Supposons que $\mathrm{Ker}(\phi) = \{e_G\}$, et soient $x, y \in G$ tels que $\phi(x) = \phi(y)$. Alors on a $\phi(x)\phi(y)^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) = e_H$, d'où $xy^{-1} \in \mathrm{Ker}(\phi)$. On en déduit que $xy^{-1} = e_G$, donc $x = y$. La réciproque est triviale. $\blacksquare$

On peut en déduire le résultat suivant :

Théorème 3.3.8 *Si l'action de G sur A est semi-régulière, alors le morphisme correspondant ϕ est injectif, et on a pour tout $a \in A$, $|a^G| = |G|$.*

PREUVE. Soit $g \in \mathrm{Ker}(\phi)$, alors par définition, on a pour tout $a \in A$, $a.g = a$, d'où $g = e_G$, et d'après la Propriété 3.3.7, ϕ est injective. Soient $a \in A$, et g et h deux éléments de G tels que $a.g = a.h$. Alors on a $a.(gh^{-1}) = a$, et par hypothèse de semi-régularité, $gh^{-1} = e_G$. On en déduit que $g = h$, et $|a^G| = |G|$. $\blacksquare$

Définition 3.3.9 Soient G un groupe agissant sur un ensemble A et $A' \subseteq A$, on définit les ensembles suivants :

$$G_{[A']} = \{g \in G \,|\, \forall a \in A', a.g = a\}, \text{ et } \mathrm{Stab}_G(A') = \{g \in G \,|\, A'.g = A'\}.$$

L'ensemble $G_{[A']}$ est appelé le *fixateur de A' dans A*. Si $A' = \{a\}$, on notera $G_{[a]}$ au lieu de $G_{[\{a\}]}$. ◇

Propriété 3.3.10 *Pour tout $A' \subseteq A$, $G_{[A']}$ et $\mathrm{Stab}_G(A')$ sont des sous-groupes de G.*

On a également la propriété suivante :

Propriété 3.3.11 *Soient A un ensemble sur lequel agit un groupe G, et A' et A'' deux ensembles tels que $A'' \subseteq A' \subseteq A$. Alors $G_{[A']}$ est un sous-groupe de $G_{[A'']}$.*

Remarque. Si $A' \subseteq A$, alors $\mathrm{Stab}_G(A)$ n'est pas nécessairement un sous-groupe de $\mathrm{Stab}_G(A')$. Ainsi, si on considère l'ensemble $A = \{1, \ldots, 5\}$ sur lequel on considère l'action naturelle de $G = \mathrm{Sym}(5)$ et on pose $A' = \{5\}$, alors $\mathrm{Stab}_G(A) = G$, et $\mathrm{Stab}_G(A') = \mathrm{Sym}(4)$.

Nous définissons maintenant la notion très employée par la suite de *sous-groupe engendré*. Nous commençons par énoncer une propriété sur l'intersection de sous-groupes :

Propriété 3.3.12 *Soit G un groupe, et $\mathcal{A}$ un ensemble de sous-groupes de G. Alors l'ensemble*

$$K = \bigcap_{H \in \mathcal{A}} H$$

est un sous-groupe de G.

Définition 3.3.13 (Sous-groupe engendré) Etant donnés un groupe G et un ensemble $A \subseteq G$, on définit le *sous-groupe de G engendré par A* par :

$$< A > = \bigcap_{A \subseteq H, H \leq G} H.$$

Les éléments de A sont alors appelés les *générateurs* de $< A >$, et on dit que A est un *ensemble générateur* de $< A >$. ◇

On peut de plus construire de façon explicite le groupe $< A >$:

Propriété 3.3.14 *Soient G un groupe, et $A \subseteq G$, alors*

$$< A > = \{a_1 \ldots a_n \,|\, n \in \mathbb{N} \wedge \forall i = 1, \ldots, n, \{a_i, a_i^{-1}\} \cap A \neq \emptyset\} \cup \{e_G\}.$$

De plus, si G est un groupe fini, alors on a

$$< A > = \{a_1 \ldots a_n \,|\, n \in \mathbb{N} \wedge \forall i = 1, \ldots, n, a_i \in A\} \cup \{e_G\}.$$

Exemple 3.3.15 Le groupe $(\mathbb{Z}, +)$ est engendré par l'élément 1.

Propriété 3.3.16 *Soient G et H deux groupes, et ϕ un morphisme de groupes de G vers H. Soit $A \subseteq G$ tel que G est engendré par A, alors $\phi(G)$ est engendré par l'ensemble $\phi(A)$.*

Une propriété importante des groupes symétriques finis est qu'ils peuvent être engendrés par deux générateurs seulement :

Propriété 3.3.17 *Soit $A = \{a_1, \ldots, a_n\}$ un ensemble fini, alors le groupe* $\mathrm{Sym}(A)$ *est engendré par les permutations $(a_1\ a_2)$ et $(a_2\ \cdots\ a_n)$.*

Définition 3.3.18 (Groupe cyclique, ordre d'un élément) Soient G un groupe, et $x \in G$. On appelle *groupe cyclique engendré par x* le groupe engendré par le singleton $\{x\}$, qu'on note $< x >$.

L'*ordre* de x, noté $|x|$, est la cardinalité du groupe $< x >$. ◇

Exemple 3.3.19 Pour tout groupe G, l'identité de G est d'ordre 1, et dans le groupe $(\mathbb{Z}, +)$, tout élément différent de 0 est d'ordre infini.

Considérons le groupe $\mathrm{GL}_2(\mathbb{R})$, et soient les éléments

$$M_1 \ = \ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ et } M_2 \ = \ \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix},$$

alors on a $M_1^2 = M_2^2 = \mathrm{id}$, et ces éléments sont donc d'ordre 2, mais il est aisé de voir que l'élément $M_3 = M_1 M_2$ est d'ordre infini.

Propriété 3.3.20 *Soit $x \in G$ un élément d'ordre n, alors le groupe $< x >$ est isomorphe à $(\mathbb{Z}_n, +_n)$.*

Définition 3.3.21 (Classes à gauche et à droite) Soient G un groupe, H un sous-groupe de G, et g un élément de G, alors les ensembles

$$gH \ = \ \{gh \,|\, h \in H\} \text{ et } Hg \ = \ \{hg \,|\, h \in H\}$$

sont respectivement appelés *classe à gauche* et *classe à droite* de H dans G. Tout élément d'une classe est appelé un *représentant* de cette classe. ◇

Propriété 3.3.22 *Soient G un groupe, et $H \leq G$, on a les propriétés suivantes :*

1. *L'ensemble des classes à gauche (resp. à droite) de H dans G forme une partition de G.*
2. *Pour tout $g, g' \in G$, on a*

$$gg' \in H \ \Leftrightarrow \ g \in Hg'^{-1} \ \Leftrightarrow \ g' \in g^{-1}H.$$

PREUVE. 1. Prenons le cas de l'ensemble des classes à gauche, la démonstration est similaire pour l'ensemble des classes à droite. Ce résultat est évident, il suffit de constater que si $g \in G$, alors gH est exactement l'orbite de g sous l'action de translation à droite de H sur G, et on a le résultat d'après le Théorème 3.2.12.
2. Supposons que $gg' \in H$, et posons $gg' = h$, alors on a $g = hg'^{-1}$ et $g' = g^{-1}h$. Donc, $g \in Hg'^{-1}$ et $g' \in g^{-1}H$. De même, il est aisé de vérifier que si $g \in Hg'^{-1}$ (resp. $g' \in g^{-1}H$), alors $gg' \in H$. ∎

Lemme 3.3.23 *Soit G un groupe agissant sur un ensemble A, et soit $a \in A$. Soit $G_{[a]}g$ une classe à droite de $G_{[a]}$ dans G, alors pour tout $h \in G$, h est élément de $G_{[a]}g$ si et seulement si $a.h = a.g$.*

PREUVE. Soit $h \in G_{[a]}g$, alors il existe un élément $h' \in G_{[a]}$ tel que $h = h'g$, et on a $a.h = a.(h'g) = (a.h').g = a.g$. Réciproquement, si $a.h = a.g$, alors $(a.h).g^{-1} = a.(hg^{-1}) = a$, d'où $hg^{-1} \in G_{[a]}$, et on a le résultat. ∎

Définition 3.3.24 Si G est un groupe et H est un sous-groupe de G, on appelle *indice de H dans G*, et on note $(G : H)$ le nombre (éventuellement infini) de classes à gauche de H dans G.

Un sous-ensemble T de G est appelé un *transversal droit* (resp. *transversal gauche*) de H dans G si et seulement si T contient un et un seul élément de chaque classe à droite (resp. classe à gauche) de G. ◇

Exemple 3.3.25 Soient G un groupe, alors un transversal gauche de I dans G est égal à G, et l'indice de I dans G est égal à l'ordre de G.

Théorème 3.3.26 (Théorème de Lagrange) *Si G est un groupe fini et H est un sous-groupe de G, alors on a*

$$|G| \;=\; |H|\,(G : H),$$

et donc, l'ordre de H et l'indice de H dans G divisent tous deux l'ordre de G.

PREUVE. Comme l'ensemble des classes à gauche de H dans G est une partition de G d'après la Propriété 3.3.22, il nous suffit de démontrer que l'ensemble de ces classes est une équipartition de G. Comme la translation à droite de H sur G est une action semi-régulière, les orbites des éléments de G ont tous la même cardinalité que H d'après le Théorème 3.3.8, d'où le résultat. ∎

Définition 3.3.27 (Classe au centre) Soient G un groupe, H et H' deux sous-groupes de G, et $g \in G$. On appelle *classe au centre de g par (H, H') dans G*, et on note HgH', l'ensemble $\{hgh' \mid h \in H,\, h' \in H'\}$. ◇

Propriété 3.3.28 *L'ensemble des classes au centre forment une partition de G.*

3.4 Les groupes symétriques

Nous allons maintenant nous intéresser plus particulièrement aux groupes symétriques finis.

Définition 3.4.1 Soient A un ensemble de cardinalité n, et G un sous-groupe de $\mathrm{Sym}(A)$, alors on dit que G est un *groupe de permutation de degré* n.

Le *support* d'une permutation $\sigma \in \mathrm{Sym}(A)$ est l'ensemble des éléments a de A tels que $a^\sigma \neq a$. Le *support* d'un groupe de permutation G est l'union des supports des éléments de G. ◇

L'intérêt des groupes symétriques est qu'ils sont aisés à représenter. De plus, on a les résultats suivants :

Propriété 3.4.2 *Soit A un ensemble de cardinalité n, alors* $\mathrm{Sym}(A)$ *est isomorphe à* $\mathrm{Sym}(n)$.

Théorème 3.4.3 (Théorème de Cayley) *Tout groupe G est isomorphe à un sous-groupe de* $\mathrm{Sym}(G)$.

PREUVE. L'action de translation à droite de G sur G est une action semi-régulière, et le mophisme ϕ correspondant est donc injectif d'après le Théorème 3.3.8. Donc, ϕ est un isomorphisme de G vers $\phi(G)$, d'où le résultat. ■

Ainsi, il n'y a aucune perte de généralité si on se restreint à l'étude des groupes de permutation. De plus, d'après la Propriété 3.4.2, nous pouvons nous restreindre à l'étude des groupes de permutation sur les ensembles $\{1, \ldots, n\}$, où $n \in \mathbb{N}$.

On a également la propriété standard suivante :

Propriété 3.4.4 *Toute permutation peut être représentée comme un produit de cycles disjoints, et deux permutations à supports disjoints commutent.*

Exemple 3.4.5 Considérons l'ensemble $A = \{1, \ldots, 6\}$, et soit la permutation σ définie par :

i	1	2	3	4	5	6
i^σ	6	2	4	5	3	1

Alors σ s'écrit sous forme du produit de cycles disjoints suivant (où par convention, on ne note pas les cycles triviaux) : $\sigma = (1\ 6)(3\ 4\ 5) = (3\ 4\ 5)(1\ 6)$.

Remarque. Dans la suite, par abus de notation, si $A \subseteq A'$ et $\sigma \in \mathrm{Sym}(A)$, alors on confondra σ avec la permutation dans $\mathrm{Sym}(A')$ qui fixe tous les éléments de $A' \setminus A$, et dont la restriction à A est égale à σ. Ainsi, si G est un sous-groupe de $\mathrm{Sym}(A)$, on pourra également considérer G comme un sous-groupe de $\mathrm{Sym}(A')$.

Lemme 3.4.6 *Soient G et G' deux sous-groupes de* $\mathrm{Sym}(A)$*, et supposons que G et G' sont à supports disjoints. Alors l'ensemble*

$$GG' \;=\; \{\sigma\sigma' \mid \sigma \in G \wedge \sigma' \in G'\}$$

est un sous-groupe de $\mathrm{Sym}(A)$.

PREUVE. Soient $\sigma_1\sigma_1'$ et $\sigma_2\sigma_2'$ deux éléments de GG', alors, comme G et G' sont à supports disjoints, on a : $\forall\sigma \in G$, $\forall\sigma' \in G'$, $\sigma\sigma' = \sigma'\sigma$. On a donc

$$(\sigma_1\sigma_1')(\sigma_2\sigma_2')^{-1} \;=\; \sigma_1\sigma_1'\sigma_2'^{-1}\sigma_2^{-1} \;=\; \sigma_1\sigma_1'\sigma_2^{-1}\sigma_2'^{-1} \;=\; \sigma_1\sigma_2^{-1}\sigma_1'\sigma_2'^{-1},$$

donc $(\sigma_1\sigma_1')(\sigma_2\sigma_2')^{-1}$ est bien élément de GG', d'où le résultat. ∎

Remarque. Il ne faut pas confondre le groupe GG' avec le groupe $G \times G'$.

Corollaire 3.4.7 *Soient G un sous-groupe de* $\mathrm{Sym}(A)$*, et $G_1, \ldots, G_m$ des sous-groupes de G à supports disjoints deux à deux. Alors :*

1. *L'ensemble $H = \prod_{i=1}^{m} G_i$ est également un sous-groupe de G, et pour tout $i = 1, \ldots, m$, G_i est un sous-groupe de H.*
2. *Si pour tout $i = 1, \ldots, m$, G_i est engendré par l'ensemble S_i, alors $\prod_{i=1}^{m} G_i$ est engendré par l'ensemble $\biguplus_{i=1}^{m} S_i$.*
3. *Si pour tout $i = 1, \ldots, m$, G_i est abélien, alors H l'est également.*

Lemme 3.4.8 *Soient $A = \{a_1, \ldots, a_n\}$, G un sous-groupe de* $\mathrm{Sym}(A)$*, pour $i \in \{1, \ldots, n\}$, posons $G_i = G_{[\{a_1,\ldots,a_i\}]}$, et posons $G_0 = G$. Pour $i = 1, \ldots, n$, soit U_i un transversal droit de G_i dans G_{i-1}, alors, pour tout $r \in \{1, \ldots, n\}$, l'ensemble $K_r = \bigcup_{i=r}^{n} U_i$ est un ensemble générateur de G_{r-1}.*

PREUVE. Nous démontrons le résultat par induction descendante sur r. Comme $G_n = \mathrm{I}$, on a $K_n = U_n = G_{n-1}$, et K_n est bien un ensemble générateur de G_{n-1}. Supposons maintenant que K_{r+1} engendre G_r, et soit $\pi \in G_{r-1}$. Alors il existe une permutation $\psi \in U_r$ telle que $\pi \in G_r\psi$, et donc, $\pi\psi^{-1} \in G_r$. On en déduit que $\pi\psi^{-1}$ est un produit d'éléments de K_{r+1}, et donc, π est bien un produit d'éléments de K_r. ∎

Corollaire 3.4.9 *Sous les hypothèses du Lemme 3.4.8, le groupe G a un ensemble de générateurs de taille $O(n^2)$. Donc, tout groupe de permutation de degré n a un ensemble de générateurs de taille $O(n^2)$.*

PREUVE. D'après le Lemme 3.4.8, l'ensemble K_1 est un ensemble générateur de G, et pour tout $a \in A$, on a $a^G \subseteq A$. Soit $i \in \{1, \ldots, n\}$, et considérons σ et μ, deux éléments distincts du transversal droit U_i. Alors, pour tout $j = 1, \ldots, i-1$, on a $a_j^\sigma = a_j^\mu$. Supposons que $a_i^\sigma = a_i^\mu$, alors $a_i^{\sigma\mu^{-1}} = a_i$ et donc, $\sigma\mu^{-1} \in G_i$, et $G_i\sigma = G_i\mu$, ce qui contredit l'hypothèse que U_i est un transversal droit. On en déduit que $a_i^\sigma \neq a_i^\mu$, donc, $|U_i| \leq |a_i^G| \leq n$, d'où le résultat. ∎

Nous prouvons enfin plusieurs propriétés vérifiées par des groupes de permutation sur deux ensembles disjoints de même cardinalité

Lemme 3.4.10 *Soient $A = \{a_1, \ldots, a_n\}$ et $B = \{b_1, \ldots, b_n\}$ deux ensembles disjoints de même cardinalité finie, G_A un sous-groupe de $\mathrm{Sym}(A)$, et posons $\pi = \prod_{i=1}^{n}(a_i\ b_i)$. Alors pour tout $\sigma, \mu \in G_A$, on a $\pi\sigma\pi\mu = \mu\pi\sigma\pi$.*

PREUVE. Soit $a_i \in A$, et posons $a_i^{\mu} = a_k$, alors on a :

$$\begin{aligned} a_i^{\pi\sigma\pi\mu} &= b_i^{\sigma\pi\mu} = b_i^{\pi\mu} = a_k, \\ a_i^{\mu\pi\sigma\pi} &= a_k^{\pi\sigma\pi} = b_k^{\sigma\pi} = a_k. \end{aligned}$$

De même, soit $b_j \in B$, et posons $a_j^{\sigma} = a_l$, alors on a :

$$\begin{aligned} b_j^{\pi\sigma\pi\mu} &= a_j^{\sigma\pi\mu} = a_l^{\pi\mu} = b_l^{\mu} = b_l, \\ b_j^{\mu\pi\sigma\pi} &= b_j^{\pi\sigma\pi} = a_j^{\sigma\pi} = a_l^{\pi} = b_l. \end{aligned}$$

Donc, on a bien $\pi\sigma\pi\mu = \mu\pi\sigma\pi$. ∎

Lemme 3.4.11 *Sous les hypothèses du Lemme 3.4.10, posons $G_B = \pi G_A \pi$, et notons G le groupe engendré par $G_A \cup \{\pi\}$. Alors on a $G = G_A G_B \uplus G_A \pi G_A$.*

PREUVE. D'après la Propriété 3.3.14, on a

$$G = \{\mu_1\pi\mu_2\pi \ldots \pi\mu_k \mid k \in \mathbb{N} \wedge \mu_i \in G_A\}.$$

On pose $G = H_1 \cup H_2$, où

$$\begin{aligned} H_1 &= \{\mu_1\pi \ldots \pi\mu_{2n+1} \mid n \in \mathbb{N} \wedge \mu_i \in G_A\}, \\ H_2 &= \{\mu_1\pi \ldots \pi\mu_{2n} \mid n \in \mathbb{N} \wedge \mu_i \in G_A\}. \end{aligned}$$

L'ensemble H_1 est donc constitué des éléments de G engendrés par un nombre pair d'occurrences de π, et l'ensemble H_2 de ceux engendrés par un nombre impair d'occurrences de π. Il est aisé de vérifier que H_1 et H_2 sont disjoints. Montrons que

$$H_1 = \{(\mu_1\mu_3 \ldots \mu_{2n+1})\,\pi\,(\mu_2\mu_4 \ldots \mu_{2n})\,\pi \mid n \in \mathbb{N} \wedge \mu_i \in G_A\} = G_A\, G_B.$$

Soit $\sigma \in H_1$, on montre par induction sur n que σ est bien de la forme requise. Pour $n = 0$, le résultat est évident. Supposons maintenant que le résultat est vrai pour $n-1$, et que

$$\sigma = \mu_1\pi \ldots \mu_{2n-1}\pi\mu_{2n}\pi\mu_{2n+1}.$$

Par hypothèse d'induction, on a alors

$$\begin{aligned} \sigma &= (\mu_1\mu_3 \ldots \mu_{2n-1})\,\pi\,(\mu_2\mu_4 \ldots \mu_{2n-2})\,\pi\,(\pi\mu_{2n}\pi\mu_{2n+1}) \\ &= \sigma_1\pi\sigma_2(\pi\mu_{2n+1}), \end{aligned}$$

où $\sigma_1 = \mu_1\mu_3 \dots \mu_{2n-1}$, et $\sigma_2 = \mu_2\mu_4 \dots \mu_{2n}$. D'après le Lemme 3.4.10 on a donc

$$\sigma \;=\; \sigma_1(\mu_{2n+1}\pi\sigma_2\pi) \;=\; (\mu_1\mu_3 \dots \mu_{2n+1})\,\pi\,(\mu_2\mu_4 \dots \mu_{2n})\,\pi,$$

d'où le résultat.

Un raisonnement similaire montre que

$$H_2 \;=\; \{(\mu_1\mu_3 \dots \mu_{2n-1})\,\pi\,(\mu_2\mu_4 \dots \mu_{2n}) \mid n \in \mathbb{N}\} \;=\; G_A\,\pi\,G_A,$$

et on a bien $G = G_AG_B \uplus G_A\pi G_A$ ∎

Théorème 3.4.12 *Soient $A = \{a_1, \dots, a_n\}$ et $B = \{b_1, \dots, b_n\}$ deux ensembles disjoints de même cardinalité finie, G_A un sous-groupe de* $\mathrm{Sym}(A)$*, et posons $\pi = \prod_{i=1}^{n}(a_i\ b_i)$. Soient G le groupe engendré par $G_A \cup \{\pi\}$, $k \in \{1, \dots, n\}$, et supposons qu'il existe une permutation $\sigma \in G$ telle que pour tout $i = 1, \dots, k$, on a $a_i^\sigma = b_{j_i}$. Alors il existe une permutation $\mu \in G_A$ telle que pour tout $i = 1, \dots, k$, $a_i^\mu = a_{j_i}$.*

PREUVE. D'après le Lemme 3.4.11, on a $G = G_AG_B \uplus G_A\pi G_A$, et comme $G_AG_B \subseteq \mathrm{Sym}(A)\mathrm{Sym}(B)$, nécessairement, σ est élément de $G_A\pi G_A$. La permutation σ est donc de la forme $\sigma = \mu\pi\sigma'$, où μ et σ' sont éléments de G_A. Soit $i \in \{1, \dots, k\}$, et posons $a_l = a_i^\mu$, alors on a :

$$a_i^\sigma \;=\; a_i^{\mu\pi\sigma'} \;=\; a_l^{\pi\sigma'} \;=\; b_l^{\sigma'} \;=\; b_l,$$

donc, comme $a_i^\sigma = b_{j_i}$, on en déduit que $l = j_i$, ce qui prouve que $a_i^\mu = a_{j_i}$. ∎

Conjugaison d'un groupe de permutation

Définition 3.4.13 (Conjugaison) Soient A et B deux ensembles, $f : A \to B$ une fonction, et $A' \subseteq A$ tel que la restriction de f à A' est injective. Pour tout $\sigma \in \mathrm{Sym}(A)$, on définit le *conjugué par f de σ dans A'*, noté $\sigma^f_{A'}$ de la façon suivante : si le support de σ n'est pas inclus dans A', alors $\sigma^f_{A'} = \mathrm{id}_B$, sinon, notons f' la restriction de f à A', alors

$$\forall b \in B,\ b^{\sigma^f_{A'}} = \begin{cases} f'([f'^{-1}(b)]^\sigma) & \text{si } b \in f(A'), \\ b & \text{sinon.} \end{cases}$$

S'il n'y a pas d'ambiguïté sur l'ensemble A', alors on pourra simplement parler du conjugué par f de σ, ce qu'on notera σ^f.

On note alors $G^f_{A'} = \{\sigma^f_{A'} \mid \sigma \in G\}$. ◇

Exemple 3.4.14 Voici quelques exemples de conjugaison :

1. Soient $A = \{1, 2, 3, 4\}$, $B = \{5, 6, 7, 8\}$ et considérons la fonction f définie par :

i	1	2	3	4
$f(i)$	5	6	7	7

   Soit $A' = \{1, 2, 3\}$ et posons $\sigma = (1\ 3\ 2)$, alors $\sigma^f_{A'} = (5\ 7\ 6)$. Soit $A'' = \{1, 2, 4\}$ et $\sigma' = (1\ 4\ 2)$, alors $\sigma'^f_{A''} = (5\ 7\ 6)$.

2. Soit $\mu \in \mathrm{Sym}(A)$, alors pour tout $\sigma \in \mathrm{Sym}(A)$, on a $\sigma_A^\mu = \mu^{-1}\sigma\mu$.

Définition 3.4.15 (Transformation affine d'un groupe) Soient A un ensemble, a un élément de A, $L \subseteq A^\star$, et $G < \mathrm{Sym}(L)$. Notons $f : L \to a.L$ la bijection qui à tout $w \in L$ associe $a.w$, alors le groupe $a.G$ est défini par $a.G = G^f$. ◇

Exemple 3.4.16 Soient $A = \{a, b, c\}$, $L = \{bc, cb\}$, et $G = < (bc\ cb) >$. Alors on a $a.G = < (abc\ acb) >$.

Propriété 3.4.17 *Soient A et B deux ensembles, $f : A \to B$, et soient l'ensemble A' et la fonction f' comme dans la Définition 3.4.13. Alors pour tout $\sigma \in \mathrm{Sym}(A)$, $\sigma^f \in \mathrm{Sym}(B)$.*

PREUVE. Il s'agit de prouver que σ^f est une fonction injective. Le résultat est immédiat si le support de σ n'est pas inclus dans A', supposons maintenant que ça soit le cas. Soient b et b' deux éléments de B, et supposons que $b^{\sigma^f} = b'^{\sigma^f}$. Alors, par définition de σ^f, b et b' sont tous deux éléments soit de $f(A')$, soit de $B \setminus f(A')$.

Si b et b' sont éléments de $B \setminus f(A')$, alors $b^{\sigma^f} = b$ et $b'^{\sigma^f} = b'$, et le résultat est immédiat.

Supposons maintenant que b et b' sont éléments de $f(A')$, alors on a

$$\begin{array}{lcccl} b^{\sigma^f} = b'^{\sigma^f} & \Rightarrow & f'([f'^{-1}(b)]^\sigma) & = & f'([f'^{-1}(b')]^\sigma) & \\ & \Rightarrow & [f'^{-1}(b)]^\sigma & = & [f'^{-1}(b')]^\sigma & (\text{car } f' \text{ est bijective}) \\ & \Rightarrow & f'^{-1}(b) & = & f'^{-1}(b') & (\text{car } \sigma \in \mathrm{Sym}(A)) \\ & \Rightarrow & b & = & b' & (\text{car } f \text{ est bijective}). \end{array}$$ ∎

Propriété 3.4.18 *Soient A, B et C trois ensembles, $f : A \to B$, $g : B \to C$, et $\sigma, \pi \in \mathrm{Sym}(A)$. Soit $A' \subseteq A$ tel que la restriction à A' de f est injective, et supposons que la restriction de g à $B' = f(A')$ est injective. Alors on a les propriétés suivantes :*

1. $(\sigma^f_{A'})^g_{B'} = \sigma^{g\circ f}_{A'}$,
2. $(\sigma\pi)^f_{A'} = \sigma^f_{A'}\pi^f_{A'}$,
3. $(\sigma^{-1})^f_{A'} = (\sigma^f_{A'})^{-1}$,
4. $\mathrm{id}^f_{A'} = \mathrm{id}$.

Corollaire 3.4.19 *G^f est un sous-groupe de* $\mathrm{Sym}(B)$.

Définition 3.4.20 (Morphisme conjugué) Soient G un groupe, A et B deux ensembles, $f : A \to B$, et ϕ un morphisme de G vers $\mathrm{Sym}(A)$. Alors on définit le *morphisme conjugué* ϕ^f par :

$$\forall g \in G,\ \phi^f(g) \ = \ (\phi(g))^f.$$ ◇

Propriété 3.4.21 *La fonction ϕ^f est un morphisme de G vers* $\mathrm{Sym}(B)$.

Ainsi, si un groupe G agit sur un ensemble A et f est une fonction de A vers un ensemble B, il est possible de "retranscrire" l'action de G sur B.

Chapitre 4

Théorie algorithmique des groupes

Dans ce chapitre, nous allons présenter plusieurs résultats de théorie algorithmique des groupes de permutations. Nous commencerons par présenter deux algorithmes qui, étant donné un groupe G défini par un ensemble générateur, permettent de calculer l'ordre de G et de tester l'appartenance d'une permutation à G en temps polynomial. Puis nous définirons la *classe de complexité de Luks*, et énumérerons certains problèmes de cette classe dont nous nous servirons par la suite pour démontrer d'autres résultats de complexité. Enfin, nous nous intéresserons au problème de *contraintes de groupe*, et démontrerons que ce problème est NP-complet.

La plupart des résultats sur le test d'appartenance et la classe de Luks proviennent de [Hof81].

4.1 Des problèmes polynomiaux

Dans ce qui suit, nous allons présenter le problème de la représentation d'un groupe de permutation. Le problème est évidemment de trouver une représentation succincte qui permette de vérifier de façon efficace des propriétés basiques du groupe, comme de tester si une permutation est élément du groupe, ou de calculer son ordre.

Dans ce qui suit, nous allons voir que le fait de définir un groupe par un ensemble générateur permet de répondre à ces questions de façon efficace. D'après le Corollaire 3.4.9, tout groupe de permutation G de degré n a un ensemble de générateurs dont la taille est polynomiale en n. Nous allons maintenant voir qu'il est possible de tester si une permutation est élément de G, et de déterminer l'ordre de G en temps polynomial en n.

Nous allons donc étudier les deux problèmes suivants :

Problème: Appartenance à un groupe, ou G_MEM
Entrée: Un ensemble fini A, un ensemble K de permutations dans $\mathrm{Sym}(A)$, et une permutation $\sigma \in \mathrm{Sym}(A)$
Question: Est-ce que σ est élément du groupe engendré par K ?

EstElem(σ) =
  i := 0
  estMembre : = **vrai**
  tant que $i < n$ **et** estMembre **faire**
    $i := i + 1$
($\star$) **si** $\exists \mu \in U_i$ tel que $i^\mu = i^\sigma$ **alors**
      $\sigma := \sigma\mu^{-1}$
    sinon estMembre := **faux**
  fin tant que
  renvoyer estMembre

FIG. 4.1 – Test d'appartenance

Problème: Ordre d'un groupe, ou G_ORD
Entrée: Un ensemble fini A, et un ensemble K de permutations dans Sym(n)
Question: Quel est l'ordre du groupe engendré par K ?

Pour plus de clarté, nous allons étudier ces deux problèmes en supposant que $A = \{1, \ldots, n\}$, mais il est clair que tous ces résultats sont valables dans le cas général.

Soit G le groupe engendré par K, pour tout $i \in \{1, \ldots, n\}$, on note $G_i = G_{[\{1,\ldots,i\}]}$, et on considère un transversal droit U_i de G_i dans G_{i-1}. Enfin, on pose $G_0 = G$. Alors, d'après le Lemme 3.4.8, l'ensemble $K' = \bigcup_{i=1}^{n} U_i$ est un ensemble générateur de G. Etant donnés ces ensembles U_i pour $i \in \{1, \ldots, n\}$, l'algorithme de la Figure 4.1 permet alors de tester si la permutation σ est élément de G.

L'algorithme fonctionne de la façon suivante : si σ est élément de G, alors nécessairement, il existe une classe à droite $G_1\mu_1$ de G_1 dans G qui contient σ. Par définition d'une classe à droite, la permutation $\sigma_1 = \sigma\mu_1^{-1}$ est alors élément de G_1. Ainsi, d'après le Lemme 3.3.23, après avoir vérifié s'il existe une permutation $\mu_1 \in U_1$ telle que $1^\sigma = 1^{\mu_1}$, il y a deux possibilités. Soit un tel μ_1 n'existe pas, dans quel cas σ n'est pas élément de G, soit un tel μ_1 existe, et σ est élément de G si et seulement si $\sigma_1 \in G_1$. Puis on cherche à déterminer s'il existe une permutation $\mu_2 \in U_2$ telle que $2^{\sigma_1} = 2^{\mu_2}$, et si une telle permutation existe, on teste si $\sigma_2 = \sigma_1\mu_2^{-1}$ est élément de G_2. En réitérant ce raisonnement, comme $G_n = \mathrm{I}$, on voit que σ est élément de G si et seulement si on peut écrire σ sous la forme $\sigma = \mu_{n-1}\mu_{n-2}\ldots\mu_1$.

Lors de l'exécution de l'algorithme, on entre dans la boucle **tant que** au plus n fois, et il est possible d'effectuer le produit de deux permutations dans Sym(n) en temps $O(n)$. Nous verrons par la suite que le test de la ligne ($\star$) peut être effectué en temps constant.

Pour $i = 1, \ldots, n$, posons $n_i = |U_i|$, n_i est donc l'indice de G_i dans G_{i-1}. D'après le Théorème de Lagrange (Théorème 3.3.26), on a donc $|G_{i-1}| = n_i|G_i|$. Comme $G_n = \mathrm{I}$, on a $|G_n| = 1$, et donc, une induction triviale sur n prouve que

$$|G| = \prod_{i=1}^{n} |U_i|.$$

Sift(π, M) =
  $i := 0$
  estMembre := **vrai**
  tant que $i < n$ **et** estMembre **faire**
    $i := i + 1$
    $j := i^{\pi}$
    si $M_{i,j}$ n'est pas vide **alors**
      $\pi := \pi(M_{i,j})^{-1}$
    sinon
      estMembre := **faux**
      $M_{i,j} := \pi$
  fin tant que
  renvoyer estMembre

FIG. 4.2 – Algorithme de tamisage

On a donc les résultats suivants :

Théorème 4.1.1 (Prop. 1, p.34 de [Hof81]) *Si pour tout $i \in \{1, \ldots, n\}$, les ensembles U_i sont donnés, alors l'algorithme* EstElem *est correct, et teste si σ est élément de G en temps $0(n^2)$. De plus, les ensembles U_i permettent également de déterminer l'ordre de G en temps $O(n^2)$.*

Matrices de représentation

Nous allons maintenant étudier les *matrices de représentation* d'un groupe de permutation. Ces matrices permettent d'effectuer le test de la ligne ($\star$) de l'algorithme de la Figure 4.1 en temps constant, et leurs entrées constituent des transversaux droits de G_i dans G_{i-1} pour tout $i = 1, \ldots, n$. Nous verrons comment, partant d'un ensemble K de permutations, il est possible de construire de telles matrices en temps polynomial.

Définition 4.1.2 Une *matrice de représentation* M est une matrice carrée de taille n, dont les entrées sont soit vides, soit des éléments de Sym(n), qui vérifie les propriétés suivantes :

1. pour tout $i \in \{1, \ldots, n\}$, $M_{i,i} = \mathrm{id}$,
2. pour tout $j \in \{1, \ldots, n\}$ et pour tout $i > j$, $M_{i,j}$ est vide,
3. pour tout $j \in \{1, \ldots, n\}$ et pour tout $i < j$, $M_{i,j}$ est soit vide, soit une permutation μ qui fixe tous les éléments de $\{1, \ldots, i-1\}$, et telle que $i^{\mu} = j$.

On dit alors que M *représente* l'ensemble de permutations T_M défini par

$$T_M \;=\; \{\mu_n \mu_{n-1} \ldots \mu_1 \,|\, \forall i = 1, \ldots, n,\ \mu_i \text{ apparaît à la ligne } i \text{ de } M\}. \qquad \diamond$$

Théorème 4.1.3 *Les matrices de représentation vérifient les propriétés suivantes :*

MatRep(K) =
  // *Initialisation de* M
  soit M une matrice carrée **dans**
  pour $i \in \{1, \ldots, n\}$ **faire**
    $M_{i,i} :=$ id
    pour $j \in \{i+1, \ldots, n\}$ **faire**
      $M_{i,j} :=$ vide
    fin pour
  fin pour
  // *Construction de* M
  soit $Q := K$ dans // Q *est une file*
  tant que Q est non vide **faire**
    soit $\pi =$ Defiler(Q) **dans**
    soit estMembre = Sift(π, M) **dans**
    si $\neg$estMembre **alors**
      soit π' la permutation ajoutée à M par la fonction Sift **dans**
        pour toute permutation $\mu \neq$ id apparaissant dans M,
        ajouter à Q les permutations $\pi'\mu$ et $\mu\pi'$
  fin tant que

FIG. 4.3 – Construction d'une matrice de représentation

- *L'ensemble* T_M *est un groupe si et seulement si pour toute paire de permutations* σ, μ *apparaissant dans* M, $\sigma\mu$ *est élément de* T_M.
- *Si* M *est une matrice de représentation pour le groupe* G, *pour* $i = 1, \ldots, n$, *posons*

$$U_i \;=\; \{\mu \,|\, \mu \textit{ est une permutation apparaissant à la ligne } i \textit{ de } M\}.$$

  Alors U_i *est un transversal droit de* G_i *dans* G_{i-1}.

Soit $K \subseteq \mathrm{Sym}(n)$, l'algorithme permettant de construire une matrice de représentation pour le groupe G engendré par K est donné dans la Figure 4.3. Cet algorithme se sert de la fonction de *tamisage* (Sift) de la Figure 4.2. Cette fonction Sift renvoie **vrai** si la permutation π est élément de T_M. Sinon, elle remplace une entrée vide par une permutation dans la matrice de représentation M, pour que π puisse être représentée par cette nouvelle représentation, et renvoie **faux**. Cet algorithme est donc très proche de celui de la Figure 4.1, sauf que si π n'est pas élément de T_M, une nouvelle entrée est ajoutée à M.

Exemple 4.1.4 Soit M la matrice de représentation suivante :

$$M \;=\; \begin{pmatrix} \mathrm{id} & (1\ 2) & \_ & \_ \\ \_ & \mathrm{id} & \_ & \_ \\ \_ & \_ & \mathrm{id} & \_ \\ \_ & \_ & \_ & \mathrm{id} \end{pmatrix},$$

et soit $\pi = (1\ 2)(3\ 4)$. Alors, lors de l'appel à la fonction Sift, comme l'entrée $M_{1,2}$ n'est pas vide, l'algorithme calcule $\pi(M_{1,2})^{-1} = (1\ 2)(3\ 4)(1\ 2) = (3\ 4)$. On a $2^{(3\ 4)} = 2$, et l'entrée $M_{3,4}$ est vide, l'algorithme lui affecte la permutation $(3\ 4)$.

L'algorithme de la Figure 4.3 commence par initialiser la matrice de représentation M, créant ainsi une matrice dont tous les éléments de la diagonale sont l'identité, et dont toutes les autres entrées sont vides. Puis, l'algorithme essaye de représenter chaque permutation dans K comme un produit de la forme $\mu_n \dots \mu_1$, où μ_i est une entrée non vide de la $i^{\text{ème}}$ ligne de M. Si π peut être représenté comme un tel produit, alors π est un générateur redondant, et il n'y a rien à faire. Sinon, M ne contient pas suffisamment d'entrées pour représenter K, et la permutation π est utilisée pour ajouter une nouvelle entrée à M. Cette opération est réalisée par la fonction Sift.

Quand tous les éléments de K ont été traités, la matrice M représente un ensemble T_M tel que $K \subseteq T_M$, mais il se peut que T_M ne soit pas un groupe. C'est pourquoi tous les produits $\pi'\mu$ et $\mu\pi'$ sont ajoutés à Q et tamisés à leur tour. Cet algorithme termine car le nombre d'entrées non vides dans M est borné par n^2, et d'après le Théorème 4.1.3, la matrice qu'on obtient représente un groupe.

On a le théorème suivant :

Théorème 4.1.5 (Théorème 9, p. 40 de [Hof81]) *Soit $K \subseteq \mathrm{Sym}(n)$, alors l'algorithme de la Figure 4.3 construit une matrice de représentation pour le groupe G engendré par K en temps $O(|K|.n^2 + n^6)$.*

Ce théorème et le Théorème 4.1.1 permettent donc de déduire que :

Corollaire 4.1.6 *Les problèmes* G_MEM *et* G_ORD *sont dans* **P**.

4.2 La classe de complexité de Luks

Nous allons maintenant définir plusieurs problèmes de théorie algorithmique des groupes qui sont dans la classe **NP**, mais dont l'appartenance à **P** n'a pas été prouvée. Ces problèmes sont tous polynomialement équivalents, et font partie de la *classe de complexité de Luks*, et pour des raisons similaires à celles pour le problème GI, ne semblent pas être **NP**-complets. Nous prouverons en particulier que ces problèmes sont plus difficiles que le problème d'isomorphisme de graphes, ce qui justifiera le fait qu'aucun algorithme polynomial n'a encore été trouvé pour les résoudre.

Le premier problème dans la classe de Luks que nous considérons est le *problème d'intersection de groupes* :

> **Problème**: Intersection de groupes, ou INTER
> **Entrée**: Un ensemble fini A, des ensembles générateurs de G et H, deux sous-groupes de $\mathrm{Sym}(A)$
> **Sortie**: Un ensemble générateur de $G \cap H$

Définition 4.2.1 Un *graphe simple* est un couple (V, E), où V est un ensemble de *sommets*, et $E \subseteq V \times V$ est un ensemble d'*arêtes*. Par la suite, sauf indication contraire, on supposera que $V = \{1, \ldots, n\}$. Un graphe *biparti* est un couple $(V \uplus V', E)$ où $E \subseteq V \times V'$.

Soit $X' = (V', E')$, on dit que X et X' sont *isomorphes* si et seulement s'il existe une fonction bijective $f : V \to V'$ telle que $\langle v, w\rangle \in E$ si et seulement si $\langle f(v), f(w)\rangle \in E'$. On dit alors que f est un *isomorphisme* de X vers X'.

Etant donné un graphe $X = (V, E)$, on dit qu'une permutation $\sigma \in \mathrm{Sym}(n)$ est un *automorphisme de* X si et seulement si c'est un isomorphisme de X vers X. Il s'agit donc de l'ensemble des éléments de $\mathrm{Sym}(n)$ tels que pour toute arête $\langle v, w\rangle \in E$, l'arête $\langle v^\sigma, w^\sigma\rangle$ est également dans E. L'ensemble des automorphismes de X est noté $\mathrm{Aut}(X)$.$\diamond$

Propriété 4.2.2 *Pour tout graphe $X = (V, E)$, l'ensemble $\mathrm{Aut}(X)$ est un sous-groupe de $\mathrm{Sym}(|V|)$.*

Considérons les deux problèmes suivants :

> **Problème**: Isomorphisme de graphes, ou GI
> **Entrée**: Deux graphes X et X'
> **Question**: X et X' sont-ils isomorphes ?
>
> **Problème**: Groupe d'automorphisme d'un graphe, ou GRAPH_AUT
> **Entrée**: Un graphe X
> **Sortie**: Un ensemble générateur de $\mathrm{Aut}(X)$.

Théorème 4.2.3 (Théorème 6 de [Hof81]) GI *et* GRAPH_AUT *sont polynomialement équivalents.*

Nous allons prouver que GRAPH_AUT se réduit polynomialement à INTER. D'après le Lemme 3.2.8, le groupe $\mathrm{Sym}(n)$ agit de façon naturelle sur $V \times V$. Notons ψ le morphisme de $\mathrm{Sym}(n)$ vers $\mathrm{Sym}(V \times V)$ correspondant, et posons $G = \psi(\mathrm{Sym}(n))$. Le morphisme ψ est clairement injectif, et $\mathrm{Sym}(n)$ et G sont donc isomorphes. On a le théorème suivant :

Théorème 4.2.4 (Théorème 7 de [Hof81]) *Soit $X = (V, E)$ un graphe, et posons $\bar{E} = (V \times V) \setminus E$. Alors $\mathrm{Aut}(X)$ et $G \cap (\mathrm{Sym}(E)\mathrm{Sym}(\bar{E}))$ sont isomorphes.*

PREUVE. Posons $G' = \psi(\mathrm{Aut}(X))$, alors $\mathrm{Aut}(X)$ et G' sont isomorphes, et on va montrer que $G' = G \cap (\mathrm{Sym}(E)\mathrm{Sym}(\bar{E}))$.

Soit $\psi(\mu) \in G'$, alors $\psi(\mu)$ est clairement élément de G. Par définition de $\mathrm{Aut}(X)$, pour tout $e \in E$ et pour tout $e' \in \bar{E}$, on a $e^{\psi(\mu)} \in E$ et $e'^{\psi(\mu)} \in \bar{E}$, ce qui prouve que $\psi(\mu)$ est également élément de $\mathrm{Sym}(E)\mathrm{Sym}(\bar{E})$.

Réciproquement, soit $\sigma \in G \cap (\mathrm{Sym}(E)\mathrm{Sym}(\bar{E}))$, alors, comme $\sigma \in G$, il existe une unique permutation $\mu \in \mathrm{Sym}(n)$ telle que $\sigma = \psi(\mu)$. De plus, comme $\sigma \in \mathrm{Sym}(E)\mathrm{Sym}(\bar{E})$, on a

$$\forall \langle e, e'\rangle \in \mathrm{Sym}(E) \times \mathrm{Sym}(\bar{E}),\ e^{\psi(\mu)} \in \mathrm{Sym}(E),\ \text{et}\ e'^{\psi(\mu)} \in \mathrm{Sym}(\bar{E}).$$

On en déduit que $\mu \in \mathrm{Aut}(X)$, et σ est bien élément de G'. ∎

Corollaire 4.2.5 *Le problème* GRAPH_AUT *se réduit polynomialement au problème* INTER.

Voici une liste de problèmes qui sont tous dans la classe de Luks.

> **Problème**: Appartenance à une classe au centre, ou DC_MEM
> **Entrée**: Un ensemble fini A, des ensembles générateurs de sous-groupes G et H de $\mathrm{Sym}(A)$ et des permutations σ et μ dans $\mathrm{Sym}(A)$
> **Question**: Est-ce que σ est élément de la classe au centre $G\mu H$?

> **Problème**: Factorisation dans deux groupes, ou FACT
> **Entrée**: Un ensemble fini A, des ensembles générateurs de sous-groupes G et H de $\mathrm{Sym}(A)$ et une permutation $\sigma \in \mathrm{Sym}(A)$
> **Question**: Existe-t-il des permutations $\pi \in G$ et $\mu \in H$ telles que $\sigma = \pi\mu$?

> **Problème**: Intersection de classe, ou CIE
> **Entrée**: Un ensemble fini A, des ensembles générateurs de sous-groupes G et H de $\mathrm{Sym}(A)$ et une permutation $\sigma \in \mathrm{Sym}(A)$
> **Question**: L'ensemble $G\sigma \cap H$ est-il vide ?

> **Problème**: Stabilisateur d'ensemble, ou STAB
> **Entrée**: Un ensemble fini A, un ensemble générateur d'un sous-groupe G de $\mathrm{Sym}(A)$ et un ensemble $A' \subseteq A$
> **Sortie**: Un ensemble générateur du groupe $\mathrm{Stab}_G(A')$.

Il est prouvé dans [Hof81] que ces problèmes sont bien dans la classe de Luks. Nous aurons également à considérer le problème suivant :

> **Problème**: Problème de l'orbite, ou OP.
> **Entrée**: Deux n-uplets $x = \langle x_1, \ldots, x_n\rangle$ et $y = \langle y_1, \ldots, y_n\rangle$ sur $\{0, 1\}$, et un ensemble de permutations $\{\sigma_1, \ldots, \sigma_m\} \subseteq \mathrm{Sym}(n)$.
> **Question**: Existe-t-il une permutation σ dans le groupe G engendré par les $\{\sigma_1, \ldots, \sigma_m\}$, telle que pour tout $i = 1, \ldots, n$, on a $x_{i^\sigma} = y_i$?

Ce dernier problème a été étudié dans [CEJS98], où le résultat suivant est prouvé :

Théorème 4.2.6 (Théorème 4.1 de [CEJS98]) *Le problème* OP *est dans la classe de Luks.*

De nombreux algorithmes efficaces existent pour résoudre ces problèmes ([But91, Sim94, Ser03]), et sont implémentés dans les systèmes MAGMA -anciennement Cayley- ([Can84, BC88, BC90, CP97]) ou GAP[1].

[1] http ://www.gap-system.org

4.3 Le problème G_CSTR

Nous allons maintenant étudier un problème sur les groupes de permutation qui est NP-complet, le problème G_CSTR. Nous considérerons certaines restrictions de ce problème, et étudierons leur complexité.

Définissons formellement ce problème :

> **Problème**: Contraintes de groupe, ou G_CSTR.
> **Entrée**: Un ensemble fini A, un ensemble générateur d'un groupe fini G agissant par un morphisme ϕ sur A, et un ensemble $\{J_a \,|\, a \in A\}$ de sous-ensembles de A.
> **Question**: Y a-t-il une permutation $\sigma \in \phi(G)$ telle que pour tout $a \in A$, $a^\sigma \in J_a$?

Il est clair que ce problème est dans NP, il suffit en effet de deviner une permutation σ, de tester si elle est dans G (ce qui peut être fait en temps polynomial d'après le Corollaire 4.1.6), et de s'assurer qu'elle satisfait toutes les contraintes. Par la suite, on supposera que G n'est pas engendré par l'identité et est donc un groupe non trivial.

Nous allons prouver que le problème G_CSTR est NP-complet en effectuant une réduction polynomiale du problème 1SUR3+SAT vers G_CSTR. Par la suite, étant donnée une instance S, V du problème 1SUR3+SAT, nous chercherons à déterminer un ensemble $I \subseteq V$ tel que pour tout $C \in S$, $|I \cap C| = 1$, I représentera implicitement l'interprétation qui interprète toutes les variables dans I à vrai, et toutes les autres à faux.

Définition 4.3.1 Soit S, V une instance du problème 1SUR3+SAT, et considérons l'opération de différence symétrique $\triangle$ sur les ensembles. Cette opération est une loi de composition interne sur l'ensemble 2^V, et on définit $\Delta = (2^V, \triangle)$. ◇

Lemme 4.3.2 *Δ est un groupe.*

PREUVE. L'ensemble vide est l'identité pour cette loi de composition qui est clairement associative, et tout élément est son propre inverse. ■

Définition 4.3.3 On définit les ensembles $A = \{\langle C, B\rangle \,|\, C \in S \wedge B \subseteq C\}$, et $A_0 = \{\langle C, \emptyset\rangle \,|\, C \in S\}$. Pour tout $a \in A$, on définit J_a par :

$$\begin{aligned} \forall \langle C, \emptyset\rangle \in A_0,\ J_{\langle C,\emptyset\rangle} &= \{\langle C, \{x\}\rangle \,|\, x \in C\}, \\ \forall a \in A \setminus A_0,\ J_a &= A. \end{aligned}$$

On définit la fonction $\Psi : \Delta \to \mathrm{Sym}(A)$ par : pour tout $I \in \Delta$ et pour tout $\langle C, B\rangle \in A$, $\langle C, B\rangle^{\Psi(I)} = \langle C, B \triangle (I \cap C)\rangle$. ◇

Comme $B \triangle (I \cap C) \subseteq C$, il est clair que la fonction Ψ est bien définie, et on a :

Lemme 4.3.4 *La fonction Ψ est un morphisme de groupes.*

PREUVE. Soit $I \in \Delta$, commençons par prouver que $\Psi(I)$ est bien une permutation de A. Soient $\langle C, B\rangle, \langle C', B'\rangle \in A$ deux éléments qui ont la même image par $\Psi(I)$, c'est-à-dire :

$$\langle C, B \vartriangle (I \cap C)\rangle \;=\; \langle C', B' \vartriangle (I \cap C')\rangle.$$

Alors on a $C = C'$, et comme $B \vartriangle (I \cap C) = B' \vartriangle (I \cap C)$, nécessairement, $B = B'$. La fonction $\Psi(I)$ est donc injective, et comme A est un ensemble fini, c'est une bijection.

Soit $J \in \Delta$, alors on a

$$\begin{aligned}
\langle C, B\rangle^{\Psi(I \vartriangle J)} &= \langle C, B \vartriangle ((I \vartriangle J) \cap C)\rangle \\
&= \langle C, B \vartriangle (I \cap C) \vartriangle (J \cap C)\rangle \;\text{ (distributivité de } \cap\text{)} \\
&= \langle C, B \vartriangle (I \cap C)\rangle^{\Psi(J)} \\
&= \langle C, B\rangle^{\Psi(I)\Psi(J)}.
\end{aligned}$$

Donc, $\Psi(I \vartriangle J) = \Psi(I)\Psi(J)$, et Ψ est bien un morphisme de groupes. ∎

Exemple 4.3.5 Considérons la clause $C = \{x, y, z\}$, et soit $I = \{x\}$, alors on a :

$$\begin{aligned}
\langle C, \emptyset\rangle^{\Psi(I)} &= \langle C, \{x\}\rangle, \\
\langle C, \{x\}\rangle^{\Psi(I)} &= \langle C, \emptyset\rangle, \\
\langle C, \{x, y\}\rangle^{\Psi(I)} &= \langle C, \{y\}\rangle.
\end{aligned}$$

Théorème 4.3.6 *L'instance S, V est dans* 1SUR3+SAT *si et seulement s'il existe une permutation $\sigma \in \Psi(\Delta)$ telle que pour tout $a \in A_0$, on a $a^\sigma \in J_a$.*

PREUVE. On a les équivalences suivantes :

$$\begin{aligned}
(S, V) \in \text{1SUR3+SAT} &\Leftrightarrow \exists I \subseteq V, \forall C \in S, |I \cap C| = 1 \\
&\Leftrightarrow \exists I \in \Delta, \forall C \in S, \exists x \in C, I \cap C = \{x\} \\
&\Leftrightarrow \exists I \in \Delta, \forall C \in S, I \cap C \in \{\{x\} \mid x \in C\} \\
&\Leftrightarrow \exists I \in \Delta, \forall C \in S, \langle C, \emptyset\rangle^{\Psi(I)} \in J_{\langle C, \emptyset\rangle} \\
&\Leftrightarrow \exists \sigma \in \Psi(\Delta), \forall a \in A_0, a^\sigma \in J_a.
\end{aligned}$$ ∎

Pour tout $\sigma \in \Psi(\Delta)$, et pour tout $a \in A \setminus A_0$, on a $a^\sigma \in J_a$, et donc :

Corollaire 4.3.7 *Le problème* 1SUR3+SAT *se réduit polynomialement au problème* G_CSTR.

PREUVE. Tout élément $I \in \Delta$ peut être écrit sous la forme $I = \bigvartriangle_{x \in I}\{x\}$, le groupe Δ est donc engendré par l'ensemble des singletons de V. De plus, comme chaque clause dans S est constituée de trois variables, on a $|A| = 8|S|$, d'où le résultat. ∎

4.3.1 Une restriction de G_Cstr

Considérons la restriction suivante du problème G_Cstr :

> **Problème**: GC_Part_Rst
> **Entrée**: Un ensemble fini A, un ensemble générateur d'un groupe G agissant par un morphisme ϕ sur A, un ensemble $\{J_a \mid a \in A\}$ de sous-ensembles de A deux à deux disjoints ou égaux, et un ensemble $A_0 \subseteq A$
> **Question**: Existe-t-il un élément $g \in G$ tel que pour tout $a \in A_0$, $a^{\phi(g)} \in J_a$?

Nous allons montrer que le problème 1sur3+Sat se réduit polynomialement à GC_Part_Rst, ce qui prouvera que ce problème est **NP**-complet. Soit S, V une instance de 1sur3+Sat, reprenons le groupe Δ de la Définition 4.3.1, ainsi que les ensembles A et A_0, et le morphisme Ψ de la Définition 4.3.3. On définit les contraintes $(J_a)_{a\in A}$ de la façon suivante :

Définition 4.3.8 Si $\langle C, \emptyset\rangle \in A_0$, alors $J_{\langle C,\emptyset\rangle} = \{\langle C, \{x\}\rangle \mid x \in C\}$, et pour tout $a \in A \setminus A_0$, $J_a = A \setminus A_0$. ◇

On a la propriété suivante :

Propriété 4.3.9 *Soient a et a' deux éléments de A_0, alors on a $J_a \cap J_{a'} = \emptyset$. Les contraintes $(J_a)_{a\in A}$ sont donc deux à deux disjointes ou égales.*

D'après le Théorème 4.3.6, il existe une solution à l'instance S, V de 1sur3+Sat si et seulement s'il existe une permutation $\sigma \in \Psi(\Delta)$ telle que pour tout $a \in A_0$, on a $a^\sigma \in J_a$. On a donc le résultat suivant :

Corollaire 4.3.10 *Le problème* 1sur3+Sat *se réduit polynomialement au problème* GC_Part_Rst.

4.4 Conclusion

Dans ce chapitre, nous avons présenté plusieurs problèmes de théorie des groupes pour des groupes de permutation définis par des ensembles de générateurs. Nous avons ainsi étudié le problème de l'appartenance d'une permutation à un tel groupe, et montré que ce problème est polynomial, ce qui nous a par la suite permis de démontrer que plusieurs autres problèmes sont dans la classe **NP**. Puis, nous avons présenté plusieurs problèmes de théorie des groupes qui sont dans la classe de Luks, et qui sont plus difficiles à résoudre que le problème d'isomorphisme de graphe, avant de nous intéresser au problème de contraintes de groupe, et à une de ses restrictions.

Nous avons énoncé les problèmes G_Cstr et GC_Part_Rst de la façon la plus générale possible pour simplifier les démonstrations de **NP**-complétude. Nous avons ainsi considéré l'action d'un groupe engendré par un ensemble E, agissant par un morphisme ϕ

sur un ensemble A. Il est clair que nous aurions pu à la place directement considérer l'action naturelle du groupe engendré par $\phi(E)$ sur A, et même supposer que $A = \{1, \ldots, n\}$. Dans les chapitres à venir, nous utiliserons indifféremment ces autres formulations de ces problèmes, afin de rendre plus lisibles les réductions que nous effectuerons vers les autres problèmes considérés.

Deuxième partie

GA-termes et GA-termes stratifiés

Chapitre 5

GA-termes

Dans ce chapitre, nous allons nous servir de techniques proches de celles employées pour la réécriture de graphes de termes (voir par exemple [BvEG+87, Klo95, KKSdV93, Ohl02]), et définir les GA-*termes*, qui nous serviront dans le chapitre suivant à représenter les termes stratifiés de [AP01].

Nous commencerons par définir les graphes étiquetés, dont les GA-termes constituent une sous-classe, puis nous définirons ces GA-termes proprement dits. Nous définirons ensuite plusieurs notions liées à ces GA-termes, comme la relation de *bisimilarité* entre deux GA-termes, et nous nous intéresserons particulièrement à la notion *d'homomorphisme* d'un GA-terme vers un autre.

5.1 Graphes étiquetés et GA-termes

Définition 5.1.1 (Graphe étiqueté) Un *graphe étiqueté* sur une signature Σ est un triplet $G = (V_G, s_G, a_G)$, où V_G est un ensemble fini et non vide dont les éléments sont des *sommets* ; $s_G : V_G \to \Sigma$ est une fonction qui étiquette chacun des sommets avec un symbole de Σ, et $a_G : V_G \to V_G^\star$ est une fonction qui affecte à chaque sommet $v \in V_G$ une liste (ou un mot) de sommets arguments, dont la longueur $|a_G(v)|$ est égale à l'arité du symbole $s_G(v)$. La *taille* d'un graphe étiqueté est définie par $|G| = |V_G|$.

Si G est un graphe étiqueté, alors le *graphe sous-jacent* de G est le graphe orienté $\mathbf{G}_G = (V_G, E)$, où $E = \{\langle u, v\rangle \in V_G^2 \mid v \text{ apparaît dans } a_G(u)\}$. ◇

Exemple 5.1.2 Soit $\Sigma = \{f, g, b\}$, où f est d'arité 2, g est d'arité 1, et b est une constante. Soit G le graphe étiqueté défini sur $V = \{\mathfrak{a}, \mathfrak{b}, \mathfrak{c}\}$, avec les fonctions s et a définies par :

v	$\mathfrak{a}$	$\mathfrak{b}$	$\mathfrak{c}$
$s(v)$	f	b	g
$a(v)$	$\mathfrak{b}.\mathfrak{c}$	ε	$\mathfrak{a}$

La Figure 5.1 est une représentation de G. Les flèches partent d'un sommet v et sont dirigées vers ses arguments (les éléments de $a(v)$). L'ordre dans lequel ces flèches sont

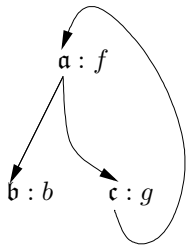

FIG. 5.1 – Exemple d'un graphe étiqueté

dessinées est important : elles sont dessinées vers le bas et de gauche à droite selon l'ordre des sommets arguments dans $a(v)$.

Le graphe sous-jacent à G est obtenu en retirant les symboles attachés aux trois sommets et en ne prenant pas en compte l'ordre dans lequel les flèches sont dessinées. Ce graphe sous-jacent est donc

$$\mathbf{G}_G = \langle \{\mathfrak{a}, \mathfrak{b}, \mathfrak{c}\}, \{\langle \mathfrak{a}, \mathfrak{b}\rangle, \langle \mathfrak{a}, \mathfrak{c}\rangle, \langle \mathfrak{c}, \mathfrak{a}\rangle\}\rangle.$$

Définition 5.1.3 (Chemins) Soit $G = (V_G, s_G, a_G)$ un graphe étiqueté. Nous définissons les *chemins* dans G, depuis un sommet *source* jusqu'à un sommet *puits*, par des listes sur l'alphabet $V_G \cup \mathbb{N}$.

Ces chemins sont définis inductivement comme suit : la liste vide ε est un chemin dans G de tout sommet à lui-même, qui est de longueur 0 (on dit que ε est le chemin *vide*), et si p est un chemin dans G de u à v de longueur k, et w est le $i^{\text{ème}}$ élément de la liste $a_G(v)$, alors $p.v.i$ est un chemin dans G de u à w de longueur $k+1$. On dit alors que v est un *parent* de w, et u un *ancêtre* de w.

La *distance* entre deux sommets est la longueur du plus court chemin entre ces sommets. Enfin, un *cycle* est un chemin non vide d'un sommet vers lui-même ; un graphe étiqueté est dit *acyclique* si et seulement s'il ne contient aucun cycle.

Soient u et v deux sommets de G, on dit que u est *accessible* depuis v si et seulement s'il existe un chemin de v à u. L'ensemble des sommets accessibles depuis v est noté $V_G|v$. Il est évident que $(V_G|v, s', a')$ est également un graphe étiqueté sur Σ, où s' et a' sont les restrictions respectives de s_G et a_G à $V_G|v$. Ce graphe sera noté $G|v$. Un sommet $r \in V_G$ est une *racine* de G si et seulement si $G = G|r$.

Soit $p = u_1.i_1.\cdots.u_n.i_n$ un chemin dans un graphe étiqueté $G = (V, s, a)$, et soit $\eta : V \to V'$. Alors on définit $\eta(p)$ comme étant la liste $\eta(u_1).i_1.\cdots.\eta(u_n).i_n$. Notons que $\eta(p)$ n'est en général pas un chemin. ◇

La notion de racine employée ici ne correspond pas à celle utilisée en réécriture de graphes de termes (une racine n'y est en effet qu'un sommet distingué). Elle est néanmoins suffisante pour notre formalisation et simplifie de nombreuses preuves.

Exemple 5.1.4 Soit T le graphe étiqueté de l'Exemple 5.1.2. Alors T possède deux racines, les sommets $\mathfrak{a}$ et $\mathfrak{c}$, et le chemin $\mathfrak{a}.2.\mathfrak{c}.1$ est un cycle dans T.

Remarque. Si la source d'un chemin est présente dans ce chemin, il n'en est pas de même de son puits. Ceci permet de concaténer des chemins : si p est un chemin de u à v, et q est un chemin de v à w, alors $p.q$ est un chemin de u à w.

Lemme 5.1.5 *Soit G un graphe étiqueté, et p et p' deux chemins distincts de même source. Alors, pour toute fonction η, les listes $\eta(p)$ et $\eta(p')$ sont distinctes.*

PREUVE. Soit q le plus grand préfixe commun à p et p'. Alors p et p' sont de la forme :

$$p \;=\; q.i.r, \text{ et } p' \;=\; q.i'.r',$$

où $i \neq i'$. On a alors

$$\eta(p) \;=\; \eta(q).i.\eta(r), \text{ et } \eta(p') \;=\; \eta(q).i'.\eta(r),$$

et ces deux listes sont évidemment distinctes. ∎

Définition 5.1.6 Soient $G = (V, s, a)$ et $G' = (V', s', a')$ deux graphes étiquetés, et considérons les chemins

$$\begin{aligned} p &= u_1.i_1.\cdots.u_n.i_n \text{ dans } G, \\ p' &= v_1.j_1.\cdots.v_n.j_n \text{ dans } G'. \end{aligned}$$

On dit que p et p' sont :
- *équivalents* si et seulement si $s(u_1).\cdots.s(u_n) = s'(v_1).\cdots.s'(v_n)$,
- *parallèles* si et seulement si $i_1.\cdots.i_n = j_1.\cdots.j_n$. ◇

Exemple 5.1.7 Considérons les deux graphes étiquetés de la Figure 5.2, qu'on nomme respectivement G et G', et les chemins :

$$\begin{aligned} p_1 &= \mathfrak{a}.1.\mathfrak{b}.1.\mathfrak{d}.1, \\ p_2 &= \mathfrak{a}.2.\mathfrak{c}.1.\mathfrak{d}.1, \\ p' &= \mathfrak{a}'.1.\mathfrak{b}'.1.\mathfrak{d}'.1. \end{aligned}$$

p_1 et p_2 sont tous deux des chemins dans G, de $\mathfrak{a}$ à $\mathfrak{a}$; p' est un chemin dans G' de $\mathfrak{a}'$ à $\mathfrak{f}'$. Alors p_1 et p' sont parallèles, et p_1, p_2 et p' sont équivalents.

Propriété 5.1.8 *Soit G un graphe étiqueté, et soient p et p' deux chemins dans G de même source, qui sont parallèles. Alors $p = p'$.*

PREUVE. Par induction triviale sur la longueur de p. ∎

Deux chemins distincts d'un même graphe étiqueté qui sont de même source ne peuvent donc pas être parallèles ; par contre, comme le montre l'Exemple 5.1.7, ils peuvent être équivalents.

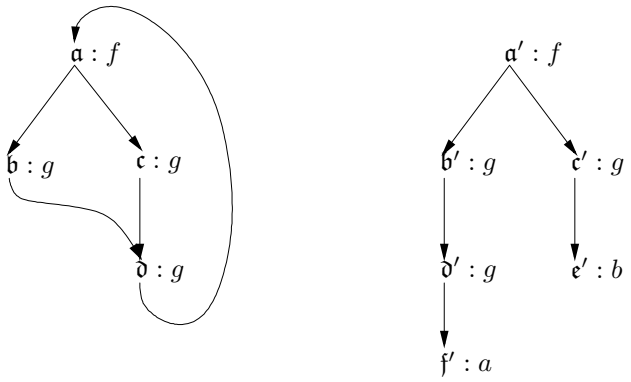

FIG. 5.2 – Graphes étiquetés de l'Exemple 5.1.7

Propriété 5.1.9 *Pour deux graphes étiquetés G et G' donnés, si p est un chemin de u à v dans G et que η est une fonction telle que $\eta(p)$ est un chemin dans G', alors p et $\eta(p)$ sont parallèles, et $\eta(p)$ est un chemin de $\eta(u)$ à $\eta(v)$.*

Définition 5.1.10 (GA-terme et A-terme) Soit un symbole $\circ \notin \Sigma$, d'arité 0, et considérons la signature étendue $\Sigma^\circ = \Sigma \cup \{\circ\}$. Un GA-*terme* sur Σ est un graphe étiqueté T sur Σ° qui possède une racine unique, notée racine(T), et qui est acyclique. L'ensemble des GA-termes sur Σ est noté GA-$\mathcal{T}(\Sigma)$.

Soit $T = (V_T, s_T, a_T)$ un GA-terme, et $v \in V_T$. On dit que v est un *sommet variable* de T si $s_T(v) = \circ$, sinon, on dit que v est un *sommet non-variable* de T. L'ensemble des sommets variables de T est noté $\mathcal{SV}(T)$.

Les GA-termes sur Σ qui n'ont pas de sommet variable sont dits *clos* ; l'ensemble de ces graphes est noté GA-$\mathcal{T}_c(\Sigma)$.

Enfin, si T est un GA-terme dont le graphe sous-jacent est un arbre, on dira que T est un A-*terme*. ◇

Définition 5.1.11 (Hauteur) Soit $T = (V, s, a)$ un GA-terme. On définit la *hauteur* de T comme la longueur du plus long chemin dans T de sa racine à un de ses sommets. Par extension, on parlera de la *hauteur* d'un sommet u dans T, signifiant par là la hauteur du graphe $T|u$.

Soient u et v deux sommets de T. S'il existe un chemin dans T de u à v, alors on dit que v est *en-dessous* de u dans T, ce qui est noté $v \leq_T u$. Si ce chemin est non vide, on notera $v <_T u$. De même, si U et W sont des sous-ensembles de V_T, on notera $U \leq_T W$ si et seulement si tous les sommets dans U sont en-dessous de tous les sommets de W dans T. Enfin, on dit que U est *indépendant* dans T si et seulement si tous les éléments de U sont mutuellement incomparables par $<_T$, c'est à dire que si u et v sont éléments de U, alors on n'a ni $u <_T v$, ni $v <_T u$. ◇

Exemple 5.1.12 Il est facile de vérifier que pour tout GA-terme T, l'ensemble $\mathcal{SV}(T)$ est un ensemble indépendant dans T.

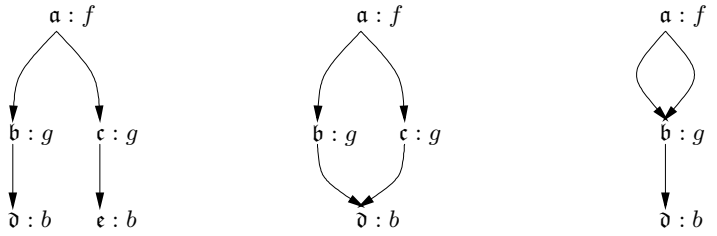

FIG. 5.3 – Trois représentations de $f(g(b), g(b))$

Propriété 5.1.13 *La relation $\leq_T$ est un ordre partiel sur V.*

PREUVE. La réflexivité et la transitivité sont triviales. Si pour deux sommets u et v de T on a $u \leq_T v$ et $v \leq_T u$, alors il existe un chemin dans T de u a v, et un autre de v à u. Comme T est acyclique, ces deux chemins sont alors triviaux, et on a $u = v$. ■

La fonction suivante traduit les GA-termes en termes. Elle permettra plus tard de décrire les GA-termes plus commodément, et de caractériser des GA-termes *bisimilaires* (notion qui sera définie ultérieurement).

Définition 5.1.14 La fonction τ de GA-$\mathcal{T}(\Sigma)$ dans $\mathcal{T}(\Sigma^\circ)$ est définie inductivement comme suit : pour T un GA-terme, soit $r = \text{racine}(T)$;
- si $s_T(r)$ est une constante $c \in \Sigma^\circ$, alors $\tau(T) = c$,
- si $s_T(r)$ est un symbole de fonction f d'arité n, alors $\tau(T) = f(t_1, \ldots, t_n)$, où les t_i sont obtenus en appliquant récursivement la fonction τ aux arguments de r ; c'est-à-dire que si $a_T(r) = v_1.\cdots.v_n$, alors $t_i = \tau(T|v_i)$, pour $1 \leq i \leq n$.

Cette fonction est bien définie, puisque tout GA-terme est acyclique.

Soient T et T' deux GA-termes. On dit que T et T' sont *bisimilaires*, ce qu'on note $T \stackrel{\circ}{=} T'$, si et seulement si $\tau(T) = \tau(T')$. ◇

Propriété 5.1.15 *La relation de bisimilarité est une relation d'équivalence.*

Exemple 5.1.16 Notons respectivement T_1, T_2 et T_3 les trois GA-termes de la Figure 5.3. Alors

$$\tau(T_1) \;=\; \tau(T_2) \;=\; \tau(T_3) \;=\; f(g(b), g(b)),$$

et ces trois GA-termes sont donc mutuellement bisimilaires.

La définition de la fonction τ induit immédiatement les propriétés suivantes :

Propriété 5.1.17 *Soient T et T' deux GA-termes, alors :*

1. *la hauteur de T est égale à la profondeur du terme $\tau(T)$,*
2. *si T et T' sont bisimilaires, alors ils sont de même hauteur.*

Le lemme suivant permet de caractériser la relation de bisimilarité :

Lemme 5.1.18 *Soient $T = (V, s, a)$ et $T' = (V', s', a')$ deux* GA*-termes de racines respectives r et r'. Alors les deux propositions suivantes sont équivalentes :*

1. *T et T' sont bisimilaires.*
2. *Pour tout sommet $v \in V$ et pour tout chemin p de r à v dans T, il existe un chemin p' dans T' de source r', qui est parallèle à p, et dont le puits v' vérifie $s'(v') = s(v)$.*

PREUVE. Montrons par induction sur la hauteur de T que si T et T' sont bisimilaires, et p est un chemin de r à v dans T, alors il existe un chemin p' de r' à v' dans T' qui est parallèle à p, et que $s'(v') = s(v)$. Le résultat est trivial si p est le chemin vide, on suppose maintenant que p est de la forme $r.i.q$. Posons $a(r) = v_1.\cdots.v_n$, $a'(r') = v'_1.\cdots.v'_n$, $T_i = T|v_i$ et $T'_i = T'|v'_i$. Alors par définition, q est un chemin de v_i à v dans T_i, et comme $T'_i \stackrel{\circ}{=} T_i$, par hypothèse d'induction, il existe un chemin q' dans T'_i, de v'_i à v', qui est parallèle à q, et on a $s'(v') = s(v)$. Donc, $p' = r'.i.q'$ est bien un chemin dans T' de r' à v' qui est parallèle à p, et on a $s'(v') = s(v)$.

On démontre également la réciproque par induction sur la hauteur de T. Supposons que le résultat soit vrai pour tous les GA-termes de hauteur inférieure ou égale à n, et que T est de hauteur $n+1$. Comme précédemment, on pose $s(r) = v_1.\cdots.v_n$, $s'(r') = v'_1.\cdots.v'_n$, et pour tout $i = 1, \ldots, n$, on note $T_i = T|v_i$, et $T'_i = T'|v'_i$. Pour $i \in \{1, \ldots, n\}$, soit v un sommet de T_i et q un chemin de v_i à v dans T_i, alors $p = r.i.q$ est un chemin de r à v dans T, et par hypothèse, il existe un chemin $p' = r'.i.q'$ parallèle à p, de r' à un sommet v' dans T' tel que $s'(v') = s(v)$. Il est alors clair que q' est un chemin de v'_i à v' dans T'_i qui est parallèle à q, par hypothèse d'induction, on a donc $T_i \stackrel{\circ}{=} T'_i$ pour tout $i = 1, \ldots, n$. Comme le chemin vide est un chemin de r à r dans T, et de r' à r' dans T', on a également $s(r) = s'(r')$, ce qui prouve que $T \stackrel{\circ}{=} T'$. ∎

Exemple 5.1.19 Soient T et T' les deux GA-termes de la Figure 5.4, ces deux GA-termes vérifient bien les hypothèses du Lemme 5.1.18 et sont donc bisimilaires (ils représentent tous deux le terme $f(g(a,a), g(a,a)))$. Cet exemple montre qu'il n'y a en général pas d'homomorphisme de T vers T', ni de T' vers T.

5.2 Homomorphismes

Nous définissons maintenant la notion d'homomorphisme d'un GA-terme vers un autre. Cette notion sera prédominante dans la définition de GA-termes stratifiés.

Définition 5.2.1 (Homomorphismes) Etant donnés deux GA-termes T et T' sur Σ, un *homomorphisme* (resp. *homomorphisme clos*) de T vers T' est une fonction $h : V_T \to V_{T'}$ telle que $h(\text{racine}(T)) = \text{racine}(T')$, et pour tout sommet $v \in V_T \setminus \mathcal{SV}(T)$ (resp. pour tout $v \in V_T$),

$$s_{T'}(h(v)) = s_T(v) \quad \text{et} \quad a_{T'}(h(v)) = h(a_T(v))$$

(où on prend pour convention que $h(v_1.\cdots.v_n) = h(v_1).\cdots.h(v_n)$).

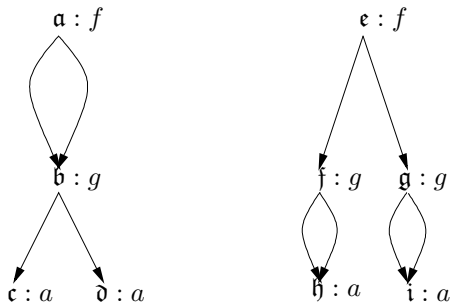

FIG. 5.4 – GA-termes de l'Exemple 5.1.19

Si l'homomorphisme h est clos, on dit que T' est *plus compact* que T, ce qu'on note $T' \Subset T$.

Le *résidu* de h est l'image dans $V_{T'}$ des sommets variables de T ; c'est-à-dire l'ensemble $h(\mathcal{SV}(T))$. L'*antirésidu* de h est l'ensemble $h(V_T \setminus \mathcal{SV}(T))$, c'est donc l'image par h des sommets non-variables de T.

Un homomorphisme h de T vers T' est un *isomorphisme* si et seulement si h est bijectif et h^{-1} est un homomorphisme de T' vers T. On dit alors que T et T' sont *isomorphes*, ce qu'on note $T \simeq T'$. ◇

Exemple 5.2.2 Soient T et T' les deux GA-termes représentés Figure 5.5. La fonction h définie ci-dessous est un homomorphisme de T vers T' ; son résidu est $\{\mathfrak{b}', \mathfrak{d}'\}$, et son antirésidu est $\{\mathfrak{a}', \mathfrak{c}'\}$. h n'est donc pas clos, car $s(\mathfrak{d}') \neq s(\mathfrak{d})$.

v	$\mathfrak{a}$	$\mathfrak{b}$	$\mathfrak{c}$	$\mathfrak{d}$
$h(v)$	$\mathfrak{a}'$	$\mathfrak{b}'$	$\mathfrak{c}'$	$\mathfrak{d}'$

Exemple 5.2.3 Dans la Figure 5.3, on vérifie aisément que le deuxième GA-terme est plus compact que le premier, et le troisième est plus compact que les deux précédents.

