Langages reconnaissables de mots indexés par des ordinaux

Nicolas Bedon

Thèse de Doctorat

Spécialité : Informatique Fondamentale

présentée par

Nicolas Bedon

pour l'obtention du titre de

Docteur de l'Université de Marne-La-Vallée

sur le sujet

Langages reconnaissables de mots indexés par des ordinaux

Soutenue le jeudi 15 janvier 1998 devant le jury composé de :

Danièle Beauquier
Jean Berstel
Olivier Carton
Pavel Goralcik
Serge Grigorieff
Dominique Perrin
Antoine Petit
Jean-Eric Pin

À mes grand-parents

Remerciements

Je remercie

- Dominique Perrin, mon directeur, pour m'avoir permis de travailler sur un sujet aussi riche et original, pour ses encouragements incessants et son enthousiasme,
- Serge Grigorieff et Antoine Petit pour avoir accepté la lourde tâche de rapporteur,
- Danièle Beauquier, Jean Berstel, Olivier Carton, Pavel Goralcik et Jean-Eric Pin pour m'avoir fait l'honneur de participer au jury.

Je remercie Olivier Carton pour son aide technique tout au long de cette thèse, particulièrement dans les ω_1-semigroupes. Je le remercie aussi pour son fervent engouement pour mon sujet ces six derniers mois, et la relecture de ce document.

Je voudrais exprimer ma gratitude envers tous les enseignants qui font leur métier avec passion. Mes pensées se tournent particulièrement (et égoïstement) vers les informaticiens qui ont satisfait ma curiosité.

```
        DOSSEG
        .MODEL  small
        .STACK  200h
        .DATA
Message         DB      'Nsjmtjgsbjjo',21h,22h,'tfdunpo',21h,'f',21h,'df'
FinMessage      DB      0

        .CODE
DebutProg       PROC    NEAR
        mov     ax,@data
        mov     ds,ax
        mov     bx,OFFSET Message
        mov     ax,OFFSET FinMessage
        dec     ax
        call    ImprimeChaine
        mov     ah,4ch                  ; Fin de programme DOS
        int     21H
DebutProg       ENDP

ImprimeChaine   PROC    NEAR
BoucleImprimeChaine:
        cmp     bx,ax
        jge     FinBoucleImprimeChaine
        mov     dl,[bx]
        call    ImprimePredChar
        xchg    ax,bx
        mov     dl,[bx]
        xchg    ax,bx
        call    ImprimePredChar
        inc     bx
        dec     ax
        jmp     BoucleImprimeChaine
FinBoucleImprimeChaine:
        jne     FinImprimeChaine
        mov     dl,[bx]
        call    ImprimePredChar
FinImprimeChaine:
        ret
ImprimeChaine   ENDP

ImprimePredChar     PROC    NEAR
ImprimePredChar:
        push    ax
        dec     dx
        mov     ah,2                    ; Fonction d'affichage DOS
        int     21h
        pop     ax
        ret
ImprimePredChar ENDP

END     DebutProg
```

Enfin, je remercie tous ceux qui m'ont apporté leur soutien et leur amitié. En particulier, je demande pardon à ceux qui ont supporté mes absences, de corps et d'esprit, durant la préparation de cette thèse. Je n'en ferais plus d'autre, promis.

Résumé

Cette thèse traite des langages reconnaissables de mots indexés par des ordinaux.

Plusieurs classes d'automates qui reconnaissent de tels mots ont été introduites par Büchi. Elles diffèrent par la longueur des mots reconnus par les automates. Nous en utilisons quatre : la classe pour les mots de longueur ω, celle pour les mots de longueur inférieure à ω^{n+1}, où n est un entier naturel, celle pour les mots de longueur dénombrable, et celle pour les mots de longueur quelconque. Nous y ajoutons la classe des automates de Kleene traditionnelle, sur les mots finis. Nous remontrons que ces différentes définitions d'automates sont équivalentes, c'est-à-dire que données deux de ces classes et un automate d'une des deux, la restriction du langage reconnu par l'automate aux mots du domaine le plus petit des deux classes est la restriction du langage reconnu par un automate de l'autre classe au même domaine. Nous donnons également une présentation unifiée de la déterminisation pour chacune des classes qui reconnaît au plus des mots de longueur dénombrable.

Les semigroupes finis sont un formalisme équivalent aux automates pour définir des ensembles de mots finis. Perrin, Pin et Wilke ont introduits des structures algébriques adaptées à l'étude des langages de mots de longueur ω, qui, quand elles sont finies, sont équivalentes aux automates. Nous généralisons l'approche algébrique de la théorie des langages reconnaissables de mots de longueur ω aux mots de longueur inférieure à ω^{n+1}, puis aux mots de longueur dénombrable. Pour cela, nous définissons deux structures algébriques, les ω^n-semigroupes et les ω_1-semigroupes, qui, quand elles sont finies, sont équivalentes respectivement aux automates pour les mots de longueur inférieure à ω^{n+1} et aux automates pour les mots de longueur dénombrable. Comme pour le cas des mots de longueur ω, une algèbre syntaxique peut être canoniquement associée à chaque langage reconnaissable. Nous définissons le produit de Schützenberger et le produit en couronne sur les ω_1-semigroupes. Nous étendons également le théorème des variétés d'Eilenberg aux mots de longueur dénombrable.

Finalement, nous remontrons l'équivalence entre langages reconnus par automates et langages définis par énoncés de logique monadique du second ordre quand on s'intéresse aux mots de longueur dénombrable. Le théorème d'équivalence de Schützenberger entre langages sans étoile et semigroupes finis apériodiques est étendu aux mots de longueur inférieure à ω^{n+1}, et le théorème d'équivalence entre langages sans étoile et langages définis par énoncés de logique du premier ordre de l'ordre linéaire de McNaughton et Papert est étendu aux mots de longueur quelconque.

Abstract

This thesis treats of recognizable languages of words indexed by ordinals.

Several classes of automata recognizing such words have been introduced by Büchi. Those classes differ by the length of words recognized by automata. We use four of them : the class for words of length ω, the one for words of length less than ω^{n+1}, where n is an integer, the class for words of denumerable length and the one for words of any length. We also use the usual Kleene automata, on words of finite length. We give another proof of the equivalence of those different definitions of automata : by choosing an automaton in one class, one can construct an automaton of an other class such that the restrictions of languages accepted by both automata to the smallest domain of both classes are identical. We also give an unified presentation for the determinisation of each class of automata whose domain is words of length at most denumerable.

Finite semigroups are another formalism equivalent to automata to define sets of finite words. Perrin, Pin and Wilke have introduced algebraic structures adapted to the study of languages of words of length ω. These structures are equivalent to automata when they are finite. We generalize the algebraic approach of the theory of recognizable languages of words of length ω to words of length less than ω^{n+1}, and to words of denumerable length : we define two algebraic structures, called ω^n-semigroups and ω_1-semigroups, equivalent, when they are finite, to automata respectively on words of length less than ω^{n+1} and of denumerable length. As for the case of words of length ω, a finite algebra can be canonically associated to any recognizable language. We define the Schützenberger and wreath products on ω_1-semigroups. We also extend the Eilenberg theorem of variety to words of denumerable length.

Finally, we give another proof of Büchi's theorem which establishes the equivalence between languages recognized by automata and languages defined by sentences of monadic second order logic for words of denumerable length. We extend the Schützenberger's theorem of equivalence between star-free languages and languages recognized by aperiodic finite semigroups to words of length less than ω^{n+1}, and McNaughton and Papert's theorem of equivalence between star-free languages and languages defined by sentences of first order logic of the linear ordering to words of any length.

Introduction

Cette thèse s'inscrit dans le cadre général de la théorie des langages reconnaissables par automates et semigroupes, et de la logique.

Globalement, les objectifs sont

- d'exposer les résultats principaux qui concernent la théorie des langages reconnaissables de mots indexés par des ordinaux par automates, en particulier de donner une présentation unifiée des algorithmes de déterminisation et de complémentation,
- d'amorcer l'extension des résultats obtenus sur les langages de mots finis et de longueur ω grâce à l'approche algébrique aux mots d'ordinalité supérieure.

La théorie des automates sur les mots finis est apparue au milieu des années 50. La motivation principale était alors la conception de machines sur le modèle du cerveau humain. Les automates sont aujourd'hui des objets au cœur de l'informatique : ils modélisent le comportement des machines séquentielles, et trouvent de nombreuses applications dans la manipulation des textes et la théorie des codes, entres autres. Dans l'article [Kle56] à l'origine de la théorie, Kleene établit l'équivalence entre les langages reconnus par automates et les langages rationnels. Ce résultat est connu sous le nom de "théorème de Kleene". Parallèlement, Schützenberger [Sch56] présente "une théorie algébrique du codage", et initie ainsi la théorie des langages reconnus par semigroupes finis. Les deux modes de reconnaissance, par automate et semigroupe fini, sont équivalents. De plus, dans chacun des deux formalismes un objet canonique peut être associé à tout langage reconnaissable L : l'automate minimal de L et le semigroupe syntaxique de L. L'automate minimal de L a la propriété intéressante d'être déterministe, ce qui montre en particulier que la classe des langages rationnels est fermée par complémentation. Cependant, de nombreuses opérations se font naturellement sur les semigroupes et pas sur les automates : ainsi, les langages reconnaissables (indifféremment par automate ou semigroupe fini) sont classifiables par les propriétés algébriques de leur semigroupe syntaxique. Un premier pas important a été fait dans cette direction par Schützenberger [Sch65] : il établit la correspondance entre les langages sans étoile et les langages reconnaissables dont le semigroupe syntaxique est apériodique, c'est-à-dire ne contient pas de groupe non triviaux. Cette idée est développée par Eilenberg [Eil76] dans son théorème des variétés.

Très tôt, Büchi utilise les automates sur les mots finis pour décider de la validité des énoncés de logique monadique du second ordre faible du successeur [Büc60]. Il établit pour cela l'équivalence entre automates et les énoncés de cette logique : un langage est reconnaissable si et seulement si on peut le définir par un énoncé de cette logique. McNaughton et Papert montrent dans [MP71] que les langages définis en restreignant cette logique au premier ordre sont exactement les sans étoile. L'extension du résultat de Büchi à la logique monadique du second ordre du successeur conduit naturellement Büchi à considérer des mots infinis (de longueur ω, dont les lettres sont indicées par tous les entiers naturels), et à définir des ensembles de tels mots avec des automates [Büc62]. Il est en particulier amené à prouver que la classe des langages reconnus par ses automates est fermée par complémentation, mais contrairement à ce qui se passe pour les mots finis, on ne sait pas associer d'automate de façon canonique à tout langage reconnaissable, et de plus chaque langage reconnaissable ne l'est pas forcément par un automate déterministe.

Muller, motivé par l'étude de la synchronisation de circuits électroniques, et indépendamment de Büchi, définit également des automates qui reconnaissent des mots de longueur ω [Mul63]. Contrairement à ceux de Büchi, ses automates sont déterministes.

L'équivalence des deux définitions est prouvée par McNaughton [McN66] en 1966. Il donne dans sa preuve un algorithme qui permet de construire un automate de Muller équivalent à un automate de Büchi. Cet algorithme de déterminisation d'automates sur les mots infinis a fait depuis l'objet de nombreuses investigations : en particulier, il a été simplifié par Choueka [Cho74], et redémontré par Safra [Saf88], qui diminue sa complexité d'une exponentielle double du nombre d'états de l'automate de départ à une exponentielle simple. Dans son article, McNaughton étend la notion de langage rationnel aux mots de longueur ω. Il y montre l'analogue du théorème de Kleene, à savoir la correspondance entre langages reconnus par automates et langages rationnels de mots de longueur ω.

En pratique, les automates qui reconnaissent des mots de longueur ω interviennent notamment dans la modélisation des machines séquentielles qui sont censées ne jamais s'arrêter, comme par exemple les systèmes d'exploitation et les réseaux, et dans l'étude de la synchronisation de machines séquentielles, ce qui était la motivation initiale de Muller.

Le logicien Büchi s'intéresse naturellement à l'extension de ses résultats aux ordinaux [Büc65, Büc64, BS73]. Il définit trois classes d'automates. La première est une extension naturelle des automates de Muller. Ces automates, les n-automates, sont déterministes. Ils reconnaissent des mots dont la longueur est inférieure à ω^{n+1}, où n est un entier fixé. Choueka en fera une étude systématique [Cho78], et en particulier étendra le théorème de Kleene aux langages de mots de longueur inférieure à ω^{n+1}. Avec la seconde classe d'automates, les D-automates, Büchi s'intéresse aux mots de longueur dénombrable. Il montre que cette classe d'automates est déterministe et que les langages qu'ils reconnaissent sont exactement ceux définissables par des énoncés de logique monadique du second ordre de l'ordre linéaire. En en changeant un peu la définition, il définit la troisième classe d'automates, dont la classe des langages reconnus n'est pas close par complémentation. Le théorème de Kleene est étendu aux langages de mots reconnus par D-automates par Wojciechowski dans [Woj83, Woj85].

Les ordinaux sont un modèle particulier du temps, où on suppose qu'une infinité d'actions peuvent être exécutées séquentiellement avant certains temps particuliers, ou bien encore qu'une infinité d'actions peuvent être réalisées dans un intervalle de temps fini. Les automates qui reconnaissent des mots dont les lettres sont indexées par des ordinaux sont donc appliqués aux modélisations de machines séquentielles dans lesquels une telle notion du temps est nécessaire.

La richesse des résultats obtenus en utilisant la présentation algébrique des langages reconnaissables de mots finis est telle que la recherche d'une algèbre adaptée à l'étude des langages reconnaissables de mots infinis est naturelle. Un premier pas dans cette direction pour les mots de longueur inférieure ou égale à ω est fait par Pécuchet [Péc86a, Péc86b], mais une approche plus satisfaisante est dûe à Wilke [Wil93], Perrin et Pin [PP97]. Grossièrement, l'algèbre définie, nommée ω-semigroupe, est un semigroupe dans lequel des produits de ω éléments sont autorisés. Comme dans le cas des mots finis, un ω-semigroupe particulier, l'ω-semigroupe syntaxique de L, peut être canoniquement associé à tout langage reconnaissable L. En théorie des langages reconnaissables de mots de longueur inférieure ou égale à ω, il y a donc un avantage important à utiliser les ω-semigroupes plutôt que les automates, puisqu'on ne sait pas associer d'automate de façon canonique à tout langage reconnaissable. Le théorème d'Eilenberg est étendu aux mots de longueur inférieure à ω par Wilke, le résultat de Schützenberger sur les sans étoile par Perrin [Per84] et celui de McNaughton et Papert par Ladner [Lad77] et Thomas [Tho79].

Les principaux résultats de cette thèse sont :
- une nouvelle preuve de l'équivalence entre les différentes classes d'automates,
- un nouvel algorithme de déterminisation des automates sur les mots dénombrables,
- l'introduction de deux structures algébriques équivalentes respectivement aux n-automates et D-automates (quand elles sont finies),
- l'extension du théorème de Schützenberger aux mots de mots de longueur inférieure à ω^{n+1},
- l'extension du théorème d'équivalence entre logique du premier ordre et langages sans étoile, indépendamment de la longueur des mots considérés,
- l'extension du théorème des variétés d'Eilenberg aux mots de longueur dénombrables.

Elle est composée de quatre chapitres.
- Dans le premier chapitre nous donnons les définitions élémentaires sur les ensembles, faisons une présentation rapide des nombres ordinaux en énonçant les résultats que nous utiliserons, et construisons des mots dont les lettres sont indexées par des nombres ordinaux.
- Le second chapitre est consacré aux automates. Nous y présentons les différentes définitions pour les automates et les principaux résultats, en particulier l'équivalence entre langages reconnus et langages rationnels, en procédant par longueur croissante des longueurs des mots considérés. Nous montrons l'équivalence entre ces différentes classes d'automates, sous hypothèse bien entendu de restriction de la longueur des mots considérés. Cette équivalence est utilisée pour, donnés un automate qui reconnaît des mots de longueur quelconque et un entier n, construire un automate

déterministe de cette même classe qui reconnaît exactement les mots de longueur inférieure à ω^{n+1} reconnus par le premier.

- Dans le troisième chapitre nous définissons des outils algébriques pour l'étude des langages reconnaissables de mots de longueur au plus dénombrable. Comme dans le chapitre précédent, nous procédons par longueur croissante des mots considérés. Nous commençons par rappeler les définitions et résultats sur les mots finis, puis de longueur ω. Ensuite nous introduisons les ω^n-semigroupes, une extension des ω-semigroupes, et nous montrons qu'ils sont utilisables pour définir des langages de mots de longueur inférieure à ω^{n+1} de façon équivalente aux n-automates. Nous prouvons qu'un ω^n-semigroupe peut être canoniquement associé à tout langage reconnaissable de mots de longueur inférieure à ω^{n+1}. La définition compliquée des ω^n-semigroupes en font des objets difficilement manipulables. Considérer des mots de longueur dénombrable quelconque nous amène à introduire une définition d'un objet algébrique plus général, et également plus simple que les ω^n-semigroupes : les ω_1-semigroupes. Nous prouvons que les ω_1-semigroupes finis sont équivalents aux D-automates. La preuve fournit en particulier un algorithme de déterminisation des D-automates. Nous montrons également qu'un ω_1-semigroupe peut canoniquement être associé à tout langage reconnaissable. Ensuite, nous étendons deux opérations très utilisées sur les semigroupes aux ω_1-semigroupes : le produit de Schützenberger et le produit en couronne. Finalement, nous généralisons la classification des langages reconnaissables de mots finis d'Eilenberg aux mots de longueur dénombrable.
- Le dernier chapitre est consacré à la logique. Nous y remontrons l'équivalence entre les D-automates et les énoncés de la logique monadique du second ordre de l'ordre linéaire. Nous prouvons ensuite que les langages sans étoile sont exactement ceux définissables par des énoncés de logique du premier ordre, et qu'un langage reconnaissable de mots de longueur inférieure à ω^{n+1} est sans étoile si et seulement si son ω^n-semigroupe syntaxique est apériodique. Les jeux d'Ehrenfeucht-Fraïssé fournissent l'argument central de cette extension des résultats de Schützenberger, McNaughton et Papert sur les mots finis aux mots de longueur inférieure à ω^{n+1}.

Tous les résultats présentés dans cette thèse sont effectifs.

Chapitre 1

Notations, terminologie et définitions de base

Nous introduisons ici les définitions et notations élémentaires qui serviront dans les autres chapitres. Nous commençons par les ensembles, suivis des nombres cardinaux, puis des nombres ordinaux, et terminons en construisant des mots dont les lettres sont indexés par des ordinaux.

1.1 Ensembles

1.1.1 Définitions de base

Une **collection** E est un groupement d'objets appelés les **éléments** de E. Si tous les éléments de E sont distincts, E est un **ensemble**. Comme il n'existe pas d'ensemble de tout les ensembles, nous parlerons de **classe** pour désigner un groupement d'éléments distincts ; par exemple, la classe de tout les ensembles. On s'autorise les mêmes opérations sur les classes que sur les ensembles. L'ensemble vide $\emptyset$ est l'unique ensemble qui ne contient rien. On note $e \in E$, et on dit que e appartient à E ou que e est dans E, si e est un élément de E. Un ensemble E' est un **sous-ensemble** de E, ou **partie** de E, si chaque élément de E' est aussi dans E. On note alors $E' \subseteq E$. Pour tout ensemble E, on a $\emptyset \subseteq E$ et $E \subseteq E$. S'il existe un élément de E qui n'est pas dans E' on note $E' \subset E$ et on dit que E' est une partie propre de E ; si chaque élément d'un des deux ensembles est aussi dans l'autre E et E' sont égaux ($E = E'$).

Soit E un ensemble, n et m deux entiers naturels tels que $m \leq n$. On note $[E]$ l'ensemble des parties de E privé de l'ensemble vide, et on pose $[E]^0 = E$, $[E]^{n+1} = [[E]^n]$ et $[E]^n_m = \cup_{i=m\dots n}[E]^i$. Le **type** $t(e)$ d'un élément e de $[E]^n_m$ est l'unique entier k tel que $e \in [E]^k$.

Les ensembles seront notés par des lettres majuscules, à moins qu'il ne s'agisse d'ensembles particuliers. L'ensemble des entiers naturels est noté par $\mathbb{N}$. On écrit $\mathbb{N}^*$ quand on le prive de 0.

1.1.2 Opérations booléennes

Soit E une collection d'ensembles. L'**union** des éléments de E, notée $\cup_{E' \in E} E'$, est l'unique ensemble constitué de tous les éléments des ensembles qui forment E. L'**intersection** des éléments de E, notée $\cap_{E' \in E} E'$, est l'unique ensemble constitué de tous les objets qui sont dans chacun des éléments de E. Deux ensembles sont **disjoints** si leur intersection est vide. Si E ne contient que deux ensembles E_1 et E_2, on note $E_1 \cup E_2$ (resp. $E_1 \cap E_2$) plutôt que $\cup_{E' \in E} E'$ (resp. $\cap_{E' \in E} E'$). Soient E et E' deux ensembles. La **différence** de E et de E', notée $E - E'$, est l'ensemble des éléments de E qui ne sont pas dans E'. Si $E' \subseteq E$ le **complément** de E' dans E, ou par rapport à E, est l'ensemble $E - E'$, qu'on note également $\overline{E'}^E$, ou plus simplement $\overline{E'}$ quand il est implicite que la complémentation est dans E.

1.1.3 Produit cartésien, projection

Soient $n \in \mathbb{N}^*$, $i \in 1 \ldots n$ et $e = (e_1, \ldots, e_n)$ un n-uplet. On définit la **projection** π_i de e sur sa $i^{ème}$ composante par $\pi_i(e) = e_i$. Par extension, si E est un ensemble de n-uplets, on pose $\pi_i(E) = \{e_i : e_i = \pi_i(e) \text{ pour un } e \in E\}$.

Soient maintenant n ensembles $E_1, \ldots, E_n$. Le **produit cartésien**, ou plus simplement produit, de $E_1, \ldots, E_n$, est l'ensemble

$$E_1 \times \cdots \times E_n = \prod_{i=1 \ldots n} E_i = \{(e_1, \ldots, e_n) : e_i \in E_i \text{ pour } i \in 1 \ldots n\}$$

On a bien entendu $\pi_i(\prod_{i=1\ldots n} E_i) = E_i$. Finalement, si E est un ensemble, on note E^n l'ensemble $\prod_{i=1\ldots n} E$.

1.2 Fonctions, relations

Une **relation** dans E est un sous ensemble de $E \times E$.

On dit qu'une relation R est une **relation d'ordre** sur E si elle vérifie, quels que soient $e_1, e_2, e_3 \in E$:
- $e_1 R e_1$ (**réflexivité**),
- $(e_1 R e_2$ et $e_2 R e_1) \Rightarrow e_1 = e_2$ (**antisymétrie**),
- $(e_1 R e_2$ et $e_2 R e_3) \Rightarrow e_1 R e_3$ (**transitivité**).

En général R est plutôt notée $\leq$. L'ordre $\leq$ est **total** si on a $e_1 \leq e_2$ ou $e_2 \leq e_1$ quels que soient $e_1, e_2 \in E$, **partiel** sinon. La relation obtenue en supprimant la réflexivité à une relation d'ordre $\leq$ est notée $<$. Inversement, à partir d'une relation $<$ antisymétrique et transitive on peut toujours construire une unique relation d'ordre $\leq$ en ajoutant la réflexivité. Par abus de langage, nous dirons que $<$ est un ordre.

Soient E et F deux ensembles, g un sous-ensemble de $E \times F$. On dit que g est une **fonction** (resp. une **application**) de E vers F, si pour tout $e \in E$ il existe au plus (resp.

exactement) un unique $f \in F$ tel que $(e,f) \in g$. L'unique élément f associé à e est appelé l'**image** de e dans F et est noté $g(e)$. Par extension, si $E' \subseteq E$, on pose $g(E') = \cup_{e \in E'} g(e)$. On dit que E est le **domaine** de g, et que F est son **codomaine**, et on note $g : E \to F$. On pose également $g^{-1}(f) = \{e \in E : g(e) = f\}$, et si $F' \subseteq F$, $g^{-1}(F') = \cup_{f \in F'} g^{-1}(f)$.

La fonction g est **injective** si $g(e) = g(e')$ implique $e = e'$ pour $e, e' \in E$. Elle est **surjective** si tout élément de F est l'image par g d'un élément de E au moins. Elle est **bijective** si elle est à la fois injective et surjective.

Une opération d'arité n sur un ensemble E est une fonction $E^n \to E$. L'arité d'une opération f est dénotée par $\theta(f)$. Une opération binaire f est commutative si $f(e,e') = f(e',e)$ et **associative** si $f(e, f(e', e'')) = f(f(e,e'), e'')$ quels que soient $e, e', e'' \in E$. S'il existe $e \in E$ tel que $f(e,e') = f(e',e) = e'$ quel que soit $e' \in E$ alors f possède un **élément neutre** e. De même, s'il existe $e \in E$ tel que $f(e,e') = f(e',e) = e$ quel que soit $e' \in E$ alors f possède un **zéro** e. En général, nous écrirons efe' plutôt que $f(e,e')$.

Soient E, E' et E'' trois ensembles, et $f : E \to E'$, $g : E' \to E''$ deux fonctions. La **fonction composée** de f et g, notée gf, est la fonction $E \to E''$ définie par $gf(e) = e''$ si et seulement si il existe $e' \in E'$ tel que $f(e) = e'$ et $g(e') = e''$.

Soient $n, m \in \mathbb{N}$. Un **type algébrique** C est une classe d'ensembles tous munis d'ordres $\leq_1, \ldots, \leq_n$ et d'opérations $f_1, \ldots, f_m$. Un élément de C est une **algèbre** de type C. Un **morphisme** d'éléments de C est une application d'un élément de C dans un autre qui préserve ordres et opérations : si $E, E' \in C$, que φ est un morphisme d'éléments de C de E vers E', que $\leq_i^E$ $(i = 1 \ldots n)$ et f_j^E $(j = 1 \ldots m)$ désignent respectivement les n ordres sur E et m opérations sur E, on a

$$\varphi(f_j^E(e_1, \ldots, e_{\theta(f_j^E)})) = f_j^{E'}(\varphi(e_1), \ldots, \varphi(e_{\theta(f_j^E)}))$$

et $e \leq_i^E e'$ si et seulement si $\varphi(e) \leq_i^{E'} \varphi(e')$ pour tout $i \in 1 \ldots n$, $j \in 1 \ldots m$ et $e, e', e_1, \ldots, e_{\theta(f_j^E)} \in E$. On dit que E' est une **sous-algèbre** d'un élément E de C s'il existe un morphisme injectif de E' dans E. Soient E et E' deux éléments de C, $X \subseteq E$ et $\varphi : E \to E'$ un morphisme. Alors φ **reconnaît** X si $\varphi^{-1}(\varphi(X)) = X$. De même, on dit que E' reconnaît X s'il existe un morphisme $\varphi : E \to E'$ qui reconnaît X. Une partie X de E est **reconnaissable** s'il existe un élément fini E' de C qui reconnaît X. De deux éléments E et E' de C on dit que E' est **quotient** de E s'il existe un morphisme surjectif de E vers E'. De deux éléments E et E' de C on dit que E **divise** E', et on note $E < E'$ si E est quotient d'une sous-algèbre de E'. Cette relation de division est transitive. Un **isomorphisme** est un morphisme bijectif. Deux éléments de C sont **isomorphes** s'il existe un isomorphisme de l'un vers l'autre. La relation "être isomorphe à" est une relation d'équivalence sur C. Nous identifierons souvent deux éléments de C identiques. Comme E est implicite dans les notations $e \leq_j^E e'$ et $ef_i^E e'$ nous écrirons plutôt $e \leq_j e'$ et $ef_i e'$ pour alléger les notations. Les morphismes seront généralement notés par les lettres grecques φ et ψ. Si $n = 0$, $j \in \mathbb{N}$ et $(E_i)_{i<j}$ est une famille d'éléments de C, le **produit direct fini** $E' = \prod_{i<j} E_i$, également noté $E_1 \times \cdots \times E_{j-1}$, est l'ensemble muni des m opérations définies par

$$f_k^{E'}(e_1, \ldots, e_{\theta(f_k^{E'})})(i) = f_k^{E_i}(e_1(i), \ldots, e_{\theta(f_k^{E_i})}(i))$$

pour $k = 1 \dots m$. Une **pseudo-variété** est une classe d'algèbres finies fermée par quotient, sous-algèbre et produit direct fini.

Une relation R réflexive, transitive et **symétrique** (i.e. $e_1 R e_2 \Rightarrow e_2 R e_1$) dans E est une **relation d'équivalence**. Si $e \in E$, la **classe d'équivalence** de e pour R est la partie de E qui contient seulement tout les éléments $e' \in E$ tels que eRe'. L'**index** d'une relation d'équivalence est le nombre de ses classes d'équivalences. Soient $m \in \mathbb{N}$ et C une classe d'ensembles tous munis d'opérations $f_1, \dots, f_m$. Une **congruence** $\sim$ d'éléments de C est une relation d'équivalence sur les éléments des éléments de C qui préserve les opérations : si $E \in C$, alors

$$e_j \sim e'_j \ (j = 1 \dots \theta(f_i)) \Rightarrow f_i(e_1, \dots, e_{\theta(f_i)}) \sim f_i(e'_1, \dots, e'_{\theta(f_i)})$$

pour tout $e_1, \dots, e_{\theta(f_i)} \in E$ et $i \in 1 \dots m$. Cette condition entraîne que l'ensemble des classes d'équivalence de E, noté $E/\sim$ et appelé **quotient** de E par $\sim$, est un élément de C, et que l'application qui a un élément de E fait correspondre sa classe d'équivalence est un morphisme surjectif de E dans $E/\sim$. De deux congruences $\sim$ et $\sim'$ sur E on dit que $\sim$ est plus fine que $\sim'$ si $e \sim e' \Rightarrow e \sim' e'$ pour tout $e, e' \in E$. Soient $n, m \in \mathbb{N}$ et C une classe d'ensembles tous munis d'ordres $\leq_1, \dots, \leq_n$ et d'opérations $f_1, \dots, f_m$. Soit également $\varphi : E \to E'$ un morphisme d'éléments de C. Nous utiliserons souvent la congruence $\sim_\varphi$ définie sur E par $e \sim_\varphi e'$ si et seulement si $\varphi(e) = \varphi(e')$, appelée **congruence nucléaire** associée à φ.

Dans cette section nous n'avons traité que les cas des fonctions dont l'arité est un entier naturel. Nous nous autoriserons les fonctions dont l'arité est un ordinal une fois les ordinaux introduits (section 1.4). Les définitions de cette section s'étendent alors naturellement.

1.3 Cardinaux

Un (nombre) **cardinal** est une extension de la notion de nombre usuel, qu'on associe aux ensembles une fois fait abstraction des notions d'ordre et de qualité des éléments. Le cardinal d'un ensemble E est noté $|E|$.

On dit que deux ensembles E et F ont même cardinal, et on note $|E| = |F|$ s'il existe une bijection de l'un dans l'autre, $|E| < |F|$ si E a même cardinal qu'un sous-ensemble de F sans que F ait même cardinal qu'un sous-ensemble de E.

La preuve du théorème suivant nécessite l'utilisation du théorème de bon ordonnance, que nous énoncerons plus tard (théorème 1.4.3, page 11) :

Théorème 1.3.1 *Soient E et F deux ensembles. Alors une et une seule des trois relations suivantes est vraie :*

– $|E| < |F|$ – $|E| = |F|$ – $|E| > |F|$

La relation $\leq$ obtenue en posant $x \leq y$ si et seulement si $x < y$ ou $x = y$ est un ordre total sur les nombres cardinaux.

Un ensemble est **infini** s'il existe une bijection entre lui-même et une de ses parties propre. Un ensemble qui n'est pas infini est **fini**.

Exemple 1.3.2 *L'ensemble* $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ *des entiers naturels est infini, puisque l'application* $x \to x + 1$ *de* $\mathbb{N}$ *dans* $\mathbb{N}^*$ *est bijective.*

Le **cardinal** d'un ensemble fini est le nombre de ses éléments. L'ordre $\leq$ sur les cardinaux d'ensembles finis coïncide avec celui sur les entiers naturels.

Le théorème suivant montre que deux ensembles infinis ne sont pas forcément de cardinaux identiques, et plus généralement qu'il existe une infinité de cardinaux d'ensembles infinis.

Théorème 1.3.3 (Cantor) *Soit* E *un ensemble ; alors* $|E| < |[E]|$.

Preuve La preuve utilise l'argument diagonal de Cantor : supposons d'abord que $|E| = |[E]|$. Il existe alors une bijection $g : E \to [E]$. Soit $P = \{e \in E : e \notin g(e)\}$. On a $P \in [E]$. Comme g est bijective, il existe un unique élément e de E tel que $g(e) = P$. Si $e \in P$ alors $e \notin g(e)$. De même, si $e \notin P$, alors $e \in g(e)$. Comme $g(e) = P$ on a une contradiction, donc g ne peux pas être une bijection, et donc nécessairement $|E| \neq |[E]|$. On montre en utilisant le même argument qu'on ne peut avoir $|E| > |[E]|$. Donc $|E| < |[E]|$. ∇

Le plus petit cardinal infini est $|\mathbb{N}|$, qu'on note $\aleph_0$. Les ensembles de cardinal inférieur ou égal à $\aleph_0$ sont dits **dénombrables**, ou encore **énumérables**. Les ensembles qui ne sont pas dénombrables sont **indénombrables**. Le premier nombre cardinal plus grand que $\aleph_0$ est noté $\aleph_1$. Les seuls cardinaux que nous utiliserons par la suite sont ceux des ensembles finis (les entiers naturels), $\aleph_0$ et $\aleph_1$. Si on les énumère de façon à respecter l'ordre $\leq$, cet ensemble est $\{0, 1, 2, 3, 4, \dots, \aleph_0, \aleph_1\}$, et son cardinal est $\aleph_0$: la bijection entre cet ensemble et $\mathbb{N}$ consiste à faire correspondre $\aleph_0$ à 0, $\aleph_1$ à 1, 0 à 2, 1 à 3,....

Théorème 1.3.4 *L'union dénombrable d'ensembles dénombrables est encore un ensemble dénombrable.*

1.4 Ordinaux

Nous donnons ici les définitions et principales propriétés relatives à l'arithmétique des ordinaux. L'objet de cette section n'est pas de refaire la théorie des ordinaux, mais d'en présenter les grandes lignes afin de familiariser le lecteur avec. Pour plus de détails, on se référera à [Sie50, Sie65] et à [Ros82]. On trouvera dans [Ros82] une bibliographie complète sur les ordinaux.

Au $IV^{ième}$ siècle avant notre ère, Aristote distingue deux sortes d'infini pour se débarasser des paradoxes introduits par les quantités infinies connues à l'époque :
- l'**infini actuel**, qui existe à un instant dans le temps : c'est l'infini selon lequel le temps, l'espace et la matière sont infiniment divisibles,
- l'**infini potentiel**, dont l'infinitude ne s'exprime que dans la durée : c'est l'infini selon lequel le temps s'écoule infiniment.

C'est seulement à la fin du $XIX^{ième}$ siècle que Cantor développe une théorie mathématique de l'infini actuel, en même temps que la théorie des ensembles : c'est la théorie des ordinaux.

On dit qu'une relation $<$ est un **ordre linéaire** sur un ensemble E si elle vérifie les conditions suivantes quels que soient $e, e' \in E$:
- transitivité,
- si $e \neq e'$ alors ou bien $e < e'$ ou bien $e' < e$, mais pas les deux (asymétrie),
- $e \not< e$.

On dit que $<$ est un **bon ordre** si toute partie non vide de E a un plus petit élément.

Exemple 1.4.1 *L'ensemble des entiers relatifs est linéairement ordonné par son ordre habituel, mais pas bien ordonné. Par contre,* $\mathbb{N}$ *est bien ordonné par son ordre habituel. L'ensemble* $\{0, 1, 2, \ldots, a\}$*, qui contient exactement* $\mathbb{N}$ *et un élément supplémentaire* a*, muni de l'ordre de la lecture de la gauche vers la droite (le plus petit est à gauche), est bien ordonné.*

Un (nombre) **ordinal** est un représentant d'une classe d'équivalence de bons ordres pour la relation “être isomorphe à”. Nous noterons les ordinaux par des lettres grecques minuscules : α, β, γ,..., et la classe des ordinaux par *Ord* . On note 0 l'ordinal de la classe d'équivalence de $\emptyset$. Un ordinal est **successeur** s'il possède un plus grand élément. S'il n'est ni 0 ni successeur, alors il est **limite**. Nous utiliserons souvent la lettre ξ pour les ordinaux limites. La classe des ordinaux successeurs est dénotée par *Succ*, celle des limites par *Lim*. On a $Ord = \{0\} \cup Succ \cup Lim$. Dans la suite, on dira que deux ordinaux sont égaux s'ils sont isomorphes, et on supposera que deux ordinaux donnés sont toujours disjoints.

Nous ordonnons maintenant *Ord* en posant $\alpha < \beta$ si et seulement si $\alpha \neq \beta$ et α est isomorphe à une partie A de β telle que si $e \in A$, alors tout élément plus petit que e dans β est aussi dans A, et que les éléments de A conservent l'ordre qu'ils avaient dans β (A est alors bien ordonné).

Théorème 1.4.2 *Ord est bien ordonné par* $<$.

Un ordinal α peut alors être assimilé à l'ensemble bien ordonné de tous les ordinaux plus petits que lui, et on a

$$\beta < \alpha \iff \beta \in \alpha \iff \beta \subset \alpha$$

Le théorème suivant, qui est équivalent à l'axiome du choix, montre qu'à tout ensemble on peut associer un ordinal :

Théorème 1.4.3 (de bon ordonnance) *Tout ensemble peut être bien ordonné.*

Comme un ensemble et un ordinal associé ont nécessairement même cardinal, on ne peut associer qu'un ordinal à un ensemble fini :

Exemple 1.4.4 *Soit $E = \{e_1, e_2, e_3\}$. On peut bien ordonner E par $<_E$ en disant que $e_1 <_E e_2 <_E e_3$, ou bien encore par exemple que $e_2 <_E e_1 <_E e_3$. Ces deux ensembles bien ordonnés sont isomorphes.*

C'est par contre faux pour les ensembles infinis :

Exemple 1.4.5 *L'ensemble des entiers naturels muni de son ordre habituel est bien ordonné. Si on construit un autre bon ordre en disant que 0 est le plus grand des éléments de $\mathbb{N}$ et en gardant l'ordre classique pour les autres éléments, les deux ensembles bien ordonnés ne sont pas isomorphes, puisqu'un a un plus grand élément et l'autre pas.*

On note n l'ordinal associé aux ensembles finis de cardinal n, ω_0, ou plus simplement ω, le plus petit ordinal de cardinal $\aleph_0$, et ω_1 le plus petit ordinal de cardinal $\aleph_1$. Nous n'utiliserons que les ordinaux plus petits que ω_1 (c'est-à-dire, les ordinaux (de cardinal) dénombrables). Les ordinaux finis et les cardinaux finis peuvent être confondus avec les entiers naturels.

Nous définissons maintenant la **somme** de deux nombres ordinaux :

Définition 1.4.6 *Soient $\alpha, \beta \in Ord$ et $<_\alpha, <_\beta$ respectivement les bons ordres sur α et β. La somme $\alpha + \beta$ est l'ensemble $\gamma = \alpha \cup \beta$ muni de l'ordre $<_\gamma$ défini par $c <_\gamma c'$ si et seulement si une des trois conditions suivantes est vérifiée :*

- *$c \in \alpha$ et $c' \in \beta$*
- *$c, c' \in \alpha$ et $c <_\alpha c'$*
- *$c, c' \in \beta$ et $c <_\beta c'$*

Intuitivement, faire la somme de deux ordinaux α et β revient à les mettre bout-à-bout, les éléments de α avant ceux de β, en respectant les ordres de α et β.

Exemple 1.4.7 *On pose $\omega = \{0, 1, 2, \dots\}$ et $1 = \{a\}$, l'ordre étant celui de la lecture de la gauche vers la droite. L'ensemble $\omega + 1 = \{0, 1, 2, \dots, a\}$ a un plus grand élément a, donc $\omega + 1 \in Succ$. Par contre, $1 + \omega = \{a, 0, 1, 2, \dots\} = \omega$ n'en a pas (comme $1 + \omega \neq 0$, $1 + \omega \in Lim$). On a donc $\omega + 1 \neq 1 + \omega$ (ils ne sont pas isomorphes).*

L'exemple précédent montre que l'addition des ordinaux n'est pas commutative, par contre elle est associative. L'élément neutre pour l'addition est 0. La somme de deux ordinaux est également un ordinal : c'est un ensemble muni d'un ordre linéaire et si $E \subseteq \alpha + \beta$, alors $E = E_1 \cup E_2$ avec $E_1 \subseteq \alpha$ et $E_2 \subseteq \beta$. Comme par définition des ensembles bien ordonnés E_1 et E_2 ont tout deux des plus petits éléments (sous réserve qu'ils ne soient pas vides), E aussi (s'il n'est pas vide non plus).

La **soustraction** d'ordinaux est définie de la manière suivante :

Théorème 1.4.8 *Si $\alpha, \beta \in Ord$ et $\alpha > \beta$, il existe un unique ordinal $\gamma > 0$ tel que $\alpha = \beta + \gamma$. On dénotera cet ordinal par $\alpha - \beta$.*

Exemple 1.4.9 *On a les égalités :*

- $\omega - n = \omega$
- $\omega + n - \omega = n$

On peut redonner une définition des ordinaux successeur en se servant de l'addition : on dit qu'on ordinal α est successeur s'il existe $\beta \in Ord$ tel que $\alpha = \beta + 1$.

On généralise maintenant l'addition aux ensembles bien ordonnés d'ordinaux :

Définition 1.4.10 *Soient E un ensemble d'ordinaux bien ordonné par $<_E$, et α un ordinal isomorphe à E. On pose $E = \cup_{\gamma<\alpha}\{\beta_\gamma\}$ avec $\beta_\gamma <_E \beta_\delta$ si et seulement si $\gamma < \delta < \alpha$. La* **somme bien ordonnée** *des éléments de E, notée $\sum_{\gamma<\alpha} \beta_\gamma$, est l'ensemble $E' = \cup_{\gamma<\alpha}\beta_\gamma$ muni de l'ordre $<_{E'}$ défini par $c <_{E'} c'$ si et seulement si une des deux conditions suivantes est vérifiée :*

- *$c \in \beta_\gamma$, $c' \in \beta_\delta$ et $\gamma < \delta$*
- *$c, c' \in \beta_\gamma$ et $c <_{\beta_\gamma} c'$*

où $<_{\beta_\gamma}$ est le bon ordre de β_γ.

La somme bien ordonnée des éléments de E est un ordinal. Soit E un ensemble. Plutôt que d'ensemble bien ordonné d'éléments de E, on parlera de **suite** d'éléments de E, et pour l'exemple précédent, on écrira $(\beta_\gamma)_{\gamma<\alpha}$. L'ordinal α est appelé le **type de la suite**. Plutôt que de somme bien ordonnée des éléments d'une suite d'ordinaux on parlera de la somme d'une suite d'ordinaux.

Ce théorème découle directement de la définition de bon ordre, et fournit un moyen de prouver qu'une propriété est fausse dans la classe des ordinaux :

Théorème 1.4.11 *Il n'existe pas de suite infiniment décroissante d'ordinaux.*

Sinon une partie de l'ensemble duquel est tirée la suite n'aurait pas de plus petit élément, ce qui est impossible car ce dernier est par définition bien ordonné.

Le théorème suivant montre en particulier qu'il n'existe pas d'ordinal plus grand ou égal à tous les autres :

Théorème 1.4.12 *La somme d'une suite d'ordinaux n'est inférieure à aucun des ordinaux de la suite.*

En effet, soit α un ordinal. On peut toujours lui ajouter 1. On a $\alpha < \alpha+1 < \alpha+2 < \ldots$. On construit ainsi la suite croissante $(\alpha + n)_{n<\omega}$. La somme des termes de cette suite est un ordinal β plus grand que chacun des termes. On trouve des ordinaux de plus en plus grand en réitérant le processus avec β à la place de α.

Ceci nous amène à introduire la notion de limite d'une suite strictement croissante d'ordinaux dont le type est un ordinal limite :

Définition 1.4.13 *Soient $\xi \in Lim$ et $(\alpha_\beta)_{\beta<\xi}$ une suite strictement croissante d'ordinaux. La limite de la suite, notée $lim(\alpha_\beta)_{\beta<\xi}$, est le plus petit ordinal plus grand que chacun des termes de la suite.*

Par exemple, $lim(n)_{n<\omega} = \omega$, et $lim(w+n)_{n<\omega} = \omega + \omega$. D'une façon générale, tout ordinal limite est limite de la suite strictement croissante de tous les ordinaux plus petits que lui.