Montrons maintenant que l'opération de composition $\circ$ est une loi de composition interne sur l'ensemble des homomorphismes (resp. homomorphismes clos).

Propriété 5.2.4 *Soient T, T' et T'' trois GA-termes tels qu'il existe un homomorphisme h de T vers T', et un homomorphisme h' de T' vers T''. Alors $h' \circ h$ est un homomorphisme de T vers T'', et si h et h' sont des homomorphismes clos, alors $h' \circ h$ est également un homomorphisme clos.*

PREUVE. La preuve que $h' \circ h$ est un homomorphisme de T vers T'' est triviale. Si h et h' sont des homomorphismes clos, alors pour tout sommet variable v de T, $h(v)$ est un sommet variable de T' par définition, et donc, $h' \circ h(v)$ est un sommet variable de T'', ce qui prouve que $h' \circ h$ est bien un homomorphisme clos. ■

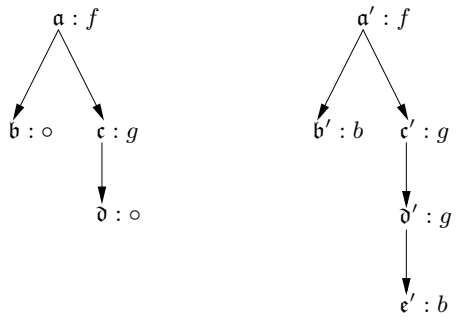

FIG. 5.5 – Les GA-termes T (à gauche) et T' (à droite)

On a les propriétés suivantes, assez évidentes, mais qui serviront fréquemment par la suite.

Propriété 5.2.5 *Soient $T = (V, s, a)$ et $T' = (V', s', a')$ deux GA-termes. S'il existe un homomorphisme h de T vers T', alors :*

1. *Si h est un homomorphisme clos de T vers T', alors h est surjective.*
2. *Soit u un sommet de V et h' la restriction de h à $V|u$. Alors h' est un homomorphisme de $T|u$ vers $T'|h(u)$. De plus, si h est clos (resp. un isomorphisme), alors h' est clos (resp. un isomorphisme).*
3. *Si p est un chemin de u à v dans T, alors $h(p)$ est un chemin de $h(u)$ à $h(v)$ dans T'.*
4. *La relation $\Subset$ est un préordre sur l'ensemble des GA-termes.*
5. *Pour tout GA-terme T, la fonction* id *est un isomorphisme de T vers T.*
6. *Si h est un isomorphisme de T vers T', alors h^{-1} est un isomorphisme de T' vers T.*
7. *La relation d'isomorphisme est une relation d'équivalence sur l'ensemble des GA-termes.*

PREUVE. Les deux premiers points sont des conséquences immédiates de la définition d'un homomorphisme. Le troisième point se démontre trivialement par induction sur la longueur du chemin en se servant du fait que $a'(h(u)) = h(a(u))$. Pour le quatrième point, la reflexivité est triviale, et la relation est transitive d'après la Propriété 5.2.4. Enfin, il est aisé de vérifier que la fonction id est un isomophisme de T vers T, et que si h est un isomorphisme de T vers T', alors h^{-1} est un isomorphisme de T' vers T, et la relation d'isomorphisme est bien une relation d'équivalence sur l'ensemble des GA-termes. ∎

Corollaire 5.2.6 *Soient $T = (V, s, a)$ et $T' = (V', s', a')$ deux GA-termes tels qu'il existe un homomorphisme h de T vers T'. Alors h est unique.*

PREUVE. Supposons qu'il existe un homomorphisme h' de T vers T' et que $h' \neq h$. Il existe donc un sommet u de T tel que $h(u) \neq h'(u)$. Posons $r = \text{racine}(T)$, et $r' =$

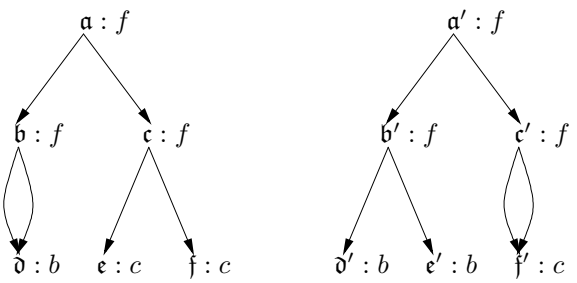

FIG. 5.6 – Deux GA-termes bisimilaires

racine(T'), on a donc $h(r) = h'(r) = r'$. Soit p un chemin de r à u dans T, quitte à remplacer u, on peut supposer que tous les sommets de ce chemin ont la même image par h et h'. Alors, d'après la Propriété 5.2.5 (3), $h(p)$ est un chemin de r' à $h(u)$ dans T', et $h'(p)$ est un chemin de r' à $h'(u)$ dans T'. Comme tous les sommets de ce chemin ont la même image par h et h', on en déduit que $h(p) = h'(p)$, ce qui contredit le fait que $h(u) \neq h'(u)$. ∎

Ainsi, nous pourrons parler de *l'homomorphisme* de T vers T' s'il existe, et cet homomorphisme peut être clos ou non.

Corollaire 5.2.7 *Soient $T = (V, s, a)$ et $T' = (V', s', a')$ deux* GA*-termes, et supposons qu'il existe un homomorphisme clos h de T vers T'. Alors T et T' sont bisimilaires.*

PREUVE. On démontre par induction sur la hauteur de T que $\tau(T) = \tau(T')$. Supposons que ce résultat soit vrai pour tout GA-terme de hauteur inférieure ou égale à k et que T est de hauteur $k+1$. Soient $r = \text{racine}(T)$, et $r' = \text{racine}(T')$, et posons $a(r) = v_1.\cdots.v_n$, et $a'(r') = v'_1.\cdots.v'_n$. D'après la Propriété 5.2.5 (2), pour tout $i = 1, \ldots, n$, la restriction de h à $V|v_i$ est un homomorphisme clos de $T|v_i$ vers $T'|v'_i$, et $T|v_i$ est de hauteur inférieure ou égale à k. Par hypothèse d'induction, on a donc $\tau(T|v_i) = \tau(T'|v'_i)$ pour tout $i = 1, \ldots, n$. Comme $s(r) = s'(r')$, on en déduit que $\tau(T) = \tau(T')$. ∎

Remarque. Si deux GA-termes sont liés par un homomorphisme clos alors ils sont bisimilaires, mais deux GA-termes bisimilaires ne sont pas forcément liés par un homomorphisme. Par exemple, la Figure 5.6 représente deux GA-termes bisimilaires, mais il n'existe aucun homomorphisme de l'un vers l'autre.

Le lemme suivant permet de caractériser les isomorphismes :

Lemme 5.2.8 *Soient $T = (V, s, a)$ et $T' = (V', s', a')$ deux* GA*-termes, et h un homomorphisme de T vers T'. Alors h est un isomorphisme si et seulement si h est clos et injectif.*

PREUVE. Si h est un isomorphisme, il est évident que c'est un homomorphisme clos et injectif, il s'agit donc de démontrer que la réciproque est également vraie.

Si h est un homomorphisme clos, alors, d'après la Propriété 5.2.5 (1), h est surjectif, et donc, si h est également injectif, c'est une bijection. Nous allons montrer que h^{-1} est un homomorphisme de T' vers T. Soit u' un sommet de T', et $u = h^{-1}(u')$. Il s'agit de montrer que $s(u) = s'(u')$, et que $a(u) = h^{-1}(a'(u'))$. Ceci est évident : comme h est un homomorphisme, on sait que $s'(h(u)) = s(u)$, et donc, on a bien $s'(u') = s(u)$. De même, comme $a'(h(u)) = h(a(u))$, on a

$$h^{-1}(a'(u')) = h^{-1}(a'(h(u))) = a(u).$$ ∎

Définition 5.2.9 ($\eta(T)$) Soient $T = (V, s, a)$ un GA-terme, et $\eta : V \to V'$ une bijection de V vers V'. Alors on définit le graphe étiqueté $\eta(T) = (V', s', a')$, où les fonctions s' et a' sont définies de la façon suivante :

- pour tout $v \in V$, $s'(\eta(v)) = s(v)$,
- pour tout $v \in V$, pour tout $i \in \{1, \ldots, \text{arité}(s(v))\}$, $a'(\eta(v))_i = \eta(a(v)_i)$. ◇

Il est alors aisé de vérifier que :

Propriété 5.2.10 *Le graphe étiqueté $\eta(T)$ est un* GA*-terme, et η est un isomorphisme de T vers $\eta(T)$.*

Nous démontrons maintenant une propriété de décomposition vérifiée par des GA-termes bisimilaires.

Lemme 5.2.11 *Soient T, T' et T'' trois* GA*-termes tels qu'il existe des homomorphismes h et h', respectivement de T'' vers T et de T'' vers T'. Si T et T' sont bisimilaires, alors pour tout sommet v de T'', on a $T|h(v) \stackrel{\circ}{=} T'|h'(v)$.*

PREUVE. Posons $T = (V, s, a)$, $T' = (V', s', a')$ et $T'' = (V'', s'', a'')$, et démontrons le résultat par induction sur la hauteur de v. Si v est la racine de T'', alors le résultat est trivial, supposons maintenant que le résultat est vrai pour tout sommet de hauteur strictement inférieure à n, et que p est de hauteur n. Soit $u \in V''$ et $i \in \{1, \ldots, \text{arité}(s''(u))\}$ tels que $v = a''(u)_i$, alors par hypothèse d'induction, on a $T|h(u) \stackrel{\circ}{=} T'|h'(u)$, et par définition d'un homomorphisme, $h(v) = a(h(u))_i$, et $h'(v) = a'(h'(u))_i$. Ceci prouve bien que $T|h(v) \stackrel{\circ}{=} T'|h'(v)$. ∎

Homomophismes et chemins

Nous allons maintenant étudier de quelle façon les homomorphismes transforment les chemins dans un GA-terme.

Lemme 5.2.12 *Soient $T = (V, s, a)$ un* GA*-terme de racine r, $T' = (V', s', a')$ un* GA*-terme de racine r', et supposons qu'il existe un homomorphisme clos h de T vers T'. Alors pour tout chemin p' de source r' dans T', il existe un unique chemin p de source r dans T tel que $p' = h(p)$.*

PREUVE. On démontre le résultat par induction sur la longueur de p'. Supposons que le résultat soit vrai pour tous les chemins de source r' dans T', de longueur inférieure ou égale à k, et que p' est de longueur $k+1$. On pose

$$p' = q'.u'.i,$$

où q' est par définition un chemin de r à u' dans T'. Par hypothèse d'induction, il existe un chemin (unique) q de source r dans T tel que $q' = h(q)$; q est donc un chemin de r à u dans T, où $u' = h(u)$.

Comme h est un homomorphisme clos, on a $s(u) = s'(u')$, ce qui prouve que $p = q.u.i$ est bien un chemin dans T, et qu'on a $p' = h(p)$. L'unicité de p est alors évidente. ∎

On a également une réciproque plus faible du Lemme 5.2.12 : si une fonction h transforme les chemins d'un GA-terme T en des chemins d'un GA-terme T' et vérifie certaines propriétés supplémentaires, alors h est un homomorphisme de T vers T'.

Lemme 5.2.13 *Soient deux* GA*-termes $T = (V, s, a)$ et $T' = (V', s', a')$ de racines respectives r et r', et une fonction $h : V \to V'$ telle que pour tout sommet $v \in V$:*

- *si v est un sommet non-variable, alors $s(v) = s'(h(v))$,*
- *si p est un chemin de r à v dans T, alors $h(p)$ est un chemin de r' à $h(v)$ dans T'.*

Alors h est un homomorphisme de T vers T'.

PREUVE. Il s'agit de prouver que pour tout v, on a $a'(h(v)) = h(a(v))$. Soit v un sommet de V, et p un chemin de r à v. On pose $a(v) = v_1.\cdots.v_n$, et soit i compris entre 1 et n. Alors, $p.v.i$ est un chemin dans T de r à v_i par définition, et donc, $h(p).h(v).i$ est par hypothèse un chemin dans T' de r' à $h(v_i)$. Ce qui prouve que $a'(h(v))_i = h(a(v))_i$, d'où le résultat. ∎

Les hypothèses du Lemme 5.2.13 peuvent être simplifiées quand on considère des A-termes :

Corollaire 5.2.14 *Soient $A = (V, s, a)$ et $A' = (V', s', a')$ deux* A*-termes de racines respectives r et r', tels que pour tout sommet non-variable v de A, si p est le chemin de r à v dans A, alors il existe dans A' un chemin de source r' et parallèle à p, dont le puits v' vérifie $s(v) = s'(v')$. Alors il existe un homomorphisme de A vers A'.*

PREUVE. Soit la fonction $h : V \to V'$ définie par : pour tout chemin p de r à v dans A, si p' est le chemin dans A' de source r' et parallèle à p, alors $h(v)$ est le puits de p'. Comme A et A' sont des A-termes, cette fonction est bien définie, et une induction triviale sur la longueur de p prouve que $h(p)$ est un chemin dans A' de source r' et de puits $h(v)$. D'après le Lemme 5.2.13, h est bien un homomorphisme de A vers A'. ∎

A-termes et homomorphismes

Nous allons maintenant nous servir de la propriété d'unicité des chemins dans les A-termes pour démontrer un certain nombre de résultats vérifiés par ces derniers.

Lemme 5.2.15 *Soient $A = (V, s, a)$ un* A*-terme, et $T_1 = (V_1, s_1, a_1)$ et $T_2 = (V_2, s_2, a_2)$ des* GA*-termes bisimilaires. S'il existe un homomorphisme h de A vers T_1, alors il existe également un homomorphisme de A vers T_2.*

PREUVE. Notons respectivement r, r_1 et r_2 les racines de A, T_1 et T_2, comme T_1 et T_2 sont bisimilaires, il est clair que r_1 et r_2 sont étiquetées par le même symbole. Nous démontrons le résultat par induction sur la hauteur de A. Si A est réduit à sa racine, alors le résultat est évident. Sinon, r, r_1 et r_2 sont nécessairement étiquetées par le même symbole de fonction. On pose

$$\begin{aligned} a(r) &= u_1.\cdots.u_n \\ a_1(r_1) &= v_1.\cdots.v_n \\ a_2(r_2) &= w_1.\cdots.w_n. \end{aligned}$$

D'après la Propriété 5.2.5 2, pour tout $i = 1, \ldots, n$, une restriction de h est un homomorphisme de $A|u_i$ vers $T_1|v_i$, et comme $T_1|v_i$ et $T_2|w_i$ sont bisimilaires, par hypothèse d'induction, il existe un homomorphisme h_i de $A|u_i$ vers $T_2|w_i$. Il est alors aisé de vérifier que la fonction

$$h' = \{\langle r, r_2\rangle\} \cup \bigcup_{i=1}^{n} h_i$$

est un homomorphisme de A vers T_2. ∎

Lemme 5.2.16 *Soit T un* GA*-terme, A un* A*-terme, et supposons qu'il existe un homomorphisme h de T vers A. Alors T est un* A*-terme, et h est injectif.*

PREUVE. Notons r la racine de T, et supposons qu'il existe un homomorphisme h de T vers A. Si T n'est pas un A-terme, alors il existe un sommet v et deux chemins distincts p et p' de r à v dans T. D'après le Lemme 5.1.5 et la Propriété 5.2.5 3, $h(p)$ et $h(p')$ sont alors deux chemins distincts de $h(r)$ à $h(v)$ dans A, ce qui contredit le fait que A est un A-terme.

Supposons maintenant que h n'est pas injectif. Il existe donc deux sommets v et v' de T tels que $h(v) = h(v')$. Alors, comme précédemment, si p est un chemin de r à v, et p' un chemin de r à v' dans T, alors $h(p)$ et $h(p')$ sont deux chemins distincts de $h(r)$ à $h(v) = h(v')$ dans A, et on aboutit à la même contradiction. ∎

Nous avons vu que la réciproque du Corollaire 5.2.7 est fausse en général. Nous montrons maintenant que si un des deux GA-termes considérés est un A-terme, alors cette réciproque est vraie.

Lemme 5.2.17 *Soient $A = (V, s, a)$ un* A*-terme, et $T = (V', s', a')$ un* GA*-terme. Si A et T sont bisimilaires, alors il existe un homomorphisme clos de A vers T.*

PREUVE. Notons r la racine de A, et r' celle de T ; nous démontrons le résultat par induction sur la hauteur h de A. Supposons que ce résultat soit vrai pour tout A-terme et GA-terme de hauteur inférieure ou égale à k, et que A est de hauteur $k+1$. On pose

$$a(r) \;=\; v_1.\cdots.v_n, \text{ et } a'(r') \;=\; v'_1.\cdots.v'_n,$$

alors, pour tout $i = 1,\ldots,n$, on a $A|v_i \mathrel{\mathring{=}} T|v'_i$, et donc, par hypothèse d'induction, on en déduit qu'il existe un homomorphisme clos h_i de $A|v_i$ vers $T|v'_i$. De plus, comme A est un A-terme, on a :

$$\forall i,j \in \{1,\ldots,n\},\ (i \neq j) \;\Rightarrow\; (V|v_i \cap V|v_j = \emptyset).$$

Ceci prouve que la fonction

$$h \;=\; \{\langle r, r'\rangle\} \uplus \biguplus_{i=1}^{n} h_i$$

est bien définie, et on a :

$$a'(h(r)) = a'(r') = v'_1.\cdots.v'_n = h(v_1).\cdots.h(v_n) = h(v_1.\cdots.v_n) = h(a(r)).$$

Donc, h est bien un homomorphisme clos de A vers T, ce qui prouve le résultat. ∎

On en déduit les résultats suivants :

Corollaire 5.2.18 *Deux A-termes bisimilaires sont isomorphes.*

PREUVE. Soient A et A' deux A-termes bisimilaires. Alors d'après le Lemme 5.2.17, il existe un homomorphisme clos de A vers A', qui est injectif d'après le Lemme 5.2.16 ; c'est donc un isomorphisme d'après le Lemme 5.2.8.

Corollaire 5.2.19 *Soient T et T' deux GA-termes, et A et A' deux A-termes tels que $T \Subset A$ et $T' \Subset A'$. Si T et T' sont bisimilaires, alors A et A' sont isomorphes.*

PREUVE. Ceci est évident : d'après le Corollaire 5.2.7, A et T sont bisimilaires, tout comme A' et T'. On a donc :

$$A \mathrel{\mathring{=}} T \mathrel{\mathring{=}} T' \mathrel{\mathring{=}} A',$$

et par transitivité, $A \mathrel{\mathring{=}} A'$. Enfin, en appliquant le Corollaire 5.2.18, on en déduit que ces A-termes sont isomorphes. ∎

La propriété d'unicité des chemins fait qu'il est souvent plus simple de travailler avec des A-termes qu'avec des GA-termes. Plus tard, nous prouverons assez facilement des résultats sur les A-termes, puis nous les généraliserons aux GA-termes. Ceci sera possible grâce à la propriété suivante de [BvEG+87] :

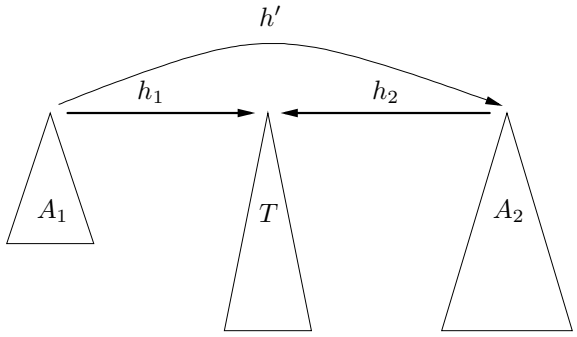

FIG. 5.7 – Lemme 5.2.21

Théorème 5.2.20 *Pour tout* GA*-terme T, il existe un* A*-terme A tel que $T \Subset A$, et cet* A*-terme est unique à isomorphisme près.*

Dans [BvEG+87], une construction explicite d'un tel A-terme est donnée, mais nous n'en aurons pas besoin dans cet exposé : seul le résultat de son existence sera nécessaire.

Le Lemme 5.2.16 prouve qu'un homomorphisme d'un GA-terme vers un A-terme vérifie nécessairement certaines propriétés. En général, il est plus difficile de savoir quelles propriétés sont vérifiées par un homomorphisme d'un A-terme vers un GA-terme quelconque. On a néanmoins le résultat suivant :

Lemme 5.2.21 *Soient T un* GA*-terme, et A_1, A_2 deux* A*-termes tels que :*

1. *il existe un homomorphisme h_1 de A_1 vers T,*
2. *il existe un homomorphisme clos h_2 de A_2 vers T.*

Alors il existe un homomorphisme injectif de A_1 vers A_2 (voir la Figure 5.7).

PREUVE. On pose $A_1 = (V_1, s_1, a_1)$, $A_2 = (V_2, s_2, a_2)$ et $T = (V, s, a)$, et on note r_1, r_2 et r leurs racines respectives.

Soit v un élément de V_1, et notons p_1 le chemin (unique) de r_1 à v dans A_1. Alors il existe un unique chemin p_2 de source r_2 dans A_2 tel que $h_2(p_2) = h_1(p_1)$ d'après le Lemme 5.2.12, et comme $h_1(p_1)$ est un chemin de r à $h_1(v)$ dans T d'après la Propriété 5.2.5 (3), $h_2(p_2)$ est également un chemin de r à $h_1(v)$ dans T. Soit v' le puits de p_2, on pose $h'(v) = v'$. On définit ainsi une fonction $h' : V_1 \to V_2$, et il est aisé de vérifier que pour tout v, si p_1 est le chemin de r_1 à v dans A_1, alors $h'(p_1)$ est le chemin de r_2 à $h'(v)$ dans A_2. Nous allons montrer que h' est un homomorphisme de A_1 vers A_2.

Soit v un élément de $V_1 \setminus \mathcal{SV}(A_1)$, et soit p_1 le chemin de r_1 à v dans A_1. Soit p_2 le chemin de A_2 tel que $h_2(p_2) = h_1(p_1)$. Par définition de h', p_2 est un chemin de r_2 à $h'(v)$ dans A_2, et comme $h_2(p_2)$ est un chemin de r à $h_1(v)$ dans T, on a

$$s_2(h'(v)) \;=\; s(h_1(v)) \;=\; s_1(v).$$

Le Lemme 5.2.13 montre alors que h' est bien un homomorphisme de A_1 vers A_2, et cet homomorphisme est injectif d'après le Lemme 5.2.16. ∎

5.3 Unifiabilité de A-termes

Dans cette partie, nous allons définir les notions de subsomption et d'unifiabilité pour des A-termes. Certains des résultats de cette partie sont également valables pour les GA-termes, mais nous cherchons à introduire des notions parallèles à celles de subsomption et d'unifiabilité pour des termes linéaires ; c'est pourquoi nous ne les démontrerons que pour les A-termes.

Définition 5.3.1 (Subsomption) Soient A un A-terme, et T un GA-terme. Si pour un sommet v de T, il existe un homomorphisme h de A vers $T|v$, on dira que A *subsume* T en v, ou que $T|v$ est une *instance* de A, et on notera $h, v : A \trianglelefteq T$.

Si v est la racine de T, alors on notera $h : A \sqsubseteq T$, ou simplement $A \sqsubseteq T$. ◇

La Propriété 5.2.4 permet alors de prouver que

Propriété 5.3.2 *La relation $\sqsubseteq$ est un préordre sur l'ensemble des A-termes.*

PREUVE. La reflexivité est triviale, et la Propriété 5.2.4 prouve que la relation est transitive. ■

On a donc une relation d'ordre sur l'ensemble quotient associé à cette relation, et nous montrons maintenant que cet ensemble quotient est constitué de l'ensemble des classes d'isomorphisme de A-termes.

Lemme 5.3.3 *La relation $\sqsubseteq$ est une relation d'ordre sur l'ensemble des A-termes quotienté par la relation $\simeq$.*

PREUVE. Il suffit de prouver que pour tous A-termes A, A', $A \simeq A'$ si et seulement si $A \sqsubseteq A'$ et $A' \sqsubseteq A$. Si η est l'isomorphisme de A vers A', alors il est clair que $\eta : A \sqsubseteq A'$ et $\eta^{-1} : A' \sqsubseteq A$. Réciproquement, si $h : A \sqsubseteq A'$ et $h' : A' \sqsubseteq A$, alors $h' \circ h$ est un homomorphisme de A vers A d'après la Propriété 5.2.4, et comme id est un homomorphisme de A vers A d'après la Propriété 5.2.5, on en déduit que $h' \circ h = \mathrm{id}$ par unicité des homomorphismes (Corollaire 5.2.6). Par symétrie, on a également $h \circ h' = \mathrm{id}$, et on en déduit que $h' = h^{-1}$; ces deux fonctions sont donc des isomorphismes, d'où $A \simeq A'$. ■

Nous montrons maintenant que la relation $\sqsubseteq$ est compatible avec la relation d'isomorphisme sur les A-termes.

Propriété 5.3.4 *Soient A_1, A_2, A'_1 et A'_2 des A-termes tels que $A_1 \sqsubseteq A_2$, $A_1 \simeq A'_1$, et $A_2 \simeq A'_2$. Alors $A'_1 \sqsubseteq A'_2$*

PREUVE. Si η_i est l'isomorphisme de A_i vers A'_i pour $i = 1, 2$, et si h est l'homomorphisme de A_1 vers A_2, alors il est clair que $\eta_2 \circ h \circ \eta_1^{-1}$ est un homomorphisme de A'_1 vers A'_2, ce qui prouve le résultat. ■

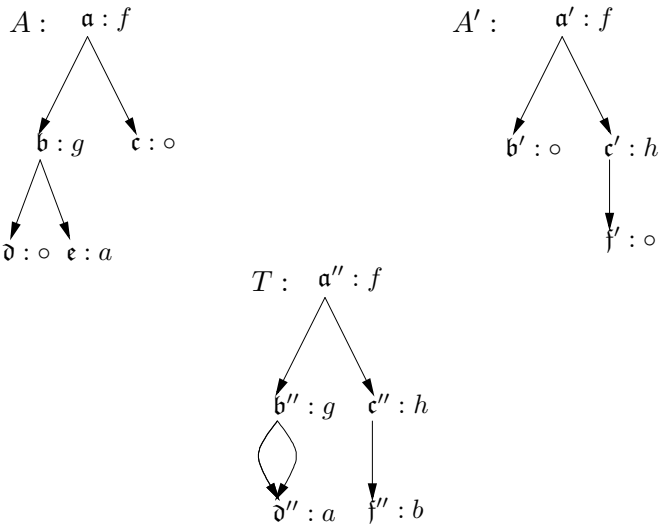

FIG. 5.8 – Exemple 5.3.6

Définition 5.3.5 (Unifiabilité) Deux A-termes A et A' sont dits *unifiables* si et seulement s'il existe un GA-terme T et des homomorphismes h et h', respectivement de A vers T et de A' vers T. ◇

Exemple 5.3.6 Notons respectivement A et A' les deux A-termes de la Figure 5.8, et T le GA-terme de la même figure. Alors A et A' sont unifiables, puisque les fonctions h et h' définies par :

v	$\mathfrak{a}$	$\mathfrak{b}$	$\mathfrak{c}$	$\mathfrak{d}$	$\mathfrak{e}$
$h(v)$	$\mathfrak{a}''$	$\mathfrak{b}''$	$\mathfrak{c}''$	$\mathfrak{d}''$	$\mathfrak{d}''$

v	$\mathfrak{a}'$	$\mathfrak{b}'$	$\mathfrak{c}'$	$\mathfrak{f}'$
$h'(v)$	$\mathfrak{a}''$	$\mathfrak{b}''$	$\mathfrak{c}''$	$\mathfrak{f}''$

sont respectivement des homomorphismes de A vers T et de A' vers T.

Nous avons le lemme de décomposition suivant, qui nous permettra par la suite d'effectuer des démonstrations par induction sur la hauteur des GA-termes considérés :

Lemme 5.3.7 *Soient $A = (V, s, a)$ et $A' = (V', s', a')$ deux A-termes unifiables de racines respectives r et r', et supposons que $a(r) = v_1.\cdots.v_n$, et que $a'(r') = v'_1.\cdots.v'_n$. Alors pour tout $i = 1, \ldots, n$, $A|v_i$ et $A'|v'_i$ sont unifiables.*

PREUVE. Soit T un GA-terme tel qu'il existe des homomorphismes h et h' respectivement de A vers T et de A' vers T. Alors, d'après la Propriété 5.2.5 (2), pour tout $i = 1, \ldots, n$,

une restriction de h (resp. h') est un homomorphisme de $A|v_i$ (resp. $A'|v'_i$) vers $T|h(v_i)$ (resp. $T|h'(v'_i)$) ; et comme $h(v_i)$ et $h'(v'_i)$ sont tous deux le $i^{\text{ème}}$ argument de la racine de T, ces éléments sont égaux, ce qui prouve bien que $A|v_i$ et $A'|v'_i$ sont unifiables. ■

Nous démontrons maintenant la réciproque du Lemme 5.3.7.

Lemme 5.3.8 *Soient $A = (V, s, a)$ et $A' = (V', s', a')$ deux* A*-termes de racines respectives r et r' telles que $s(r) = s'(r')$. Posons $a(r) = v_1.\cdots.v_n$, $a'(r') = v'_1.\cdots.v'_n$, et supposons que pour tout $i = 1, \ldots, n$, $A|v_i$ et $A'|v'_i$ sont unifiables. Alors A et A' sont unifiables.*

PREUVE. Soit $i \in \{1, \ldots, n\}$, comme par hypothèse $A|v_i$ et $A'|v'_i$ sont unifiables, il existe un GA-terme $T_i = (V'_i, s'_i, a'_i)$ de racine r'_i, et des homomorphismes h_i et h'_i, respectivement de A vers T_i, et de A' vers T_i. On considère le GA-terme $T = (V'', s'', a'')$, où $V'' = \{r''\} \uplus \bigcup V_i$, qui est de racine r'' et qui vérifie :
- $s''(r'') = s(r)$,
- $a''(r'') = r'_1.\cdots.r'_n$,
- $\forall i = 1, \ldots, n$, $T|r'_i = T_i$.

T est bien un GA-terme, et il est clair que les fonctions

$$h = \{\langle r, r''\rangle\} \cup \bigcup_{i=1}^{n} h_i \text{ et } h' = \{\langle r', r''\rangle\} \cup \bigcup_{i=1}^{n} h'_i$$

sont des homomorphismes, respectivement de A vers T et de A' vers T, ce qui prouve le résultat. ■

Lemme 5.3.9 *Soient A, A_1 et A_2 trois* A*-termes tels que A_1 et A_2 sont unifiables, $h_1 : A \sqsubseteq A_1$, et $h_2 : A \sqsubseteq A_2$. Alors pour tout sommet v de A, $A_1|h_1(v)$ et $A_2|h_2(v)$ sont unifiables.*

PREUVE. Comme A_1 et A_2 sont unifiables, il existe un GA-terme T et des homomorphismes h'_1 et h'_2, respectivement de A_1 vers T, et de A_2 vers T. Alors d'après la Propriété 5.2.4, $h = h'_1 \circ h_1$ est un homomorphisme de A vers T, et de même, $h' = h'_2 \circ h_2$ est un homomorphisme de A vers T. D'après le Corollaire 5.2.6, on a $h = h'$, et d'après la Propriété 5.2.5 (2), pour tout sommet v de A, (une restriction de) h_i est un homomorphisme de $A_i|h_i(v)$ vers $T|h(v)$, pour $i = 1, 2$. Donc, $A_1|h_1(v)$ et $A_2|h_2(v)$ sont bien unifiables. ■

Nous définissons maintenant la notion de "plus petite instance" (ou *instance la plus générale*) de A-termes unifiables, et nous prouvons que cette plus petite instance est unique à isomorphisme près.

Définition 5.3.10 Soient $A = (V, s, a)$ et $A' = (V', s', a')$ deux A-termes unifiables, de racines respectives r et r'. Quitte à prendre un A-terme isomorphe à A', on peut supposer que $V \cap V' = \emptyset$. Alors on note $A \sqcup A' = (V'', s'', a'')$ le A-terme défini par induction sur la hauteur de A de la façon suivante :

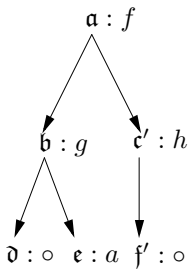

FIG. 5.9 – Exemple 5.3.11

- $V'' \subseteq V \cup V'$,
- si $s(r) = \circ$, alors $A \sqcup A' = A'$,
- sinon si $s'(r') = \circ$, alors $A \sqcup A' = A$,
- sinon, on pose $a(r) = v_1.\cdots.v_n$, $a'(r') = v'_1.\cdots.v'_n$, et $A \sqcup A'$ est le A-terme de racine r tel que $s''(r) = s(r)$, et si $a''(r) = w_1.\cdots.w_n$, alors pour tout $i = 1, \ldots, n$, w_i est la racine de $A|v_i \sqcup A'|v'_i$. ◇

Exemple 5.3.11 Reprenons les A-termes de l'Exemple 5.3.6, alors le A-terme $A \sqcup A' = (V'', s'', a'')$ est défini par (voir la Figure 5.9) :

v	$\mathfrak{a}$	$\mathfrak{b}$	$\mathfrak{c}'$	$\mathfrak{d}$	$\mathfrak{e}$	$\mathfrak{f}'$
$s''(v)$	f	g	h	$\circ$	a	$\circ$
$a''(v)$	$\mathfrak{b}.\mathfrak{c}'$	$\mathfrak{d}.\mathfrak{e}$	$\mathfrak{f}'$	ε	ε	ε

Une induction triviale prouve que $A \sqcup A'$ est un A-terme, nous allons montrer plusieurs propriétés vérifiées par ce A-terme, et en particulier qu'il est une plus petite instance de A et de A'.

Nous commençons par prouver que $A \sqcup A'$ est bien un majorant de A et de A' :

Lemme 5.3.12 *Si A et A' sont unifiables, alors $A \sqsubseteq A \sqcup A'$ et $A' \sqsubseteq A \sqcup A'$.*

PREUVE. On pose $A = (V, s, a)$, $A \sqcup A' = (V'', s'', a'')$ et on démontre le résultat par induction. On note respectivement r et r'' les racines de A et $A \sqcup A'$; si $s(r) = \circ$, alors le résultat est trivial. Sinon, on pose $a(r) = v_1.\cdots.v_n$, et $a''(r'') = w_1.\cdots.w_n$; par hypothèse d'induction, pour tout $i = 1, \ldots, n$, il existe un homomorphisme h_i de $A|v_i$ vers $A \sqcup A'|w_i$. Comme A et $A \sqcup A'$ sont des A-termes, il est aisé de vérifier que la fonction

$$h \;=\; \{\langle r, r''\rangle\} \cup \bigcup_{i=1}^{n} h_i$$

est un homomorphisme de A vers $A \sqcup A'$.

La preuve qu'il existe un homomorphisme de A' vers $A \sqcup A'$ est identique. ■

Corollaire 5.3.13 *Soient A, A_1 et A_2 trois* A*-termes tels que $A \sqsubseteq A_1$, et supposons que A_1 et A_2 sont unifiables. Alors $A \sqsubseteq A_1 \sqcup A_2$.*

PREUVE. D'après le Lemme 5.3.12, on a $A_1 \sqsubseteq A_1 \sqcup A_2$, et d'après la Propriété 5.3.2, $A \sqsubseteq A_1 \sqcup A_2$. ∎

Lemme 5.3.14 *Soient A, A_1 et A_2 trois* A*-termes tels que A_1 et A_2 sont unifiables, $h_1 : A \sqsubseteq A_1$, et $h_2 : A \sqsubseteq A_2$. Si h est l'homomorphisme de A vers $A_1 \sqcup A_2$, alors pour tout sommet v de A, on a*

$$A_1|h_1(v) \sqcup A_2|h_2(v) = (A_1 \sqcup A_2)|h(v).$$

PREUVE. L'homomorphisme h est bien défini d'après le Corollaire 5.3.13, et $A_1|h_1(v)$ et $A_2|h_2(v)$ sont unifiables d'après le Lemme 5.3.9. On note r la racine de A, r_i la racine de A_i pour $i = 1, 2$, et r' la racine de $A_1 \sqcup A_2$. Si $v = r$, alors le résultat est trivial, supposons donc que $v \neq r$, nous démontrons le résultat par induction sur la longueur du chemin p de r à v dans A. Si $p = r.j$, alors v est le $j^{\text{ème}}$ argument de r, et d'après la Propriété 5.2.5 (3), $h_i(v)$ est le $j^{\text{ème}}$ argument de r_i pour $i = 1, 2$, et $h(v)$ est le $j^{\text{ème}}$ argument de r'. Par construction, on a bien $A_1|h_1(v) \sqcup A_2|h_2(v) = (A_1 \sqcup A_2)|h(v)$.

Supposons maintenant que $p = q.u.j$, où q est le chemin non vide de r à u dans A, alors, par hypothèse d'induction, on a

$$A_1|h_1(u) \sqcup A_2|h_2(u) = (A_1 \sqcup A_2)|h(u).$$

On pose $A'_i = A_i|h_i(u)$ pour $i = 1, 2$, alors $(A_1 \sqcup A_2)|h(u) = A'_1 \sqcup A'_2$. Comme précédemment, v est le $j^{\text{ème}}$ argument de la racine de $A|u$, et donc, $h_i(v)$ est également le $j^{\text{ème}}$ argument de la racine de A'_i pour $i = 1, 2$, et $h(v)$ est le $j^{\text{ème}}$ argument de la racine de $A'_1 \sqcup A'_2$; comme $A'_i|h_i(v) = A_i|h_i(v)$ pour $i = 1, 2$ et $(A'_1 \sqcup A'_2)|h(v) = (A_1 \sqcup A_2)|h(v)$, on a le résultat. ∎

Nous pouvons maintenant montrer que si A_1 et A_2 sont des A-termes unifiables, alors $A_1 \sqcup A_2$ est un plus petit majorant de A_1 et A_2.

Théorème 5.3.15 *Soient A_1, A_2 et A' trois* A*-termes tels que $h_1 : A_1 \sqsubseteq A'$ et $h_2 : A_2 \sqsubseteq A'$. Alors il existe un homomorphisme $h : A_1 \sqcup A_2 \sqsubseteq A'$.*

PREUVE. Voir Annexe A, page 193 ∎

Corollaire 5.3.16 *Supposons que $A \sqsubseteq A'$, alors $A \sqcup A' \simeq A'$.*

PREUVE. D'après le Lemme 5.3.12, $A' \sqsubseteq A \sqcup A'$, et comme $A \sqsubseteq A'$ et $A' \sqsubseteq A'$, d'après le Théorème 5.3.15, $A \sqcup A' \sqsubseteq A'$. ∎

En particulier, on a l'idempotence de l'opérateur $\sqcup$ modulo isomorphisme.

Exemple 5.3.17 Reprenons les A-termes A et A', ainsi que le GA-terme T de l'Exemple 5.3.6 (voir la Figure 5.8). Le A-terme $A \sqcup A'$ est représenté dans la Figure 5.9, et la fonction h'' définie par

v	$\mathfrak{a}$	$\mathfrak{b}$	$\mathfrak{c}'$	$\mathfrak{d}$	$\mathfrak{e}$	$\mathfrak{f}'$
$h''(v)$	$\mathfrak{a}''$	$\mathfrak{b}''$	$\mathfrak{c}''$	$\mathfrak{d}''$	$\mathfrak{d}''$	$\mathfrak{f}''$

est un homomorphisme de $A \sqcup A'$ vers T.

Le corollaire suivant montre qu'on a la commutativité de l'opérateur $\sqcup$ modulo isomorphisme.

Corollaire 5.3.18 *Si A et A' sont des* A*-termes unifiables, alors $A \sqcup A' \simeq A' \sqcup A$.*

PREUVE. D'après le Lemme 5.3.12, on a $A \sqsubseteq A' \sqcup A$ et $A' \sqsubseteq A' \sqcup A$, et d'après le Théorème 5.3.15, on en déduit que $A \sqcup A' \sqsubseteq A' \sqcup A$. Par symétrie, on a également $A' \sqcup A \sqsubseteq A \sqcup A'$, ce qui prouve que ces deux A-termes sont bien isomorphes d'après le Lemme 5.3.3. ∎

On a également la compatibilité de l'opérateur $\sqcup$ par rapport aux isomorphismes.

Corollaire 5.3.19 *Soient A_1, A'_1, A_2 et A'_2 des* A*-termes tels que $A_1 \simeq A'_1$ et $A_2 \simeq A'_2$, et A_1 et A_2 sont unifiables. Alors A'_1 et A'_2 sont unifiables, et $A_1 \sqcup A_2 \simeq A'_1 \sqcup A'_2$.*

PREUVE. Puisque A_1 et A_2 sont unifiables, il existe un GA-terme T et des homomorphismes h_1 et h_2 respectivement de A_1 vers T et de A_2 vers T. Soient η_1 et η_2 les isomorphismes de A'_1 vers A_1 et de A'_2 vers A_2, respectivement. Alors d'après la Propriété 5.2.4, pour $i = 1, 2$, $h_i \circ \eta_i$ est un homomorphisme de A'_i vers T, ce qui prouve que A'_1 et A'_2 sont unifiables.

Comme pour $i = 1, 2$, on a $A_i \sqsubseteq A'_i$, on en déduit que $A_i \sqsubseteq A'_1 \sqcup A'_2$ d'après le Corollaire 5.3.13. D'après le Théorème 5.3.15, on a donc $A_1 \sqcup A_2 \sqsubseteq A'_1 \sqcup A'_2$. Par symétrie, on a également $A'_1 \sqcup A'_2 \sqsubseteq A_1 \sqcup A_2$, d'où le résultat. ∎

Démontrons maintenant la monotonie de l'opérateur $\sqcup$ par rapport au préordre $\sqsubseteq$.

Corollaire 5.3.20 *Soient A_1, A'_1, A_2 et A'_2 des* A*-termes tels que $h_1 : A_1 \sqsubseteq A'_1$, et $h_2 : A_2 \sqsubseteq A'_2$. Si A'_1 et A'_2 sont unifiables, alors A_1 et A_2 sont unifiables, et $A_1 \sqcup A_2 \sqsubseteq A'_1 \sqcup A'_2$.*

PREUVE. Soit T le GA-terme tel qu'il existe des homomorphismes h'_1 et h'_2, respectivement de A'_1 vers T, et de A'_2 vers T. Alors d'après la Propriété 5.2.4, $h'_1 \circ h_1$ et $h'_2 \circ h_2$ sont des homomorphismes, respectivement de A_1 vers T et de A_2 vers T, ce qui prouve que A_1 et A_2 sont unifiables.

Comme $A_1 \sqsubseteq A'_1$, alors $A_1 \sqsubseteq A'_1 \sqcup A'_2$ d'après le Corollaire 5.3.13, et de même, $A_2 \sqsubseteq A'_1 \sqcup A'_2$; d'après le Théorème 5.3.15, on a donc $A_1 \sqcup A_2 \sqsubseteq A'_1 \sqcup A'_2$. ∎

Nous prouvons que l'opérateur $\sqcup$ est compatible avec la relation d'unifiabilité :

Lemme 5.3.21 *Si A, A' et A'' sont trois* A*-termes unifiables deux à deux, alors $A \sqcup A'$ et A'' sont également unifiables.*

PREUVE. On pose $A = (V, s, a)$, $A' = (V', s', a')$, et $A'' = (V'', s'', a'')$, on note r, r' et r'' leurs racines respectives, et on démontre le résultat par induction sur la hauteur de A. Si l'une des trois racines est étiquetée par le symbole $\circ$, alors le résultat est trivial ; par exemple, si $s(r) = \circ$, alors $A \sqcup A' = A'$ est bien unifiable avec A''. On suppose maintenant qu'aucune de ces trois racines n'est étiquetée par le symbole $\circ$, elles sont donc étiquetées par le même symbole de Σ. On pose $A \sqcup A' = (V_1, s_1, a_1)$, on note r_1 sa racine, et on pose

$$\begin{aligned} a(r) &= v_1.\cdots.v_n, & a'(r') &= v'_1.\cdots.v'_n, \\ a''(r'') &= w_1.\cdots.w_n, & a_1(r_1) &= u_1.\cdots.u_n. \end{aligned}$$

Pour $i \in \{1, \ldots, n\}$, on pose $A_i = A|v_i$, et on définit de façon similaire A'_i et A''_i. Alors, d'après le Lemme 5.3.7, pour tout $i = 1, \ldots, n$, A_i, A'_i et A''_i sont mutuellement unifiables. Par hypothèse d'induction, on en déduit que $A_i \sqcup A'_i$ et A''_i sont unifiables, et comme $A_i \sqcup A'_i = (A \sqcup A')|u_i$ par définition, pour tout $i = 1, \ldots, n$, $(A \sqcup A')|u_i$ et $A''|w_i$ sont unifiables. D'après le Lemme 5.3.8, $A \sqcup A'$ et A'' sont donc bien unifiables. ∎

Nous pouvons maintenant prouver l'associativité de l'opérateur $\sqcup$ modulo isomorphisme.

Théorème 5.3.22 *Soient A_1, A_2 et A_3 trois* A*-termes unifiables deux à deux, alors*

$$(A_1 \sqcup A_2) \sqcup A_3 \;\simeq\; A_1 \sqcup (A_2 \sqcup A_3).$$

PREUVE. Comme $A_2 \sqsubseteq A_2 \sqcup A_3$ d'après le Lemme 5.3.12, on a $A_1 \sqcup A_2 \sqsubseteq A_1 \sqcup (A_2 \sqcup A_3)$ d'après le Corollaire 5.3.20. De même, comme $A_3 \sqsubseteq A_2 \sqcup A_3$, on a également $A_3 \sqsubseteq A_1 \sqcup (A_2 \sqcup A_3)$, et d'après le Théorème 5.3.15, $(A_1 \sqcup A_2) \sqcup A_3 \sqsubseteq A_1 \sqcup (A_2 \sqcup A_3)$.

De la même façon, on peut prouver que $(A_3 \sqcup A_2) \sqcup A_1 \sqsubseteq A_3 \sqcup (A_2 \sqcup A_1)$. D'après le Corollaire 5.3.18, on a

$$\begin{aligned} (A_3 \sqcup A_2) \sqcup A_1 &\simeq (A_2 \sqcup A_3) \sqcup A_1 \\ &\simeq A_1 \sqcup (A_2 \sqcup A_3). \end{aligned}$$

Le même raisonnement prouve que $A_3 \sqcup (A_2 \sqcup A_1) \simeq (A_1 \sqcup A_2) \sqcup A_3$, et donc, d'après la Propriété 5.3.4, on en déduit que $A_1 \sqcup (A_2 \sqcup A_3) \sqsubseteq (A_1 \sqcup A_2) \sqcup A_3$, ce qui prouve le résultat. ∎

Enfin, les deux prochains résultats généralisent le Lemme 5.3.21 et le Théorème 5.3.15 au cas où on a un ensemble quelconque de A-termes unifiables deux à deux.

Théorème 5.3.23 *Pour tout ensemble $C = \{A_1, \ldots, A_n\}, n \geq 2$ de* A*-termes deux à deux unifiables, le* A*-terme A_1 est unifiable avec l'élément*

$$A_2 \sqcup (A_3 \sqcup \ldots \sqcup (A_{n-1} \sqcup A_n) \ldots).$$

PREUVE. On démontre le résultat par induction sur la cardinalité n de C. Si $n = 2$, le résultat est trivial, et si $n = 3$, on a le résultat d'après le Lemme 5.3.21, supposons maintenant que $n \geq 4$, et que le résultat est vrai pour tout ensemble de cardinalité $n-1$. Alors par hypothèse d'induction, A_1 et A_2 sont tous deux unifiables avec $A_3 \sqcup \ldots \sqcup (A_{n-1} \sqcup A_n)$, et comme A_1 et A_2 sont également unifiables, d'après le Lemme 5.3.21, on a le résultat. ∎

Corollaire 5.3.24 *Soient $A, A_1, \ldots, A_n$ des* A*-termes, et supposons que pour tout $i = 1, \ldots, n$, $A_i \sqsubseteq A$. Alors on a*

$$A_1 \sqcup (A_2 \sqcup \ldots \sqcup (A_{n-1} \sqcup A_n) \ldots) \ \sqsubseteq \ A.$$

PREUVE. On démontre le résultat par induction sur n. Pour $n = 1$, le résultat est trivial, supposons maintenant que le résultat soit vrai pour $n-1$, alors par hypothèse, il existe un homomorphisme h de $A_2 \sqcup (A_3 \sqcup \ldots \sqcup (A_{n-1} \sqcup A_n) \ldots)$ vers A, et un homomorphisme h_1 de A_1 vers A. D'après le Théorème 5.3.15, on a le résultat. ∎

5.4 Action de groupe sur des GA-termes

Dans ce qui suit, nous allons définir une action de groupe sur des ensembles de GA-termes. Nous commencerons par définir une action de groupe simple sur les graphes étiquetés, et nous étudierons sous quelles conditions cette opération demeure une action sur un ensemble de GA-termes. L'action de groupe définie sur les graphes étiquetés semble simple, mais les manipulations qu'elle permet d'effectuer ne sont pas triviales.

5.4.1 Définition de l'action de groupe

L'action de groupe que nous allons définir nous permettra de représenter les permutations des sommets arguments d'un GA-terme. Nous ne cherchons pas à permuter localement les arguments d'un ou plusieurs sommets d'un GA-terme, mais plutôt à appliquer une permutation globale de ses sommets, ce qui permettra aux arguments d'un sommet d'être remplacés par des arguments d'autres sommets.

Etant donnés un ensemble de sommets V et une fonction d'étiquetage s, nous allons commencer par définir une action de $\mathrm{Sym}(V)$ sur les graphes étiquetés construits sur V et s. Puis nous étudierons certaines restrictions qui, quand elles sont imposées, garantissent que cette action est également une action sur un ensemble de GA-termes.

Définition 5.4.1 Soient V un ensemble non vide, et s une fonction de V dans Σ. On note $\mathcal{GE}(V, s)$ l'ensemble des graphes étiquetés sur Σ de la forme (V, s, a). De façon similaire, on note GA-$\mathcal{T}(V, s)$ l'ensemble des GA-termes sur Σ de la forme (V, s, a) ; on a donc GA-$\mathcal{T}(V, s) =$ GA-$\mathcal{T}(\Sigma) \cap \mathcal{GE}(V, s)$.

Pour toute permutation σ d'éléments de V, et pour tout graphe étiqueté $G = (V, s, a)$ élément de $\mathcal{GE}(V, s)$, on pose $G^\sigma = (V, s, a^\sigma)$, où la fonction $a^\sigma : V \to V^\star$ est définie par : $a^\sigma(v) = [a(v)]^\sigma$. Comme les longueurs des listes $a(v)$ et $a^\sigma(v)$ sont identiques, G^σ est un graphe étiqueté sur Σ, et on a bien $G^\sigma \in \mathcal{GE}(V, s)$. ◇

Exemple 5.4.2 Soit T le A-terme de l'Exemple 5.1.16, reproduit en haut à gauche de la Figure 5.10. On a donc $\tau(T) = f(g(a), g(b))$.

Si on pose $\sigma = (\mathfrak{b}\ \mathfrak{e})$ et $\mu = (\mathfrak{c}\ \mathfrak{d})$, alors T^σ, T^μ et $T^{\sigma\mu}$ sont définis par :

v	$\mathfrak{a}$	$\mathfrak{b}$	$\mathfrak{c}$	$\mathfrak{d}$	$\mathfrak{e}$
$s(v)$	f	g	g	b	b
$a(v)$	$\mathfrak{b}.\mathfrak{c}$	$\mathfrak{d}$	$\mathfrak{e}$	ε	ε
$a^\sigma(v)$	$\mathfrak{e}.\mathfrak{c}$	$\mathfrak{d}$	$\mathfrak{b}$	ε	ε
$a^\mu(v)$	$\mathfrak{b}.\mathfrak{d}$	$\mathfrak{c}$	$\mathfrak{e}$	ε	ε
$a^{\sigma\mu}(v)$	$\mathfrak{e}.\mathfrak{d}$	$\mathfrak{c}$	$\mathfrak{b}$	ε	ε

La Figure 5.10 représente ces différents graphes étiquetés ; chaque graphe étiqueté est obtenu en permutant les pointes des flèches de T. Par exemple, la flèche partant de $\mathfrak{c}$ et qui pointe vers $\mathfrak{e}$ dans T pointe vers $\mathfrak{b}$ dans T^σ.

Lemme 5.4.3 *On a défini une action de* $\mathrm{Sym}(V)$ *sur* $\mathcal{GE}(V, s)$.

PREUVE. Soit $G = (V, s, a)$ un élément de $\mathcal{GE}(V, s)$, et σ, σ' deux éléments de $\mathrm{Sym}(V)$. Alors, pour tout $v \in V$, on a :

$$a^{\sigma\sigma'}(v) = [a(v)]^{\sigma\sigma'} = [a(v)^\sigma]^{\sigma'} = [a^\sigma(v)]^{\sigma'} = (a^\sigma)^{\sigma'}(v),$$

d'où $a^{\sigma\sigma'} = (a^\sigma)^{\sigma'}$, et donc, $G^{\sigma\sigma'} = (G^\sigma)^{\sigma'}$. ∎

Par contre, l'Exemple 5.4.2 montre qu'un GA-terme n'est pas nécessairement transformé en GA-terme. Les graphes étiquetés T, T^σ et T^μ sont tous trois des A-termes, qui représentent respectivement les termes $f(g(a), g(b))$, $f(\,b,\, g(g(a))\,)$ et $f(\,g(g(b)),\, a\,)$. En revanche, $T^{\sigma\mu}$ n'est pas un A-terme, ni même un GA-terme.

L'Exemple 5.4.2 prouve donc que l'ensemble GA-$\mathcal{T}(V, s)$ n'est pas stable sous l'action de $\mathrm{Sym}(V)$. Cependant, chercher à déterminer un sous-groupe de $\mathrm{Sym}(V)$ qui stabilise GA-$\mathcal{T}(V, s)$ n'a pas forcément de sens, puisque ce qui nous intéresse est de permuter des arguments dans un GA-terme particulier. Il est donc naturel de chercher à ne considérer que les permutations de $\mathrm{Sym}(V)$ qui transforment *un* GA-terme donné en GA-terme. Malheureusement, l'Exemple 5.4.2 montre que cet ensemble n'est pas un groupe (car σ et μ en font partie, mais pas leur produit $\sigma\mu$).

Dans ce qui suit, nous allons donc déterminer une information dont nous pourrons nous servir pour définir un sous-groupe de $\mathrm{Sym}(V)$ *et* un ensemble de GA-termes stable par ce sous-groupe.

5.4.2 Partitions stratifiées

Une première idée simple est de ne considérer que les éléments de $\mathrm{Sym}(V)$ qui permutent un ensemble de sommets indépendants dans un GA-terme donné T. Ceci revient donc à choisir un ensemble U de sommets indépendants dans T, et de considérer l'action de $\mathrm{Sym}(U)$ sur l'ensemble des GA-termes dans lesquels U est indépendant. Malheureusement, cette solution est trop restrictive, comme le montre l'exemple suivant.

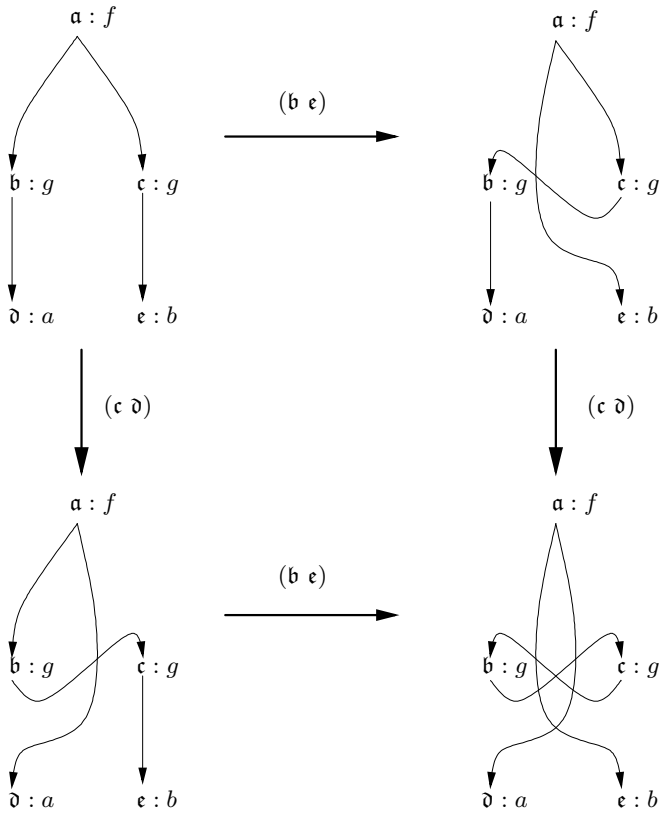

FIG. 5.10 – Graphes étiquetés de l'Exemple 5.4.2

Exemple 5.4.4 Soit E la théorie permutative définie par les axiomes suivants :

$$\begin{aligned} f(x,y) &\rightleftharpoons f(y,x), \\ g(x,y) &\rightleftharpoons g(y,x), \end{aligned}$$

et soit $t = f(a, g(b,d))$. Alors, pour tout GA-terme T, il n'est pas possible de représenter la classe d'équivalence de t modulo E comme une orbite sous l'action d'un $\mathrm{Sym}(U)$ où U serait un ensemble indépendant de sommets dans T. En effet, on a

$$f(a, g(b,d)) =_E f(g(b,d), a) =_E f(g(d,b), a),$$

et donc, si un tel T existait, l'ensemble U devrait contenir les sommets u_1 et u_2 respectivement étiquetés par a et g d'une part (première équation), et les sommets u_3 et u_4 respectivement étiquetés par b et d d'autre part (deuxième équation). Or, l'ensemble $\{u_2, u_3, u_4\}$ n'est pas indépendant dans T.

Une autre idée est de considérer une partition $\mathcal{P}$ de V, et d'étudier l'action de $\mathrm{Sym}_V(\mathcal{P})$ sur l'ensemble des GA-termes dans lesquels toutes les classes de $\mathcal{P}$ sont in-

dépendantes. L'Exemple 5.4.2 montre que cette restriction n'est pas suffisamment forte pour garantir que tout GA-terme soit transformé en GA-terme. En effet, dans cet exemple, toutes les classes de la partition $\mathcal{P} = \{\{\mathfrak{b}, \mathfrak{e}\}, \{\mathfrak{c}, \mathfrak{d}\}\}$ sont indépendantes dans le GA-terme T, et la permutation $\sigma\mu$ est bien élément de $\mathrm{Sym}_V(\mathcal{P})$. Pourtant, $T^{\sigma\mu}$ n'est pas un GA-terme.

Ainsi, la classe des groupes de la forme $\mathrm{Sym}(U)$ pour un ensemble U donné est trop restrictive pour permettre de définir l'action de groupe souhaitée, et la classe des groupes de la forme $\mathrm{Sym}_V(\mathcal{P})$ pour une partition $\mathcal{P}$ donnée ne l'est pas assez. Dans ce qui suit, nous allons restreindre cette seconde classe, et définir la notion de *partition stratifiée* dans un graphe étiqueté. Nous montrerons que l'ensemble des GA-termes dans lesquels une partition $\mathcal{P}$ est stratifiée est stable sous l'action de $\mathrm{Sym}_V(\mathcal{P})$.

Définition 5.4.5 (Partition stratifiée) Etant donné un graphe étiqueté G possédant une racine unique r, une partition $\mathcal{P}$ de V est dite *stratifiée* dans G si et seulement si pour tout sommet u de G dans une classe non triviale de $\mathcal{P}$:

- il existe un *unique* chemin de r à u,
- s'il existe un chemin non trivial de u à un sommet v, alors il existe un chemin non trivial de u à n'importe quel sommet dans la $\mathcal{P}$-classe de v. ◇

Exemple 5.4.6 Soit T le GA-terme de la Figure 5.11, et

$$\mathcal{P} = \{\{\mathfrak{a}\},\ \{\mathfrak{b}, \mathfrak{c}\},\ \{\mathfrak{d}, \mathfrak{e}\},\ \{\mathfrak{f}, \mathfrak{g}\}\}.$$

Sur la Figure 5.11, seules les classes non triviales de $\mathcal{P}$ sont entourées. Alors, $\mathcal{P}$ est une partition stratifiée dans T.

Exemple 5.4.7 Soient T et T' les GA-termes de la Figure 5.12, et $\mathcal{P}$ et $\mathcal{P}'$ les partitions définies par (voir la Figure 5.12) :

$$\begin{aligned} \mathcal{P} &= \{\{\mathfrak{a}\},\ \{\mathfrak{b}, \mathfrak{c}\},\ \{\mathfrak{d}, \mathfrak{e}\},\ \{\mathfrak{f}\}\}, \\ \mathcal{P}' &= \{\{\mathfrak{a}, \mathfrak{b}\},\ \{\mathfrak{c}\},\ \{\mathfrak{d}, \mathfrak{e}\},\ \{\mathfrak{f}\}\}. \end{aligned}$$

La partition $\mathcal{P}$ n'est pas stratifiée dans T pour deux raisons : il existe un chemin de $\mathfrak{c}$ à $\mathfrak{e}$ dans T, mais aucun de $\mathfrak{c}$ à $\mathfrak{d}$, et il y a deux chemins distincts de $\mathfrak{a}$ à $\mathfrak{d}$.

La partition $\mathcal{P}'$ n'est pas stratifiée dans T' car il existe un chemin non trivial de $\mathfrak{a}$ à $\mathfrak{b}$ dans T', mais aucun chemin non trivial de $\mathfrak{a}$ à $\mathfrak{a}$. En revanche, $\mathcal{P}$ est stratifiée dans T'.

Propriété 5.4.8 *Soit G un graphe étiqueté possédant une racine r, et soit $\mathcal{P}$ une partition stratifiée dans G. Alors il ne peut exister de chemin entre deux éléments distincts d'une même $\mathcal{P}$-classe.*

PREUVE. Ce résultat est évident : s'il existait un chemin entre deux éléments distincts u et v d'une même $\mathcal{P}$-classe dans G, ce chemin serait non trivial, et donc, par hypothèse de stratification, il existerait un chemin non trivial de u à u dans G. Ceci contredirait l'unicité du chemin de r à u dans G. ■

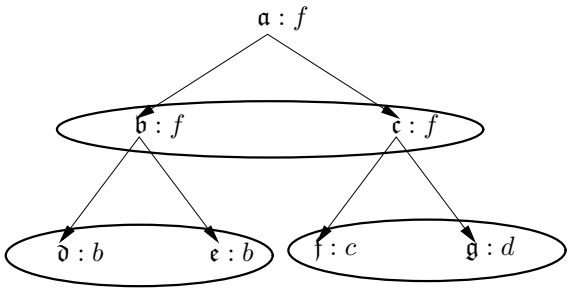

FIG. 5.11 – GA-terme de l'Exemple 5.4.6

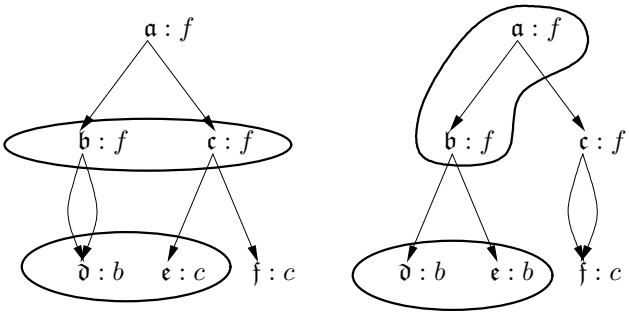

FIG. 5.12 – GA-termes de l'Exemple 5.4.7

Une conséquence immédiate de cette propriété est que :

Corollaire 5.4.9 *Si G est un graphe étiqueté de racine r et que $\mathcal{P}$ est une partition stratifiée dans G, alors la $\mathcal{P}$-classe de r est triviale.*

Remarque. Soit $\mathcal{P}$ une partition avec au moins une classe non triviale. $\mathcal{P}$ ne peut être stratifiée dans un graphe que si ce dernier ne contient qu'une racine, et il ne peut y avoir aucun cycle sur les chemins entre la racine du graphe et les sommets dans des classes non triviales. En effet, si ces conditions n'étaient pas respectées, la condition d'unicité des chemins entre la racine et les sommets des classes non triviales ne serait pas vérifiée. Ces deux propriétés sont évidemment vérifiées par tout GA-terme.

Le prochain théorème montre que si $\mathcal{P}$ est une partition stratifiée dans un GA-terme T, alors l'application des éléments de $\mathrm{Sym}_V(\mathcal{P})$ à T produit des GA-termes dans lesquels $\mathcal{P}$ est encore stratifiée. Ce résultat prouvera donc qu'on a une action de $\mathrm{Sym}_V(\mathcal{P})$ sur l'ensemble des GA-termes dans lesquels $\mathcal{P}$ est stratifiée.

Théorème 5.4.10 *Soient T un* GA*-terme (resp. un* A*-terme), et $\mathcal{P}$ une partition stratifiée dans T. Alors, pour toute permutation σ dans $\mathrm{Sym}_V(\mathcal{P})$, T^σ est un* GA*-terme (resp. un* A*-terme), et $\mathcal{P}$ est stratifiée dans T.*

PREUVE. Voir Annexe A, page 193. ∎

Par la suite, nous nous intéresserons particulièrement aux actions de groupes sur des GA-termes clos, ce qui donne lieu à la définition suivante.

Définition 5.4.11 Soit $\mathcal{P}$ une partition de V, alors on note GA-$\mathcal{T}_c(V, s, \mathcal{P})$ l'ensemble des GA-termes $T \in$ GA-$\mathcal{T}(V, s)$ tels que $\mathcal{P}$ est stratifiée dans T.

Comme l'action de groupe définie préserve l'étiquetage des sommets d'un GA-terme, on a le résultat suivant :

Théorème 5.4.12 *Pour toute partition stratifiée $\mathcal{P}$ de V, le groupe $\mathrm{Sym}_V(\mathcal{P})$ agit de façon semi-régulière sur* GA-$\mathcal{T}_c(V, s, \mathcal{P})$.

PREUVE. Le Théorème 5.4.10 prouve qu'on a une action de $\mathrm{Sym}_V(\mathcal{P})$ sur cet ensemble ; il reste à démontrer que cette action est semi-régulière.

Soient $T \in$ GA-$\mathcal{T}_c(V, s, \mathcal{P})$, $v \in V$, et supposons que $T^\sigma = T$. Alors soit v est la racine de T (et est dans ce cas également la racine de T^σ), et alors $v^\sigma = v$, soit il existe un sommet u tel que v est dans la liste $a(u)$, à une position i. Dans ce cas, on a

$$v \;=\; a(u)_i \;=\; a^\sigma(u)_i \;=\; [a(u)_i]^\sigma \;=\; v^\sigma.$$

Donc, $\sigma = \mathrm{id}$, et l'action est bien semi-régulière. ∎

Ainsi, la propriété de stratification d'une partition dans un GA-terme est une condition suffisante de préservation de la structure de ce GA-terme. C'est néanmoins loin d'être une condition nécessaire. Par exemple, supposons que $\mathcal{P}$ est une partition avec une unique classe U non triviale. Si on considère l'ensemble des GA-termes dans lesquels l'ensemble U est indépendant, il est clair que cet ensemble est stable sous l'action de $\mathrm{Sym}_V(\mathcal{P})$. Pourtant, la condition d'unicité des chemins entre la racine et les éléments de U n'est pas vérifiée par tous les GA-termes de cet ensemble, et donc, GA-$\mathcal{T}_c(V, s, \mathcal{P})$ est strictement inclus dans cet ensemble.

Il est en fait possible de généraliser la définition d'une partition stratifiée en acceptant même les partitions $\mathcal{P}$ qui ne vérifient pas la condition d'unicité des chemins ; toutes les permutations de $\mathrm{Sym}_V(\mathcal{P})$ transformeraient encore un GA-terme en GA-terme. Nous avons préféré garder cette condition dans la définition parce que les partitions que nous étudierons par la suite la vérifieront toutes, et que son absence rend certaines preuves plus ardues.

Mais même sans cette condition d'unicité des chemins, la stratification n'est pas une condition nécessaire de préservation de la structure de GA-terme : si dans l'Exemple 5.4.2 on prend la partition $\mathcal{P} = \{\{\mathfrak{a}\}, \{\mathfrak{b}, \mathfrak{c}\}, \{\mathfrak{d}, \mathfrak{e}\}\}$, cette dernière n'est pas stratifiée dans T, et pourtant tous les éléments de $\mathrm{Sym}_V(\mathcal{P})$ transforment T en un GA-terme.

5.5 Résumé

Dans ce chapitre, nous avons défini les GA-termes à partir des graphes étiquetés tels qu'ils sont définis dans la réécriture de graphes de termes. L'essentiel de ce chapitre a consisté à définir plusieurs notions sur ces GA-termes, dont la plus importante, celle d'homomorphisme d'un GA-terme vers un autre. Nous avons également prouvé plusieurs propriétés vérifiées par ces GA-termes, et par la sous-classe des A-termes. Toutes ces propriétés nous serviront ultérieurement à démontrer plusieurs théorèmes sur les GA-termes stratifiés.

Puis, nous avons défini une action de groupe simple, basée sur le groupe des permutations des sommets d'un graphe étiqueté, mais cette action ne transformait pas tous les GA-termes en GA-termes. Nous avons donc cherché à imposer des restrictions aux permutations considérées afin de garantir que les structures de GA-termes était préservée, tout en restant le plus général possible. Ceci nous a mené à la définition des *partitions stratifiées* dans un GA-terme, et nous avons démontré que pour toute partition $\mathcal{P}$, on a une action de $\mathrm{Sym}_V(\mathcal{P})$ sur l'ensemble des GA-termes dans lesquels $\mathcal{P}$ est stratifiée.

Chapitre 6

GA-termes stratifiés

Dans le chapitre précédent, nous avons défini une action sur des GA-termes basée sur les permutations de leurs sommets. Nous avons défini cette action de façon très abstraite, ne nous focalisant que sur la préservation des structures de ces GA-termes.

Dans ce chapitre, nous allons nous intéresser au lien entre cette action de groupe et la réécriture stratifiée de [AP01]. Pour cela, nous commencerons par montrer comment représenter une équation permutative $t \rightleftharpoons t'$ par un A-terme et une permutation de ses sommets. Ensuite, nous définirons les *signatures stratifiées* Σ_E, ainsi que les GA-*termes stratifiés*, qui sont des GA-termes particuliers sur $\Sigma \cup \Sigma_E$. Etant donné un GA-terme stratifié T, nous montrerons comment construire une partition stratifiée sur T à partir des sommets étiquetés par des éléments de Σ_E ; cette partition nous servira à définir une action de groupe sur les GA-termes stratifiés. Enfin, nous construirons un groupe dont chaque élément correspond à l'application (simultanée) de règles de la réécriture stratifiée définie dans [AP01]. Ce résultat nous permettra de démontrer que les ensembles stratifiés de [AP01] peuvent être obtenus à partir des orbites de ce groupe.

Enfin, nous terminerons ce chapitre en étudiant les propriétés vérifiées par des GA-termes stratifiés liés par un homomorphisme. Ces propriétés nous permettront par la suite de prouver des résultats sur les GA-termes stratifiés en les démontrant uniquement pour les A-termes stratifiés. Nous donnerons un premier exemple d'application de ces propriétés en démontrant que la relation de bisimilarité équipartitionne les ensembles stratifiés.

6.1 Motivations

Nous commençons par illustrer pour quelle raison les termes stratifiés ont été introduits dans [AP01].

Prenons une théorie équationnelle E définie par l'axiome de commutativité $f(x, y) \rightleftharpoons f(y, x)$. Soit $T = (V, s, a)$ le A-terme de la Figure 6.1, qui représente le terme $t = f(f(a, b), f(c, d))$. Il est aisé de vérifier que la classe de congruence de t modulo E comporte 8 éléments (t compris).

Prenons maintenant la partition $\mathcal{P} = \{\{\mathfrak{a}\}, \{\mathfrak{b}, \mathfrak{c}\}, \{\mathfrak{d}, \mathfrak{e}\}, \{\mathfrak{f}, \mathfrak{g}\}\}$ des sommets de T.

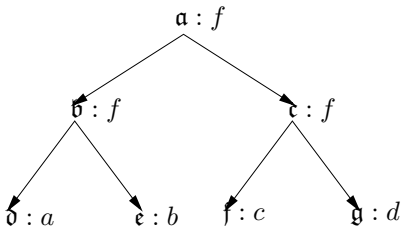

FIG. 6.1 – A-terme représentant $f(f(a,b),f(c,d))$

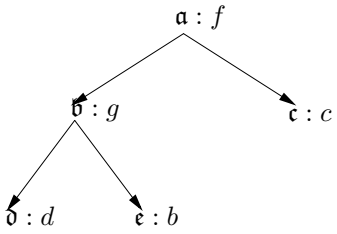

FIG. 6.2 – A-terme représentant $f(g(d,b),c)$

Cette partition a été obtenue en regroupant dans une même partie les deux sommets arguments de chaque symbole étiqueté par f. La partition $\mathcal{P}$ est stratifiée dans T, et donc, l'action du groupe $G = \mathrm{Sym}_V(\mathcal{P})$ sur T est bien définie. Ce groupe comporte 8 éléments, et l'image de T par chacune des permutations représente un terme distinct égal à t modulo E. Par exemple, si $\sigma = (\mathfrak{b}\ \mathfrak{c})(\mathfrak{f}\ \mathfrak{g})$, alors $\tau(A^\sigma) = f(f(d,c),f(a,b)) =_E t$. Donc, dans ce cas particulier, l'image par la fonction τ de l'orbite $T^{\mathcal{G}}$ est égale à la classe de congruence de t modulo E. Donc, la donnée de T et de G détermine entièrement cette classe d'équivalence.

Malheureusement, dans le cas général, les choses ne sont pas aussi simples. Considérons maintenant la théorie permutative E définie par les axiomes suivants :

$$\begin{aligned} g(x,y) &\rightleftharpoons g(y,x), \\ f(g(d,x),y) &\rightleftharpoons f(g(d,y),x). \end{aligned}$$

Soit $T = (V,s,a)$ le A-terme de la Figure 6.2, qui représente donc le terme $t = f(g(d,b),c)$. La classe de congruence de t modulo E comporte 4 éléments : t lui-même, et :

$$t_1 = f(g(b,d),c),\ t_2 = f(g(d,c),b),\ \text{et}\ t_3 = f(g(c,d),b).$$

Soit $\mathcal{P}$ la partition de V dont la seule classe non triviale est $\{\mathfrak{c},\mathfrak{d},\mathfrak{e}\}$. Cette partition est stratifiée dans T, et donc, une fois de plus, l'action du groupe $G = \mathrm{Sym}_V(\mathcal{P})$ sur T

est bien définie. On pose :

$$T_1 = T^{(\mathfrak{d}\ \mathfrak{e})},\ T_2 = T^{(\mathfrak{c}\ \mathfrak{e})},\ \text{et}\ T_3 = T^{(\mathfrak{c}\ \mathfrak{e}\ \mathfrak{d})}.$$

On a donc, pour tout $i = 1, \ldots, 3$, $\tau(T_i) = t_i$. La classe de congruence de T modulo E peut donc être représentée par l'ensemble de permutations $\{\mathrm{id}, (\mathfrak{d}\ \mathfrak{e}), (\mathfrak{c}\ \mathfrak{e}), (\mathfrak{c}\ \mathfrak{e}\ \mathfrak{d})\}$, qui *n'est pas* un groupe (par exemple $(\mathfrak{c}\ \mathfrak{e}\ \mathfrak{d})^{-1} = (\mathfrak{c}\ \mathfrak{d}\ \mathfrak{e})$ ne fait pas partie de cet ensemble).

La raison pour laquelle on n'a plus de structure de groupe est que les *contextes* dans lesquels les deux axiomes de E peuvent être appliqués se superposent mais sont distincts. Par exemple, nous pouvons appliquer le premier et le deuxième axiome à t, ce qui permet d'obtenir les termes t_1 et t_2. Cependant, il n'est possible d'appliquer que le premier axiome à t_1. Il n'est donc pas toujours possible d'appliquer les mêmes axiomes à deux termes égaux modulo E ; la classe de congruence d'un terme ne peut pas en général être représentée par un GA-terme et un groupe.

Ceci explique la restriction du raisonnement équationnel dans [AP01]. Intuitivement, cette restriction consiste à interdire que deux équations permutatives dont les contextes sont distincts mais se superposent puissent toutes deux être appliquées à la même position dans t. Ainsi, dans l'exemple précédent, on peut décider de ne jamais appliquer le deuxième axiome à la racine de t ; l'ensemble des termes qui sont égaux à t modulo E sans appliquer ce deuxième axiome est alors $\{t, t_1\}$, qui est un sous-ensemble de la classe de congruence de t modulo E, et qui peut également être représenté par l'orbite du GA-terme T par le groupe $\mathrm{Sym}(\{\mathfrak{d}, \mathfrak{e}\})$.

Ce procédé de restriction du raisonnement équationnel s'appelle la *stratification des termes*. Un terme t est stratifié en sélectionnant certaines de ses positions et un nombre restreint d'équations permutatives qui peuvent y être appliquées. Sous certaines conditions, l'ensemble des termes obtenus à partir de t et de ces équations pourra être représenté comme une orbite sous l'action d'un groupe.

Dans ce qui suit, nous allons définir la stratification de GA-termes. Comme dans [AP01], nous commencerons par définir les signatures stratifiées, qui seront ensuite employées pour étiqueter certains sommets des GA-termes stratifiés. Puis, nous démontrerons que les *ensembles stratifiés* de [AP01] peuvent être obtenus comme des orbites sous l'action d'un groupe.

6.2 Signatures stratifiées

Dans cette partie, nous allons définir les *signatures stratifiées*. Intuitivement, étant donnée une théorie permutative E, chaque élément d'une signature stratifiée Σ_E représente un ensemble d'équations permutatives basées sur un même contexte. Ces éléments seront donc employés dans un GA-terme stratifié pour décrire quelles équations peuvent être appliquées, et où elles peuvent être appliquées. Nous commencerons par montrer comment une équation permutative peut être représentée par un A-terme et une permutation de ses sommets ; nous utiliserons ensuite cette représentation pour définir les signatures stratifiées.

Une équation entre deux termes linéaires t et t' de $\mathcal{T}(\Sigma, \mathcal{V})$ est permutative si et seulement si t et t' sont variants l'un de l'autre, ce qui signifie que chaque terme est une instance de l'autre. Cette propriété est simple à exprimer sur des A-termes associés à t et t'. Nous commençons donc par définir de quelle façon associer un A-terme à un terme $t \in \mathcal{T}(\Sigma, \mathcal{V})$.

Naturellement, nous pourrions utiliser n'importe quel ensemble de sommets pour construire un A-terme associé à t, il suffit que la cardinalité de cet ensemble soit égal à la longueur de t. Un candidat naturel est l'ensemble des positions de t ; de plus, cet ensemble permet de définir simplement le A-terme qui représentera t.

Définition 6.2.1 (arbre(t)) Etant donné un élément $t \in \mathcal{T}(\Sigma, \mathcal{V})$, on note $\text{arbre}(t) = (\text{Pos}(t), s, a)$, où les fonctions $s : \text{Pos}(t) \to \Sigma^\circ$ et $a : \text{Pos}(t) \to \text{Pos}(t)^\star$ sont définies pour $p \in \text{Pos}(t)$ par :

- Si $t|p$ est une constante, alors $s(p) = t|p$, et $a(p) = \varepsilon$.
- Si $t|p$ est une variable, alors $s(p) = \circ$ et $a(p) = \varepsilon$.
- Si $t|p = f(t_1, \ldots, t_n)$, alors $s(p) = f$, et $a(p) = [p.1].\cdots.[p.n]$.

Il est clair que $\text{arbre}(t)$ est un A-terme sur Σ, qui est clos si et seulement si t est clos. Ce A-terme est appelé le *contexte associé* à t. ◇

Remarque. Dans la définition de $\text{arbre}(t)$, pour toute position p, $a(p)$ n'est pas une liste d'entiers mais une liste de listes d'entiers.

Exemple 6.2.2 Soit $t = f(g(b, y), z)$, où b est une constante, et y et z sont des variables. Alors l'ensemble des positions de t est $\text{Pos}(t) = \{\varepsilon, 1, 2, 1.1, 1.2\}$. $\text{arbre}(t)$ est donc défini par (voir la Figure 6.3) :

v	ε	1	1.1	1.2	2
$s(v)$	f	g	b	$\circ$	$\circ$
$a(v)$	[1].[2]	[1.1].[1.2]	ε	ε	ε

Notons que si $a(v) = \varepsilon$, pour un sommet v de $\text{Pos}(t)$ (comme le sommet 2, par exemple), cela signifie que v n'a pas d'arguments (ε est la liste vide), et non pas qu'il y a une flèche de v à la racine du A-terme.

Grâce à cette définition, nous pouvons reformuler la définition d'une équation permutative, en nous basant sur ces A-termes :

Définition 6.2.3 (Equation permutative) Pour toute paire $t, t' \in \mathcal{T}(\Sigma, \mathcal{V})$ de termes linéaires (non-réduits à des variables), l'équation $t \rightleftharpoons t'$ est *permutative* si et seulement si :

1. $\text{arbre}(t) = \text{arbre}(t')$,
2. $\text{Var}(t) = \text{Var}(t')$.

On dira alors que $\text{arbre}(t)$ est le *contexte associé* à cette équation permutative, ou que l'équation permutative est *basée* sur ce contexte.

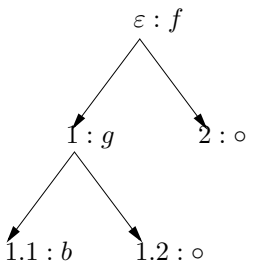

FIG. 6.3 – A-terme de l'Exemple 6.2.2

Notons que l'ensemble des sommets variables de arbre(t) est exactement l'ensemble des positions des variables dans t.

La *permutation associée* à l'équation permutative $t \rightleftharpoons t'$ est la permutation $\sigma \in \mathcal{SV}(\text{arbre}(t))$ définie de la façon suivante : pour toute variable $x \in \text{Var}(t)$, si p est la position de x dans t, et p' est la position de x dans t', alors $p^\sigma = p'$.

Une théorie E dont tous les axiomes sont des équations permutatives est une *théorie permutative*. Les contextes associés aux axiomes définissant E sont alors appelés des *contextes axiomatiques de* E. On dit que l'ensemble de ces axiomes est *uniforme* si et seulement si tous ces axiomes sont basés sur le même contexte axiomatique. ◇

Exemple 6.2.4 Soit $t = f(g(x, y), z)$, et $t' = f(g(x, z), y)$. Comme arbre(t) = arbre(t'), on en déduit que l'équation $t \rightleftharpoons t'$ est une équation permutative. Le contexte c associé à cette équation vérifie $\tau(c) = f(g(\circ, \circ), \circ)$, et la permutation associée à cette équation est $\sigma = (1.2\ 2)$.

Lemme 6.2.5 *Soit E une théorie permutative contenant deux équations permutatives e_1 et e_2 basées sur le même contexte c, et soient σ et σ' les permutations associées respectivement à e_1 et e_2. Soit t un terme tel que $c =$ arbre(t), et soit t' le terme obtenu à partir de t, après avoir successivement appliqué les équations e_1 et e_2 à la racine de t. Alors l'équation $t \rightleftharpoons t'$ est une équation permutative de contexte associé c et de permutation associée $\sigma\sigma'$, qui est donc élément de E.*

PREUVE. On pose $t = t[x_1, \ldots, x_n]$, alors il existe des permutations $\pi, \mu \in \text{Sym}(n)$ telles que e_1 et e_2 sont respectivement de la forme

$$c[x_1, \ldots, x_n] \rightleftharpoons c[x_{1^\pi}, \ldots, x_{n^\pi}], \text{ et } c[y_1, \ldots, y_n] \rightleftharpoons c[y_{1^\mu}, \ldots, y_{n^\mu}].$$

Après application de l'équation e_2 au terme $c[x_{1^\pi}, \ldots, x_{n^\pi}]$, on obtient le terme $c[x_{1^{\mu\pi}}, \ldots, x_{n^{\mu\pi}}] = t'$, et l'équation $c[x_1, \ldots, x_n] \rightleftharpoons c[x_{1^{\mu\pi}}, \ldots, x_{n^{\mu\pi}}]$ est bien une équation permutative de contexte associé c. De plus, par définition, si $x \in \{x_1, \ldots, x_n\}$, et p est la position de x dans $c[x_1, \ldots, x_n]$, alors p^σ est la position de x dans $c[x_{1^\pi}, \ldots, x_{n^\pi}]$, et $p^{\sigma\sigma'}$ est la position de x dans $c[x_{1^{\mu\pi}}, \ldots, x_{n^{\mu\pi}}]$. Donc, $\sigma\sigma'$ est la permutation associée à cette équation permutative, et on a le résultat. ■

Théorème 6.2.6 (Théorème 1.4 de [AP01]) *Soit E une théorie permutative définie par un ensemble d'axiomes uniforme, et soient $\sigma_1, \ldots, \sigma_n$ les permutations associées aux axiomes définissant E. Si c est le contexte associé à ces axiomes, alors pour toute permutation $\sigma \in \mathrm{Sym}(\mathcal{SV}(c))$, l'équation permutative basée sur c et de permutation associée σ est élément de E si et seulement si σ est élément du groupe engendré par l'ensemble $\{\sigma_1, \ldots, \sigma_n\}$.*

PREUVE. Pour $i \in \{1, \ldots, n\}$, on note e_i l'axiome de E de permutation associée σ_i, et on note G le groupe engendré par l'ensemble $\{\sigma_1, \ldots, \sigma_n\}$. Soit t un terme tel que $c = \mathrm{arbre}(t)$, et supposons que $\sigma \in G$. Alors on a

$$\sigma = \prod_{j=1}^{m} \sigma_{i_j}, \text{ où } \forall j = 1, \ldots, m,\ i_j \in \{1, \ldots, n\}.$$

Montrons par induction sur m que si t' est obtenu à partir de t après application de la séquence d'axiomes $e_{i_1}, \ldots, e_{i_m}$, alors l'équation $t \rightleftharpoons t'$ est une équation permutative de contexte associé c et de permutation associée σ. Si $m = 1$, alors $\sigma = \sigma_{i_1}$, et le résultat est trivial. Supposons maintenant que $m > 1$, et que le résultat est vrai pour tout $m' < m$. Soit t'' le terme obtenu après application de la séquence d'axiomes $e_{i_1}, \ldots, e_{i_{m-1}}$, alors par hypothèse d'induction, l'équation $t \rightleftharpoons t''$ est une équation permutative de contexte associé c, et de permutation associée $\sigma' = \prod_{j=1}^{m-1} \sigma_{i_j}$. Notons e' cette équation permutative, alors, d'après le Lemme 6.2.5, si t' est le terme obtenu à partir de t après avoir successivement appliqué les équations permutatives e' et e_{i_m}, alors l'équation $t \rightleftharpoons t'$ est une équation permutative de contexte c et de permutation associée $\sigma'\sigma_{i_m} = \sigma$, qui est élément de E.

Réciproquement, soient t et t' deux termes tels que l'équation $t \rightleftharpoons t'$ est une équation permutative de contexte associé c, et de permutation associée σ, qui est élément de E. Alors, nécessairement, il existe une séquence d'axiomes $e_{i_1}, \ldots, e_{i_m}$ qui, appliquée à t, produit le terme t'. D'après le Lemme 6.2.5, il est clair que la permutation associée à l'équation $t \rightleftharpoons t'$ est $\sigma = \prod_{j=1}^{m} \sigma_{i_j}$, et cette permutation est bien élément de G. ∎

Exemple 6.2.7 Soit E la théorie définie par les deux axiomes suivants :

$$\begin{aligned} f(g(x,y),z) &\rightleftharpoons f(g(x,z),y) \\ f(g(x,y),z) &\rightleftharpoons f(g(y,z),x). \end{aligned}$$

Ces deux axiomes sont des équations permutatives basées sur le même contexte c tel que $\tau(c) = f(g(\circ,\circ),\circ)$, et les permutations qui leur sont associés sont respectivement $\sigma = (1.2\ 2)$ et $\mu = (1.1\ 2\ 1.2)$. On en déduit que cet ensemble d'axiomes est uniforme, et que pour toute permutation σ' élément du groupe engendré par $\{\sigma, \mu\}$ (ici, le groupe $\mathrm{Sym}(\{1.1, 1.2, 2\})$), l'équation permutative basée sur le contexte c et de permutation associée σ' est élément de E.

Nous pouvons maintenant définir formellement les signatures stratifiées :

Définition 6.2.8 (Signature stratifiée) Etant donnée une théorie permutative E définie par un ensemble d'axiomes sur Σ, une *signature stratifiée* Σ_E sur E est un ensemble de symboles de la forme $\langle f, c, G\rangle$, où f est un symbole de fonction de Σ, c est un A-terme sur Σ, et G est un groupe de permutations sur les sommets variables de c, tel que :

- f est le symbole de tête[1] de c, c'est-à-dire que $s_c(\text{racine}(c)) = f$,
- l'arité de $\langle f, c, G\rangle$ est égale à l'arité de f,
- pour tout σ de G, l'équation permutative de contexte associé c et de permutation associée σ appartient à E.

Tout comme dans [AP01], nous pourrons *démarquer* un symbole stratifié, ce qui revient intuitivement à retirer l'information présente dans c et G. La fonction de démarquage $\text{dm} : \Sigma_E \to \Sigma$ est définie par : $\text{dm}(\langle f, c, G\rangle) = f$.

Nous étendrons cette fonction de démarquage aux GA-termes en définissant $\text{dm} : \text{GA-}\mathcal{T}(\Sigma \cup \Sigma_E) \to \text{GA-}\mathcal{T}(\Sigma)$ par :

$$\text{pour tout GA-terme } T = (V, s, a),\ \text{dm}(T) = (V, \text{dm} \circ s, a).$$

Cette opération revient donc à remplacer tout symbole $\langle f, c, G\rangle$ qui étiquette un sommet de T par le symbole f.

Pour des raisons de clarté, on définit également le *démarquage à la racine* de T par : $\text{dm}_\text{r}(T) = (V, s', a)$, où $s'(v)$ est égal à $s(v)$ pour tous les sommets sauf la racine de T, et $s'(\text{racine}(T)) = \text{dm} \circ s(\text{racine}(T))$. C'est donc une fonction de $\text{GA-}\mathcal{T}(\Sigma \cup \Sigma_E)$ vers lui-même. ◇

Exemple 6.2.9 Reprenons l'Exemple 6.2.7, et supposons que E est définie par les deux axiomes qui y sont mentionnées, et que la signature stratifiée Σ_E considérée est $\Sigma_E = \{\langle f, c, \mathcal{G}\rangle\}$, où $c = \text{arbre}(t)$, et $G = \text{Sym}(\{1.1, 1.2, 2\})$. Alors on a $\text{dm}(\langle f, c, G\rangle) = f$.

Soit A le A-terme de gauche dans la Figure 6.4, A représente donc un $\Sigma \cup \Sigma_E$-terme, et $\text{dm}(A)$ est le GA-terme de droite de la même figure, et représente bien un Σ-terme.

Remarque. Cette définition d'une signature stratifiée est plus générale que celle de [AP01], où les contextes qui apparaissent dans les éléments de la signature stratifiée doivent être associés à des axiomes de la théorie permutative. Ici, nous n'imposons aucune contrainte sur ces contextes.

Propriété 6.2.10 *Soient T et T' deux* GA*-termes sur $\Sigma \cup \Sigma_E$, si $T \mathrel{\mathring{=}} T'$, alors* $\text{dm}(T) \mathrel{\mathring{=}} \text{dm}(T')$.

6.3 Stratification d'un GA-terme

Etant données une signature Σ et une signature stratifiée Σ_E, nous allons maintenant considérer une classe particulière de GA-termes sur $\Sigma \cup \Sigma_E$: les GA*-termes stratifiés*. Ces

[1] Il n'est pas indispensable de dupliquer f dans ce nouveau symbole, qui aurait pu être simplement $\langle c, G\rangle$. Nous avons choisi de mentionner f explicitement pour des raisons de lisibilité.

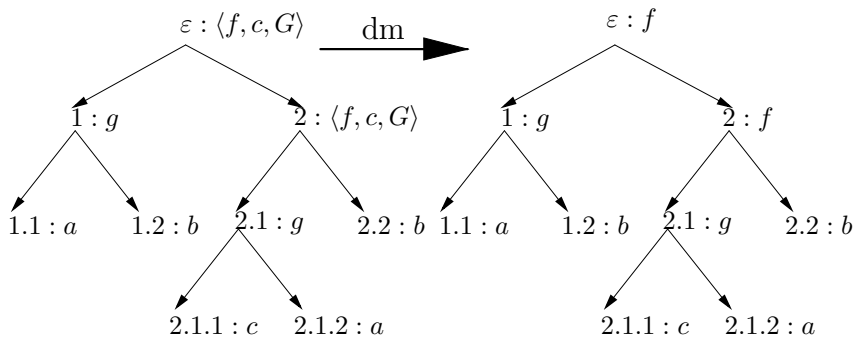

FIG. 6.4 – A et $\mathrm{dm}(A)$

derniers sont obtenus en imposant certaines conditions aux sommets étiquetés par des symboles de Σ_E. Sous ces conditions, cet étiquetage induira une partition stratifiée sur le GA-terme considéré, et l'action de groupe définie dans le chapitre précédent nous permettra de représenter les ensembles stratifiés de [AP01] comme des orbites sous l'action d'un groupe donné.

Définition 6.3.1 (GA-terme stratifié) Etant donnée une signature Σ et une signature stratifiée Σ_E, un GA-*terme stratifié* sur Σ, Σ_E est un GA-terme clos $T = (V, s, a)$ sur $\Sigma \cup \Sigma_E$ tel que :

1. pour tout sommet $v \in V$ dont le symbole $s(v)$ est élément de Σ_E, si $s(v) = \langle f, c, G\rangle$, alors il existe un homomorphisme $\mathrm{h}_{[T,v]}$ du A-terme c vers $\mathrm{dm_r}(T|v)$. Le résidu de $\mathrm{h}_{[T,v]}$ est noté $\mathrm{R}_T(v)$, et l'antirésidu $\overline{\mathrm{R}}_T(v)$;
2. $\forall u, v \in V$, si v est étiqueté par un symbole de Σ_E, et u est élément de $\overline{\mathrm{R}}_T(v) \cup \mathrm{R}_T(v)$, alors il existe un unique chemin de la racine de T à u.

Fixons l'ensemble de sommets V, et la fonction $s : V \to \Sigma \cup \Sigma_E$. L'ensemble des GA-termes stratifiés de la forme (V, s, a) est noté GA-$\mathcal{S}(V, s)$. L'ensemble des sommets v de V tels que $s(v) \in \Sigma_E$ est noté V_{s}. ◇

Exemple 6.3.2 Reprenons la signature stratifiée de l'Exemple 6.2.9, et posons $F = \langle f, c, G\rangle$. Alors $A =$ arbre($f(b,\ F(g(b,d),\ b))$) (voir Figure 6.5) est un A-terme stratifié, puisque la fonction $\mathrm{h}_{[A,2]}$ définie par :

v	ε	1	2	1.1	1.2
$\mathrm{h}_{[A,2]}(v)$	2	2.1	2.2	2.1.1	2.1.2

est un homomorphisme de c vers $\mathrm{dm_r}(A|2)$. Le résidu de $\mathrm{h}_{[A,2]}$ est l'ensemble $\mathrm{R}_A(2) = \{2.1.1,\ 2.1.2,\ 2.2\}$, et son antirésidu est $\overline{\mathrm{R}}_A(2) = \{2,\ 2.1\}$.

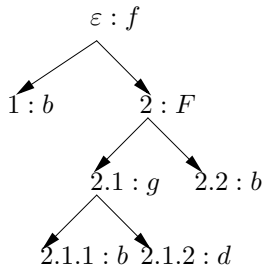

FIG. 6.5 – A-terme de l'Exemple 6.3.2

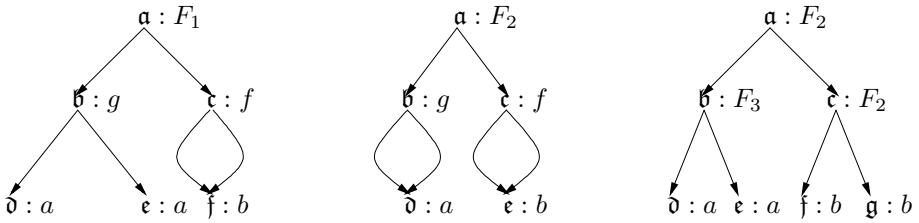

FIG. 6.6 – GA-termes stratifiés bien formés

Exemple 6.3.3 Supposons que $\Sigma' = \{F_1, F_2, F_3\}$, où pour $i = 1, 2$, $F_i = \langle f, c_i, G_i \rangle$, $F_3 = \langle g, c_3, G_3 \rangle$,

$$\tau(c_1) = f(g(\circ, \circ), \circ),\ \tau(c_2) = f(\circ, \circ),\ \text{et}\ \tau(c_3) = g(\circ, \circ),$$

et pour $i = 1, 2, 3$, G_i est un sous-groupe de $\mathrm{Sym}(\mathcal{SV}(c_i))$. Alors les trois GA-termes de la Figure 6.6 sont des GA-termes stratifiés, qui, une fois démarqués, représentent tous trois le terme $f(g(a, a), f(b, b))$.

Les deux GA-termes de la Figure 6.7, eux, ne sont pas stratifiés : le premier ne vérifie pas l'hypothèse d'unicité des chemins, et le symbole F_3 qui étiquette le sommet $\mathfrak{b}'$ dans le second fait qu'il n'existe aucun homomorphisme approprié de c_1 vers la racine $\mathfrak{a}'$.

Remarque. On voit pourquoi il est nécessaire de démarquer le symbole de tête de $T|v$ dans cette définition, puisque ce dernier est de la forme $\langle f, c, G \rangle \in \Sigma_E$, tandis que le symbole de tête de c est f ; dans le cas contraire, il ne pourrait y avoir aucun homomorphisme de c vers $T|v$. De plus, le fait que les autres symboles de $T|v$ ne soient pas démarqués signifie que tous les sommets dans l'antirésidu $\overline{\mathrm{R}}_T(v)$ autres que v sont nécessairement étiquetés par des symboles de Σ.

Remarque. Comme un GA-terme stratifié est nécessairement clos, tout homomorphisme d'un GA-terme stratifié vers un autre est également clos.

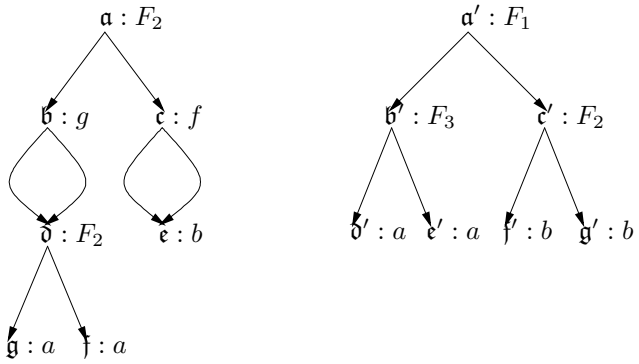

FIG. 6.7 – GA-termes stratifiés mal formés

On a immédiatement les propriétés suivantes, évidentes d'après la condition d'unicité des chemins :

Propriété 6.3.4 *Soit $T = (V, s, a)$ un GA-terme stratifié, et v un élément de V tel que $s(v) = \langle f, c, G\rangle$. Alors :*

1. *Soit V_c l'ensemble des sommets de c, alors la fonction $\mathrm{h}_{[T,v]}$ est une bijection de V_c dans $\overline{\mathrm{R}}_T(v) \cup \mathrm{R}_T(v)$.*
2. *Soit $T' = (V', s', a')$ un GA-terme stratifié, et supposons qu'il existe un homomorphisme h de T vers T'. Alors la restriction de h à V_s est une bijection entre V_s et V'_s.*

Définition 6.3.5 (Hauteur stratifiée) Soit $T = (V, s, a)$ un GA-terme stratifié de racine r. La *hauteur stratifiée* $\lfloor T \rfloor$ de T est définie inductivement de la façon suivante :

- si $s(r)$ est une constante, alors $\lfloor T \rfloor = 1$,
- si $s(r)$ est un symbole de fonction de Σ, alors

$$\lfloor T \rfloor \;=\; 1 \;+\; \max\{\lfloor T|a(r)_i \rfloor \mid 1 \leq i \leq \text{arité}(f)\},$$

- si $s(r)$ est un symbole de Σ_E, alors

$$\lfloor T \rfloor \;=\; 1 \;+\; \max\{\lfloor T|v \rfloor \mid v \in \mathrm{R}_T(r)\}.$$

Enfin, pour tout sommet v de T, la *hauteur stratifiée* de v est $\lfloor v \rfloor_T = \lfloor T|v \rfloor$. ◇

Exemple 6.3.6 Reprenons le A-terme stratifié de l'Exemple 6.3.2. Ce A-terme est de hauteur 4, et de hauteur stratifiée 3.

Dans ce qui suit, nous allons étudier les propriétés des résidus $\mathrm{R}_T(v)$ pour un GA-terme T donné, et nous verrons que ces résidus permettent de définir une partition stratifiée dans T. Puis nous prouverons que cette partition est telle que les images de T sous l'action du groupe qu'elle induit sont également des GA-termes stratifiés. Ainsi, cette action sera également une action de groupe sur un ensemble de GA-termes stratifiés. Enfin, nous démontrerons que les orbites des GA-termes sous l'action de ce groupe correspondent aux *ensembles stratifiés* de [AP01].

6.4 Propriétés structurelles des résidus $\mathrm{R}_T(v)$

Pour un GA-terme $T = (V, s, a)$ donné, nous allons analyser la structure des résidus $\mathrm{R}_T(v)$. Nous commencerons par montrer que l'ensemble $\mathcal{R}_T$ de ces résidus, complété par des singletons, est une partition stratifiée dans T. Nous pourrons donc appliquer l'action de groupe définie dans le chapitre précédent à T, et nous montrerons que toute image de T par l'action de $\mathrm{Sym}_V(\mathcal{R}_T)$ est également un GA-terme stratifié : on aura donc une action de groupe sur un sous-ensemble de GA-$\mathcal{S}(V, s)$.

Lemme 6.4.1 *Pour tout* GA*-terme stratifié T élément de* GA-$\mathcal{S}(V, s)$ *et pour toute paire de sommets distincts u, v de V_s, on a :*

1. *si u est en-dessous de v, alors u est en-dessous d'exactement un sommet de $\mathrm{R}_T(v)$,*
2. *les résidus $\mathrm{R}_T(u)$ et $\mathrm{R}_T(v)$ sont disjoints,*
3. *les antirésidus $\overline{\mathrm{R}}_T(u)$ et $\overline{\mathrm{R}}_T(v)$ sont disjoints.*

PREUVE. 1. Puisque $s(u) \in \Sigma_E$, u ne peut pas être élément de $\overline{\mathrm{R}}_T(v)$. Soit v' le premier sommet dans le chemin de v à u qui n'est pas dans $\overline{\mathrm{R}}_T(v)$. Alors v' est nécessairement élément du résidu $\mathrm{R}_T(v)$, et $u \leq_T v'$. Les éléments de $\mathrm{R}_T(v)$ sont mutuellement indépendants, et donc, si u était en-dessous de deux de ces sommets, il existerait deux chemins de la racine de T à u, ce qui est impossible puisque $u \in \overline{\mathrm{R}}_T(u)$.
2. Supposons d'abord que u et v sont indépendants, et qu'il existe un sommet $w \in \mathrm{R}_T(u) \cap \mathrm{R}_T(v)$. Alors, comme $\mathrm{R}_T(u) <_T u$ et $\mathrm{R}_T(v) <_T v$, il existe un chemin de la racine de T à w passant par u, et un autre passant par v, ce qui est impossible par hypothèse de stratification. Supposons maintenant que u est en-dessous de v. Alors le point 1 prouve que u est en-dessous d'un sommet $v' \in \mathrm{R}_T(v)$. S'il existait un sommet $u' \in \mathrm{R}_T(u) \cap \mathrm{R}_T(v)$, puisque $\mathrm{R}_T(u) <_T u \leq_T v'$, on aurait $u' <_T v'$, et donc le résidu $\mathrm{R}_T(v)$ ne serait pas indépendant, ce qui est impossible. Donc, $\mathrm{R}_T(u) \cap \mathrm{R}_T(v) = \emptyset$.
3. Supposons qu'il existe un sommet $w \in \overline{\mathrm{R}}_T(u) \cap \overline{\mathrm{R}}_T(v)$. Alors, $w \leq_T u$ et $w \leq_T v$, et par hypothèse de stratification, il existe un unique chemin de la racine de T à w. Nécessairement, soit $u \leq_T v$, soit $v \leq_T u$; sans perte de généralité, supposons que $u \leq_T v$. Alors, d'après le point 1, u est en-dessous d'un sommet $v' \in \mathrm{R}_T(v)$, et donc, $\overline{\mathrm{R}}_T(u) \leq_T v'$. Ceci prouve que w ne peut pas être élément de $\overline{\mathrm{R}}_T(v)$, et on a une contradiction avec l'hypothèse. ∎

Nous pouvons donc définir une partition des sommets du GA-terme considéré basée sur ces résidus.

Définition 6.4.2 La *partition résiduelle* $\mathcal{R}_T$ d'un GA-terme stratifié T est la partition de V dont les seules classes non triviales sont les résidus $\mathrm{R}_T(v)$ pour $v \in V_\mathrm{s}$. ◇

Exemple 6.4.3 Reprenons les GA-termes stratifiés de la Figure 6.6, et notons-les respectivement T_1, T_2 et T_3. Alors on a :

$$\begin{aligned}\mathcal{R}_{T_1} &= \{\{\mathfrak{a}\},\{\mathfrak{b}\},\{\mathfrak{c},\mathfrak{d},\mathfrak{e}\},\{\mathfrak{f}\}\},\\ \mathcal{R}_{T_2} &= \{\{\mathfrak{a}\},\{\mathfrak{b},\mathfrak{c}\},\{\mathfrak{d}\},\{\mathfrak{e}\}\},\\ \mathcal{R}_{T_3} &= \{\{\mathfrak{a}\},\{\mathfrak{b},\mathfrak{c}\},\{\mathfrak{d},\mathfrak{e}\},\{\mathfrak{f},\mathfrak{g}\}\}.\end{aligned}$$

Nous démontrons maintenant la propriété principale vérifiée par la partition résiduelle d'un GA-terme stratifié : cette dernière est stratifiée. Ceci permettra donc de définir une action de groupe basée sur cette partition.

Théorème 6.4.4 *La partition résiduelle $\mathcal{R}_T$ est stratifiée dans T.*

PREUVE. D'après la définition d'un GA-terme stratifié, il existe un unique chemin entre la racine de T et n'importe quel sommet dans une classe non triviale de $\mathcal{R}_T$. Considérons maintenant deux classes non triviales $\mathrm{R}_T(u)$ et $\mathrm{R}_T(v)$ de $\mathcal{R}_T$, où u et v sont des sommets de V_s. Supposons qu'un sommet $u' \in \mathrm{R}_T(u)$ soit strictement en-dessous d'un sommet $v' \in \mathrm{R}_T(v)$; il s'agit de montrer qu'alors toute la classe $\mathrm{R}_T(u)$ est strictement en-dessous de v'. Puisque chaque résidu est indépendant dans T, il est clair qu'on ne peut pas avoir $u = v$.

Il existe un unique chemin de la racine de T à u', notons-le p. Le fait que $u' <_T u$ et $u' <_T v' <_T v$ prouve que les sommets u, v et v' apparaissent dans p. Les sommets du sous-chemin de p allant de u à u' sont tous dans l'antirésidu $\overline{\mathrm{R}}_T(u)$, et comme $v \in V_\mathrm{s}$ et $v \neq u$, v ne peut pas être dans ce chemin. Donc, $u <_T v$.

De même, puisque les sommets du sous-chemin de p allant de v à v' sont dans $\overline{\mathrm{R}}_T(v)$, le sommet $u \in V_\mathrm{s}$ ne peut être dans ce chemin, et puisque $u <_T v$, on a nécessairement $u \leq_T v'$. Comme $\mathrm{R}_T(u) <_T u$, nous avons prouvé que $\mathrm{R}_T(u) <_T v'$, et donc que $\mathcal{R}_T$ est stratifiée dans T. ■

Ceci signifie que pour tout GA-terme stratifié (resp. A-terme stratifié) T, n'importe quelle permutation $\sigma \in \mathrm{Sym}_V(\mathcal{R}_T)$ transforme T en un GA-terme (resp. A-terme) T^σ, et que la partition $\mathcal{R}_T$ est stratifiée dans T^σ, d'après le Théorème 5.4.10. Maintenant, nous allons prouver que T^σ est stratifié. Afin de démontrer ce résultat, nous devons prouver qu'il existe des homomorphismes appropriés des A-termes attachés aux sommets $v \in V_\mathrm{s}$, vers les sous-termes $\mathrm{dm}_\mathrm{r}(T^\sigma|v)$. Nous serons plus précis que cela, et analyserons exactement le lien entre ces homomorphismes et les $\mathrm{h}_{[T,v]}$.

Pour cela, nous aurons besoin d'un lemme analogue au Lemme 6.4.1 afin de "séparer" les résidus des antirésidus. Même s'il est clair que le résidu et l'antirésidu d'un sommet $v \in V_\mathrm{s}$ sont disjoints, ceci n'est pas tout à fait le cas pour le résidu d'un sommet et l'antirésidu d'un autre.

Lemme 6.4.5 *Si u et v sont des éléments de V_s, alors le seul sommet qui peut être commun à $\mathrm{R}_T(u)$ et à $\overline{\mathrm{R}}_T(v)$ est v.*

PREUVE. On sait que ces deux ensembles sont disjoints si $u = v$, on peut donc supposer que $u \neq v$. Puisque $\mathrm{R}_T(u) <_T u$ et $\overline{\mathrm{R}}_T(v) \leq_T v$, si u et v sont indépendants, alors $\mathrm{R}_T(u)$ et $\overline{\mathrm{R}}_T(v)$ sont également disjoints. En effet, s'il existait un sommet $w \in \mathrm{R}_T(u) \cap \overline{\mathrm{R}}_T(v)$, il existerait deux chemins distincts de la racine de T à w, l'un passant par u et l'autre par v, ce qui est impossible par hypothèse de stratification. Supposons maintenant que u et v sont comparables par $<_T$.

Si $u <_T v$, alors, d'après le Lemme 6.4.1, u est en dessous d'un sommet v' de $\mathrm{R}_T(v)$, et donc $\mathrm{R}_T(u) \leq_T v'$. Les éléments de $\overline{\mathrm{R}}_T(v)$ sont soit indépendants de v', soit strictement au dessus de v', et ne peuvent donc pas être des éléments de $\mathrm{R}_T(u)$. Une fois encore, les ensembles sont disjoints.

Enfin, si $v <_T u$, d'après le Lemme 6.4.1, le sommet v est en-dessous d'un élément u' de $\mathrm{R}_T(u)$. Pour tout sommet $v' \in \overline{\mathrm{R}}_T(v)$ autre que v, on a $v' <_T v$, et donc $v' <_T u'$, et v' ne peut pas être dans l'ensemble indépendant $\mathrm{R}_T(u)$. Par contre, si $v = u'$, alors on a bien $v \in \mathrm{R}_T(u) \cap \overline{\mathrm{R}}_T(v)$. ∎

Ceci signifie que si u et v sont deux éléments de V_{s}, alors v peut ne pas être point fixe d'une permutation des éléments de $\mathrm{R}_T(u)$. Cela justifie la restriction à π dans le prochain lemme.

Lemme 6.4.6 *Soit σ une permutation dans $\mathrm{Sym}_V(\mathcal{R}_T)$, et v un sommet de T étiqueté par un élément $\langle f, c, G\rangle \in \Sigma_E$. On note π la restriction de σ à $\mathrm{R}_T(v)$, alors $\pi \circ \mathrm{h}_{[T,v]}$ est un homomorphisme de c vers $\mathrm{dm}_{\mathrm{r}}(T^\sigma|v)$.*

PREUVE. Posons $T = (V, s, a)$, $c = (V_c, s_c, a_c)$, et soit r la racine de c. Comme $\mathrm{h}_{[T,v]}$ est un homomorphisme de c vers $\mathrm{dm}_{\mathrm{r}}(T|v)$, l'image de r par $\mathrm{h}_{[T,v]}$ est la racine v de $\mathrm{dm}_{\mathrm{r}}(T|v)$. L'image de r par $\pi \circ \mathrm{dm}_{\mathrm{r}}(T|v)$ est donc $\pi(v) = v$, puisque $v \notin \mathrm{R}_T(v)$.

Pour tout sommet $w \in V_c$, si w n'est pas un sommet variable, il faut prouver que le symbole $s_c(w)$ et les arguments $a_c(w)$ sont préservés par la fonction $\pi \circ \mathrm{h}_{[T,v]}$ comme ils le sont par $\mathrm{h}_{[T,v]}$. L'image de w par $\mathrm{h}_{[T,v]}$ n'est pas un élément de $\mathrm{R}_T(v)$, et est donc un point fixe de π. Donc :

$$s(\ \pi \circ \mathrm{h}_{[T,v]}(w)\ ) \ =\ s(\ \mathrm{h}_{[T,v]}(w)\ ) \ =\ s_c(w).$$

Posons $a(\mathrm{h}_{[T,v]}(w)) = u_1.\cdots.u_n$, et soit $i \in \{1, \ldots, n\}$. Si u_i est dans le résidu $\mathrm{R}_T(v)$, alors $u_i^\sigma = u_i^\pi$. Sinon, u_i est dans l'antirésidu $\overline{\mathrm{R}}_T(v)$ mais est différent de v, et donc, d'après le Lemme 6.4.5, u_i doit être un point fixe de σ, et on a une fois de plus $u_i^\sigma = u_i^\pi = u_i$. On en déduit que

$$\begin{aligned} a^\sigma(\ \pi \circ \mathrm{h}_{[T,v]}(w)\ ) &= [a(\ \mathrm{h}_{[T,v]}(w)\ )]^\sigma \\ &= [a(\ \mathrm{h}_{[T,v]}(w)\ )]^\pi \ (\text{car } u_i^\sigma = u_i^\pi) \\ &= [\mathrm{h}_{[T,v]}(\ a_c(w)\ )]^\pi \\ &= \pi \circ \mathrm{h}_{[T,v]}(\ a_c(w)\ ). \end{aligned}$$ ∎

Par unicité des homomorphismes (Corollaire 5.2.6), on en déduit que

Corollaire 6.4.7 *Sous les hypothèses du lemme 6.4.6, on a* $\mathrm{h}_{[T^\sigma,v]} = \pi \circ \mathrm{h}_{[T,v]}$.

Une autre conséquence immédiate du Lemme 6.4.6 est que :

Corollaire 6.4.8 *Si* $T = (V, s, a)$ *est un* GA*-terme (resp.* A*-terme) stratifié, alors pour toute permutation* $\sigma \in \mathrm{Sym}_V(\mathcal{R}_T)$, T^σ *est également un* GA*-terme (resp.* A*-terme) stratifié.*

Le Lemme 6.4.6 peut également être utilisé pour prouver l'invariance de la partition résiduelle sous l'action de σ :

Théorème 6.4.9 *Pour tout* $\sigma \in \mathrm{Sym}_V(\mathcal{R}_T)$, *on a* $\mathcal{R}_{T^\sigma} = \mathcal{R}_T$.

PREUVE. Soit v un sommet de T étiqueté par un symbole $\langle f, c, G\rangle \in \Sigma_E$, et notons π_v la restriction de σ au résidu $\mathrm{R}_T(v)$, π_v est donc une permutation de $\mathrm{R}_T(v)$. Les ensembles $\mathrm{R}_T(v)$ et $\mathrm{R}_{T^\sigma}(v)$ sont respectivement les images par $\mathrm{h}_{[T,v]}$ et $\mathrm{h}_{[T^\sigma,v]} = \pi_v \circ \mathrm{h}_{[T,v]}$ de l'ensemble des sommets variables de c, donc, d'après le Lemme 6.4.6, on a $\mathrm{R}_{T^\sigma}(v) = \mathrm{R}_T(v)^{\pi_v} = \mathrm{R}_T(v)$. ∎

6.5 Réécriture stratifiée et action de groupe

Dans ce qui précède, nous avons vu comment construire des GA-termes stratifiés, et définir une partition stratifiée sur chacun de ces GA-termes stratifiés. Cette partition stratifiée permet donc de construire une action de groupe sur les GA-termes stratifiés considérés. Etant donné un GA-terme stratifié T, nous montrons maintenant comment construire un groupe $\mathcal{G}_T$ dont l'action sur T produira une orbite $T^{\mathcal{G}_T}$, telle que l'ensemble $\tau(\mathrm{dm}(T^{\mathcal{G}_T}))$ est l'ensemble stratifié $\mathrm{S}[T]$ défini dans [AP01].

Définition 6.5.1 ($\mathcal{G}_T$ et $\mathcal{G}_T(v)$) Soient T un élément de GA-$\mathcal{S}(V, s)$, et v un élément de V_s tel que $s(v) = \langle f, c, G\rangle$. La restriction de $\mathrm{h}_{[T,v]}$ à l'ensemble des sommets variables de c étant une bijection sur le résidu $\mathrm{R}_T(v)$ (d'après la Propriété 6.3.4), on peut définir le groupe $\mathcal{G}_T(v)$ comme le conjugué par $\mathrm{h}_{[T,v]}$ du groupe G, c'est-à-dire :

$$\mathcal{G}_T(v) = G^{\mathrm{h}_{[T,v]}}.$$

Le groupe $\mathcal{G}_T$ associé à T est le produit des groupes $\mathcal{G}_T(v)$ pour tous les sommets $v \in V_\mathrm{s}$, si ce dernier ensemble n'est pas vide ; sinon, $\mathcal{G}_T$ est le groupe trivial I. ◇

Exemple 6.5.2 Soit A le A-terme stratifié de l'Exemple 6.3.2. L'homomorphisme $\mathrm{h}_{[A,2]}$ était défini par :

v	ε	1	2	1.1	1.2
$h(v)$	2	2.1	2.2	2.1.1	2.1.2

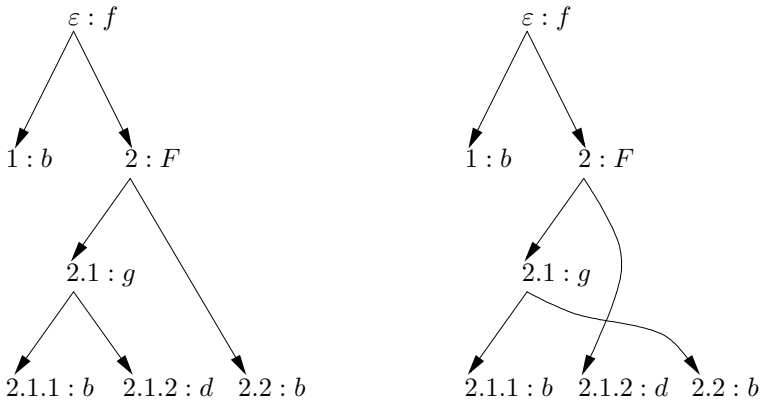

FIG. 6.8 – T et $T^{(2.1.2\ 2.2)}$

Donc,

$$\mathcal{G}_A(2) \;=\; G^{\mathrm{h}_{[A,2]}} \;=\; \mathrm{Sym}(\{1.1, 1.2, 2\})^{\mathrm{h}_{[A,2]}} = \mathrm{Sym}(\{2.1.1, 2.1.2, 2.2\}).$$

Le sommet 2 étant le seul sommet de A à être étiqueté par un élément de Σ_E, on a $\mathcal{G}_A = \mathcal{G}_A(2)$. On peut donc appliquer par exemple la permutation $\sigma = (2.1.2\ 2.2)$ à A, on est sûrs d'obtenir un A-terme stratifié (voir la Figure 6.8).

Notons qu'on avait $A = \mathrm{arbre}(\ f(b,\ F(g(b,d),\ b))\ )$, mais qu'il n'existe pas de terme t' tel que $A^\sigma = \mathrm{arbre}(t')$. Ainsi, par exemple, on a $\tau(A^\sigma)|2.2 = d = \tau(A^\sigma|2.1.2)$.

Le produit des $\mathcal{G}_T(v)$ pour $v \in V_{\mathrm{s}}$ est bien défini puisque les ensembles $\mathrm{R}_T(v)$ sont disjoints. Comme $\mathcal{G}_T(v)$ est un sous-groupe de $\mathrm{Sym}(\mathrm{R}_T(v))$, on en déduit que $\mathcal{G}_T$ est un sous-groupe de $\mathrm{Sym}_V(\mathcal{R}_T)$. Ceci signifie que les permutations dans $\mathcal{G}_T$ préservent toutes les propriétés structurelles mentionnées plus haut, et préservent aussi les groupes $\mathcal{G}_T(v)$:

Lemme 6.5.3 *Pour toute permutation $\sigma \in \mathcal{G}_T$ et tout sommet $v \in V_{\mathrm{s}}$, on a $\mathcal{G}_{T^\sigma}(v) = \mathcal{G}_T(v)$.*

PREUVE. Posons $s(v) = \langle f, c, G\rangle$, et soit π la restriction de σ à $\mathrm{R}_T(v)$. π est donc une permutation de $\mathrm{R}_T(v)$, d'où $\pi \in \mathcal{G}_T(v)$. Par le Corollaire 6.4.7, on a :

$$\mathcal{G}_{T^\sigma}(v) \;=\; G^{\pi \circ \mathrm{h}_{[T,v]}} \;=\; (G^{\mathrm{h}_{[T,v]}})^\pi \;=\; \pi^{-1}\ \mathcal{G}_T(v)\ \pi \;=\; \mathcal{G}_T(v). \qquad \blacksquare$$

Comme tous les groupes $\mathcal{G}_T(v)$ sont préservés, on en déduit immédiatement que :

Corollaire 6.5.4 *Pour tout* GA*-terme T et toute permutation $\sigma \in \mathcal{G}_T$, on a $\mathcal{G}_{T^\sigma} = \mathcal{G}_T$.*

Propriété 6.5.5 *Soit T un* GA*-terme stratifié, et v un sommet de T étiqueté par un symbole de Σ_E. Alors, pour toute permutation $\sigma \in \mathcal{G}_T$, si σ_v est la restriction de σ à l'ensemble des sommets de $T|v$, alors $\sigma_v \in \mathcal{G}_{T|v}$ et $T^\sigma|v = (T|v)^{\sigma_v}$.*

PREUVE. Pour $u \in V_s$, notons μ_u la restriction de σ à $R_T(u)$. Alors, par définition,

$$\sigma = \prod_{u \in V_s} \mu_u, \text{ et } \sigma_v = \prod_{u \in V_s, u \leq_T v} \mu_u,$$

ce qui prouve que σ_v est bien élément de $\mathcal{G}_{T|v}$, et il est alors aisé de vérifier que $T^\sigma|v = (T|v)^{\sigma_v}$. ∎

Propriété 6.5.6 *Soit $T = (V, s, a)$ un GA-terme stratifié, pour $v \in V_s$, on note S_v un ensemble générateur du groupe $\mathcal{G}_T(v)$. Alors $\cup_{v \in V_s} S_v$ est un ensemble de générateurs du groupe $\mathcal{G}_T$.*

PREUVE. Ceci est une conséquence triviale du Corollaire 3.4.7, puisque les $R_T(v)$ sont mutuellement disjoints. ∎

Lemme 6.5.7 *Soit T un GA-terme stratifié, et $\sigma \in \mathcal{G}_T$. Alors T et T^σ ont la même hauteur stratifiée.*

PREUVE. On démontre le résultat par induction sur la hauteur stratifiée de T. Supposons que le résultat soit vrai pour tous les GA-termes stratifiés de hauteur inférieure ou égale à k, et que T est de hauteur $k+1$. Supposons que la racine r de T est étiquetée par un symbole de Σ_E, l'autre cas est similaire. Alors, pour tout sommet $v \in R_T(r)$, si σ_v est la restriction de σ à l'ensemble des sommets de $T|v$, alors on a $T^\sigma|v = (T|v)^{\sigma_v}$ d'après la Propriété 6.5.5. Comme $\sigma_v \in \mathcal{G}_{T|v}$, par hypothèse d'induction, $(T|v)^{\sigma_v}$ est de même hauteur stratifiée que $T|v$. Comme ceci est vrai pour tout $v \in R_T(r)$, on a le résultat. ∎

Traduisons maintenant les résultats obtenus en termes d'actions de groupe.

Définition 6.5.8 Pour toute partition $\mathcal{P}$ de V, et tout groupe de permutation G de V, on note GA-$\mathcal{S}(V, s, \mathcal{P}, G)$ l'ensemble des GA-termes stratifiés T éléments de GA-$\mathcal{S}(V, s)$ tels que $\mathcal{R}_T = \mathcal{P}$ et $\mathcal{G}_T = G$. ◇

Il est clair que tout GA-terme stratifié T appartient à exactement un de ces ensembles, à savoir GA-$\mathcal{S}(V_T, s_T, \mathcal{R}_T, \mathcal{G}_T)$.

Théorème 6.5.9 *Pour toute partition $\mathcal{P}$ de V et tout groupe de permutation G sur V, l'ensemble GA-$\mathcal{S}(V, s, \mathcal{P}, G)$ est stable sous l'action de G.*

PREUVE. Pour tout GA-terme stratifié $T \in$ GA-$\mathcal{S}(V, s, \mathcal{P}, G)$, et pour toute permutation $\sigma \in G$, on a $\mathcal{R}_T = \mathcal{P}$ et $\mathcal{G}_T = G$, donc $\sigma \in \mathrm{Sym}_V(\mathcal{P})$. D'après le Théorème 6.4.4, $\mathcal{P}$ est stratifiée dans T, et donc, d'après le Théorème 5.4.10, T^σ est un GA-terme. Le Lemme 6.4.6 prouve que T^σ est un GA-terme stratifié, et donc que $T^\sigma \in$ GA-$\mathcal{S}(V, s)$. Enfin, on a $\mathcal{R}_{T^\sigma} = \mathcal{P}$ d'après le Théorème 6.4.9, et $\mathcal{G}_{T^\sigma} = G$ d'après le Corollaire 6.5.4, ce qui prouve que T^σ est bien un élément de GA-$\mathcal{S}(V, s, \mathcal{P}, G)$. ∎

Nous pouvons maintenant établir de quelle façon les orbites des GA-termes stratifiés par ces actions sont liées à la notion de réécriture stratifiée de [AP01].

Définition 6.5.10 (Réécriture stratifiée) Soient T et T' deux GA-termes stratifiés, et un v sommet de T étiqueté par un symbole de Σ_E. On dit que T *se réécrit en* v en T', ce qu'on note $T \to_v T'$, si et seulement s'il existe une permutation $\sigma \in \mathcal{G}_T(v)$ telle que $T' = T^\sigma$.

La *réécriture stratifiée* est l'union disjointe $\to$ des relations $\to_v$ pour tous les sommets v étiquetés par des symboles de Σ_E. La relation $\to^\star$ est la fermeture réflexive et transitive de $\to$.

L'*orbite stratifiée* de T, notée $[T]_{\mathrm{s}}$, est l'ensemble de tous les GA-termes accessibles depuis T par $\to^\star$, c'est-à-dire :

$$[T]_{\mathrm{s}} = \{T' \in \text{GA-}\mathcal{S}(V,s) \mid T \to^\star T'\}.$$

On définit également l'*ensemble stratifié* de T, noté $\mathrm{S}[T]$, comme l'ensemble de termes $\mathrm{S}[T] = \{\tau(\mathrm{dm}(T')) \mid T' \in [T]_{\mathrm{s}}\}$. ◇

Prouvons d'abord que notre définition de réécriture stratifiée correspond bien à celle de [AP01] :

Théorème 6.5.11 *Soit e une équation permutative de contexte associé c, de permutation associée σ, et soit Σ_E une signature stratifiée telle que $\langle f, c, \mathcal{G}\rangle \in \Sigma_E$, où $\sigma \in \mathcal{G}$. Si A est un* A*-terme stratifié dont un sommet v est étiqueté par $\langle f, c, \mathcal{G}\rangle$, alors, en posant $\mu = \sigma^{\mathrm{h}_{[A,v]}}$, on a*

$$e \models \tau(\mathrm{dm}(A)) \rightleftharpoons \tau(\mathrm{dm}(A^\mu)).$$

PREUVE. Soit t un terme tel que $c = \mathrm{arbre}(t)$, par abus de notation, on note e l'équation $t[v_1, \ldots, v_n] \rightleftharpoons t[v_i^\sigma, \ldots, v_n^\sigma]$, où les v_i sont les sommets variables de c, et on définit la permutation $\pi \in \mathrm{Sym}(n)$ telle que pour tout $i = 1, \ldots, n$, $v_i^\sigma = v_{i^\pi}$.

Pour $i = 1, \ldots, n$, on note $u_i = \mathrm{h}_{[A,v]}(v_i)$, et on définit $s_i = \tau(\mathrm{dm}(A|u_i))$; on a donc $\tau(\mathrm{dm}(A|v)) = t[s_1, \ldots, s_n]$. Soit $w_i = \mathrm{h}_{[A^\mu,v]}(v_i)$, alors, d'après le Corollaire 6.4.7, on a

$$w_i \;=\; \mu \circ \mathrm{h}_{[A,v]}(v_i) \;=\; [\mathrm{h}_{[A,v]}(v_i)]^\mu \;=\; \mathrm{h}_{[A,v]}(v_i^\sigma) \;=\; \mathrm{h}_{[A,v]}(v_{i^\pi}) \;=\; u_{i^\pi}.$$

Donc, pour tout i, on a $w_i = u_{i^\pi}$, et $\tau(\mathrm{dm}(A^\mu|v_i)) = t[s_{1^\pi}, \ldots, s_{n^\pi}]$.

On en déduit que $e \models t[s_1, \ldots, s_n] \rightleftharpoons t[s_{1^\pi}, \ldots, s_{n^\pi}]$, et enfin que $e \models \tau(\mathrm{dm}(A)) \rightleftharpoons \tau(\mathrm{dm}(A^\mu))$. ■

Corollaire 6.5.12 *Soit T un* GA*-terme stratifié et $t = \tau(\mathrm{dm}(T))$, alors $\mathrm{S}[t]$ est inclus dans la classe de congruence de t modulo E.*

Montrons maintenant que l'orbite stratifiée de T est exactement l'orbite de T sous l'action du groupe $\mathcal{G}_T$ associé à T.

Théorème 6.5.13 $[T]_{\mathrm{s}} = T^{\mathcal{G}_T}$.

PREUVE. Montrons tout d'abord par induction que pour tout $n \in \mathbb{N}$ et pour tout GA-terme T' tel que $T \to^n T'$, il existe une permutation $\sigma \in \mathcal{G}_T$ telle que $T' = T^\sigma$. Ceci est trivial pour $n = 0$, car dans ce cas, $T' = T$, et il suffit de prendre $\sigma = \mathrm{id}$.

Supposons que le résultat est vrai pour $n > 0$, et soit T' un graphe de terme tel que $T \to^{n+1} T'$. Par hypothèse d'induction, il existe une permutation σ dans $\mathcal{G}_T$ telle que $T \to^n T^\sigma \to T'$. Par définition de $\to$, il existe donc un sommet $v \in V_\mathrm{s}$ tel que $T^\sigma \to_v T'$, c'est-à-dire une permutation $\pi \in \mathcal{G}_{T^\sigma}(v) = \mathcal{G}_T(v)$ (d'après le Lemme 6.5.3) telle que $T' = (T^\sigma)^\pi = T^{\sigma\pi}$. Comme $\sigma\pi$ est élément de $\mathcal{G}_T$, on a le résultat.

Pour tout GA-terme T' de $[T]_\mathrm{s}$, qui est donc tel que $T \to^\star T'$, il existe un $n \in \mathbb{N}$ tel que $T \to^n T'$, et on vient de prouver qu'alors T' était dans $T^{\mathcal{G}_T}$. Ceci prouve donc que $[T]_\mathrm{s} \subseteq T^{\mathcal{G}_T}$.

Réciproquement, soit σ une permutation dans $\mathcal{G}_T$. On prend un ordre quelconque sur les éléments de V_s, et on note ces éléments $\{v_1, \ldots, v_n\}$. On considère la restriction π_i de σ au résidu $\mathrm{R}_T(v_i)$; π_i est donc dans le groupe $\mathcal{G}_T(v_i)$, pour $1 \leq i \leq n$. Enfin, on considère la séquence $\sigma_1, \ldots, \sigma_{n+1}$ de permutations définies par $\sigma_1 = \mathrm{id}$, et $\sigma_{i+1} = \sigma_i\pi_i$.

Il est clair que σ_i est élément $\mathcal{G}_T$, et donc, que π_i est dans le groupe $\mathcal{G}_{T^{\sigma_i}}(v_i)$ d'après le Lemme 6.5.3. D'après la définition de $\to_{v_i}$, on a

$$T^{\sigma_i} \to_{v_i} (T^{\sigma_i})^{\pi_i},$$

et donc $T^{\sigma_i} \to T^{\sigma_{i+1}}$. On en déduit que $T^{\sigma_1} \to^\star T^{\sigma_{n+1}}$. Comme σ_{n+1} est le produit des π_i pour $1 \leq i \leq n$, on a $\sigma_{n+1} = \sigma$. Puisque $T^{\sigma_1} = T$, on en déduit que tous les T^σ peuvent-être atteints depuis T par $\to^\star$, et on a donc l'inclusion réciproque $T^{\mathcal{G}_T} \subseteq [T]_\mathrm{s}$. ■

6.6 GA-termes stratifiés et homomorphismes

Dans cette partie, nous allons étudier les propriétés vérifiées par des GA-termes stratifiés liés par un homomorphisme (qui est nécessairement clos car tout GA-terme stratifié est clos par définition). Ces propriétés nous permettront par exemple de démontrer facilement que si deux GA-termes sont bisimilaires, alors leurs ensembles stratifiés sont égaux.

Le Théorème 5.2.20 garantit que pour tout GA-terme T, il existe un A-terme A tel que $T \Subset A$, nous prouvons maintenant que si T est un GA-terme stratifié, alors A est un A-terme stratifié.

Lemme 6.6.1 *Soient T un GA-terme stratifié, et A un A-terme tel que $T \Subset A$, alors A est un A-terme stratifié.*

PREUVE. Notons h l'homomorphisme clos de A vers T, soit v un sommet de T étiqueté par un symbole $\langle f, c, G\rangle \in \Sigma_E$, et soit u un sommet de A tel que $h(u) = v$. Il s'agit de prouver qu'il existe un homomorphisme de c vers $\mathrm{dm_r}(A|u)$. D'après la Propriété 5.2.5, une restriction de h est un homomorphisme clos de $A|u$ vers $T|v$, c'est donc également un homomorphisme clos de $\mathrm{dm_r}(A|u)$ vers $\mathrm{dm_r}(T|v)$. Comme $\mathrm{h}_{[T,v]}$ est par définition un homomorphisme de c vers $\mathrm{dm_r}(T|v)$, d'après le Lemme 5.2.21, il existe un homomorphisme de c vers $\mathrm{dm_r}(A|u)$, d'où le résultat. ■

Lemme 6.6.2 *Soient T et T' deux* GA*-termes stratifiés tels qu'il existe un homomorphisme h de T vers T'. Alors pour tout sommet u de T étiqueté par un symbole de Σ_E, on a :* $\mathrm{h}_{[T',h(u)]} = h \circ \mathrm{h}_{[T,u]}$.

PREUVE. Ce résultat est évident : u et $h(u)$ sont nécessairement étiquetés par un même symbole de Σ_E. De plus, (une restriction de) h est également un homomorphisme de $T|u$ vers $T'|h(u)$ (Propriété 5.2.5), et cette restriction est un homomorphisme de $\mathrm{dm_r}(T|u)$ vers $\mathrm{dm_r}(T'|h(u))$, puisque les racines de ces GA-termes sont étiquetées par le même symbole. D'après la Propriété 5.2.4, on en déduit que $h \circ \mathrm{h}_{[T,u]}$ est un homomorphisme de c vers $\mathrm{dm_r}(T'|h(u))$, et par unicité des homomorphismes, on a le résultat. ∎

Ce lemme permet de démontrer aisément le résultat suivant :

Corollaire 6.6.3 *Si T et T' sont deux* GA*-termes stratifiés tels qu'il existe un homomorphisme h de T vers T', alors ces deux* GA*-termes ont la même hauteur stratifiée.*

PREUVE. On démontre le résultat par induction sur la hauteur de T. On démontre le résultat dans le cas où la racine r de T est étiquetée par le symbole $\langle f, c, G\rangle \in \Sigma_E$, la démonstration dans l'autre cas est similaire. La racine r' de T' est également étiquetée par le symbole $\langle f, c, G\rangle$, et pour tout sommet $w \in \mathcal{SV}(c)$, si $v = \mathrm{h}_{[T,r]}(w)$, alors, d'après le Lemme 6.6.2, $\mathrm{h}_{[T',r']}(w) = h \circ \mathrm{h}_{[T,r]}(w) = h(v)$. D'après la Propriété 5.2.5, on en déduit donc qu'une restriction de h est un homomorphisme de $T|v$ vers $T'|h(v)$, et par hypothèse d'induction, ces deux GA-termes stratifiés ont la même hauteur stratifiée. On en déduit que T et T' ont également la même hauteur stratifiée. ∎

Lemme 6.6.4 *Soient T et T' deux* GA*-termes stratifiés de racines respectives r et r', toutes deux étiquetées par un symbole $\langle f, c, G\rangle \in \Sigma_E$, et supposons qu'il existe un homomorphisme h de* $\mathrm{dm}(T)$ *vers* $\mathrm{dm}(T')$. *Alors :*

1. *pour tout sommet $u \in \mathrm{R}_T(r)$, on a $h(u) \in \mathrm{R}_{T'}(r')$,*
2. *si $v' \in \mathrm{R}_{T'}(h(u))$ (resp. $v' \in \overline{\mathrm{R}}_{T'}(h(u))$), alors il existe un unique sommet v de T tel que $h(v) = v'$, et $v \in \mathrm{R}_T(u)$ (resp. $\overline{\mathrm{R}}_T(u)$).*

PREUVE. 1. Soit $u \in \mathrm{R}_T(r)$, alors il existe un sommet variable $w \in \mathcal{SV}(c)$ tel que $u = \mathrm{h}_{[T,r]}(w)$, d'où $h(u) = h \circ \mathrm{h}_{[T,r]}(w)$, et d'après le Lemme 6.6.2, $h(u) = \mathrm{h}_{[T',h(r)]}(w)$. Comme $h(r) = r'$, on a le résultat.
2. Soit $v' \in \mathrm{R}_{T'}(h(u))$, et soit w le sommet variable de c tel que $v' = \mathrm{h}_{[T',h(u)]}(w)$. Alors le sommet $v = \mathrm{h}_{[T,u]}(w)$ est élément de $\mathrm{R}_T(u)$, et $v' = h(v)$ d'après le Lemme 6.6.2. Supposons maintenant qu'il existe deux sommets v_1 et v_2 tels que $h(v_1) = h(v_2) = v'$, et soient p_1 et p_2 deux chemins de la racine de T à v_1 et à v_2 dans T, respectivement. Alors, d'après la Propriété 5.2.5 3 et le Lemme 5.1.5, $h(p_1)$ et $h(p_2)$ sont deux chemins distincts de la racine de T' à v' dans T', ce qui est impossible puisque $v' \in \mathrm{R}_{T'}(h(u))$. Il existe donc un unique sommet v tel que $h(v) = v'$, et v est élément de $\mathrm{R}_T(u)$. La preuve dans le cas où $v' \in \overline{\mathrm{R}}_{T'}(h(u))$ est identique. ∎

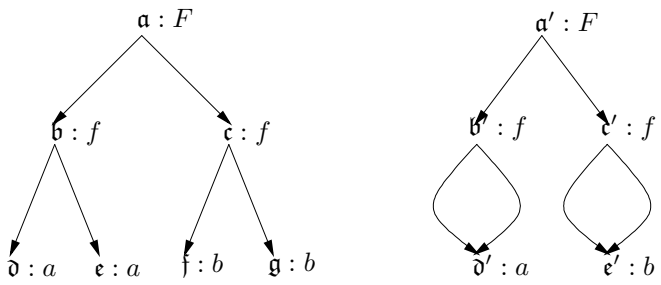

FIG. 6.9 – GA-termes stratifiés de l'Exemple 6.6.6

Corollaire 6.6.5 *Sous les hypothèses du Lemme 6.6.4, $v \in \mathrm{R}_T(u)$ (resp. $v \in \overline{\mathrm{R}}_T(u)$) si et seulement si $v' \in \mathrm{R}_{T'}(h(u))$ (resp. $v' \in \overline{\mathrm{R}}_{T'}(h(u))$). Donc, pour tout sommet u de T étiqueté par un symbole $\langle f, c, G\rangle \in \Sigma_E$, les restrictions de h à $\mathrm{R}_T(u)$ et à $\overline{\mathrm{R}}_T(u) \cup \mathrm{R}_T(u)$ sont des bijections, respectivement vers $\mathrm{R}_{T'}(h(u))$, et $\overline{\mathrm{R}}_{T'}(h(u)) \cup \mathrm{R}_{T'}(h(u))$.*

PREUVE. Si u est un sommet de T étiqueté par un symbole $\langle f, c, G\rangle \in \Sigma_E$, alors les restrictions de h à $\mathrm{R}_T(u)$ et à $\overline{\mathrm{R}}_T(u)$ sont des bijections, respectivement vers $\mathrm{R}_{T'}(h(u))$ et $\overline{\mathrm{R}}_{T'}(h(u))$ d'après le Lemme 6.6.4. Ces deux ensembles étant disjoints, on en déduit que la restriction de h à $\overline{\mathrm{R}}_T(u) \cup \mathrm{R}_T(u)$ est également une bijection. ∎

Ainsi, étant donnés deux GA-termes stratifiés T et T', s'il existe un homomorphisme h de T vers T', alors la restriction de h aux classes non triviales de la partition $\mathcal{R}_T$ est une bijection, ce qui prouve que les conjugués $\mathcal{G}_T(v)^h$, où $v \in V_{\mathrm{s}}$, et $\mathcal{G}_T^h$ sont bien définis.

Exemple 6.6.6 Soit $F = \langle f, c, G\rangle$, où $\tau(c) = f(\circ, \circ)$, et $G = \mathrm{Sym}(2)$, et soit $\Sigma_E = \{F\}$. Si T et T' sont les GA-termes stratifiés de la Figure 6.9, alors il est clair qu'il existe un homomorphisme h de T vers T', et en particulier, $h(\mathfrak{b}) = \mathfrak{b}'$, et $h(\mathfrak{c}) = \mathfrak{c}'$. Soit $\sigma = (\mathfrak{b}\ \mathfrak{c})$, alors $\sigma^h = (\mathfrak{b}'\ \mathfrak{c}')$, et comme $\mathcal{G}_T(\mathfrak{a}) = \mathrm{Sym}(\{\mathfrak{b}, \mathfrak{c}\})$, on a $(\mathcal{G}_T(\mathfrak{a}))^h = \mathrm{Sym}(\{\mathfrak{b}', \mathfrak{c}'\})$.

Lemme 6.6.7 *Soient T et T' deux GA-termes stratifiés tels qu'il existe un homomorphisme h de T vers T', et soit u un sommet de T. Si u est étiqueté par $\langle f, c, G\rangle \in \Sigma_E$, alors, pour tout $\mu \in G$, si $\sigma = \mu^{\mathrm{h}_{[T,u]}}$, alors $\sigma^h = \mu^{\mathrm{h}_{[T',h(u)]}}$.*

PREUVE. Ceci est évident, d'après la Propriété 3.4.18 et le Lemme 6.6.2, on a :

$$\sigma^h \;=\; (\mu^{\mathrm{h}_{[T,u]}})^h \;=\; \mu^{h \circ \mathrm{h}_{[T,u]}} \;=\; \mu^{\mathrm{h}_{[T',h(u)]}}.$$ ∎

Corollaire 6.6.8 *Sous les hypothèses du Lemme 6.6.7, on a*

$$\mathcal{G}_{T'}(h(u)) \;=\; (\mathcal{G}_T(u))^h, \text{ et } \mathcal{G}_{T'} \;=\; \mathcal{G}_T^h.$$

Théorème 6.6.9 *Soient T et T' deux* GA*-termes stratifiés, tels qu'il existe un homomorphisme h de T vers T'. Alors pour toute permutation $\sigma \in \mathcal{G}_T$, h est un homomorphisme de T^σ vers T'^{σ^h}.*

PREUVE. Posons $T = (V, s, a)$, $T' = (V', s', a')$, et $\mu = \sigma^h$. Alors on a $T^\sigma = (V, s, a^\sigma)$, et $T'^\mu = (V', s', a'^\mu)$; il s'agit de prouver que pour tout sommet $v \in V$, $a'^\mu(h(v)) = h(a^\sigma(v))$. Soit $v \in V$, et posons $a(v) = v_1.\cdots.v_n$, alors :

$$\begin{aligned} a'(h(v)) &= h(v_1).\cdots.h(v_n), \\ a^\sigma(v) &= v_1^\sigma.\cdots.v_n^\sigma, \\ a'^\mu(h(v)) &= h(v_1)^\mu.\cdots.h(v_n)^\mu. \end{aligned}$$

Soit $i \in \{1, \ldots, n\}$, s'il existe un sommet $u \in V_{\mathrm{s}}$ tel que $v_i \in \mathrm{R}_T(u)$, alors $h(v_i) \in \mathrm{R}_{T'}(h(u))$ d'après le Corollaire 6.6.5, et donc, comme $\mu = \sigma^h$, on a $h(v_i)^\mu = h(v_i^\sigma)$. Sinon, on a

$$v_i^\sigma = v_i, \text{ et } h(v_i)^\mu = h(v_i),$$

d'où $h(v_i)^\mu = h(v_i^\sigma)$, ce qui prouve qu'on a bien $a'^\mu(h(v)) = h(a^\sigma(v))$. ∎

Corollaire 6.6.10 *Sous les hypothèses du Théorème 6.6.9, la fonction η qui à $T^\sigma \in [T]_{\mathrm{s}}$ associe $T'^{\sigma^h} \in [T']_{\mathrm{s}}$ est une bijection ; on a donc* $\mathrm{S}[T] = \mathrm{S}[T']$.

PREUVE. La fonction η est bien définie d'après le Théorème 6.6.9. D'après le Théorème 5.4.12 et le Corollaire 6.6.8, ces deux ensembles ont la même cardinalité $|\mathcal{G}_T| = |\mathcal{G}_{T'}|$, il suffit donc de montrer que la fonction est injective. Supposons qu'il existe deux permutations $\sigma_1, \sigma_2 \in \mathcal{G}_T$ telles que $\eta(T^{\sigma_1}) = \eta(T^{\sigma_2})$. Alors $T'^{\sigma_1^h} = T'^{\sigma_2^h}$, ce qui prouve que $\sigma_1^h = \sigma_2^h$ d'après le Théorème 5.4.12, et donc, que $\sigma_1 = \sigma_2$. La fonction η est bien une bijection de $[T]_{\mathrm{s}}$ vers $[T']_{\mathrm{s}}$.

Comme pour tout $T'' \in [T]_{\mathrm{s}}$, on a $\tau(\mathrm{dm}(T'')) = \tau(\mathrm{dm}(\eta(T'')))$, on en déduit que $\mathrm{S}[T] = \mathrm{S}[T']$. ∎

Ce théorème fournit donc une description précise de la façon dont sont liés les éléments de $[T]_{\mathrm{s}}$ et $[T']_{\mathrm{s}}$ quand T et T' sont liés par un homomorphisme. Une conséquence immédiate de cette propriété, qui aurait été ardue à démontrer sans se servir du Théorème 6.6.9, est que deux GA-termes stratifiés bisimilaires produisent des ensembles stratifiés identiques.

Corollaire 6.6.11 *Si T et T' sont deux* GA*-termes stratifiés bisimilaires, alors* $\mathrm{S}[T] = \mathrm{S}[T']$.

PREUVE. Soient A et A' deux A-termes tels qu'il existe des homomorphismes clos h et h', respectivement de A vers T et de A' vers T'. Leur existence est garantie par le Théorème 5.2.20, et ces A-termes sont stratifiés d'après le Lemme 6.6.1. Comme T et T' sont bisimilaires, d'après le Corollaire 5.2.18, A et A' sont isomorphes, et donc, d'après le Corollaire 6.6.10, on a

$$\mathrm{S}[T] = \mathrm{S}[A] = \mathrm{S}[A'] = \mathrm{S}[T'].$$ ∎

La technique utilisée pour la démonstration de ce dernier résultat sera fréquemment réemployée : pour démontrer une propriété vérifiée par des GA-termes stratifiés T et T', on considérera des A-termes stratifiés A et A' tels que $T \Subset A$ et $T' \Subset A'$, sur lesquels la propriété sera démontrée. Puis, en se servant du Théorème 6.6.9, on en déduira la propriété pour T et T'.

Définition 6.6.12 ($\mathbf{h}^{T}_{[u\to v]}$) Soient T et T' deux GA-termes stratifiés, u un sommet de T, v un sommet de T', et supposons que u et v sont étiquetés par le même symbole $\langle f, c, G\rangle \in \Sigma_E$. Alors on définit $\mathrm{h}^{T}_{[u\to v]}$ comme la bijection $\mathrm{h}_{[T',v]} \circ \mathrm{h}^{-1}_{[T,u]}$ de $\mathrm{h}_{[T,u]}(V_c)$ vers $\mathrm{h}_{[T',v]}(V_c)$, où V_c est l'ensemble des sommets de c. La fonction inverse de $\mathrm{h}^{T}_{[u\to v]}$ est donc $\mathrm{h}^{T'}_{[v\to u]}$.

Quand aucune confusion n'est possible, on omettra d'expliciter T, pour simplement noter cette fonction $\mathrm{h}_{[u\to v]}$. ◇

Propriété 6.6.13 *Soient $T = (V, s, a)$ et $T' = (V', s', a')$ deux GA-termes stratifiés de racines respectives r et r' toutes deux étiquetées par un même symbole $\langle f, c, G\rangle \in \Sigma_E$. Alors pour tout sommet $v \in \overline{\mathrm{R}}_T(r)$, on a $\mathrm{h}_{[r\to r']}(a(v)) = a'(\mathrm{h}_{[r\to r']}(v))$.*

PREUVE. On pose $c = (V_c, s_c, a_c)$, soient $v \in \overline{\mathrm{R}}_T(r)$ et $u = a(v)_i$, où $i \in \{1, \ldots, \text{arité}(s(r))\}$. Alors, le sommet $w = \mathrm{h}^{-1}_{[T,r]}(v)$ est bien défini, et on a

$$\mathrm{h}_{[T,r]}(a_c(w)_i) \;=\; a(\mathrm{h}_{[T,r]}(w))_i \;=\; a(v)_i \;=\; u,$$

d'où $\mathrm{h}^{-1}_{[T,r]}(u) = a_c(w)_i$. On déduit que

$$\mathrm{h}_{[r\to r']}(u) \;=\; \mathrm{h}_{[T',r']}(a_c(w)_i) \;=\; a'(\mathrm{h}_{[T',r']}(w))_i \;=\; a'(\mathrm{h}_{[r\to r']}(u))_i,$$

d'où le résultat. ∎

Lemme 6.6.14 *Soient T_1, T_1', T_2 et T_2' des GA-termes stratifiés tels qu'il existe un homomorphisme h_1 de T_1 vers T_1' et un homomorphisme h_2 de T_2 vers T_2'.*

Soient u un sommet de T_1, v un sommet de T_2, et supposons que u et v sont tous deux étiquetés par le même symbole de Σ_E. Par abus de notation, on confond h_1 (resp. h_2) avec sa restriction à $\overline{\mathrm{R}}_{T_1}(u) \cup \mathrm{R}_{T_1}(u)$ (resp. $\overline{\mathrm{R}}_{T_2}(v) \cup \mathrm{R}_{T_2}(v)$), qui est une bijection d'après le Corollaire 6.6.5. Alors on a

$$\mathrm{h}^{T_1'}_{[h_1(u)\to h_2(v)]} \;=\; h_2 \circ \mathrm{h}^{T_1}_{[u\to v]} \circ h_1^{-1}.$$

PREUVE. D'après le Lemme 6.6.2, on a $\mathrm{h}_{[T_1',h_1(u)]} = h_1 \circ \mathrm{h}_{[T_1,u]}$, et de même, $\mathrm{h}_{[T_2',h_2(v)]} = h_2 \circ \mathrm{h}_{[T_2,v]}$. On a donc :

$$\begin{aligned}
\mathrm{h}^{T_1'}_{[h_1(u)\to h_2(v)]} &= \mathrm{h}_{[T_2',h_2(v)]} \circ \mathrm{h}^{-1}_{[T_1',h_1(u)]} \\
&= (h_2 \circ \mathrm{h}_{[v,T_2]}) \circ (h_1 \circ \mathrm{h}_{[u,T_1]})^{-1} \\
&= h_2 \circ \mathrm{h}_{[T_2,v]} \circ \mathrm{h}^{-1}_{[T_1,u]} \circ h_1^{-1} \\
&= h_2 \circ \mathrm{h}^{T_1}_{[u\to v]} \circ h_1^{-1}.
\end{aligned}$$

∎

Lemme 6.6.15 *Soient T et T' deux* GA*-termes stratifiés de racines respectives r et r', ces deux racines étant étiquetées par le même symbole de Σ_E. S'il existe une permutation $\sigma \in \mathcal{G}_T$ et un isomorphisme η de T^σ vers T', alors pour tout sommet u élément de $\overline{\mathrm{R}}_T(r) \cup \mathrm{R}_T(r)$, on a $\mathrm{h}^T_{[r\to r']}(u) = \eta(u^\sigma)$.*

PREUVE. Supposons que r et r' sont étiquetés par $\langle f, c, G\rangle$. Comme tous les sommets de $\overline{\mathrm{R}}_T(r)$ sont fixés par σ, on commence par prouver par induction que pour tout sommet w de $\overline{\mathrm{R}}_T(r)$, on a $\mathrm{h}^T_{[r\to r']}(w) = \eta(w)$. Ceci est évident pour $w = r$, supposons maintenant que le résultat est vrai pour un sommet $v \in \overline{\mathrm{R}}_T(r)$. On a alors :

$$\begin{aligned}
\mathrm{h}^T_{[r\to r']}(a_T(v)) &= \mathrm{h}_{[T',r']}(\,\mathrm{h}^{-1}_{[T,r]}(a_T(v))\,)\\
&= \mathrm{h}_{[T',r']}(\,a_c(\,\mathrm{h}^{-1}_{[T,r]}(v)\,)\,)\\
&= a_{T'}(\,\mathrm{h}_{[T',r']}(\,\mathrm{h}^{-1}_{[T,r]}(v)\,)\,)\\
&= a_{T'}(\,\eta(v)\,) \quad \text{(par hypothèse d'induction)}\\
&= \eta(\,a^\sigma_T(v)\,).
\end{aligned}$$

Ainsi, pour tout sommet u de la liste $a_T(v)$, si u est élément de $\overline{\mathrm{R}}_T(r)$, alors nécessairement, $u^\sigma = u$, et donc $\mathrm{h}^T_{[r\to r']}(u) = \eta(u^\sigma) = \eta(u)$, ce qui complète l'induction.

Pour tout $u \in \mathrm{R}_T(r)$, il existe un sommet v dans $\overline{\mathrm{R}}_T(r)$ tel que u est un élément de la liste $a_T(v)$. On a vu que $\mathrm{h}^T_{[r\to r']}(a_T(v)) = \eta(a_T(v)^\sigma)$, et donc, $\mathrm{h}^T_{[r\to r']}(u) = \eta(u^\sigma)$. ∎

Lemme 6.6.16 *Soient $A = (V, s, a)$ et $A' = (V', s', a')$ deux* A*-termes stratifiés de racines respectives r et r', toutes deux étiquetées par un même symbole de Σ_E, et supposons qu'il existe une fonction $\eta : V \to V'$ telle que :*

1. *la restriction de η à $\overline{\mathrm{R}}_A(r) \cup \mathrm{R}_A(r)$ est égale à $\mathrm{h}_{[r\to r']}$,*
2. *pour tout sommet $v \in \mathrm{R}_A(r)$, la restriction de η à $V|v$ est un isomorphisme de $A|v$ vers $A|\eta(v)$.*

Alors η est un isomorphisme de A vers A'.