La preuve du théorème suivant, que nous utiliserons souvent, nécessite l'emploi de l'axiome du choix :

Théorème 1.4.14 *Un ordinal est à la fois dénombrable et limite si et seulement si il est limite d'une suite strictement croissante de type ω d'ordinaux dénombrables.*

Comme un ordinal α est soit 0, soit successeur (i.e. il existe $\beta \in Ord$ tel que $\alpha = \beta+1$), soit limite (i.e. $\alpha = lim(\beta)_{\beta<\alpha}$), pour montrer que les ordinaux vérifient une propriété donnée on peut utiliser le **principe d'induction transfinie**. Comme dans le cas des entiers naturels, il en existe deux, un faible et un fort, qui sont équivalents :

Définition 1.4.15 (Induction forte) *Soit une propriété P sur Ord.*
Si $\forall\alpha \in Ord\ (\forall\beta \in Ord\ \beta < \alpha \Rightarrow\ P(\beta)) \Rightarrow\ P(\alpha)$, alors $\forall\alpha \in Ord\ P(\alpha)$.

Pour l'induction faible on se contente de rajouter un cas par rapport à celui sur les entiers naturels pour pouvoir accéder aux ordinaux limite.

Définition 1.4.16 (Induction faible) *Soit P une propriété sur Ord. Si :*
- $P(0)$
- $\forall\alpha \in Ord\ (P(\alpha) \Rightarrow\ P(\alpha+1))$
- $\forall\xi \in Lim\ ((\forall\alpha \in Ord\ \alpha < \xi \Rightarrow\ P(\alpha)) \Rightarrow\ P(\xi))$

Alors $\forall\alpha \in Ord\ P(\alpha)$.

Nous allons maintenant nous servir de ces principes d'induction pour définir le produit et l'exponentiation d'ordinaux.

Le produit de deux ordinaux est défini de façon à ce que $\alpha \cdot \beta = \underbrace{\alpha + \alpha + \alpha + \ldots\ldots\ldots}_{\beta \text{ fois}}$

Définition 1.4.17 (multiplication) *Soient $\alpha, \beta \in Ord$ et $\xi \in Lim$. On pose*
- $\alpha \cdot 0 = 0$
- $\alpha \cdot (\beta+1) = \alpha \cdot \beta + \alpha$
- $\alpha \cdot \xi = \lim(\alpha \cdot \beta)_{\beta<\xi}$

On vérifie très facilement par induction transfinie que le produit de deux ordinaux est encore un ordinal.

Exemple 1.4.18 *On a les égalités :*

– $1 \cdot \omega = \omega \cdot 1 = \omega$ – $n \cdot \omega = \omega$ – $\omega \cdot 3 = \omega + \omega + \omega$

Le produit vérifie entre autres les propriétés suivantes :
- il est distributif à droite par rapport à l'addition : $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$. Par contre, il est faux de dire que $(\beta + \gamma) \cdot \alpha = \beta \cdot \alpha + \gamma \cdot \alpha$, car par exemple $(1+1) \cdot \omega = 2 \cdot \omega = \omega \neq \omega + \omega$,
- il est associatif,
- il n'est pas commutatif,
- $\alpha \cdot \beta \in Lim$ si et seulement si un des deux est limite et aucun des deux n'est 0,
- il possède un élément neutre qui est 1.

Exemple 1.4.19 *On a les égalités :*

$$(\omega \cdot n) \cdot \omega = \omega \cdot (n \cdot \omega) = \omega \cdot \omega$$
$$(\omega + 1) \cdot \omega = \underbrace{(\omega + 1) + (\omega + 1) + \dots}_{\omega \text{ fois}} = \underbrace{\omega + (1 + \omega) + (1 + \omega) + \dots}_{\omega \text{ fois}}$$
$$= \underbrace{\omega + \omega + \dots}_{\omega \text{ fois}} = \omega \cdot \omega$$

Dans la suite nous noterons souvent $\alpha\beta$ plutôt que $\alpha \cdot \beta$ pour alléger les notations.

L'exponentiation d'ordinaux est définie de façon à ce que $\alpha^\beta = \underbrace{\alpha \cdot \alpha \cdot \alpha \cdot \dots\dots\dots}_{\beta \text{ fois}}$

Définition 1.4.20 (exponentiation) *Soient $\alpha, \beta \in Ord$ et $\xi \in Lim$. On pose*
- $\alpha^0 = 1$
- $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$
- $\alpha^\xi = \lim(\alpha^\beta)_{\beta<\xi}$

Elle vérifie entre autres les propriétés suivantes :
- $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$
- $(\alpha^\beta)^\gamma = \alpha^{\beta\cdot\gamma}$

Exemple 1.4.21 *On a les égalités :*
- $n^\omega = \omega$. *En effet,* $n^\omega = \lim(n^m)_{m<\omega} = \lim(m)_{m<\omega} = \omega$.
- $n^{\omega^\omega} = \omega^{\omega^\omega}$ *car* $n^{\omega^\omega} = n^{\omega^{1+\omega}} = n^{(\omega \cdot \omega^\omega)} = (n^\omega)^{\omega^\omega} = \omega^{\omega^\omega}$.

Nous sommes maintenant en mesure d'énoncer un théorème important sur les nombres ordinaux.

Théorème 1.4.22 (Forme normale d'un ordinal (Cantor))
Tout ordinal α peut s'écrire de manière unique

$$\alpha = \omega^{\alpha_1} \cdot n_1 + \omega^{\alpha_2} \cdot n_2 + \cdots + \omega^{\alpha_k} \cdot n_k$$

où k est un entier naturel, les n_i sont inférieurs à ω, et $\alpha_1 > \alpha_2 > \cdots > \alpha_k$. On appelle **degré** *de α l'ordinal α_1.*

Nous écrirons $\alpha = \sum_{i=1}^{k} \omega^{\alpha_i} \cdot n_i$ pour abréger.

Le théorème suivant est une forme réduite du théorème précédent :

Théorème 1.4.23 *Tout ordinal $\alpha < \omega^\omega$ peut s'écrire de manière unique*

$$\alpha = \omega^k \cdot n_k + \omega^{k-1} \cdot n_{k-1} + \cdots + \omega^0 \cdot n_0$$

où k est un entier naturel et les n_i sont inférieurs à ω. Ici encore, k est le degré de α.

Cette fois encore, nous écrirons $\alpha = \sum_{i=k}^{0} \omega^i \cdot n_i$ pour abréger. Attention, le i de la somme décroît (la somme n'est pas commutative) !

Notons que si $\alpha \in Lim$, $\alpha = \sum_{i=1}^{k} \omega^{\alpha_i} \cdot n_i$ avec $\alpha_k > 0$ et si $\alpha < \omega^\omega$ on a $\alpha = \sum_{i=k}^{1} \omega^i \cdot n_i$.

Exemple 1.4.24 *On cherche à donner la forme normale de $(\omega+1)\cdot 2\cdot(\omega+1)\cdot 3\cdot(\omega+1)\cdot 4$. On sait que $(\omega+1)\cdot 4 = \omega+1+\omega+1+\omega+1+\omega+1 = \omega+\omega+\omega+\omega+1 = \omega\cdot 4+1$. Donc*

$$\begin{aligned}
(\omega+1)\cdot 2\cdot(\omega+1)\cdot 3\cdot(\omega+1)\cdot 4 &= (\omega\cdot 2+1)\cdot(\omega\cdot 3+1)\cdot(\omega\cdot 4+1) \\
&= (\omega\cdot 2+1)\cdot(\omega\cdot 3\cdot\omega\cdot 4+\omega\cdot 3+1) \\
&= (\omega\cdot 2+1)\cdot(\omega^2\cdot 4+\omega\cdot 3+1) \\
&= \omega\cdot 2\cdot\omega\cdot\omega\cdot 4+\omega\cdot 2\cdot\omega\cdot 3+\omega\cdot 2+1 \\
&= \omega^3\cdot 4+\omega^2\cdot 3+\omega\cdot 2+1
\end{aligned}$$

La proposition suivante nous sera utile :

Proposition 1.4.25 *Tout nombre ordinal $\alpha < \omega^\omega$ peut s'écrire de façon unique $\alpha = \beta + \omega^n$ avec β le plus petit possible et $\beta \geq \omega^n$ ou $\beta = 0$, et $n < \omega$. L'entier n est appelé le* **type** *de α et est noté $ty(\alpha)$.*

Ces définitions seront souvent utilisées par la suite :

Définition 1.4.26 *Soit ξ un ordinal limite. Une suite croissante $(\alpha_\beta)_{\beta<\gamma}$ d'ordinaux tous plus petits que ξ est* **cofinale** *à ξ si, pour tout ordinal $\delta < \xi$, il existe $\beta < \gamma$ tel que $\alpha_\beta > \delta$.*

Définition 1.4.27 *Soient E un ensemble, $e = (e_\beta)_{\beta\leq\alpha}$ une suite d'éléments de E, et ξ un ordinal limite inférieur ou égal à α. Alors*

$$\begin{aligned}
Cof(e,\xi) = \{f \in E : \exists(\beta_\gamma)_{\gamma<\delta} \textit{ croissante}, \\
\textit{telle que } f = e_{\beta_\gamma} \textit{ et } \beta_\gamma < \xi \textit{ pour tout } \gamma < \delta, \textit{ et cofinale à } \xi\}
\end{aligned}$$

Définition 1.4.28 *Soit ξ un ordinal limite et E un ensemble d'ordinaux tous plus petits que ξ. On dit que E est* **cofinal** *avec ξ si et seulement si pour tout ordinal $\alpha < \xi$ il existe β dans E tel que β soit supérieur à α.*

Nous soulignons quelques faits sur ω_1 pour finir cette section. Son existence est montrée par le théorème de bon ordonnance. Par définition, c'est le plus petit ordinal indénombrable. Il est limite : en effet, s'il était successeur, il existerait α tel que $\omega_1 = \alpha + 1$. Or α est dénombrable, et comme nous l'avons déjà vu, la somme d'un ordinal dénombrable et de 1 donne un ordinal dénombrable, d'où une contradiction. On a le théorème suivant :

Théorème 1.4.29 *La somme et la limite d'une suite croissante d'ordinaux dénombrables de type dénombrable est un ordinal dénombrable.*

Mais, comme ω_1 est limite, $\omega_1 = \lim(\alpha)_{\alpha<\omega_1}$.

1.5 Mots

Soient A un ensemble, α un ordinal, et $(a_\beta)_{\beta<\alpha}$ une suite d'éléments de A. La suite peut être dénotée en en donnant les éléments les uns après les autres, dans l'ordre croissant. Par exemple, si $A = \{a, b, c\}$, la suite $u = (u_\alpha)_{\alpha<5}$ telle que $u_0 = a$, $u_1 = c$, $u_2 = b$, $u_3 = a$ et $u_4 = b$ est dénotée par $u = acbab$. Un **mot** de **longueur** α sur un ensemble A est une suite de type α d'éléments de A. L'ensemble A est appelé un **alphabet**. Les éléments de A sont des **lettres**. La longueur d'un mot u est dénotée par $|u|$. Le mot vide λ est l'unique mot qui vérifie $|\lambda| = 0$.

Un mot u sur un alphabet A peut également être vu comme une application $u : |u| \to A$ (rappelons qu'un ordinal peut être confondu avec l'ensemble des ordinaux plus petits que lui). On peut alors écrire $u(\beta) = u_\beta$ pour $\beta < |u|$ si dans le terme de gauche de l'égalité u est vu comme une application et dans le terme de droite comme une suite. Pour des raisons pratiques, nous verrons quelquefois les mots comme des applications, quelquefois comme des suites.

L'ensemble A^* est l'ensemble des mots (de longueur) finis sur A. L'ensemble $A^* - \{\lambda\}$ est dénoté par A^+. Si α et β sont des ordinaux, alors

- A^α est l'ensemble des mots de longueur α sur A,
- $A^{<\alpha}$ est l'ensemble des mots de longueur inférieure à α sur A,
- $A^{[\beta,\alpha[}$ est l'ensemble des mots de longueur inférieure à α et supérieure ou égale à β sur A,
- $A^\#$ est l'ensemble des mots de longueur quelconque sur A.

Si a est une lettre et α un ordinal, alors a^α est l'unique mot de $\{a\}^\alpha$. Par exemple, $a^3 = aaa$.

Si A est fini, une partie de A^*, A^+, $A^\#$, A^α, $A^{<\alpha}$ ou $A^{[\beta,\alpha[}$ est un **langage** sur A.

Soient u un mot de longueur α sur un alphabet A_u et v un mot de longueur β sur un alphabet A_v. Le **produit**, ou la **concaténation**, de u et de v, noté uv, est le mot de longueur $\alpha + \beta$ sur $A_u \cup A_v$ défini par

$$(uv)_\gamma = \begin{cases} u_\gamma & \text{si } 0 \leq \gamma < \alpha \\ v_{\gamma-\alpha} & \text{si } \alpha \leq \gamma < \alpha + \beta \end{cases}$$

Par exemple, le produit des mots *abc* et *cd* est le mot *abccd*. Si E et F sont deux ensembles de mots sur deux alphabets respectifs A_E et A_F, alors $E \cdot F$, ou plus simplement EF, est l'ensemble des mots uv sur $A_E \cup A_F$ tels que $u \in A_E$ et $v \in A_F$.

On généralise le produit de deux mots à des suites de mots de la façon suivante : soient α un ordinal, $(u_\beta)_{\beta<\alpha}$ une suite de mots et $(A_\beta)_{\beta<\alpha}$ une suite d'alphabets telles que u_β est un mot sur A_β pour tout $\beta < \alpha$. Le produit $\prod_{\beta<\alpha} u_\beta$ des mots de la suite $(u_\beta)_{\beta<\alpha}$ est le mot v de longueur $\sum_{\beta<\alpha} |u_\beta|$ sur l'alphabet $\cup_{\beta<\alpha} A_\beta$ défini par, pour tout $\gamma < |v|$,

$$v(\gamma) = u_\delta(\gamma - \epsilon)$$

où δ est le plus grand ordinal possible tel que $\sum_{\beta<\delta} |u_\beta| \leq \gamma$ et $\epsilon = \sum_{\beta<\delta} |u_\beta|$. Si E est un ensemble de mots sur un alphabet A, alors E^* est l'ensemble des mots u sur A tels que $u = \prod_{i<n} u_i$ pour une suite finie $(u_i)_{i<n}$ de mots de E. On note E^+ l'ensemble $E^* - \{\lambda\}$. De la même façon, si α est un ordinal, alors E^α est l'ensemble des mots u sur A tels que $u = \prod_{\beta<\alpha} u_\beta$ pour une suite $(u_\beta)_{\beta<\alpha}$ de mots de E. En étendant encore la notation, on pose $E^{<\alpha} = \cup_{\beta<\alpha} E^\beta$, et finalement $E^\# = \cup_{\alpha \in Ord} E^\alpha$.

Soient u un mot de longueur α sur un alphabet A, et β, γ deux ordinaux tels que $\beta < \gamma \leq \alpha$. Par $u[\beta, \gamma[$ on dénote l'unique mot sur A de longueur $\gamma - \beta$ qui vérifie $u[\beta, \gamma[(\delta) = u(\beta + \delta)$ pour chaque $\delta < \gamma - \beta$. Il est appelé **facteur** de u. C'est un **facteur propre** de u si $u \neq u[\beta, \gamma[$, c'est-à-dire si $\beta > 0$ ou $\gamma < \alpha$. Si $\gamma = \alpha$, on dit que c'est un **suffixe** de u. Si $\beta = 0$, on dit que c'est un **préfixe** de u.

Exemple 1.5.1 *Soient* $A = \{a, b, c, d\}$ *un alphabet et* $u = a^{\omega+1} b^4 c^{\omega^2} d$ *un mot sur* A. *Le mot* $u[\omega, \omega \cdot 2[= ab^4 c^\omega$ *est un facteur propre de* u.

Chapitre 2

Automates et expressions rationnelles

Ce chapitre est consacré aux automates et aux expressions rationnelles. Les automates qui reconnaissent des mots dont les lettres sont indexées par des ordinaux ont été introduits par Büchi [Büc64] pour prouver des questions de décidabilité en logique. Ils possèdent deux fonctions de transition. La première est analogue à la fonction de transition des automates qui reconnaissent des mots finis : elle permet, à partir d'un chemin d'étiquette u, et d'une lettre a, de construire un chemin d'étiquette ua. En d'autres termes, elle permet d'associer par induction un chemin dans l'automate à tout mot de longueur successeur. La seconde fonction est utilisée pour associer toujours par induction un chemin dans l'automate à un mot de longueur limite. L'idée est que tout chemin doit avoir une fin. Quand l'étiquette du chemin est de longueur limite ξ, cette fin est calculée de façon déterministe en fonction des éléments du chemin dont l'indice est inférieur à ξ. Pour définir des automates qui reconnaissent des mots de longueur quelconque, Büchi fait terminer les chemins dont l'étiquette est un mot de longueur limite ξ par l'ensemble des états qui apparaissent cofinalement à ξ aux positions successeur dans le chemin. On peut considérer les ensembles ainsi construits comme des états particuliers de l'automate, fixer des transitions sortantes (mais jamais entrantes) de ces ensembles par des lettres de l'alphabet vers les états de l'automate, et décider si un mot de longueur limite qui est l'étiquette d'un chemin qui termine dans un de ces ensembles est accepté ou non. Les chemins sont alors constitués d'états aux positions successeur, et d'ensemble d'états aux positions limite. Comme dans le cas des mots finis, il existe un autre formalisme équivalent à de tels automates pour définir des ensembles de mots sur un alphabet fini : les expressions rationnelles. Elles sont similaires aux expressions rationnelles de Kleene, mais avec deux opérateurs unaires supplémentaires : L^ω est l'ensemble des mots construits par concaténation de ω mots de L, et $L^\#$ est l'ensemble des mots construits par concaténation d'un nombre quelconque de mots de L. L'opérateur $\#$ est aux ordinaux ce que $*$ est aux entiers naturels. La classe des langages ainsi définie n'est pas fermée par complémentation.

Une légère modification de la seconde fonction de transition permet de restreindre la longueur des chemins aux ordinaux dénombrables : il suffit de dire qu'un état q fait partie d'un ensemble élément d'un chemin à la position limite ξ si et seulement si il existe une suite croissante $(\alpha_\beta)_{\beta<\omega}$ d'ordinaux inférieurs à ξ et cofinale à ξ telle que chaque élément de la suite soit l'indice d'une apparition de q dans le chemin. Dans le formalisme des expressions rationnelles, on restreint alors l'opérateur $\#$ aux ordinaux dénombrables. La classe des langages ainsi définie est alors une sous classe propre de la première, et est fermée par complémentation. De plus, chaque langage rationnel est alors reconnaissable par un automate déterministe.

En restreignant encore la longueur des mots reconnus à ω ou aux mots finis on retombe sur la théorie classique des automates de Muller ou de Kleene.

Fixé un entier n positif, Büchi a également défini des automates qui reconnaissent des mots de longueur inférieure à ω^{n+1} en généralisant les idées de Muller : comme pour les automates sur les mots de longueur quelconque, on calcule une fin à tout chemin dont l'étiquette est un mot de longueur limite ξ, mais pas de la même façon. Si $\xi = \beta + \omega^i$ alors la fin du chemin est l'ensemble des éléments e du chemin pour lesquels il existe une infinité d'entiers j tels que e apparaisse à la position $\beta + \omega^{i-1} \cdot j$ dans le chemin. On peut à nouveau considérer les ensembles ainsi construits comme des états particuliers de l'automate, et fixer des transitions sortantes (mais jamais entrantes) de ces ensembles par des lettres de l'alphabet vers les états de l'automate, et décider si un mot de longueur limite qui est l'étiquette d'un chemin qui termine dans un de ces ensembles est accepté ou non. Les chemins sont alors constitués d'états aux positions successeur, d'ensemble d'états aux positions de la forme $\beta + \omega$, d'ensembles d'ensembles d'états aux positions de la forme $\beta + \omega^2$,... de telle façon qu'encore une fois les états aux positions successeur déterminent entièrement les composantes des chemins aux positions limite. Ces automates sont équivalents à des expressions rationnelles avec l'opérateur ω précédemment défini mais sans le $\#$. La classe des langages qu'ils reconnaissent est une sous classe stricte des langages définis par les automates qui reconnaissent des mots de longueur dénombrable. De plus ces automates sont déterministes.

Ce chapitre est divisé en six sections, chacune des cinq premières étant elle-même divisée en deux sous-sections : une pour les automates et une pour les expressions rationnelles. Les deux premières sections sont constituées de définitions de base sur les automates et les expressions rationnelles, respectivement sur les mots finis et de longueur ω, ainsi que de résultats qui seront ou bien nécessaires ou bien étendus par la suite. Les troisième, quatrième et cinquième sections sont consacrées aux automates et aux expressions rationnelles respectivement sur les mots de longueur inférieure à ω^n, de longueur dénombrable et de longueur quelconque. Dans la dernière section nous remontrons l'équivalence entre les différentes définitions d'automates, sous hypothèse bien entendu de restriction de domaines. Ces correspondances sont utilisées pour, donnés un B-automate $\mathcal{A}$ et un entier n, calculer un B-automate déterministe qui reconnaît exactement les mots de longueur inférieure à ω^{n+1} du langage associé à $\mathcal{A}$.

2.1 Mots finis

Pour un exposé plus détaillé sur la théorie des automates sur les mots finis, on renvoie à [HU79] ou [Per90].

Tout au long de cette section les mots sont de longueur finie.

2.1.1 Automates

Un automate est une représentation du comportement d'un système mécanique fini. Les ordinateurs étant des millions d'interrupteurs gérés par une unité de contrôle, le tout miniaturisé, sont de tels systèmes. Un automate est formé par l'ensemble des différents états possibles du système, reliés entre eux par des conditions : le système passe d'un état dans un autre quand une condition donnée est vérifiée. Si, à partir de chaque état, et pour une condition donnée, le système ne peut passer que dans un unique état, et si l'état initial du système est non ambigu, alors il est déterministe. Il est non déterministe sinon. La théorie des automates consiste à étudier l'ensemble des conditions qui doivent être séquentiellement réalisées pour que la machine passe d'un ensemble d'états (appelés initiaux), dans un autre (appelés finaux).

Formellement,

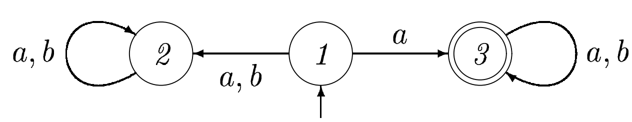
Définition 2.1.1 *Un* **automate** $\mathcal{A}$ *est un* 5*-uplet* $< Q, A, E, I, F >$ *avec*

- Q *l'ensemble fini des états,*
- A *un alphabet fini,*
- $E \subseteq (Q \times A \times Q)$ *l'ensemble des transitions,*
- $I \subseteq Q$ *l'ensemble des états initiaux,*
- $F \subseteq Q$ *l'ensemble des états finaux.*

Nous dirons que deux automates sont identiques si on obtient l'un à partir de l'autre par un simple renommage des états.

On peut représenter un automate comme un graphe, dans lequel les noeuds sont les états du système, et dont les arcs (les transitions) sont étiquetés par des lettres, qui représentent les conditions à réaliser pour passer d'un état du système dans un autre. Dans les représentations graphiques des automates, les états initiaux sont indiqués avec une petite flèche entrante, et les états finaux par un double cercle. Plutôt que de tracer plusieurs arcs avec des étiquettes différentes qui partent tous du même état pour arriver dans le même état, on regroupe les étiquettes sur un seul arc.

Exemple 2.1.2 *On représente l'automate*
$< \{1, 2, 3\}, \{a, b\}, \{(1, a, 2), (1, a, 3), (1, b, 2), (2, a, 2), (2, b, 2), (3, a, 3), (3, b, 3)\}, \{1\}, \{3\} >$
par



Un automate $< Q, A, E, I, F >$ est **complet** si, pour tout état $q \in Q$ et lettre $a \in A$, il existe $p \in Q$ tel que $(q, a, p) \in E$. Il est **déterministe** si p est unique ou n'existe pas, et $|I| = 1$.

Formellement, un **chemin** c de longueur $n + 1$ de l'état p (ou qui commence à p, ou encore d'origine p) vers l'état q (ou qui finit, termine dans q) dans un automate $< Q, A, E, I, F >$ est une suite $(q_i)_{i<n+1}$ d'éléments de Q telle que $q_0 = p$, $q_n = p$ et pour chaque $i < n$ il existe une lettre a_i de A telle que $(q_i, a_i, q_{i+1}) \in E$. Le mot $u = a_0 a_1 \ldots a_{n-1}$ est appelé une **étiquette** du chemin c. On peut se servir de la notion de chemin pour redéfinir, de façon équivalente à ce qu'on a fait précédemment, la notion de déterminisme : un automate est déterministe si aucun mot de A^* n'étiquette deux chemins différents de même origine, et si $|I| = 1$.

On utilise les automates pour définir des ensembles de mots de la façon suivante : un chemin est réussi, ou acceptant, s'il commence dans un état initial et termine dans un état final. On dit alors que l'étiquette du chemin est reconnu, ou accepté, par l'automate. L'ensemble des mots reconnus par un automate $\mathcal{A}$, noté $\mathcal{L}(\mathcal{A})$, est le **langage** reconnu par l'automate. Soit A un alphabet fini. On dit qu'une partie L de A^* est **$*$-reconnaissable** s'il existe un automate $\mathcal{A} =< Q, A, E, I, F >$ tel que $L = \mathcal{L}(\mathcal{A})$.

Exemple 2.1.3 *L'automate de l'exemple 2.1.2 est non déterministe, puisque à partir de l'état* 1 *on peut accéder à deux états différents par la lettre a. Il reconnaît l'ensemble aA^* des mots de A^* qui commencent par la lettre a.*

Les résultats suivants sont des classiques de la théorie des automates :

Théorème 2.1.4 *Soient A un alphabet fini et L une partie $*$-reconnaissable de A^*. Il existe un automate déterministe complet $\mathcal{A}$ tel que $L = \mathcal{L}(\mathcal{A})$.*

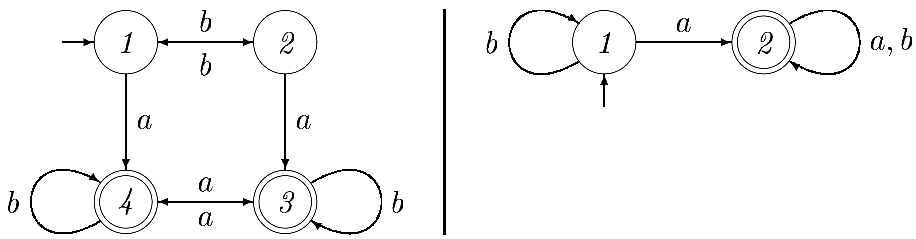
Le théorème suivant montre en particulier que les combinaisons booléennes de langages $*$-reconnaissables sont encore $*$-reconnaissables :

Théorème 2.1.5 *Soient A un alphabet fini, L et L' deux parties $*$-reconnaissables de A^*. Alors $L \cup L'$, $L \cap L'$, $L - L'$, $A^* - L$, LL' et L^* sont $*$-reconnaissables.*

Finalement, le théorème suivant montre qu'il existe une forme canonique pour les automates :

Théorème 2.1.6 *Soient A un alphabet fini et L une partie $*$-reconnaissable de A^*. Parmi tous les automates déterministes complets qui reconnaissent L, il en existe un unique, l'automate minimal de L, qui a strictement moins d'états que les autres.*

Exemple 2.1.7 *Soit $A = \{a, b\}$ un alphabet. Les deux automates suivants reconnaissent A^*aA^*.*



Celui de droite est l'automate minimal de A^*aA^*.

Une conséquence immédiate du théorème 2.1.6 est que :

Corollaire 2.1.8 *Soient $\mathcal{A} =< Q, A, E, I, F >$ et $\mathcal{B} =< Q', A, E', I', F' >$ deux automates. Alors les questions $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{B})$ et $\mathcal{L}(\mathcal{A}) = \emptyset$ sont décidables.*

Pour le prouver, il suffit de construire les automates minimaux de $\mathcal{L}(\mathcal{A})$ et de $\mathcal{L}(\mathcal{B})$. Les automates sont identiques si et seulement si $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{B})$. De plus, l'automate minimal de $\mathcal{L}(\mathcal{A})$ n'a pas d'état final si et seulement si $\mathcal{L}(\mathcal{A}) = \emptyset$.

2.1.2 Expressions rationnelles

Les **expressions rationnelles** ont été introduites par Kleene en 1956 dans le premier article [Kle56] qui traite d'automates sous la forme qu'on utilise.

Définition 2.1.9 *Soit un alphabet fini $A = \{a_1, \ldots, a_n\}$. Une* **expression rationnelle** *sur A est un mot fini sur l'ensemble $A \cup \{+, \cdot, ^*, (,), \lambda, \emptyset\}$ tel que :*
- *$\emptyset$ est une expression rationnelle.*
- *λ est une expression rationnelle,*
- *a est une expression rationnelle pour tout $a \in A$,*
- *Si e_1 et e_2 sont des expressions rationnelles, alors $e_1 + e_2$ est une expression rationnelle,*
- *Si e_1 et e_2 sont des expressions rationnelles, alors $e_1 \cdot e_2$ est une expression rationnelle, que nous noterons aussi plus simplement $e_1 e_2$,*
- *Si e est une expression rationnelle, alors (e) est une expression rationnelle,*
- *Si e est une expression rationnelle, alors e^* est une expression rationnelle.*

La partie $\overline{e}$ de A^* dénotée par une expression rationnelle e est définie par induction sur e :

- $\overline{\emptyset} = \emptyset$,
- $\overline{\lambda} = \{\lambda\}$,
- $\overline{a} = \{a\}$ *pour tout* $a \in A$,
- $\overline{e_1 + e_2} = \overline{e_1} \cup \overline{e_2}$,
- $\overline{e_1 \cdot e_2} = \overline{e_1} \cdot \overline{e_2}$,
- $\overline{(e)} = \overline{e}$,
- $\overline{e^*} = \overline{e}^*$.

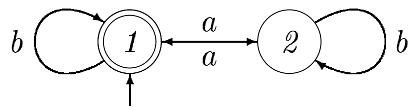
Par soucis d'allégement des notations, si e est une expression rationnelle, alors nous noterons $\overline{e}$ également par e.

On dit qu'une partie de A^* est **rationnelle** si elle est définissable par une expression rationnelle.

Voici le premier résultat important de la théorie des automates :

Théorème 2.1.10 (Kleene, 1956 [Kle56]) *Soit A un alphabet fini. Une partie de A^* est $*$-reconnaissable si et seulement si elle est rationnelle.*

Exemple 2.1.11 *L'automate*



est l'automate minimal de l'ensemble des mots de $\{a,b\}^*$ qui ont un nombre pair de a, dénoté par l'expression rationnelle $(b^*ab^*ab^*)^*$.

2.2 Mots de longueur ω

Pour un exposé plus détaillé sur la théorie des automates sur les mots de longueur ω, on renvoie à [PP97] et [Cho74].

Tout au long de cette section les mots sont de longueur ω.

2.2.1 Automates

Les automates sur les mots de longueur ω ont été introduits par Büchi en 1960 [Büc60] pour décider de la logique monadique faible du second ordre des entiers. Indépendamment, Muller [Mul63] donne en 1963 une autre définition d'automates qui reconnaissent des mots de longueur ω.

Nous avons vu qu'un mot fini est reconnu par un automate s'il est l'étiquette d'un chemin qui commence dans un état initial et qui termine dans un état final. Les chemins sont obtenus en construisant un mot sur l'ensemble des états par récurrence : si c est un chemin d'étiquette u de dernier élément p, alors cq est un chemin d'étiquette ua si et seulement si il existe une transition de p vers q par la lettre a dans l'automate. Un chemin ainsi construit étiqueté par un mot de longueur ω a également ω pour longueur, et en particulier il ne termine dans aucun état. Par conséquent la définition d'acceptation d'un mot par l'automate ne peut être la même pour les mots finis et de longueur ω si on garde la même notion de chemin.

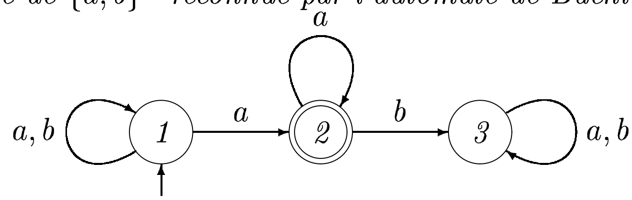
Automates de Büchi

Les définitions d'automate de Büchi, d'automate de Büchi complet, déterministe, sont les mêmes que dans le cas des mots finis (c.f. page 21).

Un **chemin** c de longueur ω d'origine p dans un automate de Büchi $\mathcal{A} =< Q, A, E, I, F >$ est une suite $(q_i)_{i<\omega}$ d'éléments de Q telle que $q_0 = p$ et pour chaque $i < \omega$ il existe une lettre a_i de A telle que $(q_i, a_i, q_{i+1}) \in E$. Le mot $(a_i)_{i<\omega}$ est appelé une étiquette du chemin c. On dit que c est réussi, ou acceptant, si p est un état initial et s'il existe au moins un état de Q qui apparaît infiniment souvent dans c, i.e. $F \cap \{q \in Q : |\{i < \omega| : q_i = q\}| = \aleph_0\} \neq \emptyset$. Le langage $\mathcal{L}^\omega(\mathcal{A})$ de mots de longueur ω reconnus par $\mathcal{A}$ est l'ensemble des mots qui sont des étiquettes de chemins de longueur ω réussis. Soit A un alphabet. On dit qu'une partie

L de A^ω est ω-**reconnaissable** s'il existe un automate de Büchi $\mathcal{A} =< Q, A, E, I, F >$ tel que $L = \mathcal{L}^\omega(\mathcal{A})$.

Exemple 2.2.1 *La partie de $\{a,b\}^\omega$ reconnue par l'automate de Büchi*



est constituée des mots de longueur ω sur $\{a,b\}$ qui n'ont qu'un nombre fini de b.

Contrairement au cas des mots finis, il existe des langages de mots de longueur ω qui sont reconnus par des automates de Büchi non déterministes, mais qui ne le sont par aucun automate de Büchi déterministe (c'est le cas pour le langage reconnu par l'automate de l'exemple précédent). De plus, il n'existe pas d'analogue du théorème 2.1.6 pour les automates de Büchi : en effet, il existe des langages de mots de longueur ω qui sont acceptés par plusieurs automates de Büchi différents mais avec le même nombre d'états, qui est minimal.

Par contre, la classe des langages ω-reconnaissables est close par opérations booléennes :

Théorème 2.2.2 *Soient A un alphabet fini, L et L' deux parties ω-reconnaissables de A^ω. Alors $L \cup L'$, $L \cap L'$, $L - L'$ et $A^\omega - L$ sont ω-reconnaissables.*

Comme corollaire immédiat :

Corollaire 2.2.3 *Soient $\mathcal{A} =< Q, A, E, I, F >$ et $\mathcal{B} =< Q', A, E', I', F' >$ deux automates de Büchi. Alors les questions $\mathcal{L}^\omega(\mathcal{A}) = \mathcal{L}^\omega(\mathcal{B})$ et $\mathcal{L}^\omega(\mathcal{A}) = \emptyset$ sont décidables.*

En effet, un automate de Büchi reconnaît au moins un mot si et seulement si il existe un chemin fini qui part d'un état initial pour arriver dans un état final et un autre chemin fini qui part de cet état pour arriver dans lui-même. De plus, le langage de l'automate de Büchi qui reconnaît $(\mathcal{L}^\omega(\mathcal{A}) \cap \overline{\mathcal{L}^\omega(\mathcal{B})}) \cup (\overline{\mathcal{L}^\omega(\mathcal{A})} \cap \mathcal{L}^\omega(\mathcal{B}))$ est vide si et seulement si $\mathcal{L}^\omega(\mathcal{A}) = \mathcal{L}^\omega(\mathcal{B})$.

Automates de Muller

Les automates de Muller [Mul63] n'ont pas d'états finaux, mais des ensembles d'états finaux. La définition d'un chemin est la même que pour les automates de Büchi. Un mot de longueur ω est reconnu par un automate de Muller si et seulement si il est l'étiquette d'un chemin qui commence dans un état initial, et dont l'ensemble des états qui apparaissent infiniment souvent est dans l'ensemble des ensembles d'états finaux. Formellement,

Définition 2.2.4 *Un* **automate de Muller** $\mathcal{A}$ *est un* 5*-uplet* $< Q, A, E, I, F >$ *avec*

- *Q l'ensemble fini des états,*

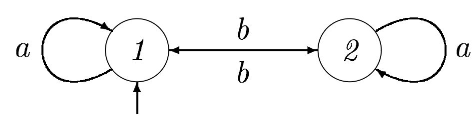
- *A un alphabet fini,*
- *$E \subseteq (Q \times A \times Q)$ l'ensemble des transitions,*
- *$I \subseteq Q$ l'ensemble des états initiaux,*
- *$F \subseteq [Q] \cup \emptyset$ l'ensemble des ensembles d'états finaux.*

Un mot sur A est reconnu par $\mathcal{A}$ s'il est l'étiquette d'un chemin $(q_i)_{i<\omega}$ qui vérifie

$$\{q : |\{i : q_i = q\}| = \aleph_0\} \in F$$

La partie de A^ω reconnue par $\mathcal{A}$ est notée $\mathcal{L}^\omega(A)$.

Exemple 2.2.5 *La partie de $\{a, b\}^\omega$ reconnue par l'automate de Muller*



avec $F = \{\{1\}, \{2\}\}$ est constituée des mots de longueur ω sur $\{a, b\}$ qui n'ont qu'un nombre fini de b.

La théorie des automates de Muller présente plus de similitudes avec celles des automates sur les mots finis que celle des automates de Büchi. En effet,

Théorème 2.2.6 (McNaughton, 1966 [McN66]) *Pour tout automate de Muller $\mathcal{A}$, il existe un automate de Muller déterministe $\mathcal{B}$ tel que $\mathcal{L}^\omega(\mathcal{B}) = \mathcal{L}^\omega(\mathcal{A})$.*

Ce résultat a été redémontré par Safra [Saf88]. Sa preuve fournit un algorithme de déterminisation des automates de Muller dont la complexité est une exponentielle simple de la taille de l'automate de Muller de départ, ce qui est considérablement inférieure à celle de l'algorithme original de McNaughton, qui est une exponentielle double.

Comme dans le cas des automates de Büchi, il n'existe pas d'analogue du théorème 2.1.6 pour les automates de Muller.

Equivalence des deux définitions

McNaughton prouva que les deux définitions d'automates sur les mots de longueur ω sont équivalentes :

Théorème 2.2.7 (McNaughton, 1966 [McN66]) *Soient A un alphabet fini et $L \subseteq A^\omega$. Alors $L = \mathcal{L}^\omega(\mathcal{A})$ pour un automate de Büchi $\mathcal{A}$ si et seulement si $L = \mathcal{L}^\omega(\mathcal{B})$ pour un automate de Muller $\mathcal{B}$.*

2.2.2 Expressions rationnelles

Les expressions rationnelles sur les mots de longueur ω ont été introduites par Muller [Mul63] et Büchi [Büc62].

Définition 2.2.8 *Soit un alphabet fini $A = \{a_1, \ldots, a_n\}$. Une ω-***expression rationnelle** *sur A est un mot fini de la forme $e_1 \cdot e_2^\omega$ sur l'ensemble $A \cup \{+, \cdot, ^*, \omega, (,), \lambda, \emptyset\}$ tel que*
- *e_1, e_2 soient deux expressions rationnelles sur A au sens des mots finis,*
- *$\lambda \notin \overline{e_2}$,*
- *$\overline{e_2} \neq \emptyset$.*

On définit des ensembles de mots de longueur ω à partir d'expressions ω-régulières en ajoutant la règle $\overline{e^\omega} = \overline{e}^\omega$ à celles de définition d'ensembles de mots finis à partir d'expressions rationnelles de la page 23. On dit qu'une partie de A^ω est **ω-rationnelle**, ou plus simplement rationnelle en l'absence d'ambiguïté, si elle est définissable par une ω-expression rationnelle.

Le théorème d'équivalence entre les langages $*$-reconnaissables et les langages rationnels sur les mots finis s'étend aux mots de longueur ω :

Théorème 2.2.9 (McNaughton, 1966 [McN66]) *Soit A un alphabet fini. Une partie de A^ω est ω-reconnaissable si et seulement si elle est ω-rationnelle.*

Exemple 2.2.10 *Les automates de Büchi et de Muller des exemples 2.2.1 et 2.2.5 reconnaissent le langage dénoté par l'expression ω-rationnelle $(a+b)^*a^\omega$.*

2.3 Mots de longueur inférieure à ω^n

Büchi, motivé par l'extension de ses résultats de décidabilité du calcul séquentiel sur les entiers naturels à des ensembles d'ordinalité supérieure, est le premier à définir des automates qui reconnaissent des mots indexés par des ordinaux plus grands que ω [Büc64].

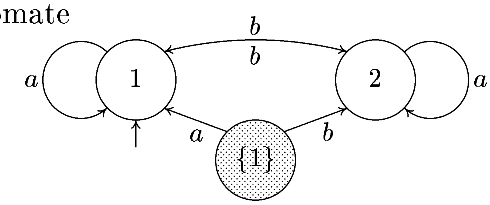
Les automates que nous présentons ici sont dûs à Büchi (on les retrouve par exemple dans [BS73]), mais Choueka les a étudiés d'une façon plus systématique du point de vue de la théorie des automates [Cho78] : Büchi ne les utilisait que pour prouver des résultats de décidabilité en logique. Nous renvoyons pour cette raison à l'article de Choueka plutôt qu'aux travaux de Büchi pour les preuves de certains résultats.

Tout au long de cette section, n est un entier fixé et les mots sont de longueur plus petite que ω^{n+1}.

2.3.1 Automates

Les automates que nous décrivons maintenant sont une généralisation de ceux de Muller : L'idée est d'associer à tout chemin d'étiquette u une fin, même si $|u|$ est limite. Soient A un alphabet fini et $u = (a_\beta)_{\beta<\omega+1}$ un mot sur A. Soit également c un chemin d'étiquette

$(a_\beta)_{\beta<\omega}$ dans un automate de Muller qui reconnaît une partie de A^ω. Considérer l'ensemble E des états infiniment répétés dans c comme un état de l'automate permet la construction de chemins d'étiquette u : on dit que $(q_\alpha)_{\alpha<\omega+2}$ est un chemin d'étiquette u si $(q_\alpha)_{\alpha<\omega} = c$, $q_\omega = E$ et il existe une transition de E vers $q_{\omega+1}$ par la lettre a_ω. Par exemple en posant $q_\alpha = 1$ pour tout α inférieur à ω, $E = \{1\}$ et $q_{\omega+1} = 2$ alors $(q_\alpha)_{\alpha<\omega+2}$ est un chemin d'étiquette $a^\omega b$ dans l'automate



Si u est un mot de longueur $\omega \cdot 2$ et si $(q_\alpha)_{\alpha<\beta+1}$ est un chemin d'étiquette $u[0,\beta[$ pour tout β inférieur à $\omega \cdot 2$ alors $(q_\alpha)_{\alpha<\omega\cdot 2+1}$ est un chemin d'étiquette u si $q_{\omega\cdot 2}$ est l'ensemble des états infiniment répétés dans la suite $(q_\alpha)_{\omega<\alpha<\omega\cdot 2}$. D'une manière plus générale si u est un mot de longueur $\omega \cdot i$ où i est un entier naturel positif et si $(q_\alpha)_{\alpha<\beta+1}$ est un chemin d'étiquette $u[0,\beta[$ pour tout β inférieur à $\omega \cdot i$ alors $(q_\alpha)_{\alpha<\omega\cdot i+1}$ est un chemin d'étiquette u si $q_{\omega\cdot i}$ est l'ensemble des états infiniment répétés dans la suite $(q_\alpha)_{\omega\cdot(i-1)<\alpha<\omega\cdot i}$. Si maintenant u est de longueur ω^2 et si $(q_\alpha)_{\alpha<\beta+1}$ est un chemin d'étiquette $u[0,\beta[$ pour tout β inférieur à ω^2 alors $(q_\alpha)_{\alpha<\omega^2+1}$ est un chemin d'étiquette u si q_{ω^2} est l'ensemble des ensembles d'états qui apparaissent infiniment souvent dans la suite $(q_{\omega\cdot i})_{i<\omega}$. On peut alors construire des chemins de longueur supérieure en considérant q_{ω^2} comme un état de l'automate comme nous l'avions fait pour q_ω. D'une manière plus générale l'élément d'indice ω^{k+1} dans un chemin est l'ensemble des éléments qui apparaissent infiniment souvent dans la suite $(q_{\omega^k\cdot i})_{i<\omega}$.