PREUVE. Il est évident que η est bijective, et comme tout A-terme stratifié est clos, d'après le Lemme 5.2.8, il suffit de prouver que η est un homomorphisme. Clairement, pour tout sommet v de A, v et $\eta(v)$ sont étiquetés par le même symbole, d'après le Lemme 5.2.13, il suffit donc de prouver que si p est un chemin de r à u dans A, alors $\eta(p)$ est un chemin de r' à $\eta(u)$ dans A'.

Si $u \in \overline{\mathrm{R}}_A(r) \cup \mathrm{R}_A(r)$, alors le résultat se démontre par induction sur la longueur du chemin p de r à u dans A. On pose $p = p_1.v.i$, alors par hypothèse d'induction, $\eta(p_1)$ est un chemin de r' à $\eta(v)$ dans A', et comme $u = a(v)_i$, d'après la Propriété 6.6.13, on a

$$\eta(u) \;=\; \mathrm{h}_{[r\to r']}(u) \;=\; \mathrm{h}_{[r\to r']}(a(v)_i) \;=\; a'(\mathrm{h}_{[r\to r']}(v))_i \;=\; a'(\eta(v))_i.$$

Donc, $\eta(p)$ est bien un chemin de r' à $\eta(u)$ dans A'.

Supposons maintenant qu'il existe un sommet $v \in \mathrm{R}_A(r)$ tel que $u <_A v$. On note alors p_1 le chemin de r à v dans A, et p_2 le chemin de v à u dans A ; on a donc $p = p_1.p_2$.

D'après ce qui précède, $\eta(p_1)$ est un chemin de r' à $\eta(v)$ dans A', et $\eta(p_2)$ est un chemin de $\eta(v)$ à $\eta(u)$ dans A' d'après le Lemme 5.2.12. Donc, $\eta(p_1).\eta(p_2) = \eta(p)$ est bien un chemin de r' à $\eta(u)$ dans A', ce qui prouve le résultat. ∎

6.7 Commentaires

Dans ce chapitre, nous avons appliqué les résultats du Chapitre 5 sur les partitions stratifiées et les actions de groupes qui peuvent en être induites pour redéfinir la réécriture stratifiée de [AP01] en termes d'action de groupe. Nous avons commencé par montrer comment associer une permutation à une équation permutative, ce qui nous a permis de définir les signatures stratifiées, grâce auxquelles nous avons défini les GA-termes stratifiés. Etant donnés un GA-terme stratifié T sur une signature Σ et une signature stratifiée Σ_E, nous avons associé à T un groupe de permutations $\mathcal{G}_T$ dont l'action est bien définie, et nous avons démontré que l'image par la fonction $\tau \circ \mathrm{dm}$ de l'orbite de T sous cette action correspond exactement à l'ensemble $\mathrm{S}[T]$ défini dans [AP01].

On pourrait se demander s'il était nécessaire d'avoir recours à des notions de réécriture de graphes, et s'il n'était pas possible de créer une action de groupe simple sur des termes usuels qui permettrait d'obtenir ces résultats. Voyons maintenant pourquoi ce n'est pas le cas.

Par construction, pour un terme t donné, si $c = \mathrm{arbre}(t)$ et $\langle f, c, G\rangle$ est élément d'une signature stratifiée Σ_E, alors G est un sous-groupe de l'ensemble des positions des variables dans t. Il est alors possible de définir une action "naturelle" de G sur l'ensemble des instances de t en posant, pour une instance t' de t donnée, $t'^{\sigma}|p = t'|p^{\sigma}$, pour tout $\sigma \in G$, et pour toute position p d'une variable dans t. Par exemple, partant de l'équation permutative $f(g(x,y),z) \rightleftharpoons f(g(z,y),x)$, si $t' = f(g(a,b),h(d))$ et $\sigma = (1.1\ 2)$, alors

$$\begin{array}{lllll} t'^{\sigma}|1.1 & = & t'|2 & = & h(d), \\ t'^{\sigma}|1.2 & = & t'|1.2 & = & b, \\ t'^{\sigma}|2 & = & t'|1.1 & = & a, \end{array}$$

d'où $t'^{\sigma} = f(g(h(d),b),a)$. La notion de *groupe de permutations de sous-termes* de [AP01] et la relation de réécriture qui lui est associée correspondent exactement à cette action.

La raison pour laquelle nous avons choisi d'adapter la notion de réécriture stratifiée de [AP01] aux graphes étiquetés est que cette action ne s'étend pas naturellement aux termes stratifiés, comme le montre l'exemple suivant.

Exemple 6.7.1 Soit E la théorie permutative définie par l'axiome de commutativité $f(x,y) \rightleftharpoons f(y,x)$, et soit $t = f(a, f(b,d))$. Le sous-groupe de $\mathrm{Sym}(\mathrm{Pos}(t))$ qu'il faudrait raisonnablement associer à t est $G_t = \mathrm{Sym}(\{1,2\})\mathrm{Sym}(\{2.1, 2.2\})$, et il est possible d'associer à chaque permutation de ce groupe un terme égal à t modulo E ; par exemple, si $\sigma = (1\ 2)(2.1\ 2.2)$, alors on peut définir $t^{\sigma} = f(f(d,b),a)$. Malheureusement, ceci ne permet pas de définir une action de groupe naturelle, puisque G_t n'est pas un sous-groupe de $\mathrm{Sym}(\mathrm{Pos}(t^{\sigma}))$.

Ainsi, la façon de définir une action sur des termes stratifiés et d'associer un groupe à un terme stratifié n'est pas claire. L'action de groupe que nous avons définie sur les GA-termes est quant à elle très simple, le groupe de permutations associé à un GA-terme stratifié est assez intuitif, et permet de représenter la relation de réécriture stratifiée d'après le Théorème 6.5.13.

Ceci n'est pas qu'un résultat théorique intéressant, il sera utile dans les chapitres suivants. Ce résultat induit trivialement un certain nombre d'autres résultats de [AP01] (et les traduit en résultats sur les GA-termes), comme la confluence de la réécriture stratifiée, ou la cardinalité finie des ensembles stratifiés de termes.

Le fait que l'action de $\mathcal{G}_T$ sur T soit semi-régulière (Théorème 5.4.12) montre que la cardinalité de $[T]_{\mathrm{s}}$ est égale à l'ordre de $\mathcal{G}_T$. Si ce groupe n'est pas trivial, alors $[T]_{\mathrm{s}}$ contient au moins deux éléments qui se réécrivent mutuellement l'un en l'autre. Donc, la réécriture stratifiée sur des GA-termes ne termine pas.

Troisième partie

Propriétés des GA-termes stratifiés

Chapitre 7

Congruence stratifiée

Dans le chapitre précédent, nous avons défini les GA-termes stratifiés et prouvé qu'étant donné un GA-terme stratifié T, les ensembles $[T]_{\mathrm{s}}$ et $T^{\mathcal{G}_T}$ sont identiques. Puis nous avons démontré plusieurs propriétés vérifiées par ces GA-termes stratifiés. Dans ce chapitre, nous allons définir une relation d'équivalence entre GA-termes stratifiés, la relation de *congruence stratifiée*, et nous présenterons un algorithme qui décide si deux GA-termes stratifiés sont liés par cette relation. Puis, nous étudierons la complexité de ce problème de décision, et enfin, nous montrerons que la relation de congruence stratifiée permet d'obtenir une formule simple pour calculer la cardinalité de la partition $[T]_{\mathrm{s}}/\stackrel{\circ}{=}$.

7.1 Une relation d'équivalence

Définition 7.1.1 (Congruence stratifiée) Deux GA-termes stratifiés T et T' sont dits *congrus* si et seulement s'il existe une permutation $\sigma \in \mathcal{G}_T$ telle que T^σ et T' sont bisimilaires. On note alors $T \bowtie T'$.

Etant donné un GA-terme stratifié T, deux sommets u et v de T sont dits *congrus* si et seulement si $T|u$ et $T|v$ sont congrus. On note alors $u \approx_T v$, ou simplement $u \approx v$ si aucune confusion n'est possible. ◇

Exemple 7.1.2 Soient c et c' deux contextes tels que $\tau(c) = f(\circ, \circ, \circ)$, et $\tau(c') = h(\circ, \circ)$, et posons $G = \mathrm{Sym}(3)$, et $G' = \mathrm{Sym}(2)$. On note $F = \langle f, c, \mathcal{G}\rangle$ et $H = \langle h, c', \mathcal{G}'\rangle$.

Soit $A = (V, s, a)$ le A-terme de la Figure 7.1, on a donc

$$\tau(A) = F(H(a, b), H(a, b), H(b, a)).$$

Il est aisé de vérifier que $V_{\mathrm{s}} = \{\varepsilon, 1, 2, 3\}$, et que :

$$\begin{aligned}
\mathcal{G}_A(\varepsilon) &= \mathrm{Sym}(3) \\
\mathcal{G}_A(1) &= \mathrm{Sym}(\{1.1, 1.2\}) \\
\mathcal{G}_A(2) &= \mathrm{Sym}(\{2.1, 2.2\}) \\
\mathcal{G}_A(3) &= \mathrm{Sym}(\{3.1, 3.2\}).
\end{aligned}$$

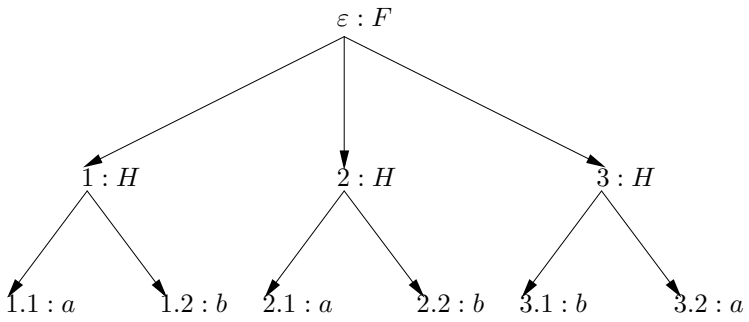

FIG. 7.1 – A-terme de l'Exemple 7.1.2

Pour tout GA-terme stratifié T tel que $\tau(T) = F(H(b,a), H(b,a), H(b,a))$, alors $A \bowtie T$. En effet, la permutation $\sigma = (1.1\ 1.2)(2.1\ 2.2)$ est élément de $\mathcal{G}_A$, et $\tau(A^\sigma) = \tau(T)$, donc A^σ et T sont bisimilaires.

Exemple 7.1.3 Soient $F = \langle f, c, G\rangle$, et $\Sigma_E = \{F\}$, où

$$\tau(c) = f(g(\circ,\circ),\circ), \text{ et } G = \mathrm{Sym}(\{1.2, 2\}).$$

Considérons le A-terme stratifié A de la Figure 7.2 ; on a donc

$$\tau(A) \ = \ f(F(g(a,d),b), F(g(a,b),d)).$$

On a $\mathcal{G}_{A|\mathfrak{a}} = \mathrm{Sym}(\{\mathfrak{c}, \mathfrak{e}\})$, et si on pose $\sigma = (\mathfrak{c}\ \mathfrak{e})$, alors $(A|\mathfrak{a})^\sigma \stackrel{\circ}{=} A|\mathfrak{a}'$, ce qui prouve que $\mathfrak{a} \approx_A \mathfrak{a}'$. Par contre $\mathcal{G}_{A|\mathfrak{b}} = \mathrm{I}$, et donc, $\mathfrak{b} \not\approx_A \mathfrak{b}'$.

σ est également élément de $\mathcal{G}_A$, et donc, A^σ est bien défini, et on a

$$\tau(A^\sigma) \ = \ f(F(g(a,b),d), F(g(a,b),d)).$$

On a donc $\mathfrak{a} \approx_{A^\sigma} \mathfrak{a}'$, et $\mathfrak{b} \approx_{A^\sigma} \mathfrak{b}'$. Ceci montre donc que la congruence des sommets de A n'est pas préservée par l'action de $\mathcal{G}_A$.

On a une première propriété évidente :

Propriété 7.1.4 *Soient T, T' deux* GA*-termes stratifiés tels que $T \bowtie T'$, alors $\tau(\mathrm{dm}(T))$ et $\tau(\mathrm{dm}(T'))$ sont congrus modulo E.*

PREUVE. Soit $\sigma \in \mathcal{G}_T$ la permutation telle que $T^\sigma \stackrel{\circ}{=} T'$, alors on a $\tau(\mathrm{dm}(T^\sigma)) = \tau(\mathrm{dm}(T'))$, et d'après le Corollaire 6.5.12, on a le résultat. ∎

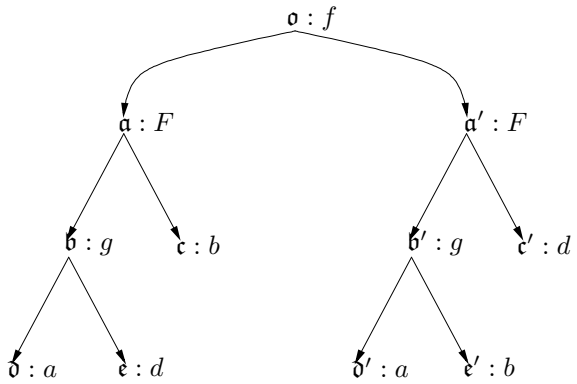

FIG. 7.2 – A-terme stratifié A de l'Exemple 7.1.3

Lemme 7.1.5 *Soient T et T' deux* GA*-termes stratifiés, et A et A' deux* A*-termes tels que $T \Subset A$ et $T' \Subset A'$. Alors*

$$(T \bowtie T') \Leftrightarrow (A \bowtie A').$$

PREUVE. Soient h et h' les homomorphismes respectivement de A vers T et de A' vers T', et supposons que $T \bowtie T'$. Alors il existe une permutation $\sigma \in \mathcal{G}_T$ telle que $T^\sigma \mathrel{\mathring{=}} T'$, et d'après le Corollaire 6.6.8, il existe une permutation $\mu \in \mathcal{G}_A$ telle que $\sigma = \mu^h$. D'après le Théorème 6.6.9, h est donc un homomorphisme de A^μ vers T^σ, et d'après le Corollaire 5.2.7, on a $A^\mu \mathrel{\mathring{=}} T^\sigma$, et $A' \mathrel{\mathring{=}} T'$. On a donc

$$A^\mu \mathrel{\mathring{=}} T^\sigma \mathrel{\mathring{=}} T' \mathrel{\mathring{=}} A',$$

et par transitivité de la relation $\mathrel{\mathring{=}}$, on en déduit que $A \bowtie A'$. Le même raisonnement prouve que si $A \bowtie A'$, alors $T \bowtie T'$, d'où le résultat. ∎

Nous prouvons maintenant que la relation de congruence stratifiée est une relation d'équivalence sur l'ensemble des A-termes stratifiés, puis nous prouverons que c'est également une relation d'équivalence sur l'ensemble des GA-termes stratifiés.

Lemme 7.1.6 *La relation de congruence stratifiée est une relation d'équivalence sur l'ensemble des* A*-termes stratifiés.*

PREUVE. La preuve que la relation est réflexive est triviale, il s'agit donc de montrer qu'elle est également symétrique et transitive. Soient A_1 et A_2 deux A-termes stratifiés, et supposons qu'il existe une permutation $\sigma \in \mathcal{G}_{A_1}$ telle que $A_1^\sigma \mathrel{\mathring{=}} A_2$. D'après le Corollaire 5.2.18, il existe donc un isomorphisme η de A_1^σ vers A_2. D'après le Corollaire 6.6.8, le conjugué π de σ^{-1} par η est élément de $\mathcal{G}_{A_2}$, et d'après le Théorème 6.6.9, η est un

isomorphisme de $A_1^{\sigma\sigma^{-1}} = A_1$ vers A_2^{π}. La fonction η^{-1} est donc un isomorphisme de A_2^{π} vers A_1, d'où $A_2 \bowtie A_1$.

Montrons maintenant que $\bowtie$ est une relation transitive. On prend A_1, A_2, σ et η comme précédemment, et un troisième A-terme A_3 tel que $A_2 \bowtie A_3$. Il existe donc une permutation $\pi \in \mathcal{G}_{A_2}$ et un isomorphisme η' de A_2^{π} vers A_3. Soit ρ le conjugué de π par η^{-1}. D'après le Corollaire 6.6.8 et le Théorème 6.6.9, ρ est élément de $\mathcal{G}_{A_1}$, et η^{-1} est un isomorphisme de A_2^{π} vers $A_1^{\sigma\rho}$. On en déduit que η est un isomorphisme de $A_1^{\sigma\rho}$ vers A_2^{π}, et que $\eta' \circ \eta$ est un isomorphisme de $A_1^{\sigma\rho}$ vers A_3. On a bien $A_1 \bowtie A_3$, ce qui prouve que $\bowtie$ est une relation d'équivalence sur les A-termes stratifiés. ∎

Théorème 7.1.7 *La relation de congruence stratifiée est une relation d'équivalence sur l'ensemble des* GA*-termes stratifiés, et la relation $\approx$ est une relation d'équivalence sur l'ensemble des sommets d'un* GA*-terme stratifié.*

PREUVE. La preuve que la relation est réflexive est triviale, et il s'agit donc de montrer qu'elle est également symétrique et transitive. Soient T et T' deux GA-termes stratifiés, et A et A' deux A-termes stratifiés tels que $T \Subset A$, et $T' \Subset A$. Alors, d'après le Lemme 7.1.5 puis le Lemme 7.1.6, on a :

$$(T \bowtie T') \;\Rightarrow\; (A \bowtie A') \;\Rightarrow (A' \bowtie A) \;\Rightarrow (T' \bowtie T),$$

la relation est donc symétrique.

Pour démontrer que la relation est transitive, supposons une fois de plus que $T \bowtie T'$, et soit T'' un GA-terme stratifié tel que $T' \bowtie T''$; il s'agit de prouver que $T \bowtie T''$. Soit A'' un A-terme stratifié tel que $T'' \Subset A''$. Alors, d'après le Lemme 7.1.5, on a $A \bowtie A'$ et $A' \bowtie A''$; d'après le Lemme 7.1.6, on en déduit que $A \bowtie A''$, et d'après le Lemme 7.1.5, que $T \bowtie T''$. ∎

Le Théorème 7.1.7 permet de définir un groupe de permutation basé sur les classes d'équivalence modulo $\approx$ dans un GA-terme stratifié.

Définition 7.1.8 ($\mathbf{E_T(u)}$) Soit $T = (V, s, a)$ un GA-terme stratifié, et u un élément de V_{s}. On pose $U = \mathrm{R}_T(u)$, l'ensemble quotient $U/\approx_T$ est donc une partition de U. On définit le groupe $\mathrm{E}_T(u) = \mathrm{Sym}_U(U/\approx_T)$. ◇

Exemple 7.1.9 Posons $H = \langle h, c, G\rangle$, où $\tau(c) = h(\circ, \circ, \circ, \circ, \circ)$, et G est un sous-groupe de $\mathrm{Sym}(\mathcal{SV}(c))$, et soit $\Sigma_E = \{H\}$. Soit T le GA-terme stratifié de la Figure 7.3, alors la partition $R = \mathrm{R}_T(\mathfrak{r})/\approx$ est définie par :

$$R \;=\; \{\{\mathfrak{a}, \mathfrak{b}, \mathfrak{d}\}, \{\mathfrak{c}, \mathfrak{e}\}\},$$

et donc $\mathrm{E}_T(\mathfrak{r}) = \mathrm{Sym}(\{\mathfrak{a}, \mathfrak{b}, \mathfrak{d}\})\mathrm{Sym}(\{\mathfrak{c}, \mathfrak{e}\})$.

Une conséquence importante du Théorème 7.1.7 est que deux GA-termes congrus ont des ensembles stratifiés identiques.

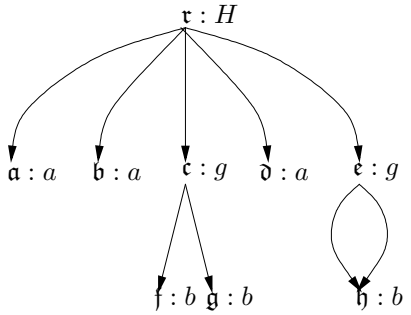

FIG. 7.3 – GA-terme de l'Exemple 7.1.9

Corollaire 7.1.10 *Si A et A' sont deux* A*-termes stratifiés congrus, alors on a* $\mathrm{S}[A] = \mathrm{S}[A']$.

PREUVE. A et A' étant congrus, il existe une permutation $\sigma \in \mathcal{G}_A$ et un isomorphisme η de A^σ vers A'. Etant donnée une permutation $\pi \in \mathcal{G}_A$, soit ρ le conjugué de $\sigma^{-1}\pi$ par η. D'après le Théorème 6.6.9, η est un isomorphisme de $A^{\sigma\sigma^{-1}\pi} = A^\pi$ vers A'^ρ, et ρ est élément de $\mathcal{G}_{A'}$. Les A-termes A^π et A'^ρ sont donc bisimilaires, et d'après la Propriété 6.2.10, $\tau(\mathrm{dm}(A^\pi)) = \tau(\mathrm{dm}(A'^\rho))$ est élément de $\mathrm{S}[A']$. Ceci prouve que $\mathrm{S}[A] \subseteq \mathrm{S}[A']$; on en déduit que $\mathrm{S}[A] = \mathrm{S}[A']$ par symétrie. ∎

Corollaire 7.1.11 *Deux* GA*-termes stratifiés congrus ont les mêmes ensembles stratifiés.*

PREUVE. Soient T et T' deux GA-termes stratifiés congrus, et A et A' deux A-termes stratifiés tels que $T \Subset A$ et $T' \Subset A'$. Alors, d'après le Lemme 7.1.5, A et A' sont congrus, donc, d'après le Corollaire 7.1.10, $\mathrm{S}[A] = \mathrm{S}[A']$. D'après le Corollaire 6.6.11, $\mathrm{S}[T] = \mathrm{S}[A]$ et $\mathrm{S}[T'] = \mathrm{S}[A']$, et on a le résultat. ∎

Nous prouvons également que deux GA-termes congrus ont la même hauteur stratifiée :

Théorème 7.1.12 *Soient T et T' deux* GA*-termes stratifiés tels que $T \bowtie T'$, alors T et T' ont la même hauteur stratifiée.*

PREUVE. Soient A et A' deux A-termes stratifiés tels que $h(A) = T$ et $h'(A') = T'$, pour deux homomorphismes h et h'. Puisque $T \bowtie T'$, alors $A \bowtie A'$ d'après le Lemme 7.1.5. Il existe donc une permutation $\sigma \in \mathcal{G}_A$ telle que $A^\sigma \simeq A'$, et donc, on a d'après le Corollaire 6.6.3 et le Lemme 6.5.7 :

$$\lfloor A' \rfloor \;=\; \lfloor A^\sigma \rfloor \;=\; \lfloor A \rfloor.$$

Comme $\lfloor T \rfloor = \lfloor A \rfloor$ et $\lfloor T' \rfloor = \lfloor A' \rfloor$ d'après le Corollaire 6.6.3, on a le résultat. ∎

Prouvons maintenant une propriété de décomposition vérifiée par la relation de congruence stratifiée.

Lemme 7.1.13 *Soient T et T' deux* GA*-termes stratifiés de racines respectives r et r', toutes deux étiquetées par le symbole $\langle f, c, G\rangle \in \Sigma_E$. Si $T \bowtie T'$, alors il existe une permutation $\sigma \in G$ telle que pour tout $w \in \mathcal{SV}(c)$, $T|\mathrm{h}_{[T,r]}(w^\sigma) \bowtie T'|\mathrm{h}_{[T',r']}(w)$.*

PREUVE. Comme $T \bowtie T'$, il existe une permutation $\mu \in \mathcal{G}_T$ telle que $T^\mu \mathrel{\mathring{=}} T'$. Posons $h = \mathrm{h}_{[T,r]}$, $h' = \mathrm{h}_{[T',r']}$, et $h'' = \mathrm{h}_{[T^\mu,r]}$, alors h'' et h' sont respectivement des homomorphismes de c vers $\mathrm{dm_r}(T^\mu)$ et de c vers $\mathrm{dm_r}(T')$. D'après le Lemme 5.2.11, on a donc :

$$\forall w \in \mathcal{SV}(c),\ T^\mu|h''(w) \mathrel{\mathring{=}} T'|h'(w).$$

Soit $\sigma \in G$ la permutation telle que la restriction μ_r de μ à $\mathrm{R}_T(r)$ soit égale à $\sigma^{\mathrm{h}_{[T,r]}}$, alors d'après le Corollaire 6.4.7, on a

$$h''(w) \ = \ \mathrm{h}_{[T^\mu,r]}(w) \ = \ \mu_r \circ \mathrm{h}_{[T,r]}(w) \ = \ \mathrm{h}_{[T,r]}(w^\sigma) \ = \ h(w^\sigma),$$

d'où $T^\mu|h(w^\sigma) \mathrel{\mathring{=}} T'|h'(w)$. Pour $w \in \mathcal{SV}(c)$, si on note μ' la restriction de μ à $T|h(w^\sigma)$, alors d'après la Propriété 6.5.5, on a $T^\mu|h(w^\sigma) = (T|h(w^\sigma))^{\mu'}$, et comme μ' est élément de $\mathcal{G}_{T|h(w^\sigma)}$, on a bien $T|h(w^\sigma) \bowtie h'(w)$. ∎

Corollaire 7.1.14 *Soit T un* GA*-terme stratifié contenant deux sommets v, v', tous deux étiquetés par un symbole $\langle f, c, G\rangle \in \Sigma_E$, et tels que $v \approx v'$. Alors il existe une permutation $\rho \in \mathcal{G}_T(v)$ telle que pour tout sommet $u \in \mathrm{R}_T(v)$, $u^\rho \approx \mathrm{h}_{[v\to v']}(u)$.*

PREUVE. Par définition, comme $v \approx v'$, alors $T|v \bowtie T|v'$, et donc, d'après le Lemme 7.1.13, il existe une permutation $\sigma \in G$ telle que pour tout sommet $w \in \mathcal{SV}(c)$, $T|\mathrm{h}_{[T,v]}(w^\sigma) \bowtie T|\mathrm{h}_{[T,v']}(w)$. Posons $\rho = \sigma^{\mathrm{h}_{[T,v]}}$, par définition, si $u = \mathrm{h}_{[T,v]}(w)$, alors $u^\rho = \mathrm{h}_{[T,v]}(w^\sigma)$, et $\mathrm{h}_{[v\to v']}(u) = \mathrm{h}_{[T,v']}(w)$, ce qui prouve que $T|u^\rho \bowtie T|\mathrm{h}_{[v\to v']}(u)$, d'où le résultat. ∎

Nous avons également une réciproque à cette propriété :

Lemme 7.1.15 *Soient $A = (V, s, a)$ et $A' = (V', s', a')$ deux* A*-termes stratifiés de racines respectives r et r', toutes deux étiquetées par $\langle f, c, G\rangle \in \Sigma_E$. Si pour tout sommet $v \in \mathrm{R}_A(r)$, on a $A|v \bowtie A'|\mathrm{h}^A_{[r\to r']}(v)$, alors $A \bowtie A'$.*

PREUVE. Pour $v \in \mathrm{R}_A(r)$, on pose $v' = \mathrm{h}^A_{[r\to r']}(v)$, et soient $\sigma_v \in \mathcal{G}_{A|v}$ et η_v l'isomorphisme de $(A|v)^{\sigma_v}$ vers $A'|v'$. On définit alors

$$\sigma \ = \ \prod_{v\in \mathrm{R}_A(r)} \sigma_v, \text{ et } \eta = \mathrm{h}^A_{[r\to r']} \cup \biguplus_{v\in \mathrm{R}_A(r)} \eta_v.$$

Montrons que η est un isomorphisme de A^σ vers A'. Comme $\eta_v(v) = \mathrm{h}^A_{[r\to r']}(v)$, la fonction η est bien définie. De plus, σ fixe tous les sommets de $\mathrm{R}_A(r)$, et la restriction de σ à $\mathrm{R}_A(r)$ est donc l'identité. D'après le Corollaire 6.4.7, on a donc $\mathrm{h}_{[A^\sigma,r]} = \mathrm{h}_{[A,r]}$, d'où $\mathrm{h}^A_{[r\to r']} = \mathrm{h}^{A^\sigma}_{[r\to r']}$. Comme la fonction $\mathrm{h}^{A^\sigma}_{[r\to r']} \cup \biguplus \eta_v$ vérifie les hypothèses du Lemme 6.6.16, on en déduit que η est bien un isomorphisme de A^σ vers A, ce qui signifie que $A \bowtie A'$. ∎

Corollaire 7.1.16 *Soient T et T' deux* GA*-termes stratifiés de racines respectives r et r' toutes deux étiquetées par le même symbole de Σ_E, et supposons que pour tout $v \in \mathrm{R}_T(r)$, on a $T|v \bowtie T'|\mathrm{h}^T_{[r\to r']}(v)$. Alors $T \bowtie T'$.*

PREUVE. Soient A et A' deux A-termes de racines respectives r_1 et r_2, tels que $T \Subset A$ et $T' \Subset A'$. On note h (resp. h') l'homomorphisme de A (resp. A') vers T (resp. T'). Soit $v \in \mathrm{R}_T(r)$, alors, d'après le Corollaire 6.6.5, il existe un unique $w \in \mathrm{R}_A(r_1)$ tel que $h(w) = v$, et d'après la Propriété 5.2.5, (une restriction de) h est un homomorphisme de $A|w$ vers $T|v$. De plus, d'après le Lemme 6.6.14, on a

$$\mathrm{h}^T_{[r\to r']} \;=\; h' \circ \mathrm{h}^A_{[r_1\to r_2]} \circ h^{-1},$$

et donc, si $v' = \mathrm{h}^T_{[r\to r']}(v)$, alors $v' = h'(\mathrm{h}^A_{[r_1\to r_2]}(w))$. Posons $w' = \mathrm{h}^A_{[r_1\to r_2]}(w)$, alors (une restriction de) h' est un homomorphisme de $A'|w'$ vers $T|v'$.

Comme $T|v \bowtie T'|v'$, d'après le Lemme 7.1.5, on en déduit que $A|w \bowtie A'|w'$. Le Lemme 7.1.15 prouve alors que $A \bowtie A'$, et le Lemme 7.1.5, que $T \bowtie T'$. ■

Corollaire 7.1.17 *Soient T et T' deux* GA*-termes stratifiés de racines respectives r et r' toutes deux étiquetées par le même symbole de Σ_E, et supposons qu'il existe une permutation $\sigma \in \mathcal{G}_T(r)$ telle que pour tout $u \in \mathrm{R}_T(r)$, $T|u^\sigma \bowtie T'|\mathrm{h}^T_{[r\to r']}(u)$. Alors $T \bowtie T'$.*

PREUVE. Comme $\sigma \in \mathcal{G}_T(r)$, σ est également élément de $\mathcal{G}_T$, et on a, pour tout $u \in \mathrm{R}_T(r)$, $T|u^\sigma = T^\sigma|u^\sigma$. De plus, d'après le Corollaire 6.4.7, on a

$$\mathrm{h}^{T^\sigma}_{[r\to r']}(u^\sigma) = \mathrm{h}_{[T',r']} \circ \mathrm{h}^{-1}_{[T^\sigma,r]}(u^\sigma) \;=\; \mathrm{h}_{[T',r']} \circ \mathrm{h}^{-1}_{[T,r]} \circ \sigma^{-1}(u^\sigma) \;=\; \mathrm{h}^T_{[r\to r']}(u).$$

On en déduit que pour tout $u \in \mathrm{R}_T(r)$, on a $T^\sigma|u^\sigma \bowtie T'|\mathrm{h}^{T^\sigma}_{[r\to r']}(u^\sigma)$, et d'après le Corollaire 7.1.16, on a donc $T^\sigma \bowtie T'$. Comme $T \bowtie T^\sigma$, par transitivité, on a le résultat. ■

7.2 Calcul des ≈-classes

Dans cette partie, nous allons étudier comment déterminer les classes d'équivalences des sommets d'un GA-terme stratifié T modulo $\approx$. Une conséquence du Théorème 7.1.12 est que si deux sommets u et v d'un GA-terme stratifié T sont congrus, alors $\lfloor u \rfloor_T = \lfloor v \rfloor_T$; dans ce qui suit, nous supposerons que les sommets à comparer sont de même hauteur stratifiée. De plus, ces sommets ne peuvent évidemment pas être équivalents modulo $\approx$ s'ils sont étiquetés par des symboles différents, donc, par la suite, nous supposerons également que les sommets à comparer sont étiquetés par le même symbole. Nous effectuerons un parcours ascendant des sommets de T, et déterminerons si $u \approx v$ une fois que seront connues les $\approx$-classes d'équivalence des sommets en-dessous de u et de v dans T

Il y aura deux cas à considérer : le cas où u et v sont étiquetés par un élément de Σ, et le cas où u et v sont étiquetés par un élément de Σ_E. Le premier cas est le plus simple à étudier, et on a le lemme suivant :

Lemme 7.2.1 *Soit $T = (V, s, a)$ un* GA*-terme stratifié, et u et v deux sommets de T étiquetés par un même élément de Σ. Alors $u \approx v$ si et seulement si le $i^{ème}$ élément de $a(u)$ et le $i^{ème}$ élément de $a(v)$ sont équivalents modulo $\approx$, pour tout i compris entre 1 et arité(f).*

PREUVE. Posons $T_u = T|u$, $T_v = T|v$, et supposons que $u \approx v$, c'est-à-dire que $T_u \bowtie T_v$. Alors, par définition, il existe une permutation $\sigma \in \mathcal{G}_{T_u}$ telle que T_u^σ et T_v sont bisimilaires. Comme σ est élément de $\mathcal{G}_{T_u}$ et que $s(u) \in \Sigma$, si $a(u) = u_1.\cdots.u_n$, alors, pour tout $i \in \{1, \ldots, n\}$, on a

$$a^\sigma(u)_i \;=\; a(u)_i^\sigma \;=\; u_i^\sigma \;=\; u_i.$$

Posons $a(v) = v_1.\cdots.v_n$, alors pour tout $i = 1, \ldots, n$, on a $T^\sigma|u_i \mathrel{\dot{=}} T|v_i$. Pour $i \in \{1, \ldots, n\}$, notons σ_i la restriction de σ à $V|u_i$, alors d'après la Propriété 6.5.5, $T^\sigma|u_i = (T|u_i)^{\sigma_i}$, et comme σ_i est élément de $\mathcal{G}_{T|u_i}$, on en déduit que $T|u_i \bowtie T|v_i$, d'où $u_i \approx v_i$.

Réciproquement, si pour tout $i = 1, \ldots, n$, u_i et v_i sont congrus, alors il existe des permutations $\sigma_1, \ldots, \sigma_n$ telles que pour tout $i = 1, \ldots, n$, $\sigma_i \in \mathcal{G}_{T_u|u_i}$, et $(T_u|u_i)^{\sigma_i} \mathrel{\dot{=}} T_v|v_i$. La permutation $\sigma = \prod_{i=1,\ldots,n} \sigma_i$ est alors élément de $\mathcal{G}_{T_u}$, et il est aisé de vérifier que $T_u^\sigma \mathrel{\dot{=}} T_v$, d'où le résultat. ∎

Ainsi, quand u et v sont étiquetés par un symbole de Σ, il suffit de tester si les arguments de u et v sont deux à deux équivalents modulo $\approx$ pour décider si u et v sont eux aussi équivalents modulo $\approx$. Par contre, si le symbole qui les étiquette est dans Σ_E, il faut avoir recours à des notions plus complexes. Dans ce qui suit, nous allons montrer comment calculer la $\approx$-classe d'équivalence d'un sommet $u \in V_{\mathrm{s}}$, une fois que la relation $\approx$ est connue pour les éléments du résidu de $\mathrm{R}_T(u)$.

Théorème 7.2.2 *Soit $T = (V, s, a)$ un* GA*-terme stratifié, et r et r' deux éléments de V_{s} étiquetés par le même symbole de Σ_E. Alors :*

1. *$r \approx_T r'$ si et seulement s'il existe une permutation $\rho \in \mathrm{R}_T(r)$ telle que les conditions* (7.1) *et* (7.2) *ci-dessous sont vraies :*

$$\forall u \in \mathrm{R}_T(r),\ u^\rho \approx_T \mathrm{h}_{[r \to r']}(u), \tag{7.1}$$

$$\rho \mathrm{E}_T(r) \cap \mathcal{G}_T(r) \neq \emptyset. \tag{7.2}$$

2. *Si ρ et ρ' sont deux permutations de $\mathrm{R}_T(r)$ telles que $u^\rho \approx_T u^{\rho'}$ pour tout u de $\mathrm{R}_T(r)$, alors $\rho \mathrm{E}_T(r) = \rho' \mathrm{E}_T(r)$.*

PREUVE. 1. Supposons que $r \approx_T r'$, alors, d'après le Corollaire 7.1.14, il existe une permutation $\rho \in \mathcal{G}_T(r)$ telle que, pour tout $u \in \mathrm{R}_T(r)$, $u^\rho \approx_T \mathrm{h}_{[r \to r']} u$, et la condition (7.1) est donc vérifiée. Clairement, la permutation ρ est également dans $\rho \mathrm{E}_T(r)$, et donc, $\rho \in \rho \mathrm{E}_T(r) \cap \mathcal{G}_T(r)$, et cette intersection est non vide.

Réciproquement, supposons qu'il existe une permutation $\rho \in \mathrm{R}_T(r)$ telle que les conditions (7.1) et (7.2) soient vérifiées. Il existe donc une permutation $\mu \in \mathrm{E}_T(r)$ telle que $\rho\mu$ est élément $\mathcal{G}_T(r)$. Par définition de $\mathrm{E}_T(r)$, pour tout sommet $u \in \mathrm{R}_T(r)$, on a

$Test(u, v) =$
  // on suppose que $s(u) = s(v)$ *et* $\lfloor u \rfloor_T = \lfloor v \rfloor_T$
  si $s(u) \in \Sigma$ **alors**
    soit $u_1.\cdots.u_n = a(u)$ **et** $v_1.\cdots.v_n = a(v)$ **dans**
    // Lemme 7.2.1
    renvoyer $\forall i \in \{1, \ldots, n\},\ u_i \in v_i[\mathcal{P}]$
  sinon soient $I := \mathrm{R}_T(u)$ **et** $J := \mathrm{R}_T(v)$
    et $\sigma := \mathrm{id}$ **et** *existe* $:=$ *vrai* **dans**
    tant que *existe* **et** $I \neq \emptyset$ **faire**
      soit $w \in I$ **dans**
($\star$) **si** $\exists w' \in w[\mathcal{P}] \cap J$ **alors**
        $\sigma := (w\ w')\sigma\ ;\ I := I \setminus \{w\}\ ;\ J := J \setminus \{w'\}$
      sinon *existe* $:= faux$
    fin tant que;
    soit $\rho = \sigma \circ \mathrm{h}_{[u \to v]}$ **dans**
    // Théorème 7.2.2
    renvoyer *existe* $\wedge\ (\rho \mathrm{E}_T(u) \cap \mathcal{G}_T(u) \neq \emptyset)$

FIG. 7.4 – Algorithme $Test$

$u^{\rho\mu} \approx_T u^\rho$, et comme $u^\rho \approx_T \mathrm{h}_{[r \to r']}(u)$ par hypothèse, on en déduit que $u^{\rho\mu} \approx_T \mathrm{h}_{[r \to r']}(u)$ par transitivité. Enfin, en appliquant le Corollaire 7.1.17, on en déduit que $T|r \bowtie T|r'$, c'est-à-dire que $r \approx_T r'$.
2. Supposons que pour tout $u \in \mathrm{R}_T(r)$, on a $u^\rho \approx_T u^{\rho'}$. Alors, en particulier, $u = u^{\rho^{-1}\rho} \approx u^{\rho^{-1}\rho'}$ et, d'après la définition de $\mathrm{E}_T(r)$, on en déduit que $\rho^{-1}\rho' \in \mathrm{E}_T(r)$. Ceci signifie que ρ' est dans la classe à gauche $\rho \mathrm{E}_T(r)$, et donc que les deux classes à gauche $\rho \mathrm{E}_T(r)$ et $\rho' \mathrm{E}_T(r)$ sont égales. ∎

Le Lemme 7.2.1 et le Théorème 7.2.2 permettent de concevoir un algorithme qui décide si deux sommets u et v d'un GA-terme stratifié T sont dans la même ≈-classe. Un tel algorithme est décrit dans la Figure 7.4. La fonction $Test$ est appelée sur les sommets u et v s'ils sont étiquetés par le même symbole et ont la même hauteur stratifiée, puisque ce sont des conditions nécessaires de congruence de u et v. La partition $\mathcal{P}$ contient les ≈-classes de tous les sommets en-dessous de u et de v dans T.

Si u et v sont étiquetés par un symbole de Σ, alors, d'après le Lemme 7.2.1, $u \approx v$ si et seulement si pour tout $i \in \{1, n\}$, $u_i \approx v_i$, c'est-à-dire si et seulement si $u_i \in v_i[\mathcal{P}]$.

Si u et v sont étiquetés par un symbole de Σ_E, alors l'algorithme tente de construire un produit de transpositions *disjointes* σ qui associe à chaque $w \in \mathrm{R}_T(u)$ un sommet $w' \in \mathrm{R}_T(v)$ tel que $w' \approx w$. Si σ existe, alors par construction, $\rho = \sigma \circ \mathrm{h}_{[u \to v]}$ est un élément de $\mathrm{Sym}(\mathrm{R}_T(u))$ qui vérifie pour tout $w \in \mathrm{R}_T(u)$, $w^\rho = (\mathrm{h}_{[u \to v]}(w))^\sigma$. Comme $\mathrm{h}_{[u \to v]}(w) \approx \mathrm{h}_{[u \to v]}(w)^\sigma$ par hypothèse, on a donc $w^\rho \approx \mathrm{h}_{[u \to v]}(w)$ pour tout $w \in \mathrm{R}_T(u)$, et la condition (7.1) du Théorème 7.2.2 est bien vérifiée par ρ. Si $\rho \mathrm{E}_T(u) \cap \mathcal{G}_T(u) \neq \emptyset$, alors la condition (7.2) du Théorème 7.2.2 est elle aussi vérifiée par ρ, et on peut conclure

que $u \approx v$. Si la permutation σ n'existe pas ou si $\rho \mathrm{E}_T(u) \cap \mathcal{G}_T(u) = \emptyset$, alors on peut conclure que $u \not\approx v$.

Il est clair que la valeur de σ dépend du choix de w' à la ligne $(\star)$, mais ce choix n'a pas d'influence sur la valeur de $Test(u, v)$. En effet, l'existence de σ (et donc la valeur de *existe*) ne dépend pas de ce choix, puisque l'algorithme cherche à déterminer l'existence d'un produit de transpositions disjointes. Considérons un exemple.

Exemple 7.2.3 Soient $I = \{\mathfrak{a}, \mathfrak{b}, \mathfrak{c}\}$, $J = \{\mathfrak{a}', \mathfrak{b}', \mathfrak{c}'\}$, et $\mathcal{P} = \{\{\mathfrak{a}, \mathfrak{b}, \mathfrak{b}', \mathfrak{c}'\}, \{\mathfrak{c}, \mathfrak{a}'\}\}$. Au premier passage dans la boucle **tant que**, supposons que $w = \mathfrak{a}$, alors il y a deux choix pour w', $\mathfrak{b}'$ et $\mathfrak{c}'$. Supposons que $w' = \mathfrak{b}'$, alors on a $\sigma := (\mathfrak{a}\ \mathfrak{b}')$. Puis, au second passage dans la boucle, on a $w = \mathfrak{b}$, et $w' = \mathfrak{c}'$, d'où $\sigma := (\mathfrak{b}\ \mathfrak{c}')(\mathfrak{a}\ \mathfrak{b}')$. Enfin, au troisième passage, on a $w = \mathfrak{c}$, d'où $\sigma := (\mathfrak{c}\ \mathfrak{a}')(\mathfrak{b}\ \mathfrak{c}')(\mathfrak{a}\ \mathfrak{b}')$. Si au premier passage dans la boucle **tant que**, on avait $w' = \mathfrak{c}'$, alors l'algorithme aurait construit la permutation $(\mathfrak{c}\ \mathfrak{a}')(\mathfrak{b}\ \mathfrak{b}')(\mathfrak{a}\ \mathfrak{c}')$.

Supposons maintenant que $\mathcal{P} = \{\{\mathfrak{a}, \mathfrak{b}, \mathfrak{b}'\}, \{\mathfrak{c}, \mathfrak{a}', \mathfrak{c}'\}\}$. Alors au premier passage dans la boucle **tant que**, pour $w = \mathfrak{a}$, on a $w' = \mathfrak{b}'$, mais au deuxième passage dans la boucle, il n'y a aucun élément de J à associer à $\mathfrak{b}$, et la valeur de *existe* est instanciée à faux. On voit donc qu'on ne peut construire σ que si, pour toutes les classes $C \in \mathcal{P}$, on a $|C \cap I| = |C \cap J|$.

De plus, si σ et σ' sont deux permutations qui vérifient la propriété requise, alors, en posant $\rho = \sigma \circ \mathrm{h}_{[u \to v]}$ et $\rho' = \sigma' \circ \mathrm{h}_{[u \to v]}$, on a :

$$\forall w \in \mathrm{R}_T(u),\ w^{\rho} \ = \ \mathrm{h}_{[u \to v]}(w)^{\sigma} \ \approx \ \mathrm{h}_{[u \to v]}(w) \ \approx \ \mathrm{h}_{[u \to v]}(w)^{\sigma'} \ = \ w^{\rho'}.$$

D'après le Théorème 7.2.2 (2), on a donc $\rho \mathrm{E}_T(u) = \rho' \mathrm{E}_T(u)$, et la valeur de $Test(u, v)$ ne dépend donc pas du choix de w' à la ligne $(\star)$.

Nous donnons enfin dans la Figure 7.5 un algorithme qui, étant donné un GA-terme $T = (V, s, a)$, permet de calculer l'ensemble quotient $V/\!\approx$. Grâce à cet algorithme, nous pouvons donc décider si deux sommets de V sont dans la même $\approx$-classe.

7.3 Complexité du problème de décision

Dans cette partie, nous allons étudier la complexité du problème suivant :

> **Problème**: Congruence stratifiée, ou S_CONGR
> **Entrée**: Deux GA-termes stratifiés T et T'
> **Question**: Est-ce que $T \bowtie T'$?

Ce problème et la construction des classes d'équivalences des sommets d'un GA-terme stratifié modulo $\approx$ sont polynomialement équivalents. En effet, par définition, toute paire de sommets u et v d'un GA-terme T sont équivalents modulo $\approx$ si et seulement si $T|u \bowtie T|v$. Réciproquement, il est aisé de tester si deux GA-termes T et T' sont congrus en calculant les classes d'équivalence modulo $\approx$ d'un unique GA-terme stratifié. Il suffit pour cela de construire un GA-terme stratifié T'' dont la racine est étiquetée par un symbole de Σ d'arité 2 (qu'on peut ajouter à Σ si nécessaire), et dont les deux sommets

```
Equiv(T) =
  soit P = {{v} | v ∈ V} dans
  pour h = 1 à ⌊T⌋ faire
    soit V = {v ∈ V | ⌊v⌋_T = h} dans
    tant que V ≠ ∅ faire
      choisir w ∈ V ;
      soit U = {u ∈ V | s(u) = s(w)} dans
      V := V \ U ;
      pour ⟨u, v⟩ ∈ U² faire
        si u[P] ≠ v[P] et Test(u, v) alors
          fusionner u[P] et v[P] dans P
      fin pour
    fin tant que
  fin pour ;
  renvoyer P
```

FIG. 7.5 – Algorithme *Equiv*

arguments v et v' sont tels que $T''|v = T$ et $T''|v' = T'$. Après un appel à $Equiv(T'')$, on peut décider si T et T' sont congrus en vérifiant si v et v' sont dans la même $\approx$-classe d'équivalence.

La condition (7.2) du Théorème 7.2.2 est une instance du problème CIE. Supposons qu'on dispose de CIE pour oracle, alors clairement, les algorithmes $Test(u, v)$ et $Equiv(T)$ sont polynomiaux. Ceci signifie que le problème CIE pour oracle permet de tester en temps polynomial si deux sommets sont équivalents modulo $\approx$, et donc de tester si deux GA-termes sont liés par la relation $\bowtie$. On a donc le résultat suivant :

Théorème 7.3.1 *On a une réduction de Turing polynomiale de* S_CONGR *vers* CIE.

Comme CIE est dans la classe de Luks, on en déduit que

Corollaire 7.3.2 *Le problème* S_CONGR *est simple pour la classe de Luks.*

Nous montrons maintenant que ce problème est également difficile pour la classe de Luks. Pour cela, nous allons considérer le problème OP.

Dans ce qui suit, partant d'une instance de OP, nous allons construire deux A-termes particulièrement simples, et prouver qu'ils sont congrus si et seulement si l'instance de OP considérée a une solution.

Définition 7.3.3 Soit la signature $\Sigma = \{f, b, d\}$, où f est un symbole de fonction d'arité n, et b et d sont des constantes, et soit c un contexte tel que $\tau(c) = f(\circ, \ldots, \circ)$.

Soit $V = \{\varepsilon\} \cup \{1, \ldots, n\}$, et (x, y, G) une instance de OP. On prend alors la signature stratifiée $\Sigma_E = \{\langle f, c, G\rangle\}$, et on définit les A-termes $A = (V, s, a)$ et $A' = (V, s', a')$, tous deux de racine ε, par :

- $s(\varepsilon) = s'(\varepsilon) = \langle f, c, G\rangle$,
- $a(\varepsilon) = a'(\varepsilon) = 1.\cdots.n$,
- pour tout $i = 1, \ldots, n$, $s(i) = b$ si $x_i = 0$, et $s(i) = d$ sinon,
- pour tout $j = 1, \ldots, n$, $s'(j) = b$ si $y_j = 0$, et $s'(j) = d$ sinon. ◇

Les A-termes c, A et A' sont construits sur le même ensemble de sommets V, et il est aisé de vérifier que l'identité sur V est un homomorphisme de c vers $\mathrm{dm_r}(A)$, et de c vers $\mathrm{dm_r}(A')$; ces deux A-termes sont donc stratifiés, et on a

$$\mathrm{h}_{[A,\varepsilon]} \;=\; \mathrm{h}_{[A',\varepsilon]} \;=\; \mathrm{id}, \text{ et } \mathcal{G}_A \;=\; \mathcal{G}_{A'} \;=\; G.$$

Exemple 7.3.4 Prenons $n = 4$, $x = \langle 0, 0, 1, 1\rangle$, $y = \langle 1, 0, 0, 1\rangle$, et soit G un sous-groupe de Sym(4). On pose $F = \langle f, c, G\rangle$, alors

$$\tau(A) = F(b, b, d, d), \text{ et } \tau(A') = F(d, b, b, d).$$

Théorème 7.3.5 *A et A' sont congrus si et seulement s'il existe une permutation $\sigma \in G$ telle que pour tout i, $x_{i^\sigma} = y_i$.*

PREUVE. Supposons que A et A' sont congrus, il existe donc une permutation $\sigma \in \mathcal{G}_A = G$ telle que $A^\sigma \simeq A'$. Ceci signifie que, pour tout $i = 1, \ldots, n$, si w_i est le $i^{\text{ème}}$ argument de $a^\sigma(\varepsilon)$, alors $A^\sigma|w_i \simeq A'|i$. Or, w_i est l'image par σ du $i^{\text{ème}}$ argument de $a(\varepsilon)$, c'est-à-dire du sommet i, et comme $\mathrm{h}_{[A,\varepsilon]} = \mathrm{id}$, on a $w_i = i^\sigma$. On en déduit donc que $A^\sigma|i^\sigma$ et $A'|i$ sont isomorphes, et que leurs racines sont étiquetées par le même symbole. Enfin, comme $s(i^\sigma) = s'(i)$, on a nécessairement $x_{i^\sigma} = y_i$.

Réciproquement, supposons qu'il existe $\sigma \in G$ tel que pour tout i, $x_{i^\sigma} = y_i$. On définit alors $h' : V \to V$ par :

- $h'(\varepsilon) = \varepsilon$,
- pour tout $i = 1, \ldots, n$, $h'(i^\sigma) = i$.

Nous allons montrer que h' est un isomorphisme de A^σ vers A'. D'abord, il est évident que h' est une bijection. Comme $a^\sigma(\varepsilon) = 1^\sigma.\cdots.n^\sigma$, on a bien $a'(h(\varepsilon)) = h(a(\varepsilon))$, et enfin, pour tout $i = 1, \ldots, n$, comme $x_{i^\sigma} = y_i$, on a également $s(i^\sigma) = s'(i)$. La fonction h' est donc bien un isomorphisme, et on a $A \bowtie A'$. ■

Exemple 7.3.6 Dans la suite de l'Exemple 7.3.4, supposons que G est engendré par la permutation $\sigma = (1\ 2\ 3)$. On a alors

$$\mathrm{S}[A] \;=\; \{f(b, b, d, d), f(b, d, b, d), f(d, b, b, d)\}.$$

A et A' sont équivalents, puisque la permutation $\mu = \sigma^2 = (1\ 3\ 2)$ est élément de $\mathcal{G}_A = G$, et que :

$$\tau(A^\mu) \;=\; \tau(A') \;=\; F(d, b, b, d).$$

Corollaire 7.3.7 *On a une réduction de Turing polynomiale de* OP *vers le problème* S_CONGR.

PREUVE. Ce résultats est évident : la signature stratifiée Σ_E et les A-termes A et A' peuvent tous être construits en temps linéaire en la longueur du n-uplet x de l'instance de OP considérée, et le groupe $\mathcal{G}_A = \mathcal{G}_{A'}$ est engendré par le même ensemble de permutations que G. ■

Le Corollaire 7.3.7 prouve que le problème S_CONGR est également difficile pour la classe de Luks, et est donc un élément de cette classe :

Théorème 7.3.8 *Le problème* S_CONGR *est dans la classe de Luks.*

7.4 Résumé

Dans ce chapitre, nous avons étudié la relation de congruence stratifiée $\bowtie$, et démontré que c'est une relation d'équivalence. Puis nous avons étudié le problème de décision associé, et démontré qu'il est dans la classe de Luks. Plus tard, nous verrons que dans certaines classes de théories permutatives, le problème du mot généralisé modulo ces théories est polynomialement équivalent au problème de la congruence stratifiée.

Chapitre 8

Problèmes liés à la déduction

Dans les deux chapitres précédents, nous avons considéré des signatures stratifiées et des GA-termes stratifiés quelconques, sans imposer la moindre restriction. Or, il est évident qu'étant donnée une théorie permutative, il est possible de construire plusieurs signatures stratifiées, dont certaines se révéleraient inefficaces si elles étaient utilisées par un démonstrateur automatique. Par exemple, étant donnée une théorie permutative E définie par un ensemble d'axiomes, il est possible de construire une signature stratifiée contenant un symbole distinct pour chaque axiome de E, mais clairement, il n'est pas possible de faire de la déduction avec des GA-termes stratifiés de façon efficace en se servant d'une telle signature stratifiée.

De même, étant donnée une signature stratifiée, il existe de nombreux GA-termes stratifiés qui, une fois démarqués, représentent le même terme, et comme pour les signatures stratifiées, certains de ces GA-termes stratifiés ne devraient pas être construits par un démonstrateur automatique efficace. L'exemple le plus simple d'un GA-terme stratifié "inefficace" en est un dont aucun symbole n'est étiqueté par un élément de Σ_E. Dans ce chapitre, étant donnée une théorie permutative, nous allons d'abord étudier quelles signatures stratifiées et GA-termes stratifiés devraient être construits par un démonstrateur automatique efficace. Nous introduirons ainsi les notions de signatures stratifiées *saturées*, et de GA-termes stratifiés *saturés*.

Puis, nous étudierons la complexité de certains problèmes de déduction sur des GA-termes stratifiés saturés. Ces problèmes correspondent aux tâches indispensables qui doivent être accomplies par un démonstrateur automatique basé sur les GA-termes stratifiés, et sont résolus par les algorithmes de [AP01]. Dans [BdlTE03b], nous avons montré que ces problèmes sont **NP**-complets dans le cas général. Cependant, la signature stratifiée et les GA-termes stratifiés employés dans notre preuve n'étaient pas saturés, et il est possible qu'imposer cette restriction réduise la complexité de ces problèmes. Dans ce chapitre, nous montrerons qu'il n'en est rien, et que même les problèmes les plus basiques, comme l'appartenance d'un terme à un ensemble stratifié S[T], demeurent **NP**-complets.

Par abus de notation, dans ce qui suit, nous écrirons $c \rightleftharpoons c^\sigma$ pour représenter une équation permutative basée sur c et de permutation associée σ.

8.1 Signatures stratifiées saturées

Considérons l'exemple suivant.

Exemple 8.1.1 Soit E la théorie permutative définie par les axiomes suivants :

$$\begin{aligned} f(x,y) &\rightleftharpoons f(y,x) \\ g(x,y,z) &\rightleftharpoons g(y,x,z) \\ g(x,y,z) &\rightleftharpoons g(z,y,x). \end{aligned}$$

On définit les contextes c_1 et c_2, ainsi que les groupes G_1 et G_2 par :

$$\begin{aligned} \tau(c_1) = f(h(\circ),h(\circ)) \quad &\text{et} \quad G_1 = \mathrm{Sym}(\{1.1, 2.1\}) \\ \tau(c_2) = g(\circ,\circ,\circ) \quad &\text{et} \quad G_2 = \mathrm{Sym}(2) \end{aligned}$$

Enfin, on note $\Sigma_E = \{\langle f, c_1, G_1\rangle, \langle g, c_2, G_2\rangle\}$, Σ_E est bien une signature stratifiée sur E.

Soit $t = f(a,b)$, alors il est possible d'appliquer l'axiome $f(x,y) \rightleftharpoons f(y,x)$ à t. Cependant, il n'existe pas d'homomorphisme de c_1 (resp. c_2) vers arbre(t), et donc, il n'existe aucun GA-terme stratifié T tel que $\tau(\mathrm{dm}(T)) = t$, et $f(b,a) \in \mathrm{S}[T]$.

De même, soit $t' = g(a,b,d)$, alors on peut appliquer l'axiome $g(x,y,z) \rightleftharpoons g(z,y,x)$ à t', mais comme la permutation (1 3) n'est pas élément de G_2, il n'existe aucun GA-terme stratifié T' tel que $\tau(\mathrm{dm}(T')) = t'$ et $g(d,b,c) \in \mathrm{S}[T']$

Si Σ_E est une signature stratifiée sur une théorie permutative E, nous pouvons donc raisonnablement imposer que pour tout axiome e de E, si t' est obtenu après application de e à la racine de t, alors il existe un GA-terme stratifié T sur Σ, Σ_E, et une permutation $\sigma \in \mathcal{G}_T$ tels que $\tau(\mathrm{dm}(T)) = t$, et $\tau(\mathrm{dm}(T^\sigma)) = t'$. Ceci donne lieu à la définition suivante :

Définition 8.1.2 (Recouvrement) Soit E une théorie permutative définie par un ensemble $A = A_{c_1} \uplus \ldots \uplus A_{c_m}$ d'axiomes, où, pour $i = 1, \ldots, n$, toutes les équations permutatives de A_{c_i} sont basées sur le contexte c_i, et si $j \neq i$, alors $c_i \neq c_j$. Pour $i \in \{1, \ldots, n\}$, si S_i est l'ensemble des permutations associées aux équations permutatives dans A_{c_i}, alors on note G_{c_i} le groupe engendré par S_i.

Si Σ_E est une signature stratifiée sur E, on dit que Σ_E *recouvre* les axiomes de E si et seulement si pour tout $i = 1, \ldots, n$, il existe un symbole $\langle f_i, c_i, G_i\rangle \in \Sigma_E$ tel que le groupe G_{c_i} est un sous-groupe de G_i. On dit que Σ_E est *minimale* si et seulement si $\Sigma_E = \{\langle f_i, c_i, G_{c_i}\rangle \mid i = 1, \ldots, n\}$. ◇

Exemple 8.1.3 Soit E la théorie permutative définie par l'ensemble d'axiomes suivant :

$$\begin{aligned} h(x_1,x_2,x_3) &\rightleftharpoons h(x_2,x_1,x_3), \\ h(x_1,x_2,x_3) &\rightleftharpoons h(x_3,x_2,x_1), \\ f(h(x_1,x_2,x_3),x_4) &\rightleftharpoons f(h(x_1,x_2,x_4),x_3). \end{aligned}$$

On définit les contextes c, c' et c'' tels que

$$\tau(c) = h(\circ, \circ, \circ),\ \tau(c') = f(h(\circ, \circ, \circ), \circ),\ \text{et } \tau(c'') = g(h(\circ, \circ, \circ)),$$

puis on définit les groupes G, G' et G'' par :

$$G = \mathrm{Sym}(\{1, 2, 3\}),\ G' = \mathrm{Sym}(\{1.3, 2\}),\ G'' = \mathrm{I}.$$

Alors la signature stratifiée $\Sigma_E = \{\langle h, c, G\rangle, \langle f, c', G'\rangle, \langle g, c'', G''\rangle\}$ recouvre les axiomes de E.

Par contre, notons que l'équation $g(h(x_1, x_2, x_3)) \rightleftharpoons g(h(x_2, x_1, x_3))$ est élément de E, mais la permutation associée $\sigma = (1.1\ 1.2)$ n'est pas élément de $G'' = \mathrm{I}$.

Evidemment, dans le cas général, la condition de recouvrement n'implique pas la *complétude des groupes*, ainsi, la signature stratifiée de l'Exemple 8.1.3 recouvre la théorie E, mais les groupes ne sont pas complets. Par exemple, soit la permutation $\sigma = (1.1\ 1.2)$, alors l'équation permutative $c'' \rightleftharpoons c''^{\sigma}$ est élément de E, et pourtant, σ n'est pas dans G''. Nous pouvons donc chercher à imposer une restriction supplémentaire aux signature stratifiées considérées :

Définition 8.1.4 (Signature stratifiée saturée) Soit E une théorie permutative, et Σ_E une signature stratifiée sur E, alors Σ_E est *saturée* si et seulement si pour tout symbole $\langle f, c, G\rangle \in \Sigma_E$, l'équation permutative $c \rightleftharpoons c^{\sigma}$ est élément de E si et seulement si $\sigma \in G$. ◇

Remarque. Cette deuxième condition interdit qu'une signature stratifiée qui est saturée contienne deux éléments $\langle f, c, G\rangle$ et $\langle f, c, G'\rangle$, puisqu'alors, on a $G = G'$.

Exemple 8.1.5 Reprenons la théorie permutative E et la signature stratifiée Σ_E de l'Exemple 8.1.3, cette dernière recouvre les axiomes de E mais n'est pas saturée. Si on définit les groupes G_1 et G_2 par

$$G_1 = \mathrm{Sym}(\{1.1, 1.2, 1.3, 2\}),\ \text{et } G_2 = \mathrm{Sym}(\{1.1, 1.2, 1.3\}),$$

alors la signature stratifiée $\Sigma'_E = \{\langle h, c, G\rangle, \langle f, c', G_1\rangle, \langle g, c'', G_2\rangle\}$ recouvre elle aussi les axiomes de E, et est saturée.

Exemple 8.1.6 Soit E la théorie permutative composée des deux axiomes suivants :

$$\begin{aligned} g(x, y) &\rightleftharpoons g(y, x), \\ f(g(x, y), z) &\rightleftharpoons f(g(z, y), x). \end{aligned}$$

Notons c et c' les contextes respectivement associés à la première et à la deuxième équation. A partir de ces équations, on définit les groupes $G = \mathrm{Sym}(2)$, associé à c, et $G' = \mathrm{Sym}(\{1.1, 2\})$, associé à c'. On peut donc construire la signature stratifiée $\Sigma_E = \{\langle g, c, G\rangle, \langle f, c', G'\rangle\}$, qui recouvre les axiomes de E.

Cependant, en partant du terme $f(g(x,y),z)$ et en appliquant la première équation, on obtient :

$$f(g(x,y),z) \rightleftharpoons f(g(y,x),z),$$

qui est une nouvelle équation permutative, basée sur le contexte c', et de permutation associée $\sigma = (1.1\ 1.2)$. Comme cette permutation n'est pas élément de G', la signature stratifiée Σ_E n'est pas saturée. Pour obtenir une signature stratifiée saturée, le groupe G' doit être *augmenté* avec cette permutation. Finalement, si on note G'' le groupe engendré par G' et σ (on a donc $G'' = \mathrm{Sym}(\{1.1, 1.2, 2\})$), alors la signature stratifiée $\Sigma'_E = \{\langle g, c, G\rangle, \langle f, c', G''\rangle\}$ est saturée.

Dans la suite, nous nous intéresserons donc à des signatures stratifiées qui recouvrent les axiomes d'une théorie E, et qui sont saturées.

8.2 GA-termes stratifiés saturés

Quand une signature stratifiée a été fixée, pour un terme t donné, il peut évidemment exister plusieurs GA-termes stratifiés qui, une fois démarqués, représentent t. Chacun de ces GA-termes stratifiés représente un ensemble de E-conséquences de t, et il n'est en général pas possible d'en privilégier un à un autre.

Exemple 8.2.1 Soit E la théorie équationnelle constituée des axiomes suivants :

$$\begin{aligned} f(x,y) &\rightleftharpoons f(y,x), \\ f(g(x,y),z) &\rightleftharpoons f(g(y,x),z). \end{aligned}$$

Soient c et c' les contextes tels que $\tau(c) = f(\circ,\circ)$ et $\tau(c') = f(g(\circ,\circ),\circ)$, on pose $F_1 = \langle f, c, \mathrm{Sym}(2)\rangle$ et $F_2 = \langle f, c', \mathrm{Sym}(\{1.1, 1.2\})\rangle$. La signature stratifiée $\Sigma_E = \{F_1, F_2\}$ est alors saturée.

Soit $t = f(g(a,b),c)$, on peut construire les GA-termes stratifiés T et T' tels que $\tau(T) = F_1(g(a,b),c)$, et $\tau(T') = F_2(g(a,b),c)$, tous deux vérifient :

$$\tau(\mathrm{dm}(T)) \;=\; \tau(\mathrm{dm}(T')) \;=\; t.$$

Cependant, comme on a

$$\mathrm{S}[T] = \{f(g(a,b),c), f(c,g(a,b))\} \text{ et } \mathrm{S}[T'] = \{f(g(a,b),c), f(g(b,a),c)\},$$

il n'y a aucune raison de privilégier un de ces GA-termes stratifiés plutôt que l'autre.

Cependant, les deux exemples suivants montrent qu'il y a certaines conditions raisonnables qui peuvent être imposées aux GA-termes stratifiés considérés.

Exemple 8.2.2 Supposons que la théorie E est constituée des axiomes suivants :

$$\begin{aligned} f(x,y) &\rightleftharpoons f(y,x), \\ g(x,y) &\rightleftharpoons g(y,x). \end{aligned}$$

Soient c et c' les contextes tels que $\tau(c) = f(\circ, \circ)$, et $\tau(c') = g(\circ, \circ)$, et posons $F_1 = \langle f, c, \mathrm{Sym}(2)\rangle$ et $F_2 = \langle g, c', \mathrm{Sym}(2)\rangle$. Alors la signature stratifiée $\Sigma_E = \{F_1, F_2\}$ recouvre les axiomes de E et est saturée.

Soit $t = f(f(a,b), g(c,d))$, il est alors possible de construire plusieurs GA-termes stratifiés sur Σ_E, qui, démarqués, représentent t. Un de ces GA-termes stratifiés est T, tel que $\tau(T) = F_1(F_1(a,b), F_2(c,d))$. Clairement, il est plus intéressant de considérer T plutôt que n'importe quel autre GA-terme stratifié T' qui vérifie $\tau(\mathrm{dm}(T')) = t$, puisqu'on a

$$\forall T', \tau(\mathrm{dm}(T')) = \tau(\mathrm{dm}(T)) \;\Rightarrow\; \mathrm{S}[T'] \subseteq \mathrm{S}[T].$$

Par exemple, si $\tau(T') = f(F_1(a,b), F_2(c,d))$, alors le terme $f(g(c,d), f(a,b))$ est élément de $\mathrm{S}[T]$, mais pas de $\mathrm{S}[T']$.

Cet exemple montre donc qu'on peut imposer de ne considérer que des GA-termes stratifiés dont le plus de sommets possible sont étiquetés par des symboles de Σ_E.

Exemple 8.2.3 Soit E la théorie constituée des axiomes suivants :

$$\begin{aligned} g(x,y) &\rightleftharpoons g(y,x), \\ f(g(x,y),z) &\rightleftharpoons f(g(z,y),x). \end{aligned}$$

Notons c et c' les contextes respectivement associés au premier et au deuxième axiome, et soient $G = \mathrm{Sym}(2)$, et $G' = \mathrm{Sym}(\{1.1, 1.2, 2\})$. Il est alors aisé de vérifier que la signature stratifiée $\Sigma_E = \{\langle g, c, G\rangle, \langle f, c', G'\rangle\}$ recouvre les axiomes de E et est saturée.

Prenons le terme $t = f(g(a,b), d)$, et considérons les deux GA-termes stratifiés distincts T et T', représentant respectivement

$$\langle f, c', G'\rangle(g(a,b), d) \text{ et } f(\langle g, c, G\rangle(a,b), d).$$

Ces deux GA-termes stratifiés utilisent chacun le plus de symboles de Σ_E possible, et vérifient donc la condition exprimée dans l'Exemple 8.2.3. Cependant, comme $\mathrm{S}[T'] \subseteq \mathrm{S}[T]$, il est préférable de considérer le GA-terme stratifié T plutôt que T'.

Dans cet exemple, il est plus intéressant de considérer T plutôt que T' parce que c est un sous-contexte strict de c', et qu'il est garanti que $\mathrm{S}[T'] \subseteq \mathrm{S}[T]$, puisque Σ_E est saturée.

Définition 8.2.4 (GA-terme stratifié saturé) Soit T un GA-terme stratifié, on dit que T est *saturé* si la signature stratifiée Σ_E est saturée, et que pour tout sommet v de T, si v vérifie les propriétés suivantes :

1. v est étiqueté par un symbole de Σ,
2. il existe un symbole $\langle f, c, G\rangle \in \Sigma_E$ et un homomorphisme h de c vers $\mathrm{dm}(T|v)$,
3. v n'est dans aucun antirésidu $\overline{\mathrm{R}}_T(u)$ pour $u \in V_{\mathrm{s}}$,
4. il existe un chemin unique entre la racine de T n'importe quel sommet du résidu ou de l'antirésidu de h,

alors il existe un sommet non-variable u de c tel que le sommet $h(u)$ de T est étiqueté par un symbole $\langle f', c', \mathcal{G}' \rangle$ de Σ_E, et c' n'est pas isomorphe à $c|u$. $\diamond$

Les quatre conditions vérifiées par v dans la définition sont les suivantes : si ce sommet est étiqueté par un symbole de Σ (condition 1), et qu'il est théoriquement possible de lui associer un symbole $\langle f, c, G \rangle$ de Σ_E (conditions 2, 3 et 4), alors nécessairement, il doit y avoir un sommet u en-dessous de v, étiqueté par un symbole de $\langle f', c', \mathcal{G}' \rangle \in \Sigma_E$, et qui implique que :

- on ne peut pas remplacer le symbole de v par $\langle f, c, G \rangle$, sans quoi le GA-terme stratifié serait mal formé (Condition 1 de la Définition 6.3.1),
- c' n'est pas un sous-contexte de c, sans quoi, par hypothèse de saturation de Σ_E, on pourrait remplacer le symbole de v par $\langle f, c, G \rangle$ et celui de u par f' ; on obtiendrait ainsi un terme stratifié bien formé qui subsumerait le précédent.

Propriété 8.2.5 *Si T est un* GA*-terme stratifié saturé, alors pour tout sommet v de T, $T|v$ est également un* GA*-terme stratifié saturé.*

Théorème 8.2.6 *Soit T un* GA*-terme stratifié, et A un* A*-terme stratifié tel que $T \Subset A$. Si A est saturé, alors T est également saturé.*

PREUVE. On pose $T = (V, s, a)$, et $A = (V', s', a')$; par hypothèse, il existe un homomorphisme clos h de A vers T. Supposons qu'il existe un sommet v de T qui vérifie les quatre conditions de la Définition 8.2.4. Soit $w \in V'$ tel que $h(w) = v$, alors la restriction de h à $V'|w$ est un homomorphisme clos de $A|w$ vers $T|v$ d'après la Propriété 5.2.5, et donc, un homomorphisme clos de $\mathrm{dm}(A|w)$ vers $\mathrm{dm}(T|v)$. D'après le Lemme 5.2.21, il existe donc un homomorphisme injectif h' de c vers $\mathrm{dm}(A|w)$. D'après le Corollaire 6.6.5, w n'est dans aucun antirésidu $\overline{\mathrm{R}}_A(u')$ pour $u' \in V'_{\mathrm{s}}$, et comme $s'(w) = s(v)$, et que A est un A-terme, w remplit les quatre conditions de la Définition 8.2.4. Par hypothèse de saturation, on en déduit qu'il existe un sommet non-variable u de c tel que $h'(u)$ est étiqueté par $\langle f', c', G' \rangle \in \Sigma_E$, et que c' n'est pas isomorphe à $c|u$.

Donc, le sommet $v' = h(u) = h(h'(u))$ est lui aussi étiqueté par $\langle f', c', G' \rangle$, et vérifie donc les conditions de la Définition 8.2.4. Donc, T est bien saturé. ■

Il est clair qu'étant donnée une théorie permutative E et un terme t, il est possible de construire un GA-terme stratifié T qui est saturé, et tel que $t \in \mathrm{S}[T]$. De plus, cette construction est évidemment polynomiale (si la signature stratifiée saturée a déjà été construite). Dans la prochaine partie, nous allons étudier certains problèmes qui doivent être résolus pour pouvoir faire de la déduction avec des GA-termes stratifiés, et nous démontrerons qu'ils sont tous **NP**-durs.

8.3 Complexité de problèmes de déduction

L'application de règles de paramodulation ou de résolution à des clauses stratifiées (c'est-à-dire des clauses constituées de GA-termes stratifiés) n'est pas une tâche triviale,

et nécessite des algorithmes complexes comme ceux proposés dans [AP01]. Il faut évidemment concevoir de nouveaux algorithmes comme par exemple un algorithme d'unification pour des GA-termes stratifiés, mais des algorithmes pour des tâches beaucoup plus basiques sont également nécessaires. Ces tâches basiques semblent elles aussi être assez complexes, et même l'algorithme de [AP01] pour tester l'appartenance d'un terme à un ensemble stratifié $\mathrm{S}[T]$ est exponentiel. Dans [BdlTE03b], nous avons étudié les complexités de ces problèmes dans le cas général. Dans ce qui suit, nous allons en étudier la complexité dans le cas où les GA-termes stratifiés (resp. A-termes stratifiés) sont saturés. Par commodité, nous nommerons ces GA-termes stratifiés saturés (resp. A-termes stratifiés saturés) des sGA-termes (resp. sA-termes). Nous commençons par présenter les problèmes à étudier, et nous montrerons qu'ils sont tous, à l'exception du problème S_INCL, dans NP. Pour le problème d'unifiabilité, nous considérerons un sous-ensemble $\mathcal{X}$ de l'ensemble des symboles de constantes de Σ comme des variables.

Les problèmes que nous étudierons sont les suivants :

Problème 1: Appartenance stratifiée, ou S_MEM.
Entrée: Un terme t et un sGA-terme T.
Question: Est-ce que t est élément de $\mathrm{S}[T]$?

Problème 2: Sous-terme stratifié, ou S_SBT.
Entrée: Un terme t et un sGA-terme T.
Question: Existe-t-il un terme $t' \in \mathrm{S}[T]$ tel que t est un sous-terme de t' ?

Problème 3: Intersection stratifiée, ou S_INTER.
Entrée: Deux sGA-termes T_1 et T_2.
Question: Est-ce que $\mathrm{S}[T_1]$ et $\mathrm{S}[T_2]$ ont un élément en commun ?

Problème 4: Unifiabilité stratifiée, ou S_UNIF
Entrée: Deux sGA-termes T_1 et T_2, et un ensemble de variables $\mathcal{X}$.
Question: Existe-t-il un terme t_1 dans $\mathrm{S}[T_1]$ et un terme t_2 dans $\mathrm{S}[T_2]$ tels que t_1 et t_2 sont unifiables sur $\mathcal{X}$?

Problème 5: Inclusion stratifiée, ou S_INCL.
Entrée: Deux sGA-termes T_1 et T_2.
Question: Est-ce que $\mathrm{S}[T_1]$ est un sous-ensemble de $\mathrm{S}[T_2]$?

Nous commençons par prouver certaines relations de complexité parmi les Problèmes 1 à 5.

Lemme 8.3.1 *Le problème* S_MEM *se réduit polynomialement à* S_SBT, *et le problème* S_INTER *à* S_UNIF.

PREUVE. Pour tout terme t et tout sGA-terme T, si t et $\tau(\mathrm{dm}(T))$ ont la même taille, on pose $t' = t$; sinon on définit t' comme étant un nouveau symbole de constante. La transformation de (t, T) à (t', T) est clairement polynomiale, et il est aisé de voir que t est élément de $\mathrm{S}[T]$ si et seulement si t' est un sous-terme d'un élément de $\mathrm{S}[T]$. On a donc une transformation polynomiale de S_MEM vers S_SBT.

Prenons deux GA-termes T_1 et T_2, et soit $\mathcal{X} = \emptyset$. On considère donc que T_1 et T_2 n'ont pas de variables, ce qui signifie que deux termes $t_1 \in \mathrm{S}[T_1]$ et $t_2 \in \mathrm{S}[T_2]$ sont unifiables si et seulement s'ils sont égaux. Le problème S_INTER est donc équivalent à la restriction de S_UNIF aux instances pour lesquelles $\mathcal{X} = \emptyset$. Donc, S_INTER se réduit polynomialement à S_UNIF. ∎

Nous montrons maintenant que les quatre premiers problèmes sont dans **NP**.

Théorème 8.3.2 *Les problèmes 1 à 4 sont dans* $\mathbf{NP}^{\mathrm{G\_MEM}}$.

PREUVE. Nous prouvons le résultat pour le problème S_MEM, les preuves sont identiques pour les autres problèmes (puisque tester l'unifiabilité pour des termes standard est polynomial[1], etc).