Formellement, les automates sont équipés d'une relation de transition, comme les automates sur les mots finis, qui permet de construire des chemins de longueur $\beta+1$ à partir d'un chemin de longueur β, avec en plus une fonction de transition qui permet le passage à la limite. Ils sont définis en fonction d'un paramètre n qui fixe la longueur du plus grand mot reconnu.

Définition 2.3.1 *Un n-***automate** *$\mathcal{A}$ est un 5-uplet $< Q, A, E, I, F >$ avec :*
- *Q l'ensemble fini des états,*
- *A un alphabet fini,*
- *$E \subseteq [Q]_0^n \times A \times Q$ l'ensemble des transitions,*
- *$I \subseteq Q$ l'ensemble des états initiaux,*
- *$F \subseteq [Q]_0^n$ l'ensemble des états finaux.*

L'automate est complet si, pour tout $q \in [Q]_0^n$ et lettre a, il existe $p \in Q$ tel que $(q, a, p) \in E$. Il est déterministe si p est unique ou n'existe pas, et $|I| = 1$.

Pour définir les chemins nous avons besoin de la définition suivante (rappelons que l'écriture $\beta + \omega^k$ fait référence à la proposition 1.4.25 page 15) :

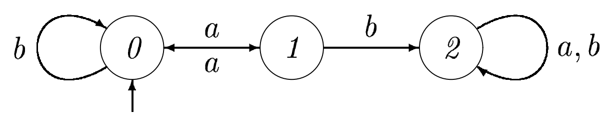
Définition 2.3.2 *Soient E un ensemble non vide, n un entier, α un ordinal plus petit que ω^{n+1} et $e = (e_\beta)_{\beta<\alpha}$ une suite d'éléments de $[E]_0^n$. On dit que e est C-**continue** si $e_\beta \in E$ pour tout ordinal successeur β inférieur à α, et pour tout ordinal $\xi = \beta + \omega^k$ limite inférieur à α,*

$$e_\xi = \{q : |\{i : e_{\beta+\omega^{k-1}\cdot i} = q\}| = \aleph_0\}$$

Remarquons que les valeurs de e indicées par des ordinaux limite sont entièrement déterminées par celles indicées par les ordinaux successeurs plus petits.

Un **chemin** $c = (q_\beta)_{\beta\leq\alpha}$ d'origine p vers q de longueur $\alpha + 1$ étiqueté par un mot $u = (a_\beta)_{\beta<\alpha}$ est une suite C-continue d'éléments de $[Q]_0^n$ telle que $q_0 = p$, $q_\alpha = q$ et $(q_\beta, a_\beta, q_{\beta+1}) \in E$ pour tout β plus petit que α. Le chemin est acceptant si $p \in I$ et $q \in F$. Le langage $\mathcal{L}(\mathcal{A})$ reconnu par $\mathcal{A}$ est l'ensemble des mots de $A^{<\omega^{n+1}}$ qui sont l'étiquette d'un chemin acceptant. Une partie L de $A^{<\omega^{n+1}}$ est n-**reconnaissable** s'il existe un n-automate $\mathcal{A}$ tel que $L = \mathcal{L}(\mathcal{A})$.

Exemple 2.3.3 *Soit $\mathcal{A} =< Q = \{0,1,2\}, A = \{a,b\}, E, \{0\}, \{\{\{0\}\}\} >$ le 2-automate suivant :*



Pour plus de clarté nous n'avons pas représenté les transitions des éléments de $[Q]_1^2$ vers les éléments de Q : toute transition d'un élément de $[Q]_1^2$ qui contient 2 ou $\{2\}$ est vers 2, toute transition d'un autre élément de $[Q]_1^2$ par a est vers 1, vers 0 par b.

Le langage $\mathcal{L}(\mathcal{A})$ est l'ensemble des mots u de $A^{<\omega^3}$ tels que

1. *$|u| = \gamma + \omega^2$,*
2. *tout facteur de u qui ne contient que des "a" est facteur d'un autre facteur de u qui ne contient que des "a" et de longueur $2 \cdot \alpha$ pour un certain ordinal α,*
3. *il existe un entier naturel j tel que pour tout i supérieur ou égal à j, $u[\gamma + \omega \cdot i, \gamma + \omega \cdot (i+1)[$ ne contient qu'un nombre fini de "a".*

En effet, soit $u \in \mathcal{L}(\mathcal{A})$. La condition 2 est nécessairement vérifiée, sinon il existe un chemin de 0 vers 2, d'où on ne sort plus. D'autre part, la forme normale de $|u|$ est nécessairement $|u| = \omega^2 \cdot i$, où i est un entier positif. La condition 1 est vérifiée en posant $\gamma = \omega^2 \cdot (i-1)$. Si on suppose finalement que 3 est fausse, alors $\{0,1\}$ ou $\{2\}$ est dans le dernier élément du chemin d'étiquette u, ce qui est impossible.

Réciproquement, on vérifie aisément que si u vérifie les conditions précédentes, alors $u \in \mathcal{L}(\mathcal{A})$.

Théorème 2.3.4 ([Cho78]) *Soient A un alphabet fini et L une partie n-reconnaissable de $A^{<\omega^{n+1}}$. Il existe un n-automate déterministe complet $\mathcal{A}$ tel que $L = \mathcal{L}(\mathcal{A})$.*

Le théorème suivant montre que les combinaisons booléennes de langages n-reconnaissables sont encore n-reconnaissables :

Théorème 2.3.5 *Soient A un alphabet fini, L et L' deux parties n-reconnaissables de $A^{<\omega^{n+1}}$. Alors $L \cup L'$, $L \cap L'$, $L - L'$, $A^{\omega^{<n+1}} - L$, LL' et L^* sont n-reconnaissables, et L^ω est $n+1$-reconnaissable.*

2.3.2 Expressions rationnelles

Les expressions rationnelles sur les mots de longueur inférieure à ω^n sont formées de façon identique à celles sur les mots finis, avec cependant un opérateur unaire supplémentaire, ω, qui est identique à celui qu'on trouve dans les ω-expressions rationnelles, mais qui cette fois-ci est libre comme l'est $*$.

Définition 2.3.6 *Soit un alphabet fini $A = \{a_1, \ldots, a_k\}$. Une C-***expression rationnelle** *sur A est un mot fini sur l'ensemble $A \cup \{+, \cdot, {}^*, {}^\omega, (,), \lambda, \emptyset\}$ tel que :*

- *$\emptyset$ est une C-expression rationnelle,*
- *λ est une C-expression rationnelle,*
- *a est une C-expression rationnelle pour tout $a \in A$,*
- *Si e_1 et e_2 sont des C-expressions rationnelles, alors $e_1 + e_2$ est une C-expression rationnelle,*
- *Si e_1 et e_2 sont des C-expressions rationnelles, alors $e_1 \cdot e_2$ est une C-expression rationnelle, que nous noterons aussi plus simplement $e_1 e_2$,*
- *Si e est une C-expression rationnelle, alors (e) est une C-expression rationnelle,*
- *Si e est une C-expression rationnelle, alors e^* est une C-expression rationnelle,*
- *Si e est une C-expression rationnelle, alors e^ω est une C-expression rationnelle.*

La partie $\overline{e}$ de $A^{<\omega^{n+1}}$ dénotée par une C-expression rationnelle e est définie par induction sur e :

- $\overline{\emptyset} = \emptyset$,
- $\overline{\lambda} = \{\lambda\}$,
- $\overline{a} = \{a\}$ *pour tout* $a \in A$,
- $\overline{e_1 + e_2} = \overline{e_1} \cup \overline{e_2}$,
- $\overline{e_1 \cdot e_2} = \overline{e_1} \cdot \overline{e_2}$,
- $\overline{(e)} = \overline{e}$,
- $\overline{e^*} = \overline{e}^*$,
- $\overline{e^\omega} = \overline{e}^\omega$.

On dit qu'une partie de $A^{<\omega^{n+1}}$ est C-**rationnelle** si elle est définissable par une C-expression rationnelle. Notons que les C-expressions rationnelles qui dénotent des parties de $A^{<\omega^{n+1}}$ ont au plus n comme profondeur d'imbrication des opérateurs ω.

Les C-expressions rationnelles sont équivalentes aux n-automates :

Théorème 2.3.7 ([Cho78]) *Soit A un alphabet fini. Une partie de $A^{<\omega^{n+1}}$ est n-reconnaissable si et seulement si elle est C-rationnelle.*

Exemple 2.3.8 *Le langage reconnu par le 2-automate de l'exemple 2.3.3 est dénoté par la C-expression rationnelle*

$$(((b+aa)^\omega)^\omega)^*((b+aa)^\omega)^*((b+aa)^*b^\omega)^\omega$$

2.4 Mots de longueur dénombrable

Pour un exposé plus détaillé sur la théorie des automates sur les mots de longueur plus petite que ω_1, on renvoie à [BS73].

Tout au long de cette section les mots sont de longueur plus petite que ω_1.

2.4.1 Automates

Nous définissons maintenant des automates qui reconnaissent des mots dont la longueur est un ordinal dénombrable quelconque. Ces automates sont plus éloignés de l'idée de Muller que ceux de Choueka : la seconde fonction de transition (qui permet le passage aux ordinaux limite) n'utilise plus la notion de répétition infinie simple, mais celle de cofinalité, qui est plus naturelle sur les ordinaux. La conséquence immédiate de ce changement d'idée est la modification de la relation de transition, et l'automate n'est plus structuré en $n+1$ "étages" comme l'est un n-automate, mais en 2. Nous prouverons plus tard, dans la section 2.5, que cette modification de la définition de la seconde fonction de transition n'ajoute ni ne retire de puissance aux automates sur les mots dénombrables par rapport aux n-automates en ce qui concerne la définition de langages de mots de longueur plus petite que ω^{n+1}.

Définition 2.4.1 *Un D-**automate** $\mathcal{A}$ est un 5-uplet $< Q, A, E, I, F >$ avec :*
- *Q l'ensemble fini des états,*
- *A un alphabet fini,*
- *$E \subseteq [Q]_0^1 \times A \times Q$ l'ensemble des transitions,*
- *$I \subseteq Q$ l'ensemble des états initiaux,*
- *$F \subseteq [Q]_0^1$ l'ensemble des états finaux.*

L'automate est complet si, pour tout $q \in [Q]_0^1$ et pour toute lettre a, il existe $p \in Q$ tel que $(q, a, p) \in E$. Il est déterministe si p est unique ou n'existe pas, et $|I| = 1$.

Pour définir les chemins nous avons besoin de la définition suivante :

Définition 2.4.2 *Soient E un ensemble non vide, α un ordinal dénombrable et $e = (e_\beta)_{\beta<\alpha}$ une suite d'éléments de $[E]_0^1$. On dit que e est D-**continue** si $e_\beta \in E$ pour tout ordinal successeur β inférieur à α, et pour tout ordinal ξ limite inférieur à α, $e_\xi \in [E]$ et si q est un élément de E alors $q \in e_\xi$ si et seulement si il existe une suite $(\alpha_\beta)_{\beta<\omega}$ strictement croissante d'ordinaux successeurs inférieurs à ξ et cofinale à ξ telle que pour tout β inférieur à ω on ait $e_{\alpha_\beta} = q$.*

Remarquons que les valeurs de e indicées par des ordinaux limite sont entièrement déterminées par celles indicées par les ordinaux successeurs plus petits.

Un **chemin** $c = (q_\beta)_{\beta\leq\alpha}$ d'origine p vers q de longueur $\alpha + 1$ étiqueté par un mot $u = (a_\beta)_{\beta<\alpha}$ est une suite D-continue d'éléments de $[Q]_0^1$ telle que $q_0 = p$, $q_\alpha = q$ et $(q_\beta, a_\beta, q_{\beta+1}) \in E$ pour tout β plus petit que α. Le chemin est acceptant si $p \in I$ et $q \in F$. Le langage $\mathcal{L}(\mathcal{A})$ reconnu par $\mathcal{A}$ est l'ensemble des mots de $A^{<\omega_1}$ qui sont l'étiquette d'un chemin acceptant. Une partie L de $A^{<\omega_1}$ est D-**reconnaissable** s'il existe un D-automate $\mathcal{A}$ tel que $L = \mathcal{L}(\mathcal{A})$.

Par application du théorème 1.4.14 la définition de chemin impose que la longueur d'un mot reconnu par un D-automate soit un ordinal dénombrable.

Nous redonnerons une preuve du théorème suivant basée sur l'utilisation des semi-groupes dans le chapitre 3 :

Théorème 2.4.3 (Büchi) *Soient A un alphabet fini et L une partie D-reconnaissable de $A^{<\omega_1}$. Il existe un D-automate déterministe complet $\mathcal{A}$ tel que $L = \mathcal{L}(\mathcal{A})$.*

Le théorème suivant montre que les combinaisons booléennes de langages D-reconnaissables sont encore D-reconnaissables :

Théorème 2.4.4 (Büchi) *Soient A un alphabet fini, L et L' deux parties D-reconnaissables de $A^{<\omega_1}$. Alors $L \cup L'$, $L \cap L'$, $L - L'$, $A^{<\omega_1} - L$, LL', L^*, L^ω et $L^{<\omega_1}$ sont D-reconnaissables.*

2.4.2 Expressions rationnelles

Les expressions rationnelles sur les mots de longueur dénombrable sont formées de façon identique à celles sur les mots de longueur inférieure à ω, avec cependant un opérateur unaire supplémentaire, $<\omega_1$, qui est une généralisation de l'opérateur $*$ aux ordinaux dénombrables quelconques et non plus seulement finis.

Définition 2.4.5 *Soit un alphabet fini $A = \{a_1, \ldots, a_n\}$. Une* D-**expression rationnelle** *sur A est un mot fini sur l'ensemble $A \cup \{+, \cdot, ^*, ^\omega, ^{<\omega_1}, (,), \lambda, \emptyset\}$ tel que :*

- *$\emptyset$ est une D-expression rationnelle,*
- *λ est une D-expression rationnelle,*
- *a est une D-expression rationnelle pour tout $a \in A$,*
- *Si e_1 et e_2 sont des D-expressions rationnelles, alors $e_1 + e_2$ est une D-expression rationnelle,*
- *Si e_1 et e_2 sont des D-expressions rationnelles, alors $e_1 \cdot e_2$ est une D-expression rationnelle, que nous noterons aussi plus simplement $e_1 e_2$,*
- *Si e est une D-expression rationnelle, alors (e) est une D-expression rationnelle,*
- *Si e est une D-expression rationnelle, alors e^* est une D-expression rationnelle,*
- *Si e est une D-expression rationnelle, alors e^ω est une D-expression rationnelle,*
- *Si e est une D-expression rationnelle, alors $e^{<\omega_1}$ est une D-expression rationnelle.*

La partie $\overline{e}$ de $A^{<\omega_1}$ dénotée par une D-expression rationnelle e est définie par induction sur e :

- $\overline{\emptyset} = \emptyset$,
- $\overline{\lambda} = \{\lambda\}$,
- $\overline{a} = \{a\}$ *pour tout* $a \in A$,
- $\overline{e_1 + e_2} = \overline{e_1} \cup \overline{e_2}$,
- $\overline{e_1 \cdot e_2} = \overline{e_1} \cdot \overline{e_2}$,
- $\overline{(e)} = \overline{e}$,
- $\overline{e^*} = \overline{e}^*$,
- $\overline{e^\omega} = \overline{e}^\omega$,
- $\overline{e^{<\omega_1}} = \overline{e}^{<\omega_1}$.

On dit qu'une partie de $A^{<\omega_1}$ est D-**rationnelle** si elle est définissable par une D-expression rationnelle.

Les D-expressions rationnelles sont équivalentes aux automates de Büchi sur les mots dénombrables :

Théorème 2.4.6 ([Woj85]) *Soit A un alphabet fini. Une partie de $A^{<\omega_1}$ est D-reconnaissable si et seulement si elle est D-rationnelle.*

2.5 Mots de longueur quelconque

Pour un exposé plus détaillé sur la théorie des automates sur les mots de longueur quelconque, on renvoie à [BS73].

2.5.1 Automates

Les longueurs des mots reconnus par D-automate étaient restreintes au dénombrable par le type de la suite de la définition de suite D-continue, qui est un ordinal dénombrable (ω). En supprimant cette restriction on obtient des automates, que nous appellerons B-automates, qui reconnaissent des mots de longueur quelconque. Nous montrerons dans la section 2.6 que les D-automates et B-automates sont équivalents pour ce qui concerne la définition de langages de mots de longueur dénombrable.

La définition formelle de B-automate est identique à celle de D-automate. Nous changeons uniquement la définition des chemins :

Définition 2.5.1 *Soient E un ensemble non vide, α un ordinal et $e = (e_\beta)_{\beta<\alpha}$ une suite d'éléments de $[E]_0^1$. On dit que e est B-**continue** si $e_\beta \in E$ pour tout ordinal successeur β inférieur à α, et pour tout ordinal ξ limite inférieur à α, $e_\xi \in [E]$ et si q est un élément de E alors $q \in e_\xi$ si et seulement si il existe un ordinal limite γ et une suite $(\alpha_\beta)_{\beta<\gamma}$ strictement croissante d'ordinaux successeurs inférieurs à ξ et cofinale à ξ telle que pour tout β inférieur à γ on ait $e_{\alpha_\beta} = q$.*

Remarquons que les valeurs de e indicées par des ordinaux limite sont entièrement déterminées par celles indicées par les ordinaux successeurs plus petits.

Un **chemin** $c = (q_\beta)_{\beta\leq\alpha}$ d'origine p vers q de longueur $\alpha + 1$ étiqueté par un mot $u = (a_\beta)_{\beta<\alpha}$ est une suite B-continue d'éléments de $[Q]_0^1$ telle que $q_0 = p$, $q_\alpha = q$ et $(q_\beta, a_\beta, q_{\beta+1}) \in E$ pour tout β plus petit que α. Le chemin est acceptant si $p \in I$ et $q \in F$. Le langage $\mathcal{L}(\mathcal{A})$ reconnu par $\mathcal{A}$ est l'ensemble des mots de $A^\#$ qui sont l'étiquette d'un chemin acceptant. Si α est un ordinal on note $\mathcal{L}^{<\alpha}(\mathcal{A})$ l'ensemble $\mathcal{L}(\mathcal{A}) \cap A^{<\alpha}$. Une partie L de $A^\#$ est B-**reconnaissable** s'il existe un B-automate $\mathcal{A}$ tel que $L = \mathcal{L}(\mathcal{A})$.

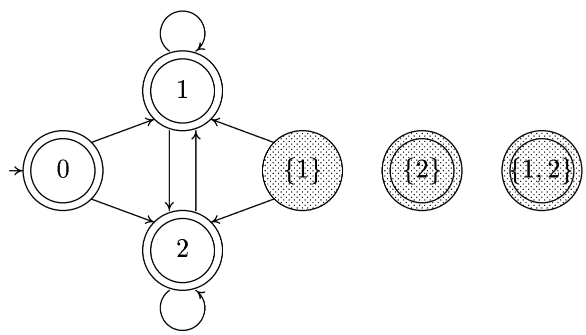
On a le théorème suivant sur la longueur des chemins dans un B-automate. Nous renvoyons à [Woj84] pour une preuve.

Théorème 2.5.2 *Soient $\mathcal{A} =< Q, A, E, I, F >$ un B-automate et p, q deux états de $\mathcal{A}$. S'il existe un chemin dans $\mathcal{A}$ de p vers q, alors il en existe un de longueur appartenant à*

$$\{\alpha = \sum_{i=m}^{0} \omega^i \cdot a_i : (\sum_{i=1}^{m} i \cdot a_i) + a_0 \leq |Q|\}$$

L'exemple suivant montre en particulier, avec le théorème précédent, que le complémentaire d'une partie B-reconnaissable n'est pas nécessairement B-reconnaissable :

Exemple 2.5.3 *Soit $\mathcal{A} =< \{0,1,2\}, \{a\}, E, \{0\}, \{0,1,2,\{2\},\{1,2\}\} >$ le B-automate non déterministe suivant :*



Tous les arcs sont évidemment étiquetés par a. L'automate $\mathcal{A}$ reconnaît tous les mots de longueur dénombrable, mais pas a^{ω_1}. Soit u un mot de longueur α sur $\{a\}$.

Si α est successeur, la suite continue c de type $\alpha + 1$ définie par $c_0 = 0$ et $c_\beta = 1$ pour tout ordinal positif β successeur inférieur à $\alpha + 1$ est bien un chemin dans $\mathcal{A}$ réussi et étiqueté par u puisque pour tout ordinal ξ limite inférieur à $\alpha + 1$ on a $c_\xi = \{1\}$, et d'autre part on a bien $(1, a, 1) \in E$ et $(\{1\}, a, 1) \in E$.

Si α est limite et dénombrable, alors il est la limite d'une suite croissante d'ordinaux $(\beta_n)_{n<\omega}$. Quitte à leur ajouter 1 on peut supposer que tous les éléments de la suite sont successeur. Si on construit une suite continue c de type $\alpha+1$ en posant $c_{\beta_i} = 2$ pour chacun de ces β_i, $c_0 = 0$ et $c_\gamma = 1$ pour les autres ordinaux successeurs inférieurs à $\alpha + 1$, on a nécessairement soit $c_\alpha = \{1,2\}$ soit $c_\alpha = \{2\}$, et on vérifie aisément que c est un chemin réussi d'étiquette u.

Supposons maintenant que $\alpha = \omega_1$ et que $u \in \mathcal{L}(\mathcal{A})$. Soit c un chemin réussi d'étiquette u. Alors, $2 \in c_{\omega_1}$. Soit $\Gamma = \{\gamma < \omega_1 : c_\gamma = 2\}$. Tous les éléments de Γ sont dénombrables, mais Γ lui est indénombrable. Soit γ_0 le plus petit élément de Γ, γ_1 le plus petit élément de Γ plus grand que γ_0,.... Nous pouvons construire ainsi une suite strictement croissante d'ordinaux $(\gamma_i)_{i<\omega}$. La limite β de cette suite est nécessairement un ordinal dénombrable par application du théorème 1.4.14. On a $\beta \in$ Lim et $2 \in c_\beta$. On devrait avoir $(c_\beta, a, c_{\beta+1}) \in E$, ce qui n'est pas le cas. Donc c n'existe pas.

En particulier, il n'y a pas d'analogue du théorème 2.4.3 pour les B-automates.

Cependant, les combinaisons booléennes de langages B-reconnaissables sont encore B-reconnaissables :

Théorème 2.5.4 ([Woj84]) *Soient A un alphabet fini, L et L' deux parties B-reconnaissables de $A^\#$. Alors $L \cup L'$, $L \cap L'$, LL', L^*, L^ω et $L^\#$ sont B-reconnaissables.*

Une autre définition pour les B-automates

Nous démontrons maintenant qu'on peut, dans un B-automate, remplacer les transitions de $[Q] \times A \times Q$ par des transitions de $[Q] \times Q$, ce qui permet de simplifier la définition de chemin : les chemins ne seront plus des suites d'éléments de $[Q]_0^1$ mais de Q. Notons qu'on peut obtenir un résultat similaire pour les D-automates, que nous utiliserons, mais sans l'énoncer, car la preuve est strictement identique au cas des B-automates.

Définition 2.5.5 *Un* **B'-automate** *$\mathcal{A}$ est un 5-uplet $< Q, A, E, I, F >$ avec :*
- *Q l'ensemble fini des états,*
- *A un alphabet fini,*
- *$E \subseteq (Q \times A \times Q) \cup ([Q] \times Q)$ l'ensemble des transitions,*
- *$I \subseteq Q$ l'ensemble des états initiaux,*
- *$F \subseteq Q$ l'ensemble des états finaux.*

On suppose que pour tout $q \in [Q]$ il existe $p \in Q$ tel que $(q, p) \in E$. L'automate est complet si, pour tout $q \in Q$ et lettre a, il existe $p \in Q$ tel que $(q, a, p) \in E$. Il est déterministe si p est unique ou n'existe pas, si pour tout $q \in [Q]$ il existe un unique $p \in Q$ tel que $(q, p) \in E$ et si $|I| = 1$.

Un **chemin** $c = (q_\beta)_{\beta \leq \alpha}$ d'origine p vers q de longueur $\alpha + 1$ étiqueté par un mot $u = (a_\beta)_{\beta < \alpha}$ est une suite d'éléments de Q telle que
- $q_0 = p$,
- $q_\alpha = q$,
- $(q_\beta, a_\beta, q_{\beta+1}) \in E$ pour tout $\beta < \alpha$,
- pour tout ordinal ξ limite inférieur à $\alpha + 1$ il existe $p \in [Q]$ tel que $r \in p$ si et seulement si il existe un ordinal limite γ et une suite $(\alpha_\beta)_{\beta < \gamma}$ strictement croissante d'ordinaux inférieurs à ξ et cofinale à ξ telle que $r = q_{\alpha_\beta}$ pour tout β inférieur à γ, et $(p, q_\xi) \in E$.

Le chemin est acceptant si $p \in I$ et $q \in F$. Le langage $\mathcal{L}(\mathcal{A})$ reconnu par $\mathcal{A}$ est l'ensemble des mots de $A^\#$ qui sont l'étiquette d'un chemin acceptant. Une partie L de $A^\#$ est **B'-reconnaissable** s'il existe un B'-automate $\mathcal{A}$ tel que $L = \mathcal{L}(\mathcal{A})$.

Nous montrons maintenant que toute partie de $A^\#$ est B'-reconnaissable si et seulement si elle est B-reconnaissable.

Théorème 2.5.6 *Soit A un alphabet fini. Une partie de $A^\#$ est B'-reconnaissable si et seulement si elle est B-reconnaissable.*

Preuve Nous commençons par construire un B'-automate à partir d'un B-automate. Soit donc $\mathcal{A} =< Q, A, E, I, F >$ un B-automate et $\mathcal{B} =< Q', A, E', I, F >$ le B'-automate défini par
- $Q' = [Q]_0^1$,

– $E' = E \cup \{(p,q) \in [Q'] \times [Q] : p \cap Q = q\}$.

Observons que $\mathcal{B}$ est déterministe si et seulement si $\mathcal{A}$ l'est. On vérifie facilement que $u \in \mathcal{L}(\mathcal{A})$ si et seulement si $u \in \mathcal{L}(\mathcal{B})$.

Soit maintenant $\mathcal{B} =< Q, A, E, I, F >$ un B'-automate et $\mathcal{A} =< Q', A, E', I, F' >$ le B-automate défini par

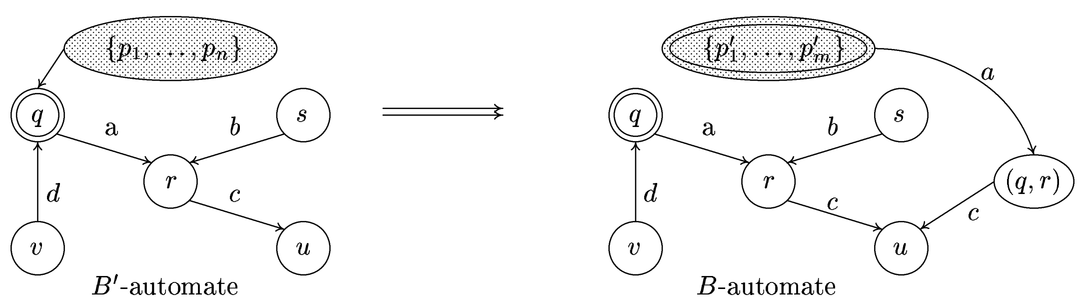
– $Q' = Q \cup Q^2$,

– $E' = \cup \begin{cases} (E - \{(p,q) \in E\}) \\ \{(p, a, (q_1, q_2)) \in [Q'] \times A \times Q^2 : (\mathcal{P}(p), q_1) \in E \text{ et } (q_1, a, q_2) \in E\} \\ \{((p_1, p_2), a, q) \in Q^2 \times A \times Q : (p_2, a, q) \in E\} \end{cases}$

– $F' = \cup \begin{cases} F \cup \{(p_1, p_2) \in Q^2 : p_2 \in F\} \\ \{p \in [Q'] : (\mathcal{P}(p), q) \in E \text{ et } q \in F \text{ pour un } q \in Q\} \end{cases}$

où si $\{p_1, \ldots, p_k\} \in [Q']$ alors $\mathcal{P}(\{p_1, \ldots, p_k\}) = \cup_{i=1\ldots k}\mathcal{P}'(p_i)$ avec $\mathcal{P}'(q) = \{q\}$ si $q \in Q$ et $\mathcal{P}'((q,r)) = \{q, r\}$ si $(q,r) \in Q^2$.

Intuitivement, on passe de $\{p'_1, \ldots p'_m\}$ à (q,r) par lecture de la lettre a dans le B-automate ainsi construit si et seulement si $\{p'_1, \ldots, p'_m\}$ dans lequel les couples (q_1, q_2) ont été remplacés par deux éléments q_1 et q_2 est égal à $\{p_1, \ldots, p_n\}$ et on passe de $\{p_1, \ldots p_n\}$ à r en passant par q dans $\mathcal{B}$ par lecture de la lettre a. La première composante des couples sert donc à mémoriser l'état par lequel on passe dans le B'-automate à partir d'un élément de $[Q]$ sans lire de lettre.



Observons que $\mathcal{A}$ est déterministe si et seulement si $\mathcal{B}$ l'est. On vérifie encore facilement que $u \in \mathcal{L}(\mathcal{A})$ si et seulement si $u \in \mathcal{L}(\mathcal{B})$. ∇

2.5.2 Expressions rationnelles

Les expressions rationnelles sur les mots de longueur quelconque sont formées de façon identique à celles sur les mots de longueur dénombrable, mais l'opérateur unaire $< \omega_1$ est remplacé par $\#$, qui est une généralisation de l'opérateur $< \omega_1$ aux ordinaux quelconques et non plus seulement dénombrables.

Définition 2.5.7 *Soit un alphabet fini $A = \{a_1, \ldots, a_n\}$. Une B-***expression rationnelle** *sur A est un mot fini sur l'ensemble $A \cup \{+, \cdot, ^*, ^\omega, ^\#, (,), \lambda, \emptyset\}$ tel que :*

– *$\emptyset$ est une B-expression rationnelle,*

– *λ est une B-expression rationnelle,*

- *a est une B-expression rationnelle pour tout $a \in A$,*
- *Si e_1 et e_2 sont des B-expressions rationnelles, alors $e_1 + e_2$ est une B-expression rationnelle,*
- *Si e_1 et e_2 sont des B-expressions rationnelles, alors $e_1 \cdot e_2$ est une B-expression rationnelle, que nous noterons aussi plus simplement $e_1 e_2$,*
- *Si e est une B-expression rationnelle, alors (e) est une B-expression rationnelle,*
- *Si e est une B-expression rationnelle, alors e^* est une B-expression rationnelle,*
- *Si e est une B-expression rationnelle, alors e^ω est une B-expression rationnelle,*
- *Si e est une B-expression rationnelle, alors $e^\#$ est une B-expression rationnelle.*

La partie $\overline{e}$ de $A^\#$ dénotée par une B-expression rationnelle e est définie par induction sur e :

- $\overline{\emptyset} = \emptyset$,
- $\overline{\lambda} = \{\lambda\}$,
- $\overline{a} = \{a\}$ *pour tout* $a \in A$,
- $\overline{e_1 + e_2} = \overline{e_1} \cup \overline{e_2}$,
- $\overline{e_1 \cdot e_2} = \overline{e_1} \cdot \overline{e_2}$,
- $\overline{(e)} = \overline{e}$,
- $\overline{e^*} = \overline{e}^*$,
- $\overline{e^\omega} = \overline{e}^\omega$,
- $\overline{e^\#} = \overline{e}^\#$.

On dit qu'une partie de $A^\#$ est B-**rationnelle** si elle est définissable par une B-expression rationnelle.

Les B-expressions rationnelles sont équivalentes aux B-automates :

Théorème 2.5.8 ([Woj85]) *Soit A un alphabet fini. Une partie de $A^\#$ est B-reconnaissable si et seulement si elle est B-rationnelle.*

Exemple 2.5.9 *Soient $\mathcal{A}$ le B-automate de l'exemple 2.5.3, et u un mot sur $\{a\}$ de longueur limite. On vérifie, en employant exactement les mêmes arguments que ceux développés dans l'exemple, que $u \in \mathcal{L}(\mathcal{A})$ si et seulement si $|u|$ est limite d'une suite strictement croissante d'ordinaux de type ω. Comme le mot vide et tout mot de longueur successeur sont acceptés par $\mathcal{A}$, le langage reconnu par $\mathcal{A}$ est dénoté par la B-expression rationnelle*

$$\lambda + a^\# a + (a^\#)^\omega$$

2.6 Equivalences entre automates

Dans cette section nous établissons des relations entre différentes définitions d'automates. Nous prouvons que les B-automates et les n-automates définissent les mêmes langages lorsqu'on se restreint aux mots de longueur inférieure à ω^{n+1}. En utilisant ce résultat, en conjonction avec le théorème 2.3.4, nous obtenons un algorithme qui permet, à partir d'un B-automate $\mathcal{A}$ et d'un entier n, de calculer un B-automate $\mathcal{B}$ déterministe tel que $\mathcal{L}(\mathcal{B}) = \mathcal{L}(\mathcal{A}) \cap A^{<\omega^{n+1}}$.

Commençons cette section sur l'équivalence entre les différents types d'automates en remarquant que les D- et B-automates définissent les mêmes langages lorsqu'on se restreint aux mots de longueur dénombrable.

Théorème 2.6.1 *Soit A un alphabet fini. Si L est un langage D-reconnaissable sur A, alors il existe un B-automate $\mathcal{A}$ tel que $\mathcal{L}^{<\omega_1}(\mathcal{A}) = L$. Réciproquement, si L est un langage B-reconnaissable sur A, alors $L \cap A^{<\omega_1}$ est D-reconnaissable.*

La preuve (élémentaire) du théorème est basée sur le fait qu'un état q apparaît cofinalement à une position limite dénombrable ξ dans un chemin si et seulement si il existe une suite strictement croissante d'ordinaux dénombrables de type ω cofinale à ξ qui indice des apparitions de q dans le chemin, comme le montre le lemme suivant :

Lemme 2.6.2 *Soit ξ un ordinal limite dénombrable. Alors il existe une suite croissante $(\alpha_\beta)_{\beta<\delta}$ d'ordinaux plus petits que ξ et cofinale à ξ si et seulement si il existe une suite croissante $(\alpha'_\beta)_{\beta<\omega}$ d'ordinaux plus petits que ξ et cofinale à ξ.*

Preuve Le sens de la gauche vers la droite est immédiat. Supposons maintenant que $(\alpha_\beta)_{\beta<\delta}$ soit une suite croissante d'ordinaux plus petits que ξ et cofinale à ξ. Alors nécessairement δ est un ordinal limite dénombrable. Par utilisation du théorème 1.4.14 il existe une suite $(\gamma_\tau)_{\tau<\omega}$ strictement croissante d'ordinaux dénombrables telle que $\delta = \lim(\gamma_\tau)_{\tau<\omega}$. Cette suite est cofinale à δ, et la sous-suite croissante $(\alpha_{\gamma_\tau})_{\tau<\omega}$ de $(\alpha_\beta)_{\beta<\delta}$ est cofinale à ξ. ∇

2.6.1 Equivalence entre B-automates et n-automates

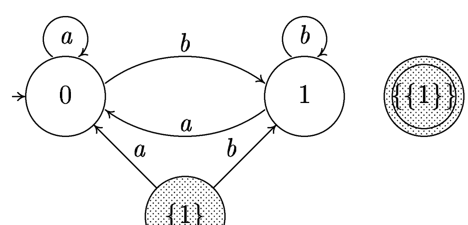
Nous remontrons maintenant que les B-automates sont équivalents aux n-automates en ce qui concerne la définition de langages de mots de longueur inférieure à ω^{n+1}. En utilisant ce résultat en conjonction avec le théorème 2.3.4 on construit à partir d'un B-automate $\mathcal{A}$ un B-automate déterministe $\mathcal{B}$ tel que $\mathcal{L}^{<\omega^{n+1}}(\mathcal{A}) = \mathcal{L}(\mathcal{B})$.

Soit n un entier. Dans cette sous-section le domaine des B-automates est restreint à celui des n-automates, c'est-à-dire qu'on ne s'intéresse qu'aux mots de longueur inférieure à ω^{n+1} dans les langages définis par B-automates.

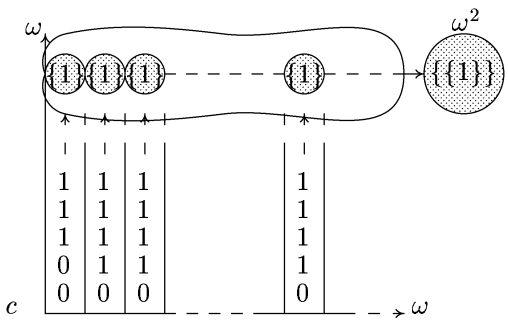
Equivalence entre B-automates et n-automates

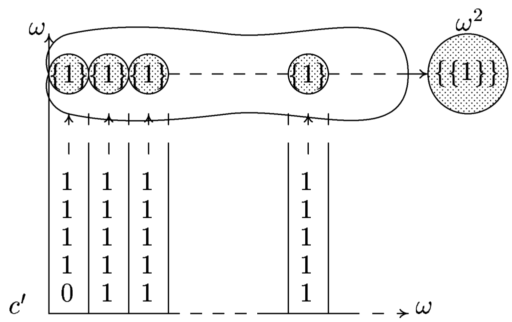
On construit pour commencer un n-automate à partir d'un B-automate. Bien que le formalisme de la construction soit lourd, l'idée est simple, elle est basée sur la remarque qu'il est possible d'exprimer la répétition cofinale d'un état dans un chemin en se servant de la structure en étages des n-automates, ce que nous illustrons par l'exemple suivant :

Exemple 2.6.3 *Soient $A = \{a, b\}$, $u = (ab^\omega)^\omega$, $v = (b^\omega)^\omega$ et $\mathcal{A}$ le 2-automate suivant :*

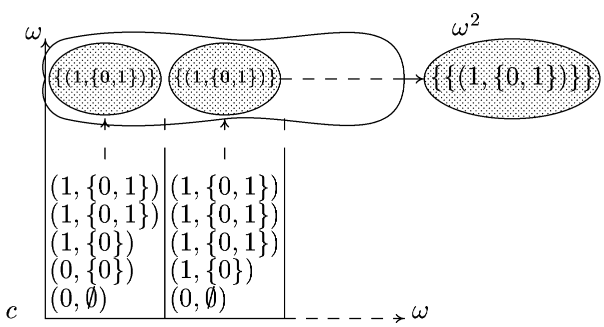


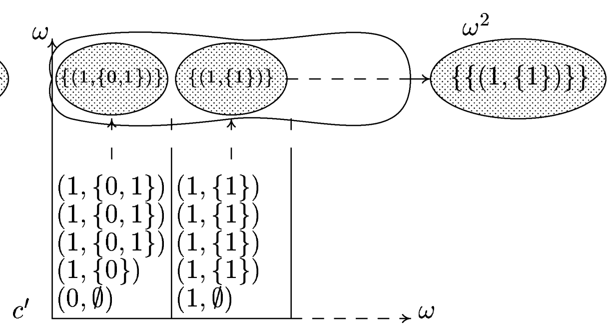
Notons $c = (q_\beta)_{\beta \leq \omega^2}$ (resp. $c' = (q'_\beta)_{\beta \leq \omega^2}$) le chemin de 0 vers $\{\{1\}\}$ d'étiquette u (resp. v) dans $\mathcal{A}$. On schématise les chemins c et c' par les dessins suivants, où chaque suite $(q_{\omega \cdot i+\alpha})_{0<\alpha\leq\omega}$ est représentée verticalement, son plus petit élément étant en bas et le plus grand en haut, et les suites de type ω^2+1 décomposées en ω suites de type $\omega+1$ plus un dernier élément de façon naturelle, la première de ces suites étant la plus à gauche, la suivante immédiatement à droite de cette dernière,...





En supposant que les éléments de $\{0,1\}$ contenus dans $(q_\beta)_{\omega \cdot i \leq \beta < \omega \cdot i+k}$ (resp. $(q'_\beta)_{\omega \cdot i \leq \beta < \omega \cdot i+k}$) aient été mémorisés dans $q_{\omega \cdot i+k}$ (resp. $q'_{\omega \cdot i+k}$) pour chaque entiers i et k, les deux chemins deviennent :





et les "mémoires" (ou, comme nous les appellerons dans la suite, **historiques***) associées à q_{ω^2} et q'_{ω^2} permettent de différencier u et v après lecture de ω^2 lettres. Si $\xi \in Lim$, l'union de la projection d'historiques associés à l'élément d'indice ξ dans un chemin contient exactement les états q tels que $\{\gamma : q_\gamma = q\}$ est cofinal avec ξ. Ceci nous permet de définir les transitions sortantes des états atteints aux positions limites.*

Définition 2.6.4 *Soit E un ensemble fini. On définit la fonction $\mathcal{P} : [E]^n \to [E]$ de mise à plat par $\mathcal{P}(\{q_1,\ldots,q_k\}) = \cup_{i=1}^{k}\mathcal{P}(q_i)$ si $\{q_1,\ldots,q_k\} \in [E]^n$, $n>0$ et $q_1,\ldots,q_k \in [E]^{n-1}$, et $\mathcal{P}(q) = \{q\}$ si $q \in [E]^0$.*

Exemple 2.6.5

$$\mathcal{P}(\{\{q_1,q_2\},\{q_2,q_3\},\{q_4,q_5,q_6\}\}) = \{q_1,q_2,q_3,q_4,q_5,q_6\}$$

Dans la définition suivante on met des indices en place d'exposants :

Définition 2.6.6 *Soit $c = (q_\beta)_{\beta \leq \alpha}$ un chemin dans un n-automate $< Q, A, E, I, F >$ tel que pour tout ordinal β successeur inférieur ou égal à α on ait $q_\beta = (s^\beta, h^\beta_k, \ldots, h^\beta_0)$, avec s^β élément d'un ensemble fini S, $h^\beta_i \in [S] \cup \{\emptyset\}$ pour tout $0 \leq i \leq k$ et $k \in \mathbb{N}$. Comme un chemin est entièrement défini par les valeurs qu'il prend aux positions successeur, on définit la suite c' comme étant l'unique séquence C-continue qui vérifie $c_\beta = (s^\beta, h^\beta_k, \ldots, h^\beta_0)$ si et seulement si $c'_\beta = s^\beta$ pour tout ordinal β successeur inférieur ou égal à α. Le chemin c' ainsi défini est appelé* **projection du chemin c de Q dans S.**

Nous introduisons d'abord quelques définitions élémentaires :

Définition 2.6.7 $\mathcal{R}'(\{(s_1, h^1_n, \ldots, h^1_0), \ldots, (s_k, h^k_n, \ldots, h^k_0)\}) = \{s_1, \ldots, s_k\}$, *où k et n sont des entiers naturels.*

Définition 2.6.8 $\mathcal{R}_k(\{(s_1, h^1_n, \ldots, h^1_0), \ldots, (s_m, h^m_n, \ldots, h^m_0)\}) = \cup^m_{i=1} h^i_k$, *où m, n et k sont des entiers naturels tels que k soit inférieur ou égal à n.*

Définition 2.6.9 $fst((a_1, \ldots, a_n)) = a_1$ *où n est un entier naturel.*

Nous donnons maintenant une construction qui, à partir d'un B-automate $\mathcal{A}$ et d'un entier n, calcule un n-automate $\mathcal{B}$ tel que, comme nous le prouverons par la suite, $\mathcal{L}(\mathcal{B}) = \mathcal{L}^{<\omega^{n+1}}(\mathcal{A})$. Nous supposons que $\mathcal{A}$ possède au plus un état initial. En effet, s'il n'en possède pas, alors $\mathcal{L}(\mathcal{A}) = \emptyset$ et la construction d'un n-automate $\mathcal{B}$ tel que $\mathcal{L}(\mathcal{B}) = \emptyset$ est triviale. Si $\mathcal{A}$ possède exactement un seul état initial, alors on ajoute un nouvel état i à l'automate, on ajoute pour chaque lettre a de l'alphabet une transition sortante de i vers chaque état q tel qu'il existe une transition d'un état initial de $\mathcal{A}$ vers q par a. On pose alors que l'unique état initial de l'automate ainsi construit est i. Il est clair que cet automate reconnaît le même langage que $\mathcal{A}$.