Soit t un terme et T un sGA-terme, d'après le Théorème 6.5.13, on sait que $\mathrm{S}[T] = \tau(\mathrm{dm}(T^{\mathcal{G}_T}))$, et donc,

$$t \in \mathrm{S}[T] \;\Leftrightarrow\; \exists \sigma \in \mathcal{G}_T \text{ tel que } t = \tau(\mathrm{dm}(T^{\sigma})).$$

Si V est l'ensemble des sommets de T, il nous suffit de choisir une permutation $\sigma \in \mathrm{Sym}(V)$, et de tester si $t = \tau(\mathrm{dm}(T^{\sigma}))$, ce qui est trivialement polynomial. Si ce premier test réussit, il suffit de s'assurer que σ est élément du groupe $\mathcal{G}_T$.

Nous pouvons déterminer un ensemble de générateurs pour le groupe $\mathcal{G}_T$ en temps polynomial. En effet, l'union des ensembles de générateurs pour les groupes $\mathcal{G}_T(v)$, pour tous les sommets v étiquetés par des symboles de Σ_E est un ensemble de générateurs de $\mathcal{G}_T$ d'après la Propriété 6.5.6, et si v est étiqueté par $\langle f, c, G\rangle \in \Sigma_E$, alors $\mathcal{G}_T(v)$ est engendré par le conjugué par $\mathrm{h}_{[T,v]}$ de l'ensemble des générateurs de G. Enfin, un appel à l'oracle G_MEM avec cet ensemble de générateurs et la permutation σ permet de savoir si σ est bien élément de $\mathcal{G}_T$. On a bien une réduction de Turing non-déterministe polynomiale de S_MEM vers G_MEM. ∎

Naturellement, l'intérêt de choisir pour oracle le problème G_MEM est que ce dernier est polynomial, ce qui prouve que les problèmes 1 à 4 sont dans la classe $\mathbf{NP}^{\mathbf{P}} = \mathbf{NP}$. Nous ne pouvons pas appliquer le même genre de raisonnement pour borner la complexité du problème 5, mais ce dernier peut être restreint au deuxième niveau de la hiérarchie polynomiale, voir [GJ79] ou [SP98].

Théorème 8.3.3 *Le problème* S_INCL *est dans la classe* $\mathbf{\Pi_2^P}$.

[1]Notons que nous testons si deux sGA-termes sont unifiables, mais que nous ne cherchons pas à déterminer d'*unificateur* pour ces sGA-termes.

PREUVE. Soient T_1 et T_2 deux sGA-termes, alors $S[T_1] \not\subseteq S[T_2]$ si et seulement s'il existe un terme $t \in S[T_1]$ qui n'est pas dans $S[T_2]$. Donc, on peut résoudre ce problème en devinant un terme t, puis en faisant appel à un oracle pour S_MEM tout d'abord sur t, T_1, puis sur t, T_2, et en renvoyant "vrai" si le premier test réussit et le second échoue. On obtient ainsi une réduction de Turing non-déterministe polynomiale à un problème dans **NP**, et donc, **co**−S_INCL est dans $\mathbf{NP}^{\mathbf{NP}} = \mathbf{\Sigma_2^P}$, ce qui signifie que S_INCL est dans $\mathbf{co}\text{-}\mathbf{\Sigma_2^P} = \mathbf{\Pi_2^P}$. ∎

8.4 NP-complétude

Dans cette partie, nous allons prouver que les Problèmes 1 à 4 sont **NP**-complets, et les problèmes 5 et 6, **NP**-durs. Pour démontrer ces résultats, nous effectuerons des réductions du problème de contraintes de groupe, G_CSTR, vers ces problèmes. Nous allons prouver que G_CSTR se réduit polynomialement aux problèmes S_MEM, S_INCL, et S_INTER, ce qui prouvera que les problèmes 1 à 4 sont **NP**-complets, et que le problème 5 est **NP**-dur.

Nous commençons par prouver le résultat pour S_MEM. Nous montrons que le problème G_CSTR peut être résolu par une instance particulièrement simple du problème d'appartenance stratifié. Partant d'une instance du problème G_CSTR, on définit les ensembles et les termes suivants :

Définition 8.4.1 On définit les ensembles I_j pour $j = 1, \ldots, n$ par :

$$\text{pour tout } j,\ I_j \ = \ \{i \mid j \in J_i\}.$$

Soit Σ la signature $\{f, g, a, b\}$, où a, b sont des constantes, et f, g sont des symboles de fonction d'arité n. Pour tout $i = 1, \ldots, n$, on pose :

$$t_i = g(a, \ldots, a, b, a, \ldots, a),$$

où la constante b est le $i^{\text{ème}}$ argument de la fonction g. Enfin, on définit le terme $t = f(t_1, \ldots, t_n)$. ◇

Exemple 8.4.2 Supposons que $n = 2$, et que $J_1 = \{1\}$, et $J_2 = \{1, 2\}$. Alors

$$I_1 = \{1, 2\},\ I_2 = \{2\},\ t_1 = g(b, a),\ t_2 = g(a, b),\ \text{et } t = f(g(b, a), g(a, b)).$$

Définition 8.4.3 Soit $I \subseteq \{1, \ldots, n\}$, on note $t_I = g(t_1, \ldots, t_n)$, où, pour tout $i = 1, \ldots, n$,
- si $i \in I$, alors t_i est une variable,
- sinon, $t_i = a$.

On définit alors le contexte $c(I) = \text{arbre}(t_I)$, l'ensemble des sommets variables de $c(I)$ est donc égal à I. Pour tout $j \in \{1, \ldots, n\}$, on définit le symbole

$$g_j \ = \ \langle g, c(I_j), \text{Sym}(I_j) \rangle.$$

Soit c le contexte tel que $\tau(c) = f(\circ, \ldots, \circ)$, alors on définit le symbole $F = \langle f, c, G\rangle$.

Pour $j \in \{1, \ldots, n\}$, soient μ_j et μ'_j des générateurs du groupe $\mathrm{Sym}(I_j)$, on considère la théorie permutative E, définie par les axiomes suivants :

$$\begin{aligned} c(I_j) &\rightleftharpoons c(I_j)^{\mu_j} \\ c(I_j) &\rightleftharpoons c(I_j)^{\mu'_j} \\ c &\rightleftharpoons c^{\sigma_i},\ i = 1, \ldots, n. \end{aligned}$$

Enfin, on définit la signature stratifiée

$$\Sigma_E = \{g_j \mid j = 1, \ldots, n\} \cup \{F\}. \qquad \diamond$$

Exemple 8.4.4 Reprenons l'Exemple 8.4.2, alors on a

$$\tau(c(I_1)) = g(\circ, \circ) \text{ et } \tau(c(I_2)) = g(a, \circ).$$

On peut donc construire les deux éléments g_1 et g_2 de la signature stratifiée Σ_E qui sont :

$$g_1 = \langle g, c(I_1), \mathrm{Sym}(2)\rangle, \text{ et } g_2 = \langle g, c(I_2), \mathrm{I}\rangle.$$

Remarque. Si I_j et I_k sont identiques, alors g_j et g_k le sont également ; Σ_E peut donc être de cardinalité inférieure à $n + 1$.

Comme tous les groupes qui apparaissent dans les éléments de Σ_E sont maximaux, on en déduit que :

Propriété 8.4.5 *La signature stratifiée Σ_E de la Définition 8.4.3 recouvre les axiomes de E et est saturée.*

Nous construisons maintenant un SGA-terme stratifié T sur Σ, Σ_E qui portera l'information associée au groupe G et aux contraintes $J_1, \ldots, J_n$.

Définition 8.4.6 Pour tout $j = 1, \ldots, n$, soit $k = \min I_j$. On associe à j le terme (sur $\Sigma \cup \Sigma_E$)

$$t'_j = g_j(a, \ldots, a, b, a, \ldots, a),$$

où la constante b est le $k^{\text{ième}}$ argument de g_j. On construit enfin les A-termes $A_j = \mathrm{arbre}(t'_j)$ pour $j = 1, \ldots, n$, et $A = \mathrm{arbre}(\ F(t'_1, \ldots, t'_n)\ )$. En particulier, dans le A-terme A, chaque symbole g_j est attaché à la position j. $\diamond$

Exemple 8.4.7 Dans la suite de l'Exemple 8.4.4, on a donc

$$\tau(A_1) = t'_1 = g_1(b, a),\ \tau(A_2) = t'_2 = g_2(a, b),\ \text{ et } \tau(A) = F(g_1(b, a), g_2(a, b)).$$

Il est aisé de vérifier que les A_j et A sont des A-termes stratifiés, et comme nous avons utilisé des symboles de Σ_E partout où c'était possible, ces A-termes stratifiés sont saturés.

Lemme 8.4.8 *Soient i et j deux éléments de $\{1,\ldots,n\}$. Alors $t_i \in \mathrm{S}[A_j]$ si et seulement si $j \in J_i$.*

PREUVE. Par construction, la restriction de $\mathrm{h}_{[A_j,\varepsilon]}$ à $\mathcal{SV}(g_j) = \{1,\ldots,n\}$ est l'identité, et le résidu de cet homomorphisme est $\mathrm{R}_{A_j}(\varepsilon) = I_j$. Comme la racine de A_j est l'unique sommet du GA-terme à être étiqueté par un symbole de Σ_E, on en déduit que le groupe $\mathcal{G}_{A_j}$ est exactement le groupe $\mathrm{Sym}(I_j)$.

Supposons que $t_i \in \mathrm{S}[A_j]$. Il existe donc une permutation $\pi \in \mathrm{Sym}(I_j)$ telle que $s_j = \tau(\mathrm{dm}(A_j^\pi)) = t_i$. Comme l'unique sommet de A_j à être étiqueté par le symbole b est le sommet k, on en déduit que b apparaît à la position k^π dans s_j, et, puisque b n'apparaît qu'à la position i dans t_i, que $k^\pi = i$. Enfin, k étant élément de I_j, on en déduit que $i = k^\pi \in I_j$, c'est-à-dire que $j \in J_i$.

Réciproquement, si $j \in J_i$, alors par définition, $i \in I_j$. Il existe donc une permutation $\pi \in \mathrm{Sym}(I_j)$ telle que $k^\pi = i$, et comme $\mathrm{Sym}(I_j) = \mathcal{G}_{A_j}$, on en déduit que $\tau(\mathrm{dm}(A_j^\pi)) = t_i$, c'est-à-dire que $t_i \in \mathrm{S}[A_j]$. ∎

On en déduit donc le résultat suivant :

Corollaire 8.4.9 *Soient i et j deux éléments de $\{1,\ldots,n\}$, et $\sigma \in \mathcal{G}_T(j)$. Alors $t_i = \tau(\mathrm{dm}((A|j)^\sigma))$ si et seulement si $j \in J_i$.*

PREUVE. Les A-termes stratifiés A_j et $A|j$ sont bisimilaires et donc isomorphes, notons η l'isomorphisme de A_j vers $A|j$. Alors d'après le Corollaire 6.6.8,

$$\mathcal{G}_{A|j} \;=\; \mathcal{G}_A(j) \;=\; \mathcal{G}_{A_j}^\eta.$$

Supposons qu'il existe une permutation $\sigma \in \mathcal{G}_T(j)$ telle que $t_i = \tau(\mathrm{dm}((A|j)^\sigma))$, alors, il existe une permutation $\pi \in \mathcal{G}_{A_j}$ telle que $\sigma = \pi^\eta$, et d'après le Théorème 6.6.9, η est un isomorphisme de A_j^π vers $(A|j)^\sigma$. Ceci prouve que $t_i = \tau(\mathrm{dm}((A_j)^\pi))$, et donc que $t_i \in \mathrm{S}[A_j]$. On en déduit d'après le Lemme 8.4.8 que $j \in J_i$.

Réciproquement, si $j \in J_i$, alors d'après le Lemme 8.4.8, il existe une permutation $\pi \in \mathcal{G}_{A_j}$ telle que $t_i = \tau(\mathrm{dm}((A_j)^\pi))$. Pour les mêmes raisons que précédemment, on en déduit qu'il existe une permutation $\sigma \in \mathcal{G}_A(j)$ telle que $t_i = \tau(\mathrm{dm}((A|j)^\sigma))$. ∎

Nous pouvons maintenant prouver que T vérifie la propriété suivante :

Théorème 8.4.10 *t est élément de $\mathrm{S}[A]$ si et seulement s'il existe une permutation $\pi \in G$ telle que pour tout $i = 1,\ldots,n$, $i^\pi \in J_i$.*

PREUVE. Comme dans le cas des A_j, la restriction de l'homomorphisme $\mathrm{h}_{[A,\varepsilon]}$ à l'ensemble $\{1,\ldots,n\}$ est l'identité, et le résidu de cet homomorphisme est $\mathrm{R}_A(\varepsilon) = \{1,\ldots,n\}$, qui est l'ensemble des sommets variables de c. Ceci prouve que $\mathcal{G}_A(\varepsilon)$ est exactement le groupe G.

Supposons qu'il existe une permutation $\sigma \in \mathcal{G}_A$ telle que $\tau(\mathrm{dm}(A^\sigma)) = t$. On note π la restriction de σ à $\{1,\ldots,n\}$, on a donc $\pi \in G$. Posons $A^\sigma = (V, s, a')$, alors on a

$a'(\varepsilon) = 1^\pi.\cdots.n^\pi$. Pour tout $j = 1,\ldots,n$, on note π_j la restriction de σ à $\mathrm{R}_A(j^\pi)$, π_j est donc élément de $\mathcal{G}_A(j)$. Puisque le $i^{\text{ème}}$ argument de $\tau(\mathrm{dm}(A^\sigma))$ doit être t_i, on a nécessairement

$$t_i \;=\; \tau(\mathrm{dm}(A^\sigma|i^\pi)) \;=\; \tau(\mathrm{dm}(A^{\pi_i}|i^\pi)) \;=\; \tau(\mathrm{dm}((A|i^\pi)^{\pi_i})).$$

On peut donc appliquer le Corollaire 8.4.9, et en déduire que $i^\pi \in J_i$. Donc, si $t \in \mathrm{S}[A]$, alors il existe une permutation π de G telle que pour tout $i = 1,\ldots,n$, $i^\pi \in J_i$.

Réciproquement, supposons qu'il existe une permutation π de T telle que pour tout $i = 1,\ldots,n$, $i^\pi \in J_i$. Alors d'après le Corollaire 8.4.9, on sait que pour tout i, il existe une permutation $\pi_i \in \mathcal{G}_A(i^\pi)$ telle que $\tau(\mathrm{dm}((A|i^\pi)^{\pi_i})) = t_i$. On pose $\sigma = \pi\pi_1\ldots\pi_n$; il est clair que σ est une permutation de $\mathcal{G}_A$, et que $\tau(\mathrm{dm}(A^\sigma)) = t$. Donc, t est alors bien un élément de $\mathrm{S}[A]$. ∎

Ceci nous permet de prouver la première réduction polynomiale :

Corollaire 8.4.11 G_CSTR *se réduit polynomialement à* S_MEM.

PREUVE. D'après le Théorème 8.4.10, toute instance du problème G_CSTR se réduit clairement aux instances t, G de S_MEM. La transformation de G et des J_i, pour $i = 1,\ldots,n$ à t, G est polynomiale : la taille de t et le nombre de sommets dans T sont en $O(n^2)$, T contient les générateurs de G, et il ne faut pas plus de deux générateurs pour engendrer les groupes $\mathrm{Sym}(I_j)$ contenus dans les g_j. ∎

Montrons maintenant que le problème G_CSTR se réduit polynomialement à S_INCL et S_INTER. Pour cela, nous aurons besoin d'étendre la signature stratifiée Σ_E et de construire un nouveau SGA-terme T'.

Définition 8.4.12 Pour $i \in \{1,\ldots,n\}$, on note

$$t'_i = g(a,\ldots,a,x,a,\ldots,a),$$

où la variable x est le $i^{\text{ème}}$ argument de g, et on définit le terme $t' = f(t'_1,\ldots,t'_n)$. Soit $c' = \mathrm{arbre}(t')$, on note D l'ensemble des sommets variables de c', et on définit le symbole $F' = \langle f, c', \mathrm{Sym}(D)\rangle$. Par la suite, nous considérerons la signature stratifiée $\Sigma'_E = \Sigma_E \cup \{F'\}$.

Enfin, on définit le A-terme $A' = \mathrm{arbre}(\ F'(t_1,\ldots,t_n)\ )$, où les t_i sont les mêmes que dans la Définition 8.4.1. ◇

Exemple 8.4.13 Reprenons l'Exemple 8.4.2, alors on a $t'_1 = g(x,a)$ et $t'_2 = g(a,x)$, d'où $t = f(g(x,a),g(a,x))$, et on a donc

$$\tau(c') = f(g(\circ,a),g(a,\circ)),\ \text{ et } D = \{1.1, 2.2\}.$$

Le A-terme A' vérifie alors $\tau(A') = F'(g(b,a),g(a,b))$.

Le groupe associé à c' est $\mathrm{Sym}(D) = \mathrm{Sym}(\mathcal{SV}(c))$ qui est maximal, et Σ'_E est donc saturée. Il est également aisé de voir que le A-terme A' est stratifié sur $\Sigma \cup \Sigma'_E$, (en prenant l'identité pour la fonction $\mathrm{h}_{[A',\varepsilon]}$), et que A' est saturé.

Nous prouvons maintenant les deux autres réductions polynomiales.

Corollaire 8.4.14 *Le problème* G_CSTR *se réduit polynomialement à* S_INCL *et à* S_INTER.

PREUVE. Par construction, on a $\tau(\mathrm{dm}(A')) = t$. De plus, pour toute permutation σ de $\mathcal{G}_{A'} = \mathrm{Sym}(D)^{\mathrm{h}_{[A',\varepsilon]}}$, comme tous les sommets de $\mathrm{R}_{A'}(\varepsilon) = \mathrm{h}_{[A',\varepsilon]}(D)$ sont étiquetés par le même symbole b, on en déduit que

$$\tau(\mathrm{dm}(A^\sigma)) \;=\; \tau(\mathrm{dm}(A)) \;=\; t.$$

On a donc $\mathrm{S}[A'] = \{t\}$, d'où

$$t \in \mathrm{S}[A] \;\Leftrightarrow\; \mathrm{S}[A'] \subseteq \mathrm{S}[A] \;\Leftrightarrow\; \mathrm{S}[A'] \cap \mathrm{S}[A] \neq \emptyset.$$

D'après le Théorème 8.4.10, ces conditions sont équivalentes à l'existence d'une permutation dans G qui satisfait toutes les contraintes $J_1, \ldots, J_n$, et la transformation de ces contraintes à l'instance A', A des problèmes S_INCL et S_INTER est clairement polynomiale. ∎

Ces réductions polynomiales du problème G_CSTR à S_MEM, S_INCL et S_INTER, associées au Lemme 8.3.1 et aux Théorèmes 8.3.2 et 8.3.3 se résument ainsi :

Théorème 8.4.15 *Les complexités des problèmes étudiés sont les suivantes :*

1. *Les problèmes* S_MEM, S_SBT, S_INTER *et* S_UNIF *sont* **NP**-*complets.*
2. *Le problème* S_INCL *est dans la classe* $\mathbf{\Pi}_2^{\mathbf{P}}$, *et est* **NP**-*dur.*

8.5 Résumé

Dans ce chapitre, nous avons étudié quelles conditions il était raisonnable d'imposer à des signatures stratifiées et à des GA-termes stratifiés. Etant donnée une théorie permutative E, nous avons commencé par définir les signatures stratifiées saturées, qui sont intuitivement des signatures stratifiées telles que pour tout élément $\langle f, c, G\rangle$, le groupe G est complet pour E. Puis, nous avons défini les GA-termes stratifiés saturés ; intuitivement, leur définition est assez simple : il s'agit de GA-termes stratifiés qui contiennent le plus possible de sommets étiquetés par des symboles de Σ_E. Le choix des sommets à étiqueter avec des symboles de Σ_E, ainsi que le choix des symboles de Σ_E à utiliser demeure non-déterministe.

Enfin nous avons étudié certains problèmes qui doivent être résolus pour pouvoir faire de la déduction avec des GA-termes stratifiés, et nous avons vu que même en imposant ces conditions de saturation, ces problèmes demeurent **NP**-durs. C'est pourquoi dans les prochains chapitres, nous étudierons des classes de théories permutatives dans lesquelles il est possible de faire de la déduction avec des GA-termes stratifiés de façon efficace.

Quatrième partie

Classes de théories permutatives

Chapitre 9

Stabilité

Dans le chapitre précédent, nous avons vu que même les problèmes les plus basiques à résoudre pour pouvoir faire de la déduction avec des GA-termes stratifiés sont **NP**-durs quand on considère des théories permutatives quelconques. Nous allons maintenant étudier quelles restrictions peuvent être imposées aux théories permutatives considérées afin de pouvoir faire de la déduction plus efficacement avec des GA-termes stratifiés.

Dans ce chapitre, nous allons introduire la notion de *stabilité* d'une signature stratifiée et d'un ensemble d'axiomes, puis nous verrons que cette restriction ne suffit pas à assurer que les théories permutatives considérées ont de suffisamment bonnes propriétés pour faire de la déduction avec des GA-termes stratifiés.

9.1 Permutations induites

Considérons l'exemple suivant :

Exemple 9.1.1 Soit E la théorie permutative définie par les axiomes suivants :

$$\begin{aligned} g(x,y) &\rightleftharpoons g(y,x) \\ f(g(x,y),z) &\rightleftharpoons f(g(x,z),y). \end{aligned}$$

On définit les contextes c, c' et les groupes G, G' par :

$$\tau(c) = g(\circ,\circ),\ \tau(c') = f(g(\circ,\circ),\circ),\ G = \mathrm{Sym}(2),\ G' = \mathrm{Sym}(\{1.2, 2\}).$$

Alors la signature stratifiée $\Sigma_E = \{\langle g, c, G\rangle, \langle f, c', G'\rangle\}$ recouvre E, mais n'est pas saturée.

Prenons le terme $t = f(g(x,y),z)$, alors on peut appliquer l'axiome de commutativité de g à la position 1 de t, on obtient le terme $t' = f(g(y,x),z)$, et l'équation $t \rightleftharpoons t'$ est une équation permutative de contexte associé c', et de permutation associée (1.1 1.2). On obtient donc une nouvelle équation permutative basée sur c' après une *unique* application de l'axiome de commutativité de g.

Dans ce qui suit, étant donné un contexte c, nous allons étudier dans quel cas l'application d'une unique équation permutative à un terme induit une nouvelle équation permutative basée sur ce contexte.

Définition 9.1.2 Soient c et c' deux contextes tels que $h, v : c \trianglelefteq c'$. Alors le *groupe d'automorphisme* de l'homomorphisme h est l'ensemble

$$\mathrm{A_c}(h) = \{\sigma \in \mathrm{Sym}(\mathcal{SV}(c)) \mid \forall w \in \mathcal{SV}(c),\ c'|h(w) \simeq c'|h(w^\sigma)\}.$$

Il s'agit donc de l'ensemble des permutations des sommets variables de c telles que h associe à tout sommet variable de c et à son image des sous-contextes de c' isomorphes.

Etant donnée une permutation $\sigma \in \mathrm{Sym}(\mathcal{SV}(c))$, l'homomorphisme h est dit *σ-stable* si et seulement si σ est élément de $\mathrm{A_c}(h)$; dans ce cas, on note $h, v : c \trianglelefteq_\sigma c'$. Enfin, étant donné un groupe G, on dit que h est *G-stable* si et seulement si pour tout $\sigma \in G$, h est σ-stable, et on note alors $h, v : c \trianglelefteq_G c'$. Dans le cas où $v = \varepsilon$, on notera également $h : c \sqsubseteq_\sigma c'$, et $h : c \sqsubseteq_G c'$. ◇

Exemple 9.1.3 Soit E la théorie permutative constituée des deux axiomes suivants :

$$\begin{aligned} f(x,y) &\rightleftharpoons f(y,x), \\ f(g(x,y),g(w,z)) &\rightleftharpoons f(g(y,x),g(w,z)). \end{aligned}$$

On note $c = (V, s, a)$ et $c' = (V', s', a')$ les contextes respectivement associés à la première et à la deuxième équation, et on définit la fonction h de V vers V' par : $\forall v \in V$, $h(v) = v$.

On a alors $h, \varepsilon : c \trianglelefteq c'$, c' est donc une instance de c à la racine. De plus, $c'|h(1)$ et $c'|h(2)$ sont isomorphes, puisqu'ils se traduisent tous deux en $g(\circ, \circ)$, ce qui prouve que $h, \varepsilon : c \trianglelefteq_{(1\ 2)} c'$, et si G est le groupe engendré par $(1\ 2)$, alors $h, \varepsilon : c \trianglelefteq_G c'$.

Propriété 9.1.4 *Supposons que $h, v : c \trianglelefteq c'$, et que h est un homomorphisme clos, alors* $\mathrm{A_c}(h) = \mathrm{Sym}(\mathcal{SV}(c))$.

PREUVE. Comme h est un homomorphisme clos, les images de tous les sommets variables de c sont des sommets variables de c', d'où le résultat. ■

Nous montrons maintenant que l'ensemble des permutations σ telles que $h, v : c \trianglelefteq_\sigma c'$ est stable par composition.

Lemme 9.1.5 *Etant donnés deux contextes c et c', considérons σ et σ', deux éléments du groupe* $\mathrm{Sym}(\mathcal{SV}(c))$*, et supposons que $h, v : c \trianglelefteq_\sigma c'$ et $h, v : c \trianglelefteq_{\sigma'} c'$. Alors $h, v : c \trianglelefteq_{\sigma\sigma'} c'$.*

PREUVE. Si $w \in \mathcal{SV}(c)$, alors par hypothèse, il existe un isomorphisme η de $c'|h(w)$ vers $c'|h(w^\sigma)$, et il existe également un isomorphisme η' de $c'|h(w^\sigma)$ vers $c'|h((w^\sigma)^{\sigma'})$. Donc, d'après la Propriété 5.2.4, $\eta' \circ \eta$ est un isomorphisme de $c'|h(w)$ vers $c'|h(w^{\sigma\sigma'})$, ce qui prouve le résultat. ■

Corollaire 9.1.6 *Soient c et c' deux contextes, soit C un sous-ensemble de* $\mathrm{Sym}(\mathcal{SV}(c))$*, et supposons que pour tout $\sigma \in C$, on a $h, v : c \trianglelefteq_\sigma c'$ pour un sommet v et un homomorphisme h donnés. Si G est le groupe engendré par C, alors $c \trianglelefteq_G c'$.*

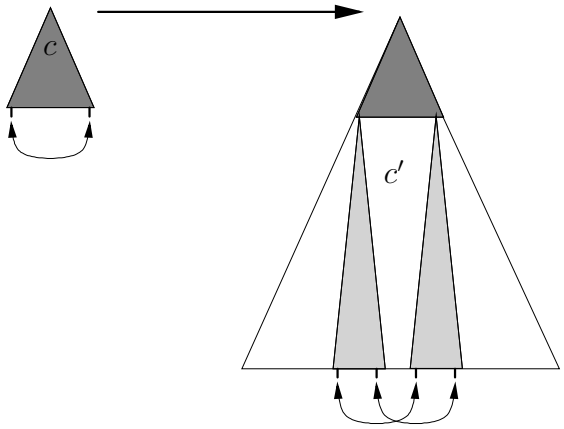

FIG. 9.1 – Principe des permutations induites

Reprenons l'Exemple 9.1.3 et le terme $t = f(g(x,y), g(w,z))$. Après application de l'équation permutative $f(x,y) \rightleftharpoons f(y,x)$ à la racine de t, on obtient le terme $t' = f(g(w,z), g(x,y))$, et l'équation $t \rightleftharpoons t'$ est une équation permutative de contexte associé c', et dont la permutation associée est celle qui intervertit la première variable de $t|1$ avec celle de $t|2$, et la deuxième variable de $t|1$ avec celle de $t|2$.

Dans le cas général, si pour un sommet p de c', on a $h, p : c \trianglelefteq_\sigma c'$, alors pour tout sommet variable v de c, la permutation induite par l'application de l'équation permutative $c \rightleftharpoons c^\sigma$ à la racine de c' associe le premier sommet variable de $c'|h(v^\sigma)$ au premier sommet variable de $c'|h(v)$, le deuxième sommet variable de $c'|h(v^\sigma)$ au deuxième sommet variable de $c'|h(v)$, et ainsi de suite. Le principe dans le cas général est représenté dans la Figure 9.1.

Définition 9.1.7 Soient c et c' deux contextes, h un automorphisme et v un sommet de c' tels que $h, v : c \trianglelefteq_\sigma c'$ pour une permutation $\sigma \in \mathrm{Sym}(\mathcal{SV}(c))$ donnée. On note r' la racine de c', et on définit la permutation $\Phi[c, c', v](\sigma) \in \mathrm{Sym}(\mathcal{SV}(c'))$ de la façon suivante : pour tout sommet $w \in \mathcal{SV}(c')$, on soit p (l'unique) chemin de r' à w dans c'.

- S'il existe un sommet variable u de c tel que $h(u)$ apparaît dans p, alors on pose $p = p_1.p_2$, où p_1 est le chemin de r' à $h(u)$ dans c', et p_2 est le chemin de $h(u)$ à w dans c' (p_2 peut éventuellement être vide). Si η est l'isomorphisme de $c'|h(u)$ vers $c'|h(u^\sigma)$, alors $\eta(p_2)$ est le chemin de $h(u^\sigma)$ à un sommet variable w' de c', et on définit
$$w^{\Phi[c,c',v](\sigma)} = w'.$$
- Sinon, on pose $w^{\Phi[c,c',v](\sigma)} = w$. ◇

Exemple 9.1.8 Soient c et c' deux contextes tels que $\tau(c) = f(\circ,\circ,\circ,\circ)$ et $\tau(c') = f(g(\circ,\circ),g(\circ,\circ),\circ,\circ)$, et soit $\sigma = (1\ 2)(3\ 4)$. La permutation σ est bien élément de $\mathrm{Sym}(\mathcal{SV}(c))$, et il est aisé de vérifier qu'il existe un homomorphisme h tel que $h,\varepsilon : c \trianglelefteq_\sigma c'$. On a alors

$$\Phi[c,c',\varepsilon](\sigma) = (1.1\ 2.1)(1.2\ 2.2)(3\ 4).$$

La fonction $\Phi[c,c',\varepsilon]$ est bien définie, et vérifie la propriété suivante :

Propriété 9.1.9 *$\Phi[c,c',\varepsilon]$ est un morphisme de groupes.*

PREUVE. Soient c et c' deux contextes, σ et σ' deux éléments de $\mathrm{Sym}(\mathcal{SV}(c))$, et supposons que $h,v : c \trianglelefteq_\sigma c'$, et $h,v : c \trianglelefteq_{\sigma'} c'$. Alors, d'après le Lemme 9.1.5, on a $h,v : c \trianglelefteq_{\sigma\sigma'} c'$, et on pose

$$\sigma_1 = \Phi[c,c',v](\sigma),\ \sigma_2 = \Phi[c,c',v](\sigma'),\ \text{et}\ \sigma_3 = \Phi[c,c',v](\sigma\sigma').$$

Il s'agit de prouver que $\sigma_3 = \sigma_1\sigma_2$.

Soit w un sommet variable de c', p le chemin de la racine de c' à w, et supposons qu'il existe un sommet $u \in \mathcal{SV}(c)$ tel que $h(u)$ apparaît dans p. On pose alors $p = p_1.p_2$, où p_1 est le chemin de la racine de c' à $h(u)$, et p_2 est le chemin de $h(u)$ à w dans c'.

Par définition, si η est l'isomorphisme de $c'|h(u)$ vers $c'|h(u^\sigma)$, alors $\eta(p_2)$ est le chemin de $h(u^\sigma)$ à w^{σ_1} dans c', et si η' est l'isomorphisme de $c'|h(u^\sigma)$ vers $c'|h(u^{\sigma\sigma'})$, alors $\eta' \circ \eta$ est un homomorphisme de $c'|h(u)$ vers $c'|h(u^{\sigma\sigma'})$, et $\eta' \circ \eta(p_2)$ est le chemin de $h(u^{\sigma\sigma'})$ à $(w^{\sigma_1})^{\sigma_2}$ dans c'.

Notons η'' l'isomorphisme de $c'|h(u)$ vers $c'|h(u^{\sigma\sigma'})$, alors $\eta''(p_2)$ est le chemin de $h(u^{\sigma\sigma'})$ à w^{σ_3} dans c', et par unicité des homomorphismes (Corollaire 5.2.6), $\eta'' = \eta' \circ \eta$, on en déduit donc que $w^{\sigma_3} = w^{\sigma_1\sigma_2}$.

Si aucun des sommets apparaissant dans p n'est l'image par h d'un sommet variable de c, alors $w^{\sigma_1} = w^{\sigma_2} = w^{\sigma_3} = w$, et on a à nouveau $w^{\sigma_1\sigma_2} = w^{\sigma_3}$, ce qui prouve que $\sigma_3 = \sigma_1\sigma_2$. ∎

Nous démontrons maintenant que si $h,v : c \trianglelefteq_\sigma c'$ pour une permutation $\sigma \in \mathcal{SV}(c)$ donnée, alors l'équation permutative $c' \rightleftharpoons c'^{\Phi[c,c',v](\sigma)}$ est une conséquence logique de l'équation permutative $c \rightleftharpoons c^\sigma$.

Théorème 9.1.10 *Soient c et c' deux contextes, $\sigma \in \mathcal{SV}(c)$, et supposons qu'il existe un homomorphisme h et un sommet v tel que $h,v : c \trianglelefteq_\sigma c'$. Alors*

$$c \rightleftharpoons c^\sigma \ \models\ c' \rightleftharpoons c'^{\Phi[c,c',v](\sigma)}.$$

PREUVE. Voir Annexe A, page 199. ∎

Corollaire 9.1.11 *Soit Σ_E une signature stratifiée contenant des éléments $\langle f,c,G\rangle$ et $\langle f',c',G'\rangle$ tels qu'il existe un sommet w de c' et une permutation $\sigma \in G$ tels que $c \sqsubseteq_\sigma c'|w$, et $\sigma' = \Phi[c,c',w](\sigma) \in G'$.*

Soient T et T' deux GA*-termes stratifiés tels que :*

1. *il existe un isomorphisme* η *de* $\mathrm{dm}(T')$ *vers* $\mathrm{dm}(T)$,
2. *la racine* r' *de* T' *est étiquetée par le symbole* $\langle f', c', G' \rangle$,
3. *si* $u = \mathrm{h}_{[T',r']}(w)$, *alors* $\eta(u)$ *est étiqueté par* $\langle f, c, G \rangle$.

On pose $\delta = \sigma^{\mathrm{h}_{[T,\eta(u)]}}$ *et* $\delta' = \sigma'^{\mathrm{h}_{[T',r']}}$, *alors on a* $\mathrm{dm_r}(T^{\delta}) \stackrel{\circ}{=} \mathrm{dm_r}(T'^{\delta'})$.

Corollaire 9.1.12 *Soit* Σ_E *une signature stratifiée saturée contenant des éléments* $\langle f, c, G \rangle$ *et* $\langle f', c', G' \rangle$. *S'il existe un homomorphisme* h *et un sommet* v *tel que* $h, v : c \trianglelefteq c'$, *alors* $\Phi[c, c', v](G \cap \mathrm{A_c}(h))$ *est un sous-groupe de* G'.

PREUVE. D'après le Théorème 9.1.10, pour toute permutation $\sigma \in G \cap \mathrm{A_c}(h)$, la permutation $\Phi[c, c', v](\sigma)$ est élément de G' par hypothèse de saturation. Comme $\Phi[c, c', v]$ est un morphisme de groupes d'après la Propriété 9.1.9, on a le résultat. ■

9.2 Signatures stratifiées stables

Dans le chapitre précédent, nous avons pu réduire le problème G_CSTR vers le problème S_MEM grâce au fait que, pour un t_i donné, il peut exister plusieurs GA-termes T tels que $t_i \in \mathrm{S}[T]$. Dans notre démonstration, seules les racines des A-termes A_j considérés étaient étiquetées par des symboles de Σ_E, et nous nous sommes donc servis du fait qu'il existe plusieurs symboles d'une signature stratifiée qui peuvent étiqueter la racine d'un GA-terme stratifié T tel que $t_i \in \mathrm{S}[T]$. Dans ce qui suit, nous allons imposer une restriction aux signatures stratifiées considérées afin d'éliminer ce non déterminisme en nous servant de la notion de *stabilité*.

Définition 9.2.1 Si $C = \{A_1, \ldots, A_n\}$ est un ensemble de A-termes mutuellement unifiables, alors on note $\sqcup C$ l'unique contexte isomorphe au A-terme

$$c_1 \sqcup (c_2 \sqcup \ldots \sqcup (c_{n-1} \sqcup c_n) \ldots).$$

Par abus de notation, on pourra également noter ce contexte $c_1 \sqcup c_2 \sqcup \ldots \sqcup c_n$. ◇

Exemple 9.2.2 Soient c_1, c_2 et c_3 les contextes respectivement définis par :

$$\tau(c_1) = f(\circ, \circ, \circ, a),\ \tau(c_2) = f(g(\circ, a), \circ, \circ, \circ),\ \text{et}\ \tau(c_3) = f(\circ, h(\circ), b, a).$$

Alors le contexte $c = c_1 \sqcup c_2 \sqcup c_3$ est défini par

$$\tau(c) \ = \ f(g(\circ, a), h(\circ), b, a).$$

Nous démontrons quelques propriétés du contexte $\sqcup C$.

Propriété 9.2.3 *Soient* C *un ensemble de* A*-termes deux à deux unifiables,* $c = \sqcup C$, *et* A *un* A*-terme tel que* $A \sqsubseteq c$. *On pose* $C' = \{A \sqcup A' \mid A' \in C\}$, *alors* $\sqcup C' = c$.

PREUVE. Ceci est évident : comme $A \sqsubseteq c$, et $A' \sqsubseteq c$ pour tout $A' \in C$, alors $A \sqcup A' \sqsubseteq c$ d'après le Théorème 5.3.15, d'où $\sqcup C' \sqsubseteq c$. Comme $A' \sqsubseteq A \sqcup A'$ pour tout $A' \in C$, on a également $c \sqsubseteq \sqcup C'$, d'où l'égalité. ■

Lemme 9.2.4 *Soient C_1 et C_2 deux ensembles de* A*-termes deux à deux unifiables, et supposons que les contextes $c_1 = \sqcup C_1$ et $c_2 = \sqcup C_2$ sont unifiables. Posons $C_3 = C_1 \cup C_2$, alors $c_1 \sqcup c_2 = \sqcup C_3$.*

PREUVE. Le contexte $\sqcup C_3$ est bien défini, en effet, si $A_1 \in C_1$, alors $A_1 \sqsubseteq c_1 \sqcup c_2$, et par symétrie, pour tout A-terme $A_2 \in C_2$, on a également $A_2 \sqsubseteq c_1 \sqcup c_2$. Ceci prouve que les éléments de C_3 sont deux à deux unifiables, et $\sqcup C_3$ est bien défini. Soit $A \in C_3$, alors on a $A \sqsubseteq c_1 \sqcup c_2$, et d'après le Corollaire 5.3.24, $\sqcup C_3 \sqsubseteq c_1 \sqcup c_2$. Réciproquement, pour tout $A \in C_1$, on a $A \sqsubseteq \sqcup C_3$, et donc $c_1 \sqsubseteq \sqcup C_3$. Par symétrie, $c_2 \sqsubseteq \sqcup C_3$, et d'après le Théorème 5.3.15, on a $c_1 \sqcup c_2 \sqsubseteq \sqcup C_3$, d'où l'égalité. ■

Lemme 9.2.5 *Soit $C = \{c_1, \ldots, c_n\}$ un ensemble de contextes deux à deux unifiables, notons $c = \sqcup C$, et soit p un sommet non-variable de c. Alors il existe un contexte $c' \in C$ tel que p est un sommet non-variable de c. De plus, si on définit l'ensemble de contextes C' par :*

$$C' \ = \ \{c'|p \,|\, c' \in C \wedge p \textit{ est un sommet non-variable de } c'\},$$

alors $\sqcup C' \simeq c|p$.

PREUVE. Supposons que pour tout $c' \in C$, p n'est pas un sommet de c', ou p est un sommet variable de c'. Alors si c'' est le contexte obtenu à partir de c en étiquetant le sommet p de c par le symbole $\circ$, alors il est clair que $c'' \neq c$, et pour tout $c' \in C$, on a $c' \sqsubseteq c''$, ce qui contredit la définition du contexte $\sqcup C$.

Démontrons par induction sur la cardinalité de C' que $\sqcup C' \simeq c|p$. Si $|C'| = 1$, alors le résultat est évident. Supposons que le résultat soit vrai pour tout ensemble de cardinalité $k-1$, où $k \geq 2$, et que C' est de cardinalité k. On pose $C' = C'' \cup \{c'|p\}$. Soit $C_1 = C \setminus \{c'\}$, alors par hypothèse d'induction, si $c_1 = \sqcup C_1$, alors p est un sommet non-variable de c_1, et $\sqcup C'' \simeq c_1|p$. On a alors $c = c_1 \sqcup c'$, et d'après le Lemme 5.3.14, on a bien $\sqcup C' \simeq c|p$. ■

Définition 9.2.6 (Stabilité) Etant donnée une théorie permutative E définie par un ensemble d'axiomes, une signature stratifiée Σ_E est dite *stable* par rapport aux axiomes de E si et seulement si elle recouvre les axiomes de E, et que pour tout $\langle f, c, G\rangle, \langle f, c', G'\rangle \in \Sigma_E$, si c et c' sont unifiables, et si $c'' = c \sqcup c'$, alors il existe un élément $\langle f, c'', G''\rangle \in \Sigma_E$ tel que :

- $c \sqsubseteq_G c''$,
- $c' \sqsubseteq_{G'} c''$.

On pourra également dire que Σ_E est stable, sans préciser par rapport à quel ensemble d'axiomes.

Soit une théorie permutative E définie par un ensemble d'axiomes, cet ensemble d'axiomes est dit *stable* si et seulement s'il existe une signature stratifiée Σ_E qui recouvre ces axiomes et qui est stable. ◇

Exemple 9.2.7 Soit E la théorie définie par les axiomes suivants :

$$\begin{aligned} f(g(x_1,x_2),x_3,x_4) &\rightleftharpoons f(g(x_2,x_1),x_3,x_4),\\ f(g(x_1,x_2),x_3,x_4) &\rightleftharpoons f(g(x_1,x_2),x_4,x_3),\\ f(x_1,h(x_2,x_3),h(x_4,x_5)) &\rightleftharpoons f(x_1,h(x_4,x_3),h(x_2,x_5)). \end{aligned}$$

Notons $c = \text{arbre}(f(g(x_1,x_2),x_3,x_4))$, $c' = \text{arbre}(f(x_1,h(x_2,x_3),h(x_4,x_5)))$, et soient G et G' les groupes définis par

$$G = \text{Sym}(\{1.1,1.2\})\text{Sym}(\{2,3\}), \text{ et } G' = \text{Sym}(\{2.1,3.1\}),$$

alors la signature stratifiée $\Sigma_E = \{\langle f,c,G\rangle, \langle f,c',G'\rangle\}$ recouvre E.

Posons $c'' = c \sqcup c'$, alors on a $\tau(c'') = f(g(\circ,\circ),h(\circ,\circ),h(\circ,\circ))$, et il est aisé de vérifier que $c \sqsubseteq_G c''$ et $c' \sqsubseteq_{G'} c''$. Donc, la signature stratifiée

$$\Sigma'_E \;=\; \{\langle f,c,G\rangle, \langle f,c',G'\rangle, \langle f,c'',\mathrm{I}\rangle\}$$

est stable par rapport aux axiomes de E.

Exemple 9.2.8 Soit c un contexte, et considérons la théorie permutative E définie par un ensemble d'axiomes uniforme de la forme

$$A \;=\; \{c \rightleftharpoons c^{\sigma_i} \mid i = 1,\ldots,n\},$$

où pour tout $i = 1,\ldots,n$, $\sigma_i \in \mathcal{SV}(c)$. Si G est le groupe engendré par les $\sigma_i, i = 1,\ldots,n$, alors la signature stratifiée $\Sigma_E = \{\langle f,c,G\rangle\}$ est trivialement stable par rapport à cet axiome.

Cet exemple montre donc que toute théorie permutative définie par un ensemble d'axiomes uniforme est stable par rapport à cet ensemble d'axiomes.

Théorème 9.2.9 *Soit Σ_E une signature stratifiée saturée contenant deux éléments $\langle f,c,G\rangle$ et $\langle f,c',G'\rangle$ tels que $c \sqsubseteq_G c'$. Si T et T' sont deux* GA*-termes stratifiés dont les racines r et r' sont respectivement étiquetées par $\langle f,c,G\rangle$ et $\langle f,c',G'\rangle$, et vérifiant* $\mathrm{dm_r}(T) \stackrel{\circ}{=} \mathrm{dm_r}(T')$, *alors* $\mathrm{S}[T] \subseteq \mathrm{S}[T']$.

PREUVE. Soit $\sigma \in G$, on pose $\sigma' = \Phi[c,c',\varepsilon](\sigma)$, $\mu = \sigma^{\mathrm{h}_{[T,r]}}$, et $\mu' = \sigma'^{\mathrm{h}_{[T',r']}}$, σ' est alors élément de G' d'après le Corollaire 9.1.12, et donc, μ' est élément de $\mathcal{G}_{T'}(r')$. D'après le Corollaire 9.1.11, on a alors $\mathrm{dm_r}(T^\mu) \stackrel{\circ}{=} \mathrm{dm_r}(T'^{\mu'})$. Par définition, on a

$$\mathrm{S}[T] = \bigcup_{\mu \in \mathcal{G}_T(r)} \mathrm{S}[\mathrm{dm_r}(T^\mu)], \text{ et } \mathrm{S}[T'] = \bigcup_{\mu \in \mathcal{G}_{T'}(r')} \mathrm{S}[\mathrm{dm_r}(T'^{\mu'})],$$

et comme $\mathrm{dm_r}(T^\mu) \stackrel{\circ}{=} \mathrm{dm_r}(T'^{\mu'})$, d'après le Corollaire 6.6.11, on en déduit que $\mathrm{S}[\mathrm{dm_r}(T^\mu)] = \mathrm{S}[\mathrm{dm_r}(T'^{\mu'})]$, ce qui prouve qu'on a bien $\mathrm{S}[T] \subseteq \mathrm{S}[T']$. ∎

Le Théorème 9.2.9 montre que si une théorie permutative est définie par un ensemble d'axiomes stable, alors il est possible dans certains cas de rendre déterministe le choix du symbole qui étiquette la racine d'un GA-terme stratifié. Malheureusement, nous allons voir que la condition de stabilité ne permet pas à elle seule d'assurer que les théories considérées auront de bonnes propriétés pour faire de la déduction avec des GA-termes stratifiés.

Dans ce qui suit, nous allons voir que le problème du mot généralisé modulo une théorie permutative est NP-dur, même en imposant que la théorie permutative soit définie par un ensemble d'axiomes stable. Le principe de la démonstration nous permettra également de prouver que le problème de rendre saturée une signature stratifiée stable est lui aussi NP-dur. Puis nous démontrerons que le problème de l'unification est infinitaire pour les théories permutatives définies par des ensembles d'axiomes stables. Ces résultats justifieront que les restrictions additionnelles que nous imposerons aux théories permutatives à considérer sont assez fortes.

9.3 Le problème du mot généralisé

Dans cette partie, nous allons montrer que le problème du mot généralisé modulo une théorie permutative définie par un ensemble d'axiomes uniforme est NP-dur. Pour cela, nous allons effectuer une réduction de Turing polynomiale du problème GC_PART_RST vers ce problème.

Prenons une instance de GC_PART_RST, c'est-à-dire un sous-groupe G de $\mathrm{Sym}(n)$, des ensembles $J_1, \ldots, J_n$ inclus dans $\{1, \ldots, n\}$ tous non-vides et deux à deux disjoints ou égaux, et un entier k compris entre 1 et n. On cherche donc à déterminer s'il existe une permutation $\theta \in G$ telle que pour tout $i \in \{1, \ldots, k\}$, $i^\theta \in J_i$.

Pour résoudre ce problème, on considère une signature Σ telle que l'ensemble $\{f, h, a_1, \ldots, a_n\}$ est inclus dans Σ, où f est d'arité 6, h est d'arité n et les a_i sont des constantes pour tout i. On définit les contextes c_h, c'_h et c_f, ainsi que le terme t_h par :

$$\begin{array}{rclcrcl} \tau(c_h) & = & h(\circ, \ldots, \circ), & & \tau(c_f) & = & f(\circ, \circ, c_h, c_h, \circ, \circ), \\ \tau(c'_h) & = & h(b_1, \ldots, b_k, \circ, \ldots, \circ), & & t_h & = & h(d_1, \ldots, d_n), \end{array}$$

où les b_i et les d_j pour $i = 1, \ldots, k$ et $j = 1, \ldots, n$ sont définis par :

$$\begin{array}{l} \text{soit } l = \min\{q \mid J_i = J_q\}, \quad \text{alors} \quad b_i = a_l; \\ \text{soit } l' = \min\{q \mid j \in J_q\}, \quad \text{alors} \quad d_j = a_{l'}. \end{array}$$

Exemple 9.3.1 Supposons que $n = 3$, $k = 2$, et posons $J_1 = \{2\}$, $J_2 = \{1\}$, et $J_3 = \{3\}$. Alors :

$$\begin{array}{rclcrcl} \tau(c_h) & = & h(\circ, \circ, \circ), & & \tau(c_f) & = & f(\circ, \circ, h(\circ, \circ, \circ), h(\circ, \circ, \circ), \circ, \circ), \\ \tau(c'_h) & = & h(a_1, a_2, \circ), & & t_h & = & h(a_2, a_1, a_3). \end{array}$$

Nous définissons maintenant une théorie permutative E uniforme :

Définition 9.3.2 Soit c le contexte tel que $\tau(c) = f(c_f, \circ, c_h, c'_h, \circ, \circ)$, soient les permutations suivantes :

$$\begin{aligned} \mu_1 &= (1.5\ 1.6), \\ \mu_2 &= (1.1\ 2), \\ \delta &= \prod_{i=1}^{n} (3.i\ 1.4.i), \end{aligned}$$

et notons $\{\delta_1, \ldots, \delta_m\}$ un ensemble de générateurs pour le groupe $3.G$ (voir la Définition 3.4.15).

On considère la théorie permutative E définie par l'ensemble d'axiomes

$$\{c \rightleftharpoons c^{\delta}\} \ \cup \ \{c \rightleftharpoons c^{\mu_i} \mid i = 1, 2\} \ \cup \ \{c \rightleftharpoons c^{\delta_i} \mid i = 1, \ldots, m\},$$

et on note G_c le groupe engendré par les permutations qui apparaissent dans les axiomes de E. ◇

Exemple 9.3.3 Dans la suite de l'Exemple 9.3.1, supposons que $G = \mathrm{Sym}(2)$. Alors :

$$3.G = \mathrm{Sym}(\{3.1, 3.2\}), \text{ et } \delta = (3.1\ 1.4.1)(3.2\ 1.4.2)(3.3\ 1.4.3).$$

On a la propriété suivante :

Propriété 9.3.4 *Soit G' le groupe engendré par $\{\delta, \delta_1, \ldots, \delta_n\}$, alors toute permutation de G_c est de la forme $\lambda_1\lambda_2\tau$, où*
- $\lambda_1 \in \mathrm{Sym}(\{1.5, 1.6\})$,
- $\lambda_2 \in \mathrm{Sym}(\{1.1, 2\})$,
- $\tau \in G'$.

Soit c' le contexte tel que $\tau(c') = f(c_f, c_f, t_h, c'_h, \circ, \circ)$, et soit $\sigma = (2.5\ 2.6)$. Dans ce qui suit, nous allons prouver que l'équation permutative $c' \rightleftharpoons c'^{\sigma}$ est élément de E si et seulement s'il existe une solution à l'instance de GC_PART_RST considérée.

Un exemple détaillé

Reprenons l'Exemple 9.3.1, où $n = 3$, et soit

$$t = f(t_f,\ t'_f,\ h(a_2, a_1, a_3),\ h(a_1, a_2, x_{21}),\ x_{22},\ x_{23}),$$

où :

$$\begin{aligned} t_f &= f(x_1,\ x_2,\ h(x_3, x_4, x_5),\ h(x_6, x_7, x_8),\ x_9,\ x_{10}), \\ t'_f &= f(x_{11},\ x_{12},\ h(x_{13}, x_{14}, x_{15}),\ h(x_{16}, x_{17}, x_{18}),\ x_{19},\ x_{20}), \end{aligned}$$

et pour tout $i = 1, \ldots, 23$, x_i est une variable ; on a donc $c' = \mathrm{arbre}(t)$. On pose $\mu = (3.1\ 3.2) \in 3.G$, et soit t_1 le terme obtenu à partir de t après application de l'équation permutative $c \rightleftharpoons c^{\mu}$ à la racine de t. On a donc

$$t_1 = f(t_f,\ t'_f,\ h(a_1, a_2, a_3),\ h(a_1, a_2, x_{21}),\ x_{22},\ x_{23}).$$

Après avoir appliqué l'équation $c \rightleftharpoons c^{\mu_2}$ à la racine de t_1, on obtient un terme t_2 dont le sous-terme à la position 1 est

$$t_2|1 = f(t'_f,\ x_2,\ h(x_3, x_4, x_5),\ h(x_6, x_7, x_8),\ x_9,\ x_{10}).$$

Enfin, en appliquant l'équation $c \rightleftharpoons c^{\delta}$ à la racine de t_2, on obtient le terme t_3 dont le sous-terme à la position 1 est :

$$t_3|1 = f(t'_f,\ x_2,\ h(x_3, x_4, x_5),\ h(a_1, a_2, a_3),\ x_9,\ x_{10}).$$

Donc, $t_3|1$ est une instance de c, et on peut donc appliquer l'équation permutative $c \rightleftharpoons c^{\mu_1}$ à la position 1 de t_3, on obtient le terme t_4 dont le sous-terme à la position 1 est

$$t_4|1 = f(t''_f,\ x_2,\ h(x_3, x_4, x_5),\ h(a_1, a_2, a_3),\ x_9,\ x_{10}),$$

où

$$t''_f = f(x_{11},\ x_{12},\ h(x_{13}, x_{14}, x_{15}),\ h(x_{16}, x_{17}, x_{18}),\ x_{20},\ x_{19}).$$

La seule différence entre les termes t'_f et t''_f est donc que les positions des variables x_{19} et x_{20} sont interverties. En appliquant successivement aux racines de t_4 puis des autres termes obtenus les équations permutatives $c \rightleftharpoons c^{\delta}$, $c \rightleftharpoons c^{\mu_1}$ et $c \rightleftharpoons c^{\mu}$, on obtient le terme

$$t' = f(t_f,\ t''_f,\ h(a_1, a_2, a_3),\ h(a_2, a_1, x_{21}),\ x_{22},\ x_{23}).$$

Il est alors aisé de vérifier que l'équation $t \rightleftharpoons t'$ est une équation permutative de contexte associé c', et de permutation associée $(2.5\ 2.6) = \sigma$. Donc, $c' \rightleftharpoons c'^{\sigma}$ est une conséquence de E, et ceci est dû au fait que, comme la permutation μ est élément de $3.G$, alors $\theta = (1\ 2) \in G$, et pour $i = 1, 2$, $i^{\theta} \in J_i$.

Cas général

Nous allons maintenant montrer le résultat dans le cas général. Pour plus de lisibilité, nous utiliserons les mêmes notations que dans l'exemple précédent ; par exemple, on aura :

$$t_f \ = \ f(x_1,\ x_2,\ h(x_3, \ldots, x_{n+2}),\ h(x_{n+3}, \ldots, x_{2n+2}),\ x_{2n+3},\ x_{2n+4}).$$

Supposons que l'équation permutative $c' \rightleftharpoons c'^{\sigma}$ est élément de E. Comme t est une instance de c à la racine et nulle part ailleurs, et que toutes les permutations de G_c fixent les positions 2.5 et 2.6, nécessairement, il doit exister une permutation $\lambda \in G_c$ telle que l'application de l'équation $c \rightleftharpoons c^{\lambda}$ à la racine de t produit un terme t_1 qui est évidemment instance de c à la racine, mais qui possède un sous-terme strict qui est également instance de c.

Il y a deux sous-termes stricts de t dont le symbole de tête est f, $t|1$ et $t|2$, et aucun d'entre eux n'est une instance de c, donc, si un sous-terme strict de t_1 est une instance de c, ce sous-terme est nécessairement $t'_1 = t_1|1$, puisque le sommet 2 est un sommet variable de c. En particulier, si t'_1 est instance de c, alors pour tout $i = 1, \ldots, k$, on

doit avoir $t'_1|4.i = b_i$. Or, $t'_1|4.i = t_1|1.4.i$, et comme les sommets $1.4.i$ sont des sommets variables de c pour tout i, on en déduit que nécessairement,

$$t'_1|4.i \;=\; t_1|1.4.i \;=\; t|(1.4.i)^\lambda \;=\; b_i.$$

Posons $A = \{1.4.j \mid j = 1, \ldots, n\}$, et $B = \{3.k \mid k = 1, \ldots, n\}$, alors, par définition des groupes G_c et G', on a

$$(1.4.i)^{G_c} = (1.4.i)^{G'} \subseteq A \cup B.$$

Comme les seuls sous-termes de la forme $t|p$ pour $p \in A$ à pouvoir être identiques aux b_i sont les d_j, nécessairement, pour tout $i = 1, \ldots, k$, il existe un entier j_i tel que $t|(1.4.i)^\lambda = t|3.j_i = d_{j_i} = b_i$.

D'après la Propriété 9.3.4, on a $\lambda = \lambda_1\lambda_2\tau$, et donc, par hypothèse, $(1.4.i)^\tau = 3.j_i$. D'après le Théorème 3.4.12, on en déduit qu'il existe une permutation $\mu \in 3.G$ telle que pour tout $i = 1, \ldots, k$, $(3.i)^\mu = 3.j_i$, c'est-à-dire une permutation $\theta \in G$ telle que pour tout $i = 1, \ldots, k$, $i^\theta = j_i$. Posons $d_{j_i} = b_i = a_l$, alors, par définition, on a $i^\theta = j_i \in J_l$ et $J_l = J_i$, d'où $i^\theta \in J_i$. On a donc prouvé que si $c' \rightleftharpoons c'^\sigma$ est une conséquence de E, alors il existe une permutation $\theta \in G$ telle que pour tout $i = 1, \ldots, k$, $i^\theta \in J_i$.

Réciproquement, supposons qu'il existe une permutation $\theta \in G$ telle que pour tout $i = 1, \ldots, k$, $i^\theta \in J_i$. Prenons t comme précédement, et soit τ la permutation dans $3.G$ telle que pour tout $i = 1, \ldots, k$, $(3.i)^\tau = 3.(i^\sigma)$. Alors, après application de l'équation $c \rightleftharpoons c^\tau$ à la racine de t, on obtient le terme t_1 qui est tel que, pour tout $i \in \{1, \ldots, k\}$, $t_1|3.i = t|3.(i^\sigma)$. Posons $a_l = t|3.(i^\sigma)$, on a donc $i^\sigma \in J_l$, et comme $i^\sigma \in J_i$, on en déduit que $J_l = J_i$ et que $t|4.i = b_i = a_l$. Ceci prouve qu'après appliquation de l'équation $c \rightleftharpoons c^{\mu_2}$ à la racine de t_1, on obtient un terme t_2 tel que $t_2|1.4.1 = t'_f$. Enfin, après application de $c \rightleftharpoons c^\delta$ à la racine de t_2, on obtient le terme t_3 qui est tel que le sous-terme $t'_3 = t_3|1$ est instance de c à la racine. On peut donc appliquer la permutation $c \rightleftharpoons c_1^\mu$ à $t_3|1$ et ainsi obtenir un terme t_4, puis successivement appliquer les permutations $c \rightleftharpoons c^\delta$, $c \rightleftharpoons c^{\mu_2}$ et $c \rightleftharpoons c^{\tau^{-1}}$ aux racines de t_4 et des autres termes obtenus. On obtient un terme t' qui est identique à t sauf que les variables aux positions 2.5 et 2.6 sont interverties. On en déduit que l'équation permutative $c' \rightleftharpoons c'^\sigma$ est élément de E.

Ainsi, n'importe quelle instance du problème GC_PART_RST peut-être résolue en prenant le problème du mot généralisé pour une théorie permutative défini par un ensemble d'axiomes uniforme pour oracle. Les tailles des contextes c et c', ainsi que celle du terme t' sont évidemment polynomiales en n, et le nombre d'équations dans la théorie E est linéaire en le nombre de générateurs de G, c'est-à-dire polynomial en n. Ceci prouve que la transformation de l'instance de GC_PART_RST en celle du problème du mot généralisé pour une théorie permutative définie par un ensemble d'axiomes uniforme est polynomiale, et qu'on a donc une réduction de Turing polynomiale de GC_PART_RST vers ce problème. On en déduit donc que :

Corollaire 9.3.5 *Le problème du mot généralisé pour une théorie permutative uniforme est* NP*-dur.*

Saturation d'une signature stratifiée stable

Nous pouvons aisément adapter la démonstration précédente pour prouver qu'il est difficile de construire une signature stratifiée stable qui est saturée. Pour cela, nous allons étudier le problème suivant :

> **Problème**: Complétude des groupes, ou GRP_COMPL.
> **Entrée**: Une signature stratifiée Σ_E stable, un élément $\langle f', c', G' \rangle \in \Sigma_E$, et une permutation $\sigma \in \mathcal{SV}(c')$.
> **Question**: Est-ce que l'équation permutative $c' \rightleftharpoons c'^{\sigma}$ est élément de E ?

Il est évident que si nous pouvons rendre Σ_E saturée, alors il suffit de tester en temps polynomial si $\sigma \in G'$. Nous allons démontrer que ce problème est **NP**-dur, même si Σ_E ne contient que deux éléments. Il suffit pour cela de reprendre le contexte c et le groupe G_c de la Définition 9.3.2, et de définir le contexte c'' tel que

$$\tau(c'') = g(f(c_f, c_f, t_h, c'_h, \circ, \circ));$$

on a donc $\tau(c''|1) = \tau(c')$. Soit $\Sigma'_E = \{\langle f, c, G_c \rangle, \langle g, c'', \mathrm{I} \rangle\}$, comme c et c'' ne sont pas unifiables à la racine, Σ'_E est trivialement stable. On pose $\sigma' = (1.2.5\ 1.2.6) \in \mathcal{SV}(c'')$, il est clair que l'équation $c'' \rightleftharpoons c''^{\sigma'}$ est élément de E si et seulement si l'équation $c' \rightleftharpoons c'^{\sigma}$ est également élément de E ; on a donc le résultat suivant :

Corollaire 9.3.6 *Le problème* GRP_COMPL *est* **NP**-*dur pour une signature stratifiée stable, et donc, le problème de la construction d'une signature stratifiée saturée est également* **NP**-*dur, même pour une signature stratifiée stable.*

9.4 Un problème d'unification de type infinitaire

Dans cette partie, nous allons étudier le problème de l'unification dans une théorie permutative définie par un ensemble d'axiomes stable. Il a d'abord été conjecturé dans [Jou87] que le problème de l'unification dans une théorie permutative était de type finitaire, ce qui a été infirmé par Schmidt-Schauß dans [SS88]. La théorie permutative employée dans [SS88] n'est pas définie par un ensemble d'axiomes stable, mais dans [KK90], Kirchner et Klay ont montré qu'il existe des théories permutatives définies par un unique axiome pour lesquelles l'unification est de type infinitaire. Dans ce qui suit, nous allons donner l'exemple d'une théorie permutative particulièrement simple, définie par un unique axiome, et exhiber un problème d'unification possédant un CSU minimal de cardinalité infinie.

Soit $\Sigma = \{f\}$, où f est un symbole de fonction d'arité 2, E la théorie définie par l'axiome suivant :

$$e : \ f(f(x,y),z) \ \rightleftharpoons \ f(f(y,x),z),$$

et S le problème d'unification élémentaire suivant :

$$S \ = \ \{f(x_1, x_2) =^{?}_{E} f(x_3, x_2)\}.$$

Nous allons prouver que tout CSU minimal pour S contient nécessairement une infinité d'unificateurs. Pour démontrer cela, nous allons construire un ensemble infini d'unificateurs et prouver que chacun d'entre eux est le plus général possible. Nous commençons par prouver certaines propriétés vérifiées par la théorie E.

Définition 9.4.1 Soit s un terme, u_1 et u_2 deux variables, et définissons les ensembles suivants :

$$\begin{aligned} \mathcal{S}_1 &= \{f(f(u_1, s'), u_2) \mid f(s', u_1) =_E f(s, u_1)\}, \\ \mathcal{S}_2 &= \{f(f(s', u_1), u_2) \mid f(s', u_1) =_E f(s, u_1)\}. \end{aligned}$$

On définit également l'ensemble $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2$. ◇

Lemme 9.4.2 *L'ensemble $\mathcal{S}$ est fermé sous $\leftrightarrow_E$.*

PREUVE. Soit $t = f(f(u_1, s'), u_2)$ un élément de $\mathcal{S}_1$, et supposons que $t \leftrightarrow_E t'$, alors l'équation e peut être appliquée
- à la racine de t,
- en-dessous de la position 1.2 dans t.

t' peut donc prendre deux formes :

$$\begin{aligned} t' &= f(f(s', u_1), u_2), \\ t' &= f(f(u_1, s''), u_2), \text{ où } s' \leftrightarrow_E s''. \end{aligned}$$

Dans le premier cas, $t' \in \mathcal{S}_2$, et dans le deuxième, $t' \in \mathcal{S}_1$.

Supposons que $t = f(f(s', u_1), u_2)$ est un élément de $\mathcal{S}_2$, et supposons que $t \leftrightarrow_E t'$, alors on peut appliquer l'équation e à la racine ou en-dessous de la position 1 de t ; t' peut donc prendre deux formes :

$$\begin{aligned} t' &= f(f(u_1, s'), u_2), \\ t' &= f(f(s'', u_1), u_2), \text{ où } f(s', u_1) \leftrightarrow_E f(s'', u_1). \end{aligned}$$

Dans le premier cas, $t' \in \mathcal{S}_1$, et dans le deuxième, $t' \in \mathcal{S}_2$, et on a le résultat. ■

Théorème 9.4.3 *Sous les hypothèses du Lemme 9.4.2, si $t = f(f(u_1, s), u_2)$, alors $[t]_E = \mathcal{S}$.*

PREUVE. Comme $t \in \mathcal{S}$, le Lemme 9.4.2 prouve que $[t]_E \subseteq \mathcal{S}$. Nous prouvons maintenant qu'on a également l'inclusion réciproque. Soit $t' \in \mathcal{S}$, si $t' \in \mathcal{S}_1$, alors t' est de la forme $f(f(u_1, s'), u_2)$, et on a :

$$\begin{aligned} f(f(u_1, s'), u_2) &=_E f(f(s', u_1), u_2) \\ &=_E f(f(s, u_1), u_2) \\ &=_E f(f(u_1, s), u_2). \end{aligned}$$

Il est aisé de vérifier que si $t' \in \mathcal{S}_2$, alors on a également $t' =_E t$, donc $\mathcal{S} \subseteq [t]_E$ et on a l'égalité. ■

Corollaire 9.4.4 *Soient s_1, s_2 des termes, et u_1, u_2 et y des variables. Alors*

$$f(f(u_1, s_1), y) =_E f(f(u_2, s_2), y)$$

si et seulement si

$$\begin{array}{lll} u_1 = u_2 & et & f(s_1, u_1) =_E f(s_2, u_1) \\ & ou & \\ u_1 = s_2 & et & s_1 = u_2. \end{array}$$

Définition 9.4.5 Soit $U = \{u_i \mid i \in \mathbb{N}\}$ un ensemble dénombrable de variables. On définit inductivement l'ensemble de termes suivant :

$$\begin{array}{rcl} t_1 & = & f(u_0, u_1), \\ t_i & = & f(u_i, t_{i-1}) \quad \text{si } i \geq 2. \end{array}$$ ◇

Lemme 9.4.6 *Pour tout $i \in \mathbb{N}^*$, et tout renommage θ, on a $[t_i\theta]_E = \{t_i\theta\}$.*

PREUVE. On démontre le résultat par induction sur i. Le résultat est évident pour $i = 1$, supposons maintenant que le résultat est vrai pour $i = k - 1$, où $k \geq 2$. Alors $t_i\theta = f(u_i\theta, t_{i-1}\theta)$, et on ne peut donc pas appliquer l'équation e à la racine de ce terme. Par hypothèse d'induction, on a $[t_{i-1}\theta]_E = \{t_{i-1}\theta\}$, d'où le résultat. ■

Lemme 9.4.7 *Considérons le renommage $\tau = (u_1\ u_0)$, alors pour tout $i \geq 1$ et pour toute variable y, on a $f(t_i, y) =_E f(t_i\tau, y)$.*

PREUVE. On démontre le résultat par induction sur i. Pour $i = 1$, en appliquant l'équation e à la racine, on a

$$f(f(u_1, u_0), y) =_E f(f(u_0, u_1), y).$$

Supposons maintenant que le résultat est vrai pour $i = k - 1$, pour $k \geq 2$, alors on a $f(t_k, y) = f(f(u_k, t_{k-1}), y)$, et par hypothèse d'induction, on a

$$f(t_{k-1}, y) =_E f(t_{k-1}\tau, y),$$

pour toute variable y. On a donc

$$\begin{array}{rcl} f(t_k, y) & = & f(f(u_k, t_{k-1}), y)) \\ & =_E & f(f(t_{k-1}, u_k), y) \\ & =_E & f(f(t_{k-1}\tau, u_k), y) \\ & =_E & f(f(u_k, t_{k-1}\tau), y) \\ & = & f(t_k\tau, y). \end{array}$$ ■

Théorème 9.4.8 *Pour tout $i \geq 1$, la substitution*

$$\theta_i = \{x_1 \leftarrow t_i, x_3 \leftarrow t_i\tau\}$$

est une solution au problème d'unification S.

PREUVE. Ce résultat est une conséquence immédiate du Lemme 9.4.7. ∎

Prouvons maintenant que les θ_i sont des solutions les plus générales possible.

Lemme 9.4.9 *Pour $i \geq 1$, supposons qu'il existe des termes t_a et t_b tels que :*

1. *$f(t_a, y) =_E f(t_b, y)$,*
2. *il existe une substitution θ telle que $t_a\theta =_E t_i$ et $t_b\theta =_E t_i\tau$.*

Alors on a $t_a = f(w_1, s_1)$ et $t_b = f(w_2, s_2)$, où les w_i sont des variables telles que $w_1\theta = w_2\theta = u_i$, et $s_1\theta = t_{i-1}$ et $s_2\theta = t_{i-1}\tau$.

PREUVE. Tout d'abord, d'après le Lemme 9.4.6, on a $t_a\theta = t_i$ et $t_b\theta = t_i\tau$; supposons maintenant que t_a est une variable. Alors, comme $f(t_a, y) =_E f(t_b, y)$, et qu'on ne peut alors pas appliquer l'équation e à la racine de $f(t_a, y)$, on en déduit que $f(t_a, y) = f(t_b, y)$, d'où $t_a = t_b$. On devrait donc avoir

$$t_i \;=\; t_a\theta \;=\; t_b\theta \;=\; t_i\tau,$$

ce qui est impossible. Donc, nécessairement, on a $t_a = f(s'_1, s_1)$, et par symétrie, $t_b = f(s'_2, s_2)$. Comme $s'_1\theta = u_i$, s'_1 est nécessairement une variable, et de même, s'_2 est une variable. Le terme t_a est donc de la forme $f(w_1, s_1)$, où w_1 est une variable, et t_b est de la forme $f(w_2, s_2)$, où w_2 est une variable. Enfin, puisque $t_a\theta = t_i$ et $t_b\theta = t_i\tau$, on a $w_1\theta = w_2\theta = u_i$, $s_1\theta = t_{i-1}$ et $s_2\theta = t_{i-1}\tau$. ∎

Lemme 9.4.10 *Sous les hypothèses du Lemme 9.4.9, la restriction de θ à $\mathrm{Var}(t_a) \cup \mathrm{Var}(t_b)$ est un renommage.*

PREUVE. On prouve le résultat par induction sur i. Pour $i = 1$, d'après le Lemme 9.4.9, on a :

$$w_1\theta = u_1,\ w_2\theta = u_0,\ s_1\theta = u_0 \text{ et } s_2\theta = u_1.$$

Comme $w_1\theta \neq w_2\theta$, on ne peut pas avoir $w_1 = w_2$, et donc, d'après le Corollaire 9.4.4, comme $f(t_a, y) =_E f(t_b, y)$, on a nécessairement

$$w_1 = s_2 \text{ et } w_2 = s_1.$$

Donc, la restriction de θ à $\mathrm{Var}(t_a) \cup \mathrm{Var}(t_b)$ est un renommage.

Supposons maintenant que le résultat soit vrai pour $i = k - 1$ pour $k \geq 2$, et que $t_a\theta =_E t_k$, et $t_b\theta =_E t_k\tau$. Alors, puisque $w_1\theta = u_k$ et $s_2\theta = t_{k-1}\tau$, on ne peut pas avoir $w_1 = s_2$, et d'après le Corollaire 9.4.4, on a nécessairement $w_1 = w_2$ et $f(s_1, w_1) =_E f(s_2, w_1)$. Soit θ' la restriction de θ aux variables qui apparaissent dans s_1 et s_2, alors, par hypothèse d'induction, θ' est un renommage. Comme $w_1\theta = u_k$, et que u_k n'apparaît pas dans t_{k-1}, ni dans $t_{k-1}\theta$, la restriction de θ aux variables qui apparaissent dans t_a et t_b est également un renommage. ∎

Théorème 9.4.11 *Pour tout $i \geq 1$, si μ est une substitution qui est solution de S et est plus générale que θ_i, alors il existe un renommage θ tel que $\mu\theta = \theta_i$.*

PREUVE. Supposons qu'une telle substitution existe, et soient t_a et t_b les images respectives de x_1 et x_3 par μ. Comme μ est plus générale que θ_i par hypothèse, il existe une substitution θ telle que $t_a\theta =_E t_i$, et $t_b\theta =_E t_i\tau$. D'après le Lemme 9.4.10, θ est alors un renommage. ■

Corollaire 9.4.12 *Tout CSU du problème S doit contenir tous les $\theta_i, i \geq 1$, à un renommage près.*

Corollaire 9.4.13 *E est de type infinitaire.*

Ainsi, l'hypothèse de stabilité des axiomes définissant une théorie permutative E n'est pas suffisante pour garantir que cette théorie est de type finitaire.

9.5 Résumé

Dans ce chapitre, nous avons cherché à imposer des restrictions aux théories permutatives considérées pour pouvoir faire de la déduction avec des GA-termes stratifiés de façon efficace. La condition de stabilité définie permet de résoudre certains problèmes de non déterminisme, mais nous avons vu que cette condition n'est pas suffisamment puissante pour garantir de bonnes propriétés de complexité. Ainsi, nous avons démontré que le problème du mot généralisé est NP-dur pour des théories permutatives définies par des ensembles d'axiomes stables, tout comme le problème de la construction d'une signature stratifiée stable et saturée. Puis, nous avons étudié des théories permutatives définies par des ensembles d'axiomes stables, et avons vu que même dans le cas où la théorie considérée est définie par un unique axiome, il existe des problèmes d'unification avec des CSU de cardinalité infinie.

Dans le prochain chapitre, nous allons donc imposer des restrictions supplémentaires aux théories étudiées afin d'éviter ces problèmes.

Chapitre 10

Unif-stabilité

Dans le chapitre précédent, nous avons vu que la condition de stabilité n'est pas suffisamment forte pour garantir que les théories considérées ont de bonnes propriétés pour faire de la déduction avec des GA-termes. Nous allons maintenant définir la notion d'unif-stabilité.

La condition de stabilité définie dans le chapitre précédent a été obtenue en imposant des restrictions aux contextes qui sont unifiables à leur racine. Dans les démonstrations de la NP-dureté du problème du mot généralisé, ou du type infinitaire de l'unification modulo des théories permutatives stables, nous nous sommes servis du fait qu'un contexte peut s'unifier avec un sous-contexte *strict*, et que la condition de stabilité n'impose aucune restriction dans ce cas là.

Dans ce chapitre, nous allons définir les signatures stratifiées *unif-stables*, ainsi que les ensembles d'axiomes *unif-stables*. Après avoir défini ces notions, nous donnerons plusieurs exemples de théories permutatives définies par des ensembles d'axiomes unif-stables. Et nous prouverons qu'il est possible de décider en temps polynomial si un ensemble d'axiomes est unif-stable ou non.

Grâce à cette notion d'unif-stabilité, pour tout terme t, nous pourrons construire en temps polynomial un GA-terme stratifié T tel que la classe de congruence de t modulo E est égale à $\mathrm{S}[T]$. Enfin, nous étudierons les complexités des problèmes liés à la déduction définis dans le Chapitre 8, ainsi que celle du problème du mot généralisé modulo une théorie permutative définie par un ensemble d'axiomes unif-stable, et prouverons que ces problèmes sont tous dans la classe de Luks.

10.1 Théories unif-stables

Définition 10.1.1 (Unif-stabilité) Etant donnée une théorie permutative E définie par un ensemble d'axiomes, une signature stratifiée Σ_E est dite *unif-stable par rapport aux axiomes de* E si et seulement si :

- Σ_E est stable,
- pour toute paire $\langle f, c, G\rangle, \langle f', c', G'\rangle$ d'éléments de Σ_E, s'il existe un sommet non-variable $p \neq \varepsilon$ tel que c et $c'|p$ sont unifiables, alors $c \sqsubseteq_G c'|p$.

Un ensemble d'axiomes définissant une théorie permutative est dit *unif-stable* si et seulement s'il existe une signature stratifiée qui est unif-stable par rapport à ces axiomes. ◇

Exemple 10.1.2 Soit E la théorie permutative définie par les axiomes suivants :

$$\begin{aligned} f(x_1, x_2) &\rightleftharpoons f(x_2, x_1) \\ g(x_1, x_2) &\rightleftharpoons g(x_2, x_1) \\ f(g(x_1, x_2), g(x_3, x_4)) &\rightleftharpoons f(g(x_3, x_2), g(x_1, x_4)). \end{aligned}$$

On définit les contextes c, c' et c'' tels que $\tau(c) = f(\circ, \circ)$, $\tau(c') = g(\circ, \circ)$ et $\tau(c'') = f(g(\circ, \circ), g(\circ, \circ))$. Alors la signature stratifiée

$$\Sigma_E \;=\; \{\langle f, c, \mathrm{Sym}(2)\rangle, \langle g, c', \mathrm{Sym}(2)\rangle, \langle f, c'', \mathrm{Sym}(\{1.1, 2.1\})\rangle\}$$

est stable par rapport aux axiomes E. Comme $c' \simeq c''|1$ et $c' \simeq c''|2$, d'après la Propriété 9.1.4, on a

$$c' \sqsubseteq_{\mathrm{Sym}(2)} c''|1 \text{ et } c' \sqsubseteq_{\mathrm{Sym}(2)} c''|2,$$

ce qui prouve que Σ_E est unif-stable par rapport aux axiomes de E.