Définition 2.6.10 *Soit $\mathcal{A} =< Q, A, E, \{i\}, F >$ un B-automate. On construit à partir de $\mathcal{A}$ un n-automate $< Q', A, E', \{i'\}, F' >$ de la manière suivante ($m \leq n$) :*

- $Q' = Q \times \underbrace{([Q] \cup \{\emptyset\}) \times \cdots \times ([Q] \cup \{\emptyset\})}_{n-1 \text{ fois}}$.
- $i' = (i, \underbrace{\emptyset, \ldots, \emptyset}_{n-1 \text{ fois}})$.
- *Si $a \in A$, alors $((s, h_{n-2}, \ldots, h_0), a, (s', h'_{n-2}, \ldots, h'_0)) \in E'$ si et seulement si $s \in Q$, $s' \in Q$, $h'_i = h_i \cup \{s\}$ pour tout $i \leq n-2$, et $(s, a, s') \in E$.*
- *Si $a \in A$ et $X \in [Q']^m$, alors $(X, a, (s', h'_{n-2}, \ldots, h'_0)) \in E'$ si et seulement si $s' \in Q$, $h'_i = \emptyset$ pour tout $i < m$, $h'_i = \mathcal{R}_i(\mathcal{P}(X))$ pour tout $i \geq m$ et*
$$\begin{cases} (\mathcal{R}_{m-2}(\mathcal{P}(X)), a, s') \in E & si\ n \geq m > 1 \\ (\mathcal{R}'(X), a, s') \in E & si\ m = 1 \end{cases}$$
- *Si $s' = (s, h_{n-2}, \ldots, h_0) \in Q'$ alors $s' \in F' \iff s \in F$.*
- *Si $X \in [Q']^m$ alors* $X \in F' \iff \begin{cases} \mathcal{R}_{m-2}(\mathcal{P}(X)) \in F & si\ n \geq m > 1 \\ \mathcal{R}'(X) \in F & si\ m = 1 \end{cases}$

*Le n-automate ainsi obtenu à partir d'un B-automate $\mathcal{A}$ sera appelé le $B2C$-***automate** *de $\mathcal{A}$.*

L'idée générale de la construction est de simuler le B-automate de départ. Les états du n-automate ainsi construit sont composés d'un état du B-automate de départ et de $n-1$ historiques. Le n-automate est construit de telle façon que $(p, h_{n-2}, \ldots, h_0)$ est la dernière composante d'un chemin d'étiquette u dans l'automate si et seulement si p est la dernière composante d'un chemin d'étiquette u dans le B-automate de départ. Chaque historique d'indice inférieur à m est remis à zéro après la lecture de chaque préfixe du mot en entrée de l'automate dont la longueur est de la forme $\beta + \omega^m$. L'information accumulée dans les historiques permet, à chaque point limite ξ du chemin, de connaître les états du B-automate répétés cofinalement à ξ, et donc de pouvoir calculer les transitions sortantes de l'état atteint.

Comme montré ci-dessous, l'ajout d'historiques ne modifie en rien la répétition infinie d'un état.

Lemme 2.6.11 *Soient $\mathcal{A} =< Q, A, E, I, F >$ un B-automate et $\mathcal{B}$ le $B2C$-automate de $\mathcal{A}$. Supposons que $\mathcal{B}$ soit un n-automate pour un certain entier n. Soient u un mot de $A^{<\omega^{n+1}}$, $c_1 = (q_{1,\beta})_{\beta \leq \alpha}$ un chemin d'étiquette u dans $\mathcal{B}$, et $c_2 = (q_{2,\beta})_{\beta \leq \alpha}$ la projection de c_1 sur Q. Alors $s \in \mathcal{R}'(\mathcal{P}(q_{1,\beta+\omega^m})) \iff s \in \mathcal{P}(q_{2,\beta+\omega^m})$ pour m entier positif.*

Preuve Par définition de la C-continuité, il suffit de montrer que $s \in \mathcal{R}'(\mathcal{P}(q_{1,\omega^m})) \iff s \in \mathcal{P}(q_{2,\omega^m})$. La suite c_2 étant obtenue par projection de c_1, le sens $\Rightarrow$ est facile. Voyons le sens $\Leftarrow$, par récurrence en deux étapes sur m.

Si $m = 1$, $s \in \mathcal{P}(q_{2,\omega}) \iff s \in q_{2,\omega}$ par définition de P. Donc par définition de la C-continuité $\Gamma = \{\gamma : q_{2,\gamma} = s\}$ est infini. On construit la suite $(\gamma_i)_{i<\omega}$ par γ_0 est le plus petit ordinal de Γ, γ_1 celui qui lui est immédiatement supérieur,.... On a $q_{2,\gamma_j} = s$ si et seulement si il existe $h^j_{n-2}, \ldots, h^j_0$ tels que $q_{1,\gamma_j} = (s, h^j_{n-2}, \ldots, h^j_0)$. Par définition des historiques, si $(q_{1,\beta})_{\beta<\omega} = (s_0, h^0_{n-2}, \ldots, h^0_0), (s_1, h^1_{n-2}, \ldots, h^1_0), \ldots, (s_k, h^k_{n-2}, \ldots, h^k_0), \ldots$ on a $k > k' \Rightarrow \forall i, h^{k'}_i \subseteq h^k_i$, et comme Q est fini à partir d'un certain k_l on a $h^k_i = h^{k_l}_i$ pour tout k supérieur à k_l et i inférieur ou égal à $n-2$. Il vient donc que $\{\gamma : q_{1,\gamma} = (s, h^{k_l}_{n-2}, \ldots, h^{k_l}_0)\}$ est infini et donc par définition de la C-continuité, $(s, h^{k_l}_{n-2}, \ldots, h^{k_l}_0) \in q_{1,\omega} = \mathcal{P}(q_{1,\omega}) \Rightarrow s \in \mathcal{R}'(\mathcal{P}(q_{1,\omega}))$.

Notre hypothèse de récurrence est (1) : $s \in \mathcal{P}(q_{2,\omega^m}) \Rightarrow s \in \mathcal{R}'(\mathcal{P}(q_{1,\omega^m}))$. Montrons que $s \in \mathcal{P}(q_{1,\omega^m \cdot k}) \Rightarrow s \in \mathcal{R}'(\mathcal{P}(q_{1,\omega^m \cdot k}))$ pour tout entier k positif. Si $k = 1$ alors on revient à (1). Supposons $s \in \mathcal{P}(q_{2,\omega^m \cdot k}) \Rightarrow s \in \mathcal{R}'(\mathcal{P}(q_{1,\omega^m \cdot k}))$ et démontrons que (2) :$s \in \mathcal{P}(q_{1,\omega^m \cdot (k+1)}) \Rightarrow s \in \mathcal{R}'(\mathcal{P}(q_{1,\omega^m \cdot (k+1)}))$. On a $\omega^m \cdot (k+1) = \omega^m \cdot k + \omega^m$ or $\omega^m \cdot k > \omega^m$ et donc par la définition de la continuité (2) est vrai si (1) est vrai, et (1) l'est. Donc pour tout entier k positif on a $s \in \mathcal{P}(q_{2,\omega^m \cdot k}) \Rightarrow s \in \mathcal{R}'(\mathcal{P}(q_{1,\omega^m \cdot k}))$.

Montrons maintenant que $s \in \mathcal{P}(q_{2,\omega^{m+1}}) \Rightarrow s \in \mathcal{R}'(\mathcal{P}(q_{1,\omega^{m+1}}))$. Si $s \in \mathcal{P}(q_{2,\omega^{m+1}})$ alors il existe $X \in [Q]^m$ tel que $X \in q_{2,\omega^{m+1}}$ et $s \in \mathcal{P}(X)$ et donc par définition de la continuité $\{k : q_{2,\omega^m \cdot k} = X\}$ est infini, i.e. $\{k : s \in \mathcal{P}(q_{2,\omega^m \cdot k})\}$ est infini et donc par hypothèse de récurrence $\{k : s \in \mathcal{R}'(\mathcal{P}(q_{1,\omega^m \cdot k}))\}$ est infini et donc toujours par définition de la C-continuité $s \in \mathcal{R}'(\mathcal{P}(q_{1,\omega^{m+1}}))$. ∇

Soit E un ensemble et $s = (q_\beta)_{\beta<\omega}$ une suite d'éléments de E. Nous noterons $In(s)$ l'ensemble des éléments de E qui apparaissent infiniment souvent dans s.

Lemme 2.6.12 *Soient A un alphabet, α un ordinal, $u \in A^\alpha$, $\{c_{1,i} : i \in I$ et $c_{1,i} = (q_{i,1,\beta})_{\beta\leq|u|}\}$ l'ensemble des chemins d'étiquette u et d'origine i dans un B-automate $\mathcal{A} =< Q, A, E, \{i\}, F >$ et $\{c_{2,j} : j \in J$ et $c_{2,j} = (q_{j,2,\beta})_{\beta\leq|u|}\}$ l'ensemble des chemins d'étiquette u et d'origine i' dans le $B2C$-automate $\mathcal{A}' =< Q', A, E', \{i'\}, F' >$ de $\mathcal{A}$. Alors pour tout $i \in I$, il existe $j \in J$ (et inversement, pour tout $j \in J$, il existe $i \in I$) tels que :*

- *(A) : Si $\alpha \in Succ$, $fst(q_{j,2,\beta}) = q_{i,1,\beta}$ pour tout ordinal β successeur inférieur ou égal à α.*
- *(B) : Si $\alpha \in Lim$ et si sa décomposition donne $\alpha = \beta + \omega^m$ avec $m > 0$ et $\beta = 0$ ou $\beta \geq \omega^m$, tel que β soit le plus petit possible, alors :*

$$\begin{cases} \mathcal{R}'(q_{j,2,\alpha}) = q_{i,1,\alpha} & si\ m = 1 \\ \mathcal{R}_{m-2}(\mathcal{P}(q_{j,2,\alpha})) = q_{i,1,\alpha} & si\ n \geq m > 1 \end{cases}$$

Preuve Par induction transfinie.

Si $\alpha = 0$, on a $q_{j,2,0} = (i, \emptyset, \ldots, \emptyset)$ et $fst(q_{j,2,0}) = i = q_{i,1,0}$.

Supposons maintenant que le lemme soit vrai pour tout β inférieur ou égal à α, et montrons qu'il l'est aussi pour $\alpha + 1$. L'hypothèse de récurrence nous indique que, pour un B-automate, le $B2C$-automate correspondant et un mot u, s'il y a un chemin dans un des automates pour u, il existe un chemin dans l'autre sur u qui vérifie (A) et (B). Prenons deux tels chemins et prolongeons-les d'une transition chacun par une même lettre. Si $\alpha \in Succ$, $fst(q_{j,2,\alpha}) = q_{i,1,\alpha}$ et par définition du $B2C$-automate $(q_{i,1,\alpha}, u_\alpha, q_{i,1,\alpha+1}) \in E \iff ((q_{i,1,\alpha}, h_{n-2}, \ldots, h_0), u_\alpha, (q_{i,1,\alpha+1}, h_{n-2} \cup \{q_{i,1,\alpha}\}, \ldots, h_0 \cup \{q_{i,1,\alpha}\})) \in E'$, on a donc bien $fst(q_{j,2,\alpha+1}) = q_{i,1,\alpha+1}$. Si $\alpha \in Lim$ et $\alpha = \omega$, par hypothèse de récurrence $\mathcal{R}'(q_{j,2,\alpha}) = q_{i,1,\alpha}$, et par définition de E'

$$\begin{aligned} &(\mathcal{R}'(q_{j,2,\alpha}), u_\alpha, q_{i,1,\alpha+1}) \in E \\ &\qquad\iff (q_{j,2,\alpha}, u_\alpha, (q_{i,1,\alpha+1}, \mathcal{R}_{n-2}(\mathcal{P}(q_{j,2,\alpha})), \ldots, \mathcal{R}_1(\mathcal{P}(q_{j,2,\alpha})), \emptyset) \in E' \end{aligned}$$

et on a bien $fst(q_{j,2,\alpha+1}) = q_{i,1,\alpha+1}$. Si $\alpha = \omega^m$ et $m > 1$, par hypothèse de récurrence $q_{i,1,\alpha} = \mathcal{R}_{m-2}(\mathcal{P}(q_{j,2,\alpha}))$ et par définition de E' $(\mathcal{R}_{m-2}(\mathcal{P}(q_{j,2,\alpha})), u_\alpha, q_{i,1,\alpha+1}) \in E \iff (q_{j,2,\alpha}, u_\alpha, (q_{i,1,\alpha+1}, \mathcal{R}_{n-2}(\mathcal{P}(q_{j,2,\alpha})), \ldots, \mathcal{R}_m(\mathcal{P}(q_{j,2,\alpha})), \emptyset, \ldots, \emptyset)) \in E'$ et encore $fst(q_{j,2,\alpha+1}) = q_{i,1,\alpha+1}$.

Supposons maintenant que $\alpha \in Lim$ et que le lemme soit vrai pour tout ordinal γ inférieur à α, et décomposons α en $\alpha = \beta + \omega^m$ comme dans l'énoncé. On a évidemment $q_{i,1,\alpha} = \{s : \{\gamma : q_{i,1,\gamma} = s\}$ est cofinal avec $\alpha\} = \{s : \{\gamma > \beta : q_{i,1,\gamma} = s\}$ est cofinal avec $\alpha\}$. Cette remarque et la définition de C-continuité des α-séquences nous permet de restreindre notre étude à $\alpha = \omega^m$. Si $\alpha = \omega$, par simple application du lemme précédent, et parce que pour une suite de type ω les définitions de B- et C-continuités sont équivalentes,

on a $\mathcal{R}'(q_{j,2,\alpha}) = q_{i,1,\alpha}$. Examinons maintenant le cas $m > 1$, et supposons que $s \in q_{i,1,\omega^m}$, alors $\{\gamma < \omega^m : q_{i,1,\gamma} = s\}$ est cofinal avec ω^m. Par hypothèse de récurrence, $q_{i,1,\gamma} = s \Rightarrow fst(q_{j,2,\gamma}) = s$ et donc $\{\gamma < \omega^m : fst(q_{j,2,\gamma}) = s\}$ est cofinal avec ω^m, et donc $\Gamma = \{k : \forall l \text{ tel que } n-1 > l \geq m-2 \quad s \in \mathcal{R}_l(\mathcal{P}(q_{j,2,\omega^{m-1}.k}))\}$ est infini puisque les h_i ne sont vidés que quand on transite de $q_{j,2,\omega^{i+1}.k}$ à $q_{j,2,\omega^{i+1}.k+1}$, et qu'on a le lemme précédent. Comme Γ est infini, en utilisant encore une fois le lemme précédent, il vient que $s \in \mathcal{R}_l(\mathcal{P}(q_{j,2,\omega^m}))$ pour tout l tel que $m-2 \leq l < n-1$ et donc en particulier $s \in \mathcal{R}_{m-2}(\mathcal{P}(q_{j,2,\omega^m}))$.
Maintenant la réciproque. Supposons que $s \in \mathcal{R}_{m-2}(\mathcal{P}(q_{j,2,\omega^m}))$. Alors $q_{j,2,\omega^m} = In(c)$ où $c = (q_\beta)_{\beta<\omega}$ est l'unique suite de type ω continue telle que $q_i = q_{j,2,\omega^{m-1}.i}$ pour tout i inférieur à ω, et donc $s \in \mathcal{R}_{m-2}(\mathcal{P}(q_{j,2,\omega^m}))$ implique il existe $X \in [Q]^{m-1}$ tel que $s \in \mathcal{R}_{m-2}(\mathcal{P}(X))$ et $\{k < \omega : q_{j,2,\omega^{m-1}.k} = X\}$ est infini. Comme h_{m-2} n'est vidé que quand on transite de $q_{j,2,\omega^{m-1}.k}$ à $q_{j,2,\omega^{m-1}.k+1}$ et par la définition du remplissage des historiques, on a que $\{k < \omega : \exists\gamma\ \omega^{m-1} \cdot k < \gamma < \omega^{m-1} \cdot (k+1)\ fst(q_{j,2,\gamma}) = s\}$ est infini, et donc par hypothèse de récurrence $\{k < \omega : \exists\gamma\ \omega^{m-1} \cdot k < \gamma < \omega^{m-1} \cdot (k+1)\ q_{i,1,\gamma} = s\}$ est infini, et donc $\{\gamma : q_{i,1,\gamma} = s\}$ est cofinal avec ω^m, d'où $s \in q_{i,1,\omega^m}$. ∇

Lemme 2.6.13 *Soient n un entier, $\mathcal{A} =< Q, A, E, i, F >$ un B-automate et $\mathcal{B} =< Q', A, E', i', F' >$ le B2C-automate de $\mathcal{A}$. Alors $\mathcal{L}(\mathcal{B}) = \mathcal{L}^{<\omega^{n+1}}(\mathcal{A})$.*

Preuve Soient u un mot de longueur α reconnu par $\mathcal{A}$ et $(q_{1,\beta})_{\beta\leq|u|}$ un chemin réussi dans $\mathcal{A}$ étiqueté par u. Nous savons par le lemme précédent qu'il existe un chemin réussi $(q_{2,\beta})_{\beta\leq|u|}$ dans $\mathcal{A}'$ étiqueté par u qui vérifie :

$$\begin{cases} \mathcal{R}'(q_{2,\alpha}) = q_{1,\alpha} & \text{si } m = 1 \\ \mathcal{R}_{m-2}(\mathcal{P}(q_{2,\alpha})) = q_{1,\alpha} & \text{si } n \geq m > 1 \end{cases}$$

Si $\alpha \in Succ$ on a donc $fst(q_{2,\alpha}) = q_{1,\alpha}$ or $q_{1,\alpha} \in F \Rightarrow (q_{1,\alpha}, h_{n-2}, \ldots, h_0) \in F'$ par définition de F' donc u est reconnu par $\mathcal{A}'$. Si $\alpha = \beta + \omega^m$ et $m = 1$ on a $q_{1,\alpha} = \mathcal{R}'(q_{2,\alpha})$ et $\mathcal{R}'(q_{2,\alpha}) \in F \Rightarrow q_{2,\alpha} \in F'$ donc u est reconnu par $\mathcal{A}'$. Si $m > 1$ on a $\mathcal{R}_{m-2}(\mathcal{P}(q_{2,\alpha})) = q_{1,\alpha}$ et $\mathcal{R}_{m-2}(\mathcal{P}(q_{2,\alpha})) \in F \Rightarrow q_{2,\alpha} \in F'$ donc u est reconnu par $\mathcal{A}'$. La réciproque se démontre de façon identique. ∇

Nous pouvons maintenant énoncer le résultat attendu :

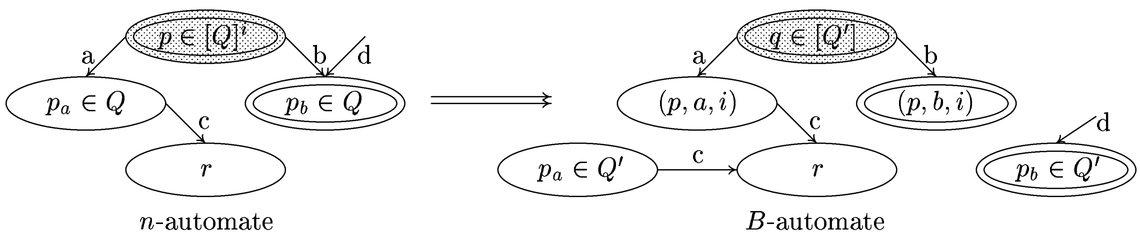
Théorème 2.6.14 (Büchi) *Soient n un entier et $\mathcal{A}$ un B-automate. A partir de $\mathcal{A}$, on peut construire un n-automate $\mathcal{B}$ tel que $\mathcal{L}^{<\omega^{n+1}}(\mathcal{A}) = \mathcal{L}(\mathcal{B})$. Réciproquement, si $\mathcal{A}$ est un n-automate, on peut construire un B-automate $\mathcal{B}$ tel que $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{B})$.*

Preuve Nous venons de montrer la première partie du théorème. Pour l'autre sens, il suffit de remarquer que les expressions C-rationnelles sont également B-rationnelles. ∇

Déterminisation des B-automates

Soit n un entier. Nous venons de donner un algorithme pour construire un n-automate $\mathcal{B}$ en partant d'un B-automate $\mathcal{A}$ tel que $\mathcal{L}^{<\omega^{n+1}}(\mathcal{A}) = \mathcal{L}(\mathcal{B})$. D'après le théorème 2.3.4, on peut construire un n-automate déterministe $\mathcal{C}$ tel que $\mathcal{L}(\mathcal{C}) = \mathcal{L}(\mathcal{B})$. Nous donnons maintenant une construction qui permet, à partir d'un n-automate déterministe, de calculer un B-automate déterministe qui reconnaît le même langage. On en déduira un algorithme qui, à partir de $\mathcal{A}$, permet de calculer un B-automate déterministe $\mathcal{D}$ tel que $\mathcal{L}(\mathcal{D}) = \mathcal{L}^{<\omega^{n+1}}(\mathcal{A})$.

Si on suppose donné un n-automate $\mathcal{A} =< Q, A, E, \{i\}, F >$ déterministe, pour chaque $p \in [Q]_1^n$ la figure suivante explique le principe de la construction :



L'idée maîtresse est de faire transiter chaque élément p de $[Q]^i$ pour chaque $0 < i \leq n$, vers de nouveaux états qui ne seront accessibles qu'immédiatement après le passage par p. Nous appellerons de tels états **états témoins** pour des raisons évidentes. Dans le schéma précédent (p, a, i) et (p, b, i) sont des états témoins du passage par $p \in [Q]^i$. Alors, il faut calculer un équivalent de p pour la définition d'état aux points limites des B-automates.

Définition 2.6.15 *Soit $\mathcal{A} =< Q_A, A, E_A, \{i_A\}, F_A >$ un n-automate déterministe. On construit à partir de $\mathcal{A}$ le B-automate $\mathcal{B} =< Q_B, A, E_B, \{i_B\}, F_B >$ déterministe qui reconnaît le même langage avec l'algorithme qui suit. Comme les automate considérés sont déterministes, afin de simplifier les notations E_A (resp. E_B) est vu non plus comme une relation mais comme une fonction de $[Q_A]_0^n \times A$ (resp. $[Q_B]_0^1 \times A$) dans Q_A (resp. Q_B). Dans l'algorithme la restriction de E_A au domaine $Q_A \times A$ est dénotée par $E_A|_1$.*

$Q_B = Q_A$; $E_B = E_A|_1$; $F_B = F_A \cap [Q_A]_0^1$; $i_B = i_A$

$\forall p \in [Q_A]$ /Définitions de C- et B-continuité coincident pour les suites de type ω/

Pour tout $a \in A$

$q = (p, a, 1)$ nouvel état $\notin Q_B$

$Q_B \leftarrow Q_B \cup \{q\}$

$E_B(p, a) = q$

Pour tout $a' \in A$

$E_B(q, a') = E_A(E_A(p, a), a')$

Si $E_A(p, a) \in F_A$

$F_B \leftarrow F_B \cup \{q\}$

Pour i allant de 2 à n

Pour tout $p \in [Q_A]^i = \{p_1, \ldots p_k\}$

Pour tout $a \in A$

(p, a, i) nouvel état $\notin Q_B$

$Q_B \leftarrow Q_B \cup \{(p, a, i)\}$

Si $E_A(p, a) \in F_A$

$F_B \leftarrow F_B \cup \{(p, a, i)\}$

Pour tout $q \in [Q_B]$ tel que $(\forall j \in [1 \ldots k] \exists r \in q \exists a \in A : r = (p_j, a, i-1))$ $\wedge (\nexists (r, a, i-1) \in q : r \notin p) \wedge (\nexists (r, a, k) : k > i-1))$

Pour tout $a \in A$

$E_B(q, a) = (p, a, i)$

Pour tout $a' \in A$

$E_B((q, a, i), a') = E_A(E_A(p, a), a')$

Si $p \in F_A$

$F_B \leftarrow F_B \cup \{q\}$

Nous appellerons le B-automate ainsi obtenu à partir d'un n-automate déterministe $\mathcal{A}$ le $C2B$-**automate** *de $\mathcal{A}$.*

Afin de montrer que le $C2B$-automate de $\mathcal{A}$ reconnaît le même langage que $\mathcal{A}$ il nous faut deux petits lemmes sur les ordinaux :

Lemme 2.6.16 *Soient α un ordinal limite qui se décompose de façon unique en $\alpha = \beta + \omega^n$, avec $0 < n < \omega$, et r tel que $n \leq r < \omega$. Il n'existe pas d'ensemble d'ordinaux de type r cofinal avec α.*

Preuve La forme normale de α est

$$\alpha = \omega^{i_1} \cdot m_1 + \cdots + \omega^{i_k} \cdot m_k + \omega^{i_{k+1}} \cdot m_{k+1}$$

avec $i_{k+1} = n$ et m_{k+1} positif. Soit γ l'ordinal dont la forme normale est

$$\gamma = \omega^{i_1} \cdot m_1 + \cdots + \omega^{i_k} \cdot m_k + \omega^{i_{k+1}} \cdot (m_{k+1} - 1) + 1$$

Evidemment, γ est inférieur à α. Le plus petit ordinal β de type r plus grand que γ est $\gamma + \omega^r$, et on vérifie aisément que $\beta \geq \alpha$. Il n'existe donc pas d'ordinal β tel que $ty(\beta) = r$ et $\gamma < \beta < \alpha$. ∇

Lemme 2.6.17 *Soient α un ordinal limite inférieur à ω^ω dont la décomposition unique est $\alpha = \beta + \omega^n$, avec $\omega > n > 0$ et Γ un ensemble d'ordinaux de type $n-1$ tous plus petits que α et cofinal avec α. Alors il existe une infinité d'éléments de Γ qui s'écrivent $\beta + \omega^{n-1} \cdot k$, avec $k < \omega$.*

Preuve Puisque Γ est cofinal avec α, pour tout ordinal γ inférieur à α il existe $\delta \in \Gamma$ tel que $\gamma < \delta < \alpha$. D'autre part, $\alpha = \beta + \omega^n$ implique $\beta < \alpha$. Soit $\gamma \in \Gamma$ tel que $\gamma > \beta$. L'ordinal γ s'écrit de façon unique $\gamma = \beta + \omega^{n-1} \cdot k$, avec $0 < k < \omega$, et comme $\gamma < \alpha$ et que Γ est cofinal avec α il existe γ' dans Γ qui vérifie $\gamma' > \gamma$, et de nouveau γ' s'écrit de façon unique $\gamma = \beta + \omega^{n-1} \cdot k'$, $k < k' < \omega$. Comme Γ est cofinal avec α on peut réitérer infiniment la même opération, d'où le lemme. ∇

Lemme 2.6.18 *Soient $\mathcal{A} =< Q_A, A, E_A, \{i_A\}, F_A >$ un n-automate déterministe, $\mathcal{B} =< Q_B, A, E_B, \{i_B\}, F_B >$ le C2B-automate de $\mathcal{A}$, u un mot sur A de longueur inférieure à ω^{n+1}, et $(q_{C,\beta})_{\beta \leq |u|}$ (resp. $(q_{B,\beta})_{\beta \leq |u|}$) le chemin d'étiquette u d'origine i_A (resp. i_B) dans $\mathcal{A}$ (resp. $\mathcal{B}$). Alors suivant α un des trois prédicats suivants est vrai :*

- *(1) $q_{B,\alpha} = \{(p_1, \_, n-1), \ldots, (p_k, \_, n-1)\} \cup P \iff q_{C,\alpha} = \{p_1, \ldots, p_k\}$ si α s'écrit de manière unique $\alpha = \beta + \omega^n$, $n > 0$, $P \subseteq [Q_B]$ ne contenant que des états dont les noms sont des noms d'états de Q_A ou des triplets dont la troisième composante est strictement inférieure à $n-1$, $p_1, \ldots, p_k \in [Q_A]^{n-1}$ et $\_$ désignant n'importe quel élément de A.*
- *(2) $q_{B,\alpha} = (p, a, n) \iff q_{C,\xi} = p$ si $\alpha = \xi + 1$, $ty(\xi) = n$ avec $n > 0$.*
- *(3) $q_{B,\alpha} = q_{C,\alpha}$ autrement.*

Preuve Par induction transfinie sur α.

Si $\alpha = 0$, $q_{B,0} = i_B = i_A = q_{C,0}$.

Soit $\alpha \in Ord$. Supposons le lemme vrai pour α, et montrons qu'il est vrai pour $\alpha + 1$. Si $\alpha \in Lim$ on a (1) et il suit immédiatement (2) par construction. Si $\alpha \in Succ$ on a (2) ou (3). Si (3) alors (3) encore après lecture d'une lettre, car dans ce cas $E_B(q, a) = E_A(q, a)$. Si (2), $\alpha = \xi + 1$, $q_{B,\alpha+1} = E_B(q_{B,\alpha} = (p, u_\xi, ty(\xi)), u_\alpha) = E_A(E_A(q_{C,\xi} = p, u_\xi), u_\alpha) = q_{C,\alpha+1}$ donc (3).

Maintenant, prenons $\alpha \in Lim$, supposons le lemme vrai pour tout $\beta < \alpha$ et essayons d'en déduire le lemme pour α.

Supposons $q_{C,\alpha} = \{p_1, \ldots, p_k\}$. On peut supposer sans perte de généralité que $k = 1$. Posons d'autre part $\alpha = \beta + \omega^n$. Alors, il existe une infinité de k tels que $q_{C,\beta+\omega^{n-1}\cdot k} = p_1$ ce qui signifie que $\{\beta + \omega^{n-1} \cdot k : k < \omega,\ q_{C,\beta+\omega^{n-1}\cdot k} = p_1\}$ est cofinal avec α. Or, par hypothèse de récurrence, $p_1 = q_{C,\beta+\omega^{n-1}\cdot k} \iff q_{B,\beta+\omega^{n-1}\cdot k+1} = (p_1, u_{\beta+\omega^{n-1}\cdot k}, n-1)$ et donc $\{\beta + \omega^{n-1} \cdot k + 1 : q_{B,\beta+\omega^{n-1}\cdot k+1} = (p_1, u_{\beta+\omega^{n-1}\cdot k}, n-1)\}$ est cofinal avec α, car A est fini. De ceci on déduit qu'il existe $a \in A$ tel que $(p_1, a, n-1) \in q_{B,\alpha}$.

Inversement, $(p_1, a, n-1) \in q_{B,\alpha} \Rightarrow \{\gamma < \alpha : q_{B,\gamma} = (p_1, \gamma, n-1)\}$ est cofinal avec α, c'est-à-dire par hypothèse de récurrence que $\Gamma = \{\gamma < \alpha : q_{C,\gamma} = p_1\}$ est cofinal avec α. Comme $p_1 \in [Q_A]^{n-1}$, $ty(\gamma) = n-1$ pour tout $\gamma \in \Gamma$. Par le lemme 2.6.17 il vient que $\{\gamma \in \Gamma : \gamma = \beta + \omega^{n-1} \cdot k, k < \omega, q_{C,\gamma} = p_1\}$ est infini et donc $p_1 \in q_{C,\alpha}$.

Supposons maintenant que $r = (q, a, j) \in q_{C,\alpha}$ avec $j > n - 1$. Alors $\{\gamma < \alpha : q_{B,\gamma} = r\}$ est cofinal avec α, c'est-à-dire par hypothèse de récurrence que $\Gamma = \{\gamma < \alpha : q_{C,\gamma} = q\}$ est cofinal avec α. Comme $q \in [Q_A]^j$, si $\gamma \in \Gamma$ alors $ty(\gamma) = j$, contradiction avec le lemme 2.6.16.

Nous avons montré (1), ceci achève la démonstration du lemme. ∇

Théorème 2.6.19 *Soit $\mathcal{A}$ un n-automate déterministe et $\mathcal{B}$ le $C2W$-automate de $\mathcal{A}$. Alors $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{B})$.*

Preuve Soient $\mathcal{A} =< Q_A, A, E_A, \{i_A\}, F_A >$ un n-automate déterministe et $\mathcal{B} =< Q_B, A, E_B, \{i_B\}, F_B >$ le $C2B$-automate correspondant. Soit u un mot de longueur α tel que $u \in \mathcal{L}(\mathcal{A})$, et $(q_{C,\beta})_{\beta \leq \alpha}$ (resp. $(q_{B,\beta})_{\beta \leq \alpha}$) le chemin d'étiquette u d'origine i_A (resp. i_B) dans $\mathcal{A}$ (resp. $\mathcal{B}$).

Si $\alpha \in Lim$, $\alpha = \beta + \omega^n$, $\omega > n > 0$, soit $q_{C,\alpha} = \{p_1, \ldots, p_k\}$. Par construction, tous les éléments de $[Q_B]$ qui vérifient la condition de la ligne (18) de l'algorithme appartiennent à F_B si $\{p_1, \ldots, p_k\} \in F_A$, or $q_{B,\alpha}$ est un de ces éléments, donc u est reconnu par $\mathcal{B}$. Si maintenant $\alpha = \xi + 1$, $ty(\xi) = n$, $\omega > n > 0$, $u \in \mathcal{L}(\mathcal{A}) \Rightarrow q_{C,\alpha} = E_A(q_{C,\xi}, u_\xi) \in F_A$, par construction $E_A(q_{C,\xi}, u_\xi) \in F_A \Rightarrow (q_{C,\xi}, u_\xi, n) \in F_B$, et comme par le lemme précédent $q_{B,\alpha} = (q_{C,\xi}, u_\xi, n)$, $u \in \mathcal{L}(\mathcal{B})$. Autrement, $q_{C,\alpha} \in F_A$ et comme $F_A \cap [Q_A]_0^1 \subseteq F_B$ et que $q_{C,\alpha} = q_{B,\alpha}$, u est reconnu par $\mathcal{B}$.

La preuve de correction se fait de façon similaire. ∇

Corollaire 2.6.20 *Soient $\mathcal{A}$ un B-automate et n un entier. A partir de $\mathcal{A}$ on peut construire un B-automate déterministe $\mathcal{B}$ tel que $\mathcal{L}^{<\omega^{n+1}}(\mathcal{A}) = \mathcal{L}(\mathcal{B})$.*

Preuve On construit d'abord le $B2C$-automate de $\mathcal{A}$, qu'on déterminise. Soit $\mathcal{C}$ le n-automate obtenu. Le $C2B$-automate de $\mathcal{C}$ est le B-automate déterministe recherché. ∇

Chapitre 3

Semigroupes

Nous allons maintenant définir des ensembles de mots sur un alphabet A en utilisant des morphismes de semigroupes finis. Sur les mots finis, ce formalisme est équivalent aux automates : un langage de mots finis est reconnaissable (par un semigroupe fini) si et seulement si il est rationnel. De plus, un semigroupe fini, le semigroupe syntaxique de L, peut être attaché à tout langage reconnaissable L de mots finis. Les langages reconnaissables peuvent alors être classés par les propriétés algébriques de leur semigroupe syntaxique. Cette idée a été initiée par Schützenberger [Sch65], qui montre qu'un langage de mots finis est sans étoile, c'est-à-dire descriptible par une expression rationnelle dans laquelle la complémentation est autorisée mais l'étoile interdite, si et seulement si son semigroupe syntaxique est fini et apériodique (i.e. ne contient pas de groupes non triviaux). Nous verrons au chapitre suivant que les langages sans étoile forment une sous classe importante des langages rationnels puisque ce sont exactement ceux définissables par des formules de logique du premier ordre de l'ordre linéaire, alors que les langages rationnels sont exactement ceux définis par des formules de logique du second ordre monadique de l'ordre linéaire. Le théorème des variétés d'Eilenberg [Eil76] généralise les idées de Schützenberger.

Les semigroupes sont inadaptés à l'étude des langages rationnels de mots infinis, puisqu'ils n'autorisent pas de produits infinis. Wilke [Wil91], Perrin et Pin [PP97] ont introduits une structure algébrique basée sur les semigroupes dans lesquels des produits de type ω sont autorisés : les ω-semigroupes. Comme pour le cas des mots finis, un langage de mots de longueur ω est reconnaissable (par ω-semigroupe fini) si et seulement si il est ω-rationnel. Il y a un avantage important à utiliser les ω-semigroupes plutôt que les automates pour les langages de mots de longueur ω : on peut associer de façon canonique un ω-semigroupe fini (l'ω-semigroupe syntaxique de L) à chaque langage reconnaissable de mots de longueur ω, ce qui permet d'étendre les résultats de classification de Schützenberger et d'Eilenberg. Le théorème de Schützenberger a été étendu par Perrin [Per84] et celui des variétés par Wilke [Wil91].

Ce chapitre est divisé en cinq sections : les deux premières donnent les principaux résultats sur les mots finis et de longueur ω, la troisième est constituée de définitions dont nous nous servirons dans les suivantes. Dans la quatrième nous introduisons une structure algébrique adaptée à l'étude des mots de longueur inférieure à ω^{n+1}, les ω^n-semigroupes. Nous prouvons que quand ces structures sont finies, elles sont de signature finie et elles reconnaissent exactement les ensembles C-reconnaissables. Nous définissons également la congruence syntaxique associée à chaque langage reconnaissable. Ces résultats sont étendus aux langages de mots de longueur dénombrable dans la cinquième section. En suivant le même plan que dans la précédente, nous commençons par y définir une structure algébrique pour les langages de mots de longueur dénombrable, les ω_1-semigroupes. Nous prouvons ensuite l'équivalence des ω_1-semigroupes finis et des D-automates, en donnant des algorithmes pour passer d'un modèle à l'autre. De cette preuve d'équivalence entre les ω_1-semigroupes finis et D-automates on tire en particulier un algorithme de déterminisation des D-automates, retrouvant ainsi un résultat essentiel de Büchi. La classe des ensembles D-reconnaissable est donc fermée par complémentation. Nous donnons aussi la congruence syntaxique associée à chaque langage reconnaissable, et montrons l'effectivité du calcul de l'ω_1-semigroupe syntaxique d'un langage reconnaissable. Ici s'arrêtent les similitudes entre cette section et la précédente. Les ω_1-semigroupes étant une structure algébrique plus simple que les ω^n-semigroupes, nous définissons dessus deux opérations traditionnelles sur les semigroupes : le produit de Schützenberger et le produit en couronne. Finalement, nous étendons le théorème d'Eilenberg de correspondance entre variétés de langages et pseudo-variétés de semigroupes aux langages de mots de longueur dénombrable.

3.1 Mots finis

Un **semigroupe** est un ensemble muni d'une opération binaire interne associative, qu'on appelle habituellement produit. Par exemple, l'ensemble A^+ des mots sur un alphabet A muni du produit de concaténation des mots est un semigroupe, qu'on appelle le **semigroupe libre** sur A.

La notion de semigroupe est sous-jacente à celle d'automate : en effet, soient A un alphabet et $\mathcal{A}$ un automate qui reconnaît une partie de A^+. L'automate partitionne A^+ en classes d'équivalence de la façon suivante : deux mots u et v sont équivalents si et seulement si, pour tout couple d'états (q, p) de l'automate, u est l'étiquette d'un chemin de q vers p si et seulement si v l'est aussi. Si on appelle S l'ensemble des classes d'équivalence sur les mots ainsi définies et $\varphi : A^+ \to S$ l'application qui à un mot associe sa classe d'équivalence, on peut naturellement munir S d'un produit en posant $\varphi(u)\varphi(v) = \varphi(uv)$. On vérifie facilement que ce produit est associatif, donc S est un semigroupe, qui, de plus, est fini.

Les notions de reconnaissances par automate et par semigroupe fini sont équivalentes pour les langages dont le mot vide est exclu :

Théorème 3.1.1 *Soit A un alphabet fini. Une partie de A^+ est rationnelle si et seulement si elle est reconnue par un semigroupe fini.*

De même qu'à tout langage $*$-reconnaissable on peut associer un automate minimal, on peut aussi lui associer un semigroupe fini canonique :

Théorème 3.1.2 *Soient A un alphabet, L une partie de A^+ et $\sim_L$ la congruence sur A^+ définie par $u \sim_L v$ si et seulement si $xuy \in L \iff xvy \in L$ pour tout mots $x, y \in A^*$. Alors L est reconnaissable si et seulement si $\sim_L$ est d'index fini. De plus, un semigroupe S reconnaît L si et seulement si $A^+/\sim_L$ divise S.*

Le semigroupe $A^+/\sim_L$ est appelé le **semigroupe syntaxique** de L.

L'utilisation de semigroupes finis rend l'étude des langages reconnaissables plus aisée : en effet, ce sont des objets plus simples à manipuler, sans la notion de séquentialité présente dans les automates.

On peut ainsi caractériser les langages reconnaissables par les propriétés algébriques de leur semigroupe syntaxique. Le premier résultat important dans cette voie est dû à Schützenberger :

Définition 3.1.3 *Soit A un alphabet fini. L'ensemble des langages* **sans étoile** *sur A est le plus petit ensemble qui contient $\{a\}$ pour chaque lettre $a \in A$ fermé par les opérations booléennes, où la complémentation est prise par rapport à A^+, et le produit de concaténation, en nombre fini.*

En d'autres termes, les langages sans étoile sont définis par des expressions rationnelles dans lesquelles λ est exclu et l'opérateur $*$ remplacé par la complémentation par rapport à A^+. La classe des langages sans étoile est donc une sous-classe stricte des langages rationnels qui ne contiennent pas le mot vide.

Exemple 3.1.4 *Le langage $(ab)^+$ de $\{a, b\}^+$ est sans étoile, puisque*

$$(ab)^+ = (a\overline{\emptyset} \cap \overline{\emptyset}b) - (\overline{\emptyset}aa\overline{\emptyset} \cup \overline{\emptyset}bb\overline{\emptyset})$$

Un semigroupe S est **apériodique** s'il existe un entier k tel que pour tout $s \in S$ l'égalité $s^k = s^{k+1}$ soit vérifiée.

Théorème 3.1.5 (Schützenberger, 1965 [Sch65]) *Soit A un alphabet fini. Une partie de A^+ reconnaissable est sans étoile si et seulement si son semigroupe syntaxique est apériodique.*

Exemple 3.1.6 *Le langage $L = (b^*aab^*)^+$ sur $A = \{a, b\}$ composé des mots de A^+ qui ont un nombre pair d'occurrences consécutives de la lettre "a" n'est pas sans étoile. En effet, si on note $[u]$ la classe d'équivalence d'un mot u de A^+ pour la congruence $\sim_L$ du théorème 3.1.2, alors $a \not\sim_L a^2$, $[a]^{2k} = [a^2]$ et $[a]^{2k+1} = [a]$. Donc $A^+/\sim_L$ n'est pas apériodique, puisqu'il n'existe pas d'entier k tel que $[a]^k = [a]^{k+1}$.*

C'est Eilenberg qui développa la théorie de la classification des langages reconnaissables par les propriétés algébriques de leur semigroupe syntaxique :

Définition 3.1.7 *Soient S un semigroupe et P une partie de S. Les* **résiduels** *de P sont définis de la façon suivante : si $s \in S$,*

- $s^{-1}P = \{t \in S : st \in P\}$
- $Ps^{-1} = \{t \in S : ts \in P\}$.

Soit A un alphabet et $\boldsymbol{V}$ une pseudo-variété de semigroupes. On note par $A^+\mathcal{V}$ l'ensembles des langages reconnaissables sur A dont le semigroupe syntaxique est dans $\boldsymbol{V}$.

Définition 3.1.8 *Une* **classe de langages reconnaissables** *est une application $\mathcal{C}$ qui à chaque alphabet A associe un ensemble $A^+\mathcal{C}$ de langages reconnaissables sur A.*

Définition 3.1.9 *Une* **variété** *$\mathcal{V}$ de langages est une classe de langages reconnaissables telle que*
- *pour tout alphabet A, $A^+\mathcal{V}$ est fermée par les opérations booléennes,*
- *si $\varphi : A^+ \to B^+$ est un morphisme de semigroupes libres, $L \in B^+\mathcal{V}$ entraîne $\varphi^{-1}(L) \in A^+\mathcal{V}$,*
- *si $L \in A^+\mathcal{V}$ et si $a \in A$, alors $a^{-1}L, La^{-1} \in A^+\mathcal{V}$.*

Théorème 3.1.10 (Eilenberg, 1976 [Eil76]) *L'application qui à chaque pseudo-variété $\boldsymbol{V}$ de semigroupes associe une classe $\mathcal{V}$ de langages reconnaissables est une bijection entre l'ensemble des pseudo-variétés de semigroupes et l'ensemble des variétés de langages.*

Par exemple, la classe des semigroupes finis et apériodiques forme une pseudo-variété de semigroupes, et les langages reconnaissables dont le semigroupe syntaxique est dans cette variété sont exactement les langages sans étoile, qui forment une variété de langage. Pour plus de détails sur les variétés nous renvoyons à [Eil76] et [Pin84]. On peut traiter le cas du mot vide en remplaçant partout dans cette section A^+ par A^*. Les semigroupes contiennent alors un élément neutre et deviennent des **monoïdes**, et les langages sans étoile peuvent contenir le mot vide.