Nous allons présenter deux exemples de théories définies par des ensembles d'axiomes unif-stables : les théories *plates*, qui ont été mentionnées dans [AP01], et étudiées plus en détail dans [Ave04], et les théories *pseudo-orthogonales*, introduites dans [BdlTE04a].

Définition 10.1.3 (Signature stratifiée plate) Un contexte c est dit *plat* si et seulement si $\tau(c)$ est de la forme $f(\circ, \ldots, \circ)$. Une signature stratifiée Σ_E est dite plate si et seulement si pour tout $\langle f, c, G\rangle \in \Sigma_E$, le contexte c est plat. Un ensemble d'axiomes définissant une théorie permutative est dit *plat* si et seulement s'il existe une signature stratifiée qui recouvre ces axiomes et qui est plate. ◇

Exemple 10.1.4 Soit E la théorie équationnelle définie par les axiomes suivants :

$$\begin{aligned} f(x_1, x_2, x_3) &\rightleftharpoons f(x_2, x_1, x_3) \\ f(x_1, x_2, x_3) &\rightleftharpoons f(x_3, x_2, x_1) \\ g(x_1, x_2) &\rightleftharpoons g(x_2, x_1). \end{aligned}$$

Les contextes c et c' tels que $\tau(c) = f(\circ, \circ, \circ)$ et $\tau(c') = g(\circ, \circ)$ sont plats, et la signature stratifiée

$$\Sigma_E \;=\; \{\langle f, c, \mathrm{Sym}(3)\rangle, \langle g, c', \mathrm{Sym}(2)\rangle\}$$

est donc plate, et comme elle recouvre les axiomes de E, l'ensemble de ces axiomes est également plat.

Exemple 10.1.5 L'axiome de commutativité est trivialement plat. Par contre, l'axiome suivant :

$$f(x, y, a) \;\rightleftharpoons\; f(y, x, a),$$

où a est une constante, n'est pas plat.

Définition 10.1.6 (Pseudo-orthogonalité) Soit une signature stratifiée Σ_E, on dit que Σ_E est *pseudo-orthogonale* si et seulement si pour toute paire $\langle f, c, G\rangle$, $\langle f', c', G'\rangle$ d'éléments de Σ_E, si c est unifiable avec un sommet non-variable p de c', alors c et $c'|p$ sont isomorphes.

On dit qu'un ensemble d'axiomes définissant une théorie permutative est *pseudo-orthogonal* si et seulement s'il existe une signature stratifiée qui recouvre ces axiomes qui est pseudo-orthogonale. ◇

Exemple 10.1.7 Soit E la théorie permutative définie par les axiomes suivants :

$$\begin{aligned} f(g(x,y),z) &\rightleftharpoons f(g(y,x),z) \\ g(x,y) &\rightleftharpoons g(y,x). \end{aligned}$$

Posons $\tau(c) = f(g(\circ,\circ),\circ)$, $\tau(c') = g(\circ,\circ)$, et soit Σ_E est la signature stratifiée définie par

$$\Sigma_E = \{\langle f, c, \mathrm{Sym}(\{1.1, 1.2\})\rangle, \langle g, c', \mathrm{Sym}(2)\rangle\},$$

alors Σ_E est clairement pseudo-orthogonale, et donc, l'ensemble des axiomes définissant E est également pseudo-orthogonal.

Exemple 10.1.8 Nous avons vu dans l'Exemple 10.1.5 que l'axiome

$$f(x,y,a) \rightleftharpoons f(y,x,a)$$

n'est pas plat, par contre, cet axiome est trivialement pseudo-orthogonal.

Lemme 10.1.9 *Tout ensemble d'axiomes plat est pseudo-orthogonal.*

PREUVE. Soit un ensemble d'axiomes plat, et Σ_E une signature stratifiée plate qui recouvre ces axiomes. Si $\langle f, c, G\rangle$ et $\langle f', c', G'\rangle$ sont deux éléments de Σ_E, alors, le seul sommet non-variable de c' étant sa racine, nécessairement, si c et c' sont unifiables, alors ils sont isomorphes (et même égaux). Ceci prouve que la signature stratifiée Σ_E est bien pseudo-orthogonale, d'où le résultat. ■

Théorème 10.1.10 *Tout ensemble d'axiomes pseudo-orthogonal est unif-stable.*

PREUVE. Soit un ensemble d'axiomes pseudo-orthogonal, et Σ_E une signature stratifiée pseudo-orthogonale qui recouvre ces axiomes E. Soient $\langle f, c, G\rangle$ et $\langle f', c', G'\rangle$ deux éléments de Σ_E, et supposons que c est unifiable avec $c'|p$, pour un sommet non-variable p de c'. Alors c et $c'|p$ sont isomorphes par hypothèse de pseudo-orthogonalité, et donc, d'après la Propriété 9.1.4, $c \sqsubseteq_G c'|p$. La signature stratifiée Σ_E est donc unif-stable par rapport à l'ensemble d'axiomes, qui est bien unif-stable. ■

Définition 10.1.11 ($\Gamma_E(c')$) Soit E une théorie permutative définie par un ensemble d'axiomes, et soit Σ_E une signature stratifiée qui recouvre les axiomes de E. On définit l'ensemble

$$C = \{\langle f, c, G\rangle \in \Sigma_E \mid c \text{ est un contexte axiomatique de } E\},$$

et, pour tout contexte c', on définit le groupe $\Gamma_E(c')$ engendré par

$$\bigcup\{\Phi[c, c', p](G) \mid \langle f, c, G\rangle \in C \ \wedge \ h, p : c \trianglelefteq_G c'\}. \qquad \diamond$$

Exemple 10.1.12 Soit E la théorie permutative définie par les axiomes suivants :

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &\rightleftharpoons f(x_2, x_1, x_3, x_4) \\ g(x_1, x_2) &\rightleftharpoons g(x_2, x_1). \end{aligned}$$

On définit les contextes c et c' tels que $\tau(c) = f(\circ, \circ, \circ, \circ)$ et $\tau(c') = g(\circ, \circ)$, et on pose

$$\Sigma_E \ = \ \{\langle f, c, \mathrm{Sym}(2)\rangle, \langle g, c', \mathrm{Sym}(2)\rangle\}.$$

La signature stratifiée Σ_E recouvre bien E, et l'ensemble C de la Définition 10.1.11 est égal à Σ_E. Soit c'' le contexte tel que

$$\tau(c'') \ = \ f(h(\circ), h(\circ), g(\circ, \circ), g(\circ, \circ)),$$

alors il existe des homomorphismes h_i, pour $i = 1, 2, 3$, tels que :

$$h_1, \varepsilon : c \trianglelefteq_G c'', \ h_2, 3 : c' \trianglelefteq_{G'} c'', \text{ et } h_3, 4 : c' \trianglelefteq_{G'} c''.$$

Donc, le groupe $\Gamma_E(c'')$ est engendré par les groupes

$$\begin{aligned} \Phi[c\,, c'', \varepsilon](G) &= \mathrm{Sym}(\{1.1, 2.1\}), \\ \Phi[c', c'', 3](G') &= \mathrm{Sym}(\{3.1, 3.2\}), \\ \Phi[c', c'', 4](G') &= \mathrm{Sym}(\{4.1, 4.2\}). \end{aligned}$$

Remarque. Pour tout symbole $\langle f, c, G\rangle \in \Sigma_E$, on a $\mathrm{id}, \varepsilon : c \trianglelefteq_G c$, et comme $\Phi[c, c, \varepsilon](G) = G$, G est toujours un sous-groupe de $\Gamma_E(c)$.

Nous allons montrer que si Σ_E est une signature stratifiée unif-stable pour les axiomes d'une théorie permutative E, alors pour tout contexte c, et pour toute permutation $\sigma \in \mathcal{SV}(c)$, $E \models c \rightleftharpoons c^\sigma$ si et seulement si $\sigma \in \Gamma_E(c)$. On pourra alors dire que le groupe $\Gamma_E(c)$ est *complet* pour c. Nous commençons par montrer que les permutations induites préservent la condition d'unif-stabilité.

Lemme 10.1.13 *Soient c, c' et c'' des contextes et $\sigma \in \mathrm{Sym}(\mathcal{SV}(c))$ tels que :*
- *$h, v : c \trianglelefteq_\sigma c'$,*
- *$h', v' : c' \trianglelefteq c''$,*
- *soient h_1 la restriction de h' aux sommets de $c'|v$ et $h'_1 = h_1 \circ h$, on a $h'_1, h_1(v) : c \trianglelefteq_\sigma c''$.*

Posons $\mu = \Phi[c, c', v](\sigma)$, alors $h', v' : c' \trianglelefteq_\mu c''$ (voir la Figure 10.1).

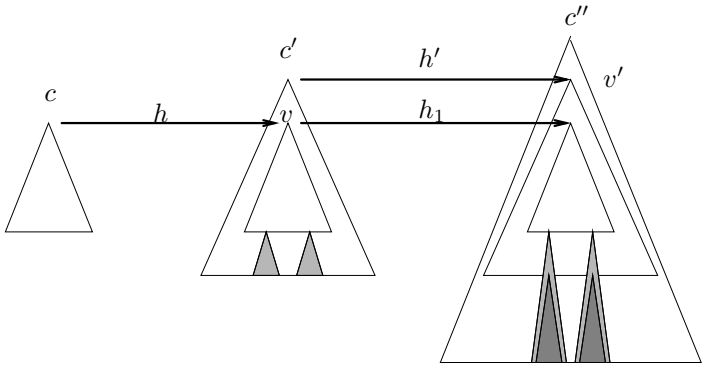

FIG. 10.1 – Lemme 10.1.13

PREUVE. D'après la Propriété 5.2.4, h'_1 est bien un homomorphisme de c vers c''. On note r' la racine de c', il s'agit de montrer que pour tout sommet $w' \in \mathcal{SV}(c')$, $c''|h'(w')$ et $c''|h'(w'^{\mu})$ sont isomorphes. Si $w'^{\mu} = w'$, alors le résultat est évident, supposons maintenant que $w'^{\mu} \neq w'$.

Soit p le chemin de r' à w' dans c', et soit $u \in \mathcal{SV}(c)$ tel que $h(u)$ apparaît dans p; on pose $p = p_1.p_2$, où p_1 est le chemin de r' à $h(u)$ dans c', et p_2 est le chemin de $h(u)$ à w' dans c'. Par définition, si η est l'isomorphisme de $c'|h(u)$ vers $c'|h(u^{\sigma})$, alors $\eta(p_2)$ est le chemin de $h(u^{\sigma})$ à w'^{μ} dans c'.

On pose $q = h_1(p_2)$, q est donc un chemin de $h'_1(u)$ à $h_1(w')$ dans c'', de même, $q' = h_1 \circ \eta(p_2)$ est un chemin de $h'_1(u^{\sigma})$ à $h_1(w'^{\mu})$ dans c''. Par hypothèse, $h'_1, h_1(v) : c \trianglelefteq_{\sigma} c''$, on en déduit qu'il existe également un isomorphisme η' de $c''|h'_1(u)$ vers $c''|h'_1(u^{\sigma})$. Comme q et q' sont parallèles, $\eta'(q)$ est un chemin dans c'' qui est parallèle à q' et de même source $\eta' \circ h'_1(u) = h'_1(u^{\sigma})$. D'après la Propriété 5.1.8, on a donc $q' = \eta'(q)$, d'où $h'(w'^{\mu}) = h_1(w'^{\mu}) = \eta' \circ h_1(w') = \eta' \circ h'(w')$.

Enfin, d'après la Propriété 5.2.5, (une restriction de) η' est un isomorphisme de $c''|h'(w')$ vers $c''|\eta'(h'(w'))$, c'est-à-dire un isomorphisme de $c''|h'(w')$ vers $c''|h'(w'^{\mu})$, d'où le résultat. ∎

Corollaire 10.1.14 *Soit Σ_E une signature stratifiée unif-stable, et considérons $\langle f', c', G' \rangle$ et $\langle f'', c'', G'' \rangle$, deux éléments de Σ_E tels que $h', v' : c' \trianglelefteq c''$. Si $G_1 = \Gamma_E(c')$, alors $h', v' : c' \trianglelefteq_{G_1} c''$.*

PREUVE. Soit $\langle f, c, G \rangle \in \Sigma_E$ tel que $h, v : c \trianglelefteq c'$, et soit $\sigma \in G$. Si h_1 est la restriction de h' aux sommets de $c'|v$ et $h'_1 = h_1 \circ h$, alors h'_1 est un homomorphisme de c vers $c''|h_1(v)$ d'après la Propriété 5.2.4, et par hypothèse d'unif-stabilité, on a $h'_1, h_1(v) : c \trianglelefteq_{\sigma} c''$. D'après le Lemme 10.1.13, on en déduit que si $\mu = \Phi[c, c', v](\sigma)$, alors $h', v' : c' \trianglelefteq_{\mu} c''$. D'après le Corollaire 9.1.6, on a le résultat. ∎

Corollaire 10.1.15 *Soit Σ_E une signature stratifiée unif-stable par rapport aux axiomes définissant une théorie permutative E, et définissons la signature stratifiée Σ'_E par :*

$$\Sigma'_E \;=\; \{\langle f, c, \Gamma_E(c)\rangle \mid \langle f, c, G\rangle \in \Sigma_E\}.$$

Alors Σ'_E est également unif-stable par rapport aux axiomes de E.

PREUVE. Soient $\langle f, c, G\rangle$ et $\langle f', c', G'\rangle$ deux éléments de Σ'_E. Supposons que c et c' sont unifiables, et soit $c'' = c \sqcup c'$, alors, comme Σ_E est stable, il existe un élément $\langle f, c'', G''\rangle \in \Sigma_E$, d'où $\langle f, c'', \Gamma_E(c'')\rangle \in \Sigma'_E$. Comme $c \sqsubseteq c''$, d'après le Corollaire 10.1.14, on a $c \sqsubseteq_G c''$.

Supposons maintenant qu'il existe un sommet non-variable v tel que c et $c'|v$ sont unifiables. Alors, comme Σ_E est unif-stable, on en déduit que $c \sqsubseteq c'|v$. D'après le Corollaire 10.1.14, on a $c \sqsubseteq_G c'|v$, et Σ'_E est bien unif-stable. ∎

Nous pouvons maintenant énoncer la première propriété fondamentale des théories unif-stables :

Théorème 10.1.16 *Si Σ_E est une signature stratifiée unif-stable, alors Σ_E est saturée si et seulement si, pour tout $\langle f, c, G\rangle \in \Sigma_E$, $G = \Gamma_E(c)$.*

PREUVE. Par définition, Σ_E est saturée si et seulement si pour tout élément $\langle f, c, G\rangle \in \Sigma_E$, et pour toute permutation $\sigma \in \mathcal{SV}(c)$, si l'équation permutative $c \rightleftharpoons c^\sigma$ est élément de E, alors $\sigma \in G$. D'après le Théorème 9.1.10, pour toute permutation σ dans $\Gamma_E(c)$, l'équation $c \rightleftharpoons c^\sigma$ est élément de E. Il s'agit maintenant de prouver que pour toute permutation $\sigma \in \mathcal{SV}(c)$, si l'équation permutative $c \rightleftharpoons c^\sigma$ est élément de E, alors $\sigma \in \Gamma_E(c)$.

Soit t un terme tel que $c = \text{arbre}(t)$. Alors, pour tout terme t' dans la classe de congruence de t modulo E, il existe une séquence d'axiomes $e_1, \ldots, e_n$, pour $n \geq 0$, et une séquence de termes $t_1 = t, t_2, \ldots, t_{n+1} = t'$, tels que pour $i = 1, \ldots, n$, le terme t_{i+1} est obtenu à partir de t_i en appliquant l'axiome e_i à la position non-variable p_i de t_i. Nous allons prouver par induction sur la longueur des séquences d'axiomes que l'équation $t \rightleftharpoons t'$ est une équation permutative de contexte associé c et dont la permutation associée est élément de $\Gamma_E(c)$. Le résultat est trivial si $n = 0$, supposons que le résultat soit vrai pour toute séquence d'axiomes de longueur $n-1$, pour $n \geq 1$, et soit une séquence $e_1, \ldots, e_n$ de longueur n. Alors, par hypothèse d'induction, l'équation $t \rightleftharpoons t_n$ est une équation permutative de contexte associé c, et de permutation associée $\sigma' \in \Gamma_E(c)$. Donc, en particulier, on a $c = \text{arbre}(t_n)$, et comme t_{n+1} est obtenu à partir de t_n après application de l'axiome e_n à la position p_n de t_n, si c_n est le contexte associé à e_n, et σ_n la permutation associée à cette équation, alors nécessairement, $c_n \sqsubseteq c|p_n$. Par hypothèse d'unif-stabilité, on a donc $c_n \sqsubseteq_{\sigma_n} c|p_n$. D'après le Théorème 9.1.10, on en déduit que l'équation $t_n \rightleftharpoons t'$ est une équation permutative de contexte associé c, et de permutation associée $\mu = \Phi[c_n, c, p_n](\sigma_n)$. Comme cette équation est élément de $\Gamma_E(c)$ par construction, l'équation $t \rightleftharpoons t'$ est bien une équation permutative de contexte associé c, et dont la permutation associée est élément de $\Gamma_E(c)$. On a bien prouvé que si $c \rightleftharpoons c^\sigma \in E$, alors $\sigma \in \Gamma_E(c)$. ∎

Corollaire 10.1.17 *Si E est une théorie permutative définie par un ensemble d'axiomes unif-stable, alors il existe une signature stratifiée Σ'_E qui est unif-stable par rapport aux axiomes de E, et saturée.*

PREUVE. Par définition, comme l'ensemble d'axiomes définissant E est unif-stable, il existe une signature stratifiée Σ_E qui est unif-stable par rapport à ces axiomes. La signature stratifiée Σ'_E définie dans le Corollaire 10.1.15 est alors unif-stable, et elle est saturée d'après le Théorème 10.1.16. ∎

Exemple 10.1.18 Reprenons la théorie permutative E et la signature stratifiée Σ_E de l'Exemple 10.1.12, et soit $\Sigma'_E = \Sigma_E \cup \{\langle f, c'', \Gamma_E(c'')\rangle\}$. Alors cette signature stratifiée est unif-stable et saturée.

Exemple 10.1.19 Reprenons la théorie permutative E de l'Exemple 10.1.2, qui est définie par l'ensemble d'axiomes suivant :

$$\begin{aligned} f(x_1, x_2) &\rightleftharpoons f(x_2, x_1) \\ g(x_1, x_2) &\rightleftharpoons g(x_2, x_1) \\ f(g(x_1, x_2), g(x_3, x_4)) &\rightleftharpoons f(g(x_3, x_2), g(x_1, x_4)). \end{aligned}$$

Alors, comme le groupe $\mathrm{Sym}(\{1.1, 2.1\})$ n'est pas complet pour c'', la signature stratifiée

$$\Sigma_E = \{\langle f, c, \mathrm{Sym}(2)\rangle, \langle g, c', \mathrm{Sym}(2)\rangle, \langle f, c'', \mathrm{Sym}(\{1.1, 2.1\})\rangle\}$$

qui est définie dans l'Exemple 10.1.2 n'est pas donc saturée. On a :

$$\begin{aligned} \Phi[c'', c'', \varepsilon](\mathrm{Sym}(\{1.1, 2.1\})) &= \mathrm{Sym}(\{1.1, 2.1\}), \\ \Phi[c, c'', \varepsilon](\mathrm{Sym}(2)) &= \mathrm{Sym}(\{1.1, 2.1\})\ \mathrm{Sym}(\{1.2, 2.2\}), \\ \Phi[c', c'', 1](\mathrm{Sym}(2)) &= \mathrm{Sym}(\{1.1, 1.2\}), \\ \Phi[c', c'', 2](\mathrm{Sym}(2)) &= \mathrm{Sym}(\{2.1, 2.2\}). \end{aligned}$$

Le groupe $\Gamma_E(c'')$ est engendré par ces quatre groupes, on en déduit que $\Gamma_E(c'') = \mathrm{Sym}(\{1.1, 1.2, 2.1, 2.2\})$. Donc, la signature stratifiée

$$\Sigma'_E = \{\langle f, c, \mathrm{Sym}(2)\rangle, \langle g, c', \mathrm{Sym}(2)\rangle, \langle f, c'', \Gamma_E(c'')\rangle\}$$

est unif-stable et saturée.

10.2 Extension unif-stable

Le prochain exemple montre qu'étant donnée une théorie permutative E définie par un ensemble d'axiomes, une signature stratifiée unif-stable par rapport aux axiomes de E peut contenir un nombre d'éléments exponentiel en le nombre d'axiomes de E.

Exemple 10.2.1 Soient f un symbole de fonction d'arité $n+2$, a un symbole de constante, et pour $i = 1, \ldots, n$, soit c_i le contexte tel que $\tau(c_i) = f(\circ, \ldots, a, \ldots, \circ)$, où la constante a est le $(i+2)^{\text{ème}}$ argument de f. Considérons la théorie permutative définie par l'ensemble d'axiomes $\{c_i \rightleftharpoons c_i^{\sigma_i} \mid i = 1, \ldots, n\}$, où pour tout $i = 1, \ldots, n$, $\sigma_i \in \mathrm{Sym}(2)$. Il est clair que les c_i sont unifiables deux à deux. Pour tout $A \subseteq \{1, \ldots, n\}$ tel que $A \neq \emptyset$, on définit le contexte $c_A = \sqcup\{c_i \mid i \in A\}$, on a donc $c_{\{i\}} = c_i$.

Soit la signature stratifiée $\Sigma_E = \{\langle f, c_A, \Gamma_E(c)\rangle \mid A \subseteq \{1, \ldots, n\} \wedge A \neq \emptyset\}$. Par exemple, supposons que $n = 2$, $\sigma_1 = \mathrm{id}$, $\sigma_2 = (1\ 2)$, et posons $A = \{1, 2\}$, alors on a $c_1 = f(\circ, \circ, a, \circ)$, $c_2 = f(\circ, \circ, \circ, a)$, et $c_A = f(\circ, \circ, a, a)$, d'où

$$\Sigma_E \ = \ \{\langle f, c_1, \mathrm{I}\rangle, \langle f, c_2, \mathrm{Sym}(2)\rangle, \langle f, c_A, \mathrm{Sym}(2)\rangle\}.$$

La signature stratifiée Σ_E est unif-stable par rapport aux axiomes de E, et comporte $2^n - 1$ éléments. De plus, comme une signature stratifiée unif-stable est nécessairement fermée pour l'opération $\sqcup$, aucun sous-ensemble strict de Σ_E ne vérifie cette propriété.

Dans la suite, nous allons définir la notion d'*extension unif-stable* d'une signature stratifiée, et nous montrerons qu'il est possible de décider en temps polynomial si un ensemble d'axiomes est unif-stable ou non.

Définition 10.2.2 (Extension unif-stable) Etant données une théorie permutative E définie par un ensemble d'axiomes, et une signature stratifiée qui recouvre les axiomes de E, on dit que la signature stratifiée Σ'_E est une *extension unif-stable* de Σ_E si et seulement si Σ'_E est unif-stable par rapport aux axiomes de E, et que pour tout symbole $\langle f, c, G\rangle \in \Sigma_E$, il existe un symbole $\langle f, c, G'\rangle \in \Sigma'_E$ tel que G est un sous-groupe de G'.$\diamond$

Dans ce qui suit, nous allons étudier une condition suffisante d'existence d'une extension unif-stable.

Lemme 10.2.3 *Soient c_1 et c_2 deux contextes unifiables, et soit c tel que $c \sqsubseteq_G c_1$ et $c \sqsubseteq_G c_2$, pour un groupe G donné. Alors on a $c \sqsubseteq_G c_1 \sqcup c_2$.*

PREUVE. On note h_i l'homomorphisme de c vers c_i pour $i = 1, 2$, et h l'homomorphisme de c vers $c_1 \sqcup c_2$ (qui est bien défini d'après le Corollaire 5.3.13). Soit $\sigma \in G$, et soit v un sommet variable de c. Alors par hypothèse, $c_1|h_1(v^\sigma) \simeq c_1|h_1(v)$, et $c_2|h_2(v^\sigma) \simeq c_2|h_2(v)$. Comme $c_1|h_1(v)$ et $c_2|h_2(v)$ sont unifiables d'après le Lemme 5.3.14, on en déduit d'après le Corollaire 5.3.18 que :

$$c_1|h_1(v) \sqcup c_2|h_2(v) \ \simeq \ c_1|h_1(v^\sigma) \sqcup c_2|h_2(v^\sigma).$$

D'après le Lemme 5.3.14, $c_1|h_1(v) \sqcup c_2|h_2(v) \simeq (c_1 \sqcup c_2)|h(v)$, et $c_1|h_1(v^\sigma) \sqcup c_2|h_2(v^\sigma) \simeq (c_1 \sqcup c_2)|h(v^\sigma)$. Donc, pour tout sommet variable v de c, et pour toute permutation $\sigma \in G$, on a $(c_1 \sqcup c_2)|h(v) \simeq (c_1 \sqcup c_2)|h(v^\sigma)$, ce qui prouve qu'on a bien $c \sqsubseteq_G c_1 \sqcup c_2$. ■

Corollaire 10.2.4 *Soient $C = \{c_1, \ldots, c_n\}$ un ensemble de contextes deux à deux unifiables, c un contexte, et G un sous-groupe de* $\mathrm{Sym}(\mathcal{SV}(c))$. *On pose $c' = \sqcup C$,*

1. *si pour tout* $i = 1, \ldots, n$, *on a* $c \sqsubseteq_G c_i$, *alors* $c \sqsubseteq_G c'$,
2. *soit* $p \neq \varepsilon$ *un sommet de* c', *si pour tout* $c_i \in C$ *tel que* p *est un sommet non-variable de* c_i, *on a* $c \sqsubseteq_G c_i|p$, *alors* $c \sqsubseteq_G c'|p$.

PREUVE. 1. On démontre le résultat par induction sur la cardinalité de C. Le résultat est trivial si $n = 1$, et si $n = 2$, le résultat est une conséquence immédiate du Lemme 10.2.3. Supposons maintenant que le résultat soit vrai pour tout sous-ensemble de C de cardinalité $n-1$, où $n \geq 3$, et que C est de cardinalité n. On pose $C' = \{c_2, \ldots, c_n\}$, alors, par hypothèse d'induction, on a $c \sqsubseteq_G \sqcup C'$, et comme $c \sqsubseteq_G c_1$, on en déduit d'après le Lemme 10.2.3 que $c \sqsubseteq_G (\sqcup C') \sqcup c_1$. D'après le Lemme 9.2.4, $(\sqcup C') \sqcup c_1 = c'$, d'où le résultat.
2. On définit l'ensemble C' de contextes par :

$$C' \;=\; \{c''|p \mid p \text{ est un sommet non-variable de } c'' \in C\},$$

alors, pour tout $c''|p \in C'$, on a $c \sqsubseteq_G c''|p$, et comme $c''|p \sqsubseteq c'|p$, les éléments de C' sont deux à deux unifiables. D'après le point 1 de ce lemme, on en déduit que $c \sqsubseteq_G \sqcup C'$, et d'après le Lemme 9.2.5, on a $\sqcup C' \simeq c'|p$, ce qui prouve que $c \sqsubseteq_G c'|p$. ∎

Théorème 10.2.5 *Soit* Σ_E *une signature stratifiée qui recouvre les axiomes de* E, *et supposons que pour toute paire* $\langle f, c, G\rangle, \langle f', c', G'\rangle \in \Sigma_E$, *on a les propriétés suivantes :*
- *si* c *et* c' *sont unifiables, alors* $c \sqsubseteq_G c \sqcup c'$,
- *si* $v \neq \varepsilon$ *est un sommet non-variable de* c' *tel que* c *et* $c'|v$ *sont unifiables, alors* $c \sqsubseteq_G c'|v$.

Alors il existe une signature stratifiée Σ'_E *qui est une extension unif-stable de* Σ_E, *et qui est saturée.*

PREUVE. On pose $C = \{c \mid \langle f, c, G\rangle \in \Sigma_E\}$, et on définit la signature stratifiée

$$\Sigma'_E \;=\; \{\langle f', c', \Gamma_E(c')\rangle \mid c' = \sqcup C' \wedge C' \subseteq C \wedge C' \neq \emptyset\}.$$

Nous allons montrer que Σ'_E est une signature stratifiée unif-stable, d'après le Théorème 10.1.16, nous aurons la preuve que Σ'_E est également saturée. Soient C_1 et C_2 deux sous-ensembles non vides de C composés de contextes deux à deux unifiables. On pose $c_1 = \sqcup C_1$, $c_2 = \sqcup C_2$, et $G_1 = \Gamma_E(c_1)$.

Supposons d'abord que c_1 et c_2 sont unifiables, et soient $C_3 = C_1 \cup C_2$ et $c_3 = c_1 \sqcup c_2$. Alors $c_3 = \sqcup C_3$ d'après le Lemme 9.2.4, et il s'agit de prouver que $c_1 \sqsubseteq_{G_1} c_3$. Soient c un contexte axiomatique de E et v un sommet non-variable de c_1 tels que $c \sqsubseteq c_1|v$. Comme Σ_E recouvre les axiomes de E, il existe un symbole $\langle f, c, G\rangle \in \Sigma_E$. Si $v = \varepsilon$, alors comme c_1 et c_2 sont unifiables, pour tout $c'_3 \in C_3$, c et c'_3 sont unifiables. Par hypothèse, on a alors $c \sqsubseteq_G c \sqcup c'_3$, et d'après le Corollaire 10.2.4 1, $c \sqsubseteq_G c \sqcup c_3$. Comme $c \sqsubseteq c_1 \sqsubseteq c_3$, d'après la Propriété 9.2.3, on a $c \sqcup c_3 = c_3$, d'où $c \sqsubseteq_G c_3$.

Si $v \neq \varepsilon$, comme v est un sommet non-variable de c_1, c'est donc également un sommet non-variable de c_3. D'après le Lemme 9.2.5, il existe un contexte $c'_3 \in C_3$ tel que v est un sommet non-variable de c'_3. Comme $c_1|v$ et $c'_3|v$ sont unifiables, on en déduit que c et

$c'_3|v$ sont également unifiables, d'où $c \sqsubseteq_G c'_3|v$ par hypothèse. D'après le Corollaire 10.2.4 2, on en déduit que $c \sqsubseteq_G c_3|v$.

On a donc, pour tout $\sigma \in G$, $c \sqsubseteq_\sigma c_1|v$ et $c \sqsubseteq_\sigma c_3|v$. Comme $c_1 \sqsubseteq c_3$, d'après le Lemme 10.1.13, si $\mu = \Phi[c, c_1, v](\sigma)$, alors $c_1 \sqsubseteq_\mu c_3$. D'après le Corollaire 9.1.6, on en déduit que $c_1 \sqsubseteq_{G_1} c_3$.

Supposons maintenant que c_1 et $c_2|v'$ sont unifiables, où $v' \neq \varepsilon$ est un sommet non-variable de c_2, il s'agit de prouver que $c_1 \sqsubseteq_{G_1} c_2|v'$. Soit c'_2 un élément de C_2 tel que v' est un sommet non-variable de c'_2 (l'existence de c'_2 est garantie par le Lemme 9.2.5), alors, pour tout $c'_1 \in C_1$, c'_1 et $c'_2|v'$ sont unifiables, et par hypothèse, $c'_1 \sqsubseteq c'_2|v'$. D'après le Théorème 5.3.15, on en déduit que $c_1 \sqsubseteq c'_2|v'$, et donc, $c_1 \sqsubseteq c_2|v'$. Notons h l'homomorphisme de c_1 vers $c_2|v'$.

Soit c un contexte axiomatique, il existe donc un symbole $\langle f, c, G\rangle \in \Sigma_E$, et supposons que $c \sqsubseteq c_1|v$, pour un sommet non-variable v de c_1. Posons $w = h(v)$, alors c est unifiable avec $c_2|w$, et comme v est un sommet non-variable de c_1, w est un sommet non-variable de c_2. Soit c''_2 un élément de C_2 tel que w est un sommet non-variable de c''_2. Comme $c''_2|w \sqsubseteq c_2|w$, on en déduit que $c_1|v$ et $c''_2|w$ sont unifiables, et donc, que c et $c''_2|w$ sont unifiables. Par hypothèse, on a donc $c \sqsubseteq_G c''_2|w$, et d'après le Corollaire 10.2.4 2, on en déduit que $c \sqsubseteq_G c_2|w$. Comme précédemment, d'après le Lemme 10.1.13, on en déduit que pour toute permutation $\sigma \in G$, si $\mu = \Phi[c, c_1, v](\sigma)$, alors $c_1 \sqsubseteq_\mu c_2|v'$, d'où $c_1 \sqsubseteq_{G_1} c_2|v'$. ■

Le Théorème 10.2.5 fournit donc une procédure de construction, sous certaines conditions, d'une signature stratifiée qui est unif-stable et saturée. Ce théorème permet également de tester si une théorie permutative définie par un ensemble d'axiomes est unif-stable :

Corollaire 10.2.6 *Soit E une théorie définie par un ensemble d'axiomes, et soit Σ_E une signature stratifiée minimale qui recouvre les axiomes de E, telle que pour tout $\langle f, c, G\rangle \in \Sigma_E$, c est un contexte axiomatique de E. Alors l'ensemble des axiomes définissant E est unif-stable si et seulement si Σ_E vérifie les conditions du Théorème 10.2.5.*

PREUVE. Si Σ_E vérifie les conditions du Théorème 10.2.5, alors il est clair que l'ensemble des axiomes définissant E est unif-stable. Réciproquement, supposons que cet ensemble d'axiomes est unif-stable, alors d'après le Corollaire 10.1.17, il existe une signature stratifiée Σ'_E qui est unif-stable par rapport à ces axiomes, et saturée. Soient $\langle f, c, G\rangle, \langle f', c', G'\rangle \in \Sigma_E$, alors, comme Σ_E recouvre les axiomes de E, les éléments $\langle f, c, \Gamma_E(c)\rangle$ et $\langle f', c', \Gamma_E(c')\rangle$ sont éléments de Σ'_E d'après le Théorème 10.1.16, et G (resp. G') est un sous-groupe de $\Gamma_E(c)$ (resp. $\Gamma_E(c')$). Si c et c' sont unifiables, alors par hypothèse, $c \sqsubseteq_{\Gamma_E(c)} c \sqcup c'$, et donc, $c \sqsubseteq_G c \sqcup c'$. De même, s'il existe un sommet non-variable $p \neq \varepsilon$ tel que c et $c'|p$ sont unifiables, alors $c \sqsubseteq_{\Gamma_E(c)} c'|p$, et donc $c \sqsubseteq_G c'|p$. Donc, Σ_E vérifie bien les hypothèses du Théorème 10.2.5. ■

Il est clair qu'il est possible de construire une signature stratifiée Σ_E vérifiant les hypothèses du Corollaire 10.2.6 et de tester si Σ_E vérifie bien les conditions du Théorème 10.2.5 en temps polynomial en le nombre d'axiomes de E, ce corollaire prouve donc que le problème de tester si l'ensemble des axiomes définissant une théorie permutative est unif-stable est polynomial.

Strat(A) =
  soit st_rec(v) =
    soit $f = s(v)$ **dans**
    soit $C = \{c \mid \langle f, c, G\rangle \in \Sigma_E \ \wedge \ c \sqsubseteq A|v\}$ **dans**
      si $C = \emptyset$ **alors**
        pour $i = 1, \ldots,$ arité($s(v)$) **faire** st_rec($a(v)_i$) **fin pour**
      sinon
        soit $c = \sqcup C$ et $h : c \sqsubseteq A|v$ **dans**
        $s(v) := \langle f, c, \Gamma_E(c)\rangle$;
        pour $w \in \mathcal{SV}(c)$ **faire** st_rec($h(w)$) **fin pour**
      fin si
  dans
  st_rec(racine(A))

FIG. 10.2 – Algorithme Strat

10.3 Déduction et unif-stabilité

Nous allons maintenant étudier de quelle façon faire de la déduction avec des GA-termes stratifiés modulo une théorie permutative E définie par un ensemble d'axiomes unif-stable. Nous commencerons par définir une fonction qui, à un terme t associe un A-terme stratifié A, et montrerons que l'ensemble stratifié S[A] est exactement la classe de congruence de t modulo E. Puis nous verrons que les problèmes liés à la déduction dans le Chapitre 8 sont dans la classe de Luks, tout comme le problème du mot généralisé modulo une théorie E définie par un ensemble d'axiomes unif-stable.

Avant de faire de la déduction avec des GA-termes stratifiés, il faut construire ces GA-termes stratifiés. Nous nous servirons du Théorème 10.2.5 pour décrire une fonction déterministe qui associe un A-terme stratifié à un terme donné, et ce A-terme stratifié sera construit en temps polynomial en le nombre d'axiomes de E.

Définition 10.3.1 (Strat(A) et As(t)) Soient E une théorie permutative définie par un ensemble d'axiomes, et Σ_E une signature stratifiée vérifiant les hypothèses du Corollaire 10.2.6. Alors la fonction Strat qui à un A-terme clos associe un A-terme stratifié est définie dans la Figure 10.2.

Pour tout terme t, on définit le A-terme As(t) par : As(t) = Strat(arbre(t)). ◇

Le A-terme As(t) est donc construit sur la signature $\Sigma \cup \Sigma'_E$, où Σ'_E est la signature stratifiée, unif-stable par rapport aux axiomes de E, définie dans le Théorème 10.2.5. Bien que la taille de Σ'_E puisse éventuellement être exponentielle en le nombre d'axiomes de E, il n'est pas nécessaire de la construire explicitement, et c'est pourquoi la construction de As(t) est polynomiale en le nombre d'axiomes de E.

Exemple 10.3.2 Soit E la théorie permutative définie par les axiomes suivants :

$$\begin{aligned} f(g(h(x_1,x_2),h(x_3,x_4)),x_5,x_6) &\rightleftharpoons f(g(h(x_2,x_1),h(x_4,x_3)),x_5,x_6) \\ f(x_1,h(x_2,x_3),x_4) &\rightleftharpoons f(x_1,h(x_3,x_2),x_4) \\ g(x_1,x_2) &\rightleftharpoons g(x_2,x_1) \end{aligned}$$

On note respectivement c_1, c_2 et c_3 les contextes associés à ces trois axiomes, on définit les groupes G_1, G_2 et G_3 par :

$$G_1 = \{\mathrm{id}, (1.1.1\ 1.1.2)(1.2.1\ 1.2.2)\},\ G_2 = \mathrm{Sym}(\{2.1, 2.2\}),\ G_3 = \mathrm{Sym}(2),$$

et on pose $F_1 = \langle f, c_1, G_1\rangle$, $F_2 = \langle f, c_2, G_2\rangle$ et $F_3 = \langle g, c_3, G_3\rangle$. Alors la signature stratifiée $\Sigma_E = \{F_1, F_2, F_3\}$ vérifie les hypothèses du Corollaire 10.2.6, et peut être étendue en une signature unif-stable Σ'_E d'après le Théorème 10.2.5.

Considérons maintenant le terme

$$t = f(g(h(a,b),h(a,d)),h(a,b),g(a,d)),$$

et soit $A = \mathrm{arbre}(t)$. La procédure Strat effectue un appel à st_rec(r), où r est la racine de A. On a $c_1 \sqsubseteq A$ et $c_2 \sqsubseteq A$, et si $c_4 = c_1 \sqcup c_2$, alors la procédure st_rec étiquette donc la racine r de A par le symbole $F_4 = \langle f, c_4, \Gamma_E(c_4)\rangle$, et effectue des appels récursifs à la procédure st_rec sur les éléments de $\mathrm{R}_A(r)$. Lors de l'appel à st_rec sur le sommet 3, on a $c_3 \sqsubseteq A|3$, et donc, ce sommet est étiqueté par le symbole F_3. On a donc :

$$\tau(\mathrm{As}(t)) = F_4(\ g(h(a,b),h(a,d)),\ h(a,b),\ F_3(a,d)\ ).$$

On a une première propriété de décomposition, évidente d'après les définitions de Strat et de As(t) :

Propriété 10.3.3 *Soit $A = (V, s, a)$ un* A*-terme de racine r, et posons $A' = (V, s', a) =$* Strat(A).

- *Si $s'(r) \in \Sigma$, alors pour tout sommet v apparaissant dans $a(r)$, on a $A'|v =$* Strat$(A|v)$.
- *Si $s'(r) \in \Sigma_E$, alors pour tout sommet $v \in \mathrm{R}_A(r)$, on a $A'|v =$* Strat$(A|v)$.

La procédure Strat préserve aussi les isomorphismes :

Propriété 10.3.4 *Si A et A' sont des* A*-termes clos tels que $A \simeq A'$, alors* Strat$(A) \simeq$ Strat(A')

Théorème 10.3.5 *Soit Σ'_E l'extension unif-stable de Σ_E définie dans le Théorème 10.2.5. Alors, pour tout terme t,* As(t) *est un* A*-terme stratifié sur $\Sigma \cup \Sigma'_E$, qui est saturé.*

PREUVE. Soit $A = (V, s, a) = \mathrm{As}(t)$, il est clair que A est un A-terme sur $\Sigma \cup \Sigma'_E$, nous commençons par montrer que ce A-terme est stratifié. Soit $v \in V$ un sommet tel que $s(v) = \langle f, c, G\rangle \in \Sigma'_E$, alors c est de la forme $\sqcup C$ pour un ensemble C de contextes tels que pour tout $c' \in C$, $c' \sqsubseteq \mathrm{dm}(A|v)$. D'après le Corollaire 5.3.24, il existe alors un homomorphisme h tel que $h : c \sqsubseteq \mathrm{dm}(A|v)$.

Si u est un sommet de $A|v$ qui est étiqueté par un élément de Σ'_E, alors la procédure st_rec a été appelée sur le sommet u, ce qui signifie qu'il existe un sommet variable w de c tel que u est en-dessous de $h(w)$. Donc, h est également un homomorphisme de c vers $\mathrm{dm_r}(A|v)$, et A est bien un A-terme stratifié.

Montrons maintenant que ce A-terme stratifié est saturé. Supposons qu'il existe un sommet $v \in V$ qui vérifie les conditions de la Définition 8.2.4, alors, comme il existe un sommet $\langle f, c, G\rangle \in \Sigma'_E$ et un homomorphisme de c vers $\mathrm{dm}(A|v)$, l'ensemble C défini dans l'algorithme de la Figure 10.2 est non vide, et comme $s(v) \in \Sigma$, nécessairement, lors de l'appel à la procédure $\mathrm{As}(t)$, il n'y a eu aucun appel à la procédure $\mathrm{st\_rec}(v)$, ce qui signifie que nécessairement, v est dans un antirésidu $\overline{\mathrm{R}}_A(u)$ pour un sommet $u \in V_{\mathrm{s}}$. Donc, $\mathrm{As}(t)$ est bien un A-terme stratifié qui est saturé. ∎

Le problème du mot généralisé

Nous allons maintenant étudier le problème du mot généralisé modulo une théorie définie par un ensemble d'axiomes unif-stable. Nous montrerons que deux termes clos t et t' sont congrus modulo E si et seulement si $\mathrm{As}(t) \bowtie \mathrm{As}(t')$.

Nous commençons par démontrer que pour tout A-terme stratifié A, si un contexte subsume $\mathrm{dm}(A)$, alors pour tout $A' \in [A]_{\mathrm{s}}$, ce contexte subsume également $\mathrm{dm}(A')$.

Lemme 10.3.6 *Soit Σ_E une signature stratifiée unif-stable, A un A-terme stratifié dont la racine r est étiquetée par le symbole $\langle f, c_1, G_1\rangle \in \Sigma_E$, et $\langle f, c_2, G_2\rangle$ un symbole de Σ_E tel que $c_2 \sqsubseteq \mathrm{dm}(A)$. On note $c = c_1 \sqcup c_2$, et pour $\sigma \in G_1$, on définit $\mu = \sigma^{\mathrm{h}_{[A,r]}}$, alors $c \sqsubseteq \mathrm{dm}(A^\mu)$.*

PREUVE. Soit un A-terme A' dont la racine r' est étiquetée par le symbole $\langle f, c, G\rangle \in \Sigma_E$, et tel que $\mathrm{dm_r}(A) \simeq \mathrm{dm_r}(A')$. Par hypothèse d'unif-stabilité, $c_1 \sqsubseteq_{G_1} c$, donc, la permutation $\delta = \Phi[c_1, c, \varepsilon](\sigma)$ est bien définie. Posons $\delta' = \delta^{\mathrm{h}_{[A',r']}}$, alors d'après le Corollaire 9.1.11, $\mathrm{dm_r}(A^\mu) \mathrel{\mathring{=}} \mathrm{dm_r}(A'^{\delta'})$, d'où $\mathrm{dm}(A^\mu) \mathrel{\mathring{=}} \mathrm{dm}(A'^{\delta'})$. D'après le Corollaire 5.2.18, on en déduit que $\mathrm{dm}(A^\mu)$ et $\mathrm{dm}(A'^{\delta'})$ sont isomorphes, et comme $c \sqsubseteq \mathrm{dm}(A'^{\delta'})$, on a $c \sqsubseteq \mathrm{dm}(A^\mu)$. ∎

Lemme 10.3.7 *Soit Σ_E une signature stratifiée unif-stable, et A un A-terme stratifié contenant un sommet v étiqueté par le symbole $\langle f, c, G\rangle \in \Sigma_E$. Soit $\langle f', c', G'\rangle$ un symbole de Σ_E tel que $c' \sqsubseteq \mathrm{dm}(A)$. Pour $\sigma \in G$, on pose $\mu = \sigma^{\mathrm{h}_{[A,v]}}$, alors on a $c' \sqsubseteq \mathrm{dm}(A^\mu)$.*

PREUVE. On note V' l'ensemble des sommets de c', et h l'homomorphisme de c' vers $\mathrm{dm}(A)$. S'il existe un sommet $w \in \mathcal{SV}(c')$ tel que $v \leq_A h(w)$, alors tous les sommets de $h(V' \setminus \mathcal{SV}(c'))$ sont fixés par la permutation μ, et il est aisé de vérifier que la fonction $\mu \circ h$ est un homomorphisme de c' vers $\mathrm{dm}(A^\mu)$.

Sinon, soit w le sommet non-variable de c' tel que $h(w) = v$, alors c et $c'|w$ sont unifiables, et par hypothèse d'unif-stabilité, on a $c \sqsubseteq_G c'|w$. Soit A' un A-terme stratifié dont la racine r' est étiquetée par le symbole $\langle f', c', G' \rangle$, et tel que $\mathrm{dm}(A) \simeq \mathrm{dm}(A')$. On pose $\delta = \Phi[c, c', w](\sigma)$ et $\delta' = \delta^{\mathrm{h}_{[A',r']}}$, alors d'après le Corollaire 9.1.11, on a $\mathrm{dm}(A^\mu) \stackrel{\circ}{=} \mathrm{dm}(A'^{\delta'})$, et d'après le Corollaire 5.2.18, on en déduit que $\mathrm{dm}(A^\mu) \simeq \mathrm{dm}(A'^{\delta'})$. Comme $c' \sqsubseteq \mathrm{dm}(A'^{\delta'})$, on a bien $c' \sqsubseteq \mathrm{dm}(A^\mu)$. ∎

Corollaire 10.3.8 *Soit $A = (V, s, a)$ un A-terme stratifié sur une signature stratifiée Σ_E qui est unif-stable, et soit $\mu \in \mathcal{G}_A$. Alors les ensembles de contextes qui subsument $\mathrm{dm}(A)$ et $\mathrm{dm}(A^\mu)$ sont identiques.*

PREUVE. Toute permutation $\mu \in \mathcal{G}_A$ est de la forme $\prod_{v \in V'} \sigma_v$, où $V' \subseteq V_\mathrm{s}$ est un ensemble non vide, et $\sigma_v \in \mathcal{G}_A(v)$. Montrons le résultat par induction sur la cardinalité de V'. Si $V' = \{v\}$, alors on a le résultat d'après le Lemme 10.3.7. Supposons maintenant que le résultat soit vrai pour tout sous-ensemble de V_s de cardinalité $n-1$, et que V' est de cardinalité n. On pose $V' = V'' \cup \{v\}$, et soit $\mu = \prod_{w \in V'} \sigma_w = \mu' \sigma_v$. Notons respectivement C_1 et C_2 les ensembles de contextes qui subsument $\mathrm{dm}(A)$ et $\mathrm{dm}(A^{\mu'})$, alors, par hypothèse d'induction, on a $C_1 = C_2$, et si C_3 est l'ensemble de contextes qui subsument $\mathrm{dm}(A^\mu)$, alors $C_3 = C_2$ d'après le Lemme 10.3.7. On a bien $C_1 = C_3$, d'où le résultat. ∎

Nous allons démontrer que pour tout A-terme A_1, si $A = \mathrm{Strat}(A_1)$ et $\sigma \in \mathcal{G}_A$, alors pour tout A-terme A_2 tel que $A_2 \simeq \mathrm{dm}(A^\sigma)$, on a $\mathrm{Strat}(A_2) \simeq A$. Nous commençons par étudier le cas où $\sigma \in \mathcal{G}_A(r)$.

Lemme 10.3.9 *Etant donnée une signature stratifiée Σ_E unif-stable et saturée, soit A_1 un A-terme, et posons $A = \mathrm{Strat}(A_1)$. Supposons que la racine r de A est étiquetée par le symbole $\langle f, c, G \rangle \in \Sigma_E$, et soit $\sigma \in \mathcal{G}_A(r)$. Soit A_2 un A-terme isomorphe à $\mathrm{dm}(A^\sigma)$ et $A' = \mathrm{Strat}(A_2)$, alors $A^\sigma \simeq A'$.*

PREUVE. On définit les ensembles suivants :

$$\begin{aligned} C &= \{c' \mid c' \text{ est un contexte axiomatique de } E \ \wedge \ c' \sqsubseteq A_1\}, \\ C' &= \{c' \mid c' \text{ est un contexte axiomatique de } E \ \wedge \ c' \sqsubseteq A_2\}. \end{aligned}$$

On a donc $c = \sqcup C$, et d'après le Corollaire 10.3.8, $C' = C$, ce qui prouve que la racine r' de A' est également étiquetée par le symbole $\langle f, c, G \rangle$.

Posons $A'_1 = \mathrm{dm}(A^\sigma)$, et notons η l'isomorphisme de A'_1 vers A_2. Soit v un sommet de A, alors il est clair que $v \in \mathrm{R}_A(r)$ si et seulement si $\eta(v) \in \mathrm{R}_{A'}(r')$. Comme $\sigma \in \mathcal{G}_A(r)$, on a $A^\sigma|v = A|v$, d'où $A'_1|v = A_1|v$, et comme $A'_1|v$ et $A_2|\eta(v)$ sont isomorphes, on a $A_1|v \simeq A_2|\eta(v)$. D'après la Propriété 10.3.3, on a $A|v = \mathrm{Strat}(A_1|v)$ et $A'|\eta(v) = \mathrm{Strat}(A_2|\eta(v))$, donc, d'après la Propriété 10.3.4, on en déduit que $A^\sigma|v = A|v \simeq A'|\eta(v)$.

Enfin, les sommets r et r' étant étiquetés par le même symbole de Σ_E, il est clair que la restriction de η à $\overline{\mathrm{R}}_A(r) \cup \mathrm{R}_A(r)$ est égale à la fonction $\mathrm{h}^{A^\sigma}_{[r \to r']}$. D'après le Lemme 6.6.16, on en déduit que η est bien un isomorphisme de A^σ vers A'. ∎

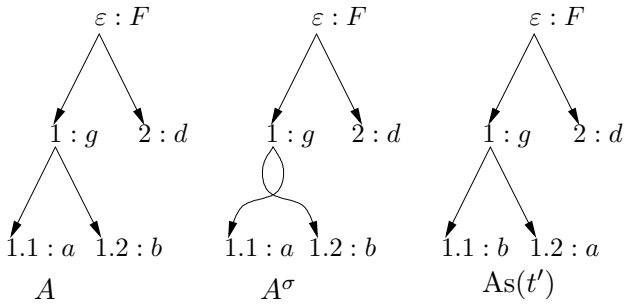

FIG. 10.3 – A-termes de l'Exemple 10.3.10

Exemple 10.3.10 Soit E la théorie permutative définie par l'unique axiome

$$f(g(x,y),z) \quad \rightleftharpoons \quad f(g(y,x),z),$$

soit c le contexte tel que $\tau(c) = f(g(\circ,\circ),\circ)$, et soit $G = \mathrm{Sym}(\{1.1, 1.2\})$. On pose $F = \langle f, c, G\rangle$, alors la signature stratifiée $\Sigma_E = \{F\}$ est trivialement unif-stable. Soit $t = f(g(a,b),d)$, alors le A-terme $\mathrm{As}(t)$ est représenté à gauche de la Figure 10.3. La permutation $\sigma = (1.1\ 1.2)$ est élément de $\mathcal{G}_A$, et le A-terme A^σ est représenté au centre de la même figure. Enfin, si $t' = \tau(\mathrm{dm}(A^\sigma))$, alors $\mathrm{As}(t')$ est représenté à droite de la même figure, et il est aisé de vérifier que A^σ et $\mathrm{As}(t')$ sont bien isomorphes.

Lemme 10.3.11 *Soit A_1 un A-terme, on pose $A = (V, s, a) = \mathrm{Strat}(A_1)$, et on note r sa racine. Pour $v \in V_s$, soit $\sigma \in \mathcal{G}_A(v)$, si A_2 est un A-terme isomorphe à $\mathrm{dm}(A^\sigma)$ et $A' = \mathrm{Strat}(A_2)$, alors $A^\sigma \simeq A'$.*

PREUVE. On démontre le résultat par induction sur la profondeur de v. Si $v = r$, le résultat est immédiat d'après le Lemme 10.3.9. Supposons maintenant que le résultat est vrai pour tout sommet de profondeur strictement inférieure à k dans un A-terme, et que v est de profondeur k dans A. Supposons que $s(r) = \langle f, c, G\rangle \in \Sigma_E$, la démonstration dans le cas où $s(r) \in \Sigma$ est identique.

Il existe un unique sommet $u \in \mathrm{R}_A(r)$ tel que v est en-dessous de u dans A, et v est évidemment de profondeur strictement inférieure à k dans $A|u$. Notons η l'isomorphisme de $\mathrm{dm}(A^\sigma)$ vers A_2, alors (une restriction de) η est un isomorphisme de $\mathrm{dm}(A^\sigma|u)$ vers $A_2|\eta(u)$. Comme $\sigma \in \mathcal{G}_{A|u}$, on a $A^\sigma|u = (A|u)^\sigma$, et la fonction η est donc un isomorphisme de $\mathrm{dm}((A|u)^\sigma)$ vers $A_2|\eta(u)$. D'après la Propriété 10.3.3, on a $A|u = \mathrm{Strat}(A_1|u)$, et par hypothèse d'induction, on en déduit que $A^\sigma|u = (A|u)^\sigma \simeq \mathrm{Strat}(A_2|\eta(u))$.

Soit r' la racine de A', alors $\eta(u) \in \mathrm{R}_{A'}(r')$, et d'après la Propriété 10.3.4, $\mathrm{Strat}(A_2|\eta(u)) = A'|\eta(u)$. Donc, $A^\sigma|u \simeq A'|\eta(u)$.

Pour tout $w \in \mathrm{R}_A(r) \setminus u$, on a $A^\sigma|w = A|w$, et donc $A_1|w \simeq A_2|\eta(w)$. D'après la Propriété 10.3.4, on en déduit que $A|w \simeq A'|\eta(w)$, puisque $\eta(w) \in \mathrm{R}_{A'}(r')$. Comme les

sommets r et r' sont étiquetés par le même symbole, la restriction de η à $\overline{\mathrm{R}}_A(r) \cup \mathrm{R}_A(r)$ est égale à $\mathrm{h}^{A^\sigma}_{[r \to r']}$, et d'après le Lemme 6.6.16, on en déduit que A^σ et A' sont isomorphes. ■

Corollaire 10.3.12 *Soient A_1 un* A*-terme, $A = \mathrm{Strat}(A_1)$, et T un* GA*-terme tel que $T \stackrel{\circ}{=} A$. Alors on a :*

1. *pour tout $\sigma \in \mathcal{G}_A$, et pour tout* A*-terme A_2 tel que $A_2 \simeq \mathrm{dm}(A^\sigma)$, on a $A^\sigma \simeq \mathrm{Strat}(A_2)$,*
2. *pour tout $\sigma \in \mathcal{G}_T$, si $\mathrm{dm}(T^\sigma) \stackrel{\circ}{=} \mathrm{dm}(T)$, alors $T^\sigma \stackrel{\circ}{=} T$.*

PREUVE. 1. Toute permutation $\sigma \in \mathcal{G}_A$ est de la forme $\prod_{v \in V'} \sigma_v$, où $V' \subseteq V_\mathrm{s}$ est un ensemble non vide, et $\sigma_v \in \mathcal{G}_A(v)$. Montrons le résultat par induction sur la cardinalité de V'. Si $V' = \{v\}$, alors on a le résultat d'après le Lemme 10.3.11.

Supposons maintenant que le résultat soit vrai pour tout sous-ensemble de V_s de cardinalité $n-1$, et que V' est de cardinalité n. On pose $V' = V'' \cup \{v\}$, et soit $\sigma = \prod_{w \in V'} \sigma_w = \mu\sigma_v$. Soient A_3 un A-terme isomorphe à $\mathrm{dm}(A^\mu)$, et $A' = \mathrm{Strat}(A_3)$, alors par hypothèse d'induction, on a $A^\mu \simeq A'$. Notons η l'isomorphisme de A^μ vers A', et posons $\delta = \sigma^\eta_v$, alors d'après le Corollaire 6.6.8, δ est élément de $\mathcal{G}_{A'}(\eta(v))$, et d'après le Théorème 6.6.9, η est un isomorphisme de A^σ vers A'^δ. Comme $A_2 \simeq \mathrm{dm}(A^\sigma)$, on a $A_2 \simeq \mathrm{dm}(A'^\delta)$, et d'après le Lemme 10.3.11, $A'^\delta \simeq \mathrm{Strat}(A_2)$. Par transitivité de la relation $\simeq$, on en déduit que $A^\sigma \simeq \mathrm{Strat}(A_2)$.

2. D'après le Lemme 5.2.17, il existe un homomorphisme h de A vers T, d'après le Corollaire 6.6.8, il existe une permutation $\mu \in \mathcal{G}_A$ telle que $\sigma = \mu^h$, et d'après le Théorème 6.6.9, h est un homomorphisme de A^μ vers T^σ. Les A-termes $\mathrm{dm}(A^\mu)$ et $\mathrm{dm}(A)$ sont donc bisimilaires, et d'après le Corollaire 5.2.18, ils sont isomorphes. On a $A^\mu \simeq \mathrm{Strat}(\mathrm{dm}(A^\mu))$ d'après le point 1, et $A = \mathrm{Strat}(\mathrm{dm}(A))$ d'après la Propriété 10.3.4, d'où $A \simeq A^\mu$. Par transitivité de la relation $\stackrel{\circ}{=}$, on en déduit que $T^\sigma \stackrel{\circ}{=} T$. ■

Nous pouvons maintenant faire le lien entre la relation de congruence modulo E et la relation de congruence stratifiée.

Théorème 10.3.13 *Etant donnée une théorie permutative E définie par un ensemble d'axiomes, soient t un terme, $e : c \rightleftharpoons c^\sigma$ un axiome de E, et t' le terme obtenu après application de l'axiome e à la position p de t. Posons $A = \mathrm{As}(t)$ et $A' = \mathrm{As}(t')$, alors $A \bowtie A'$.*

PREUVE. On pose $A = (V, s, a)$, comme l'équation $c \rightleftharpoons c^\sigma$ peut être appliquée à la position p de t, nécessairement, $c \sqsubseteq A|p$. Supposons d'abord que le sommet p de A est étiqueté par un symbole $\langle f', c', G' \rangle \in \Sigma_E$. On définit C comme l'ensemble des contextes axiomatiques de E qui subsument $A|p$, alors $c' = \sqcup C$ par définition, et donc, $c \sqsubseteq c'$. Par hypothèse d'unif-stabilité, on a donc $c \sqsubseteq_\sigma c'$, et comme $G' = \Gamma_E(c')$, nécessairement, $\sigma' = \Phi[c, c', \varepsilon](\sigma) \in G'$. Posons $\mu = \sigma'^{\mathrm{h}_{[A,p]}}$, alors, d'après le Théorème 6.5.11, on a $\tau(\mathrm{dm}(A^\mu)) = t'$, et donc, $\mathrm{dm}(A^\mu)$ et $\mathrm{dm}(A')$ sont isomorphes. D'après la Propriété 10.3.4, on a donc $\mathrm{Strat}(\mathrm{dm}(A^\mu)) \simeq \mathrm{Strat}(\mathrm{dm}(A'))$, et d'après le le Corollaire 10.3.12, on en déduit que A^μ et A' sont isomorphes, c'est-à-dire que $A \bowtie A'$.

Supposons maintenant que le sommet p de A est étiqueté par le symoble $f' \in \Sigma$. Alors, comme l'ensemble C est non-vide, nécessairement, il existe un sommet u au-dessus de p dans A tel que $s(u) = \langle f'', c'', G'' \rangle \in \Sigma_E$, et $p \in \overline{\mathrm{R}}_A(u)$. Il existe donc un homomorphisme h et une position p' tels que $h, p' : c \trianglelefteq c'$, et par hypothèse d'unif-stabilité, on a $h, p' : c \trianglelefteq_\sigma c'$. Comme précédemment, on peut définir $\sigma' = \Phi[c, c', p'](\sigma)$ qui est élément de G', et $\mu = \sigma'^{\mathrm{h}_{[A,u]}}$, alors, d'après le Théorème 6.5.11, on a $\tau(\mathrm{dm}(A^\mu)) = t'$. Une fois de plus, on en déduit que $A \bowtie A'$. ∎

Corollaire 10.3.14 *Soient t et t' deux termes, et supposons que $t =_E t'$. Alors* $\mathrm{As}(t) \bowtie \mathrm{As}(t')$.

PREUVE. Comme $t =_E t'$, d'après le Théorème de Birkhoff (voir [BN98]), il existe une séquence $e_1, \ldots, e_n$ d'axiomes de E et une séquence $t_1, \ldots, t_{n+1}$ de termes tels que $t_1 = t$, $t_{n+1} = t'$, et pour tout $i = 1, \ldots, n$, t_{i+1} est obtenu en appliquant l'axiome e_i à la position p_i de t_i. Nous allons montrer par induction sur n que $A \bowtie A'$. Si $n = 1$, alors on a le résultat d'après le Théorème 10.3.13. Supposons maintenant que le résultat est vrai pour tout terme obtenu par une séquence de $n-1$ axiomes, et que t' est obtenu par une séquence de n axiomes. Considérons le terme t_2, qui est obtenu après l'application de l'axiome e_1 à la position p_1 de t. D'après le Théorème 10.3.13, en posant $A_2 = \mathrm{As}(t_2)$, on a $A \bowtie A_2$, et par hypothèse d'induction, $A_2 \bowtie A'$. Par transitivité de la relation $\bowtie$, on en déduit que $A \bowtie A'$, d'où le résultat. ∎

Théorème 10.3.15 *Soient A et A' deux* A*-termes clos, et posons $t = \tau(A)$, et $t' = \tau(A')$. Soient T et T' deux* GA*-termes stratifiés tels que $T \triangleq \mathrm{Strat}(A)$ et $T' \triangleq \mathrm{Strat}(A')$. Alors $t =_E t'$ si et seulement si $T \bowtie T'$.*

PREUVE. Comme $t = \tau(\mathrm{dm}(T))$ et $t' = \tau(\mathrm{dm}(T'))$, il est clair que si $T \bowtie T'$, alors $t =_E t'$ d'après le Corollaire 6.5.12. Réciproquement, si $t =_E t'$, alors $\mathrm{As}(t) \bowtie \mathrm{As}(t')$ d'après le Corollaire 10.3.14, et comme $A \simeq \mathrm{arbre}(t)$ et $A' \simeq \mathrm{arbre}(t')$, d'après la Propriété 10.3.4, on a $\mathrm{Strat}(A) \simeq \mathrm{As}(t)$ et $\mathrm{Strat}(A') \simeq \mathrm{As}(t')$. D'après le Lemme 7.1.5, on en déduit que $\mathrm{Strat}(A) \bowtie \mathrm{Strat}(A')$. D'après le Lemme 5.2.17, on a $T \Subset \mathrm{Strat}(A)$ et $T' \Subset \mathrm{Strat}(A')$, d'après le Lemme 7.1.5, on en déduit que

$$T \bowtie \mathrm{Strat}(A) \bowtie \mathrm{Strat}(A') \bowtie T',$$

et on a le résultat par transitivité de la relation $\bowtie$. ∎

On en déduit donc le résultat de complexité suivant :

Corollaire 10.3.16 *Le problème du mot généralisé modulo une théorie unif-stable est dans la classe de Luks.*

On a également le résultat de complétude suivant :

Corollaire 10.3.17 *Soit t un terme, et T un* GA*-terme tel que $T \triangleq \mathrm{As}(t)$, alors la classe de congruence de t modulo E est égale à $\mathrm{S}[T]$.*

PREUVE. L'ensemble $\mathrm{S}[T]$ est inclus dans la classe de congruence de t modulo E d'après le Corollaire 6.5.12. Réciproquement, si t' est congru à t modulo E, alors $\mathrm{As}(t') \bowtie T$ d'après le Théorème 10.3.15, et donc, il existe une permutation $\sigma \in \mathcal{G}_T$ telle que $T^\sigma \doteq T'$, d'où $t' = \tau(\mathrm{dm}(A^\sigma))$, et on a bien $t' \in \mathrm{S}[T]$. ∎

Complexité des problèmes liés à la déduction

Dans le Chapitre 8, nous avons défini cinq problèmes sur des GA-termes stratifiés, et démontré qu'ils sont tous **NP**-durs dans le cas général. Nous montrons maintenant que dans le cas où la signature stratifiée considérée est unif-stable, certains de ces problèmes sont plus simples à résoudre.

Théorème 10.3.18 *Soient t et t' deux termes, et T et T' deux* GA*-termes tels que $T \doteq \mathrm{As}(t)$, et $T' \doteq \mathrm{As}(t')$. Alors les propositions suivantes sont équivalentes :*

1. $\mathrm{S}[T] = \mathrm{S}[T']$,
2. $\mathrm{S}[T] \subseteq \mathrm{S}[T']$,
3. $\mathrm{S}[T] \cap \mathrm{S}[T'] \neq \emptyset$,
4. $T \bowtie T'$,
5. $t' \in \mathrm{S}[T]$.

PREUVE. Si $\mathrm{S}[T] = \mathrm{S}[T']$, alors on a évidemment $\mathrm{S}[T] \subseteq \mathrm{S}[T']$, et si $\mathrm{S}[T] \subseteq \mathrm{S}[T']$, alors on a $\mathrm{S}[T] \cap \mathrm{S}[T'] = \mathrm{S}[T] \neq \emptyset$.

Supposons maintenant que $\mathrm{S}[T] \cap \mathrm{S}[T'] \neq \emptyset$, et soit $t'' \in \mathrm{S}[T] \cap \mathrm{S}[T']$. Alors, d'après le Corollaire 6.5.12, $t =_E t''$ et $t' =_E t''$, d'où $t =_E t'$. D'après le Théorème 10.3.15, on en déduit que $T \bowtie T'$.

Si $T \bowtie T'$, alors pour tout $\sigma \in \mathcal{G}_T$, on a également $T^\sigma \bowtie T'$, et il existe une permutation $\pi \in \mathcal{G}_{T'}$ telle que $T^\sigma \doteq T'^\pi$. On a donc $\tau(\mathrm{dm}(T^\sigma)) = \tau(\mathrm{dm}(T'^\pi))$, ce qui prouve que $\mathrm{S}[T] \subseteq \mathrm{S}[T']$, et par symétrie, on a $\mathrm{S}[T] = \mathrm{S}[T']$.

Enfin, d'après le Corollaire 10.3.17, $t' \in \mathrm{S}[T]$ si et seulement si t et t' sont dans la même classe de congruence modulo E, et d'après le Théorème 10.3.15, on en déduit que $t' \in \mathrm{S}[T]$ si et seulement si $T \bowtie T'$. ∎

Corollaire 10.3.19 *Soit E une théorie permutative définie par un ensemble d'axiomes unif-stable, et considérons les restrictions des problèmes* 1, 3 *et* 5 *du Chapitre 8 au cas où les* GA*-termes stratifiés sont bisimilaires à des* A*-termes de la forme* $\mathrm{As}(t)$*. Alors ces restrictions sont toutes dans la classe de Luks.*

PREUVE. Tous ces problèmes sont équivalents au problème de la congruence stratifiée S_CONGR, qui est dans la classe de Luks (Théorème 7.3.8), et sont donc également dans la classe de Luks. ∎

10.4 NP-complétude des autres problèmes

Dans la partie précédente, nous avons vu que les restrictions de trois des cinq problèmes définis dans le Chapitre 8 au cas où la signature stratifiée considérées est unif-stable sont dans la classe de Luks. Nous allons maintenant montrer que les restrictions des deux problèmes restants, S_UNIF et S_SBT, au cas où la signature stratifiée considérée est unif-stable, demeurent NP-complets.

Notons ces restrictions S_UNIF_US et S_SBT_US, nous commençons par démontrer que le problème S_SBT_US est NP-complet, même si la théorie considérée est définie par un ensemble d'axiomes pseudo-orthogonal. Pour cela, nous allons démontrer que le problème GC_PART_RST se réduit polynomialement au problème S_SBT_US.

Soit une instance de GC_PART_RST, c'est-à-dire :
- un ensemble $\{\sigma_1, \ldots, \sigma_m\} \subseteq \mathrm{Sym}(n)$,
- des ensembles non vides $J_1, \ldots, J_n$ deux à deux disjoints ou égaux, tels que pour tout $i = 1, \ldots, n$, $J_i \subseteq \{1, \ldots, n\}$,
- un entier $k \in \{1, \ldots, n\}$.

On cherche donc à déterminer s'il existe une permutation γ dans le groupe G engendré par $\{\sigma_1, \ldots, \sigma_m\}$ telle que pour tout $i = 1, \ldots, k$, $i^\gamma \in J_i$.

Définition 10.4.1 Soit $\eta : \{1, \ldots, n\} \to \{1.1, \ldots, 1.k, 2, \ldots, n-k+1\}$ la bijection définie de la façon suivante ;

$$\eta(i) = \begin{cases} 1.i & \text{si } i \in \{1, \ldots, k\} \\ i - k + 1 & \text{sinon.} \end{cases}$$

Pour $j \in \{1, \ldots, m\}$, on définit la permutation $\mu_j = \sigma_j^\eta$, et on note G' le groupe engendré par $\{\mu_1, \ldots, \mu_m\}$. ◇

Exemple 10.4.2 Supposons que $n = 4$ et $k = 2$, et soit $\sigma = (1\ 3)(2\ 4)$, alors $\sigma^\eta = (1.1\ 2)(1.2\ 3)$.

Définition 10.4.3 Soit la signature $\Sigma = \{f, g, a_1, \ldots, a_n\}$, où f est d'arité $n - k + 1$, g est d'arité k, et les a_i sont des constantes distinctes deux à deux, et soit le contexte c tel que $\tau(c) = f(g(\circ, \ldots, \circ), \circ, \ldots, \circ)$. On considère la théorie permutative E définie par l'ensemble d'axiomes suivant :

$$A \ = \ \{c \rightleftharpoons c^{\mu_i} \mid i = 1, \ldots, m\}.$$

Posons $F = \langle f, c, G' \rangle$ et soit $\Sigma'_E = \{F\}$, alors cette signature stratifiée est clairement pseudo-orthogonale, et saturée.

On définit les termes t et t' de la façon suivante :

$$\begin{aligned} t &= f(g(b_1, \ldots, b_k), b_{k+1}, \ldots, b_n), \\ t' &= g(d_1, \ldots, d_k), \end{aligned}$$

où pour tout $i = 1, \ldots, n$, $b_i = a_l$, où $l = \min\{q \mid i \in J_q\}$, et pour tout $j = 1, \ldots, k$, $d_j = a_{l'}$, où $l' = \min\{q \mid J_j = J_q\}$. Enfin, on pose $A = \mathrm{As}(t)$. ◇

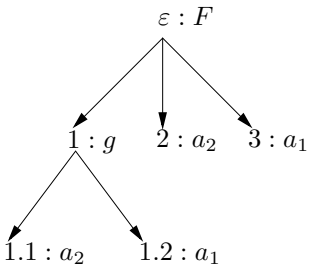

FIG. 10.4 – A-terme stratifié de l'Exemple 10.4.4

Exemple 10.4.4 Supposons que $n = 4$ et $k = 2$, et soient les ensembles

$$J_1 = \{2, 4\}\ J_2 = \{1, 3\},\ J_3 = \{1, 3\},\ \text{et}\ J_4 = \{2, 4\}.$$

Alors on a $t = f(g(a_2, a_1), a_2, a_1)$, $t' = g(a_1, a_2)$, et le A-terme A est représenté dans la Figure 10.4.

Remarque. Par construction, pour tout $i = 1, \ldots, n$, b_i étiquette le sommet $\eta(i)$ du A-terme A.

On a le théorème suivant :

Théorème 10.4.5 *Le terme t' est le sous-terme d'un élément de* $\mathrm{S}[A]$ *si et seulement s'il existe une permutation $\gamma \in G$ telle que pour tout $i = 1, \ldots, k$, $i^\gamma \in J_i$.*

PREUVE. Posons $A = (V, s, a)$, et pour $\mu \in \mathcal{G}_A$, supposons que t' est un sous-terme de $\tau(\mathrm{dm}(A^\mu))$. Comme le seul sommet de A à être étiqueté par un élément de Σ_E est sa racine et que $\mathrm{h}_{[A,\varepsilon]} = \mathrm{id}$, alors on a $\mathcal{G}_A = \mathcal{G}_A(\varepsilon) = G'$, et μ est donc un élément de G'. Comme seul le sommet 1 est étiqueté par le symbole g dans A, nécessairement, on a $t' = \tau(\mathrm{dm}(A^\mu|1))$, et par définition, on a

$$a^\mu(1) \ = \ (1.1)^\mu . \cdots . (1.k)^\mu,$$

donc, nécessairement, pour tout $i = 1, \ldots, k$, $s((1.i)^\mu) = d_i$.

Soit $\gamma \in G$ la permutation telle que $\mu = \gamma^\eta$, alors comme b_j étiquette le sommet $\eta(j)$ pour tout $j = 1, \ldots, n$, et que $\eta^{-1}(1.i) = i$ pour tout $i = 1, \ldots, k$, on en déduit que

$$s((1.i)^\mu) \ = \ s((1.i)^{\gamma^\eta}) \ = \ s(\eta([\eta^{-1}(1.i)]^\gamma)) \ = \ s(\eta(i^\gamma)) \ = \ b_{i^\gamma}.$$

Donc, en posant $t' = \tau(\mathrm{dm}(A^\mu|1))$, on a $b_{i^\gamma} = d_i$ pour tout $i = 1, \ldots, k$. Posons $a_l = b_{i^\gamma} = d_i$, alors par définition, $i^\gamma \in J_l$ et $J_l = J_i$, on en déduit que pour tout $i = 1, \ldots, k$, $i^\gamma \in J_i$.

Réciproquement s'il existe une permutation $\gamma \in G$ telle que pour tout $i = 1, \ldots, i$, $i^\gamma \in J_i$, en posant $\mu = \gamma^\eta$, il est aisé de vérifier que t' est un sous-terme de A^μ. ∎

D'après le Corollaire 6.6.11, si T est un GA-terme stratifié tel que $T \stackrel{\circ}{=} \mathrm{As}(t)$, alors $\mathrm{S}[T] = \mathrm{S}[\mathrm{As}(t)]$, donc :

Corollaire 10.4.6 *Pour tout* GA*-terme T, si $T \stackrel{\circ}{=} \mathrm{As}(t)$, alors t' est un sous-terme d'un élément de $\mathrm{S}[T]$ si et seulement s'il existe une permutation $\gamma \in G$ telle que pour tout $i = 1, \ldots, k$, $i^\gamma \in J_i$.*

Clairement, la transformation de l'instance de GC_PART_RST à l'instance de S_SBT_US est polynomiale, et on en déduit le résultat suivant :

Corollaire 10.4.7 *Le problème* GC_PART_RST *se réduit polynomialement au problème* S_SBT_US.

Le Corollaire 10.4.7 prouve donc que le problème S_SBT_US est **NP**-complet. Nous allons maintenant montrer que si on impose que la théorie permutative considérée soit définie par un ensemble d'axiomes plat, alors la restriction de ce problème est dans la classe de Luks.

La propriété vérifiée par les signatures stratifiées plates dont nous nous servirons est la suivante :

Lemme 10.4.8 *Si Σ_E est une signature stratifiée plate, alors pour tout terme t, si $A = (V, s, a) = \mathrm{arbre}(t)$, alors la procédure* st_rec *de l'algorithme construisant* $\mathrm{Strat}(A)$ *(Figure 10.2) est appelée sur tous les sommets de A.*

PREUVE. Ceci est évident : pour tout $\langle f, c, G\rangle \in \Sigma_E$, le contexte c est plat, et donc, pour tout sommet v de A étiqueté par un symbole de Σ_E, l'ensemble des sommets arguments de $a(v)$ et l'ensemble $\mathrm{R}_A(v)$ sont égaux. ∎

Corollaire 10.4.9 *Sous les hypothèses du Lemme 10.4.8, pour toute position p de t, les* A*-termes* $\mathrm{Strat}(A)|p$ *et* $\mathrm{As}(t|p)$ *sont isomorphes.*

PREUVE. Ceci est une conséquence immédiate de la Propriété 10.3.3. ∎

On a donc le résultat suivant :

Théorème 10.4.10 *Soient t et t' deux termes, p une position de t, et posons $A = \mathrm{As}(t)$. Alors il existe une permutation $\sigma \in \mathcal{G}_A$ telle que t' est égal à $\tau(\mathrm{dm}(A^\sigma|p))$ si et seulement si $\mathrm{As}(t') \bowtie A|p$.*

PREUVE. Posons $t_p = \tau(\mathrm{dm}(A^\sigma|p))$, et supposons que $t' = t_p$. Alors, $\mathrm{As}(t') = \mathrm{As}(t_p)$, et d'après le Corollaire 10.4.9, on en déduit que $\mathrm{As}(t')$ et $A^\sigma|p$ sont isomorphes. Soit σ_p la restriction de σ aux sommets de $A|p$, alors, d'après la Propriété 6.5.5, σ_p est élément de $\mathcal{G}_{A|p}$, et $A^\sigma|p = (A|p)^{\sigma_p}$. On en déduit donc que $\mathrm{As}(t') \bowtie A|p$.

Réciproquement, si $\mathrm{As}(t')$ et $A|p$ sont congrus, alors il existe une permutation $\sigma \in \mathcal{G}_{A|p}$ telle que $\mathrm{As}(t')$ et $(A|p)^\sigma$ sont isomorphes. Comme σ est également élément de $\mathcal{G}_A$, et $(A|p)^\sigma = A^\sigma|p$, on en déduit que $t' = \tau(\mathrm{dm}(A^\sigma|p))$. ∎

Corollaire 10.4.11 *Soient t, t' deux termes, et T un* GA*-terme stratifié tel que $T \stackrel{\circ}{=} \mathrm{As}(t)$, alors t' est un sous-terme d'un élément de $\mathrm{S}[T]$ si et seulement s'il existe un sommet v de T tel que $\mathrm{As}(t') \bowtie T|v$.*

Donc, quand la signature stratifiée considérée est plate, si nous prenons le problème S_CONGR comme oracle, alors nous pouvons décider en temps polynomial si t' est un sous-terme d'un élément de $\mathrm{S}[T]$. On a donc le résultat suivant :

Corollaire 10.4.12 *La restriction du problème* S_SBT *au cas où la signature stratifiée considérée est plate et $T \stackrel{\circ}{=} \mathrm{As}(t)$ pour un terme t donné est dans la classe de Luks.*

Ainsi, dans le cas où la théorie permutative considérée est définie par un ensemble d'axiomes plats, les restrictions de tous les problèmes définis dans le Chapitre 8, sauf le Problème 4, sont dans la classe de Luks. Prenons maintenant la théorie permutative E définie par l'axiome de commutativité $f(x, y) \rightleftharpoons f(y, x)$, cet axiome est plat, et donc unif-stable. Soient t_1, t_2 deux termes, et T_1, T_2 deux GA-termes stratifiés tels que $T_1 \stackrel{\circ}{=} \mathrm{As}(t_1)$, et $T_2 \stackrel{\circ}{=} \mathrm{As}(t_2)$. Alors il est clair que l'instance T_1, T_2 est solution de S_UNIF si et seulement si t_1 et t_2 sont unifiables modulo E. Or, on a le résultat suivant de [GJ79, problème AN16], ou [BN98] :

Théorème 10.4.13 *Le problème de l'unifiabilité modulo la théorie de la commutativité est* NP*-complet.*

On en déduit donc que

Corollaire 10.4.14 *La restriction du problème* S_UNIF *aux théories définies par des ensembles d'axiomes plats est* NP*-complet.*

Ainsi, même dans cette classe particulièrement restreinte de théories permutatives, le problème de l'unifiabilité stratifiée demeure NP-complet.

10.5 Résumé

Dans ce chapitre, nous avons défini les théories permutatives définies par des ensembles d'axiomes unif-stables, et démontré qu'elles vérifient de nombreuses propriétés intéressantes pour faire de la déduction avec des GA-termes stratifiés. Ainsi, étant donné une théorie permutative E définie par un ensemble d'axiomes unif-stable, nous avons démontré que pour tout terme t, il est possible de construire en temps polynomial un GA-terme stratifié T tel que la classe de congruence de t modulo E est égale à $\mathrm{S}[T]$. Puis, nous avons démontré que les restrictions des problèmes liés à la déduction définis dans le Chapitre 8, à l'exception du problème de l'unifiabilité stratifiée, sont tous dans la classe de Luks, tout comme le problème du mot généralisé modulo une théorie unif-stable. Enfin, nous avons vu que le problème de l'unifiabilité stratifiée demeure NP-complet, même pour une classe de théories permutatives particulièrement restreinte. Dans le prochain chapitre, nous allons voir que tout problème d'unification modulo une théorie définie par un ensemble d'axiomes unif-stable admet un CSU minimal de cardinalité finie.

Chapitre 11

Unif-stabilité et unification

Dans le Chapitre 9, nous avons vu qu'il existe des problèmes d'unification modulo une théorie permutative définie par un unique axiome qui sont infinitaires. Dans ce chapitre, nous allons présenter un algorithme qui permet de calculer un CSU fini pour tout problème d'unification modulo une théorie définie par un ensemble d'axiomes unif-stable.

Pour cela, nous définirons les problèmes d'unification sur des GA-termes. Comme dans le Chapitre 8, nous supposerons que la signature Σ contient un sous-ensemble $\mathcal{X}$ de constantes qui joueront le rôle de variables dans les GA-termes, pour les problèmes d'unification.

Il peut paraître surprenant de devoir considérer un tel ensemble $\mathcal{X}$ de constantes comme des variables, et de ne pas se servir des sommets variables des GA-termes. Nous avons choisi de ne pas nous servir de ces sommets variables pour des raisons de clarté. Par exemple, il est difficile de définir une notion de substitution basée sur ces sommets variables, comme le montre l'exemple suivant.

Exemple 11.0.1 Soit $\Sigma_E = \{\langle f, c, \mathrm{Sym}(3)\rangle\}$, où $\tau(c) = f(\circ, \circ, \circ)$, et soit $t = f(x, x, y)$, où x et y sont des variables. Il est clair que $\mathrm{arbre}(t) = c$. Supposons qu'on ait défini une notion de substitution appropriée sur les sommets variables de A, et qu'on cherche à appliquer une substitution $\gamma = \{x \leftarrow g(z, z)\}$ à t. Alors à γ on devrait associer une substitution θ qui aux sommets variables 1 et 2 de A associe des GA-termes T et T' tels que $T \stackrel{\circ}{=} T' \stackrel{\circ}{=} \mathrm{arbre}(g(z, z))$, et on aurait

$$\tau(A\theta) \;=\; f(g(\circ, \circ), g(\circ, \circ), \circ).$$

Puis, si on souhaite appliquer au terme $t\gamma$ la substitution $\gamma' = \{z \leftarrow a\}$, alors la substitution θ' correspondante devrait associer à quatre des sommets variables de $A\theta$ des GA-termes représentant la constante a.

Cette méthode est évidemment compliquée à mettre en oeuvre, et très inefficace. Une façon de procéder serait d'imposer que les sommets variables soient partagés. Cependant, ce partage est particulièrement difficile à réaliser, car nous devrons considérer plusieurs contextes pour résoudre les problèmes d'unification, et deux contextes peuvent avoir des sommets variables en commun, qu'il faut pourtant distinguer.

Le fait de considérer certaines constantes comme des variables et de ne considérer que des GA-termes clos permet d'éviter ces problèmes, même si les contextes à considérer nécessiteront un traitement particulier.

11.1 Unification sur des GA-termes

Notions standard

Dans ce qui suit, nous allons adapter les notions standard de l'unification sur des termes au cas des GA-termes, et définirons par exemple la notion de GA-*substitution*.

On suppose que la signature Σ contient un ensemble infini $\mathcal{X}$ de constantes, qui sont assimilées à des variables pour les problèmes d'unification, et qu'on dispose d'un ensemble infini $\mathbb{V}$ de sommets, ce qui nous permet de construire des GA-termes sur des ensembles de sommets disjoints. Sauf mention explicite, les éléments de $\mathcal{X}$ seront notés $x, y, z \ldots$

Pour simplifier certaines démonstrations, sauf indication contraire, nous supposerons que pour tout symbole de fonction f de Σ, la théorie E contient comme axiome l'équation triviale $f(x_1, \ldots, x_n) \rightleftharpoons f(x_1, \ldots, x_n)$. Ainsi, si Σ_E est une signature stratifiée qui est unif-stable par rapport à E et saturée, alors pour tout symbole de fonction $f \in \Sigma$, la signature stratifiée Σ_E contiendra l'élément $\langle f, c, \Gamma_E(c)\rangle$, où $\tau(c) = f(\circ, \ldots, \circ)$.

Nous supposons maintenant fixées la théorie permutative E, et la signature stratifiée Σ_E. Sauf mention explicite, nous supposerons que pour tout contexte c considéré, il existe un élément $\langle f, c, G\rangle$ dans Σ_E.

Définition 11.1.1 Etant donné un GA-terme $T = (V, s, a)$, on définit l'ensemble $\mathrm{Var}(T)$ par :

$$\mathrm{Var}(T) \;=\; s(V) \cap \mathcal{X}.$$

On étend cette définition aux ensembles de GA-termes de la façon suivante : si S est un ensemble de GA-termes, alors $\mathrm{Var}(S) = \cup_{T \in S} \mathrm{Var}(T)$.

Enfin, pour tout $x \in \mathcal{X}$, on définit le A-terme $A_x = (\{r_x\}, \langle r_x, x\rangle, \varepsilon)$. ◇

Définition 11.1.2 (GA-substitution) Soit $\{T_1, \ldots, T_n\}$ un ensemble de GA-termes, où pour tout $i = 1, \ldots, n$, $T_i = (V_i, s_i, a_i)$, une GA-*substitution* θ *pour* $T_1, \ldots, T_n$ est une fonction partielle finie de $\mathcal{X}$ vers l'ensemble des GA-termes sur Σ telle que :

- pour tout $\langle x, T\rangle, \langle x', T'\rangle \in \theta$, si $T = (V, s, a)$ et $T' = (V', s', a')$, alors $(T \neq T') \Rightarrow (V \cap V' = \emptyset)$,
- pour tout $i = 1, \ldots, n$, pour tout $\langle x, T\rangle \in \theta$, si $T = (V, s, a)$, alors $V \cap V_i = \emptyset$.

Par la suite, les éléments de θ seront notés $x \leftarrow T$ au lieu de $\langle x, T\rangle$, et s'il n'y a pas d'ambiguïté possible, on dira simplement que θ est une GA-substitution, sans préciser pour quels GA-termes.

Etant donnée une GA-substitution θ, on définit les ensembles $\mathrm{Dom}(\theta)$ et $\mathrm{Ran}(\theta)$ par :

$$\begin{aligned} \mathrm{Dom}(\theta) &= \{x \mid x \leftarrow T \in \theta\}, \\ \mathrm{Ran}(\theta) &= \{T \mid x \leftarrow T \in \theta\}. \end{aligned}$$

La *cardinalité* de la GA-substitution θ est alors définie par $|\theta| = |\mathrm{Dom}(\theta)|$.

Enfin, par abus de notation, si $x \leftarrow T \in \theta$, alors on pourra noter $A_x\theta$ au lieu de T.$\diamond$

Définition 11.1.3 (Application d'une GA-substitution) Soient $T = (V, s, a)$ un GA-terme et $\theta = \{x_1 \leftarrow T_1, \ldots, x_n \leftarrow T_n\}$ une GA-substitution pour T, où pour tout $i = 1, \ldots, n$, $T_i = (V_i, s_i, a_i)$ est de racine r_i. On note

$$V_\theta \ = \ \{v \in V \mid s(v) \in \mathrm{Dom}(\theta)\},$$

et on définit le GA-terme $T\theta = (V', s', a')$ de la façon suivante :

- $V' \ = \ (V \setminus V_\theta) \uplus \biguplus \{V_i \mid v \in V_\theta \wedge s(v) = x_i\}$,
- Pour tout $v \in V \setminus V_\theta$, $s'(v) = v$, et pour tout $v \in V_i$, $s'(v) = s_i(v)$,
- Pour tout $v \in V \setminus V_\theta$, et pour tout $j \in \{1, \ldots, \text{arité}(s(v))\}$,

$$a'(v)_j = \begin{cases} r_i & \text{si } s(a(v)_j) = x_i \in \mathrm{Dom}(\theta), \\ a(v)_j & \text{sinon.} \end{cases}$$

- Pour tout $v \in V_i$, $a'(v) = a_i(v)$.

Etant donnés un ensemble S de GA-termes et une GA-substitution θ pour S, on définit l'ensemble

$$S\theta \ = \ \{T\theta \mid T \in S\}. \qquad \diamond$$

Exemple 11.1.4 Soient A_1 et A_2 les deux A-termes en haut de la Figure 11.1, et soit $\theta = \{x \leftarrow A_1, y \leftarrow A_2\}$. Si T est le GA-terme en bas à gauche de la Figure 11.1, qui représente donc le terme $f(x, y, y)$, alors θ est une GA-substitution pour T, et le GA-terme $T\theta$ est représenté en bas à droite de la Figure 11.1.

Remarque. Il est clair que pour tout $x \in \mathcal{X}$, si $x \leftarrow T \in \theta$, alors $A_x\theta = T$, ce qui justifie la notation introduite dans la Définition 11.1.2.

On a les propriétés suivantes :

Propriété 11.1.5 *Soit T un GA-terme, c un contexte, θ une GA-substitution, et supposons qu'il existe un homomorphisme h de c vers T, alors il existe également un homomorphisme de c vers $T\theta$.*

Propriété 11.1.6 *Soit T un GA-terme, et θ une GA-substitution, alors pour tout sommet v de T, on a $T\theta|v = (T|v)\theta$.*

Définition 11.1.7 ($\tau(\theta)$) Soit θ une GA-substitution, alors on note $\tau(\theta)$ la substitution définie par :

$$\tau(\theta) \ = \ \{x \leftarrow \tau(T) \mid x \leftarrow T \in \theta\}.$$

Si U est un ensemble de GA-substitutions, alors on définit

$$\tau(U) \ = \ \{\tau(\theta) \mid \theta \in U\}. \qquad \diamond$$

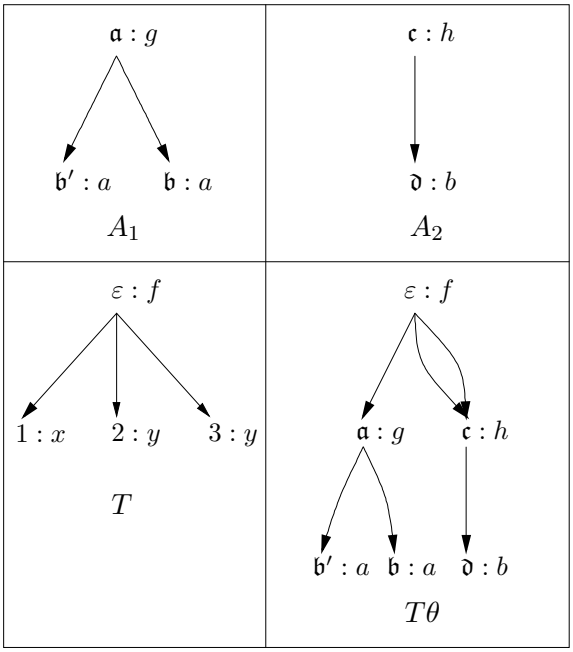

FIG. 11.1 – GA-termes de l'Exemple 11.1.4

Exemple 11.1.8 Reprenons la GA-substitution θ de l'Exemple 11.1.4, alors on a $\tau(\theta) = \{x \leftarrow g(a,a), y \leftarrow h(b)\}$.

La propriété suivante fait le lien entre une GA-substitution et la substitution qui lui est associée.

Propriété 11.1.9 *Pour tout* GA*-terme T, et pour toute* GA*-substitution θ, si $t = \tau(T)$ et $\gamma = \tau(\theta)$, alors $\tau(T\theta) = t\gamma$.*

Nous adaptons maintenant d'autres notions standard sur les substitutions au cas des GA-substitutions.

Définition 11.1.10 (GA-substitutions bisimilaires) Deux GA-substitutions θ et θ' sont dites *bisimilaires* si et seulement si $\mathrm{Dom}(\theta) = \mathrm{Dom}(\theta')$, et pour tout $x \in \mathrm{Dom}(\theta)$, $A_x\theta \stackrel{\circ}{=} A_x\theta'$. ◇

Propriété 11.1.11 *Soient θ et θ' deux* GA*-substitutions, alors $\theta \stackrel{\circ}{=} \theta'$ si et seulement si $\tau(\theta) = \tau(\theta')$.*

Définition 11.1.12 (Composition de GA-substitutions) Soit une GA-substitution $\theta = \{x_i \leftarrow T_i \mid i = 1, \ldots, n\}$ pour un GA-terme T, et soit θ' une GA-substitution pour $\{T\} \cup \mathrm{Ran}(\theta)$. Alors on définit la GA-substitution $\theta\theta'$ par :

$$\theta\theta' \;=\; \{x_i \leftarrow T_i\theta' \mid i = 1, \ldots, n\} \;\cup\; \{x' \leftarrow T_{x'}\theta' \mid x' \in \mathrm{Dom}(\theta') \setminus \mathrm{Dom}(\theta)\}.$$

Une GA-substitution θ est dite *idempotente* si et seulement si $\theta\theta = \theta$. $\diamond$

Propriété 11.1.13 *Soient θ, θ' et θ'' trois GA-substitutions telles que θ' est une GA-substitution pour $\mathrm{Ran}(\theta)$, et θ'' est une GA-substitution pour $\mathrm{Ran}(\theta) \cup \mathrm{Ran}(\theta')$. Alors on a :*

- $\tau(\theta\theta') = \tau(\theta)\tau(\theta')$,
- $(\theta\theta')\theta'' \stackrel{\circ}{=} \theta(\theta'\theta'')$.

Définition 11.1.14 Soient θ et θ' deux GA-substitutions, alors on dit que θ est *plus générale que θ' modulo E sur $X \subset \mathcal{X}$*, ce qu'on note $\theta \lesssim_E^X \theta'$, si et seulement s'il existe une GA-substitution ϕ pour $\mathrm{Ran}(\theta)$ telle que pour tout $x \in \mathrm{Dom}(\theta) \cap X$, $\tau(A_x\theta\phi) =_E \tau(A_x\theta')$. Si E est la théorie vide, on notera $\theta \lesssim \theta'$.

Enfin, on notera $\theta \sim_E^X \theta'$ (resp. $\theta \sim \theta'$) si et seulement si $\theta \lesssim_E^X \theta'$ et $\theta' \lesssim_E^X \theta$ (resp. $\theta \lesssim \theta'$ et $\theta' \lesssim \theta$). $\diamond$

Exemple 11.1.15 Soit E la théorie permutative définie par l'unique axiome

$$f(g(x_1, x_2), x_3) \rightleftharpoons f(g(x_3, x_2), x_1),$$

notons c le contexte tel que $\tau(c) = f(g(\circ, \circ), \circ)$, soit $G = \mathrm{Sym}(\{1.1, 2\})$, et posons $F = \langle f, c, G\rangle$. Alors la signature stratifiée $\Sigma_E = \{F\}$ est unif-stable par rapport à l'axiome définissant E.

On définit les GA-substitutions θ et θ' telles que :

$$\tau(\theta) = \{x \leftarrow f(y, a)\}, \text{ et } \tau(\theta') = \{x \leftarrow f(g(a, b), z)\}.$$

Soit $X = \{x\}$, alors $\theta \lesssim_E^X \theta'$. En effet, prenons une GA-substitution ϕ telle que $\tau(\phi) = \{y \leftarrow g(z, b)\}$, et posons $T = A_x\theta\phi$, et $T' = A_x\theta'$. Soient A et A' des A-termes tels que $A \stackrel{\circ}{=} T$ et $A' \stackrel{\circ}{=} T'$, alors il est clair que les racines respectives r et r' de $\mathrm{Strat}(A)$ et $\mathrm{Strat}(A')$ sont toutes deux étiquetées par le symbole F. Soient $\sigma = (1.1\ 2) \in G$, et $\mu = \sigma^{\mathrm{h}_{[A,r]}}$, alors il est aisé de vérifier que $(\mathrm{Strat}(A))^\mu \stackrel{\circ}{=} \mathrm{Strat}(A')$, ce qui prouve que $\mathrm{Strat}(A) \bowtie \mathrm{Strat}(A')$. D'après le Théorème 10.3.15, on en déduit que $\tau(A) =_E \tau(A')$, d'où $\tau(T) =_E \tau(T')$.

Propriété 11.1.16 *Soient θ et θ' deux GA-substitutions, et $X \subset \mathcal{X}$, alors $\theta \lesssim_E^X \theta'$ si et seulement si $\tau(\theta) \lesssim_E^X \tau(\theta')$.*

PREUVE. Par définition, $\theta \lesssim_E^X \theta'$ si et seulement s'il existe une GA-substitution ϕ pour $\mathrm{Ran}(\theta)$ telle que pour tout $x \in \mathrm{Dom}(\theta) \cap X$, $\tau(A_x\theta\phi) =_E \tau(A_x\theta')$. D'après la Propriété 11.1.13, on a $\tau(A_x\theta\phi) = x\tau(\theta)\tau(\phi)$, d'où le résultat. ∎

Définition 11.1.17 (Unification) Soit $\{T_1, \ldots, T_n, T'_1, \ldots, T'_n\}$ un ensemble de GA-termes, tels que pour tout $i = 1, \ldots, n$, $T_i = (V_i, s_i, a_i)$ et $T'_i = (V'_i, s'_i, a'_i)$. On dit que l'ensemble $S = \{T_1 =_E^? T'_1, \ldots, T_n =_E^? T'_n\}$ est un *problème de E-unification sur des GA-termes*. Une GA-substitution θ est une *solution* de S si et seulement si

$\forall i = 1, \ldots, n,\ \tau(T_i\theta) =_E \tau(T'_i\theta)$. On définit également le problème de E-unification $\tau(S)$ par :

$$\tau(S) = \{\tau(T_1) =^?_E \tau(T'_1), \ldots, \tau(T_n) =^?_E \tau(T'_n)\}.$$

On dit que S est *sous forme résolue* si et seulement si

$$\tau(S) = \{x_1 =^?_E \tau(T'_1),\ \ldots,\ x_n =^?_E \tau(T'_n)\},$$

où pour tout $i = 1, \ldots, n$, $x_i \in \mathcal{X}$ n'apparaît qu'une fois dans $\tau(S)$. On appelle alors GA-*substitution induite par* S toute GA-substitution θ telle que

$$\tau(\theta) \ = \ \{x_i \leftarrow \tau(T'_i) \mid i = 1, \ldots, n\}.$$

On dit que S est de *cardinalité* $|S| = n$, on définit *l'ensemble des sommets de* S par $\mathrm{Som}(S) = \bigcup_{i=1}^{n}(V_i \cup V'_i)$, et on définit la *taille* de S par $\|S\| = |\mathrm{Som}(S)|$. Enfin, l'ensemble des variables de S est $\mathrm{Var}(S) = \bigcup_{T =^?_E T'}(\mathrm{Var}(T) \cup \mathrm{Var}(T'))$.

Si E est la théorie vide, on dira qu'on a un *problème d'unification syntaxique sur des* GA-*termes*, et on notera

$$S \ = \ \{T_1 =^? T'_1,\ \ldots,\ T_n =^? T'_n\},$$

on notera également

$$\tau(S) \ = \ \{\tau(T_1) =^? \tau(T'_1), \ldots, \tau(T_n) =^? \tau(T'_n)\}.$$

Un *problème de* E*-unification étendu sur des* GA-*termes* M est un ensemble de problèmes de E-unification sur des GA-termes, et on note

$$\tau(M) \ = \ \{\tau(S) \mid S \in M\}.$$

Si tous les problèmes de E-unification dans M sont sous forme résolue, on dit que M est sous-forme résolue, et on appelle *ensemble de* GA-*substitutions induit par* M tout ensemble de la forme $\bigcup_{S \in M} \theta_S$, où pour tout $S \in M$, θ_S est une GA-substitution induite par S.

L'ensemble des solutions d'un problème de E-unification sur des GA-termes S est noté $\mathcal{U}_E(S)$, et l'ensemble des solutions d'un problème de E-unification étendu sur des GA-termes M est défini par

$$\mathcal{U}_E(M) \ = \ \bigcup_{S \in M} \mathcal{U}_E(S).$$

◇

Remarque. Si $S = \emptyset$, alors S est trivialement sous forme résolue, et on a $\theta_S = \emptyset$.

Propriété 11.1.18 *Soient S un problème d'unification sur des* GA-*termes et θ une* GA-*substitution, alors θ est solution de S si et seulement si $\tau(\theta)$ est solution de $\tau(S)$. On a donc $\tau(\mathcal{U}_E(S)) = \mathcal{U}_E(\tau(S))$.*

Définition 11.1.19 Soient S un problème de E-unification sur des GA-termes, et X l'ensemble des éléments de $\mathcal{X}$ qui apparaissent dans S, alors un ensemble U de GA-substitutions est un *ensemble complet d'unificateurs*, ou CSU de S si et seulement si $U \subseteq \mathcal{U}_E(S)$, et pour toute GA-substitution $\theta' \in \mathcal{U}_E(S)$, il existe $\theta \in U$ telle que $\theta \lesssim_E^X \theta'$.

S'il existe un CSU de S qui contient un élément unique, on dit que cet élément est un *unificateur le plus général* (ou mgu) pour S. ◇

Lemme 11.1.20 *Soit S un problème de E-unification sur des GA-termes, alors $U \subseteq \mathcal{U}_E(S)$ est un CSU de S si et seulement si $\tau(U)$ est un CSU de $\tau(S)$.*

PREUVE. D'après la Propriété 11.1.18, $U \subseteq \mathcal{U}_E(S)$ si et seulement si $\tau(U) \subseteq \mathcal{U}_E(\tau(S))$, et pour tout $\theta' \in \mathcal{U}_E(S)$, la GA-substitution $\theta \in U$ vérifie $\theta \lesssim_E^X \theta'$ si et seulement si $\tau(\theta) \lesssim_E^X \tau(\theta')$ d'après la Propriété 11.1.16. ■

Propriété 11.1.21 *Si S est un problème de E-unification sous forme résolue, alors θ_S est un mgu pour S. Si M est un problème de E-unification sous forme résolue, alors tout ensemble de GA-substitutions induit par M est un CSU pour M.*

Remarque. D'après le Lemme 11.1.20, il existe toujours une GA-substitution idempotente qui est un mgu d'un problème d'unification syntaxique sur des GA-termes donné. Par la suite, étant donné un tel problème d'unification, nous ne considérerons que des mgu idempotents de ce problème.

Unification avec des contextes

Nous aurons besoin par la suite de considérer des problèmes d'unification dans lesquels apparaissent des contextes, bien que ces derniers ne soient pas des GA-termes clos. Nous allons maintenant définir des A-termes clos qui représenteront ces contextes et démontrer plusieurs propriétés vérifiées par ces A-termes, et les contextes qu'ils représentent.

Définition 11.1.22 (Fonction de clôture) Soit c un contexte, X un sous-ensemble fini de $\mathcal{X}$, et V' un sous-ensemble fini de $\mathbb{V}$. Alors l'image de c par la fonction $\mathrm{Cl}_{[X,V']}$ est un A-terme $A = (V, s, a)$ tel que :

- $V \subseteq \mathbb{V} \setminus V'$,
- il existe un homomorphisme h de c vers A,
- pour tout sommet $v \in \mathcal{SV}(c)$, $s(h(v)) \in \mathcal{X} \setminus X$, et pour tout $v' \in \mathcal{SV}(c)$, si $v \neq v'$, alors $s(h(v)) \neq s(h(v'))$.

S'il n'y a pas d'ambiguïté, on pourra noter $\mathrm{Cl}(c)$ au lieu de $\mathrm{Cl}_{[X,V']}(c)$. ◇

Exemple 11.1.23 Soit c le contexte représenté à gauche dans la Figure 11.2, on a donc $\tau(c) = f(g(\circ, \circ), \circ)$. Supposons que $V' = \{\varepsilon, 1, 1.1, 1.2, 2\}$, et $X = \emptyset$, alors $\mathrm{Cl}_{[X,V']}(c)$ est représenté à droite de la même figure.

Propriété 11.1.24 *Soit c un contexte, T un GA-terme, et posons $A' = \mathrm{Cl}(c) = (V', s', a')$. Alors il existe un homomorphisme h de c vers T si et seulement s'il existe une GA-substitution θ telle que $A'\theta \doteq T$.*

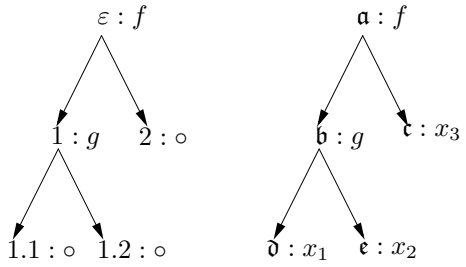

FIG. 11.2 – Le contexte c et le A-terme $\mathrm{Cl}_{[\mathcal{X}',V']}(c)$ de l'Exemple 11.1.23

PREUVE. Notons h' l'homomorphisme de c vers A', et supposons qu'il existe un homomorphisme h de c vers T. Alors on définit la GA-substitution θ de la façon suivante : pour tout $v \in \mathcal{SV}(c)$, si $s'(h'(v)) = x$, alors $\tau(A_x\theta) = \tau(T|h(v))$. Il est alors clair que pour tout $v \in \mathcal{SV}(c)$, $(A'\theta)|h'(v) \stackrel{\circ}{=} T|h(v)$, et comme h est un homomorphisme de c vers T, on a bien $A'\theta \stackrel{\circ}{=} T$.

Réciproquement, si $A'\theta \stackrel{\circ}{=} T$, alors, comme il existe un homomorphisme de c vers $A'\theta$, d'après le Lemme 5.2.15, il existe également un homomorphisme de c vers T. ■

Définition 11.1.25 ($\gamma_c(T, T')$) Soient $T = (V, s, a), T' = (V', s', a')$ deux GA-termes, et c un contexte. Si $c \sqsubseteq T$ et $c \sqsubseteq T'$, on pose $\gamma_c(T, T') = \emptyset$. Sinon, on considère deux A-termes $A_1 = (V_1, s_1, a_1)$ et $A_2 = (V_2, s_2, a_2)$ de la forme $\mathrm{Cl}(c)$, construits sur des ensembles disjoints de sommets et de variables, et tels que pour $i = 1, 2$,

$$V_i \cap (V \cup V') = \emptyset, \text{ et } \mathrm{Var}(A_i) \cap (\mathrm{Var}(T) \cup \mathrm{Var}(T')) = \emptyset.$$

S'il existe un mgu pour le problème d'unification syntaxique

$$\{T =^? A_1,\ T' =^? A_2\},$$

alors on note $\gamma_c(T, T')$ sa restriction à $\mathrm{Var}(T) \cup \mathrm{Var}(T')$. ◇

Exemple 11.1.26 Soient T, T' des GA-termes tels que $\tau(T) = f(x, a)$, et $\tau(T') = f(g(a, y), x)$, et soit c un contexte tel que $\tau(c) = f(g(\circ, \circ), \circ)$. Considérons le problème d'unification syntaxique S tel que

$$\tau(S) = \{f(x, a) =^? f(g(x_1, x_2), x_3),\ f(g(a, y), x) =^? f(g(x_4, x_5), x_6)\}.$$

Il existe un mgu pour S, et donc, la GA-substitution $\theta = \gamma_c(T, T')$ est bien définie, et vérifie $\tau(\theta) = \{x \leftarrow g(x_1, x_2), y \leftarrow x_5\}$. On a donc

$$\tau(T\theta) = f(g(x_1, x_2), a), \text{ et } \tau(T'\theta) = f(g(a, x_5), g(x_1, x_2)).$$

Propriété 11.1.27 *Soient T et T' deux* GA*-termes et c un contexte, si $\gamma_c(T,T')$ existe, alors il existe un homomorphisme de c vers $T\gamma_c(T,T')$.*

PREUVE. Si $c \sqsubseteq T$ et $c \sqsubseteq T'$, alors le résultat est trivial. Sinon, soit θ un mgu du problème d'unification syntaxique $\{T =^? A_1,\ T' =^? A_2\}$, alors on a $T\theta \stackrel{\circ}{=} A_1\theta$, et il existe donc un homomorphisme h' de $A_1\theta$ vers $T\theta$ d'après le Lemme 5.2.17. Par définition, il existe un homomorphisme de c vers A_1, et d'après la Propriété 11.1.5, il existe un homomorphisme h de c vers $A_1\theta$. On en déduit que $h' \circ h$ est un homomorphisme de c vers $T\theta = T\gamma_c(T,T')$, d'où le résultat. ∎

Lemme 11.1.28 *Sous les hypothèses de la Définition 11.1.25, supposons que les racines de T et T' sont étiquetées par un symbole de $\Sigma \setminus \mathcal{X}$, et supposons qu'il existe un mgu θ pour le problème d'unification $\{T =^? A_1,\ T' =^? A_2\}$.*

Soit une variable $x \in (\mathrm{Var}(T) \cup \mathrm{Var}(T')) \cap \mathrm{Dom}(\theta)$, posons $T'' = A_x\theta$, et soit w un sommet non-variable de T''. Alors il existe un sommet non-variable v de c, qui n'est pas la racine de c, tel que $c|v \sqsubseteq T''|w$.

PREUVE. On pose $\gamma = \tau(\theta)$, $t = \tau(T)$, $t' = \tau(T')$, $t_1 = \tau(A_1)$, $t_2 = \tau(A_2)$. Soit $x \in (\mathrm{Var}(t) \cup \mathrm{Var}(t')) \cap \mathrm{Dom}(\gamma)$, et notons $s = \tau(T''|w)$, nous allons montrer que s est une instance de $t_1|v$.

Soit P_1 (resp. P_2) l'ensemble des positions p telles que $t|p = x$ (resp. $t'|p = x$), et $P = \mathrm{Pos}(t_1) = \mathrm{Pos}(t_2)$. Comme les racines de T et T' ne sont pas des symboles de $\mathcal{X}$, il est clair que ε n'est élément ni de P_1, ni de P_2. Supposons que, partant du problème d'unification syntaxique $\{t =^? t_1, t' =^? t_2\}$, on n'applique que la règle de décomposition standard. On obtient alors un problème de la forme $S \cup S'$, où

$$S \ = \ \{x =^? t_1|p \mid p \in P_1 \cap P\} \cup \{x =^? t_2|p \mid p \in P_2 \cap P\},$$

et où x n'apparaît pas dans S'. Comme seule la règle de décomposition a été appliquée, et que t_1 et t_2 sont des termes linéaires, on a $\mathrm{Var}(S) \cap \mathrm{Var}(S') = \emptyset$. On en déduit que la restriction de γ à $\mathrm{Var}(S)$ est un mgu de S, et comme x n'apparaît pas dans les $t_i|p$, il est clair que $x\gamma$ est l'instance la plus générale de ces termes linéaires.

Notons $f \in \Sigma$ le symbole de tête de s, et q la position de $x\gamma$ telle que $s = (x\gamma)|q$. Alors il existe au moins un terme $t_1|p$ dont le symbole de tête à la position q est f. Le terme $x\gamma$ est alors instance du sous-terme $(t_1|p)|q = t_1|p.q$, et si on pose $v = p.q$, alors v est un sommet non-variable de c et est différent de la racine de c, et s est bien une instance de $t_1|v$.

Comme s est une instance de $t_1|v$, on en déduit qu'il existe une GA-substitution θ telle que $(A_1|v)\theta \stackrel{\circ}{=} T''|w$, et d'après la Propriété 11.1.24, il existe un homomorphisme de $c|v$ vers $T''|w$. ∎

Lemme 11.1.29 *Soient T et T' deux* GA*-termes, c un contexte, et ϕ une* GA*-substitution telle que $c \sqsubseteq T\phi$ et $c \sqsubseteq T'\phi$. Alors $\gamma_c(T,T') \lesssim \phi$.*

PREUVE. Soit $S = \{T =^? A_1, T' =^? A_2\}$ le problème d'unification syntaxique tel que $\gamma_c(T, T')$ est la restriction d'un mgu de S à $\mathrm{Var}(T) \cup \mathrm{Var}(T')$. Notons $X = \mathrm{Var}(A_1) \cup \mathrm{Var}(A_2)$, et $Y = \mathrm{Var}(T) \cup \mathrm{Var}(T')$, il est clair qu'il existe une permutation $\sigma \in \mathrm{Sym}(\mathcal{X})$ telle qu'aucune variable de X n'apparaît dans le domaine ou le codomaine de $\phi' = \phi\sigma$, et ϕ' est également solution de S. Comme $c \sqsubseteq T\phi'$ et $c \sqsubseteq T'\phi'$, d'après la Propriété 11.1.24, il existe des GA-substitutions δ_1 et δ_2, dont les domaines sont respectivement inclus dans $\mathrm{Var}(A_1)$ et $\mathrm{Var}(A_2)$, telles que $T\phi' \doteq A_1\delta_1$ et $T'\phi' \doteq A_2\delta_2$. Par construction, $\mathrm{Var}(A_1) \cap \mathrm{Var}(A_2) = \emptyset$, et la GA-substitution $\delta = \delta_1 \cup \delta_2$ est donc bien définie. On a alors :

$$\begin{array}{rcl} T\phi'\delta & = & T\phi' \quad \text{et} \quad T'\phi'\delta = T'\phi', \\ A_1\phi'\delta & = & A_1\delta \quad \text{et} \quad A_2\phi'\delta = A_2\delta. \end{array}$$

Ceci prouve donc que la GA-substitution $\phi'\delta$ est solution de S, et est donc subsumée par le mgu considéré. La restriction de $\phi'\delta$ à Y est égale à ϕ', qui est donc subsumée par $\gamma_c(T, T')$, et il existe une GA-substitution δ' telle que $\gamma_c(T, T')\delta' \doteq \phi' = \phi\sigma$. On en déduit que $\gamma_c(T, T')\delta'\sigma^{-1} \doteq \phi$, d'où le résultat. ∎

Nous allons maintenant définir une opération de greffage sur des GA-termes.

Définition 11.1.30 ($T[v \rightsquigarrow r_1]$) Soient $T = (V, s, a)$ et $T_1 = (V_1, s_1, a_1)$ deux GA-termes tels que si $V \cap V_1 \neq \emptyset$, alors il existe un sommet $u \in V$ tel que $T_1 = T|u$.

Notons r_1 la racine de T_1, étant donné un sommet v, on définit le GA-terme $T[v \rightsquigarrow r_1]$ de la façon suivante : si $v \notin V$, alors $T[v \rightsquigarrow r_1] = T$, sinon, posons $V_v = V|v$, alors $T[v \rightsquigarrow r_1] = (V', s', a')$ où :

- $V' = (V \setminus V_v) \cup V_1$,
- $\forall u \in V_1$, $s'(u) = s_1(u)$ et $a'(u) = a_1(u)$,
- $\forall u \in V \setminus V_v$, $s'(u) = s(u)$, et pour tout $i \in \{1, \ldots, \text{arité}(s(u))\}$, si $a(u)_i = v$, alors $a'(u)_i = r_1$, sinon $a'(u)_i = a(u)_i$.

Si S est un problème de E-unification sur des GA-termes, alors on définit

$$S[v \rightsquigarrow r_1] \;=\; \{T[v \rightsquigarrow r_1] =^?_E T'[v \rightsquigarrow r_1] \mid T =^?_E T' \in S\}. \qquad \diamond$$

Exemple 11.1.31 Considérons les GA-termes T et T_1, à gauche de la Figure 11.3, alors le GA-terme $T[\mathfrak{c} \rightsquigarrow \mathfrak{d}]$ est représenté à droite de la même figure.

On a les propriétés suivantes :

Propriété 11.1.32 *Soient $T = (V, s, a)$, $T' = (V', s', a')$ et $T'' = (V'', s'', a'')$ trois GA-termes de racines respectives r, r' et r'', dont les ensembles de sommets sont deux à deux disjoints. Alors on a :*

- $T[r \rightsquigarrow r] = T$,
- $(T[r \rightsquigarrow r'])[r' \rightsquigarrow r''] = T[r \rightsquigarrow r'']$,
- $(T[r \rightsquigarrow r'])[r' \rightsquigarrow r] = T$.

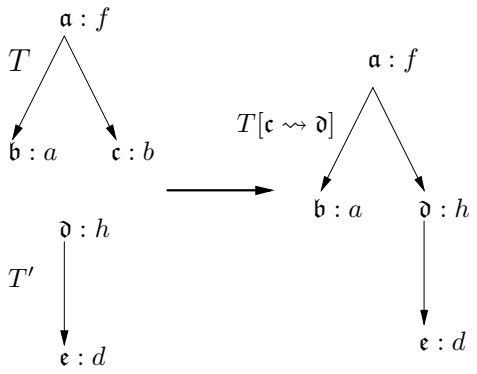

FIG. 11.3 – Un exemple de greffage

Montrons que l'ensemble des solutions d'un problème d'unification est également conservé par cette opération :

Propriété 11.1.33 *Soit $S' = \{T =^?_E T'\} \cup S$ un problème de E-unification sur des* GA-*termes, où T et T' sont de racines respectives r et r', et θ une solution de S', alors θ est solution de $\{T =^?_E T'\} \cup S[r \rightsquigarrow r']$.*

Lemme 11.1.34 *Soient $T = (V, s, a)$ et $T' = (V', s', a')$ deux* GA-*termes de racines respectives r et r', et $S' = \{T =^?_E T'\} \cup S$ un problème d'unification sur des* GA-*termes, alors*

$$\mathcal{U}_E(S') \;=\; \mathcal{U}_E(\{T =^?_E T'\} \cup S[r \rightsquigarrow r']).$$

PREUVE. D'après la Propriété 11.1.33, on a

$$\mathcal{U}_E(S') \subseteq \mathcal{U}_E(\{T =^?_E T'\} \cup S[r \rightsquigarrow r']),$$

montrons maintenant l'inclusion réciproque. Soit θ une solution du problème d'unification $\{T =^?_E T'\} \cup S[r \rightsquigarrow r']$, et considérons $T_1 = (V_1, s_1, a_1)$ un GA-terme isomorphe à T', et tel que $V_1 \cap (V \cup V') = \emptyset$. Notons r_1 la racine de T_1, alors il est clair que θ est également solution de $\{T =^?_E T_1\} \cup S[r \rightsquigarrow r_1]$. D'après la Propriété 11.1.33, on en déduit que θ est solution de $\{T =^?_E T_1\} \cup (S[r \rightsquigarrow r_1])[r_1 \rightsquigarrow r]$, et d'après la Propriété 11.1.32, θ est donc solution de $\{T =^?_E T_1\} \cup S$. Comme T_1 et T' sont isomorphes, θ est également solution de S', d'où l'égalité. ∎

Définition 11.1.35 ($T \nprec c$ et $\mathbf{V}_{T,c}$) Soient $T = (V, s, a)$ un GA-terme, et $\langle f, c, G\rangle$ un élément de Σ_E, alors on note $T \nprec c$ si et seulement si

– il n'existe aucun homomorphisme de c vers T,

– il existe une GA-substitution θ telle que $c \sqsubseteq T\theta$.

Etant donnés un GA-terme T et un contexte c, on définit l'ensemble

$$\mathrm{V}_{T,c} \;=\; \{\langle T|v, c\rangle \mid v \in V \wedge s(v) \notin \mathcal{X} \wedge T|v \nprec c\}.$$

Si S est un problème de E-unification, alors on définit l'ensemble

$$\mathcal{V}(S) \;=\; \bigcup_{\langle f,c,G\rangle \in \Sigma_E,\ T =^?_E T' \in S} (\mathrm{V}_{T,c} \cup \mathrm{V}_{T',c}).$$

Pour toute GA-substitution θ, on définit les ensembles $\mathrm{V}_{T,c}\theta$ et $\mathcal{V}(S)\theta$ par :

$$\begin{aligned} \mathrm{V}_{T,c}\theta &= \{\langle T'\theta, c\rangle \mid \langle T', c\rangle \in \mathrm{V}_{T,c}\}, \\ \mathcal{V}(S)\theta &= \bigcup_{\langle f,c,G\rangle \in \Sigma_E,\ T =^?_E T' \in S} (\mathrm{V}_{T,c}\theta \cup \mathrm{V}_{T',c}\theta). \end{aligned}$$ ◇

Exemple 11.1.36 Soit T un GA-terme tel que $\tau(T) = f(x, x)$, et soit c un contexte tel que $\tau(c) = f(g(\circ, \circ), \circ)$. Il n'existe donc aucun homomorphisme de c vers T. Soit θ une GA-substitution telle que $\tau(\theta) = \{x \leftarrow g(a, a)\}$, alors $\tau(T\theta) = f(g(a, a), g(a, a))$ et $c \sqsubseteq T\theta$, donc $T \nprec c$.

Propriété 11.1.37 *Soient $T = (V, s, a)$ un GA-terme, $\langle f, c, G\rangle$ un symbole de Σ_E, et θ une GA-substitution. Pour tout $v \in V$, on pose $T_v = T|v$, alors on a :*

1. $\mathrm{V}_{T_v,c} \subseteq \mathrm{V}_{T,c}$,
2. *si* $\langle T_v\theta, c\rangle \in \mathrm{V}_{T\theta,c}$, *alors* $\langle T_v, c\rangle \in \mathrm{V}_{T,c}$.

PREUVE. Le premier point est une conséquence immédiate de la définition de $\mathrm{V}_{T,c}$. Supposons maintenant que $\langle T_v\theta, c\rangle \in \mathrm{V}_{T\theta,c}$, alors il existe une GA-substitution θ' et un homomorphisme h de c vers $(T_v\theta)\theta'$, et donc, $\theta\theta'$ est une GA-substitution telle que h est un homomorphisme de c vers $T_v(\theta\theta')$. De plus, d'après la Propriété 11.1.5, s'il n'existe aucun homomorphisme de c vers $T_v\theta$, alors il n'existe aucun homomorphisme de c vers T_v, donc, $\langle T_v, c\rangle$ est bien élément de $\mathrm{V}_{T,c}$. ■

11.2 E-unification sur des GA-termes

Règles de transformation

Nous allons maintenant définir les règles de transformation qui permettent de résoudre les problèmes de E-unification sur des GA-termes. Ces règles sont proches de celles utilisées dans [BN98] pour faire de l'unification modulo la théorie de la commutativité, à l'exception de la règle de P-décomposition. Afin de présenter cette dernière règle de manière simple, nous commençons par définir une fonction qui associe un problème d'unification étendu à un problème d'unification.

Définition 11.2.1 (D(T, T', F, S)) Soient $F = \langle f, c, G\rangle$ un élément de Σ_E, S un problème de E-unification sur des GA-termes, et T et T' deux GA-termes dont les racines ne sont pas étiquetées par des éléments de $\mathcal{X}$. Alors on définit l'ensemble $\mathrm{D}(T, T', F, S)$ de la façon suivante.

- Si la GA-substitution $\gamma_c(T, T')$ n'existe pas, alors $\mathrm{D}(T, T', F, S) = \emptyset$.
- Sinon, soit $\theta = \gamma_c(T, T')$. On note respectivement h et h' les homomorphismes de c vers $T\theta$ et de c vers $T'\theta$, puis, pour tout $\sigma \in \mathrm{Sym}(\mathcal{SV}(c))$, on définit le problème de E-unification S_σ par :

$$S_\sigma = \{T\theta|h(v^\sigma) =^?_E T'\theta|h'(v) \mid v \in \mathcal{SV}(c)\} \cup \{A_x =^?_E A_x\theta \mid x \in \mathrm{Dom}(\theta)\} \cup S\theta,$$

et on pose $\mathrm{D}(T, T', F, S) = \{S_\sigma \mid \sigma \in G\}$. ◇

Exemple 11.2.2 Supposons que Σ_E est une signature stratifiée unif-stable contenant l'élément $\langle f, c, G\rangle$, où $\tau(c) = f(k(\circ), \circ)$, et $G = \mathrm{Sym}(\{1.1, 2\})$. On considère deux GA-termes T et T', tels que $\tau(T) = f(x, d)$ et $\tau(T') = f(k(a), d)$, ainsi qu'un problème de E-unification sur des GA-termes S, tel que $\tau(S) = \{g(x, a) =^?_E g(y, a)\}$.

Alors la GA-substitution $\gamma_c(T, T')$ existe, et on a $\tau(\gamma_c(T, T')) = \{x \leftarrow k(x_1)\}$, donc, en posant $\sigma = \mathrm{id}$ et $\mu = (1.1\ 2)$, on a

$$\begin{aligned}
\tau(S_\sigma) &= \{x_1 =^?_E a, d =^?_E d\} \cup \{x =^?_E k(x_1)\} \cup \{g(k(x_1), a) =^?_E g(y, a)\},\\
\tau(S_\mu) &= \{d =^?_E a, x_1 =^?_E d\} \cup \{x =^?_E k(x_1)\} \cup \{g(k(x_1), a) =^?_E g(y, a)\}.
\end{aligned}$$

Exemple 11.2.3 Soit E la théorie permutative définie par les axiomes suivants :

$$\begin{aligned}
f(x_1, x_2) &\rightleftharpoons f(x_1, x_2)\\
g(x_1, x_2) &\rightleftharpoons g(x_1, x_2)\\
f(g(x_1, x_2), x_3) &\rightleftharpoons f(g(x_1, x_3), x_2).
\end{aligned}$$

Soient c, c' et c'' les contextes tels que $\tau(c) = f(\circ, \circ)$, $\tau(c') = g(\circ, \circ)$, et $\tau(c'') = f(g(\circ, \circ), \circ)$, et soit $G'' = \mathrm{Sym}(\{1.2, 2\})$. Posons $F_1 = \langle f, c, \mathrm{I}\rangle$, $G = \langle g, c', \mathrm{I}\rangle$ et $F_2 = \langle f, c'', \mathrm{I}\rangle$, alors la signature stratifiée $\Sigma_E = \{F_1, G, F_2\}$ est unif-stable et saturée. Soient T, T' des GA-termes tels que $\tau(T) = f(x, a)$ et $\tau(T') = f(y, b)$, on a alors $\gamma_c(T, T') = \emptyset$, et $\gamma_{c''}(T, T')$ vérifie

$$\tau(\gamma_{c''}(T, T')) = \{x \leftarrow g(y_1, y_2), y \leftarrow g(z_1, z_2)\}.$$

Soient les problèmes de E-unifications S_1, S_2, S_3 tels que :

$$\begin{aligned}
\tau(S_1) &= \{x =^?_E y,\ a =^?_E b\},\\
\tau(S_2) &= \{y_1 =^?_E z_1,\ y_2 =^?_E z_2,\ a =^?_E b,\ x =^?_E g(y_1, y_2),\ y =^?_E g(z_1, z_2)\},\\
\tau(S_3) &= \{y_1 =^?_E z_1,\ a =^?_E z_2,\ y_2 =^?_E b,\ x =^?_E g(y_1, y_2),\ y =^?_E g(z_1, z_2)\}.
\end{aligned}$$

On a alors

$$\mathrm{D}(T, T', F_1, \emptyset) = \{S_1\},\ \mathrm{D}(T, T', G, \emptyset) = \emptyset,\ \text{et } \mathrm{D}(T, T', F_2, \emptyset) = \{S_2, S_3\}.$$

Définition 11.2.4 (Règles de transformation) Soient des GA-termes T et T' de racines respectives r et r', S un problème de E-unification sur des GA-termes, et M un problème de E-unification étendu.

Pour la règle de P-décomposition, on pose $S'' = S[r \rightsquigarrow r']$ s'il existe $\langle f, c, G\rangle \in \Sigma_E$ tel que $T \leftthreetimes c$, et $S'' = S[r' \rightsquigarrow r]$ sinon. On considère les règles de transformation suivantes :

1. **trivialité :**
   $\{\{T =^?_E T'\} \cup S\} \cup M \rightarrow \{S\} \cup M$ si $T \stackrel{\circ}{=} T'$,
2. **orientation :**
   $\{\{T =^?_E T'\} \cup S\} \cup M \rightarrow \{\{T' =^?_E T\} \cup S\} \cup M$ si r' est étiqueté par un élément de $\mathcal{X}$, et r non,
3. **contradiction :**
   $\{\{T =^?_E T'\} \cup S\} \cup M \rightarrow M$ si r et r' ne sont pas étiquetés par le même symbole de $\Sigma \setminus \mathcal{X}$,
4. **test d'occurrence :**
   $\{\{T =^?_E T'\} \cup S\} \cup M \rightarrow M$ si r est étiqueté par un sommet $x \in \mathcal{X}$, et qu'il existe un sommet $v' \neq r'$ de T' étiqueté par x,
5. **remplacement :**
   $\{\{T =^?_E T'\} \cup S\} \cup M \rightarrow \{\{T =^?_E T'\} \cup S\theta\} \cup M$ si r est étiqueté par un élément $x \in (\mathcal{X} \cap \mathrm{Var}(S)) \setminus \mathrm{Var}(T')$, et $\theta = \{x \leftarrow T'\}$,
6. **P-décomposition :**
   $\{\{T =^?_E T'\} \cup S\} \cup M \rightarrow [\bigcup_{F \in \Sigma_E} \mathrm{D}(T, T', F, S'')] \cup M$ si r et r' sont étiquetés par le même symbole de fonction de Σ. ◇

Exemple 11.2.5 Reprenons l'Exemple 11.2.3, et supposons qu'on cherche à résoudre le problème de E-unification $S = \{T =^?_E T'\}$. Alors, après application de la règle de P-décomposition, on a $\{S\} \rightarrow \{S_1, S_2, S_3\}$. On peut appliquer la règle de contradiction sur S_1 et S_2, et on obtient $\{S\} \rightarrow^* \{S_3\}$, puis, en appliquant les règles d'orientation et de remplacement sur S_3, on a $\{S\} \rightarrow^* \{S_4\}$, où

$$\tau(S_4) \;=\; \{y_1 =^?_E z_1, z_2 =^?_E a, y_2 =^?_E b, x =^?_E g(z_1, b), y =^?_E g(z_1, a)\}.$$

Dans ce qui suit, nous allons montrer que pour tout problème de E-unification sur des GA-termes S, les règles de la Définition 11.2.4 terminent, et que si $\{S\} \rightarrow^* M$, où M est sous forme résolue, alors tout ensemble de GA-substitutions induit par M est un CSU pour S.

Complétude

Nous commençons par démontrer que pour tout problème de E-unification S, si $\{S\} \rightarrow^* M$ où M est sous forme résolue, alors $\mathrm{Re}(M)$ est un CSU pour S.

Lemme 11.2.6 *Soient T et T' deux* GA*-termes, et c un contexte tel que $\theta = \gamma_c(T, T')$ existe. Alors pour toute* GA*-substitution ϕ telle que $c \sqsubseteq T\phi$ et $c \sqsubseteq T'\phi$, on a $\theta\phi \stackrel{\circ}{=} \phi$.*

PREUVE. Si $c \sqsubseteq T\phi$ et $c \sqsubseteq T'\phi$, alors d'après le Lemme 11.1.29, on a $\theta \lesssim \phi$, ce qui prouve qu'il existe une GA-substitution δ telle que $\phi \stackrel{\circ}{=} \theta\delta$. Comme θ est idempotente, on a :

$$\theta\phi \stackrel{\circ}{=} \theta(\theta\delta) = (\theta\theta)\delta = \theta\delta \stackrel{\circ}{=} \phi.$$

■

Corollaire 11.2.7 *Sous les hypothèses du Lemme 11.2.6, si S est un problème de E-unification, alors ϕ est une solution de S si et seulement si ϕ est également solution de $S\theta$.*

PREUVE. D'après le Lemme 11.2.6, pour tout GA-termes T et T', on a $\tau(T\phi) = \tau(T\theta\phi)$ et $\tau(T'\phi) = \tau(T'\theta\phi)$, d'où

$$(\tau(T\theta\phi) =_E \tau(T'\theta\phi)) \Leftrightarrow (\tau(T\phi) =_E \tau(T'\phi)).$$

■

Nous allons prouver que si $S' = \{T =^?_E T'\} \cup S$ est un problème de E-unification, et F est un symbole de Σ_E, alors on a $\mathcal{U}_E(\mathrm{D}(T, T', S, F)) \subseteq \mathcal{U}_E(S')$. Nous commençons par démontrer un premier lemme, qui fournit une condition suffisante pour que deux A-termes soient congrus.

Lemme 11.2.8 *Soient T et T' deux GA-termes, $F = \langle f, c, G\rangle$ un élément de Σ_E, S un problème de E-unification, et supposons qu'il existe une GA-substitution $\phi \in \mathcal{U}_E(\mathrm{D}(T, T', F, S))$. Soient deux A-termes stratifiés A_1 et A'_1 dont les racines r et r' sont étiquetées par F. Posons $h_1 = \mathrm{h}_{[A_1,r]}$ et $h'_1 = \mathrm{h}_{[A'_1,r']}$, et supposons que A_1 et A'_1 vérifient :*

1. $\mathrm{dm}(A_1) \stackrel{\circ}{=} T\phi$ *et* $\mathrm{dm}(A'_1) \stackrel{\circ}{=} T'\phi$,
2. *pour tout* $v \in \mathcal{SV}(c)$,

$$A_1|h_1(v) = \mathrm{Strat}(\mathrm{dm}(A_1|h_1(v))), \text{ et } A'_1|h'_1(v) = \mathrm{Strat}(\mathrm{dm}(A'_1|h'_1(v))).$$

Alors on a $A_1 \bowtie A'_1$.

PREUVE. Notons respectivement h et h' les homomorphismes de c vers $T\phi$ et de c vers $T'\phi$, et supposons que ϕ est solution de S_σ, où $\sigma \in G$. Alors, par hypothèse, pour tout sommet variable v de c, on a $\tau(T\phi|h(v^\sigma)) =_E \tau(T'\phi|h'(v))$.

Comme $\tau(T\phi|h(v)) = \tau(\mathrm{dm}(A_1|h_1(v)))$, et $\tau(T'\phi|h'(v)) = \tau(\mathrm{dm}(A'_1|h'_1(v)))$, on en déduit que $\tau(\mathrm{dm}(A|h_1(v^\sigma))) =_E \tau(\mathrm{dm}(A'|h'_1(v)))$. D'après le Théorème 10.3.15, on en déduit que $\mathrm{Strat}(\mathrm{dm}(A|h_1(v^\sigma))) \bowtie \mathrm{Strat}(\mathrm{dm}(A'_1|h'_1(v)))$, d'où $A_1|h_1(v^\sigma) \bowtie A'_1|h'_1(v)$.

Posons $\sigma' = \sigma^{h_1}$, alors, pour tout $u \in \mathrm{R}_{A_1}(r)$, $A_1|u^{\sigma'} \bowtie A'_1|\mathrm{h}^A_{[r\to r']}(u)$, et d'après le Théorème 7.2.2, on en déduit que $A_1 \bowtie A'_1$. ■

Corollaire 11.2.9 *Soient T, T' deux GA-termes, $F = \langle f, c, G\rangle$ un élément de Σ_E, et $S' = \{T =^?_E T'\} \cup S$ un problème de E-unification. Alors on a*

$$\mathcal{U}_E(\mathrm{D}(T, T', F, S)) \subseteq \mathcal{U}_E(S').$$

PREUVE. Soit $\phi \in \mathcal{U}_E(\mathrm{D}(T, T', F, S))$, il existe donc une permutation $\sigma \in G$ telle que ϕ est solution de S_σ. On considère deux A-termes stratifiés A_1 et A'_1 vérifiant les hypothèses du Lemme 11.2.8, on a donc $A_1 \bowtie A'_1$, d'où $\tau(\mathrm{dm}(A_1)) =_E \tau(\mathrm{dm}(A'_1))$. Comme $\tau(T\phi) = \tau(\mathrm{dm}(A_1))$ et $\tau(T'\phi) = \tau(\mathrm{dm}(A'_1))$, on en déduit que $\tau(T\phi) =_E \tau(T'\phi)$, et ϕ est solution de $\{T =^?_E T'\}$.

Posons $\theta = \gamma_c(T, T')$, comme $c \sqsubseteq T\phi$ et $c \sqsubseteq T'\phi$, alors d'après le Corollaire 11.2.7, ϕ étant solution de $S\theta$, c'est également une solution de S, d'où $\phi \in \mathcal{U}_E(S')$. ∎

Montrons maintenant l'inclusion réciproque.

Lemme 11.2.10 *Soit $S' = \{T =^?_E T'\} \cup S$ un problème de E-unification, alors on a*

$$\mathcal{U}_E(S') \subseteq \mathcal{U}_E(\bigcup_{F \in \Sigma_E} \mathrm{D}(T, T', F, S)).$$

PREUVE. Soit ϕ une solution de S', alors $\tau(T\phi) =_E \tau(T'\phi)$. Posons $A = \mathrm{As}(\tau(T\phi))$ et $A' = \mathrm{As}(\tau(T'\phi))$, alors d'après le Corollaire 10.3.14, on a $A \bowtie A'$. Notons respectivement r et r' les racines de A et A', et soit $F = \langle f, c, G\rangle$ le symbole de Σ_E qui étiquette ces sommets[1]. Posons $h = \mathrm{h}_{[A,r]}$ et $h' = \mathrm{h}_{[A',r']}$, alors d'après le Théorème 7.2.2, il existe une permutation $\sigma \in G$ telle que pour tout $v \in \mathcal{SV}(c)$, $A|h(v^\sigma) \bowtie A'|h'(v)$, d'où, pour tout $v \in \mathcal{SV}(c)$, $\tau(\mathrm{dm}(A)|h(v^\sigma)) =_E \tau(\mathrm{dm}(A')|h'(v))$.

Par construction, A et $\tau(T\phi)$ sont bisimilaires, et comme $\mathrm{h}_{[A,r]}$ est un homomorphisme de c vers A, d'après le Lemme 5.2.15, il existe un homomorphisme de c ver $T\phi$. De même, on peut prouver qu'il existe un homomorphisme de c vers $T'\phi$, et donc, l'existence de $\gamma_c(T, T')$ est garantie. L'ensemble $\mathrm{D}(T, T', F, S)$ est donc non vide, et nous allons montrer que ϕ est solution de S_σ.

Posons $\theta = \gamma_c(T, T')$, d'après le Lemme 11.2.6, on a $T\phi \doteq T\theta\phi$ et $T'\phi \doteq T'\theta\phi$. Donc, si h_1 (resp. h'_1) est l'homomorphisme de c vers $T\theta\phi$ (resp. $T'\theta\phi$), alors pour tout $v \in \mathcal{SV}(c)$,

$$\tau(\mathrm{dm}(A)|h(v)) = \tau((T\theta\phi)|h_1(v)), \text{ et } \tau(\mathrm{dm}(A')|h'(v)) = \tau((T'\theta\phi)|h'_1(v)),$$

d'où, pour tout $v \in \mathcal{SV}(c)$, $\tau((T\theta\phi)|h_1(v^\sigma)) =_E \tau((T'\theta\phi)|h'_1(v))$.

Notons h_2 (resp. h'_2) l'homomorphisme de c vers $T\theta$ (resp. $T'\theta$). L'existence de h_2 et h'_2 est garantie par la Propriété 11.1.27, et on a

$$(T\theta\phi)|h_1(v) = (T\theta|h_2(v))\phi \text{ et } (T'\theta\phi)|h'_1(v) = (T'\theta|h'_2(v))\phi.$$

On en déduit que $\tau((T\theta|h_2(v^\sigma))\phi) =_E \tau((T'\theta|h'_2(v))\phi)$. Donc, ϕ est solution de

$$\{T\theta|h_2(v^\sigma) =^?_E T'\theta|h'_2(v) \mid v \in \mathcal{SV}(c)\}.$$

D'après le Lemme 11.2.6, pour tout $x \in \mathrm{Dom}(\theta)$, $A_x\phi \doteq A_x\theta\phi$, et donc, ϕ est solution de $\{A_x =^?_E A_x\theta \,|x \in \mathrm{Dom}(\theta)\}$. Enfin, d'après le Corollaire 11.2.7, ϕ est également solution de $S\theta$, et donc, ϕ est bien solution de S_σ. ∎

[1] cet élément existe, puisqu'on a supposé que pour tout symbole $f \in \Sigma$, E contient l'équation triviale $f(x_1, \ldots, x_n) \rightleftharpoons f(x_1, \ldots, x_n)$ comme axiome.

Théorème 11.2.11 *Soient T, T' deux* GA*-termes, et $S' = \{T =^?_E T'\} \cup S$ un problème de E-unification. Alors*

$$\mathcal{U}_E(S') \;=\; \mathcal{U}_E(\bigcup_{F\in\Sigma_E} \mathrm{D}(T,T',F,S)).$$

PREUVE. D'après le Corollaire 11.2.9, pour tout $F \in \Sigma_E$, on a $\mathcal{U}_E(\mathrm{D}(A,A',F,S)) \subseteq \mathcal{U}_E(S')$, ce qui prouve que

$$\bigcup_{F\in\Sigma_E} \mathcal{U}_E(\mathrm{D}(T,T',F,S)) \;=\; \mathcal{U}_E(\bigcup_{F\in\Sigma_E} \mathrm{D}(T,T',F,S)) \;\subseteq\; \mathcal{U}_E(S').$$

Le Lemme 11.2.10 prouve l'inclusion réciproque. ∎

Lemme 11.2.12 *Etant donnés deux* GA*-termes T et T' de racines respectives r et r', et un problème de E-unification sur des* GA*-termes S, on a*

$$\mathcal{U}_E(\bigcup_{F\in\Sigma_E} \mathrm{D}(T,T',F,S)) \;=\; \mathcal{U}_E(\bigcup_{F\in\Sigma_E} \mathrm{D}(T,T',F,S[r \rightsquigarrow r'])).$$

PREUVE. D'après le Théorème 11.2.11, on a

$$\mathcal{U}_E(\bigcup_{F\in\Sigma_E} \mathrm{D}(T,T',F,S)) \;=\; \mathcal{U}_E(\{T =^?_E T'\} \cup S),$$
$$\mathcal{U}_E(\bigcup_{F\in\Sigma_E} \mathrm{D}(T,T',F,S[r \rightsquigarrow r'])) \;=\; \mathcal{U}_E(\{T =^?_E T'\} \cup S[r \rightsquigarrow r']).$$

D'après le Lemme 11.1.34, $\mathcal{U}_E(\{T =^?_E T'\} \cup S) = \mathcal{U}_E(\{T =^?_E T'\} \cup S[r \rightsquigarrow r'])$, d'où l'égalité. ∎

Théorème 11.2.13 *Soient M et M' deux problèmes de E-unification étendus, tels que $M \to M'$. Alors $\mathcal{U}_E(M) = \mathcal{U}_E(M')$.*

PREUVE. Le résultat est immédiat pour les quatre première règles. Supposons maintenant que M' est obtenu à partir de M après avoir appliqué la règle de remplacement, on a donc $M = \{\{T =^?_E T'\} \cup S\} \cup M''$ et $M' = \{\{T =^?_E T'\} \cup S\theta\} \cup M''$, où $\theta = \{x \leftarrow T'\}$, et x étiquette la racine de T. Notons $S = \{T_i =^?_E T'_i \mid i = 1,\ldots,n\}$, et soit ϕ une GA-substitution. On pose $\tau(T') = s$, $\gamma = \tau(\phi)$, et pour $i = 1,\ldots,n$, $t_i = \tau(T_i)$ et $t'_i = \tau(T'_i)$. D'après le Corollaire 2.3.6, pour tout $i = 1,\ldots,n$, on a

$$(x\gamma =_E s\gamma \text{ et } t_i\gamma =_E t'_i\gamma) \;\Leftrightarrow\; (x\gamma =_E s\gamma \text{ et } t_i\{x \leftarrow s\}\gamma =_E t'_i\{x \leftarrow s\}\gamma),$$

donc, ϕ est solution de $\{T =^?_E T'\} \cup S$ si et seulement si ϕ est solution de $\{T =^?_E T'\} \cup S\theta$, d'où le résultat.

Enfin, le Théorème 11.2.11 et le Lemme 11.2.12 prouvent le résultat pour la règle de P-décomposition. ∎

Corollaire 11.2.14 *Pour tout problème de E-unification S, et pour tout problème de E-unification étendu M sous forme résolue tel que $\{S\} \to^* M$, l'ensemble* $\mathrm{Re}(M)$ *est un CSU pour S.*

11.3 Terminaison et complexité

Nous allons définir une mesure de complexité associée à un problème d'unification étendu, et démontrer que chaque application d'une règle de la Définition 11.2.4 fait strictement décroître cette mesure de complexité. Comme la règle de P-décomposition peut introduire de nouveaux sommets et de nouvelles variables dans les problèmes d'unification considérés, il n'est pas aisé de définir une mesure de complexité standard dont la valeur décroît après l'application de cette règle. Nous allons nous servir de l'hypothèse d'unif-stabilité pour définir une telle mesure, et nous montrerons que le nombre de GA-termes sur lesquels l'application de la règle de P-décomposition introduit de nouveaux sommets décroît strictement. Cette mesure de complexité nous permettra également de borner la cardinalité maximale des CSU déterminés par les règles de transformation.

Nous commençons par démontrer certaines propriétés d'inclusion vérifiées par les ensembles $\mathrm{V}_{T,c}$.

Lemme 11.3.1 *Soient T et T_1 deux* GA*-termes vérifiant les hypothèses de la Définition 11.1.30, notons r_1 la racine de T_1, et soit v un sommet de T. Posons $T' = T[v \rightsquigarrow r_1]$, alors pour tout contexte c, on a $\mathrm{V}_{T',c} \subseteq \mathrm{V}_{T,c} \cup \mathrm{V}_{T_1,c}$.*

PREUVE. Si v n'est pas un sommet de T, alors on a $T' = T$, et le résultat est évident. Sinon, soit w un sommet de T' tel que $\langle T'|w, c\rangle \in \mathrm{V}_{T',c}$. Si w est un sommet de T, alors par construction, $T'|w = T|w$, et donc $T|w \not< c$, et $\langle T'|w, c\rangle \in \mathrm{V}_{T,c}$. Sinon, w est un sommet de T_1, d'où $T'|w = T_1|w$, et on a $T_1|w \not< c$, d'où $\langle T'|w, c\rangle \in \mathrm{V}_{T_1,c}$. ∎

Lemme 11.3.2 *Soient $T = (V, s, a)$ et $T' = (V', s', a')$ des* GA*-termes, $\langle f, c, G\rangle$ un symbole de Σ_E, et $\theta = \{x \leftarrow T'\}$. Alors, on a*

$$\mathrm{V}_{T\theta,c} \quad \subseteq \quad \mathrm{V}_{T,c}\theta \cup \mathrm{V}_{T',c}.$$

PREUVE. Soit $\langle T_1, c\rangle \in \mathrm{V}_{T\theta,c}$, et notons r_1 la racine de T_1. Si $r_1 \in V'$, alors par définition du GA-terme $T\theta$, on a $T_1 = T'|r_1$ et par définition, on a $\langle T_1, c\rangle \in \mathrm{V}_{T',c}$. Sinon, nécessairement, $r_1 \in V$, et on a $T_1 = (T\theta)|r_1$. On a donc $s(r_1) \notin \mathcal{X}$, et $T_1 = (T|r_1)\theta$ d'après la Propriété 11.1.6. D'après la Propriété 11.1.37 2, on en déduit que $\langle T|r_1, c\rangle \in \mathrm{V}_{T,c}$, et $\langle T_1, c\rangle$ est bien élément de $\mathrm{V}_{T,c}\theta$. ∎

Nous prouvons maintenant que pour certains problèmes de E-unification S, l'ensemble $\mathcal{V}(S)$ est nécessairement vide.

Lemme 11.3.3 *Soient T et T' deux* GA*-termes et c un contexte tels que la* GA*-substitution $\theta = \gamma_c(T, T')$ existe. Pour $x \in \mathrm{Dom}(\theta)$, soit $S = \{A_x =^?_E A_x\theta\}$, alors $\mathcal{V}(S) = \emptyset$.*

PREUVE. On pose $T'' = (V'', s'', a'') = A_x\theta$, alors on a

$$\mathcal{V}(S) \quad = \quad \bigcup_{\langle f', c', G'\rangle \in \Sigma_E} (\mathrm{V}_{A_x,c'} \cup \mathrm{V}_{T'',c'}),$$

et par définition, pour tout $\langle f', c', G' \rangle \in \Sigma_E$, on a $\mathrm{V}_{A_x,c'} = \emptyset$. Nous allons maintenant prouver qu'on a également $\mathrm{V}_{T'',c'} = \emptyset$. Supposons qu'il existe un élément $\langle T_1, c' \rangle \in \mathrm{V}_{T'',c'}$, alors il existe un sommet non-variable $v_1 \in V''$ tel que $T_1 = T''|v_1$, et on a $s''(v_1) \notin \mathcal{X}$ et $T_1 \not\asymp c'$. Soit ϕ une GA-substitution telle qu'il existe un homomorphisme de c' vers $T_1\phi$.

Comme $T'' = A_x\theta$, et v_1 est un sommet non-variable de T'', d'après le Lemme 11.1.28, il existe un sommet non-variable v de c, différent de la racine de c, tel que $c|v \sqsubseteq T_1$. D'après la Propriété 11.1.5, il existe donc un homomorphisme de $c|v$ vers $T_1\phi$, ce qui prouve que $c|v$ et c' sont unifiables. Par hypothèse d'unif-stabilité, on en déduit que $c' \sqsubseteq c|v$, et donc, $c' \sqsubseteq T_1$, ce qui contredit l'hypothèse $T_1 \not\asymp c'$. ∎

Ce lemme permet de démontrer une autre propriété d'inclusion vérifiée par les ensembles $\mathrm{V}_{T,c}$:

Lemme 11.3.4 *Soient T, T' deux* GA*-termes, $\langle f, c, G \rangle$ un élément de Σ_E, et supposons que $\theta = \gamma_c(T, T')$ existe. Alors pour tout* GA*-terme T_1 et pour tout symbole $\langle f', c', G' \rangle \in \Sigma_E$, on a $\mathrm{V}_{T_1\theta,c'} \subseteq (\mathrm{V}_{T_1,c'})\theta$.*

PREUVE. On démontre que pour tout sous-ensemble ϕ de θ et pour tout GA-terme T_1, on a $\mathrm{V}_{T_1\phi,c'} \subseteq \mathrm{V}_{T_1,c'}\phi$ par induction sur la cardinalité de ϕ. Si $|\phi| = 1$, alors ϕ est de la forme $\{x \leftarrow A_x\theta\}$, et d'après le Lemme 11.3.2, on a $\mathrm{V}_{T_1\phi,c'} \subseteq \mathrm{V}_{T_1,c'}\phi \cup \mathrm{V}_{A_x\theta,c'}$. D'après le Lemme 11.3.3, on a $\mathrm{V}_{A_x\theta,c'} = \emptyset$, et donc $\mathrm{V}_{T_1\phi,c'} \subseteq \mathrm{V}_{T_1,c'}\phi$.

Supposons maintenant que $\phi = \phi' \uplus \{x \leftarrow T''\} = \phi'\{x \leftarrow T''\}$ (car θ étant idempotente, la variable x n'apparaît pas dans ϕ'), et que le résultat est vrai pour ϕ', alors on a

$$\mathrm{V}_{T_1\phi,c'} \;\subseteq\; (\mathrm{V}_{T_1\phi',c'})\{x \leftarrow T''\} \;\subseteq\; (\mathrm{V}_{T_1,c'})\phi'\{x \leftarrow T''\} \;=\; (\mathrm{V}_{T_1,c'})\phi. \qquad ∎$$

Corollaire 11.3.5 *Sous les hypothèses du Lemme 11.3.4, et si S est un problème de E-unification étendu, alors on a $\mathcal{V}(S\theta) \subseteq \mathcal{V}(S)\theta$.*

PREUVE. Posons $S = \{T_1 =^?_E T'_1, \ldots, T_n =^?_E T'_n\}$, et soit $i \in \{1, \ldots, n\}$. Alors, d'après le Lemme 11.3.4, pour tout $\langle f', c', G' \rangle \in \Sigma_E$, on a $\mathrm{V}_{T_i\theta,c'} \cup \mathrm{V}_{T'_i\theta,c'} \subseteq (\mathrm{V}_{T_i,c'} \cup \mathrm{V}_{T'_i,c'})\theta$, d'où le résultat. ∎

Nous pouvons enfin démontrer qu'étant donné un problème de E-unification S, l'application de la règle de P-décomposition sur S produit un problème de E-unification étendu dont chaque élément S' vérifie $|\mathcal{V}(S')| \leq |\mathcal{V}(S)|$.

Théorème 11.3.6 *Soient T et T' deux* GA*-termes dont les racines r et r' sont étiquetées par le même symbole de fonction de Σ, et $S' = \{T =^?_E T'\} \cup S$ un problème de E-unification.*

On pose $K = \{\langle f, c, G \rangle \in \Sigma_E \mid T \not\asymp c\}$ et $K' = \{\langle f, c, G \rangle \in \Sigma_E \mid T' \not\asymp c\}$. Si $K \neq \emptyset$, alors on pose $k = |K|$ et $S'' = S[r \rightsquigarrow r']$, sinon, on pose $k = |K'|$ et $S'' = S[r' \rightsquigarrow r]$.

Soit $F \in \Sigma_E$, alors, pour tout $S_\sigma \in \mathrm{D}(T, T', F, S'')$, on a $|\mathcal{V}(S_\sigma)| \leq |\mathcal{V}(S')| - k$.

PREUVE. On pose $F = \langle f, c, G\rangle$, on note $\theta = \gamma_c(T, T')$, et soient h et h' les homomorphismes respectivement de c vers T et de c vers T'. D'après le Lemme 11.3.3, on a $\mathcal{V}(\{A_x =^?_E A_x\theta \mid x \in \mathrm{Dom}(\theta)\}) = \emptyset$.

D'après le Lemme 11.3.1, on a $\mathcal{V}(S'') \subseteq \mathcal{V}(S)$, et d'après le Corollaire 11.3.5, on en déduit que $\mathcal{V}(S''\theta) \subseteq \mathcal{V}(S'')\theta \subseteq \mathcal{V}(S)\theta$.