3.2 Mots de longueur ω

Les semigroupes ne sont pas un outil adapté à l'étude des langages reconnaissables de mots de longueur ω : en effet, ces derniers étant le produit d'éléments de suites de type ω de mots finis, il faudrait que les semigroupes soient équipés d'un tel produit. Pécuchet [Péc86a, Péc86b] a fait une première tentative dans l'étude des langages reconnaissables de mots de longueur ω par semigroupes, mais l'introduction de structures algébriques adaptées, les ω-semigroupes et les algèbres de Wilke, est due à Perrin, Pin et Wilke [PP97, Wil91].

Définition 3.2.1 *Un* **ω-semigroupe** *est une algèbre (S_+, S_ω) composée d'un semigroupe S_+ et d'un ensemble S_ω munie*
- *d'une application $S_+ \times S_\omega \to S_\omega$, appelée* **produit mixte**, *qui à un couple (s,t) associe un élément de S_ω noté st,*
- *d'une application $\pi : S_+^\omega \to S_\omega$, appelée* **$\omega$-produit**,

de telle façon que
- *pour tout $s, t \in S_+$ et $u \in S_\omega$, on ait $s(tu) = (st)u$,*

- *pour toute suite strictement croissante d'entiers de type* ω $(k_i)_{i<\omega}$ *et pour toute suite* $(s_i)_{i<\omega}$ *de type* ω *d'éléments de* S_+*, on ait*

$$\pi(s_0 s_1 \dots s_{k_0-1}, s_{k_0} s_{k_0+1} \dots s_{k_1-1}, \dots) = \pi(s_0, s_1, \dots)$$

- *pour toute suite* $(s_i)_{i<\omega}$ *de type* ω *d'éléments de* S_+*, on ait*

$$s_0 \pi(s_1, s_2, \dots) = \pi(s_0, s_1, s_2, \dots)$$

Intuitivement, la structure d'ω-semigroupe permet les produits d'éléments de suites d'éléments de S_+ de type ω, et cela de façon associative, en interdisant toutefois de multiplier à droite un élément de S_ω par un élément de l'ω-semigroupe.

Exemple 3.2.2 *Soit* A *un alphabet. Alors* $S = (A^+, A^\omega)$ *est naturellement muni d'une structure d'*ω*-semigroupe par le produit de deux mots finis, le produit d'une suite de type* ω *de mots finis et le produit d'un mot fini à gauche d'un mot de longueur* ω*. On appelle* S *l'*ω*-semigroupe libre sur* A*.*

Les ω-semigroupes ont cependant un inconvénient majeur : ce ne sont pas des objets finis, puisque la description de l'ω-produit π est infinie, même si l'ω-semigroupe est fini. Wilke a prouvé que quand S_+ est fini, alors l'ω-produit $\pi(s_0, s_1, \dots)$ est entièrement déterminé par ceux de la forme $\pi(s, s, s, \dots)$. En d'autres termes, il suffit de définir explicitement les ω-produits de la forme $\pi(s, s, s, \dots)$ pour les avoir tous définis. Les ω-semigroupes dont les composantes S_+ et S_ω sont finies deviennent ainsi des objets vraiment finis. Ceci justifie l'introduction d'une nouvelle structure algébrique :

Définition 3.2.3 *Une* **algèbre de Wilke** *est une algèbre* (S_+, S_ω) *composée d'un semigroupe* S_+ *fini et d'un ensemble fini* S_ω*, munie*
- *d'une application* $S_+ \times S_\omega \to S_\omega$*, appelée* **produit mixte***, qui à un couple* (s, t) *associe un élément de* S_ω *noté* st *de telle façon que* $s(tu) = (st)u$ *pour tout* $s, t \in S_+$ *et* $u \in S_\omega$*,*
- *d'une application de* S_+ *dans* S_ω*, notée* $s \to s^\omega$*, telle que, pour tout* $s, t \in S_+$*,* $s(ts)^\omega = (st)^\omega$*, et* $(s^n)^\omega = s^\omega$ *pour tout entier* $n > 0$*.*

Les structures d'ω-semigroupe fini et d'algèbre de Wilke sont équivalentes, c'est-à-dire que tout ω-semigroupe fini peut être considéré comme une algèbre de Wilke et réciproquement :

Théorème 3.2.4 *Soit* (S_+, S_ω) *un couple composé d'un semigroupe fini* S_+ *et d'un ensemble fini* S_ω*. Supposons que* (S_+, S_ω) *soit muni d'une structure d'algèbre de Wilke. Alors* (S_+, S_ω) *peut être muni d'une façon unique d'une structure d'*ω*-semigroupe telle que, pour tout* $s \in S_+$*,* $\pi(s, s, s, \dots) = s^\omega$*, et le produit mixte soit conservé. Réciproquement, si* (S_+, S_ω) *est muni d'une structure d'*ω*-semigroupe, alors il peut être muni d'une façon unique d'une structure d'algèbre de Wilke telle que, pour tout* $s \in S_+$*,* $\pi(s, s, s, \dots) = s^\omega$*, et le produit mixte soit conservé.*

Ceci nous permet de confondre algèbres de Wilke et ω-semigroupes finis par la suite.

Soit A un alphabet fini. Les automates sur les mots de longueur ω et les algèbres de Wilke sont équivalents pour la reconnaissance de parties de A^ω :

Théorème 3.2.5 *Soit A un alphabet fini. Une partie de A^ω est ω-rationnelle si et seulement si elle est reconnue par un ω-semigroupe fini.*

Contrairement à ce qui se passe en théorie des automates sur les mots de longueur ω, où il n'y a pas d'automate minimal associé à un langage reconnaissable, à chaque langage ω-reconnaissable L de mots de longueur ω sur un alphabet A on peut associer un ω-semigroupe canonique :

Théorème 3.2.6 *Soient A un alphabet, L une partie reconnaissable de A^ω et $\sim_L$ la congruence sur (A^+, A^ω) définie sur A^+ par $u \sim_L v$ si et seulement si, pour tout mots $x, y \in A^*$ et $z \in A^+$,*

- $xuyz^\omega \in L \iff xvyz^\omega \in L$
- $x(uy)^\omega \in L \iff x(vy)^\omega \in L$

et sur A^ω par $u \sim_L v$ si et seulement si, pour tout mot $x \in A^*$,

$$xu \in L \iff xv \in L$$

Alors $\sim_L$ est d'index fini. De plus, un ω-semigroupe S reconnaît une partie reconnaissable L de A^ω si et seulement si $(A^+, A^\omega)/\sim_L$ divise S.

Si L est une partie reconnaissable de A^ω l'ω-semigroupe $(A^+, A^\omega)/\sim_L$ est appelé l'**ω-semigroupe syntaxique** de L. La définition de la congruence $\sim_L$ associée à un langage de mots de longueur ω est due à Arnold [Arn85].

Ce résultat étend la correspondance de Schützenberger entre les langages sans étoile de mots finis et les semigroupes finis apériodiques aux mots de longueur ω :

Définition 3.2.7 *Soit A un alphabet fini. L'ensemble des langages* **sans étoile** *sur A est le plus petit ensemble qui contient $\emptyset$ fermé par les opérations booléennes, où la complémentation est prise par rapport à A^ω, et par produit à gauche par les parties sans étoile de A^*, en nombre fini.*

Exemple 3.2.8 *Le langage $(ab)^\omega$ de $\{a, b\}^\omega$ est sans étoile, puisque*

$$(ab)^\omega = (a\overline{\emptyset}^{A^\omega}) - (\overline{\emptyset}^{A^*} aa \overline{\emptyset}^{A^\omega} \cup \overline{\emptyset}^{A^*} bb \overline{\emptyset}^{A^\omega})$$

Un ω-semigroupe (S_+, S_ω) est **apériodique** si son semigroupe S_+ est apériodique.

Théorème 3.2.9 (Perrin, 1984 [Per84]) *Un langage reconnaissable de mots de longueur ω est sans étoile si et seulement si son ω-semigroupe syntaxique est apériodique.*

Exemple 3.2.10 *Le langage $L = (b^*aab^*)^\omega$ sur $A = \{a, b\}$ n'est pas sans étoile. En effet, si on note $[u]$ la classe d'équivalence d'un mot u de A^+ pour la congruence $\sim_L$ du théorème 3.2.6, alors $a \not\sim_L a^2$, $[a]^{2k} = [a^2]$ et $[a]^{2k+1} = [a]$. Donc $(A^+, A^\omega)/\sim_L$ n'est pas apériodique, puisqu'il n'existe pas d'entier k tel que $[a]^k = [a]^{k+1}$.*

Pécuchet [Péc86a, Péc86b] a fait un premier pas dans l'extension de la théorie des variétés d'Eilenberg aux langages reconnaissables de mots de longueur ω, mais les résultats que nous présentons ici sont dus à Wilke [Wil91, Wil93]. Soulignons que par définition, un morphisme dω-semigroupe permet de reconnaître à la fois des ensembles de mots finis et de longueur ω. L'extension de Wilke du théorème d'Eilenberg porte sur les parties reconnaissables (par morphisme d'ω-semigroupes) de $A^+ \cup A^\omega$ (on ne peut étendre le théorème d'Eilenberg aux mots de longueur ω sans considérer aussi les mots finis).

Définition 3.2.11 *Soient $S = (S_+, S_\omega)$ un ω-semigroupe et P une partie de S. On définit les* **résiduels** *de P de manière similaire au cas des mots finis : si $s \in S_+$,*

- $s^{-1}P = \{t \in S : st \in P\}$
- $Ps^{-\omega} = \{t \in S_+ : (ts)^\omega \in P\}$

et si $s \in S_\omega$,

$$Ps^{-1} = \{t \in S_+ : ts \in P\}.$$

Soit A un alphabet et $\boldsymbol{V}$ une pseudo-variété d'ω-semigroupes. On note par $A^\infty\mathcal{V}$ l'ensembles des parties de $A^\infty = A^+ \cup A^\omega$ reconnaissables dont l'ω-semigroupe syntaxique est dans $\boldsymbol{V}$.

Définition 3.2.12 *Une* **classe de langages reconnaissables** *est une application $\mathcal{C}$ qui à chaque alphabet A associe un ensemble $A^\infty\mathcal{C}$ de parties de A^∞ reconnaissables.*

Définition 3.2.13 *Une* **variété** *$\mathcal{V}$ de langages est une classe de langages reconnaissables telle que*

- *pour tout alphabet A, $A^\infty\mathcal{V}$ est fermée par les opérations booléennes,*
- *si $\varphi : A^\infty \to B^\infty$ est un morphisme d'ω-semigroupes libres, $L \in B^\infty\mathcal{V}$ entraîne $\varphi^{-1}(L) \in A^\infty\mathcal{V}$,*
- *si $L \in A^\infty\mathcal{V}$ et si $u \in A^*$, alors $u^{-1}L, Lu^{-\omega} \in A^\infty\mathcal{V}$ et si $u \in A^\omega$ alors $Lu^{-1} \in A^\infty\mathcal{V}$.*

Théorème 3.2.14 (Wilke, 1993 [Wil93]) *L'application qui associe à chaque pseudo-variété $\boldsymbol{V}$ d'ω-semigroupes une classe $\mathcal{V}$ de langages reconnaissables est une bijection entre l'ensemble des pseudo-variétés d'ω-semigroupes et l'ensemble des variétés de langages.*

Par exemple, la classe des ω-semigroupes finis et apériodiques forme une pseudo-variété de ω-semigroupes, et les langages dont le ω-semigroupe syntaxique est dans cette variété sont exactement les langages sans étoile, qui forment une variété de langage. Pour plus de détails sur les variétés nous renvoyons à [Wil93] et [PP97].

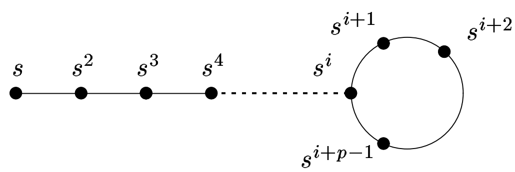
3.3 Définitions avancées

Dans cette section nous donnons des définitions techniques et des résultats classiques (ou des adaptations de résultats classiques) qui serviront par la suite.

On commence par rappeler quelques définitions de base : Un **monoïde** est un semigroupe équipé d'un élément neutre pour le produit, généralement noté 1. Si S est un semigroupe, on note S^1 le monoïde $S \cup \{1\}$ si S n'est pas un monoïde, S sinon. Un sous ensemble I d'un semigroupe S est un **idéal** de S si $S^1 I S^1 = I$. Un élément e d'un semigroupe est dit **idempotent** si $e^2 = e$.

Proposition 3.3.1 *Tout élément d'un semigroupe fini a une puissance idempotente.*

Preuve Soient S un semigroupe fini, $s \in S$, et $T = \{s, s^2, s^3, \dots\}$ le sous-semigroupe de S engendré par S. Comme S est fini, il existe deux entiers positifs i et p tels que $s^i = s^{i+p}$ pour tout entier k. Si i et p sont minimaux, alors i est appelé l'**indice** de s et p sa **période**. La structure multiplicative de S est donnée par le schéma suivant :



Le sous-semigroupe $\{s^i, s^{i+1}, \dots, s^{i+p-1}\}$ de T est alors un groupe isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et contient donc un idempotent, qui de plus est unique. ∇

Si S est un semigroupe fini, le plus petit entier π tel que s^π soit un idempotent pour tout $s \in S$ est appelé l'**exposant** de S.

Soient S un semigroupe fini et s_1, s_2 deux éléments de S. Les quatre préordres (relations réflexives et transitives) suivants, permettent l'étude de la structure multiplicative de S :

$$\begin{aligned}
s_1 \leq_{\mathcal{J}} s_2 &\iff S^1 s_1 S^1 \subseteq S^1 s_2 S^1 \\
s_1 \leq_{\mathcal{R}} s_2 &\iff s_1 S^1 \subseteq s_2 S^1 \\
s_1 \leq_{\mathcal{L}} s_2 &\iff S^1 s_1 \subseteq S^1 s_2 \\
s_1 \leq_{\mathcal{H}} s_2 &\iff s_1 \leq_{\mathcal{R}} s_2 \text{ et } s_1 \leq_{\mathcal{L}} s_2
\end{aligned}$$

En d'autres termes, $s_1 \leq_{\mathcal{J}} s_2$ si et seulement si il existe $t_1, t_2 \in S^1$ tel que $s_1 = t_1 s_2 t_2$, $s_1 \leq_{\mathcal{R}} s_2$ si et seulement si il existe $t \in S^1$ tel que $s_1 = s_2 t$, et $s_1 \leq_{\mathcal{L}} s_2$ si et seulement si il existe $t \in S^1$ tel que $s_1 = t s_2$.

On tire de ces quatre préordres les quatre relations d'équivalence suivantes, appelées **relations de Green** :

$$\begin{array}{rcl} s_1 \mathcal{J} s_2 & \Longleftrightarrow & s_1 \leq_{\mathcal{J}} s_2 \text{ et } s_2 \leq_{\mathcal{J}} s_1 \\ s_1 \mathcal{R} s_2 & \Longleftrightarrow & s_1 \leq_{\mathcal{R}} s_2 \text{ et } s_2 \leq_{\mathcal{R}} s_1 \\ s_1 \mathcal{L} s_2 & \Longleftrightarrow & s_1 \leq_{\mathcal{L}} s_2 \text{ et } s_2 \leq_{\mathcal{L}} s_1 \\ s_1 \mathcal{H} s_2 & \Longleftrightarrow & s_1 \leq_{\mathcal{H}} s_2 \text{ et } s_2 \leq_{\mathcal{H}} s_1 \end{array}$$

En particulier, $s_1 \mathcal{H} s_2$ si et seulement si $s_1 \mathcal{R} s_2$ et $s_1 \mathcal{L} s_2$.

Les relations $\mathcal{R}$ et $\mathcal{L}$ commutent. Nous définissons une cinquième relation de Green $\mathcal{D}$ par $\mathcal{D}$=$\mathcal{RL}$=$\mathcal{LR}$, c'est-à-dire que $s_1 \mathcal{D} s_2$ si et seulement si il existe $t \in S$ tel que $s_1 \mathcal{R} t \mathcal{L} s_2$, ou bien encore de façon équivalente $s_1 \mathcal{D} s_2$ si et seulement si il existe $t \in S$ tel que $s_1 \mathcal{L} t \mathcal{R} s_2$.

Proposition 3.3.2 *Dans un semigroupe fini, $\mathcal{D}$=$\mathcal{J}$.*

Si $\mathcal{K} \in \{\mathcal{D}, \mathcal{R}, \mathcal{L}, \mathcal{H}\}$, alors une classe d'équivalence pour $\mathcal{K}$ est appelée une **$\mathcal{K}$-classe**. La $\mathcal{K}$-classe d'un élément s de S est notée $\mathcal{K}(s)$. Un semigroupe est **$\mathcal{K}$-trivial** si et seulement si $s_1 \mathcal{K} s_2$ implique $s_1 = s_2$.

Voici une caractérisation des semigroupes finis apériodiques :

Théorème 3.3.3 *Un semigroupe fini est apériodique si et seulement si il est $\mathcal{H}$-trivial.*

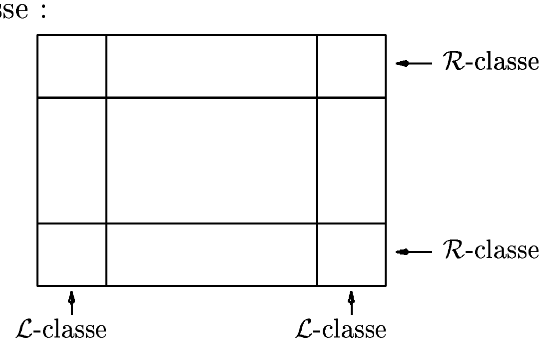
Les trois résultats suivants sont des classiques de la théorie des semigroupes :

Proposition 3.3.4 *Une $\mathcal{H}$-classe de S qui contient un idempotent e est un groupe d'élément neutre e.*

Proposition 3.3.5 *Soit S un semigroupe, et e, e' deux idempotents de S. Alors $e \mathcal{D} e'$ si et seulement si il existe $x, y \in S$ tels que $e = xy$ et $e' = yx$.*

Proposition 3.3.6 *Soit S un semigroupe, et s, s' deux éléments de S tels que $s \mathcal{D} s'$. Alors $ss' \in \mathcal{R}(s) \cap \mathcal{L}(s')$ si et seulement si $\mathcal{R}(s') \cap \mathcal{L}(s)$ contient un idempotent.*

Une $\mathcal{D}$-classe est traditionnellement représentée par une "boîte à œufs", dans laquelle chaque colonne est une $\mathcal{L}$-classe, chaque ligne une $\mathcal{R}$-classe et chaque intersection de ligne et de colonne une $\mathcal{H}$-classe :



On indique la présence d'un idempotent dans une $\mathcal{H}$-classe par une étoile.

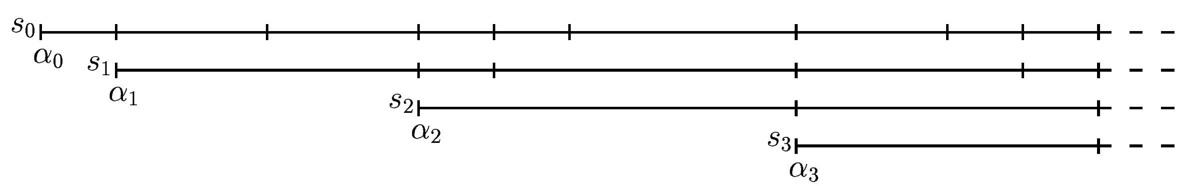
Nous renvoyons au chapitre 3 de [Pin84] pour plus de détails sur les relations de Green, et sur la représentation des semigroupes finis par leur structure en $\mathcal{D}$-classes.

Un couple (s, e) d'éléments d'un semigroupe est **lié** si $se = s$ et e est un idempotent.

La théorie des semigroupes qui reconnaissent des ensembles de mots de longueur infinie est basée sur le théorème suivant, qui est une application d'un théorème plus général dû à Ramsey :

Théorème 3.3.7 (Ramsey) *Soient A un alphabet, S un semigroupe fini, $\varphi : A^{[1,\omega_1[} \to S$ un morphisme de semigroupe qui à chaque mot non vide de longueur dénombrable sur A associe un élément de S et u un mot sur A dont la longueur est un ordinal limite dénombrable. Alors il existe une suite $(u_i)_{i<\omega}$ de mots sur A et un couple lié (s, e) d'éléments de S tels que $u = \prod_{i<\omega} u_i$, $\varphi(u_0) = s$ et $\varphi(u_i) = e$ pour tout entier i positif.*

Preuve Posons $\xi = |u|$. D'abord, nous construisons une suite $(v_i)_{i<\omega}$ de mots telle que $u = \prod_{i<\omega} v_i$, $\varphi(v_0) = r$ et $\varphi(v_i) = t$ pour tout entier i positif, pour deux éléments r et t de S. Pour cela, on fabrique une suite de triplets $(s_i, \alpha_i, U_i) \in S \times \xi \times [\xi]$ de type ω. Nous expliquons d'abord la construction de $(s_{i+1}, \alpha_{i+1}, U_{i+1})$ à partir de (s_i, α_i, U_i), et nous verrons ensuite le cas de base. Supposons (s_i, α_i, U_i) connu. On prend $\alpha_{i+1} = min(U_i - \{\alpha_i\})$. Comme S est fini, il existe $s \in S$ tel qu'il existe une infinité d'éléments $\beta > \alpha_{i+1}$ de U_i tels que $\varphi(u[\alpha_{i+1}, \beta[) = s$. On prend alors $s_{i+1} = s$ et U_{i+1} l'ensemble de tels β, auquel on ajoute α_{i+1}. Le triplet (s_0, α_0, U_0) est choisi de la même manière, mais sans employer l'hypothèse de récurrence : les éléments de U_0 sont pris dans ξ de façon à former une suite de type ω cofinale à ξ et on pose $\alpha_0 = 0$. La situation est résumée par le schéma suivant :



Puisque S est fini, il existe une suite d'entiers $(i_j)_{j<\omega}$ telle que $s_{i_j} = s_{i_k}$ quel que soient les entiers j et k. Posons $t = s_{i_0}$, $v_{j+1} = u[\alpha_{i_j}, \alpha_{i_{j+1}}[$ pour tout entier j, $v_0 = u[0, \alpha_{i_0}[$ et $r = \varphi(v_0)$. Par construction de la suite, $\varphi(v_{i+1}) = t$ pour tout entier i, et $u = \prod_{i<\omega} v_i$. Maintenant, par utilisation de la proposition 3.3.1, t a une puissance idempotente $e = t^k$. Pour obtenir le découpage de u souhaité dans l'énoncé du théorème, il suffit de poser $u_0 = v_0 v_1 \ldots v_k$ et $u_{i+1} = \prod_{j=k(i+1)+1}^{k(i+2)} v_j$ pour tout entier i. ∇

Notons qu'il n'est pas nécessaire que l'alphabet soit fini dans l'énoncé du précédent théorème. Il en découle en particulier que

Corollaire 3.3.8 *Soient A un alphabet, S un semigroupe fini, $\varphi : A^{[1,\omega_1[} \to S$ un morphisme de semigroupe, u un mot sur A dont la longueur est un ordinal limite dénombrable,* *et $(u_i)_{i<\omega}$ une suite de mots sur A telle que $u = \prod_{i<\omega} u_i$. Alors il existe une suite strictement croissante d'entiers $(j_k)_{k<\omega}$ et un couple lié (s,e) de S tels que $j_0 = 0$, $\varphi(\prod_{i=j_0}^{j_1-1} u_i) = s$ et $\varphi(\prod_{i=j_k}^{j_{k+1}-1} u_i) = e$ pour tout entier k positif.*

Preuve Soient B l'alphabet dont les lettres sont les mots de $A^{[1,\omega_1[}$, et $\psi : B^+ \to A^{[1,\omega_1[}$ le morphisme de semigroupe défini par $\psi(u) = u$. Le résultat vient alors directement de l'application du théorème précédent au morphisme $\varphi\psi : B^+ \to S$ et au mot $u_0u_1u_2\ldots$ (de longueur ω) sur B, puisque $\varphi\psi(u) = \varphi(u)$. ∇

Le couple lié (s,e) associé à un mot de longueur limite dénombrable par le théorème 3.3.7 n'est pas unique. Les couples solution sont reliés entre eux par une relation d'équivalence, la relation de conjugaison :

Définition 3.3.9 *Soient S un semigroupe fini, (s,e) et (s',e') deux couples liés de S. On dit que (s,e) et (s',e') sont* **conjugués** *s'il existe $x,y \in S^1$ tels que $e = xy$, $e' = yx$ et $s' = sx$.*

Comme $s'y = sxy = se = s$ la définition précédente est symétrique.

Proposition 3.3.10 *La relation de conjugaison est une relation d'équivalence.*

On peut donner une définition équivalente, mais plus technique, de la relation de conjugaison :

Proposition 3.3.11 *Deux couples liés (s,e) et (s',e') sont conjugués si et seulement si il existe $x \in S^1$ tel que $s' = sx$, $xe' \mathcal{R} e$ et $e \mathcal{D} e'$.*

Pour une preuve nous renvoyons à [PP97].

Théorème 3.3.12 *Soient A un alphabet, S un semigroupe fini, $\varphi : A^{[1,\omega_1[} \to S$ un morphisme de semigroupes surjectif, (s,e) et (s',e') deux couples liés de S. Les couples (s,e) et (s',e') sont conjugués si et seulement si $\varphi^{-1}(s)\varphi^{-1}(e)^\omega \cap \varphi^{-1}(s')\varphi^{-1}(e')^\omega \neq \emptyset$.*

3.4 Mots de longueur inférieure à ω^n

Un ω-semigroupe (S_+, S_ω) ne permet pas de reconnaître des mots de longueur supérieure à ω, car le produit à droite d'un élément de S_ω n'est pas défini. On remédie à ceci en munissant le couple (S_+, S_ω) d'un produit qui fait de $S_+ \cup S_\omega$ un semigroupe. La structure algébrique ainsi obtenue permet de reconnaître des mots de longueur inférieure à ω^2. Si on y ajoute un ensemble S_{ω^2}, une application $(S_+ \cup S_\omega) \times S_{\omega^2} \to S_{\omega^2}$ et une application $\pi' : S_\omega^\omega \to S_{\omega^2}$ respectivement similaires au produit mixte et à l'application $\pi : S_f^\omega \to S_\omega$ qui équipent l'ω-semigroupe (S_+, S_ω), alors la structure obtenue permet de reconnaître des mots de longueur ω^3. Dans cette section nous développons cette idée pour obtenir des structures algébriques, les ω^n-semigroupes, qui reconnaissent des mots de longueur inférieure à ω^{n+1} pour un entier n fixé. Notons une nuance dans la nomenclature : les

ω-semigroupes permettent de reconnaître des ensembles de mots de longueur au plus ω, alors que les ω^n-semigroupes permettent de reconnaître des ensembles de mots de longueur inférieure à ω^{n+1}.

3.4.1 Définitions algébriques

Soit n un entier. La structure algébrique adaptée à l'étude des langages reconnaissables de mots de longueur inférieure à ω^{n+1} que nous proposons maintenant est un semigroupe dans lequel certains produits d'α éléments, où α est un ordinal inférieur à ω^{n+1}, sont autorisés. L'associativité des produits finis d'éléments d'un semigroupe est étendue à ces produits : la valeur d'un produit d'α éléments ne dépend pas de la façon dont il est calculé. De plus, ces structures sont graduées, comme le sont les C-automates, limitant ainsi la longueur des mots qu'elles reconnaissent : elles sont partitionnées en $n+1$ sous-semigroupes $S_0, \dots, S_n$ de telle façon que si $s \in S_i$ et $t \in S_j$, alors $st \in S_{\max(i,j)}$. De plus, le produit d'ω éléments de S_i est un élément de S_{i+1} si i est inférieur à n, n'est pas défini sinon. L'intuition est qu'un mot dont la longueur est comprise dans l'intervalle $[\omega^i, \omega^{i+1}[$ est envoyé par morphisme dans S_i.

Dans la définition suivante nous notons les suites en en énumérant les éléments séparés par une virgule pour plus de clarté. Cette notation sera encore utilisée par la suite.

Définition 3.4.1 *Soit n un entier naturel. Un ω^n-***semigroupe** *S est un ensemble muni d'une fonction ψ de domaine l'ensemble des suites d'éléments de S de type inférieur à ω^{n+1} et de codomaine S, de telle façon que*

1. *en identifiant une suite composée d'un unique élément s à s lui-même, $\psi(s) = s$ pour tout $s \in S$,*
2. *si α est un ordinal inférieur à ω^{n+1}, $(s_\beta)_{\beta<\alpha}$ une suite d'éléments de S, alors pour toute suite strictement croissante d'ordinaux $(\gamma_\delta)_{\delta<\delta_l}$ telle que $\gamma_0 = 0$ et avec $\delta_l \le \alpha$,*

$$\psi(s_0, s_1, \dots) = \psi(\psi(s_{\gamma_0}, s_{\gamma_0+1}, \dots), \psi(s_{\gamma_1}, s_{\gamma_1+1}, \dots), \psi(s_{\gamma_2}, s_{\gamma_2+1}, \dots), \dots)$$

3. *S, qui est alors muni d'une structure de semigroupe, est partionné en $n+1$ sous-semigroupes $S_0, S_1, \dots, S_n$,*
4. *$\cup_{i\le j} S_i$ est un semigroupe d'idéal S_j quel que soit j inférieur ou égal à n,*
5. *si $s = (s_k)_{k<\omega}$ est une suite d'éléments de S_i, alors $\psi(s) \in S_{i+1}$ si $i < n$, et n'est pas défini sinon.*

Le **type** *d'un élément s de S, noté $ty(s)$, est l'unique m tel que $s \in S_m$.*

Exemple 3.4.2 *Si A est un alphabet, alors $A^{[1,\omega^{n+1}[}$ muni du produit de mots a une structure d'ω^n-semigroupe : A_0 est alors l'ensemble $A^{[1,\omega[}$ des mots finis non vides, $A_1 = A^{[\omega,\omega^2[}$,…,$A_i = A^{[\omega^i,\omega^{i+1}[}$ pour $i \le n$. On appelle $A^{[1,\omega^{n+1}[}$ le ω^n-semigroupe libre sur A.*

Comme pour le cas des ω-semigroupes, la définition des ω^n-semigroupes n'est pas satisfaisante car la présence de ψ en font des objets de signature infinie. Nous allons, en plusieurs étapes, montrer que les ω^n-semigroupes dont l'ensemble de support est fini sont équivalents à des structures algébriques qui elles sont de signature finie. Les arguments que nous utiliserons seront similaires à ceux employés pour montrer l'équivalence entre ω-semigroupes finis et algèbres de Wilke.

Nous commençons par donner une autre définition pour les ω^n-semigroupes, dont nous allons montrer qu'elle est équivalente à la précédente.

Définition 3.4.3 *Soit n un entier naturel. Un* $\overline{\omega^n}$**-semigroupe** *S est un semigroupe partitionné en $n+1$ sous-semigroupes $S_0, \ldots, S_n$ tels que $\cup_{i \leq j} S_i$ soit un semigroupe d'idéal S_j quel que soit j inférieur ou égal à n, et équipé d'une famille de n ω-produits $\overline{\pi}_i : S_i^\omega \to S_{i+1}$ pour i inférieur à n tels que*

- *pour chaque suite strictement croissante d'entiers $(k_n)_{n>0}$ et toute suite $(s_n)_{n<\omega} \in S_i^\omega$*

$$\overline{\pi}_i(s_0 s_1 \ldots s_{k_1-1}, s_{k_1} s_{k_1+1} \ldots s_{k_2-1}, \ldots) = \overline{\pi}_i(s_0, s_1, s_2, \ldots)$$

- *pour chaque $s \in S_i$ et chaque suite $(s_n)_{n<\omega} \in S_i^\omega$*

$$s\overline{\pi}_i(s_0, s_1, \ldots) = \overline{\pi}_i(s, s_0, s_1, \ldots)$$

Lemme 3.4.4 *Soit S un ensemble muni des opérations de la définition 3.4.3 qui en font un $\overline{\omega^n}$-semigroupe. Alors S peut être muni d'une façon et d'une seule d'une application ψ comme dans la définition 3.4.1 qui en fait un ω^n-semigroupe, et telle que*

1. *pour toute suite finie $(s_i)_{i<j}$ d'éléments de S*

$$\psi((s_i)_{i<j}) = s_0 s_1 \ldots s_{j-1}$$

2. *pour toute suite $(s_i)_{i<\omega}$ de type ω d'éléments de S_i, avec $i < n$,*

$$\psi((s_i)_{i<\omega}) = \overline{\pi}_i(s_0, s_1, \ldots)$$

Réciproquement, si S est un ensemble muni d'une fonction ψ comme dans la définition 3.4.1 qui en fait un ω^n-semigroupe, alors S peut être équipé d'une façon et d'une seule d'une structure de $\overline{\omega^n}$-semigroupe telle que 1 et 2 soient vérifiées.

Preuve Supposons d'abord que S soit muni des opérations de la définition 3.4.3. Définissons ψ de telle manière que 1 et 2 soient vérifiées. Soit maintenant $s = (s_i)_{i<\omega}$ une suite de type ω d'éléments quelconques de S. Soient $m = max(ty(s_0), ty(s_1), \ldots)$ et $(k_i)_{i<\alpha}$ la suite des indices des éléments de s telle que $s_{k_i} \in S_m$ pour chaque $i < \alpha$. Si $\alpha = \omega$ et $m = n$, alors $\psi(s)$ n'est pas défini. Si $\alpha = \omega$ et $m < n$, alors on pose $\psi(s) = \overline{\pi}_m(s_0 \ldots s_{k_0}, s_{k_0+1} \ldots s_{k_1}, \ldots)$. Si $\alpha < \omega$ on pose $\psi(s) = s_0 \ldots s_{k_{\alpha-1}} \psi((s_i)_{k_\alpha \leq i<\omega})$ ce qui définit $\psi(s)$ par induction sur le plus grand des types des éléments de s. Maintenant, si $s = (s_\beta)_{\beta<\alpha}$ est une suite quelconque d'éléments de S de type α tel que $\omega < \alpha < \omega^{n+1}$, on définit $\psi(s)$ en décomposant s en suites plus petites en fonction de la forme normale de α : si $\alpha = \sum_{j=0}^{k} \omega^{i_j} \cdot a_{i_j}$ est la forme normale de α telle que $a_{i_j} > 0$ pour tout j inférieur ou égal à k, alors on pose

$$\begin{aligned}\psi(s) = \psi(&\psi((s_\beta)_{\beta<\omega^{i_0}}), \psi((s_\beta)_{\omega^{i_0}\leq\beta<\omega^{i_0}\cdot 2}), \dots, \psi((s_\beta)_{\omega^{i_0}\cdot(a_{i_0}-1)\leq\beta<\omega^{i_0}\cdot a_{i_0}}),\\
&\psi((s_\beta)_{\omega^{i_0}\cdot(a_{i_0})\leq\beta<\omega^{i_0}\cdot a_{i_0}+\omega^{i_1}}), \dots, \psi((s_\beta)_{\omega^{i_0}\cdot a_{i_0}+\omega^{i_1}\cdot(a_{i_1}-1)\leq\beta<\omega^{i_0}\cdot a_{i_0}+\omega^{i_1}\cdot a_{i_1}}),\\
&\vdots\\
&\psi((s_\beta)_{\sum_{j=0}^{k-1}\omega^{i_j}\cdot a_{i_j}\leq\beta<(\sum_{j=0}^{k-1}\omega^{i_j}\cdot a_{i_j})+\omega^{i_k}}), \dots, \psi((s_\beta)_{(\sum_{j=0}^{k-1}\omega^{i_j}\cdot a_{i_j})+\omega^{i_k}\cdot(a_{i_k}-1)\leq\beta<\alpha})\\
&)\end{aligned}$$

Les propriétés 3, 4 et 5 de la définition 3.4.1 sont clairement vérifiées. Reste à montrer 2. Soient $s = (s_\beta)_{\beta<\alpha}$ une suite d'éléments de S, $m = max(ty(s_0), ty(s_1), \dots)$ et $(\gamma_\delta)_{\delta<\delta_l}$ une suite strictement croissante d'ordinaux telle que $\gamma_0 = 0$ et $\delta_l < \alpha$. Si α est fini la propriété 2 est vraie par définition de ψ. Supposons que $\alpha = \omega$, et montrons par induction sur m que 2 est vraie. Si $m = 0$, tous les éléments de s sont de type 0. Si $n > 0$ alors le résultat vient par définition de ψ et en utilisant les propriétés de $\overline{\pi}_0$. Supposons maintenant $m > 0$, et soit $(k_i)_{i<\gamma}$ la suite des indices des éléments de s de type m. On distingue alors quatre cas. Supposons d'abord que $\delta_l = \omega$ et $\gamma = \omega$. Si $m = n$ alors ni $\psi(\psi(s_{\gamma_0}, s_{\gamma_0+1}, \dots, s_{\gamma_1-1}), \psi(s_{\gamma_1}, s_{\gamma_1+1}, \dots, s_{\gamma_2-1}), \psi(s_{\gamma_2}, s_{\gamma_2+1}, \dots, s_{\gamma_3-1}), \dots)$ ni $\psi(s_0, s_1, \dots)$ ne sont définis. Sinon, on a

$$\begin{aligned}&\psi(\psi(s_{\gamma_0}, s_{\gamma_0+1}, \dots, s_{\gamma_1-1}), \psi(s_{\gamma_1}, s_{\gamma_1+1}, \dots, s_{\gamma_2-1}), \psi(s_{\gamma_2}, s_{\gamma_2+1}, \dots, s_{\gamma_3-1}), \dots)\\
&= \overline{\pi}_m(s_{\gamma_{i_0}} \dots s_{\gamma_{i_1}-1}, s_{\gamma_{i_1}} \dots s_{\gamma_{i_2}-1}, \dots)\end{aligned}$$

où la suite $(i_j)_{j<\omega}$ est imposée par la définition de ψ. Ceci est égal, en utilisant les propriétés de $\overline{\pi}_m$, à

$$\begin{aligned}&= \overline{\pi}_m(s_0 \dots s_{k_0}, s_{k_0+1} \dots s_{k_1}, \dots)\\
&= \psi(s_0, s_1, \dots)\end{aligned}$$

Notons que l'hypothèse de récurrence n'est pas utilisée dans ce cas là, que nous avons groupé avec les autres pour plus de clarté. Supposons maintenant que $\delta_l = \omega$, que $\gamma < \omega$ et $k_{\gamma-1} \in [\gamma_i, \gamma_{i+1}[$. En utilisant l'hypothèse de récurrence, la définition de ψ et les propriétés de $\overline{\pi}_m$ il vient

$$\begin{aligned}&\psi(\psi(s_{\gamma_0}, \dots, s_{\gamma_1-1}), \psi(s_{\gamma_1}, \dots, s_{\gamma_2-1}), \psi(s_{\gamma_2}, \dots, s_{\gamma_3-1}), \dots)\\
&= (s_{\gamma_0} \dots s_{\gamma_1-1}) \dots (s_{\gamma_i} \dots s_{\gamma_{i+1}-1})\psi(\psi(s_{\gamma_{i+1}}, \dots, s_{\gamma_{i+2}-1}), \dots)\\
&= s_{\gamma_0} \dots s_{\gamma_i} \dots s_{k_{\gamma-1}} \dots s_{\gamma_{i+1}-1}\psi(s_{\gamma_{i+1}}, s_{\gamma_{i+1}+1}, \dots)\\
&= s_{\gamma_0} \dots s_{\gamma_i} \dots s_{k_{\gamma-1}}\psi(s_{k_{\gamma-1}+1}, \dots, s_{\gamma_{i+1}-1}, s_{\gamma_{i+1}}, s_{\gamma_{i+1}+1}, \dots)\\
&= \psi(s_0, s_1, s_2, \dots)\end{aligned}$$

Supposons maintenant que $\delta_l < \omega$ et $\gamma < \omega$. On distingue alors deux sous-cas : $k_{\gamma-1} < \gamma_{\delta_l-1}$ ou non. Nous supposerons que c'est faux, l'autre sous-cas se résout de façon similaire. On a

$$\begin{aligned}
&\psi(\psi(s_{\gamma_0},\dots,s_{\gamma_1-1}),\psi(s_{\gamma_1},\dots,s_{\gamma_2-1}),\dots,\psi(s_{\gamma_{\delta_l-1}},\dots))\\
&= s_{\gamma_0}\dots s_{\gamma_{\delta_l-1}-1}\psi(s_{\gamma_{\delta_l-1}},\dots,s_{k_\gamma-1},\dots)\\
&= s_{\gamma_0}\dots s_{k_{\gamma-1}}\psi(s_{k_{\gamma-1}+1},\dots)\\
&= \psi(s_0,s_1,s_2,\dots)
\end{aligned}$$

Finalement, le dernier des quatre cas, $\delta_l < \omega$ et $\gamma = \omega$: si $m = n$ alors ni $\psi(s_0, s_1, \dots)$ ni $\psi(\psi(s_{\gamma_0},\dots,s_{\gamma_1-1}),\psi(s_{\gamma_1},\dots,s_{\gamma_2-1}),\dots,\psi(s_{\gamma_{\delta_l-1}},\dots))$ ne sont définis. Sinon, on a

$$\begin{aligned}
&\psi(\psi(s_{\gamma_0},\dots,s_{\gamma_1-1}),\psi(s_{\gamma_1},\dots,s_{\gamma_2-1}),\dots,\psi(s_{\gamma_{\delta_l-1}},\dots))\\
&= s_{\gamma_0}\dots s_{\gamma_{\delta_l-1}-1}\psi(s_{\gamma_{\delta_l-1}},\dots)\\
&= s_{\gamma_0}\dots s_{\gamma_{\delta_l-1}-1}\overline{\pi}_m((s_{\gamma_{\delta_l-1}},\dots,s_{k_i}),(s_{k_i+1},\dots,s_{k_{i+1}}),\dots)\\
&= (s_{\gamma_0}\dots s_{\gamma_{\delta_l-1}-1},s_{\gamma_{\delta_l-1}},\dots,s_{k_i})\overline{\pi}_m((s_{k_i+1},\dots,s_{k_{i+1}}),\dots)\\
&= \overline{\pi}_m((s_{\gamma_0}\dots s_{\gamma_{\delta_l-1}-1},s_{\gamma_{\delta_l-1}},\dots,s_{k_i}),(s_{k_i+1},\dots,s_{k_{i+1}}),\dots)\\
&= \psi((s_{\gamma_0}\dots s_{\gamma_{\delta_l-1}-1},s_{\gamma_{\delta_l-1}},\dots,s_{k_i}),(s_{k_i+1},\dots,s_{k_{i+1}}),\dots)\\
&= \psi(s_0,s_1,s_2,\dots)
\end{aligned}$$

On vérifie par induction sur α que la propriété 2 est encore vraie pour $\alpha > \omega$. ∇

Nous reprenons maintenant l'idée de Wilke sur les ω-semigroupes finis, qui consiste à remplacer les applications d'arité infinie par des applications unaires. Voici l'adaptation correspondante de la définition d'$\overline{\omega^n}$-semigroupe :

Définition 3.4.5 *Soit n un entier naturel. Une* ω^n**-algèbre de Wilke** *S est un semigroupe fini partitionné en $n+1$ sous-semigroupes $S_0,\dots,S_n$ tels que $\cup_{i\leq j}S_i$ soit un semigroupe d'idéal S_j quel que soit j inférieur ou égal à n, et équipé d'une famille de n applications $\omega_i : S_i \to S_{i+1}$ pour i inférieur à n telles que, pour deux éléments quelconques s et t de S_i,*

- *$s(ts)^{\omega_i} = (st)^{\omega_i}$*
- *$(s^n)^{\omega_i} = s^{\omega_i}$ pour tout entier n positif*

Pour abréger nous omettrons les indices des applications ω_i : on note s^ω pour $s^{\omega_{ty(s)}}$.

Le théorème suivant montre l'équivalence entre ω^n-semigroupes finis et ω^n-algèbres de Wilke :

Théorème 3.4.6 *Soient n un entier naturel, et S un semigroupe fini partitionné en $n+1$ sous-semigroupes $S_0,\dots,S_n$ tels que S_j soit un idéal de $\cup_{i\leq j}S_i$ quel que soit j inférieur ou égal à n et muni des opérations de la définition 3.4.3 qui en font un $\overline{\omega^n}$-semigroupe. Alors S peut être muni d'une façon et d'une seule d'applications ω_i comme dans la définition 3.4.5 qui en font une ω^n-algèbre de Wilke, et telle que, pour tout $s \in S$ de type inférieur à n,*

$$s^{\omega_{ty(s)}} = \overline{\pi}_{ty(s)}(s,s,s,\dots) \tag{3.1}$$

Réciproquement, si S est un semigroupe fini partitionné en $n+1$ sous-semigroupes $S_0, \dots,$ S_n tels que S_j soit un idéal de $\cup_{i \leq j} S_i$ quel que soit j inférieur ou égal à n et muni d'applications ω_i comme dans la définition 3.4.5 qui en font une ω^n-algèbre de Wilke, alors S peut être équipé d'une façon et d'une seule d'une structure d'$\overline{\omega^n}$-semigroupe telle que 3.1 soit vérifiée.

La preuve est directement issue de la théorie des ω-semigroupes :

Preuve Le sens des $\overline{\omega^n}$-semigroupes vers les ω^n-algèbres de Wilke est trivial. Passons à l'autre. Soit S un semigroupe fini comme dans l'énoncé. Pour toute suite $(s_i)_{i<\omega}$ d'éléments de S_i, avec $i < n$, il existe d'après le théorème 3.3.7 un couple lié (s, e) d'éléments de S et une suite strictement croissante $(k_n)_{n<\omega}$ d'entiers tels que

- $s_0 s_1 \dots s_{k_0 - 1} = s$
- $s_{k_n} s_{k_n+1} \dots s_{k_{n+1}-1} = e$ pour tout entier n

on pose $\overline{\pi}_i(s_0, s_1, \dots) = se^\omega$. Comme le couple (s, e) du théorème 3.3.7 n'est pas unique, il faut vérifier que $se^\omega = s'e'^\omega$ pour tout autre couple lié (s', e') solution. D'après le théorème 3.3.12, (s, e) et (s', e') sont conjugués. Il existe donc $x, y \in S^1$ tels que $e = xy$, $e' = yx$ et $s' = sx$. Comme $s(ts)^\omega = (st)^\omega$ il vient $se^\omega = s(xy)^\omega = sx(yx)^\omega = s'e'^\omega$. On prouve maintenant que l'application $\overline{\pi}_i$ ainsi définie vérifie bien les propriétés de la définition 3.4.3. Pour toute suite strictement croissante $(r_n)_{n<\omega}$ d'entiers on a bien sûr $\overline{\pi}_i(s_0, s_1, \dots) = \overline{\pi}_i(s_0 \dots s_{r_0}, s_{r_0+1} \dots s_{r_1}, \dots)$. Si $t \in S$, on a $ts_0 s_1 \dots s_{k_0-1} = ts$ et $s_{k_n} s_{k_n+1} \dots s_{k_{n+1}-1} = e$ pour tout entier n, donc $\overline{\pi}_i(t, s_0, s_1, \dots) = tse^\omega = t\overline{\pi}_i(s_0, s_1, \dots)$. Comme finalement pour tout $s \in S$ on a $\overline{\pi}_i(s, s, s, \dots) = (s^\pi)^\omega = s^\omega$, il vient $\overline{\pi}_i(s, s, s, \dots) = s^\omega$. ∇

Il en résulte que ω^n-semigroupes finis et ω^n-algèbres de Wilke sont équivalents. Dans la suite nous les confondrons souvent.

Les notions de **morphisme d'ω^n-semigroupes** et de reconnaissance par morphisme viennent directement de l'algèbre universelle, même si les opérations qu'on s'autorise ne sont pas d'arité finie.

On dit qu'un ω^n-semigroupe S est **engendré** par S_0 si pour tout $s \in S$ il existe une suite $(t_\beta)_{\beta<\alpha}$ d'éléments de S_0 telle que $\psi(t_0, t_1, \dots) = s$.

La preuve de la proposition suivante est triviale :

Proposition 3.4.7 *Soient A un alphabet et n un entier. Soient également T un ω^n-semigroupe et φ une application de A dans T_0. Alors φ peut être étendue d'une façon unique en un morphisme $\varphi' : A^{[1,\omega^{n+1}[} \to T$ d'ω^n-semigroupes tel que $\varphi(a) = \varphi'(a)$ pour tout $a \in A$.*

Corollaire 3.4.8 *Soient A un alphabet et n un entier. Soient également $\varphi : A^{[1,\omega^{n+1}[} \to T$ et $\varphi' : U \to T$ deux morphismes d'ω^n-semigroupes tels que φ' soit surjectif. Alors il existe un morphisme $\varphi'' : A^{[1,\omega^{n+1}[} \to U$ tel que $\varphi = \varphi'\varphi''$.*

Exemple 3.4.9 *Soient $A = \{a, b\}$ et $S_0 = \{a, b, ab, ba, aba, 0, 1\}$, $S_1 = \{a^\omega, ab^\omega, ba^\omega, 0',$ $a^\omega a, ab^\omega a, ba^\omega a\}$ et $S = S_0 \cup S_1$ l'ω^1-semigroupe donné par la structure en $\mathcal{D}$-classes*

$^*\,1, a$

$^*\,b$	ba
ab	$^*\,aba$

$^*\,a^\omega$	$^*\,a^\omega a$
ab^ω	$^*\,ab^\omega a$
$^*\,ba^\omega$	$ba^\omega a$

$^*\,0$

$^*\,0'$

où $0'$ est un zéro pour S, 0 un zéro pour S_0, $0x = x0 = 0'$ pour tout $x \in S_1$, 1 est l'élément neutre de S pour le produit seulement, $a^2 = 1$, $b^\omega = ba^\omega$, $bab = 0$, $a^\omega b = a^\omega$, $a^\omega ab = (ab)^\omega = 0'$. Soit également $\varphi : A^{[1,\omega^2[} \to S$ le morphisme d'ω^1-semigroupes défini par $\varphi(a) = a$, $\varphi(b) = b$ et par utilisation de la proposition 3.4.7. Alors S reconnaît $L = (aa+b)^{<\omega^2} - \lambda$ puisque $L = \varphi^{-1}(\{1, b, a^\omega, ba^\omega\})$.

Exemple 3.4.10 *Soient $A = \{a, b\}$ et $S_0 = \{a, b, 0, ab, ba\}$, $S_1 = \{0', (ab)^\omega, (ba)^\omega, (ab)^\omega a, (ba)^\omega a\}$ et $S = S_0 \cup S_1$ l'ω^1-semigroupe donné par la structure en $\mathcal{D}$-classes*

a	$^*\,ab$
$^*\,ba$	b

$^*\,(ab)^\omega$	$(ab)^\omega a$
$(ba)^\omega$	$^*\,(ba)^\omega a$

$^*\,0$

$^*\,0'$

où 0 est un zéro pour S_0, $0'$ est un zéro pour S, $0x = x0 = 0'$ pour tout $x \in S_1$, $a^2 = b^2 = 0$, $aba = a$, $bab = b$, $(ab)^\omega ab = (ab)^\omega$, $(ba)^\omega ab = (ba)^\omega (ab)^\omega = (ba)^\omega$ et $(ab)^\omega b = (ba)^\omega b = 0'$. Soit également $\varphi : A^{[1,\omega^2[} \to S$ le morphisme d'ω^1-semigroupes défini par $\varphi(a) = a$, $\varphi(b) = b$ et par utilisation de la proposition 3.4.7. Alors S reconnaît $L = (ab)^{<\omega^2} - \lambda$ puisque $L = \varphi^{-1}(\{ab, (ab)^\omega\})$.

Voici une proposition tirée de la théorie des algèbres universelles :

Proposition 3.4.11 *Soit $\varphi : S \to T$ un morphisme d'ω^n-semigroupes, et $\varphi' : S \to S/{\sim_\varphi}$ le morphisme d'ω^n-semigroupes naturel qui associe à chaque élément de S sa classe de congruence dans $S/{\sim_\varphi}$. Il existe un unique morphisme d'ω^n-semigroupes $\varphi'' : S/{\sim_\varphi} \to T$ tel que $\varphi = \varphi''\varphi'$. De plus, φ'' est un isomorphisme de $S/{\sim_\varphi}$ dans $\varphi(S)$.*

3.4.2 Equivalence entre ω^n-algèbres de Wilke et n-automates

Nous montrons maintenant que la classe des langages reconnaissables par ω^n-semigroupes finis est exactement la classe des langages n-reconnaissables qui ne contiennent pas le mot vide.

Théorème 3.4.12 *Soit A un alphabet fini. Une partie de $A^{[1,\omega^{n+1}[}$ est n-reconnaissable si et seulement si elle est reconnue par un ω^n-semigroupe fini.*

Des n-automates vers les ω^n-algèbres de Wilke

Pour construire un ω^n-semigroupe fini en partant d'un n-automate on utilise la technique naturelle, qui consiste à coder une classe de mots qui ont la même action sur tous les états de l'automate par une matrice.

Pour passer d'un automate qui reconnaît des mots finis à un semigroupe, on code une classe de mots finis par une matrice carrée de booléens indicée verticalement et horizontalement par les états de l'automate, de telle manière que l'élément de la matrice associé au couple (p, q) soit "vrai" si et seulement si chaque mot de la classe que code la matrice est l'étiquette d'un chemin de p vers q. L'ensemble des matrices muni du produit habituel forme alors un semigroupe, et l'application qui à chaque mot associe sa matrice est un morphisme de semigroupes, qui reconnaît le langage de l'automate de départ.

Dans le cas des mots de longueur inférieure à ω^{n+1}, nous devons graduer l'ensemble des matrices, et l'équiper d'applications ω qui en font un ω^n-semigroupe. Les matrices que nous allons utiliser sont indicées horizontalement et verticalement par tous les éléments de $[Q]_0^n$, où Q est l'ensemble des états du n-automate de départ. Pour définir les applications ω, nous n'avons pas seulement besoin de savoir s'il existe un chemin d'un élément de $[Q]_0^n$ vers un autre, mais également d'en connaître le contenu, afin de pouvoir calculer les états infiniment répétés dans un chemin. Nous mettons cette information dans la matrice : si m est la matrice associée à un mot u, l'élément de m associé au couple (p, q) est la liste des contenus des différents chemins étiquetés par u qui vont de p vers q. Comme un chemin ne contient un élément de $[Q]^i$ que si son étiquette est un mot de longueur supérieure ou égale à ω^i, les contenus sont utilisés pour graduer le semigroupe des matrices obtenu.

Soient donc $\mathcal{A} =< Q, A, E, I, F >$ un n-automate et M l'ensemble des matrices de taille $|[Q]_0^n| \times |[Q]_0^n|$ à coefficient dans $[Q]_2^{n+2} \cup \{\emptyset\}$ et dont les lignes et colonnes sont indicées par les éléments de $[Q]_0^n$. L'ensemble M est évidement fini. Si u est un mot de $A^{[1,\omega^{n+1}[}$, $c = (q_\alpha)_{\alpha \leq |u|}$ est un chemin de p vers q d'étiquette u dans $\mathcal{A}$, et $l = \cup_{\alpha \leq |u|} q_\alpha$ alors c est dénotée par

$$c : p \xrightarrow[l]{u} q$$

A chaque mot non vide u sur A de longueur $|u| = \sum_{i=m}^{0} \omega^i \cdot a_i$, avec $a_m > 0$, inférieure à ω^{n+1} nous allons associer une matrice $\mu(u)$ de M de telle manière que

$$\mu(u)_{p,q} = \{l \subseteq [Q]_0^n : \exists c : p \xrightarrow[l]{u} q\}$$

Naturellement, pour $a \in A$,

$$\mu(a)_{p,q} = \{\{p,q\}\} \text{ si et seulement si } (p,a,q) \in E$$

Le **type** d'un composant c d'une matrice de M qui n'est pas l'ensemble vide est le plus petit entier m tel que $c \in [Q]_2^m$. Observons que tous les composants d'une matrice qui ne sont pas l'ensemble vide sont tous du même type. Nous partitionnons M en $n+1$ sous ensembles $M_0, \dots, M_n$ de telle façon que $m \in M_i$ si et seulement si

$$m_{p,q} \in \begin{cases} [Q]_2^{i+2} \cup \{\emptyset\} & \text{si } t(q) \leq i, \\ \{\emptyset\} & \text{si } t(q) > i. \end{cases}$$

On a alors, $\mu(u)_{p,q} \in M_i$ si et seulement si $\omega^i \leq |u| < \omega^{i+1}$. Le **type** de la matrice m, $t(m)$, est l'entier i. Pour des raisons pratiques la matrice nulle, dont tout les éléments sont $\emptyset$, a tous les types.

Nous allons maintenant équiper M d'une structure de semigroupe en le munissant d'un produit associatif. Nous allons pour ceci définir un opérateur binaire $\sqcup$, qui prend en argument deux ensembles d'ensembles :

Définition 3.4.13 *Soient S un ensemble, r et r' deux entiers, $l_1, \dots l_r$ et $l'_1, \dots l'_{r'}$ respectivement des ensembles d'éléments de $[S]_0^i$ et $[S]_0^j$ pour deux entiers i et j. L'opérateur $\sqcup$ est défini par :*

$$\sqcup \begin{cases} \emptyset \sqcup a = a \sqcup \emptyset = \emptyset \\ \{l_1, \dots, l_r\} \sqcup \{l'_1, \dots, l'_{r'}\} = \{l_1 \cup l'_1, \dots, l_1 \cup l'_{r'}, \dots, l_r \cup l'_1, \dots, l_r \cup l'_{r'}\} \end{cases}$$

Proposition 3.4.14 *L'opérateur $\sqcup$ est associatif et commutatif.*

Preuve La commutativité est évidente. Soient a, b, c trois ensembles d'ensembles. Si $a \sqcup (b \sqcup c) = \emptyset$ alors soit a, b ou c est $\emptyset$, et $(a \sqcup b) \sqcup c = \emptyset$. Supposons maintenant qu'ils soient tous les trois non vides et que $a \sqcup (b \sqcup c) = \{l_1, \dots, l_m\}$ pour un entier m. Alors pour tout $i \in 1 \dots m$ on a $l_i = l_i^a \cup l_i^{bc}$ où $l_i^a \in a$ et $l_i^{bc} \in b \sqcup c$, et $l_i^{bc} = l_i^b \cup l_i^c$ où $l_i^b \in b$ et $l_i^c \in c$. Comme $\cup$ est associatif il vient $l_i \in (a \sqcup b) \sqcup c$. La preuve dans l'autre sens est similaire. ∇

Nous pouvons maintenant équiper M avec un produit de matrices $\odot$: si a et b sont deux matrices de M,

$$(a \odot b)_{p,q} = \bigcup_{k \in [Q]_0^n} (a_{p,k} \sqcup b_{k,q})$$

En supposant que $l \in \mu(u)_{p,q}$ si et seulement si $p \xrightarrow[l]{u} q$ pour tout mot u de $A^{[1,\omega^{n+1}[}$ et $p, q \in [Q]_0^n$, et que u et v sont deux mots de $A^{[1,\omega^{n+1}[}$ tels que $\mu(u) = a$ et $\mu(v) = b$, alors la définition du produit de matrices indique que $p \xrightarrow[l]{uv} q$ si et seulement si il existe $l_1, l_2 \subseteq [Q]_0^n$ et $k \in [Q]_0^n$ tels que $p \xrightarrow[l_1]{u} k$, $k \xrightarrow[l_2]{v} q$ et $l = l_1 \cup l_2$.

Proposition 3.4.15 *Si $a \in M_i$ and $b \in M_j$ alors $a \odot b \in M_{max(i,j)}$.*

Preuve Soient $k \in [Q]_0^n$, $a_{p,k} = \{l_1, \ldots, l_r\} \in [Q]_2^{i+2}$, $b_{k,q} = \{l'_1, \ldots, l'_{r'}\} \in [Q]_2^{j+2}$. Immédiatement, $l \cup l' \in [Q]_1^{max(i,j)+1}$ pour chaque $l \in a_{p,k}$ et $l' \in b_{k,q}$. Donc $a_{p,k} \sqcup b_{k,q} \in [Q]_2^{max(i,j)+2}$ et $\cup_{k \in [Q]_0^n}(a_{p,k} \sqcup b_{k,q}) \in [Q]_2^{max(i,j)+2}$ car l'union est évidemment compatible avec le type. Si $a_{p,k} = \emptyset$ ou $b_{k,q} = \emptyset$ pour tout $k \in [Q]_0^n$ alors $a_{p,k} \sqcup b_{k,q} = \emptyset$ et $\cup_{k \in [Q]_0^n}(a_{p,k} \sqcup b_{k,q}) = \emptyset$. Donc $\cup_{k \in [Q]_0^n}(a_{p,k} \sqcup b_{k,q}) \in [Q]_2^{max(i,j)+2} \cup \{\emptyset\}$. Maintenant, si $t(q) > max(i,j)$, on a $t(q) > j$ donc $k \in [Q]_0^n$ $b_{k,q} = \emptyset$ et $(a \odot b)_{p,q} = \emptyset$ pour tout $k \in [Q]_0^n$. ∇

Lemme 3.4.16 *Soient m un entier, $a_1, \ldots, a_m$ et b des ensembles d'ensembles. Alors*

$$(\cup_{1 \leq i \leq m} a_i) \sqcup b = \cup_{1 \leq i \leq m}(a_i \sqcup b)$$

Preuve Si $b = \emptyset$ alors les membres droit et gauche de l'égalité sont tout deux égaux à l'ensemble vide. Si $\cup_{1 \leq i \leq m} a_i = \emptyset$ alors $a_i = \emptyset$ pour tout $i \in 1 \ldots m$ et les deux membres de l'égalité sont égaux à l'ensemble vide. Sinon, les deux membres de l'égalité sont nécessairement différents de l'ensemble vide. Pour prouver que le membre de gauche est inclus dans celui de droite, supposons que $l \in (\cup_{1 \leq i \leq m} a_i) \sqcup b$. Alors $l = l_1 \cup l_2$ pour $l_1 \in a_r$ pour chaque $r \in 1 \ldots m$ et $l_2 \in b$. Donc $l_1 \cup l_2 \in a_r \sqcup b$ et $l \in \cup_{1 \leq i \leq m}(a_i \sqcup b)$. La preuve de l'inclusion dans l'autre sens est similaire. ∇

Nous sommes maintenant prêts à prouver que le produit de matrices $\odot$ est associatif :

Proposition 3.4.17 *Soient i_1, i_2, i_3 trois entiers et $a \in M_{i_1}$, $b \in M_{i_2}$, $c \in M_{i_3}$. Alors $((a \odot b) \odot c)_{p,q} = (a \odot (b \odot c))_{p,q}$.*

Preuve

$$\begin{aligned}
((a \odot b) \odot c)_{p,q} &= \bigcup_{k \in [Q]_0^n} ((\bigcup_{k' \in [Q]_0^n} (a_{p,k'} \sqcup b_{k',k})) \sqcup c_{k,q}) = \bigcup_{k \in [Q]_0^n} (\bigcup_{k' \in [Q]_0^n} ((a_{p,k'} \sqcup b_{k',k}) \sqcup c_{k,q})) \\
&= \bigcup_{k \in [Q]_0^n} (\bigcup_{k' \in [Q]_0^n} (a_{p,k'} \sqcup (b_{k',k} \sqcup c_{k,q}))) = \bigcup_{k' \in [Q]_0^n} (\bigcup_{k \in [Q]_0^n} (a_{p,k'} \sqcup (b_{k',k} \sqcup c_{k,q}))) \\
&= \bigcup_{k' \in [Q]_0^n} (a_{p,k'} \sqcup \bigcup_{k \in [Q]_0^n} (b_{k',k} \sqcup c_{k,q})) \quad = \quad (a \odot (b \odot c))_{p,q}
\end{aligned}$$

∇

Donc M équipé du produit de matrices $\odot$ est un semigroupe fini, et de plus M_i est un idéal pour $\cup_{j \leq i} M_i$. Nous noterons le produit de deux matrices m et m' de M par mm' plutôt que $m \odot m'$ afin d'alléger les notations. Il nous faut maintenant munir M des applications $\omega_i : M_i \to M_{i+1}$ pour $i \in 0 \ldots n-1$.

Nous définissons d'abord une famille d'opérateurs de projection $\mathcal{P}_i$ en posant, si $l_1, \ldots,$ l_m sont des ensembles, $\mathcal{P}_i(\{l_1, \ldots, l_m\}) = \{\mathcal{P}'_i(l_1), \ldots, \mathcal{P}'_i(l_m)\}$, où $\mathcal{P}'_i(l) = [S]^i \cap l$. $\mathcal{P}_i$ va nous permettre de ne garder dans un ensemble d'ensembles d'éléments de $[Q]_0^n$ que les éléments de $[Q]^i$.

Définition 3.4.18 *Soit s une matrice de M. Un s-**chemin** de p vers q est une suite $(t_i)_{i<\omega}$ d'états telle que $t_0 = p$, $s_{t_i,t_{i+1}} \neq \emptyset$ pour tout entier j et pour tout entier k supérieur à k',*

$$q \in \bigsqcup_{j>k} \mathcal{P}_i(s_{t_j,t_{j+1}})$$

Si s est une matrice de M_i, on définit s^{ω_i} de la façon suivante : un sous-ensemble l de $[Q]_0^i \cup \{q\}$ appartient à $s^{\omega_i}_{p,q}$ si et seulement si il existe un s-chemin $(t_i)_{i<\omega}$ de p vers q, une suite $(l_i)_{i<\omega}$ et un entier k' tels que

- $l = \{q\} \cup \cup_{j<\omega} l_j$,
- $l_j \in s_{t_j,t_{j+1}}$ pour tout entier j,
- $q = \cup_{j>k} \mathcal{P}'_i(l_j)$ pour tout entier k supérieur à k'.

Afin de montrer que les opérateurs ω_i ainsi définis vérifient bien les propriétés de ceux de la définition 3.4.5 nous avons besoin des propriétés triviales suivantes, que nous utiliserons sans référer au lemme :

Lemme 3.4.19 *Soient k un entier, et $(a_i)_{1\leq i\leq 4}$ une famille de composants de matrices de M. Alors*

- *si $l \in a_1$ alors $\mathcal{P}'_k(l) \in \mathcal{P}_k(a_1)$,*
- *$\mathcal{P}_k(a_1 \sqcup a_2) = \mathcal{P}_k(a_1) \sqcup \mathcal{P}_k(a_2)$,*
- *si $a_1 \subseteq a_3$ et $a_2 \subseteq a_4$ alors $a_1 \sqcup a_2 \subseteq a_3 \sqcup a_4$,*
- *si $a_1 \subseteq a_2$ alors $\mathcal{P}_k(a_1) \subseteq \mathcal{P}_k(a_2)$.*

Lemme 3.4.20 *L'opérateur ω_i qui à chaque matrice de M_i associe une matrice s^{ω_i} de M_{i+1} vérifie les propriétés de l'opérateur ω_i de la définition 3.4.5.*

Preuve Nous prouvons d'abord que $(s^n)^\omega_{p,q} \subseteq s^\omega_{p,q}$ pour tout entier n. Supposons que $l \in (s^n)^\omega_{p,q}$ et posons $l' = l - \{q\}$. Il existe un s^n-chemin $(t_i)_{i<\omega}$ de p vers q. Nous écrivons

$$t_0 \xrightarrow[l_0]{} t_1 \xrightarrow[l_1]{} t_2 \;\cdots\; t_i \xrightarrow[l_i]{} t_{i+1} \;\cdots$$

où la suite $(l_j)_{j\leq\omega}$ est choisie de telle manière que $l_j \in s^n_{t_j,t_{j+1}}$, $q = \cup_{j>k}\mathcal{P}'_i(l_j)$ et $l' = \cup_{j\geq 0} l_j$. A partir de chaque l_j on peut construire une suite de $n+1$ états $(r^j_m)_{0\leq m\leq n}$ de telle façon que pour tout j, $r^j_0 = t_j$ et $r^j_n = t_{j+1}$, pour tout $m < n$, $s_{r^j_m,r^j_{m+1}} \neq \emptyset$ et $l_j \in \sqcup_{0\leq m<n} s_{r^j_m,r^j_{m+1}}$. Considérons la suite $r^0_0, r^0_1, \ldots, r^0_n, r^1_0, r^1_1, \ldots$ de type ω. Comme $l_j \in \sqcup_{0\leq m<n} s_{r^j_m,r^j_{m+1}}$, $l' = \cup_{j\geq 0} l_j \in \sqcup_{j\geq 0} \sqcup_{0\leq m<n} s_{r^j_m,r^j_{m+1}} = \sqcup_{j\geq 0} s_{r_j,r_{j+1}}$. D'un autre coté, si $l_j \in \sqcup_{0\leq m<n} s_{r^j_m,r^j_{m+1}}$ alors $\mathcal{P}'_i(l_j) \in \mathcal{P}_i(\sqcup_{0\leq m<n} s_{r^j_m,r^j_{m+1}})$ donc $q = \cup_{j>k}\mathcal{P}'_i(l_j) \in \sqcup_{j>k}\mathcal{P}_i(\sqcup_{0\leq m<n} s_{r^j_m,r^j_{m+1}}) = \sqcup_{j>k} \sqcup_{0\leq m<n} \mathcal{P}_i(s_{r^j_m,r^j_{m+1}}) = \sqcup_{j>k}\mathcal{P}_i(s_{r^j_m,r^j_{m+1}})$. Donc cette suite est un s-chemin de p vers q et $l \in s^\omega_{p,q}$.

Supposons maintenant que $l \in s^\omega_{p,q}$ et $l' = l - \{q\}$. Il existe un s-chemin $t_0 t_1 \ldots$ de p vers q. Considérons la suite $t_0, t_n, t_{2n}, \ldots$ de type ω. Comme $\sqcup_{0\leq m<n} s_{t_{nj+m},t_{nj+m+1}} \subseteq s^n_{t_{nj},t_{n(j+1)}}$, on a $l' \in \sqcup_{j\geq 0} s_{t_j,t_{j+1}} = \sqcup_{j\geq 0} \sqcup_{0\leq m<n} s_{t_{nj+m},t_{nj+m+1}} \subseteq \sqcup_{j\geq 0} s^n_{t_{nj},t_{n(j+1)}}$. D'un autre coté, en utilisant le même genre d'argument, $q \in \sqcup_{j>k}\mathcal{P}_i(s_{t_j,t_{j+1}}) = \mathcal{P}_i(\sqcup_{j>k} s_{t_j,t_{j+1}}) =$

$\mathcal{P}_i(\sqcup_{j>k} \sqcup_{0\leq m<n} s_{t_{nj+m},t_{nj+m+1}}) \subseteq \mathcal{P}_i(\sqcup_{j>k} s^n_{t_{nj},t_{n(j+1)}}) = \sqcup_{j>k}\mathcal{P}_i(s^n_{t_{nj},t_{n(j+1)}})$. Donc cette suite est un s^n-chemin de p vers q et $l \in (s^n)^\omega_{p,q}$.

On montre maintenant que $(s(ts)^\omega)_{p,q} = (st)^\omega_{p,q}$. Supposons pour commencer que $l \in (st)^\omega_{p,q}$. Soit $(u_i)_{i<\omega}$ le st-chemin de p vers q et $l' = l - \{q\}$. Il existe une suite $(r_m)_{m<\omega}$ telle que $s_{u_m,r_m} \neq \emptyset$, $t_{r_m,u_{m+1}} \neq \emptyset$, $s_{u_m,r_m} \sqcup t_{r_m,u_{m+1}} \subseteq (st)_{u_m,u_{m+1}}$, $q \in \sqcup_{j>k}\mathcal{P}_i(s_{u_j,r_j} \sqcup t_{r_j,u_{j+1}})$ et $l' \in \sqcup_{j\geq 0}(s_{u_j,r_j} \sqcup t_{r_j,u_{j+1}})$. Considérons la suite $r_0, u_1, r_1, u_2, r_2, \ldots$ de type ω. Comme on a $q \in \sqcup_{j>k+1}\mathcal{P}_i(t_{r_j,u_{j+1}} \sqcup s_{u_{j+1},r_{j+1}}) \subseteq \sqcup_{j>k+1}\mathcal{P}_i(ts_{r_j,r_{j+1}})$, cette suite est un ts-chemin de r_0 vers q et $(\sqcup_{j\geq 0}(t_{r_j,u_{j+1}} \sqcup s_{u_{j+1},r_{j+1}})) \sqcup \{\{q\}\} \in (ts)^\omega_{r_0,q}$. Maintenant, comme $s_{p,r_0} \neq \emptyset$ il vient $l \in s_{p,r_0} \sqcup ((\sqcup_{j\geq 0}(t_{r_j,u_{j+1}} \sqcup s_{u_{j+1},r_{j+1}})) \sqcup \{\{q\}\}) \subseteq (s(ts)^\omega)_{p,q}$.

$$\begin{tikzcd}
u_0 \arrow[r] & u_1 \arrow[r] & \cdots\cdots \arrow[r] & u_k \arrow[rr, "(st)_{u_k,u_{k+1}}", "l_k"'] \arrow[dr, "l_k^s", "s_{u_k,r_k}"'] & & u_{k+1} \arrow[r] & \cdots\cdots \\
 & & \cdots\cdots \arrow[rr] & & r_k \arrow[ur, "l_k^t"', "t_{r_k,u_{k+1}}"] \arrow[r] & \cdots\cdots &
\end{tikzcd}$$

Supposons finalement que $l \in (s(ts)^\omega)_{p,q}$. D'après la définition du produit de matrices ceci implique qu'il existe un état r tel que $s_{p,r} \neq \emptyset$ et $l \in s_{p,r} \sqcup (ts)^\omega_{r,q}$. En utilisant le même type d'argument que dans la partie précédente de cette preuve on peut montrer qu'il existe un état r' tel que $t_{r,r'} \neq \emptyset$ et $l \in s_{p,r} \sqcup t_{r,r'} \sqcup (st)^\omega_{r',q}$, c'est-à-dire qu'il existe un st-chemin $r', u_1, u_2, \ldots$ de r' vers q. Donc $(st)_{p,r'} \neq \emptyset$, la suite $p, r', u_1, u_2, \ldots$ de type ω est un st-chemin de p vers q et $l \in (st)^\omega_{p,q}$. Ceci termine la preuve du lemme. ∇

Nous avons donc montré que

Proposition 3.4.21 *L'ensemble $\cup_{i=0}^n M_i$ muni du produit $\odot$ et des applications $\omega_i : M_i \to M_{i+1}$ pour $i \in 0 \ldots n-1$ est une ω^n-algèbre de Wilke.*

On vérifie par induction transfinie sur $|u|$ que

Proposition 3.4.22 *Soit u un mot de $A^{[1,\omega^{n+1}[}$. Alors $l \in \mu(u)_{p,q}$ si et seulement si il existe un chemin $c : p \xrightarrow[l]{u} q$.*

Finalement,

Proposition 3.4.23 *A partir d'un n-automate $\mathcal{A} =< Q, A, E, I, F >$ qui reconnaît une partie X de $A^{[1,\omega^{n+1}[}$ on peut effectivement construire un ω^n-semigroupe fini qui reconnaît X.*

Preuve L'ω^n-algèbre de Wilke $S = \mu(A^{[1,\omega^{n+1}[})$ peut effectivement être construite à partir de $\mathcal{A}$. Soient $P = \{s \in S : \exists i \in I\ \exists f \in F\ s_{i,f} \neq \emptyset\}$ et S' l'ω^n-semigroupe construit à partir de S en application du théorème 3.4.6 et du lemme 3.4.4. Alors S' reconnaît X. ∇

Des ω^n-semigroupes finis vers les n-automates

Soit A un alphabet fini. Nous allons montrer que tout langage de $A^{[1,\omega^{n+1}[}$ reconnu par un ω^n-semigroupe fini est n-reconnaissable en construisant une C-expression rationnelle par induction sur n. L'argument utilisé dans la preuve est une extension naturelle des grammaires sans contextes linéaires droites sur les mots finis. Nous donnerons implicitement dans la section suivante un algorithme pour construire directement un automate à partir d'un ω^n-semigroupe fini.

Nous avons besoin de la proposition suivante, qui est une conséquence du corollaire 3.3.8 :

Proposition 3.4.24 *Soient A un alphabet, n un entier, S un ω^n-semigroupe fini, $\varphi : A^{[1,\omega^{n+1}[} \to S$ un morphisme de ω^n-semigroupes et u un mot sur A tel que $|u| = \sum_{i=m}^{0} \omega^i \cdot a_i$, avec $m \leq n$ et a_m un entier positif. Alors*

- *si $|u| = \omega^m$, il existe une suite $(u_i)_{i<\omega}$ de mots sur A et un couple lié (s,e) de S_{m-1} tels que $u = \prod_{i<\omega} u_i$, $\varphi(u_0) = s$, et $\varphi(u_r) = e$ pour tout entier r positif,*
- *si $|u| > \omega^m$, il existe une suite $(u_i)_{i\leq\omega}$ de mots sur A, un couple lié (s,e) de S_{m-1} et un élément t de $\cup_{i\leq m} S_i$ tels que $u = \prod_{i\leq\omega} u_i$, $\varphi(u_0) = s$, $\varphi(u_r) = e$ pour tout entier r positif et $\varphi(u_\omega) = t$.*

Preuve Posons $v_i = u[\omega^{m-1} \cdot i, \omega^{m-1} \cdot (i+1)[$ pour tout entier i. Par application du corollaire 3.3.8 au mot $\prod_{i<\omega} v_i$ et à la suite $(v_i)_{i<\omega}$, il existe une suite strictement croissante d'entiers $(j_k)_{k<\omega}$ et un couple lié (s,e) de S tels que $j_0 = 0$, $\varphi(\prod_{i=j_0}^{j_1-1} v_i) = s$ et $\varphi(\prod_{i=j_k}^{j_{k+1}-1} v_i) = e$ pour tout entier k positif. Comme l'image par φ d'un mot sur A de longueur $\sum_{i=r}^{0} \omega^i \cdot a_i$, où a_r est un entier positif et $r \leq n$, est évidemment un élément de S_r, le couple (s,e) est élément de $S_{m-1} \times S_{m-1}$. Posons $u_k = \prod_{i=j_k}^{j_{k+1}-1} v_i$ pour tout entier k. Si $|u| > \omega^m$ on pose également $u_\omega = u[\omega^m, |u|[$ et $t = \varphi(u_\omega)$. La suite $(u_i)_{i<\omega}$ (resp. $(u_i)_{i\leq\omega}$) et (s,e) (resp. (s,e,t)) vérifient bien les conditions de l'énoncé si $|u| = \omega^m$ (resp. $|u| > \omega^m$). ∇

Proposition 3.4.25 *Soient A un alphabet fini, S un ω^n-semigroupe fini, $\varphi : A^{[1,\omega^{n+1}[} \to S$ un morphisme d'ω^n-semigroupes, i un entier inférieur ou égal à n et X une partie de S_i. Alors $\varphi^{-1}(X)$ est C-rationnelle.*

Afin de simplifier les notations dans la preuve nous notons S^1 l'ω^n-semigroupe S auquel on ajoute un élément neutre 1 pour le produit, qui est plus fort que celui de S s'il en possédait un. On a donc $1 \cdot s = s \cdot 1 = s$ pour tout $s \in S^1$. Si T est un ω^n-semigroupe et $\varphi : T \to S$ un morphisme de ω^n-semigroupes, alors le morphisme de ω^n-semigroupes $\varphi I : T \to S^1$, qui est la composée de φ et du morphisme de ω^n-semigroupes identité $I : S \to S^1$, reconnaît une partie X de T si et seulement si φ la reconnaît. Toujours par soucis de simplification des notations nous noterons φ le morphisme de ω^n-semigroupes φI. Bien entendu, on a $\varphi^{-1}(1) = \emptyset$. Si R est un ensemble de mots, alors on pose $R \cdot \varphi^{-1}(1) = R$: attention, il s'agit ici uniquement d'un jeu d'écriture, et non d'une modification du produit d'ensemble de mots habituel, qui donne $R \cdot \emptyset = \emptyset$. En d'autres termes, si $\varphi^{-1}(t) = \emptyset$, on a $R \cdot \varphi^{-1}(t) = R$ si et seulement si $t = 1$, $R \cdot \varphi^{-1}(t) = \emptyset$ sinon. Cette liberté d'écriture nous permet de dire, en application de la proposition 3.4.24, que si A est un alphabet, n un entier, S un ω^n-semigroupe fini, $\varphi : A^{[1,\omega^{n+1}[} \to S$ un morphisme de ω^n-semigroupes et u un mot sur A tel que $|u| = \sum_{i=m}^{0} \omega^i \cdot a_i$, avec $m \leq n$ et a_m un entier positif, alors $u \in \varphi^{-1}(s)\varphi^{-1}(e)^\omega\varphi^{-1}(t)$ pour un couple lié (s, e) de S_{m-1} et $t \in (\cup_{i \leq m} S_i)^1$. Elle nous évite d'avoir à traiter deux cas comme dans l'énoncé de la proposition 3.4.24.

Une **grammaire sans contexte** est un quintuplet (A, V, T, P, S) où V est un ensemble fini de variables, T un ensemble fini de C-expressions rationnelles sur l'alphabet A, P est un ensemble fini d'équations de la forme $E = w$, où E est une variable et w un mot fini sur $V \cup T$. Finalement, S est une variable spéciale appelée symbole de départ.

Si $G = (A, V, T, P, S)$ est une grammaire sans contexte, $A = w$ une équation de P, w_1 et w_2 deux mots de $(V \cup T)^*$ alors $w_1 A w_2 \underset{G}{\Rightarrow} w_1 w w_2$. On note $\overset{*}{\underset{G}{\Rightarrow}}$ la fermeture réflexive et transitive de $\underset{G}{\Rightarrow}$. L'ensemble des mots sur A définis par la grammaire G est

$$\mathcal{L}(G) = \{w : S \overset{*}{\underset{G}{\Rightarrow}} e,\ e \in T^*,\ w \in \overline{e}\}$$

Une grammaire sans contexte est linéaire droite si toutes les équations sont de la forme $E = wF$ ou $E = w$ où E et F sont des variables et w un élément de T.

Théorème 3.4.26 *Soit $G = (A, V, T, P, S)$ une grammaire sans contexte linéaire droite. A partir de G on peut effectivement construire une C-expression rationnelle e telle que $\overline{e} = \mathcal{L}(G)$.*

Dans la preuve du théorème nous utilisons la définition suivante :

Définition 3.4.27 *Soit $\mathcal{A} =< Q, A, E, I, F >$ un n-automate. Un* **sous-automate** *de $\mathcal{A}$ est un n-automate $\mathcal{B} =< Q', A, E', I', F' >$ avec*

- $Q' \subseteq Q$,
- $I' = I \cap Q'$,
- $E' = E \cap [Q']_0^n \times A \times Q'$,
- $F' = F \cap [Q']_0^n$.