D'après la Propriété 11.1.37 1 et le Lemme 11.3.4, pour tout symbole $\langle f', c', G'\rangle \in \Sigma$, et tout sommet $v \in \mathcal{SV}(c)$, on a $\mathrm{V}_{T\theta|h(v),c'} \subseteq \mathrm{V}_{T\theta,c'} \subseteq (\mathrm{V}_{T,c'})\theta$, et de même, $\mathrm{V}_{T'\theta|h'(v),c'} \subseteq (\mathrm{V}_{T',c'})\theta$. On en déduit donc que

$$\bigcup_{v\in\mathcal{SV}(c)} \mathrm{V}_{T\theta|h(v^\sigma),c'} \cup \mathrm{V}_{T'\theta|h'(v),c'} \;\subseteq\; (\mathrm{V}_{T,c'} \cup \mathrm{V}_{T',c'})\theta.$$

Ceci étant valable pour tout symbole $\langle f', c', G'\rangle$ dans Σ_E, on a donc

$$\bigcup_{v\in\mathcal{SV}(c)} \mathcal{V}(\{T\theta|h(v^\sigma) =^?_E T'\theta|h'(v)\}) \;\subseteq\; \mathcal{V}(\{T =^?_E T'\})\theta.$$

On en déduit enfin que $\mathcal{V}(S_\sigma) \subseteq \mathcal{V}(\{T =^?_E T'\})\theta \cup \mathcal{V}(S)\theta = \mathcal{V}(S')\theta$.

Sans perte de généralité, supposons qu'il existe un symbole $\langle f', c', G'\rangle \in \Sigma_E$ tel que $T \nprec c'$, alors $\langle T, c'\rangle \in S'$. Comme $r \notin \mathrm{Som}(S_\sigma)$, $\langle T\theta, c'\rangle$ ne peut pas être élément de $\mathcal{V}(S_\sigma)$, d'où $\mathcal{V}(S_\sigma) \subseteq [\mathcal{V}(S') \setminus \{\langle T, c'\rangle\}]\theta$. On en déduit donc que $|\mathcal{V}(S_\sigma)| \leq |\mathcal{V}(S')| - k$. ■

Nous démontrons enfin que la cardinalité d'un ensemble $\mathcal{V}(S)$ ne peut pas augmenter après l'application d'une autre règle de la Définition 11.2.4.

Lemme 11.3.7 *Si $\{S\} \cup M \to \{S'\} \cup M$ pour les règles de trivialité, d'orientation ou de remplacement, alors on a $|\mathcal{V}(S')| \leq |\mathcal{V}(S)|$.*

PREUVE. Le résultat est évident pour la règle de trivialité et la règle d'orientation. Pour la règle de remplacement, supposons que $S = \{T =^?_E T'\} \cup S''$, où la racine de T est étiquetée par un élément $x \in (\mathcal{X} \cap \mathrm{Var}(S'')) \setminus \mathrm{Var}(T')$, on a donc $S' = \{T =^?_E T'\} \cup S''\theta$, où $\theta = \{x \leftarrow T'\}$. Par définition, pour tout symbole $\langle f, c, G\rangle \in \Sigma_E$, on a $\mathrm{V}_{T,c} = \emptyset$, et d'après le Lemme 11.3.2, pour tout GA-terme T_1 et tout symbole $\langle f, c, G\rangle \in \Sigma_E$, on a $\mathrm{V}_{T_1\theta,c} \subseteq \mathrm{V}_{T_1,c}\theta \cup \mathrm{V}_{T',c}$, d'où :

$$\begin{aligned}
\mathcal{V}(S''\theta) &= \bigcup_{\langle f,c,G\rangle\in\Sigma_E, T_1=^?_E T_1'\in S''} (\mathrm{V}_{T_1\theta,c} \cup \mathrm{V}_{T_1'\theta,c}) \\
&\subseteq \bigcup_{\langle f,c,G\rangle\in\Sigma_E, T_1=^?_E T_1'\in S''} ((\mathrm{V}_{T_1,c})\theta \cup (\mathrm{V}_{T_1',c})\theta \cup \mathrm{V}_{T',c}) \\
&= \mathcal{V}(S'')\theta \cup \mathcal{V}(\{T =^?_E T'\}).
\end{aligned}$$

On en déduit que $\mathcal{V}(S') \subseteq \mathcal{V}(S'')\theta \cup \mathcal{V}(\{T =^?_E T'\})$. Comme il n'existe aucun sommet de T' qui est étiqueté par le symbole x, on a $\mathrm{V}_{T',c}\theta = \mathrm{V}_{T',c}$ pour tout $\langle f, c, G\rangle \in \Sigma_E$, d'où $\mathcal{V}(\{T =^?_E T'\})\theta = \mathcal{V}(\{T =^?_E T'\})$.

On en déduit que $\mathcal{V}(S') \subseteq (\mathcal{V}(S'') \cup \mathcal{V}(\{T =^?_E T'\}))\theta = \mathcal{V}(S)\theta$, et donc, $|\mathcal{V}(S')| \leq |\mathcal{V}(S)|$. ■

Nous adaptons maintenant d'autres mesures classiques servant à prouver la terminaison de problèmes d'unification sur des termes, au cas des problèmes de E-unification sur des GA-termes. Ces mesures nous permettront de démontrer que les règles de transformation de la Définition 11.2.4 termine, et, par la même occasion, de borner la cardinalité des CSU déterminés par ces règles de transformation. Nous commençons par définir des constantes associées aux signatures stratifiées considérées.

Définition 11.3.8 On définit les constantes suivantes :
- $s = \max\{|c| \mid \langle f, c, G\rangle \in \Sigma_E\}$,
- $g = \max\{|G| \mid \langle f, c, G\rangle \in \Sigma_E\}$,
- $k = |\Sigma_E|$. ◇

Définition 11.3.9 (Mesures) Soit S un problème de E-unification sur des GA-termes. On associe à S le quintuplet $\langle m_0, m_1, m_2, m_3, m_4\rangle$, où :
- $m_0 = |\mathcal{V}(S)|$,
- $m_1 = |\mathrm{Som}(S)|$,
- m_2 est le nombre d'éléments de $\mathrm{Var}(S)$ qui apparaissent plusieurs fois dans $\tau(S)$,
- $m_3 = |S|$,
- m_4 est le nombre d'éléments de la forme $T =^?_E T'$, où la racine de T' est étiquetée par un symbole de $\mathcal{X}$, et celle de T non.

On ordonne l'ensemble des mesures de problèmes de E-unification avec l'ordre lexicographique $\prec$ sur les quintuplets.

On définit alors la *mesure* d'un problème de E-unification étendu M comme le multiensemble $\dot{M}$ des mesures des éléments de M. On ordonne l'ensemble des mesures des problèmes de E-unification étendus avec l'ordre sur les multiensembles induit par l'ordre lexicographique sur les quintuplets, et on notera cet ordre $\lessdot$.

Si M et M' sont deux problèmes de E-unification étendus de mesures respectives $\dot{M}$ et $\dot{M}'$, on notera $M < M'$ si et seulement si $\dot{M} \lessdot \dot{M}'$. ◇

Lemme 11.3.10 *Soient S un problème de E-unification et M un problème de E-unification étendu. Soit S' un problème de E-unification tel que le problème de E-unification étendu $\{S'\} \cup M$ est obtenu à partir de $\{S\} \cup M$ par la règle de trivialité, d'orientation ou de remplacement. On note respectivement les mesures associées à S et S'*

$$\langle m_0, m_1, m_2, m_3, m_4\rangle \text{ et } \langle m'_0, m'_1, m'_2, m'_3, m'_4\rangle,$$

alors on a :

règle	m'_0	m'_1	m'_2	m'_3	m'_4
trivialité	$\leq m_0$	$\leq m_1$	$\leq m_2$	$< m_3$	_
orientation	$\leq m_0$	$\leq m_1$	$\leq m_2$	$\leq m_3$	$< m_4$
remplacement	$\leq m_0$	$\leq m_1$	$< m_2$	_	_

PREUVE. Règles de trivialité et d'orientation : d'après le Lemme 11.3.7, on a $m'_0 \leq m_0$, et il est clair que $m'_1 \leq m_1$ et $m'_2 \leq m_2$. Pour la règle de trivialité, on a $m'_3 < m_3$, et pour la règle d'orientation, $m'_3 \leq m_3$ et $m'_4 < m_4$.

Règle de remplacement : supposons que $S' = \{T =^?_E T'\} \cup S''\theta$, où θ est de la forme $\{x \leftarrow T'\}$. D'après le Lemme 11.3.7, on a $m'_0 \leq m_0$, et comme aucun nouveau sommet n'est introduit dans $S''\theta$, on a $m'_1 \leq m_1$. La variable x n'apparaît pas dans $\tau(S''\theta)$, et donc, $m'_2 < m_2$. ■

Lemme 11.3.11 *Soit $S' = \{T =^?_E T'\} \cup S$ un problème de E-unification, où les racines de T et T' sont étiquetées par un symbole de fonction de Σ, et notons $\langle m_0, m_1, m_2, m_3, m_4\rangle$ la mesure asociée à S'.*

On pose $K = \{\langle f, c, G\rangle \in \Sigma_E \mid T \nearrow c\}$ et $K' = \{\langle f, c, G\rangle \in \Sigma_E \mid T' \nearrow c\}$. Si $K \neq \emptyset$, alors on pose $k_1 = |K|$, sinon on pose $k_1 = |K'|$.

Après application de la règle de P-décomposition, pour tout $F = \langle f, c, G\rangle \in \Sigma_E$ et pour tout $S_\sigma \in \mathrm{D}(A, A', F, S)$ dont la mesure associée est $\langle m'_0, m'_1, m'_2, m'_3, m'_4\rangle$, on a :

	m'_0	m'_1	m'_2	m'_3	m'_4
$k_1 \neq 0$	$\leq m_0 - k_1$	_	_	_	_
$k_1 = 0$	$\leq m_0$	$\leq m_1 - 1$	_	_	_

PREUVE. Supposons que $k_1 \neq 0$, alors, d'après le Théorème 11.3.6, on a $m'_0 \leq m_0 - k_1$.

Si $k_1 = 0$, alors les ensembles K et K' sont vides, et comme θ existe, on a nécessairement $c \sqsubseteq T$ et $c \sqsubseteq T'$. Par définition de $\gamma_c(T, T')$, on a donc $\theta = \emptyset$. D'après le Théorème 11.3.6, on a $m'_0 \leq m_0$, et comme la racine de T' n'est pas élément de $\mathrm{Som}(S_\sigma)$, on a $m'_1 \leq m_1 - 1$. ■

On en déduit donc que :

Théorème 11.3.12 *L'ensemble de règles de la Définition 11.2.4 termine.*

PREUVE. Nous démontrons que si $M \rightarrow M'$, alors $M' < M$. Ce résultat est immédiat pour les règles de contradiction et d'occurence, puisqu'on a alors $M' \subseteq M$. Sinon, soit $\{S\} \cup M$ un problème de E-unification étendu, de mesure associée $\langle m_0, m_1, m_2, m_3, m_4\rangle$.

Considérons les règles de trivialité, d'orientation et de remplacement, on a $\{S\} \cup M \rightarrow \{S'\} \cup M$, notons $\langle m'_0, m'_1, m'_2, m'_3, m'_4\rangle$ la mesure de S'. Alors, d'après le Lemme 11.3.10, on a $\langle m_0, m_1, m_2, m_3, m_4\rangle \prec \langle m'_0, m'_1, m'_2, m'_3, m'_4\rangle$, d'où $\{S'\} \cup M < \{S\} \cup M$.

Supposons que la règle de P-décomposition a été appliquée au problème étendu $\{\{T =^?_E T'\} \cup S''\} \cup M$, où les racines de T et T' sont étiquetées par des symboles de fonction de Σ. Si $F = \langle f, c, G\rangle \in \Sigma_E$ est un élément tel que $\mathrm{D}(T, T', F, S) \neq \emptyset$, alors pour $\sigma \in G$, on note $\langle m'_0, m'_1, m'_2, m'_3, m'_4\rangle$ la mesure de S_σ. Alors, d'après le Lemme 11.3.11, on a $\langle m_0, m_1, m_2, m_3, m_4\rangle \prec \langle m'_0, m'_1, m'_2, m'_3, m'_4\rangle$.

Donc, quelle que soit la règle de transformation appliquée, si $M \rightarrow M'$, alors $M' < M$. ■

Ainsi, le Théorème 11.3.12 prouve que l'ensemble de règles de la Définition 11.2.4 termine, et le Théorème 11.2.13 prouve que pour tout problème de E-unification étendu M, l'ensemble des solutions de M est préservé par l'application de ces règles de transformation. Il est clair qu'un problème de E-unification étendu est sous forme normale pour ces règles de transformation si et seulement s'il est sous forme résolue, on a donc le résultat suivant :

Corollaire 11.3.13 *Pour tout problème de E-unification S, l'ensemble des règles de la Définition 11.2.4 permet de déterminer un CSU pour S.*

Cardinalité des CSU

Soit S un problème de E-unification de mesure $\langle m_0, m_1, m_2, m_3, m_4\rangle$, et supposons que $\{S\} \rightarrow^* M$. Nous allons majorer la cardinalité de M. La seule règle de transformation qui augmente cette cardinalité est la règle de P-décomposition, qui remplace un problème de E-unification par au plus gk problèmes (chaque élément $F \in \Sigma_E$ peut créer au plus g problèmes, et il y a k éléments dans Σ_E). La cardinalité de M dépend donc du nombre maximal de fois que la règle de P-décomposition a été appliquée dans toute dérivation de $\{S\}$ à M. D'après le Lemme 11.3.11, le nombre de fois que la règle de P-décomposition peut être appliquée dépend uniquement des valeurs de m_0 et m_1. D'après le Lemme 11.3.10, seule la règle de P-décomposition permet d'augmenter les valeurs de m_0 et m_1.

Définition 11.3.14 On note $\mathrm{T}(n, m)$ le nombre de problèmes d'unification créés par la règle de P-décomposition dans une dérivation partant d'un problème de E-unification dont la mesure vérifie $m_0 = n$ et $m_1 = m$. ◇

Théorème 11.3.15 *Pour tout $n, m \in \mathbb{N}$, on a $\mathrm{T}(n, m) \leq (gk)^{n(1+2s)+m}$.*

PREUVE. On démontre le résultat par induction sur les paires $\langle n, m\rangle$. Supposons que le résultat soit vrai pour toute paire $\langle n', m'\rangle \prec \langle n, m\rangle$, et soit un problème de E-unification dont la mesure vérifie $m_0 = n$ et $m_1 = m$.

Si $K = \{\langle f, c, G\rangle \in \Sigma_E \mid T \nprec c\} \neq \emptyset$, alors on pose $k_1 = |K|$, sinon on pose $k_1 = |\{\langle f, c, G\rangle \in \Sigma_E \mid T' \nprec c\}|$. Il y a deux cas à considérer.

- Si $k_1 = 0$, alors la règle de P-décomposition crée au plus gk problèmes de E-unification, et si $\langle m'_0, m'_1, m'_2, m'_3, m'_4\rangle$ est la mesure associée à un de ces problèmes, alors d'après le Lemme 11.3.11, on a $m'_0 \leq m_0$ et $m'_1 \leq m_1 - 1$. On a donc $\mathrm{T}(n, m) \leq (gk)\mathrm{T}(n, m-1)$, et par hypothèse d'induction, $\mathrm{T}(n, m-1) \leq (gk)^{n(1+2s)+(m-1)}$, d'où $\mathrm{T}(n, m) \leq (gk)^{n(1+2s)+m}$.
- Si $k_1 \neq 0$, alors la règle de P-décomposition crée au plus gk problèmes de E-unification, et si $\langle m'_0, m'_1, m'_2, m'_3, m'_4\rangle$ est la mesure associée à un de ces problèmes, alors d'après le Lemme 11.3.11, on a $m'_0 \leq m_0 - k_1 \leq m_0 - 1$ et $m'_1 \leq m_1 + 2s$. On a donc $\mathrm{T}(n, m) \leq (gk)\mathrm{T}(n-1, m+2s)$, et par hypothèse d'induction, $\mathrm{T}(n-1, m+2s) \leq (gk)^{(n-1)(1+2s)+(m+2s)}$, d'où $\mathrm{T}(n, m) \leq (gk)^{n(1+2s)+m}$. ■

Corollaire 11.3.16 *Soit S un problème de E-unification sur des* GA*-termes de taille n, et U un CSU pour S obtenu à partir des règles de transformation. Alors*

$$|U| \;\leq\; (gk)^{n(1+k+2ks)}.$$

PREUVE. Posons $S = \{T_1 =^?_E T'_1, \ldots, T_n =^?_E T'_n\}$, et pour tout $i \in \{1, \ldots, n\}$, posons $T_i = (V_i, s_i, a_i)$ et $T'_i = (V'_i, s'_i, a'_i)$. Il est clair que pour tout contexte c et pour tout

GA-terme T, on a $|\mathrm{V}_{T,c}| \leq |T|$, et donc, pour tout symbole $\langle f, c, G\rangle \in \Sigma_E$, et pour tout $i = 1, \ldots, n$, on a $|\mathrm{V}_{T_i,c} \cup \mathrm{V}_{T'_i,c}| \leq |V_i \cup V'_i|$. On en déduit donc que

$$|\bigcup_{i=1}^{n}(\mathrm{V}_{T_i,c} \cup \mathrm{V}_{T'_i,c})| \ \leq \ \|S\|.$$

Comme Σ_E contient k contextes, on en déduit que $|\mathcal{V}(S)| \leq kn$.

D'après le Théorème 11.3.15, on a $|U| \leq (gk)^{kn(1+2s)+n}$, d'où le résultat. ∎

Ainsi, étant donnée une théorie permutative définie par un ensemble d'axiomes unif-stable, nous pouvons calculer un CSU pour tout problème d'unification S, et cet CSU a une cardinalité bornée par une exponentielle simple en la taille de S. Il est donc par exemple plus efficace de résoudre un problème d'unification S modulo des théories permutatives définies par des ensembles d'axiomes unif-stables, que de les résoudre modulo des théories contenant des opérateurs associatifs et commutatifs, pour lesquels les CSU ont une taille bornée par une exponentielle double en la taille de S (voir [KN92]).

11.4 Résumé

Dans ce chapitre, nous avons d'abord défini des règles de transformation permettant de calculer un CSU pour tout problème de E-unification, quand E est défini par un ensemble d'axiomes unif-stable. Nous avons dû développer des outils spéciaux pour prouver que cet ensemble de règles termine, et l'hypothèse d'unif-stabilité a joué un rôle important dans la démonstration de la terminaison de cet ensemble de règles.

Le problème de l'unification modulo une théorie permutative avait été abordé dans [AP01] mais pas résolu. En effet, les auteurs y présentent un algorithme d'unification qui, étant donnés deux GA-termes stratifiés T et T', renvoie un ensemble de substitutions tel que $\mathrm{S}[T]\theta$ et $\mathrm{S}[T']\theta$ ont une intersection non vide. Mais, comme le remarquent les auteurs ([AP01, p. 261]), leur algorithme ne permet pas de faire de l'unification modulo une théorie permutative. Dans [Ave04], Jürgen Avenhaus a présenté un algorithme permettant de faire de l'unification modulo une théorie définie par un ensemble d'axiomes plat.

Nos travaux généralisent donc ceux de [Ave04], et prouvent que l'unification est simplement exponentielle pour toute une classe de théories permutatives.

Chapitre 12

Bilan et perspectives

Dans ce mémoire, nous avons adapté des techniques de réécriture de graphes de termes afin de développer des outils efficaces pour faire de la déduction modulo des théories permutatives. Nous avons d'abord défini les GA-termes, qui représentent les termes standard, puis les GA-termes stratifiés, qui représentent les termes stratifiés introduits dans [AP01]. Nous avons défini une action de groupe simple sur les GA-termes, et prouvé que les ensembles stratifiés de [AP01] peuvent être obtenus à partir d'orbites sous l'action d'un groupe. Nous avons ensuite défini la relation de congruence stratifiée sur les GA-termes stratifiés, et démontré que le problème de décision qui lui est associé est dans la classe de Luks, et peut donc en général être résolu de façon efficace.

Nous nous sommes intéressés aux tâches basiques qui devaient être accomplies par un démonstrateur automatique basé sur des GA-termes stratifiés, et avons démontré qu'elles sont NP-complètes, et cherché à imposer des restrictions aux théories permutatives considérées afin de réduire cette complexité. Nous avons ainsi défini la classe des théories permutatives définies par des ensembles d'axiomes unif-stables. Nous avons enfin démontré que l'unification modulo de telles théories est finitaire, et présenté un algorithme qui permet de calculer un CSU de taille simplement exponentielle pour tout problème d'unification.

L'essentiel de ces travaux ont été publiés, dans [BdlTE03a, BdlTE03b] et [BdlTE04a] pour la formalisation et l'étude de la complexité des problèmes liés à la déduction, et dans [BdlTE04b] et [BdlTE05] pour les théories permutatives définies par des ensembles d'axiomes unif-stables.

Autres travaux

Nous avons également effectué d'autres travaux au cours de cette thèse, qui n'ont pas été présentés dans ce mémoire.

1. En théorie algorithmique des groupes, nous avons étudié plusieurs restrictions du problème G_CSTR, ces restrictions portant sur la cardinalité des contraintes $(J_a)_{a\in A}$, et sur la structure des groupes qui agissent sur A. Nous avons prouvé par exemple que la restriction de ce problème aux instances telles que toutes les

contraintes sont de cardinalité au plus 2 et les groupes sont des p-groupes, demeure NP-complète.

Anna Lubiw a exhibé dans [Lub81] un problème de théorie des groupes qui est NP-complet. Ce problème est le suivant : étant donné un graphe $X = (V, E)$, existe-t-il une permutation $\sigma \in \mathrm{Aut}(X)$ sans point fixe ? Comme tout groupe est isomorphe au groupe d'automorphisme d'un graphe ([Fru38]), il est naturel que dans [Bab95], László Babai ait interprété ce résultat comme étant valable pour les groupes, et non pas pour les graphes. Il n'est cependant ni standard, ni aisé de représenter un groupe comme le groupe d'automorphisme d'un graphe, et il n'y a à notre connaissance aucun résultat permettant de borner la taille d'un graphe en fonction de l'ordre du groupe considéré. Le problème suivant est plus standard : étant donné un groupe de permutation G défini par un ensemble de générateur, existe-t-il une permutation dans G sans point fixe ? Nous avons démontré que ce problème est également NP-complet.

2. Nous avons effectué une étude plus poussée des GA-termes, et par exemple introduit les notions de *compactage* et *compactage stratifié* dans une optique d'implémentation, ces notions permettant de construire des GA-termes (resp. GA-termes stratifiés) contenant le moins de sommets possible. Nous avons également prouvé que le problème consistant à déterminer la cardinalité d'un ensemble stratifié est dans la classe de Luks sous l'hypothèse d'unif-stabilité, et simplifié les règles de transformation de l'unification pour résoudre les problèmes de filtrage.

Le système daTac est un démonstrateur automatique pour la logique du premier ordre avec égalité, qui a été implémenté par Laurent Vigneron ([RV95]). Ce démonstrateur est basé sur la résolution, la paramodulation et la réécriture, et permet de faire de la déduction modulo des opérateurs commutatifs et associatifs-commutatifs. Nous avions initialement l'intention d'intégrer les outils que nous avons développés pour traiter les théories définies par des ensembles d'axiomes unif-stables à ce démonstrateur. Nous espérions tester leur efficacité, et comparer leurs performances à celles d'autres démonstrateurs automatiques. Malheureusement, il a été impossible par manque de temps d'effectuer ces travaux. Il serait néanmoins intéressant de pouvoir tester ces outils sur des cas concrets.

Perspectives

En général, étant donnée une théorie définie par un ensemble d'axiomes, le sous-ensemble de ces axiomes qui sont des équations permutatives n'est pas unif-stable. Nous ne pouvons donc pas simplement séparer les équations permutatives de celles qui ne le sont pas et faire de la déduction modulo la théorie permutative induite. Il faut donc sélectionner un sous-ensemble unif-stable de ces équations permutatives, et il y a plusieurs stratégies qui peuvent être employées pour sélectionner un tel sous-ensemble. Nous avons commencé à concevoir certaines stratégies, et il serait intéressant de les étudier plus en détail.

Nous avons également exploré mais pas encore résolu certains problèmes plus théoriques. Par exemple, nous nous sommes demandés si les problèmes de filtrage modulo

une théorie définie par un ensemble d'axiomes unif-stable sont #P-complets. Le principe de résolution des problèmes de filtrage pour ces théories est proche de celui employé pour résoudre de tels problèmes pour la théorie de la commutativité, qui sont eux #P-complets (voir [HK95]). C'est donc sans doute également le cas pour les problème de filtrage sous l'hypothèse d'unif-stabilité. Il n'est cependant pas possible d'adapter la preuve de la #P-complétude des problèmes de filtrage modulo la commutativité à ce contexte plus général.

Dans [NO97], Narendran et Otto ont considéré une classe de théories équationnelles qui contient l'ensemble des théories permutatives. Cette classe est constituée des théories équationnelles définies par des équations de la forme $t \rightleftharpoons t'$, où t et t' ne sont pas nécessairement linéaires, mais vérifient $\text{arbre}(t) = \text{arbre}(t')$, et contiennent le même nombre d'occurrence de chaque variable. Un exemple d'une telle équation est $f(g(x), f(y, y)) \rightleftharpoons f(g(y), f(x, y))$. Narendran et Otto ont démontré que le problème de l'unifiabilité modulo de telles théories est indécidable, et il serait intéressant de voir si ce résultat est également valable pour la classe des théories permutatives.

Annexe A

Démonstrations

A.1 GA-termes

Unifiabilité de A-termes

Théorème 5.3.15 *Soient A_1, A_2 et A' trois* A*-termes tels que $h_1 : A_1 \sqsubseteq A'$ et $h_2 : A_2 \sqsubseteq A'$. Alors il existe un homomorphisme $h : A_1 \sqcup A_2 \sqsubseteq A'$.*

PREUVE. On pose $A_i = (V_i, s_i, a_i)$ pour $i = 1, 2$, et $A' = (V', s', a')$, on note respectivement r_1, r_2 et r' les racines de ces trois A-termes, et on démontre le résultat par induction sur la hauteur de A_1. Si $s_1(r_1) = \circ$, alors $A_1 \sqcup A_2 = A_2$, et h_2 est un homomorphisme de $A_1 \sqcup A_2$ vers A'. De même, si $s_2(r_2) = \circ$, alors h_1 est un homomorphisme de $A_1 \sqcup A_2$ vers A'. Sinon, on pose $a_1(r_1) = v_1.\cdots.v_n$, $a_2(r_2) = w_1.\cdots.w_n$, et $a'(r') = u'_1.\cdots.u'_n$, alors, d'après la Propriété 5.2.5 (2), pour $i = 1, 2$ et pour tout $j = 1, \ldots, n$, (une restriction de) h_i est un homomorphisme de $A_i|v_j$ vers $A'|u'_j$. Par hypothèse d'induction, on en déduit qu'il existe un homomorphisme h'_j de $A_1|v_j \sqcup A_2|w_j$ vers $A'|u'_j$.

On pose $A_1 \sqcup A_2 = (V, s, a)$, on note r sa racine, et supposons que $a(r) = u_1.\cdots.u_n$. Alors, par définition, on a $A|u_j = A_1|v_j \sqcup A_2|w_j$ pour tout $j = 1, \ldots, n$, ce qui prouve que les h'_j sont des homomorphismes de $A|u_j$ vers $A'|u'_j$. Il est alors clair que la fonction

$$h = \{\langle r, r'\rangle\} \cup \bigcup_{j=1}^{n} h'_j$$

est un homomorphisme de $A = A_1 \sqcup A_2$ vers A'. ∎

Action de groupe sur des GA-termes

Démonstration du Théorème 5.4.10

Dans ce qui suit, nous montrons que si $\mathcal{P}$ est une partition stratifiée dans un GA-terme T, alors l'application des éléments de $\mathrm{Sym}_V(\mathcal{P})$ à T produit des GA-termes dans lesquels $\mathcal{P}$ est encore stratifiée. Ce résultat prouvera donc qu'on a une action de $\mathrm{Sym}_V(\mathcal{P})$ sur l'ensemble des GA-termes dans lesquels $\mathcal{P}$ est stratifiée.

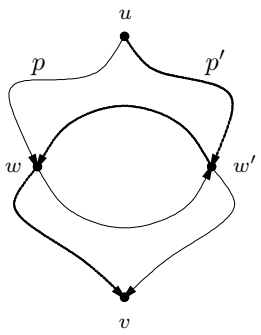

FIG. A.1 – Chemin de u à v dans un graphe étiqueté

On a le lemme suivant, qui montre qu'un certain ordre est préservé dans deux chemins distincts d'une même source à un même puits dans un graphe étiqueté *acyclique*.

Lemme A.1.1 *Soient p et p' deux chemins distincts d'un sommet u à un sommet v dans un graphe étiqueté G.*

Si w et w' sont deux sommets distincts apparaissant à la fois dans p et p' qui sont tels que :

1. *w' apparaît entre w et v dans p,*
2. *w apparaît entre w' et v dans p',*

alors il existe un cycle dans G.

PREUVE. Ceci est évident : si w' apparaît dans le sous-chemin de w à v dans p, alors on a un chemin non trivial de w à w' dans G, et si w apparaît dans le sous-chemin de w' à v dans p', alors on a également un chemin non trivial de w' à w dans G (voir la Figure A.1). ■

Nous étudions de quelle façon sont préservés certains chemins simples dans un graphe étiqueté.

Définition A.1.2 (Destination fixée dans un chemin) Etant donné un graphe étiqueté $G = (V, s, a)$ et un chemin p de source u dans G. Soit $\sigma \in \mathrm{Sym}(V)$, on dit que σ *fixe la destination de p* si et seulement si tous les sommets qui apparaissent dans p, sauf éventuellement u, sont des points fixes de σ. On dira également que p *a sa destination fixée par σ*.

Si $\mathcal{P}$ est une partition de V, alors on dit que $\mathcal{P}$ *fixe la destination de p* si et seulement si pour toute permutation $\sigma \in \mathrm{Sym}_V(\mathcal{P})$, σ fixe la destination de p, ce qui signifie que tous les sommets de p autres que sa source sont dans des $\mathcal{P}$-classes triviales.. On dira également que p *a sa destination fixée par $\mathcal{P}$*. ◇

Lemme A.1.3 *Soient G un graphe étiqueté, σ une permutation des sommets de G, et u, v deux sommets de V tels qu'il existe un chemin p de u à v dans G. Si σ fixe la destination de p, alors p est un chemin de u à v^σ dans G^σ.*

PREUVE. Posons $p = u_1.i_1.\cdots.u_n.i_n$ où, par hypothèse, $u_2, \ldots, u_n$ sont des points fixes de σ. Par définition d'un chemin, u_2 est le $i_1^{\text{ème}}$ élément de la liste $a_G(u_1)$ (autrement dit, $a_G(u_1)_{i_1} = u_2$). Or, le $i_1^{\text{ème}}$ élément de la liste $a_{G^\sigma}(u_1)$ est

$$a_{G^\sigma}(u_1)_{i_1} \;=\; a^\sigma_G(u_1)_{i_1} \;=\; [a_G(u_1)_{i_1}]^\sigma \;=\; u_2^\sigma \;=\; u_2,$$

et de même jusqu'à u_{n-1}. Enfin, on a :

$$a_{G^\sigma}(u_n)_{i_n} \;=\; a^\sigma_G(u_n)_{i_n} \;=\; [a_G(u_n)_{i_n}]^\sigma \;=\; v^\sigma.$$

Ceci prouve que p est un chemin dans G^σ de $u_1 = u$ à v^σ. ∎

Lemme A.1.4 *Soient G un graphe étiqueté, $\mathcal{P}$ une partition stratifiée dans G et σ un élément de* $\mathrm{Sym}_V(\mathcal{P})$. *Soit u un sommet de G qui est soit la racine de G, soit dans une classe non triviale de $\mathcal{P}$. Enfin, soit v un sommet tel qu'il existe un chemin non trivial de u à v dans G.*

1. *Si tous les chemins de u à v dans G ont leur destination fixée par $\mathcal{P}$, alors pour tout $v' \in v[\mathcal{P}]$, tous les chemins de u à v' dans G ont également leur destination fixée par $\mathcal{P}$.*
2. *Il existe un chemin de u à v dans G^σ.*

PREUVE. 1. Supposons qu'il existe un chemin de u à v' dans G qui contient un sommet $w \neq u$ tel que la classe $w[\mathcal{P}]$ est non triviale. Alors w est évidemment accessible depuis u dans G, et le sous-chemin de w à v' est nécessairement non trivial. Mais comme il existe un chemin de w à v' dans G, par hypothèse de stratification, il existe également un chemin de w à v dans G, et il existe donc un chemin de u à w et un chemin de w à v, c'est à dire un chemin de u à v qui passe par w. Ceci contredit l'hypthèse faite que tous les chemins de u à v ne contiennent que des sommets dans des $\mathcal{P}$-classes triviales.
2. Soient $\pi = \sigma^{-1}$ et p un chemin de u à v^π dans G. Alors p existe nécessairement puisque par hypothèse, u est soit la racine de G, soit dans une classe non triviale de $\mathcal{P}$, et que v et v^π sont dans la même $\mathcal{P}$-classe. On commence par décomposer p en une séquence de chemins non vides de la façon suivante : soient $u_1, \ldots, u_n$, pour $n \geq 0$, les sommets de p distincts de u qui sont dans des classes non triviales de $\mathcal{P}$, et qui apparaissent dans cet ordre dans p. On pose $u_0 = u$ et $u_{n+1} = v$, puis pour $i = 0, \ldots, n-1$, on définit p_i comme le sous-chemin de p de u_i à u_{i+1}. On a donc $p = p_0.\cdots.p_n$, et pour $i = 0, \ldots, n-1$, les p_i sont les *uniques* chemins de u_i à u_{i+1} par hypothèse de stratification.

Toujours par hypothèse de stratification, pour $i = 0, \ldots, n-1$, il existe un chemin q_i de u_i à u_{i+1}^π dans G, et ce chemin est unique. u_{i+1}^π est évidemment dans la $\mathcal{P}$-classe de u_{i+1}, et donc, d'après le point *1*, comme $\mathcal{P}$ fixe la destination de p_i, $\mathcal{P}$ fixe également la destination de q_i. Enfin, si v est dans une $\mathcal{P}$-classe non triviale, alors par hypothèse

de stratification, il existe un chemin de u_n à v^π, et ce chemin est unique. On le note q_n, et sa destination est également fixée par $\mathcal{P}$. Sinon, si v est dans une $\mathcal{P}$-classe triviale, on pose $q_n = p_n$.

Montrons que $q = q_0.\cdots.q_n$ est un chemin de u à v dans G^σ. Comme les q_i ont leur destination fixée par $\mathcal{P}$, on peut appliquer le Lemme A.1.3 et en déduire que pour tout $i = 0, \ldots, n$, q_i est un chemin dans G^σ de u_i à $(u_{i+1}^\pi)^\sigma = u_{i+1}$. Donc, q est une séquence de chemins dans G^σ de $u_0 = u$ à u_1, de u_1 à u_2, etc. C'est donc bien un chemin dans G^σ de u à $u_{n+1} = v$. ∎

La deuxième assertion de ce lemme permet alors de déduire que :

Corollaire A.1.5 *Soient G un graphe étiqueté possédant une racine r, et $\mathcal{P}$ une partition stratifiée dans G. Alors, pour tout σ de $\mathrm{Sym}_V(\mathcal{P})$, r est également une racine de G^σ.*

Lemme A.1.6 *Soient G un graphe étiqueté, $\mathcal{P}$ une partition stratifiée dans G, et $\sigma \in \mathrm{Sym}_V(\mathcal{P})$. Alors il existe un cycle dans G si et seulement s'il en existe un dans G^σ.*

PREUVE. Supposons qu'il n'existe aucun cycle passant par un sommet u dans G, et qu'il existe un chemin non trivial p de u à u dans G^σ. Posons $u_0 = u$ et $p = u_0.i_0.\cdots u_n.i_n$, où $n \geq 0$. On peut supposer sans perte de généralité qu'aucun sous-chemin de p n'est un cycle, les u_i étant donc distincts deux à deux.

Si pour $i = 1, \ldots, n$, tous les u_i sont des points fixes de σ, alors le Lemme A.1.3 appliqué à $\pi = \sigma^{-1}$ prouve que p est un chemin de u à u^π dans G. Si $u^\pi = u$, alors p est un cycle de u à u dans G, ce qui est impossible par hypothèse. Si $u^\pi \neq u$, alors u est dans la même $\mathcal{P}$-classe non triviale que u^π, ce qui est impossible d'après la Propriété 5.4.8

Donc, nécessairement, il doit exister un sommet u_j dans p, avec $j \neq 0$, tel que $u_j^\sigma \neq u_j$. Le chemin

$$u_j.i_j.\cdots.u_n.j_n.u_0.i_0.\cdots.u_{j-1}.i_{j-1}$$

est alors un cycle non trivial dans G^σ de u_j à u_j. Si tous les autres sommets de p sont fixés par σ, alors, comme dans le cas de u, il existe un chemin non trivial de u_j à u_j dans G, ce qui est impossible par hypothèse de stratification. Il doit donc y avoir un autre sommet w dans p, distinct de u_j, tel que $w^\sigma \neq w$. Le cycle p contient donc deux sommets distincts dans des classes non triviales, et il existe dans G^σ des chemins de u_j à w et de w à u_j. Le Lemme A.1.4 appliqué à G^σ et π prouve qu'il existe alors dans G un chemin de u_j à w, et un autre de w à u_j. On obtient à nouveau une contradiction avec l'hypothèse faite qu'il n'existe aucun cycle non trivial dans G.

Réciproquement, on peut appliquer exactement le même raisonnement non plus sur le graphe étiqueté G avec la permutation σ, mais sur le graphe étiqueté G^σ avec la permutation σ^{-1} : en supposant qu'il n'existe aucun cycle non trivial dans G^σ et qu'il en existe un dans G, on aboutit à la même contradiction. ∎

Corollaire A.1.7 *Si $\mathcal{P}$ est une partition stratifiée dans un* GA*-terme T, alors, pour toute permutation σ de $\mathrm{Sym}_V(\mathcal{P})$, T^σ est un* GA*-terme.*

PREUVE. Ceci est une conséquence immédiate du Corollaire A.1.5 et du Lemme A.1.6. ∎

Une autre conséquence immédiate du Corollaire A.1.7 est que ce résultat est également valable pour les A-termes.

Corollaire A.1.8 *Si $\mathcal{P}$ est une partition stratifiée dans un A-terme A, alors, pour toute permutation σ de $\mathrm{Sym}_V(\mathcal{P})$, A^σ est également un A-terme.*

PREUVE. D'après le Corollaire A.1.7, A^σ est un GA-terme, il s'agit donc de prouver que son graphe sous-jacent est un arbre. Le nombre d'arêtes du graphe sous-jacent à A est :

$$\sum_{v \in V} |a(v)| = \sum_{v \in V} \text{arité}(s(v)).$$

Donc, tous les graphes sous-jacents à des graphes étiquetés de $\mathcal{GE}(V, s)$ possèdent le même nombre d'arêtes, et comme le graphe sous-jacent à A a une structure d'arbre, ce nombre d'arêtes est égal à $|V| - 1$. Comme r est racine de A^σ d'après le Corollaire A.1.5, le graphe sous-jacent à A^σ est connexe, et comme tout graphe connexe à n sommets et $n - 1$ arêtes est un arbre, on en déduit que A^σ est un A-terme. ∎

La condition de stratification permet donc de conserver la structure de GA-terme et de A-terme. Il reste maintenant à prouver que cette condition de stratification est elle aussi conservée dans les GA-termes obtenus.

Théorème A.1.9 *Soit $T = (V, s, a)$ un GA-terme, et $\mathcal{P}$ une partition stratifiée dans T. Alors, pour tout $\sigma \in \mathrm{Sym}_V(\mathcal{P})$, $\mathcal{P}$ est stratifiée dans T^σ.*

PREUVE. Dans ce qui suit, on note r la racine de T (et de T^σ), et on pose $\pi = \sigma^{-1}$.

Soient u et v deux sommets de T^σ, où u est dans une $\mathcal{P}$-classe non triviale, tels qu'il existe un chemin non trivial de u à v dans T^σ. Alors, en appliquant le Lemme A.1.4 sur le graphe T^σ avec la permutation π, on en déduit qu'il existe également un chemin non trivial de u à v dans $(T^\sigma)^\pi = T$. Comme $\mathcal{P}$ est stratifiée dans T, on en déduit que pour tout sommet v' dans la $\mathcal{P}$-classe de v, il existe un chemin dans T de u à v'. En appliquant le Lemme A.1.4 sur T avec la permutation σ, on en déduit donc qu'il existe également un chemin de u à v' dans T^σ.

Prouvons maintenant par l'absurde que pour tout sommet u dans une $\mathcal{P}$-classe non triviale, le chemin de r à u dans T^σ est unique. Supposons donc qu'il existe un sommet u dans une $\mathcal{P}$-classe non triviale, et deux chemins distincts p et p' de r à u dans T^σ. Comme r est dans une classe triviale de $\mathcal{P}$, ces deux chemins sont non triviaux. Le fait que p et p' soient distincts ne signifie naturellement pas que leurs sommets sont nécessairement distincts. Par exemple,il suffirait d'avoir $a(r) = u.u$ pour obtenir deux chemins distincts de r à u, dont tous les sommets sont identiques.

Supposons d'abord que tous les sommets de p et de p' sont identiques. Quitte à remplacer u par un autre sommet de p (et p') au-dessus de u, on peut supposer que tous les sommets entre r et u sont dans des classes triviales de $\mathcal{P}$. D'après le Lemme A.1.3, p et p' sont alors des chemins distincts de r à u^π dans T, ce qui est impossible car u^π est dans la même $\mathcal{P}$-classe que u.

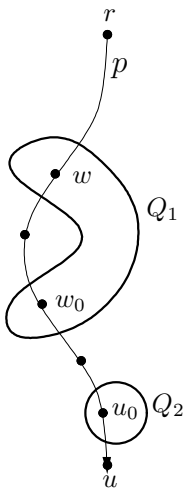

FIG. A.2 – Les ensembles Q_1 et Q_2 (Théorème A.1.9).

Supposons maintenant qu'il existe un sommet w qui est dans p mais pas dans p'. Alors on note R_1 l'ensemble des sommets de V qui apparaissent dans p mais pas dans p', et on définit

$$Q_1 \;=\; \{v \in R_1 \,|\, v[\mathcal{P}] \text{ est une classe non triviale}\}.$$

Q_1 peut éventuellement être vide, mais l'élément $w_0 = \min_{\leq_T}(Q_1 \cup \{w\})$ est bien défini.

On note R_2 l'ensemble des sommets de $V|w_0$ qui apparaissent dans p et dans p', puis on définit

$$Q_2 \;=\; \{v \in R_2 \,|\, v[\mathcal{P}] \text{ est une classe non triviale}\}.$$

L'ensemble Q_2 peut également être vide, mais le sommet $u_0 = \max_{\leq_T}(Q_2 \cup \{u\})$ est bien défini, il est dans une $\mathcal{P}$-classe non triviale, et on a $u_0 <_T w_0$. De plus, par construction, le sous-chemin de p de w_0 à u_0 a sa destination fixée par $\mathcal{P}$ (voir la Figure A.2).

En appliquant le Lemme A.1.4 sur T^σ avec la permutation π, on en déduit qu'il existe un chemin dans T de r à w_0, et le chemin de w_0 à u_0 dans T^σ est un chemin de w_0 à u_0^π dans T, d'après le Lemme A.1.3. Donc, il existe dans T un chemin de r à u_0^π qui passe par w_0.

Supposons maintenant qu'il existe un sommet w' dans le sous-chemin de p' de r à u_0, qui n'apparaît pas dans p. Alors on note R_1' l'ensemble des sommets qui apparaissent dans p' mais pas dans p, et on définit

$$Q_1' \;=\; \{v \in R_1' \,|\, u_0 \leq_T v \text{ et } v[\mathcal{P}] \text{ est une classe non triviale}\}.$$

On pose $w_0' = \min_{\leq_T}(Q_1' \cup \{w'\})$, alors comme précédemment, $u_0 <_T w_0'$, et le sous-chemin de p' de w_0' à u_0 a sa destination fixée par $\mathcal{P}$. Le raisonnement précédent prouve qu'il existe alors un chemin de r à u_0^π dans T qui passe par w_0', et on a une contradiction,

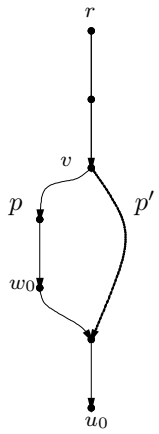

FIG. A.3 – Chemins de r à u_0 dans T^σ

puisqu'il existe alors deux chemins distincts de r à u_0 dans T, l'un qui passe par w_0, et l'autre par w_0'.

Enfin, si tous les sommets du sous-chemin de p' de r à u_0 sont également dans p, alors on note v le plus petit ancêtre de w_0 pour la relation $\leq_T$ qui est dans p' (voir la Figure A.3). Alors par hypothèse, le sous-chemin de p' de v à u_0 a sa destination fixée par $\mathcal{P}$, puisque tous les sommets qui y apparaissent, sauf éventuellement v, sont également dans le sous-chemin de p de w_0 à u_0, et que w_0 n'en fait pas partie. Ce sous-chemin est donc un chemin de v à u_0^π dans T qui ne passe évidemment pas par w_0. Il existe donc dans T un chemin de r à u_0^π qui passe par v, d'après le Lemme A.1.3. Si v n'apparaît pas dans le chemin de r à u_0^π qui passe par w_0 dans T, on a une contradiction puisqu'on a alors un chemin de r à u_0 qui passe par w_0, et un autre qui passe par v. Si v y apparaît, il est nécessairement dans le sous-chemin de r à w_0 d'après le Lemme A.1.1, et on a à nouveau deux chemins distincts de r à u_0^π dans T : l'un passant par v et w_0, et l'autre passant uniquement par v. ∎

Les Corollaires A.1.7 et A.1.8, ainsi que le Théorème A.1.9 prouvent le Théorème 5.4.10.

A.2 Stabilité

Nous allons prouver que l'équation permutative $c' \rightleftharpoons c'^{\Phi[c,c',v](\sigma)}$ est une conséquence logique de l'équation permutative $c \rightleftharpoons c^\sigma$. Nous allons montrer que si c et c' sont deux contextes tels que $h, p' : c \trianglelefteq_\sigma c'$, alors pour tout terme t qui est instance de c' à la position p, il revient au même d'appliquer l'équation permutative $c \rightleftharpoons c^\sigma$ à la position $p.p'$ de t', et l'équation permutative $c' \rightleftharpoons c'^{\Phi[c,c',p']}(\sigma)$ à la position p de t.

Nous prouvons d'abord un premier lemme :

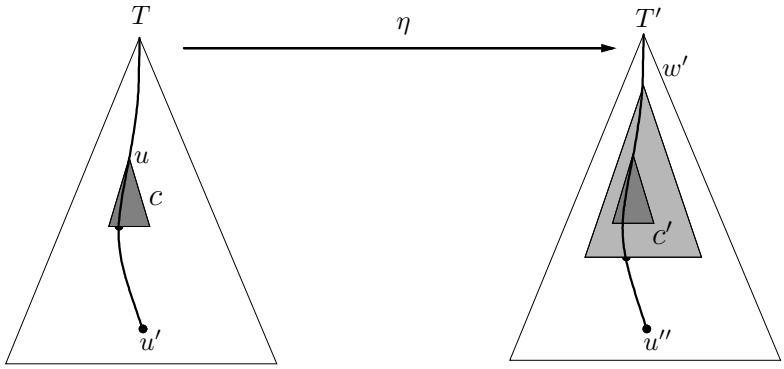

FIG. A.4 – Lemme A.2.1 et Théorème A.2.3

Lemme A.2.1 *Soient c et c' deux contextes tels que $h, v : c \trianglelefteq c'$. Soient $T = (V, s, a)$ et $T' = (V', s', a')$ deux* GA*-termes stratifiés tels que (voir la Figure A.4) :*
- *il existe un isomorphisme η de $\mathrm{dm}(T)$ vers $\mathrm{dm}(T')$,*
- *il existe un sommet $w' \in V'$ tel que $s'(w') = \langle f', c', G' \rangle \in \Sigma_E$,*
- *il existe un sommet $u \in V$ tel que $s(u) = \langle f, c, G \rangle$, et $\eta(u) = \mathrm{h}_{[T',w']}(v)$.*

Alors pour tout sommet v' de c, on a $\eta \circ \mathrm{h}_{[T,u]}(v') = \mathrm{h}_{[T',w']} \circ h(v')$.

PREUVE. Par définition, $\mathrm{h}_{[T,u]}$ est un homomorphisme de c vers $\mathrm{dm}(T)|u$, et donc, la fonction $\eta \circ \mathrm{h}_{[T,u]}$ est un homomorphisme de c vers $\mathrm{dm}(T')|\eta(u)$ d'après la Propriété 5.2.4. Comme $\mathrm{h}_{[T',w']}$ est un homomorphisme de c' vers $\mathrm{dm}(T')|w'$, alors d'après la Propriété 5.2.5 (2), une restriction h' de $\mathrm{h}_{[T',w']}$ est un homomorphisme de $c'|v$ vers $\mathrm{dm}(T')|\mathrm{h}_{[T',w']}(v)$. Comme h est un homomorphisme de c vers $c'|v$, $h' \circ h$ est un homomorphisme de c vers $\mathrm{dm}(T')|\mathrm{h}_{[T',w']}(v)$. Enfin, $\eta(u) = \mathrm{h}_{[T',w']}(v)$ par hypothèse, et par unicité des homomorphismes (Corollaire 5.2.6), on a le résultat. ∎

Corollaire A.2.2 *Sous les hypothèses du Lemme A.2.1, on a $\eta(\mathrm{R}_T(w)) \subseteq \overline{\mathrm{R}}_{T'}(w') \cup \mathrm{R}_{T'}(w')$.*

PREUVE. Par définition, on a $\eta(\mathrm{R}_T(u)) = \eta \circ \mathrm{h}_{[T,u]}(\mathcal{SV}(c))$, et d'après le Lemme A.2.1, $\eta(\mathrm{R}_T(u)) = \mathrm{h}_{[T',w']} \circ h(\mathcal{SV}(c))$. Si $V_{c'}$ est l'ensemble des sommets de c', on a $h(\mathcal{SV}(c)) \subseteq V_{c'}$, et comme $\mathrm{h}_{[T',w']}(V_{c'}) = \overline{\mathrm{R}}_{T'}(w') \cup \mathrm{R}_{T'}(w')$, on obtient le résultat. ∎

Théorème A.2.3 *Soient $\langle f, c, G \rangle$ et $\langle f', c', G' \rangle$ deux éléments de Σ_E, et σ une permutation dans G telle que $h, v : c \trianglelefteq_\sigma c'$. Soient $T = (V, s, a)$ et $T' = (V', s', a')$ deux* GA*-termes stratifiés tels que (voir la Figure A.4) :*
- *il existe un isomorphisme η de $\mathrm{dm}(T)$ vers $\mathrm{dm}(T')$,*
- *il existe un sommet $w \in V$ et un homomorphisme h' de c' vers $\mathrm{dm}(T|w)$,*

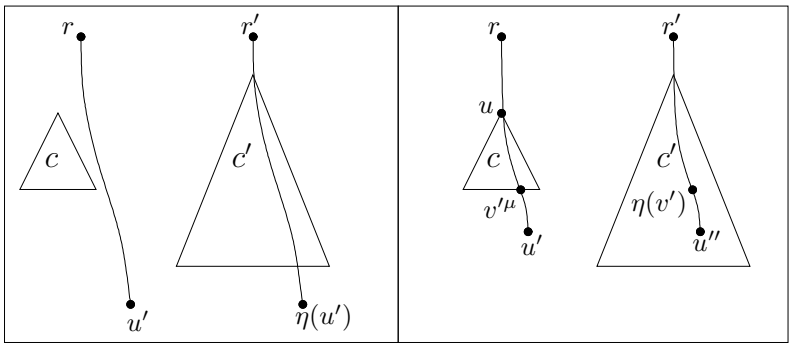

FIG. A.5 – Théorème A.2.3, cas 1 et 2

– *si* $u = h'(v)$, *alors* $s(u) = \langle f, c, G\rangle$,
– *le sommet* $w' = \eta(w)$ *est étiqueté par* $\langle f', c', G'\rangle$.

On pose $\mu = \sigma^{\mathrm{h}_{[T,u]}}$ *et* $\delta = (\Phi[c, c', v](\sigma))^{\mathrm{h}_{[T',w']}}$, *alors* $\mathrm{dm}(T^\mu) \stackrel{\circ}{=} \mathrm{dm}(T'^\delta)$.

De plus, si pour tout sommet $u' \in V \setminus \{u, w\}$, *on a* $s(u') = s'(\eta(u'))$, *alors pour tout chemin* p *de* r *à* u' *dans* T, *le chemin* p' *de source* r' *et parallèle à* p *dans* T' *a son puits* u'' *qui vérifie* $s(u') = s'(u'')$.

PREUVE. Notons r la racine de T, r' la racine de T', et posons $c' = (V_{c'}, s_{c'}, a_{c'})$. Nous allons montrer que pour tout chemin p de r à u' dans T^μ, il existe un chemin p' dans T'^δ de source r', qui est parallèle à p, et dont le puits u'' vérifie $\mathrm{dm} \circ s'(u'') = \mathrm{dm} \circ s(u')$. D'après le Lemme 5.1.18, ceci prouvera que $\mathrm{dm}(T^\mu) \stackrel{\circ}{=} \mathrm{dm}(T'^\delta)$. Soit p un chemin de r à u' dans T^μ, il y a plusieurs cas à considérer :

1. Si ni u', ni les sommets apparaissant dans p ne sont éléments de $\mathrm{R}_T(u)$ (voir la Figure A.5, dessin de gauche), alors tous ces éléments sont des points fixes de μ, et d'après le Lemme A.1.3, p est un chemin de r à u' dans T. La fonction η étant un isomorphisme de $\mathrm{dm}(T)$ vers $\mathrm{dm}(T')$, $\eta(p)$ est alors un chemin de r' à $u'' = \eta(u')$ dans T' d'après la Propriété 5.2.5 (3). Si ni u'', ni les sommets apparaissant dans $\eta(p)$ ne sont dans $\mathrm{R}_{T'}(w')$, alors ces éléments sont tous des points fixes de δ, et $\eta(p)$ est également un chemin de r' à u'' dans T'^δ d'après le Lemme A.1.3. Enfin, si $u' \notin \{u, w\}$, alors $s(u') = s'(\eta(u')) = s'(u'')$, et sinon, $\mathrm{dm} \circ s(u') = \mathrm{dm} \circ s'(u'')$.
   Supposons maintenant que u'' ou un des sommets apparaissant dans $\eta(p)$ est élément de $\mathrm{R}_{T'}(w')$. Comme $\mathrm{R}_{T'}(w')$ est un ensemble indépendant dans T', cet élément est unique, notons-le w''. Comme T' est un GA-terme stratifié, il existe un unique chemin de r' à w'', et ce chemin est donc un préfixe de $\eta(p)$, ce qui prouve que w'' n'est en-dessous d'aucun $\eta(v')$ pour $v' \in \mathrm{R}_T(u)$. Donc, par définition de $\Phi[c, c', v](\sigma)$, on a $w''^\delta = w''$. Ainsi, dans ce cas, $\eta(p)$ est encore un chemin de r' à u'' dans T'^δ d'après le Lemme A.1.3. Ce chemin est parallèle à p d'après la Propriété 5.1.9, et on a $\mathrm{dm} \circ s'(u'') = \mathrm{dm} \circ s(u')$. Enfin, si $u' \notin \{u, w\}$, alors il est clair que $s(u') = s'(u'')$.
2. Supposons que u' est en-dessous d'un sommet $v'^\mu \in \mathrm{R}_T(u)$, et que $\eta(u') \in \overline{\mathrm{R}}_{T'}(w')$

(voir la Figure A.5, dessin de droite). On pose alors $p = p_1.p_2$, où p_1 est un chemin de r à v'^{μ} dans T^{μ}, et p_2 est un chemin de v'^{μ} à u' dans T^{μ} (p_2 peut éventuellement être vide). D'après le Lemme A.1.3, p_1 est donc un chemin de r à v' dans T, et p_2 un chemin de v'^{μ} à u' dans T.

D'après la Propriété 5.2.5 (3), $\eta(p_1)$ est un chemin de r' à $\eta(v')$, et $\eta(p_2)$ un chemin de $\eta(v'^{\mu})$ à $\eta(u')$ dans T'. D'après le Corollaire A.2.2, $\eta(v') \in \overline{\mathrm{R}}_{T'}(w') \cup \mathrm{R}_{T'}(w')$, et comme $\eta(u') \in \overline{\mathrm{R}}_{T'}(w')$ par hypothèse, nécessairement, $\eta(v')$ est élément de $\overline{\mathrm{R}}_{T'}(w')$. Donc, tous les sommets apparaissant dans $\eta(p_1)$ sont des points fixes de δ, et $\eta(p_1)$ est un chemin de r' à $\eta(v')$ dans T'^{δ}.

Posons $w_1 = \mathrm{h}^{-1}_{[T,u]}(v')$, alors $v'^{\mu} = \mathrm{h}_{[T,u]}(w_1^{\sigma})$ par définition, et $\eta(v'^{\mu}) = \mathrm{h}_{[T',w']}(h(w_1^{\sigma}))$ d'après le Lemme A.2.1. Soit $w_2 = \mathrm{h}^{-1}_{[T',w']}(\eta(u'))$, alors $q = \mathrm{h}^{-1}_{[T',w']}(\eta(p_2))$ est un chemin de $h(w_1^{\sigma})$ à w_2 dans c'. Le chemin q est donc parallèle à p, et on a $s_{c'}(w_2) = s(u')$, car $\eta(u') \in \overline{\mathrm{R}}_{T'}(w')$, et w_2 est donc un sommet non-variable de c'.

On note η_1 l'isomorphisme de $c'|h(w_1^{\sigma})$ vers $c'|h(w_1)$, alors $q' = \eta_1(q)$ est un chemin de $h(w_1)$ vers un sommet $w_3 = \eta_1(w_2)$ dans c', qui est parallèle à q, et on a $s_{c'}(w_3) = s_{c'}(w_2)$. D'après le Lemme A.2.1, on en déduit que $p_3 = \mathrm{h}_{[T',w']}(q')$ est un chemin de $\mathrm{h}_{[T',w']}(h(w_1)) = \eta \circ \mathrm{h}_{[T,u]}(w_1) = \eta(v')$ vers $u'' = \mathrm{h}_{[T',w']}(w_3)$ dans T', qui est parallèle à q', et $s'(u'') = s_{c'}(w_3)$. Donc, $p' = \eta(p_1).p_3$ est un chemin de r' à u'' dans T'. Comme aucun des sommets apparaissant dans p_3 n'est élément de $\mathrm{R}_{T'}(w')$, on en déduit que p' est également un chemin de r' à u'' dans T'^{δ} qui est parallèle à p, et que $s'(u'') = s(u')$.

3. Supposons que u' soit en-dessous de $v'^{\mu} \in \mathrm{R}_T(u)$ et que $\eta(v'^{\mu}) \in \mathrm{R}_{T'}(w')$ (Figure A.6, dessin de gauche). On pose alors $p = p_1.p_2$, où p_1 est un chemin de r à v'^{μ} dans T^{μ}, et p_2 est un chemin de v'^{μ} à u' dans T^{μ} (p_2 peut éventuellement être vide). Alors, comme précédemment, p_1 est un chemin de r à v' dans T, et donc $\eta(p_1)$ est un chemin de r' à $\eta(v')$ dans T', et un chemin de r' à $\eta(v')^{\delta}$ dans T'^{δ}. Par définition, si $w_1 = \mathrm{h}^{-1}_{[T,u]}(v')$, alors $w_1^{\sigma} = \mathrm{h}^{-1}_{[T,u]}(v'^{\mu})$, et comme $\eta \circ \mathrm{h}_{[T,u]}(w_1^{\sigma}) \in \mathrm{R}_{T'}(w')$ par hypothèse, alors $h(w_1^{\sigma}) \in \mathcal{SV}(c')$ d'après le Lemme A.2.1. Par définition, on a alors $h(w_1)^{\Phi[c,c',v](\sigma)} = h(w_1^{\sigma})$, d'où :

$$\begin{aligned} \eta(w)^{\delta} &= \mathrm{h}_{[T',v']}(h(w_1)^{\Phi[c,c',v](\sigma)}) \\ &= \mathrm{h}_{[T',v']}(h(w_1^{\sigma})) \\ &= \eta \circ \mathrm{h}_{[T,u]}(w_1^{\sigma}) \\ &= \eta(v'^{\mu}). \end{aligned}$$

Donc, $\eta(p_1)$ est un chemin de r' à $\eta(v'^{\mu})$ dans T'^{δ}, et comme $\eta(p_2)$ est un chemin de $\eta(v'^{\mu})$ à $\eta(u')$ dans T' et T'^{δ}, on en déduit que $\eta(p)$ est un chemin de r' à $u'' = \eta(u')$ dans T'^{δ}. Ce chemin est parallèle à p, et si $u' \notin \{u, w\}$, alors $s(u') = s'(u'')$, sinon, $\mathrm{dm} \circ s(u') = \mathrm{dm} \circ s'(u'')$.

4. Supposons que u' est en-dessous de $v_1^{\mu} \in \mathrm{R}_T(u)$, et de v_2 tel que $\eta(v_2) \in \mathrm{R}_{T'}(v')$, où $v_1^{\mu} \neq v_2$ (Figure A.6, dessin de droite). On pose alors $p = p_1.p_2.p_3$, où p_1 est un

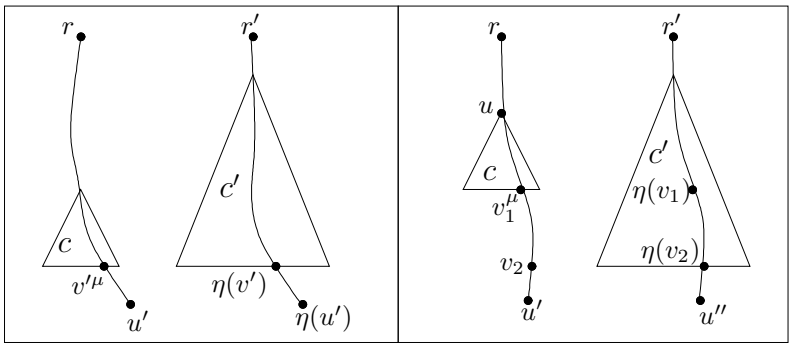

FIG. A.6 – Théorème A.2.3, cas 3 et 4

chemin de r à v_1^μ, p_2 un chemin de v_1^μ à v_2, et p_3 un chemin de v_2 à u' dans T^μ (p_3 est éventuellement vide). Comme $v_1^\mu \neq v_2$, alors $\eta(v_1) \in \overline{\mathrm{R}}_{T'}(w')$, et $\eta(p_1)$ est un chemin de r' à $\eta(v_1)$ dans T' et dans T'^δ, et $\eta(p_2)$ est un chemin de $\eta(v_1^\mu)$ à $\eta(v_2)$ dans T'. Si $u_1 = \mathrm{h}^{-1}_{[T,u]}(v_1)$, alors $u_1^\sigma = \mathrm{h}^{-1}_{[T,u]}(v_1^\mu)$ par définition, et d'après le Lemme A.2.1, $h(u_1^\sigma) = \mathrm{h}^{-1}_{[T',w']} \circ \eta(v_1^\mu)$. Posons $w_2 = \mathrm{h}^{-1}_{[T',w']}(\eta(v_2))$, alors $q = \mathrm{h}^{-1}_{[T',w']}(\eta(p_2))$ est un chemin de $h(u_1^\sigma)$ à w_2 dans c', et ce chemin est évidemment parallèle à p_2. Soit η_1 l'isomorphisme de $c'|h(u_1^\sigma)$ vers $c'|h(u_1)$, alors $\eta_1(q)$ est un chemin de u_1 à un sommet $w_3 \in \mathcal{SV}(c')$ dans c', et par définition, $w_3^{\Phi[c,c',v](\sigma)} = w_2$. Posons $q' = \mathrm{h}_{[T',w']}(\eta_1(q))$, alors q' est un chemin de $\mathrm{h}_{[T',w']} \circ h(u_1)$ à $\mathrm{h}_{[T',w']}(w_3)$ dans T', et q' est parallèle à q. D'après le Lemme A.2.1, on a $\mathrm{h}_{[T',w']} \circ h(u_1) = \eta \circ \mathrm{h}_{[T,u]}(u_1) = \eta(v_1)$, et donc, q' est un chemin de $\eta(v_1)$ à $\mathrm{h}_{[T',w']}(w_3^{\Phi[c,c',v](\sigma)})$ dans T'^δ. Comme $\mathrm{h}_{[T',w']}(w_3^{\Phi[c,c',v](\sigma)}) = \mathrm{h}_{[T',w']}(w_2) = \eta(v_2)$, on en déduit que q' est un chemin de $\eta(v_1)$ à $\eta(v_2)$ dans T'^δ. Enfin, $\eta(p_3)$ est un chemin de $\eta(v_2)$ à $u'' = \eta(u')$ dans T' et dans T'^δ, et ce chemin est parallèle à p_3, donc, $\eta(p_1).q'.\eta(p_3)$ est un chemin de r' à u'' dans T'^δ qui est parallèle à p. Comme u' ne peut pas être élément de $\{u, w\}$, on a nécessairement $s'(u'') = s(u')$. ∎

Bibliographie

[AP01] J. Avenhaus and D. Plaisted. General algorithms for permutations in equational inference. *Journal of Automated Reasoning*, 26 :223–268, April 2001.

[Ave04] Jürgen Avenhaus. Efficient algorithms for computing modulo permutation theories. In David Basin and Michaël Rusinowitch, editors, *IJCAR*, volume 3097 of *Lecture Notes in Computer Science*, pages 415–429. Springer, 2004.

[Baa87] Franz Baader. The theory of idempotent semigroups is of unification type zero. *J. Autom. Reason.*, 2(3) :283–286, 1987.

[Baa89] Franz Baader. Characterizations of unification type zero. In Nachum Dershowitz, editor, *RTA'89*, volume 355 of *Lecture Notes in Computer Science*, pages 2–14. Springer, 1989.

[Bab95] László Babai. Automorphism groups, isomorphism, reconstruction. In R. L. Graham, M. Grotschel, and L. Lovasz, editors, *Handbook of Combinatorics*, volume 2. Elsevier and The MIT Press, 1995.

[BC88] G. Butler and J. Cannon. Cayley version 4 : the User Language. In P. Gianni, editor, *Proceedings ISSAC 1988*, Lecture Notes in Computer Science, pages 456–466. Springer, 1988.

[BC90] G. Butler and J. Cannon. The Design of Cayley - A Language for Modern Algebra. In Alfonso Miola, editor, *Proceedings DISCO '90*, volume 429 of *Lecture Notes in Computer Science*. Springer, 1990.

[BD89] L. Bachmair and Nachum Dershowitz. Completion for rewriting modulo a congruence. *Theor. Comput. Sci.*, 67(2-3) :173–201, 1989.

[BdlTE03a] T. Boy de la Tour and M. Echenim. On leaf permutative theories and occurrence permutation groups. In Ingo Dahn and Laurent Vigneron, editors, *FTP'2003*, volume 86 of *Electronic Notes in TCS*, Valencia, Spain, june 2003. Elsevier.

[BdlTE03b] T. Boy de la Tour and M. Echenim. **NP**-completeness results for deductive problems on stratified terms. In Moshe Vardi and Andrei Voronkov, editors, *LPAR*, LNAI 2850, pages 315–329, Almaty, Kazakhstan, september 2003. Springer Verlag.

[BdlTE04a] Thierry Boy de la Tour and Mnacho Echenim. On the complexity of deduction modulo leaf permutative equations. *Journal of Automated Reasoning*, 33(3-4) :271–317, 2004.

[BdlTE04b] Thierry Boy de la Tour and Mnacho Echenim. Overlapping leaf permutative equations. In David Basin and Michaël Rusinowitch, editors, *Second International Joint Conference IJCAR*, volume 3097 of *Lecture Notes in Artificial Intelligence*, pages 430–444, Cork, Ireland, july 2004. Springer Verlag.

[BdlTE05] Thierry Boy de la Tour and Mnacho Echenim. Unification in a class of permutative theories. In Jürgen Giesl, editor, *RTA*, volume 3467 of *Lecture Notes in Computer Science*, pages 430–444, Nara, Japan, april 2005. Springer.

[Bet55] Evert W. Beth. Semantic entailment and formal derivability. *Koninklijke Nederlandse Akademie van Wentenschappen, Proceedings of the Section of Sciences*, 18 :309–342, 1955.

[BN98] F. Baader and T. Nipkow. *Term Rewriting and All That.* Cambridge University Press, 1998.

[BS01] F. Baader and W. Snyder. Unification theory. In J.A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, volume I, pages 447–533. Elsevier Science Publishers, 2001.

[But91] G. Butler. *Fundamental algorithms for permutation groups.* Lecture Notes in Computer Science 559. Springer Verlag, 1991.

[BvEG+87] H. P. Barendregt, M. C. J. D. van Eekelen, J. R. W. Glauert, J. R. Kennaway, M. J. Plasmeijer, and M. R. Sleep. Term graph rewriting. In J. W. de Bakker, A. J. Nijman, and P. C. Treleaven, editors, *PARLE'87*, volume 2 of *LNCS 259*, pages 141–158. Springer Verlag, june 1987.

[Can84] J.J. Cannon. An Introduction to the Group Theory Language, Cayley. *Computer Group Theory*, pages 145–158, 1984.

[CEJS98] Edmund M. Clarke, E. Allen Emerson, Somesh Jha, and A. Prasad Sistla. Symmetry reductions in model checking. In Alan J. Hu and Moshe Y. Vardi, editors, *CAV'98*, LNCS 1427, pages 147–158, Vancouver, BC, Canada, june 1998. Springer Verlag.

[Coo71] Stephen A. Cook. The complexity of theorem-proving procedures. In *STOC '71 : Proceedings of the third annual ACM symposium on Theory of computing*, pages 151–158, New York, NY, USA, 1971. ACM Press.

[CP97] J. Cannon and C. Playoust. An Introduction to MAGMA. *Springer-Verlag*, 1997.

[Deh11] M. Dehn. Ueber unendlichediskontinuierliche gruppen. *Math. Annalen*, 71 :116–144, 1911.

[DF03] David Dummit and Richard Foote. *Abstract Algebra.* Wiley, 2003.

[DLL83] M. Davis, G. Logemann, and D. Loveland. A machine program for theorem proving. In J. Siekmann and G. Wrightson, editors, *Automation of Reasoning 1 : Classical Papers on Computational Logic 1957-1966*, pages 267–270. Springer, Berlin, Heidelberg, 1983.

[DM79] Nachum Dershowitz and Zohar Manna. Proving termination with multiset orderings. *Commun. ACM*, 22(8) :465–476, 1979.

[Dom92] Eric Domenjoud. A technical note on ac-unification. the number of minimal unifiers of the equation alpha x_1 + . . . + alpha x_p =ac beta y_1 + . . . + beta y_q. *J. Autom. Reasoning*, 8(1) :39–44, 1992.

[DP01] Nachum Dershowitz and David A. Plaisted. Rewriting. In J.A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*, volume I, pages 535–610. Elsevier Science Publishers, 2001.

[Fag84] François Fages. Associative-commutative unification. In Robert E. Shostak, editor, *CADE*, volume 170 of *Lecture Notes in Computer Science*, pages 194–208. Springer, 1984.

[FH86] François Fages and Gérard P. Huet. Complete sets of unifiers and matchers in equational theories. *Theor. Comput. Sci.*, 43 :189–200, 1986.

[Fru38] R. Frucht. Herstellung von graphen mit vorgegebener abstrakter gruppe. *Compositio Math.*, 6 :239–250, 1938.

[GJ79] M. Garey and D. S. Johnson. *Computers and intractability : a guide to the theory of* **NP***-completeness*. Freeman, San Francisco, California, 1979.

[Hin55] K. J. J. Hintikka. Form and content in quantification theory. *Acta Philosohica Fennica*, 8 :7–55, 1955.

[HK95] Miki Hermann and Phokion G. Kolaitis. The complexity of counting problems in equational matching. *J. Symb. Comput.*, 20(3) :343–362, 1995.

[Hof81] C. Hoffmann. *Group-theoretic algorithms and graph isomorphism*. Lecture Notes in Computer Science 136. Springer Verlag, 1981.

[JK86] Jean-Pierre Jouannaud and Hélène Kirchner. Completion of a set of rules modulo a set of equations. *SIAM J. Comput.*, 15(4) :1155–1194, 1986.

[Jou87] Jean-Pierre Jouannaud. A set of eleven important open problems in term rewriting based theorem proving. *Bulletin of the EATCS*, 31 :272–273, 1987.

[KB83] D. E. Knuth and P. B. Bendix. Simple word problems in universal algebras. In J. Siekmann and G. Wrightson, editors, *Automation of Reasoning 2 : Classical Papers on Computational Logic 1967-1970*, pages 342–376. Springer, Berlin, Heidelberg, 1983.

[KK90] Claude Kirchner and Francis Klay. Syntactic theories and unification. In John Mitchell, editor, *Proceedings of the Fifth Annual IEEE Symp. on Logic in Computer Science*, pages 270–277. IEEE Computer Society Press, june 1990.

[KKSdV93] J. R. Kennaway, J. W. Klop, M. R. Sleep, and F. J. de Vries. *An introduction to term graph rewriting*, pages 1–13. John Wiley and Sons Ltd., Chichester, UK, UK, 1993.

[Klo95] Jan Willem Klop. Term graph rewriting. In Gilles Dowek, Jan Heering, Karl Meinke, and Bernhard Möller, editors, *HOA*, volume 1074 of *Lecture Notes in Computer Science*, pages 1–16, 1995.

[KN92] D. Kapur and P. Narendran. Double-exponential complexity of computing a complete set of ac-unifiers. In Andre Scedrov, editor, *Proceedings of the Seventh Annual IEEE Symp. on Logic in Computer Science, LICS 1992*, pages 11–21. IEEE Computer Society Press, June 1992.

[LB77a] D. S. Lankford and A. Ballantyne. Decision procedures for simple equational theories with associative commutative axioms : complete sets of associative commutative reductions. Technical report, Univ. of Texas at Austin, Dept. of Mathematics and Computer Science, 1977.

[LB77b] D. S. Lankford and A. Ballantyne. Decision procedures for simple equational theories with permutative axioms : complete sets of permutative reductions. Technical report, Univ. of Texas at Austin, Dept. of Mathematics and Computer Science, 1977.

[Lub81] Anna Lubiw. Some NP-complete problems similar to graph isomorphism. *SIAM Journal on Computing*, 10(1) :11–21, 1981.

[Luk82] Eugene M. Luks. Isomorphism of graphs of bounded valence can be tested in polynomial time. *J. Comput. Syst. Sci.*, 25(1) :42–65, 1982.

[Luk93] Eugene M. Luks. Permutation groups and polynomial-time computation. volume 11 of *Amer. Math. Soc. DIMACS Series*, pages 139–175. (DIMACS, 1991), 1993.

[NO97] Paliath Narendran and Friedrich Otto. Single versus simultaneous equational unification and equational unification for variable-permuting theories. *J. Autom. Reasoning*, 19(1) :87–115, 1997.

[Nov55] P. S. Novikov. On the algorithmic unsolvability of the word problem in group theory. *Trudy Mat. Inst. Steklov*, 44 :1–143, 1955.

[NR01] Robert Nieuwenhuis and Albert Rubio. Paramodulation-based theorem proving. In *Handbook of Automated Reasoning*, pages 371–443. Elsevier Science Publishers, 2001.

[Ohl02] Enno Ohlebusch. *Advanced Topics in Term Rewriting.* Springer-Verlag, April 2002.

[Plo72] G. Plotkin. Building-in equational theories. In D. Michie and B. Meltzer, editors, *Machine Intelligence.* Edinburgh University Press, 1972.

[PS81] Gerald E. Peterson and Mark E. Stickel. Complete sets of reductions for some equational theories. *J. ACM*, 28(2) :233–264, 1981.

[Rob65] J. A. Robinson. A machine-oriented logic based on the resolution principle. *J. ACM*, 12, 1965.

[RV95] Michaël Rusinowitch and Laurent Vigneron. Automated deduction with associative-commutative operators. *App. Algebra Eng. Commun. Comput.*, 6 :23–56, 1995.

[Sch78] Thomas J. Schaefer. The complexity of satisfiability problems. In *STOC '78 : Proceedings of the tenth annual ACM symposium on Theory of computing*, pages 216–226, New York, NY, USA, 1978. ACM Press.

[Sco64] W.R. Scott. *Group Theory*. Dover Publications, Inc., Mineola, N.Y., 1964.

[Ser03] A. Seress. *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2003.

[Sie79] Jörg H. Siekmann. Unification of commutative terms. In Edward W. Ng, editor, *EUROSAM*, volume 72 of *Lecture Notes in Computer Science*, pages 530–545. Springer-Verlag, 1979.

[Sim70] C. C. Sims. Computational methods in the study of permutation groups. In J. Leech, editor, *Computational problems in abstract algebra*, Proc. Conf. Oxford 1967, pages 169–183, London, 1970. Pergamon.

[Sim71] Charles C. Sims. Computation with permutation groups. In *SYMSAC '71 : Proceedings of the second ACM symposium on Symbolic and algebraic manipulation*, pages 23–28, New York, NY, USA, 1971. ACM Press.

[Sim94] C. C. Sims. *Computation with finitely presented groups*, volume 48 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1994.

[Sla74] James R. Slagle. Automated theorem-proving for theories with simplifiers commutativity, and associativity. *J. ACM*, 21(4) :622–642, 1974.

[Smu63] Raymond M. Smullyan. A unifying principle in quantification theory. *Proceedings of the National Academy of Sciences of the U.S.A.*, 49(6) :828–832, 1963.

[SP98] Uwe Schöning and Randall Pruim. *Gems of Theoretical Computer Science*. Springer-Verlag, 1998.

[SS87] Manfred Schmidt-Schauss. Unification under associativity and idempotence is of type nullary. *J. Autom. Reason.*, 2(3) :277–281, 1987.

[SS88] Manfred Schmidt-Schauß. Solution to problems p140 and p141. *Bulletin of the EATCS*, 34 :274–275, 1988.

[Sti81] Mark E. Stickel. A unification algorithm for associative-commutative functions. *Journal of the ACM*, 28(2) :423–434, April 1981.

[Tau97] Patrice Tauvel. *Mathématiques générales pour l'agrégation*. Masson, 1997.

[WOLB92] Larry Wos, Ross Overbeek, Ewing Lusk, and Jim Boyle. *Automated reasoning (2nd ed.) : introduction and applications*. Mc Graw-Hill, Inc., 1992.

Index