Preuve du théorème 3.4.26. Plutôt qu'une C-expression rationnelle nous allons construire un n-automate, pour un certain entier n. A partir de chaque élément e de T on peut effectivement construire un n_e-automate déterministe $\mathcal{A}_e$ tel que $\overline{e} = \mathcal{L}(\mathcal{A}_e)$. Pour chaque élément E de V on construit un n_E-automate $\mathcal{A}_E$ de la façon suivante. On part d'un automate dont l'alphabet est A, qui n'a qu'un état nommé E, aucune transition, aucun état final et aucun état initial. Pour chaque équation de G de la forme $E = eF$ ou $E = e$, avec $e \in T$ et $F \in V$, on ajoute à l'automate qu'on construit une copie de $\mathcal{A}_e$. Nous appelons $\mathcal{A}_{E=eF}$ (resp. $\mathcal{A}_{E=e}$) le sous-automate de $\mathcal{A}_E$ constitué de cette copie. Pour chaque transition partant de l'état initial de cette copie vers un état q par la lettre a on ajoute une transition de E vers q par a. On dit alors que les état initiaux et finaux de $\mathcal{A}_E$ sont ceux des copies des automates $\mathcal{A}_e$ ajoutées. Supposons ceci fait pour tous les éléments de V, et construisons un automate $\mathcal{A}_G$ constitué de l'union de tous ces automates, c'est-à-dire dont l'ensemble des états (resp. ensembles des états initiaux, finaux, ensemble des transitions) est formé par l'union des ensembles d'états (resp. ensembles des états initiaux, finaux, ensemble des transitions) des automates $\mathcal{A}_E$ pour tout $E \in V$, en procédant à un renommage si nécessaire, et l'alphabet est A. On relie maintenant les différents sous-automates de la façon suivante : on ajoute une transition par la lettre a partant d'un état final d'un sous-automate $\mathcal{A}_{E=eF}$ vers l'état atteint par lecture de la lettre a en partant de l'état initial d'un sous-automate $\mathcal{A}_{E'=e'F'}$ (resp. $\mathcal{A}_{E'=e'}$), qui éventuellement peut être $\mathcal{A}_{E=eF}$, si et seulement si il existe une suite finie $E_1 = e_1F_1, \ldots, E_n = e_nF_n$ (resp. $E_1 = e_1F_1, \ldots, E_n = e_n$) d'équations de G telle que $E_1 = E$, $e_1 = e$, $F_1 = F$, $\lambda \in \overline{e_i}$ pour tout $1 < i < n$, $F_i = E_{i+1}$ pour tout $1 \leq i \leq n-1$, $E_n = E'$, $e_n = e'$ et $F_n = F'$ (resp. $E_n = E'$ et $e_n = e'$). De même, on ajoute une transition par la lettre a partant de S vers l'état atteint par lecture de la lettre a en partant de l'état initial d'un sous-automate $\mathcal{A}_{E'=e'F'}$ (resp. $\mathcal{A}_{E'=e'}$) si et seulement si il existe une suite finie $E_1 = e_1F_1, \ldots, E_n = e_nF_n$ (resp. $E_1 = e_1F_1, \ldots, E_n = e_n$) d'équations de G telle que $E_1 = S$, $\lambda \in \overline{e_i}$ pour tout $1 \leq i < n$, $F_i = E_{i+1}$ pour tout $1 \leq i \leq n-1$, $E_n = E'$, $e_n = e'$ et $F_n = F'$ (resp. $E_n = E'$ et $e_n = e'$). On marque l'utilisation d'une des transitions ainsi ajoutées dans un chemin en utilisant des techniques d'historiques similaires à celles employées dans la sous-sous-section 2.6.1 afin de ne les employer qu'un nombre fini de fois dans un même chemin. Par soucis d'uniformité nous marquons également toutes les transitions sortantes de S, mais ceci n'a aucune importance puique comme il n'existe pas de transition vers S on ne peut employer qu'une fois une seule de ces transitions dans un chemin. L'état initial de l'automate ainsi construit est alors S, et les états finaux sont ceux des automates $\mathcal{A}_{E=e}$ auquels on ajoute les états des sous-automates $\mathcal{A}_E$ pour lesquels il existe une transition sortante vers un sous-automate $\mathcal{A}_{E'=e'}$ dont l'état initial est également final. On a alors le lemme suivant :

Lemme 3.4.28 *$u \in \mathcal{L}(A_G)$ si et seulement si $u \in \mathcal{L}(G)$.*

Preuve D'abors le sens de la gauche vers la droite. Supposons que $|u| = \alpha$ et soit $c = (q_\beta)_{\beta \leq \alpha}$ un chemin acceptant étiqueté par u. Supposons également que q_α soit un état du sous-automate $\mathcal{A}_{E=eF}$ (le raisonnement est quasi-identique si le sous-automate est $\mathcal{A}_{E=e}$ pour $E = e$ une équation de G). Par construction de $\mathcal{A}_G$ il existe une suite d'ordinaux $(\beta_i)_{0<i\leq n}$ strictement croissante et nécessairement finie telle que $\beta_1 = 0$, $\beta_n = \alpha$ et $(q_{\beta_{i+1}}, u_{\beta_{i+1}}, q_{\beta_{i+1}+1})$ soit une transition marquée de $\mathcal{A}_G$ pour tout i inférieur à $n-1$. Toujours par construction de $\mathcal{A}_G$, pour chaque $i \leq n-1$ il existe un sous-automate $\mathcal{A}_{E_i=e_iF_i}$ tel que q_γ soit un état de $\mathcal{A}_{E_i=e_iF_i}$ pour tout $\beta_i < \gamma \leq \beta_{i+1}$ (si $i = n-1$ le sous-automate en question peut être $\mathcal{A}_{E_{n-1}=e_{n-1}}$ pour une certaine equation $E_{n-1} = e_{n-1}$ de G, et seulement dans ce cas là), et de plus $u[\beta_i, \beta_{i+1}[\in \overline{e_i}$. Donc $u \in \overline{e_0e_1\ldots e_{n-1}}$. Encore par construction de $\mathcal{A}_G$, pour tout $i < n-1$ il existe une suite finie $E'_{i,1} = e'_{i,1}F'_{i,1}, \ldots, E'_{i,m_i} = e'_{i,m_i}F'_{i,m_i}$ d'équations de G telle que $E'_{i,1} = E_i$, $e'_{i,1} = e_i$, $F'_{i,1} = F_i$, $\lambda \in \overline{e'_{i,j}}$ pour tout $1 < j < m_i$, $F'_{i,j} = E'_{i,j+1}$ pour tout $1 \leq j < m_i$, $E'_{i,m_i} = E_{i+1}$, $e'_{i,m_i} = e_{i+1}$ et $F'_{i,m_i} = F_{i+1}$ (éventuellement $E'_{n-2,m_{n-2}} = E_{n-1}$ et $e'_{n-2,m_{n-2}} = e_{n-1}$). De même il existe une suite finie $E'_1 = e'_1F'_1, \ldots, E'_m = e'_mF'_m$ d'équations de G telle que $E'_1 = S$, $\lambda \in \overline{e'_i}$ pour tout $1 \leq j < m$, $F'_j = E'_{j+1}$ pour tout $1 \leq j < m$, $E'_m = E_0$, $e'_m = e_0$ et $F'_m = F_0$. Finalement, puisque

q_α est un état du sous-automate $\mathcal{A}_{E=eF}$, il existe une équation $E' = e'$ de G et une suite $E''_1 = e''_1 F''_1, \ldots, E''_k = e''_k F''_k$ d'équations de G telles que $E = E''_1$, $e = e''_1$, $F = F''_1$, $\lambda \in \overline{e''_i}$ pour tout $1 < i \leq k$, $F''_i = E''_{i+1}$ pour tout $1 \leq i < k$, $F''_k = E'$ et $\lambda \in \overline{e'}$. Par conséquent

$$S \underset{G}{\overset{*}{\Rightarrow}} e'_1 \ldots e'_{m-1} e_0 e'_{0,2} \ldots e'_{0,m_1-1} e_1 e'_{1,2} \ldots e'_{n-1,m_{n-1}-1} e e''_2 \ldots e''_k e'$$

et comme $u \in \overline{e_0 e_1 \ldots e_{n-1}}$ on a $u \in \mathcal{L}(G)$. Réciproquement, si $u \in \mathcal{L}(G)$ il existe $e \in T^*$ telle que $S \Rightarrow^*_G e$ et $u \in \overline{e}$. Il existe donc une suite $E_1 = e_1 F_1, \ldots, E_n = e_n F_n, E_{n+1} = e_{n+1}$ telle que $F_i = E_{i+1}$ pour tout $1 \leq i \leq n$, $S = E_1$ et $e = e_1 e_2 \ldots e_n e_{n+1}$. On vérifie aisément que $u \in \mathcal{L}(A)$. ∇

Ce qui termine la preuve du théorème. ∇

Nous retournons maintenant à la preuve de la proposition 3.4.25 :

Preuve La preuve est par induction sur i. Si $i = 0$, alors on se rapporte à la théorie des mots finis : le théorème 3.1.1 montre que $\varphi^{-1}(X)$ est rationnelle, donc C-rationnelle. Supposons maintenant que i soit positif. Nous allons montrer que

$$\varphi^{-1}(X) = \bigcup_{(s,e,t) \in Y_X} \varphi^{-1}(s) \varphi^{-1}(e)^\omega \varphi^{-1}(t)$$

où Y_X est l'ensemble des triplets $(s, e, t) \in S_{i-1} \times S_{i-1} \times S^1$ tels que (s, e) est un couple lié, $se^\omega t \in X$ et $ty(t) \leq i$. Tout d'abord, si u est un mot du membre droit de l'égalité, alors $\varphi(u) = se^\omega t \in X$ et donc u est également un mot du membre gauche. Supposons maintenant que $u \in \varphi^{-1}(X)$. En utilisant la proposition 3.4.24 il existe $(s, e, t) \in Y_X$ tel que $\varphi(u) = se^\omega t$. Il reste à prouver que le membre droit de l'égalité est C-rationnel. Comme les parties C-rationnelles sont fermées par union finie nous supposons que $|Y_X| = 1$. Par hypothèse de récurrence, $\varphi^{-1}(s)$ et $\varphi^{-1}(e)$ sont toutes deux C-rationnelles, donc $\varphi^{-1}(s)\varphi^{-1}(e)^\omega$ l'est aussi. D'autre part, on a nécessairement $ty(t) \leq i$. Si $ty(t) < i$ alors l'hypothèse de récurrence et la fermeture des parties C-rationnelles par produit fini montre directement le résultat. Supposons que $ty(t) = i$. On a de nouveau l'égalité

$$\varphi^{-1}(t) = \bigcup_{(s,e,t_1) \in Y_t} \varphi^{-1}(s) \varphi^{-1}(e)^\omega \varphi^{-1}(t_1)$$

où Y_t est l'ensemble des triplets $(s, e, t_1) \in S_{i-1} \times S_{i-1} \times S^1$ tels que (s, e) est un couple lié, $se^\omega t_1 = t$ et $ty(t_1) \leq i$. Le même raisonnement est applicable à tous les t_1 de Y_t, et ainsi de suite autant de fois que necessaire. Comme S_i est fini, on trouve le système fini d'équations

$$\begin{aligned}
\varphi^{-1}(X) &= \bigcup_{(s,e,t)\in Y_X} \varphi^{-1}(s)\varphi^{-1}(e)^\omega\varphi^{-1}(t)\\
\varphi^{-1}(t) &= \bigcup_{(s,e,t_1)\in Y_t} \varphi^{-1}(s)\varphi^{-1}(e)^\omega\varphi^{-1}(t_1)\\
&\vdots\\
\varphi^{-1}(t_n) &= \bigcup_{(s,e,t_n)\in Y_{t_n}} \varphi^{-1}(s)\varphi^{-1}(e)^\omega\varphi^{-1}(t_k)
\end{aligned}$$

où chaque t_k de Y_{t_n} est élément de $\{t, t_1, t_2, \ldots, t_n\}$. A partir de cet ensemble d'équations on constitue une grammaire sans contexte linéaire droite dont les variables sont $\varphi^{-1}(X)$ et chaque $\varphi^{-1}(t_j)$ avec $ty(t_j) = i$, l'alphabet A, l'ensemble des C-expressions rationnelles est l'union de l'ensemble des $\varphi^{-1}(s)\varphi^{-1}(e)^\omega$ et de l'ensemble des $\varphi^{-1}(s)\varphi^{-1}(e)^\omega\varphi^{-1}(t_j)$ avec $ty(t_j) < i$ et le symbole de départ $\varphi^{-1}(X)$. D'après le théorème 3.4.26 $\varphi^{-1}(X)$ est C-rationnelle. ∇

Les propositions 3.4.23 et 3.4.25 donnent respectivement le premier et le second sens de la preuve du résultat principal de cette section.

3.4.3 ω^n-semigroupe syntaxique

Soient A un alphabet et X une partie reconnaissable de $A^{[1,\omega^{n+1}[}$. Nous montrons maintenant que parmi tous les ω^n-semigroupes finis qui reconnaissent X il en existe un unique qui divise tous les autres, et qui par conséquent est minimal en termes de nombre d'éléments. On peut donc associer à chaque partie reconnaissable X de $A^{[1,\omega^{n+1}[}$ un ω^n-semigroupe de façon canonique. Cet ω^n-semigroupe s'appelle l'ω^n-semigroupe syntaxique de X. Ceci étend les théorèmes 3.1.2 et 3.2.6 aux ensembles de mots de longueur inférieure à ω^{n+1}.

Soient S une ω^n-algèbre de Wilke et P une partie de S. Nous commençons par définir une congruence d'algèbre de Wilke associée à la partie P.

Lemme 3.4.29 *Soient n un entier, S une ω^n-algèbre de Wilke et P un sous ensemble de S. La relation d'équivalence $\sim_P$ définie par, pour tout entier i inférieur ou égal à n et $x, y \in S_i$, $x \sim_P y$ si, pour tout $r, t \in S^1$,*

$$rxt \in P \iff ryt \in P \tag{3.2}$$

et, pour tout entier $m > 1$ et $y_0, y_1, \ldots, y_m \in S^1$ tels que $y_0(\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_m$ soit défini

$$y_0(\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_m \in P \iff y_0(\ldots(((yy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_m \in P \tag{3.3}$$

est une congruence d'ω^n-algèbre de Wilke.

Preuve Montrons d'abord que $x \sim_P y \Rightarrow rxt \sim_P ryt$ pour tout $r, t \in S^1$. Supposons que $x \sim_P y$. Soient r, t deux éléments de S^1. D'après 3.2 il vient que $r'xt' \in P \iff r'yt' \in P$ pour tout $r', t' \in S^1$. En particulier, $(r'r)x(tt') \in P \iff (r'r)y(tt') \in P$ quels que soient $r', t' \in S^1$. Comme le produit est associatif $r'(rxt)t' \in P \iff r'(ryt)t' \in P$ pour tout $r', t' \in S^1$. Donc 3.2 est prouvée. Passons à 3.3. On a, pour tout entier $m > 1$ et $y_0, y_1, \ldots, y_m \in S^1$ tels que $y_0(\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_m$ soit défini

$$y_0((\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_{m-1})^\omega y_m \in P \iff y_0((\ldots(((yy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_{m-1})^\omega y_m \in P$$

en substituant y_i par $y_i r$ pour chaque i inférieur à m, et y_1 par ty_1 dans l'équivalence ainsi obtenue on trouve

$$y_0 r((\ldots(((xty_1 r)^\omega y_2 r)^\omega y_3 r)^\omega \ldots)^\omega y_{m-1} r)^\omega y_m \in P \iff y_0 r((\ldots(((yty_1 r)^\omega y_2 r)^\omega y_3 r)^\omega \ldots)^\omega y_{m-1} r)^\omega y_m \in P$$

c'est-à-dire

$$y_0(r(\ldots(((xty_1 r)^\omega y_2 r)^\omega y_3 r)^\omega \ldots)^\omega y_{m-1})^\omega y_m \in P \iff y_0(r(\ldots(((yty_1 r)^\omega y_2 r)^\omega y_3 r)^\omega \ldots)^\omega y_{m-1})^\omega y_m \in P$$

en appliquant le même argument $m-2$ fois

$$y_0((\ldots(((rxty_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_{m-1})^\omega y_m \in P \iff y_0((\ldots(((ryty_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_{m-1})^\omega y_m \in P$$

donc $x \sim_P y \Rightarrow rxt \sim_P ryt$ pour tout $r, t \in S^1$.

Il reste à prouver que si i est inférieur à n alors $x \sim_P y \Rightarrow x^\omega \sim_P y^\omega$. Supposons que $x \sim_P y$. Alors, pour chaque $y_0, y_1, y_2 \in S^1$ tels que $y_0(xy_1)^\omega y_2$ soit défini, c'est-à-dire que pour tout $y_0, y_1, y_2 \in S^1$ tels que $ty(y_1) < n$, on a $y_0(xy_1)^\omega y_2 \in P \iff y_0(yy_1)^\omega y_2 \in P$. Il suffit de prendre $y_1 = 1$ pour obtenir 3.2. La preuve de 3.3 utilise exactement le même argument. ∇

Intuitivement, on obtient effectivement l'ω^n-semigroupe syntaxique d'une partie X reconnaissable d'un ω^n-semigroupe par application de la congruence précédement définie sur l'ω^n-algèbre de Wilke associée à un ω^n-semigroupe fini qui reconnaît X.

Proposition 3.4.30 *Soient n un entier, T un ω^n-semigroupe, et X une partie reconnaissable de T. Parmi toutes les congruences d'ω^n-semigroupes $\sim_X$ telles que $T/\sim_X$ reconnaisse X, il en existe une unique moins fine que toutes les autres. Le nombre de classes d'équivalences pour cette congruence, qui est minimal, est fini. Cette congruence d'ω^n-semigroupes, appelée* **congruence syntaxique de** X, *est définie par : pour tout entier i inférieur ou égal à n et $x, y \in T_i$, $x \sim_X y$ si, pour tout $r, t \in T^1$,*

$$rxt \in X \iff ryt \in X \tag{3.4}$$

et, pour tout entier $m > 1$ *et* $y_0, y_1, \ldots, y_m \in T^1$ *tels que* $y_0(\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_m$ *soit défini,*

$$y_0(\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_m \in X \iff y_0(\ldots(((yy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_m \in X \qquad (3.5)$$

L'ω^n-semigroupe quotient $T/\sim_X$ est appelé **l'ω^n-semigroupe syntaxique** de X.

Preuve Nous devons d'abord montrer que ceci défini bien une congruence d'ω^n-semigroupes. Soient S un ω^n-semigroupe fini et $\varphi : T \to S$ un morphisme d'ω^n-semigroupes surjectif tels que φ reconnaisse X (on peut toujours supposer que φ est surjectif, quitte à changer S pour $\varphi(T)$). Soit également $P = \varphi(X)$. On montre le lemme suivant :

Lemme 3.4.31 *On a* $u \sim_X v \iff \varphi(u) \sim_P \varphi(v)$ *pour tout* $u, v \in T$.

Preuve D'abord le sens de la gauche vers la droite. Pour tout $r, t \in S^1$, il existe $r', t' \in T^1$ tels que $\varphi(r') = r$ et $\varphi(t') = t$ (on suppose que $\varphi(1) = 1$). Donc $r\varphi(u)t \in P \iff r'ut' \in X \iff r'vt' \in X \iff r\varphi(v)t \in P$. On prouve la seconde égalité en utilisant le même argument. Passons à la réciproque. Supposons que $\varphi(u) \sim_P \varphi(v)$. Ceci implique que $r\varphi(u)t \in P \iff r\varphi(v)t \in P$ pour tout $r, t \in S^1$. Pour tout $r, t \in T^1$,

$$\begin{aligned} rut \in X \iff \varphi(rut) \in P \iff \varphi(r)\varphi(u)\varphi(t) \in P \\ \iff \varphi(r)\varphi(v)\varphi(t) \in P \iff rvt \in X \end{aligned}$$

Donc la première équivalence est prouvée. La seconde se montre en utilisant le même argument. ∇

Retournons maintenant à la preuve de la proposition. Pour une preuve de $u \sim_X v \Rightarrow rut \sim_X rvt$ quels que soient $r, t \in T^1$ nous renvoyons à la première partie de la preuve du lemme 3.4.29. Il reste à montrer que $\sim_X$ préserve les ω-produits $\overline{\pi}_i$ de la définition 3.4.3. Soient $(u_i)_{i<\omega}$ et $(v_i)_{i<\omega}$ deux suites d'éléments de T_j pour j inférieur à n et telles que $u_i \sim_X v_i$ pour tout entier i. Soient $r, t \in T^1$ et $\psi : T^2 \to S^2$ le morphisme d'ω^n-semigroupes défini par $\psi((x, y)) = (\varphi(x), \varphi(y))$. D'après le corollaire 3.3.8 il existe une suite strictement croissante d'entiers $(j_k)_{k<\omega}$ et un couple lié $((s, s'), (e, e'))$ de S^2 tels que $j_0 = 0$, $\psi(\prod_{i=j_0}^{j_1-1}(u_i, v_i)) = (s, s')$ et $\psi(\prod_{i=j_k}^{j_{k+1}-1}(u_i, v_i)) = (e, e')$ pour tout entier k positif. Comme $\varphi(u_i) \sim_P \varphi(v_i)$ pour tout entier i,

$$s = \varphi(\prod_{i=j_0}^{j_1-1} u_i) = \prod_{i=j_0}^{j_1-1} \varphi(u_i) \sim_P \prod_{i=j_0}^{j_1-1} \varphi(v_i) = \varphi(\prod_{i=j_0}^{j_1-1} v_i) = s'$$

On montre en utilisant le même argument que $e \sim_P e'$. On a alors

$$\begin{aligned} ru_0u_1 \ldots t \in X \iff \varphi(r)\varphi(u_0u_1\ldots)\varphi(t) \in P \iff \varphi(r)se^\omega\varphi(t) \in P \\ \iff \varphi(r)s'e'^\omega\varphi(t) \in P \iff \varphi(r)\varphi(v_0v_1\ldots)\varphi(t) \in P \iff rv_0v_1\ldots t \in X \end{aligned}$$

Donc 3.4 est montrée. La preuve de 3.5 utilise exactement le même argument. Pour finir il faut montrer que toute autre congruence $\sim'_X$ d'ω^n-semigroupe telle que $T/\sim'_X$ reconnaisse

X est plus fine que $\sim_X$. Supposons l'existence de $\sim'_X$, et soit $\varphi : T \to T/\sim'_X$ le morphisme de ω^n-semigroupes naturel qui à chaque élément de T associe sa classe d'équivalence dans $T/\sim'_X$. Posons $\varphi'(X) = P'$. Alors, $\varphi'(x) = \varphi'(y) \iff x \sim'_X y$. Supposons que $x \sim'_X y$ et soient $u, v \in T^1$. On peut écrire

$$uxv \in X \iff \varphi'(u)\varphi'(x)\varphi'(v) \in P' \iff \varphi'(u)\varphi'(y)\varphi'(v) \in P' \iff uyv \in X$$

ce qui prouve la première équivalence de $x \sim_X y$. La preuve de la seconde est similaire. Donc $x \sim'_X y \Rightarrow x \sim_X y$, et $\sim'_X$ est plus fine que $\sim_X$. En particulier, $\sim_X$ a moins de classes d'équivalence que $\sim'_X$ si $\sim_X$ et $\sim'_X$ sont différentes. Le lemme 3.4.31 montre que le nombre de classes d'équivalence de $\sim_X$ est fini. La preuve de la proposition est donc terminée. ∇

Exemple 3.4.32 *Soit $\{a, b\}$ un alphabet. L'ω^1-semigroupe de l'exemple 3.4.9 est l'ω^1-semigroupe syntaxique de $(aa + b)^{<\omega^2} - \lambda$.*

Exemple 3.4.33 *Soit $\{a, b\}$ un alphabet. L'ω^1-semigroupe de l'exemple 3.4.10 est l'ω^1-semigroupe syntaxique de $(ab)^{<\omega^2} - \lambda$.*

L'ω^n-semigroupe d'une partie reconnaissable X est le plus petit, au sens de la division, qui reconnait X :

Théorème 3.4.34 *Soient A un alphabet, n un entier et X une partie reconnaissable de $A^{[1,\omega^{n+1}[}$. Un ω^n-semigroupe T reconnait X si et seulement si $S(X)$ divise T. De plus, si T divise un troisième ω^n-semigroupe U, alors U reconnait X.*

Preuve Soit d'abord $\varphi : A^{[1,\omega^{n+1}[} \to T$ un morphisme qui reconnait X. Alors $\varphi(A^{[1,\omega^{n+1}[})$ est un sous-ω^{n+1}-semigroupe de T qui reconnait X. Par la proposition 3.4.11 $A^{[1,\omega^{n+1}[}/\sim_\varphi$ est isomorphe à $\varphi(A^{[1,\omega^{n+1}[})$. D'autre part, $\sim_\varphi$ est plus fine que $\sim_X$ donc

$$S(X) = A^{[1,\omega^{n+1}[}/\sim_X < T$$

Supposons maintenant que $S(X) < T$. Il existe alors un sous-ω^{n+1}-semigroupe U de T et un morphisme surjectif $\varphi' : U \to S(X)$. Soit $\varphi : A^{[1,\omega^{n+1}[} \to S(X)$. D'après le corollaire 3.4.8 il existe un morphisme $\varphi'' : A^{[1,\omega^{n+1}[} \to U$ tel que $\varphi'' = \varphi'\varphi$. En posant $P = \varphi'^{-1}\varphi(X)$ on a alors

$$\varphi''^{-1}(P) = \varphi''^{-1}(\varphi'^{-1}\varphi(X)) = \varphi^{-1}\varphi(X) = X$$

ce qui montre que X est reconnu par U et donc par T. On montre de la même façon la seconde partie de l'énoncé. ∇

3.5 Mots de longueur dénombrable

La théorie des ω^n-semigroupes repose sur le fait que tout ordinal inférieur à ω^ω s'écrit en forme normale de Cantor comme somme d'un nombre fini de termes (théorème 1.4.23)

$$\alpha = \omega^k \cdot n_k + \omega^{k-1} \cdot n_{k-1} + \cdots + \omega^0 \cdot n_0$$

où k et les n_i sont des entiers naturels, et que $\omega^{n+1} = \omega^n \cdot \omega$, c'est-à-dire qu'un mot de longueur ω^{n+1} se décompose en ω facteurs de longueur ω^n, ce qui nous permet d'utiliser le théorème de Ramsey.

Le théorème 1.4.14 nous indique que tout mot de longueur un ordinal limite dénombrable admet une décomposition en ω facteurs, ce qui va nous permettre d'utiliser à nouveau le théorème de Ramsey pour calculer l'image de mots dans une nouvelle structure algébrique, les ω_1-semigroupes, plus pauvre que les ω^n-semigroupes. En effet ces derniers sont composés d'"étages", et l'étage dans lequel se trouve l'image d'un mot dépend de sa longueur : un mot dont la longueur est dans l'intervalle $[\omega^i, \omega^{i+1}[$ a pour image un élément du i-ième étage dans un ω^n-semigroupe. Cette idée est à abandonner quand on traite de mots de longueur supérieure ou égale à ω^ω.

Nous suivons dans cette section un plan analogue à celui de la précédente : nous définissons d'abord les ω_1-semigroupes, puis nous montrons qu'ils admettent une description finie quand leur nombre d'élément est fini. Nous prouvons ensuite l'équivalence entre ω_1-semigroupes finis et D-automates, puis nous montrons qu'on peut effectivement associer un ω_1-semigroupe syntaxique à chaque langage reconnaissable de mots de longueur dénombrable. Nous généralisons les opérations de produit de Schützenberger et produit en couronne aux ω_1-semigroupes. Enfin, nous étendons le théorème de correspondance entre variétés de langages et pseudo-variétés de semigroupes au cas des mots de longueur dénombrable.

3.5.1 Définitions algébriques

Nous définissons maintenant la principale structure algébrique de cette section. Intuitivement, les ω_1-semigroupes sont une généralisation des semigroupes dans lesquels les produits d'éléments de suites de type dénombrable sont autorisés, et cela de façon associative.

Définition 3.5.1 *Soient α_1 et α_2 deux ordinaux dénombrables tels que $\alpha_1 < \alpha_2$, S un ensemble et $(s_\gamma)_{\alpha_1 \leq \gamma < \alpha_2}$ une suite d'éléments de S. Une* **factorisation** *de $(s_\gamma)_{\alpha_1 \leq \gamma < \alpha_2}$ est une suite strictement croissante $(\beta_\gamma)_{\gamma \leq \delta}$ telle que $\beta_0 = \alpha_1$, $\beta_\delta = \alpha_2$, et si $(\gamma_i)_{i<\omega}$ est une suite strictement croissante de type ω d'ordinaux inférieurs à δ et $(\beta_{\gamma_i})_{i<\omega}$ est cofinale avec ξ, il existe $\gamma \leq \delta$ tel que $\beta_\gamma = \xi$.*

Définition 3.5.2 *Un ω_1-***semigroupe** *est un ensemble S équipé, pour chaque ordinal positif α dénombrable, d'une application $\overline{\alpha} : S^\alpha \to S$ qui vérifie : pour toute suite $(s_\gamma)_{\gamma<\alpha}$ de type α d'éléments de S et pour chaque factorisation $(\beta_\gamma)_{\gamma\leq\delta}$ de $(s_\gamma)_{\gamma<\alpha}$,*

$$\overline{\delta}((\overline{\beta_{\gamma+1} - \beta_\gamma}((s_\varsigma)_{\beta_\gamma \leq \varsigma < \beta_{\gamma+1}}))_{\gamma<\delta}) = \overline{\alpha}((s_\varsigma)_{0\leq\varsigma<\alpha})$$

*L'application $\overline{\alpha}$ est dite α-***associative***. Nous écrirons quelquefois s plutôt que $\overline{1}(s)$ et $\overline{\alpha}(s_0, s_1, \dots)$ plutôt que $\overline{\alpha}((s_\gamma)_{\gamma<\alpha})$.*

Nous aurions pu, comme nous l'avions fait pour les ω^n-semigroupes, équiper les ω_1-semigroupes avec une unique application qui étend le produit des semigroupes usuels et dont l'arité n'est pas fixe, plutôt qu'avec autant d'applications qu'il y a d'ordinaux dénombrables comme nous l'avons fait ici. Les deux présentations sont équivalentes.

Exemple 3.5.3 *Soit A un alphabet. L'ensemble $A^{<\omega_1}$ des mots sur A de longueur dénombrable, muni du produit de concaténation de mots, est un ω_1-semigroupe, appelé l'ω_1-semigroupe libre sur A.*

Comme dans un ω_1-semigroupe la description de chaque application $\overline{\alpha}$ n'est pas finie dès que α est infini, et comme de plus il en existe une infinité, les ω_1-semigroupes ne sont pas des objets vraiment intéressants, même quand leur nombre d'élément est fini. Nous allons montrer, toujours en utilisant les idées de Wilke, que quand un ω_1-semigroupe S est fini, pour tout ordinal α dénombrable supérieur à ω et toute suite $(s_\gamma)_{\gamma<\alpha}$, le produit $\overline{\alpha}((s_\gamma)_{\gamma<\alpha})$ est entièrement déterminé par $\overline{2}$ et les produits de la forme $\overline{\omega}(s)$, où s est une suite de type ω d'éléments de S tous identiques. Les ω_1-semigroupes finis deviennent alors des objets vraiment finis.

Définition 3.5.4 *Une* ω_1**-algèbre de Wilke** *S est un semigroupe fini muni d'une application interne unaire ω qui vérifie, pour tout $s, t \in S$*
- *$s(ts)^\omega = (st)^\omega$,*
- *$(s^n)^\omega = s^\omega$ pour tout $n > 0$.*

Remarque 3.5.5 *Il suffit de définir l'application ω sur les idempotents d'une ω_1-algèbre de Wilke S pour la définir sur tous les éléments de S. En effet, si $s \in S$, alors $s^\omega = (s^\pi)^\omega = s^\pi(s^\pi)^\omega$, or (s^π, s^π) est un couple lié de S.*

Le théorème suivant montre qu'ω_1-semigroupes finis et ω_1-algèbres de Wilke sont équivalents :

Théorème 3.5.6 *Soit S un ensemble fini equipé d'un produit associatif binaire et d'une application interne unaire $\omega : S \to S$ qui vérifie les deux propriétés de l'application ω de la définition 3.5.4. Alors S peut être muni d'une façon et d'une seule avec, pour tout ordinal dénombrable α positif, une application $\overline{\alpha} : S^\alpha \to S$ qui est α-associative et telle que $\overline{2}((s_\gamma)_{0\leq\gamma\leq1}) = s_0 \cdot s_1$ pour tout $s_0, s_1 \in S$ et pour tout $s \in S$, si s' désigne la suite de type ω dont tous les éléments sont s, alors $\overline{\omega}(s') = s^\omega$.*

Réciproquement, si S est un ensemble fini muni, pour tout ordinal dénombrable α positif, une application $\overline{\alpha} : S^\alpha \to S$ qui est α-associative, il peut être muni d'une façon et d'une seule d'un produit associatif binaire $\cdot$ tel que $\overline{2}((s_\gamma)_{0\leq\gamma\leq1}) = s_0 \cdot s_1$ pour tout $s_0, s_1 \in S$ et d'une application interne unaire $\omega : S \to S$ qui vérifie les deux propriétés de l'application ω de la définition 3.5.4 et telle que pour tout $s \in S$, si s' désigne la suite de type ω dont tous les éléments sont s, alors $\overline{\omega}(s') = s^\omega$.

Preuve Soit d'abord S un ensemble fini muni, pour chaque ordinal dénombrable α, d'une application $\overline{\alpha} : S^\alpha \to S$ qui est α-associative. Le produit défini par $s_0 \cdot s_1 = \overline{2}((s_\gamma)_{0\leq\gamma\leq1})$

pour chaque $s_0, s_1 \in S$ est associatif car

$$x_0 \cdot (x_1 \cdot x_2) = \overline{2}(x_0, \overline{2}(x_1, x_2)) = \overline{3}(x_0, x_1, x_2) = \overline{2}(\overline{2}(x_0, x_1), x_2) = (x_0 \cdot x_1) \cdot x_2$$

Posons $s^\omega = \overline{\omega}(s')$, où s' est la suite de type ω dont tous les éléments sont s. On peut aisément vérifier que l'application ω ainsi définie vérifie les deux propriétés de la définition 3.5.4.

Supposons maintenant que S soit un ensemble fini muni d'une application interne unaire $\omega : S \to S$ qui vérifie les deux propriétés de l'application ω de la définition 3.5.4 et avec un produit binaire associatif. Pour chaque ordinal dénombrable α positif on définit par induction transfinie une application $\overline{\alpha} : S^\alpha \to S$ par $\overline{1}(s_0) = s_0$, $\overline{2}(s_0, s_1) = s_0 \cdot s_1$, $\overline{\alpha+1}((s_\gamma)_{\gamma<\alpha+1}) = \overline{2}(\overline{\alpha}((s_\gamma)_{\gamma<\alpha}), s_\alpha)$ et finalement, si $\alpha \in \mathit{Lim}$ et $(\beta_\gamma)_{\gamma<\omega}$ est une suite strictement croissante d'ordinaux inférieurs à α et cofinale à α telle que $\beta_0 = 0$, $\overline{\beta_1 - \beta_0}((s_\gamma)_{\gamma<\beta_1}) = s$ et $\overline{\beta_{i+1} - \beta_i}((s_\gamma)_{\beta_i \leq \gamma < \beta_{i+1}}) = e$ pour tout $0 < i < \omega$ où (s, e) est un couple lié de S, alors $\overline{\alpha}((s_\gamma)_{\gamma<\alpha}) = s \cdot e^\omega$. Le couple (s, e) et la suite $(\beta_\gamma)_{\gamma<\omega}$ existent toujours d'après le théorème 1.4.14 et le corollaire 3.3.8. Pour montrer que cette définition est cohérente il faut prouver que $\overline{\alpha}((s_\gamma)_{\gamma<\alpha})$ ne dépend pas du couple lié et de la suite choisies : si $(\beta'_\gamma)_{\gamma<\omega}$ et (s', e') sont d'autres choix, il suffit d'utiliser la proposition 3.3.11 pour voir que (s, e) et (s', e') sont deux couples liés conjugués. Il existe donc $x, y \in S^1$ tels que $e = xy$, $e' = yx$ et $s' = sx$. Comme $s(ts)^\omega = (st)^\omega$ il vient $se^\omega = s(xy)^\omega = sx(yx)^\omega = s'e'^\omega$. Il faut maintenant prouver que $\overline{\alpha}$ est α-associative. On procède par induction transfinie sur α. Le cas où $\alpha = 1$ est trivial. Supposons maintenant que α est un ordinal successeur et soient $(s_\gamma)_{\gamma<\alpha+1}$ une suite de type $\alpha+1$ d'éléments de S et $(\beta_\gamma)_{\gamma\leq\delta}$ une factorisation de $(s_\gamma)_{\gamma<\alpha+1}$. On montre que

$$\overline{\delta}((\overline{\beta_{\gamma+1} - \beta_\gamma}((s_\varsigma)_{\beta_\gamma \leq \varsigma < \beta_{\gamma+1}}))_{\gamma<\delta}) = \overline{\alpha+1}((s_\varsigma)_{0\leq\varsigma<\alpha+1})$$

Soit $(\beta'_\gamma)_{\gamma\leq\delta'}$ la suite définie par :

$$\begin{cases} \delta' = \delta, \forall \gamma \leq \delta' \ \beta'_\gamma = \beta_\gamma & \text{si } \beta_{\delta-1} = \alpha \\ \delta' = \delta + 1, \beta'_\delta = \alpha, \beta'_{\delta'} = \alpha + 1, \forall \gamma < \delta \ \beta'_\gamma = \beta_\gamma & \text{sinon} \end{cases}$$

En utilisant la définition de $\overline{\alpha+1}$ et l'hypothèse de récurrence il vient

$$\overline{\alpha+1}((s_\gamma)_{\gamma<\alpha+1}) = \overline{2}(\overline{\alpha}((s_\gamma)_{\gamma<\alpha}), s_\alpha) = \overline{2}(\overline{\delta'-1}((\overline{\beta'_{\gamma+1} - \beta'_\gamma}((s_\varsigma)_{\beta'_\gamma \leq \varsigma < \beta'_{\gamma+1}}))_{\gamma<\delta'-1}), s_\alpha)$$

Si $\beta_{\delta-1} = \alpha$ le résultat découle directement de la définition de $\overline{\delta}$. Si on suppose que $\beta_{\delta-1} \neq \alpha$, comme $\beta_{\delta-1} < \alpha < \beta_\delta$ on a $\delta \notin \mathit{Lim}$, donc ceci est égal à

$$\overline{2}(\overline{2}(\overline{\delta-1}((\overline{\beta'_{\gamma+1} - \beta'_\gamma}((s_\varsigma)_{\beta'_\gamma \leq \varsigma < \beta'_{\gamma+1}}))_{\gamma<\delta-1}), \overline{\beta'_\delta - \beta'_{\delta-1}}((s_\varsigma)_{\beta'_{\delta-1} \leq \varsigma < \beta'_\delta})), s_\alpha)$$

Comme on peut aisément vérifier que $\overline{2}(s_0, \overline{2}(s_1, s_2)) = \overline{2}(\overline{2}(s_0, s_1), s_2)$ ceci est égal à

$$\begin{aligned} &\overline{2}(\overline{\delta-1}((\overline{\beta'_{\gamma+1} - \beta'_\gamma}((s_\varsigma)_{\beta'_\gamma \leq \varsigma < \beta'_{\gamma+1}}))_{\gamma<\delta-1}), \overline{2}(\overline{\beta'_\delta - \beta'_{\delta-1}}((s_\varsigma)_{\beta'_{\delta-1} \leq \varsigma < \beta'_\delta}), s_\alpha)) \\ &= \overline{2}(\overline{\delta-1}((\overline{\beta'_{\gamma+1} - \beta'_\gamma}((s_\varsigma)_{\beta'_\gamma \leq \varsigma < \beta'_{\gamma+1}}))_{\gamma<\delta-1}), \overline{\beta'_{\delta'} - \beta'_{\delta-1}}((s_\varsigma)_{\beta'_{\delta-1} \leq \varsigma < \beta'_{\delta'}})) \\ &= \overline{\delta}((\overline{\beta_{\gamma+1} - \beta_\gamma}((s_\varsigma)_{\beta_\gamma \leq \varsigma < \beta_{\gamma+1}}))_{\gamma<\delta}) \end{aligned}$$

Finalement, supposons que $\alpha \in Lim$, et soient $(s_\gamma)_{\gamma<\alpha}$ une suite de type α d'éléments de S et $(\beta_\gamma)_{\gamma\leq\delta}$ une factorisation de $(s_\gamma)_{\gamma<\alpha}$. Ou bien $(\beta_\gamma)_{\gamma<\delta}$ est cofinale avec α ou non. Supposons d'abord qu'elle le soit. Il existe un couple lié (s, e) et une suite $(\gamma_i)_{i<\omega}$ de type ω d'ordinaux inférieurs à δ tels que

– $\gamma_0 = 0$,
– $\overline{\beta_{\gamma_1} - \beta_{\gamma_0}}((s_\gamma)_{\beta_{\gamma_0}\leq\gamma<\beta_{\gamma_1}}) = s$,
– $\overline{\beta_{\gamma_{i+1}} - \beta_{\gamma_i}}((s_\gamma)_{\beta_{\gamma_i}\leq\gamma<\beta_{\gamma_{i+1}}}) = e$ pour tout entier i positif,
– $(\beta_{\gamma_i})_{i<\omega}$ est cofinale avec α.

La suite $(\gamma_i)_{i<\omega}$ est cofinale avec δ. En utilisant l'hypothèse de récurrence il vient

$$\overline{\beta_{\gamma_{i+1}} - \beta_{\gamma_i}}((s_\gamma)_{\beta_{\gamma_i}\leq\gamma<\beta_{\gamma_{i+1}}}) = \overline{\gamma_{i+1} - \gamma_i}((\overline{\beta_{\gamma+1} - \beta_\gamma}((s_\varsigma)_{\beta_\gamma\leq\varsigma<\beta_{\gamma+1}}))_{\gamma_i\leq\gamma<\gamma_{i+1}})$$

et le résultat vient de la définition de $\overline{\delta}$. Supposons maintenant que $(\beta_\gamma)_{\gamma<\delta}$ n'est pas cofinale avec α. Il suit que $\delta \in Succ$ et $\beta_\delta - \beta_{\delta-1} \in Lim$. Il existe un couple lié (s, e) de S et une factorisation $(\gamma_i)_{i\leq\omega}$ de $(s_\gamma)_{\beta_{\delta-1}\leq\gamma<\beta_\delta}$ telle que

– $(\gamma_i)_{i<\omega}$ est cofinale avec α,
– $\overline{(\beta_{\delta-1} + \gamma_1) - (\beta_{\delta-1} + \gamma_0)}((s_\varsigma)_{\beta_{\delta-1}+\gamma_0\leq\varsigma<\beta_{\delta-1}+\gamma_1}) = s$,
– $\overline{(\beta_{\delta-1} + \gamma_{i+1}) - (\beta_{\delta-1} + \gamma_i)}((s_\varsigma)_{\beta_{\delta-1}+\gamma_i\leq\varsigma<\beta_{\delta-1}+\gamma_{i+1}}) = e$ pour tout entier i positif

donc $\overline{\beta_\delta - \beta_{\delta-1}}((s_\varsigma)_{\beta_{\delta-1}\leq\varsigma<\beta_\delta}) = se^\omega$ par définition. Soit $x = \overline{\beta_{\delta-1} - \beta_0}((s_\varsigma)_{\beta_0\leq\varsigma<\beta_{\delta-1}})$ si $\delta - 1 > 0$, l'élément neutre pour le produit de S sinon. Comme la suite $(\gamma'_i)_{i\leq\omega}$ définie par $(\gamma'_i)_{i\leq\omega} = (\gamma_i)_{i\leq\omega}$ si $\delta - 1 = 0$, $\gamma'_0 = 0$, $\gamma'_{i+1} = \gamma_i$ pour tout entier i et $\gamma'_\omega = \alpha$ sinon est une factorisation de $(s_\gamma)_{\gamma<\alpha}$ telle que $(\gamma'_i)_{i<\omega}$ soit cofinale avec α qui vérifie $\overline{\beta_{\gamma'_2} - \beta_{\gamma'_0}}((s_\varsigma)_{\varsigma<\beta_{\gamma'_2}}) = xs$ et $\overline{\beta_{\gamma'_{i+1}} - \beta_{\gamma'_i}}((s_\varsigma)_{\beta_{\gamma'_i}\leq\varsigma<\beta_{\gamma'_{i+1}}}) = e$ pour tout entier $i \geq 2$ on a $\overline{\alpha}((s_\varsigma)_{\varsigma<\alpha}) = xse^\omega$. On a donc

$$\begin{aligned}
&\overline{\delta}((\overline{\beta_{\gamma+1} - \beta_\gamma}((s_\varsigma)_{\beta_\gamma\leq\varsigma<\beta_{\gamma+1}}))_{\gamma<\delta}) \\
&= \overline{2}(\overline{\delta - 1}((\overline{\beta_{\gamma+1} - \beta_\gamma}((s_\varsigma)_{\beta_\gamma\leq\varsigma<\beta_{\gamma+1}}))_{\gamma<\delta-1}), \overline{\beta_\delta - \beta_{\delta-1}}((s_\varsigma)_{\beta_{\delta-1}\leq\varsigma<\beta_\delta})) \\
&= \overline{2}(\overline{\beta_{\delta-1}}((s_\varsigma)_{\beta_0\leq\varsigma<\beta_{\delta-1}}), \overline{\beta_\delta - \beta_{\delta-1}}((s_\varsigma)_{\beta_{\delta-1}\leq\varsigma<\beta_\delta})) \\
&= xse^\omega
\end{aligned}$$

ce qui termine la preuve de l'α-associativé.

Il reste à vérifier que si $s' = (s''_i)_{i<\omega}$ est une suite de type ω telle que tous ses éléments soit s pour un $s \in S$, alors $\overline{\omega}(s') = s^\omega$. Soit π l'exposant de S et $(\beta_\gamma)_{\gamma\leq\omega}$ la factorisation de s' définie par $\beta_i = i\pi$ pour tout entier i et $\beta_\omega = \omega$. On a $\overline{\beta_{i+1} - \beta_i}((s''_\gamma)_{\beta_i\leq\gamma<\beta_{i+1}}) = s^\pi$ pour tout entier i, et comme (s^π, s^π) est un couple lié de S il vient que $\overline{\omega}(s') = s^\pi(s^\pi)^\omega = (s^\pi)^\omega = s^\omega$. ∇

Dans la suite nous confondrons souvent ω_1-semigroupes finis et ω_1-algèbres de Wilke.

De la même façon qu'on peut toujours ajouter un élément neutre à un semigroupe pour en faire un monoïde, on peut toujours ajouter un élément neutre 1 à un ω_1-semigroupe pour en faire un **ω_1-monoïde**. Un élément 1 d'un ω_1-semigroupe S est dit **neutre** si, pour tout ordinal α dénombrable et suite $(s_\beta)_{\beta<\alpha}$ d'éléments de S, alors $\overline{\alpha}((s_\beta)_{\beta<\alpha}) = \overline{\gamma}((s'_\beta)_{\beta<\gamma})$, où

$(s'_\beta)_{\beta<\gamma}$ est la suite construite à partir de $(s_\beta)_{\beta<\alpha}$ en en retirant les 1. Dans le cas particulier où $(s_\beta)_{\beta<\alpha}$ n'est composée que de 1 alors on doit avoir $\overline{\alpha}((s_\beta)_{\beta<\alpha}) = 1$.

Un élément 1 d'une ω_1-algèbre de Wilke S est neutre si $1 \cdot s = s \cdot 1 = s$ quel que soit $s \in S$ et $1^\omega = 1$.

Si S est un ω_1-semigroupe (resp. une ω_1-algèbre de Wilke), dans la suite nous noterons S^1 l'ω_1-monoïde (resp. ω_1-algèbre de Wilke) obtenu en ajoutant un élément neutre 1 à S s'il n'en avait pas déjà un.

Encore une fois, les notions de **morphisme d'ω_1-semigroupes** et de reconnaissance par morphisme viennent directement de l'algèbre universelle, même si les opérations qu'on s'autorise ne sont pas d'arité finie.

Voici l'analogue de la proposition 3.4.7 pour les ω_1-semigroupes :

Proposition 3.5.7 *Soient A un alphabet et n un entier. Soient également T un ω_1-semigroupe et φ une application de A dans T. Alors φ peut être étendue d'une façon unique en un morphisme $\varphi' : A \to T$ d'ω_1-semigroupes tel que $\varphi(a) = \varphi'(a)$ pour tout $a \in A$.*

Corollaire 3.5.8 *Soient A un alphabet et n un entier. Soient également $\varphi : A^{<\omega_1} \to T$ et $\varphi' : U \to T$ deux morphismes d'ω_1-semigroupes tels que φ' soit surjectif. Alors il existe un unique morphisme $\varphi'' : A^{<\omega_1} \to U$ tel que $\varphi = \varphi'\varphi''$.*

Exemple 3.5.9 *Soient $A = \{a, b\}$ et $S = \{a, b, 0, 1, ab, ba, aba, a^\omega, a^\omega a\}$ l'ω_1-semigroupe donné par la structure en $\mathcal{D}$-classes*

* $1, a$

* b	ba
ab	* aba
* a^ω	* $a^\omega a$

* 0

où 0 un zéro pour S, 1 est l'élément neutre de S pour le produit seulement, $a^2 = 1$, $bab = 0$, $ba^\omega = b$, $a^\omega b = a^\omega$, $a^\omega ab = 0$, $b^\omega = b$ et $(a^\omega)^\omega = a^\omega$. Soit également $\varphi : A^{[1,\omega_1[} \to S$ le morphisme d'ω_1-semigroupes défini par $\varphi(a) = a$, $\varphi(b) = b$ et par utilisation de la proposition 3.5.7. Alors S reconnait $L = (aa + b)^{<\omega_1} - \lambda$ puisque $L = \varphi^{-1}(\{1, b, a^\omega\})$.

Exemple 3.5.10 *Soient $A = \{a, b\}$ et $S = \{a, b, 0, ab, ba\}$ l'ω_1-semigroupe donné par la structure en $\mathcal{D}$-classes*

a	$^*\,ab$
$^*\,ba$	b

$^*\,0$

où 0 est un zéro pour S, $a^2 = b^2 = 0$, $aba = a$, $bab = b$ et $(ab)^\omega = ab$. Soit également $\varphi : A^{[1,\omega_1[} \to S$ le morphisme d'ω_1-semigroupes défini par $\varphi(a) = a$, $\varphi(b) = b$ et par utilisation de la proposition 3.5.7. Alors S reconnait $L = (ab)^{<\omega_1} - \lambda$ puisque $L = \varphi^{-1}(\{ab\})$.

Nous donnons maintenant quelques résultats qui nous serons utiles par la suite. Le premier est l'analogue de la proposition 3.4.11 pour les mots de longueur dénombrable :

Proposition 3.5.11 *Soit $\varphi : S \to T$ un morphisme d'ω_1-semigroupes, et $\varphi' : S \to S/{\sim_\varphi}$ le morphisme d'ω_1-semigroupes naturel qui associe à chaque élément de S sa classe de congruence dans $S/{\sim_\varphi}$. Il existe un unique morphisme d'ω_1-semigroupes $\varphi'' : S/{\sim_\varphi} \to T$ tel que $\varphi = \varphi''\varphi'$. De plus, φ'' est un isomorphisme de $S/{\sim_\varphi}$ dans $\varphi(S)$.*

Proposition 3.5.12 *Soient $(\sim_i)_{i<n}$ une famille de congruences d'ω_1-semigroupes sur S, et $\sim$ la congruence définie par $s \sim s'$ si et seulement si $s \sim_i s'$ pour tout i inférieur à n. Alors $S/\sim$ est un sous-ω_1-semigroupe de $\prod_{i<n} S/\sim_i$.*

Preuve Soient $\varphi_i : S \to S/\sim_i$ les morphismes naturels associés à $\sim_i$ pour chaque $i < n$ et $\varphi : S \to \prod_{i<n} S/\sim_i$ le morphisme d'ω_1-semigroupes défini par $\varphi(s) = (\varphi_1(s), \ldots, \varphi_{n-1}(s))$. Les congruences $\sim$ et $\sim_\varphi$ sont alors identiques, et en utilisant la proposition 3.5.11 $S/\sim_\varphi$ est isomorphe à $\varphi(S)$. ∇

Proposition 3.5.13 *Soient $\sim$ et $\sim'$ deux congruences sur un ω_1-semigroupe S telle que $s \sim' t$ implique $s \sim t$ pour tout $s, t \in S$. Alors $S/\sim$ est quotient de $S/\sim'$.*

Nous étendons maintenant la notion de résiduel au cas des ω_1-semigroupes :

Définition 3.5.14 *Soient S un ω_1-semigroupe et P une partie de S. Les* **résiduels** *de P sont définis de la façon suivante : si $s \in S$,*
- $s^{-1}P = \{t \in S : st \in P\}$
- $Ps^{-\omega} = \{t \in S : (ts)^\omega \in P\}$
- $Ps^{-1} = \{t \in S : ts \in P\}$.

Nous allons maintenant vérifier que si P est reconnu par un ω_1-semigroupe S et $s \in S$, les résiduels $s^{-1}P$, $Ps^{-\omega}$ et Ps^{-1} le sont également.

Proposition 3.5.15 *Soient S et T deux ω_1-semigroupes, $\varphi : S \to T$ un morphisme d'ω_1-semigroupes qui reconnait une partie X de S, et $s \in S$. Alors $s^{-1}X$, Xs^{-1} et $Xs^{-\omega}$ sont également reconnus par φ.*

Preuve Soit $P = \varphi(X)$. Montrons d'abord que $s^{-1}X$ est reconnu par φ.

$$\begin{aligned} s^{-1}X &= \{t \in S : st \in X\} \\ &= \{t \in S : \varphi(st) \in P\} \\ &= \{t \in S : \varphi(s)\varphi(t) \in P\} \\ &= \varphi^{-1}((\varphi(s))^{-1}P) \end{aligned}$$

La preuve pour Xs^{-1} est similaire. Finallement,

$$\begin{aligned} Xs^{-\omega} &= \{t \in S : (ts)^{\omega} \in X\} \\ &= \{t \in S : \varphi((ts)^{\omega}) \in P\} \\ &= \{t \in S : (\varphi(t)\varphi(s))^{\omega} \in P\} \\ &= \varphi^{-1}(P(\varphi(s))^{-\omega}) \end{aligned}$$

∇

Proposition 3.5.16 *Soient S, T et U trois ω_1-semigroupes, et $\varphi_S : U \to S$ (resp. $\varphi_T : U \to T$) un morphisme d'ω_1-semigroupes qui reconnait $L_S \subseteq U$ (resp. L_T). Alors $S \times T$ reconnaît $L_S \cup L_T$ et $L_S \cap L_T$.*

Preuve Soient $P_\cup = \{(s, s') \in S \times T : s \in \varphi_S(L_S)$ ou $s' \in \varphi_T(L_T)\}$, $P_\cap = \{(s, s') \in S \times T : s \in \varphi_S(L_S)$ et $s' \in \varphi_T(L_T)\}$ et $\varphi : U \to S \times T$ le morphisme d'ω_1-semigroupes definit par $\varphi((s, s')) = (\varphi_S(s), \varphi_T(s'))$. Alors $\varphi^{-1}(P_\cup) = L_S \cup L_T$ et $\varphi^{-1}(P_\cap) = L_S \cap L_T$. ∇

3.5.2 Equivalence entre ω_1-monoides finis et D-automates

Dans cette section nous (re)donnons des preuves pour les théorèmes suivants :

Théorème 3.5.17 *Soit A un alphabet fini. Une partie de $A^{<\omega_1}$ est D-rationnelle si et seulement si elle est reconnue par un ω_1-semigroupe fini.*

Dans la preuve nous donnons des algorithmes pour construire un ω_1-semigroupe fini à partir d'un D-automate, et un D-automate déterministe à partir d'un ω_1-semigroupe fini. Ce qui montre en particulier que

Théorème 3.5.18 (Büchi) *Soit A un alphabet fini et L une partie D-reconnaissable de $A^{<\omega_1}$. Il existe un D-automate déterministe complet $\mathcal{A}$ tel que $L = \mathcal{L}(\mathcal{A})$.*

Comme corollaire immédiat :

Corollaire 3.5.19 (Büchi) *Soit A un alphabet fini et L une partie D-reconnaissable de $A^{<\omega_1}$. Alors $A^{<\omega_1} - L$ est D-reconnaissable.*

Des D-automates vers les ω_1-algèbres de Wilke

Nous donnons ici un algorithme qui permet d'obtenir une ω_1-algèbre de Wilke à partir d'un D-automate $\mathcal{A} =< Q, A, E, I, F >$. Nous reprenons pour ceci les idées développées pour construire une ω^n-algèbre de Wilke à partir d'un n-automate, que nous adaptons au cas des mots de longueur dénombrable.

Si u est un mot de $A^{[1,\omega_1[}$, $c = (q_\alpha)_{\alpha\leq|u|}$ est un chemin de p vers q d'étiquette u dans $\mathcal{A}$, et $l = \cup_{\alpha\leq|u|} q_\alpha$ alors l'existence de c est dénotée par

$$c : p \xrightarrow[l]{u} q$$

Soit $K^{Q\times Q}$ l'ensemble des matrices carrées indexées par les éléments de Q et dont les coefficients sont dans $K = [Q]^2 \cup \{\emptyset\}$. Nous allons coder l'automate par des matrices de $K^{Q\times Q}$, et associer à chaque mot u de longueur positive dénombrable une matrice $\mu(u)$ de telle manière que $\mu : A^{[1,\omega_1[} \to K^{Q\times Q}$ soit un morphisme de ω_1-semigroupe et

$$\mu(u)_{p,q} = \{l \subseteq Q : \exists c : p \xrightarrow[l]{u} q\}$$

Naturellement, pour $a \in A$,

$$\mu(a)_{p,q} = \{\{p, q\}\} \text{ si et seulement si } (p, a, q) \in E$$

Si S est un semigroupe, $[S]$ peut naturellement être muni d'une structure de semi-anneau : la somme de deux éléments A et B de $[S]$ est $A \cup B$ et le produit $\{ab : a \in A, b \in B\}$. Finalement, l'ensemble des matrices finies de taille $n \times m$ dont les coefficients sont dans un semi-anneau est aussi un semi-anneau. En particulier, $K^{Q\times Q}$ est un semigroupe. De plus, $K^{Q\times Q}$ est un ensemble fini.

Nous équipons maintenant $K^{Q\times Q}$ d'une application interne ω de telle manière que $K^{Q\times Q}$ soit une ω_1-algèbre de Wilke.

Définition 3.5.20 *Soit $s \in K^{Q\times Q}$. Un s-**chemin** t de p vers q est une suite*

$$(t_0, l_0)(t_1, l_1)(t_2, l_2)\cdots$$

de type ω d'éléments de $Q\times[Q]$ telle que $p = t_0$, $l_j \in s_{t_j,t_{j+1}}$ pour tout entier j et finalement $(In(t), q) \in E$, où $In(t) = \{\ q\ :\ $ il existe une infinité d'entiers i tels que $q \in l_i\}$. Nous dénotons aussi t par

$$t_0 \xrightarrow[l_0]{} t_1 \xrightarrow[l_1]{} t_2 \xrightarrow[l_2]{} \cdots \xrightarrow[l_{i-1}]{} t_i \xrightarrow[l_i]{} t_{i+1} \xrightarrow[l_{i+1}]{} \cdots$$

On dit que $l \in (s^\omega)_{p,q}$ si et seulement si il existe un s-chemin $(t_0, l_0)(t_1, l_1)(t_2, l_2)\ldots$ de p vers q tel que $l = \{q\} \cup \cup_{i\in\mathbb{N}} l_i$.

Proposition 3.5.21 *Les propriétés de la définition 3.5.4 sont vérifiées par l'application ω ainsi définie.*

Preuve Montrons d'abord que $(st)^\omega = s(ts)^\omega$. Soit $l \in ((st)^\omega)_{p,q}$. Il existe un st-chemin c de p vers q

$$c_0 \xrightarrow[l_0]{} c_1 \xrightarrow[l_1]{} c_2 \xrightarrow[l_2]{} \cdots \xrightarrow[l_{i-1}]{} c_i \xrightarrow[l_i]{} c_{i+1} \xrightarrow[l_{i+1}]{} \cdots$$

tel que $l = \{q\} \cup \cup_{i\in\mathbb{N}} l_i$. D'après la définition de st-chemin on a aussi $(In(c), q) \in E$ et $l_j \in (st)_{c_j,c_{j+1}}$ pour tout entier j. D'après la définition de produit de matrices pour tout entier j il existe $k_j \in Q$ tel que $l_j = l_j^s \cup l_j^t$ avec $l_j^s \in s_{c_j,k_j}$ et $l_j^t \in t_{k_j,c_{j+1}}$.

$$\begin{tikzcd}
c_0 \arrow[r] & c_1 \arrow[r] & \cdots\cdots\cdots \arrow[r] & c_j \arrow[rr, "(st)_{c_j,c_{j+1}}", "l_j"'] \arrow[dr, "l_j^s", "s_{c_j,k_j}"'] & & c_{j+1} \arrow[r] & \cdots\cdots \\
& & & \cdots\cdots\cdots \arrow[r] & k_j \arrow[ur, "l_j^t"', "t_{k_j,c_{j+1}}"] \arrow[r] & \cdots\cdots &
\end{tikzcd}$$

La suite $k = (k_0, l_0^t \cup l_1^s)(k_1, l_1^t \cup l_2^s)(k_2, l_2^t \cup l_3^s)\ldots$ de type ω est un ts-chemin de k_0 vers q comme $l_j^t \cup l_{j+1}^s \in (ts)_{k_j,k_{j+1}}$ pour tout entier j et $In(k) = In(c)$. On a donc $\{q\} \cup \cup_{i\in\mathbb{N}}(l_i^t \cup l_{i+1}^s) \in ((ts)^\omega)_{k_0,q}$. Maintenant, comme $l_0^s \in s_{c_0,k_0}$, d'après la définition de produit de matrices il vient

$$l_0^s \cup \{q\} \cup \bigcup_{i\in\mathbb{N}}(l_i^t \cup l_{i+1}^s) = \{q\} \cup \bigcup_{i\in\mathbb{N}}(l_i^s \cup l_i^t) = \{q\} \cup \bigcup_{i\in\mathbb{N}} l_i = l \in (s(ts)^\omega)_{p,q}$$

La réciproque et la seconde propriété de la définition 3.5.4 peuvent être prouvées avec des arguments similaires. ∇

Proposition 3.5.22 *Soit u un mot de longueur positive dénombrable sur A. Alors $l \in \mu(u)_{p,q}$ si et seulement si il existe un chemin $c : p \xrightarrow[l]{u} q$.*

Preuve La preuve est par induction transfinie sur $|u|$. On montre d'abord l'inclusion de la gauche vers la droite. Si $|u| = 1$ comme $\mu(u)_{p,q} = \{\{p,q\}\}$ si et seulement si $(p,u,q) \in E$ alors $l = \{p,q\}$ et $c : p \xrightarrow[l]{u} q$. Supposons maintenant que $|u| \in \mathit{Succ}$. Alors $u = u'a$ avec $a \in A$. Comme $\mu(u'a)_{p,q} = (\mu(u')\mu(a))_{p,q}$ il existe $k \in Q$ tel que $l = l' \cup l''$, $l' \in \mu(u)_{p,k}$ et $l'' \in \mu(a)_{k,q}$. Par hypothèse de récurrence il existe $c' : p \xrightarrow[l']{u'} k$ et $c'' : k \xrightarrow[l'']{a} q$, donc $c : p \xrightarrow[l]{u} q$. Passons au cas où $|u| \in \mathit{Lim}$. D'après le théorème 3.3.7 u s'écrit $u = u_0u_1u_2\ldots$ de telle façon que $\mu(u_0) = s$ et $\mu(u_i) = e$ pour tout entier i positif. Comme $\mu(u) = se^\omega$, d'après la définition de produit de matrices il existe $k_0 \in Q$ tel que $l = l' \cup l''$, $l' \in s_{p,k_0}$ et $l'' \in (e^\omega)_{k_0,q}$. En utilisant l'hypothèse de récurrence il existe $c_0 : p \xrightarrow[l']{u_0} k_0$. Maintenant, comme $l'' \in (e^\omega)_{k_0,q}$ il existe un e-chemin $t : (t_1,l_1)(t_2,l_2)\ldots$ de k_0 vers q tel que $l'' = \{q\} \cup \cup_{i>0} l_i$. Comme $l_i \in \mu(u_i)_{t_i,t_{i+1}}$ pour tout entier positif par hypothèse de récurrence il existe un chemin $c_i : t_i \xrightarrow[l_i]{u_i} t_{i+1}$. En considérant la mise bout-à-bout de ces chemins $t_1 \xrightarrow[l_1]{u_1} t_2 \xrightarrow[l_2]{u_2} t_3 \ldots$, comme l'ensemble des états répétés cofinalement avec $|u_1u_2\ldots|$ est $In(t)$ et $(In(t), q) \in E$ on obtient un chemin $k_0 \xrightarrow[l'']{u_1u_2\ldots} q$, ce qui amène la conclusion.

Passons à l'inclusion de la droite vers la gauche. Si $|u| = 1$, comme $p \xrightarrow[l]{u} q$ on a $(p, u, q) \in E$ et $l = \{p, q\} \in \mu(u)_{p,q}$. Supposons maintenant que $|u| \in \mathit{Succ}$. Soit $u = u'a$. Comme $p \xrightarrow[l]{u'a} q$ il existe l', l'' et $k \in Q$ tels que $l = l' \cup l''$, $p \xrightarrow[l']{u'} k$ et $k \xrightarrow[l'']{a} q$. Par hypothèse de récurrence $l' \in \mu(u')_{p,k}$ et $l'' \in \mu(a)_{k,q}$, donc $l' \cup l'' = l \in (\mu(u')\mu(a))_{p,q} = \mu(u)_{p,q}$. Supposons finalement que $|u| \in \mathit{Lim}$, que $c : p \xrightarrow[l]{u} q$ et que $(q_\beta)_{\beta \leq |u|}$ est la suite d'états qui compose c. Soient (s, e) un couple lié et $(u_i)_{i \in \mathbb{N}}$ tels que $u = u_0u_1u_2\ldots$, $\mu(u_0) = s$ et $\mu(u_i) = e$ pour tout entier i positif. Soit $B = \{q \in l : \{\gamma < |u| : q_\gamma = q\}$ est cofinal avec $|u|\}$. On a $(B, q) \in E$. Soient $\gamma_i = \sum_{j<i} |u_j|$ et $l_i = \cup_{\gamma_i \leq \beta \leq \gamma_{i+1}} \{q_\beta\}$ pour tout entier i. La suite $k : (q_{\gamma_1}, l_1)(q_{\gamma_2}, l_2)(q_{\gamma_3}, l_3)\ldots$ de type ω vérifie $In(k) = B$ et $l_i \in e_{q_{\gamma_i}, q_{\gamma_{i+1}}}$ et donc est un e-chemin de q_{γ_1} vers q. Il suit que $\{q\} \cup \cup_{i>0} l_i \in (e^\omega)_{q_{\gamma_1}, q}$. Comme $p \xrightarrow[l_0]{u_0} q_{\gamma_1}$ par hypothèse de récurrence $l_0 \in s_{p, q_{\gamma_1}}$, donc $\{q\} \cup \cup_{i \in \mathbb{N}} l_i = l \in (se^\omega)_{p,q} = \mu(u)_{p,q}$. ∇

L'application $\mu' : A^{<\omega_1} \to (K^{Q \times Q})^1$ définie par $\mu'(u) = \mu(u)$ si $|u| > 0$ et $\mu'(\lambda) = 1$ est un morphisme de ω_1-semigroupe, et μ' reconnaît $\mathcal{L}(\mathcal{A})$. En effet, en posant

$$P = \{s \in K^{Q \times Q} \;:\; \exists i \in I,\; f \in F,\; s_{i,f} \neq \emptyset\} \cup P'$$

où $P' = \{1\}$ si et seulement si $\lambda \in \mathcal{L}(\mathcal{A})$, $P' = \emptyset$ sinon, on a $\mu'(u) \in P$ si et seulement si $u \in \mathcal{L}(\mathcal{A})$.

Des ω_1-monoides finis vers les D-automates

Soient A un alphabet, S un ω_1-monoïde fini, et $\varphi : A^{<\omega_1} \to S$ un morphisme d'ω_1-monoïdes qui reconnaît une partie P de $A^{<\omega_1}$.

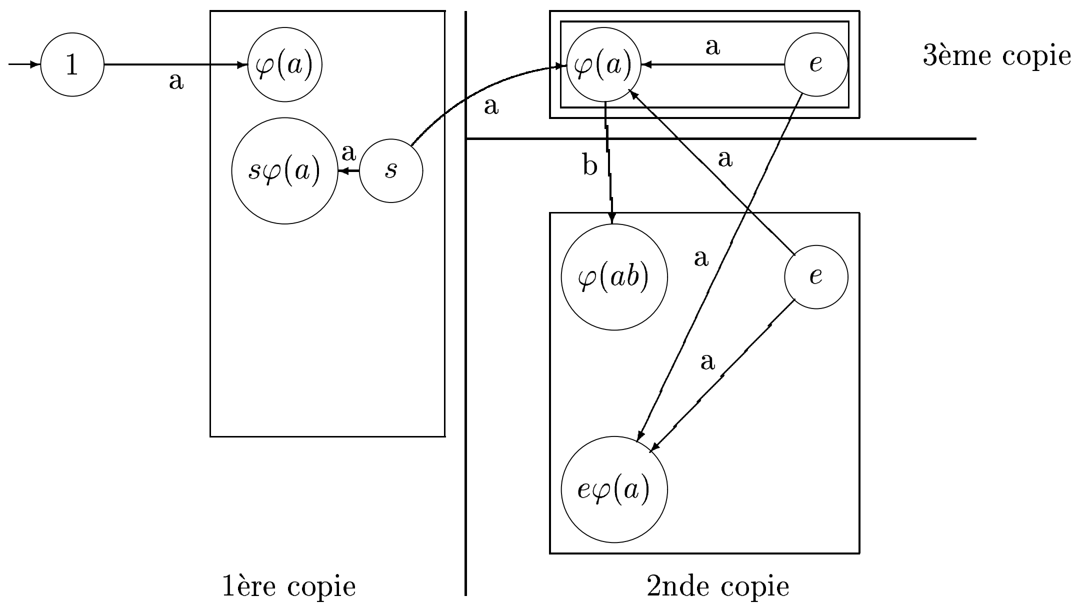
Nous allons construire un D-automate déterministe qui calcule l'image d'un mot u de $A^{<\omega_1}$ dans S.

La base de la construction est la suivante : on commence dans un premier temps par fabriquer un automate de Büchi non déterministe associé à un couple lié (s, e) de S, qui reconnaît un mot de longueur ω si et seulement si ce dernier a pour image se^ω dans S. Nous appellerons un tel automate **automate de $(\mathbf{s}, \mathbf{e})$**. Les idées sous-jascentes à cette construction sont dans [Lad77], même si les notions de semigroupes et ω-semigroupes en sont absentes.

Automate de $(\mathbf{s}, \mathbf{e})$ Soit (s, e) un couple lié de S. On commence par construire, à partir de S, l'automate (déterministe) de l'action à droite : les états de cet automate sont les éléments de S, et il existe une transition de p vers q par la lettre a si et seulement si $q = p \cdot \varphi(a)$. On construit un nouvel automate à partir de trois copies de cet automate en les reliant de la façon suivante (on appelle x_1 l'état x de la première copie, x_2 celui de la seconde, et x_f celui de la troisième) :

- pour toute lettre a et toute transition de s_1 vers t_1 par a on ajoute une transition de s_1 vers $\varphi(a)_f$ par a
- pour toute lettre a et toute transition de e_2 vers t_2 par a on ajoute une transition de s_2 vers $\varphi(a)_f$ par a
- on supprime toutes les transitions de la troisième copie
- pour tout état x_f et lettre a on ajoute une transition de x_f vers $(x_f\varphi(a))_2$ par a
- pour toute lettre a et transition de e_2 vers t_2 par a on ajoute une transition de e_f vers $\varphi(a)_f$ par a
- les états finaux de l'automate ainsi construit sont ceux de la troisième copie
- si S possède un élément neutre 1 alors l'unique état initial de l'automate ainsi construit est 1_1, sinon on ajoute un nouvel élément 1 à la première copie, des transitions de 1_1 vers $\varphi(a)_1$ pour chaque lettre a et on dit que 1 est l'état initial de l'automate ainsi obtenu.

On a le schéma suivant :



La condition d'acceptation d'un mot par l'automate est une condition de Büchi, aisément transformable en condition de Muller. Il est clair qu'un mot $u \in A^\omega$ est reconnu par cet automate si et seulement si $\varphi(u) = se^\omega$.

Dans la suite, si q est un état de la première copie, on note $q\varphi(a)$ l'unique état de la première copie de nom $q\varphi(a)$, et si q est de la seconde ou de la troisième copie, $q\varphi(a)$ désigne l'unique état de la seconde copie de nom $q\varphi(a)$. Par abus de notations nous omettrons les indices quand ils ne sont pas nécessaires.

La construction Soit (s, e) un couple lié de S. On commence par construire un automate déterministe $\mathcal{A}_{(s,e)}$ qui indique, pour un mot de longueur ω, si ce dernier a pour image se^ω dans S. Pour celà on utilise les automates que nous venons de décrire, auquels on ajoute les idées de [McN66] pour le passage à la limite. Nous conservons d'ailleurs des éléments de terminologie de [McN66].

Soit n le nombre d'états dans l'automate de (s, e), plus 1. Soit F l'ensemble des états de la troisième copie de cet automate. On utilise n copies de cet automate. A chaque copie i on associe des **propriétés**, constituées :

- d'une mémoire finie Aff^i qui mémorise des numéros de machines (i.e. de copie d'automates),
- d'une lampe verte V^i,
- d'une lampe rouge R^i.

On note Aff^i_t l'état de la mémoire Aff^i au temps α, V^i_α (resp. R^i_α) si i allume sa lampe verte (resp. rouge) au temps α. Les deux lampes sont des booléens. Par défaut, une lampe ne reste allumée qu'un temps. Les copies de machines sont gérées par une machine de contrôle, qui dispose également d'une mémoire finie Anc. Une copie est soit **active** (sensible à l'entrée), soit **inactive** (insensible). Au départ de la lecture du mot, toutes les copies sont inactives, sauf une. Quand à la lecture du mot on rencontre des transitions non déterministes (i.e. il existe plusieurs transitions partant de l'état courant par une même lettre) la machine active suit un chemin et provoque éventuellement l'activation de machines inactives pour suivre les autres chemins. Cette opération s'appelle la **division**. Quand deux machines arrivent par une transition dans le même état, une devient inutile : on réalise alors une **fusion** entre les deux machines. Lors d'une division ou d'une fusion on modifie les propriétés des machines concernées. Nous expliquons maintenant plus formellement comment se passent les transitions pour l'ensemble des n machines entre le temps α et le temps $\alpha + 1$, par lecture de la lettre a. Si i est un numéro de machine, on note q^i_α l'état dans lequel se trouve l'automate i au temps α et $\delta(q^i_\alpha, a)$ l'ensemble des états atteignables à partir de q^i_α en lisant la lettre a. Les états dans lesquels se trouvent les machines sont modifiées du temps α au temps $\alpha + 1$ par lecture de la lettre a de telle façon que :

1. Il n'existe pas deux machines i et j actives au temps $\alpha + 1$ telles que $q^j_{\alpha+1} = q^i_{\alpha+1}$
2. Si i est active au temps α alors pour tout $q \in \delta(q^i_\alpha, a)$ il existe j telle que $q^j_{\alpha+1} = q$
3. Si i est active au temps $\alpha+1$ alors il existe j active au temps α telle que $q^i_{\alpha+1} \in \delta(q^j_\alpha, a)$
4. Si i reste active au temps $\alpha + 1$ alors $q^i_{\alpha+1} \in \delta(q^i_\alpha, a) - F$ si i n'allume pas sa lampe rouge au temps $\alpha + 1$
5. Si i allume sa lampe rouge au temps $\alpha+1$, alors au temps $\alpha+1$ i devient soit inactive, soit $q^i_{\alpha+1} = \varphi(a)_f$
6. Soit i une machine active à α. i allume sa lampe rouge et perd ses mémoires à $\alpha+1$ si et seulement si il existe une machine k telle que $q^k_{\alpha+1} = q^i_\alpha \varphi(a)$ et k est plus ancienne que i
7. j active à $\alpha + 1$ allume sa lampe verte à $\alpha + 1$ si et seulement si il existe i active à α telle que $q^j_{\alpha+1} \in \delta(q^i_\alpha, u_\alpha) - F$ et $j \in Aff^i_\alpha$
8. Si j est active à $\alpha + 1$ alors

$$Aff^j_{\alpha+1} = \left(\bigcup_{i \in T} Aff^i_\alpha \cup \{i\} \right) - \left(\{i : R^i_{\alpha+1} \text{ ou } V^i_{\alpha+1}\} \cup \{j\} \right)$$

où $T = \{i$ actives à α telles que $q^j_{\alpha+1} \in \delta(q^i_\alpha, a)\}$

9. Si i est active au temps α, j à $\alpha + 1$, et $q^j_{\alpha+1} \in \delta(q^i_\alpha, a) - F$ alors j est plus ancienne que i.

On dit que la machine i **démarre** j au temps α si i est active au temps α, j au temps $\alpha + 1$, $q^j_{\alpha+1} = \varphi(a)_f$ et $q^j_{\alpha+1} \in \delta(q^i_\alpha, a)$.

La mémoire Anc est modifiée à chaque activation ou désactivation d'une machine de sorte qu'elle permette d'établir si une machine i a été activée avant une autre machine j ou pas. Ceci établit un ordre partiel sur les machines, qu'on rend total en disant que si i et j sont deux machines qui deviennent actives en même temps alors i est plus ancienne que j si la plus vieille machine qui provoque l'activation de i est plus ancienne que la plus vieille machine qui provoque l'activation de j. On dit qu'une machine i provoque l'activation d'une machine j au temps α si j allume sa lampe rouge au temps α ou j est inactive au temps α, j est active au temps $\alpha + 1$, $q^j_{\alpha+1} = \varphi(a)_f$ et $q^i_\alpha \in \{s_1, e_2, e_f\}$.

On construit $\mathcal{A}_{(s,e)}$ pour chacun des p couples liés (s, e) de S, et on les fait fonctionner en parallèle. L'ensemble des états finaux de l'automate de (s, e) est noté $F_{(s,e)}$, ou plus simplement F quand le couple (s, e) pourra clairement être déterminé en fonction du contexte. On prouvera plus tard qu'on obtient ainsi un automate déterministe qui donne l'image d'un mot de longueur ω dans S. On ajoute maintenant des liens entre les machines de $\mathcal{A}_{(s,e)}$ et $\mathcal{A}_{(s',e')}$ pour (s, e) et (s', e') deux couples liés de S, de façon à ce que quand une machine i est dans un état final $\varphi(a)_f$, alors pour tous les couples liés (s, e) de S une machine j de $\mathcal{A}_{(s,e)}$ soit dans l'état $\varphi(a)$ dans la première copie. La machine j doit pouvoir mémoriser qu'elle est en train de calculer l'image par φ du même facteur du mot que i dans une mémoire qui lui est associée, Ass^j, qui est modifiée au fur et à mesure de la lecture du mot de façon à ce que si 6 se produit pour i à l'instant α alors au même instant i est remplacé par k dans Ass^j, où k est la machine définie dans 6, et que si 6 se produit pour j, alors Ass^k est modifiée de façon à mémoriser qu'elle suit le même facteur du mot que i.

Soient maintenant $e = \{e_1, \ldots, e_k\}$ un état limite de l'automate, et α l'instant où cet état est atteint. Supposons qu'il existe une machine j qui fonctionne cofinalement à α (c'est-à-dire, qui est active et n'allume pas sa lampe rouge cofinalement à α). Soit (s, e) le couple lié associé à cette machine. Supposons qu'il existe une machine k de $\mathcal{A}_{(s',e')}$ telle que $j \in Ass^k$, k fonctionne cofinalement à α et il existe x une machine de $\mathcal{A}_{(s',e')}$ telle que $k \in Aff^x$, x fonctionne et allume sa lampe verte cofinalement à α. Alors on définit les transitions sortantes de e de telle façon qu'on considère qu'à l'instant α la machine j est dans l'état $s'e'^\omega$ de la première copie si les états que x répète cofinalement à α sont de la première copie, de la seconde sinon, $x \in Ass^j_\alpha$ si et seulement si x apparait dans Ass^j cofinalement à α et x est considérée comme active à α, et que $x \in Aff^j_\alpha$ si et seulement si x apparait cofinalement souvent à α dans Aff^j, x est considérée active à α et x n'allume pas sa lampe verte cofinalement à α. Les machines qui ne vérifient pas une telle propriété sont considérées inactives au temps α et allument leur lampe rouge à $\alpha + 1$. L'état e est final si et seulement si les machines qui sont actives dès la lecture de la première lettre sont dans un état qui est dans $\varphi(P)$.

On montre maintenant que l'automate ainsi défini reconnaît exactement les mêmes mots que φ. Nous commençons par définir la notion de continuité, qui nous sera utile par la suite.

Définition 3.5.23 *Soit m une machine activée à l'instant α (on note (m,α), ou bien, par abus de notation, m), et m' une machine active à l'instant $\alpha' > \alpha$. On dit que m'* **continue** *(m,α), et on note $m' = c_{\alpha'}((m,\alpha))$, s'il existe une suite finie de machines $(m_j)_{0<j\leq n}$ telle que*

- *$m_1 = m$*
- *$m_n = m'$*
- *Si $n > 1$*
  - *pour chaque $0 < i < n$ il existe un instant α_i où $q^{m_{i+1}}_{\alpha_i+1} = q^{m_i}_{\alpha_i}\varphi(a)$ et m_{i+1} est plus ancienne que m_i*
  - *m_1 n'allume pas sa lampe rouge dans l'intervalle de temps $]\alpha,\alpha_1]$*
  - *pour chaque $0 < i < n-1$ la machine m_{i+1} n'allume pas sa lampe rouge dans l'intervalle de temps $]\alpha_i,\alpha_{i+1}]$*
  - *m_n n'allume pas sa lampe rouge dans l'intervalle de temps $]\alpha_{n-1},\alpha']$*
- *Si $n = 1$, m n'allume pas sa lampe rouge dans l'intervalle de temps $]\alpha+1,\alpha']$ si $\alpha' > \alpha$*

Lemme 3.5.24 *Soit m une machine activée au temps α et $\alpha' > \alpha$. Il existe m' telle que $m' = c_{\alpha'}((m,\alpha))$.*

Preuve Par induction transfinie sur $\alpha' - \alpha$. Pour $\alpha' = \alpha + 1$ on prend $n = 1$ et on a bien $m = c_{\alpha+1}((m,\alpha))$. Supposons maintenant que l'énoncé soit vrai pour $\alpha' - \alpha$, on montre qu'il reste vrai pour $\alpha' + 1 - \alpha$ par lecture d'une lettre a du mot. Soit $m' = c_{\alpha'-\alpha}(m)$. A l'instant $\alpha' + 1 - \alpha$ deux alternatives se présentent : ou bien m' allume sa lampe rouge, ou bien non. Supposons d'abord que non ; celà signifie que $q^{m'}_{\alpha'+1-\alpha} = q^{m'}_{\alpha'-\alpha}\varphi(a)$ et donc $m' = c_{\alpha'+1-\alpha}(m)$. Supposons maintenant que oui. Soit $(m_i)_{0<i\leq n}$ la suite définie dans l'énoncé de la définition 3.5.23. On pose $m = m_1$ et $m' = m_n$. Si m_n allume sa lampe rouge au temps $\alpha' + 1 - \alpha$, alors il existe une machine m_{n+1} plus vieille que m_n qui vérifie $q^{m_{n+1}}_{\alpha'+1-\alpha} = q^{m_n}_{\alpha'-\alpha}\varphi(a)$. D'autre part, m_{n+1} n'allume pas sa lampe rouge dans l'intervalle $]\alpha'-\alpha,\alpha'+1-\alpha]$, donc $m_{n+1} = c_{\alpha'+1-\alpha}(m)$.

On suppose maintenant que l'énoncé est vrai pour tout $\alpha'' - \alpha < \alpha' - \alpha \in \mathit{Lim}$, et on le montre pour $\alpha' - \alpha$. On montre que n ne peut pas être plus grand que le nombre x de machines. Celà signifie qu'à partir d'un certain $\alpha < \alpha'' < \alpha'$ il existe une machine (m',α'''') démarée à α'''' telle que pour tout $\alpha' > \alpha''' > \alpha''$ on ait $(m',\alpha'''') = c_{\alpha'''}(m)$, ce qui prouve le résultat. Supposons qu'il y ait $x+1$ machines dans la suite. Alors il en existe une qui a été utilisée deux fois. On note $(m'',\alpha_{m''_1})$ la première apparition de cette machine dans la suite, où $\alpha_{m''_1}$ est l'instant où elle a été démarrée, et $(m'',\alpha_{m''_2})$ la seconde apparition, où $\alpha_{m''_2}$ est l'instant où elle a été démarrée. Comme la relation d'ancienneté est stricte, on a que $\alpha_{m''_2} < \alpha_{m''_1}$, ce qui est impossible. ∇

Remarque 3.5.25 *Si on note $m_{(s,e)}$ l'unique machine de $\mathcal{A}_{(s,e)}$ active dès la première* *lettre du mot, alors à chaque instant α $m_{(s,e)} = c_\alpha(m_{(s,e)})$ puisqu'il n'existe pas de machine plus ancienne que $m_{(s,e)}$.*

Nous utiliserons ce lemme implicitement dans la suite :

Lemme 3.5.26 *Soit m une machine active au temps α, et $\alpha' \geq \alpha$. On pose $m' = c_{\alpha'}(m)$. Alors $q_{\alpha'}^{m'}$ est un état de la première copie si et seulement si q_α^m est un état de la première copie. De même, si $\alpha' > \alpha$, $q_{\alpha'}^{m'}$ est un état de la seconde copie si et seulement si q_α^m est un état de la seconde ou de la troisième copie.*

Preuve Nous prouvons d'abord la partie de l'énoncé qui traite de la première copie, par induction transfinie sur $\alpha' - \alpha$. Si $\alpha' = \alpha$ le résultat est immédiat. Supposons le lemme vrai pour $\alpha' - \alpha$, on le montre pour $\alpha' + 1 - \alpha$. Soient $m' = c_{\alpha'-\alpha}(m)$ et $m'' = c_{\alpha'+1-\alpha}(m')$. Comme $q_{\alpha'+1-\alpha}^{m''} \in \delta(q_{\alpha'-\alpha}^{m'}, u_{\alpha'}) - F$, $q_{\alpha'-\alpha}^{m'}$ est de la première copie si et seulement si $q_{\alpha'+1-\alpha}^{m''}$ l'est aussi et on a le résultat par hypothèse de récurrence. Passons au cas limite. Soit $m' = c_{\alpha'-\alpha}(m)$. Si q_α^m est un état de la première copie par hypothèse de récurrence les états de m' répétés cofinalement à $\alpha' - \alpha$ le sont aussi, et par définition de l'automate $q_{\alpha'-\alpha}^{m'}$ l'est aussi. Réciproquement, si $q_{\alpha'-\alpha}^{m'}$ est un état de la première copie, les états répétés cofinalement à $\alpha' - \alpha$ par m' le sont aussi, et par hypothèse de récurrence q_α^m également.

La preuve de la partie de l'énoncé du lemme qui concerne les seconde et troisième copies se fait de façon similaire. ∇

Lemme 3.5.27 *Soit m_1 une machine activée au temps α_1, $\alpha' > \alpha_1$, m_1' telle que $m_1' = c_{\alpha'}(m_1)$. Soit m_2 une machine activée au temps $\alpha_2 \leq \alpha_1$ et active au temps $\alpha_1 + 1$ telle que $m_1 \in Ass_{\alpha_1+1}^{m_2}$, et m_2' telle que $m_2' = c_{\alpha'}(m_2)$. Alors $m_1' \in Ass_{\alpha'}^{m_2'}$. Réciproquement, si $m_1' \in Ass_{\alpha'}^{m_2'}$, alors il existe m_1 une machine activée au temps α_1, $\alpha' > \alpha_1$ telle que $m_1' = c_{\alpha'}(m_1)$ et m_2 une machine activée au temps $\alpha_2 \leq \alpha_1$ et active au temps $\alpha_1 + 1$ telle que $m_1 \in Ass_{\alpha_1+1}^{m_2}$, et telle que $m_2' = c_{\alpha'}(m_2)$.*

Preuve D'abord le sens de la gauche vers la droite. Le cas de base $\alpha' = \alpha_1 + 1$ est trivial comme $q_{\alpha_1+1}^{m_1} = \varphi(u_{\alpha_1})_f$, $m_1 = c_{\alpha_1+1}(m_1)$, $m_2 = c_{\alpha_1+1}(m_2)$ et $m_1 \in Ass_{\alpha_1+1}^{m_2}$. Supposons l'implication vraie à α', on montre qu'elle est vraie à $\alpha' + 1$. Au temps $\alpha' + 1$ on peut se trouver dans quatre situations.

- si ni m_1' ni m_2' n'allument leur lampe rouge à l'instant $\alpha' + 1$ alors $q_{\alpha'+1}^{m_1'} = q_{\alpha'}^{m_1'}\varphi(u_{\alpha'})$ et $q_{\alpha'+1}^{m_2'} = q_{\alpha'}^{m_2'}\varphi(u_{\alpha'})$, et par définition de Ass on a $m_1' \in Ass_{\alpha'+1}^{m_2'}$.
- Si m_1' allume sa lampe rouge au temps $\alpha' + 1$ mais pas m_2', alors il existe m_3 telle que m_3 est plus ancienne que m_1' et $q_{\alpha'+1}^{m_3} = q_{\alpha'}^{m_1'}\varphi(u_{\alpha'})$. La machine m_1' est donc remplacée par m_3 dans $Ass_{\alpha'+1}^{m_2'}$. D'autre part, on a bien $m_3 = c_{\alpha'+1}(m_1)$.
- Si m_2' allume sa lampe rouge au temps $\alpha' + 1$ mais pas m_1' on utilise des arguments similaires.
- Si m_1' et m_2' allument leur lampes rouges respectives au temps $\alpha' + 1$ on utilise également des arguments similaires.

Maintenant, on suppose que $\alpha' - \alpha \in \mathit{Lim}$. En reprenant les arguments de la preuve du lemme 3.5.24 pour le cas limite, il existe un temps $\alpha' > \alpha'' > \alpha$ et deux machines m_1' et m_2' telles que $m_1' = c_{\alpha''}(m_1)$, $m_2' = c_{\alpha''}(m_2)$ et que ni m_1' ni m_2' n'allument leur lampe rouge dans l'intervalle de temps $]\alpha'', \alpha'[$. Par hypothèse de récurrence $m_1' \in Ass_{\alpha'''}^{m_2'}$ pour tout $\alpha' > \alpha''' > \alpha''$ et donc par définition de Ass on a $m_1' \in Ass_{\alpha'}^{m_2'}$.

Le sens de la droite vers la gauche utilise des arguments similaires. ∇

Lemme 3.5.28 *Soit m et m' deux machines de $\mathcal{A}_{(s,e)}$ actives respectivement aux temps α et α'. $m \in Aff_{\alpha'}^{m'}$ si et seulement si il existe un entier $n > 1$, une suite $(m_i)_{0<i\leq n}$ de machines et une suite strictement croissante $(\alpha_i)_{0<i<n}$ de temps telles que*

- $m = m_1$
- $m' = c_{\alpha'}(m_n)$
- *m n'allume pas de lampe dans l'intervalle de temps $]\alpha, \alpha']$*
- *pour tout $i \in [1 \ldots n-1]$*
  - *si $m'' = c_{\alpha_i}(m_i)$ alors $q_{\alpha_i}^{m''} \in \{s_1, e_2, e_f\}$*
  - $q_{\alpha_i+1}^{m_{i+1}} = \varphi(u_{\alpha_i})_f$

Preuve Nous commençons par le sens de la gauche vers la droite en procédant par induction transfinie sur $\alpha' - \alpha$. D'abord le cas de base $\alpha' = \alpha + 1$. Si $m \in Aff_{\alpha'}^{m'}$ alors m n'allume pas ses lampes à α', $m \neq m'$ et $q_{\alpha'}^{m'} \in \delta(q_{\alpha}^{m}, u_{\alpha})$. Comme m n'allume pas sa lampe rouge à α' alors $q_{\alpha}^{m} \in \{s_1, e_2, e_f\}$ et $q_{\alpha'}^{m} \in \delta(q_{\alpha}^{m}, u_{\alpha}) - F$ et donc $q_{\alpha'}^{m'} = \varphi(u_{\alpha})_f$.

Supposons maintenant le résultat vrai à α', on le montre pour $\alpha' + 1$. Si $m \in Aff_{\alpha'+1}^{m'}$ alors

- il existe une machine k active à α' telle que $q_{\alpha'+1}^{m'} \in \delta(q_{\alpha'}^{k}, u_{\alpha'})$ et m est k ou $m \in Aff_{\alpha'}^{k}$
- m n'allume pas de lampe à $\alpha' + 1$
- m' n'est pas m

Par hypothèse de récurrence,

- m n'allume pas de lampe dans $]\alpha, \alpha']$ donc m n'allume pas de lampe dans $]\alpha, \alpha' + 1]$
- si m est k alors on se retrouve dans une situation similaire au cas de base
- si $m \in Aff_{\alpha'}^{k}$ alors trois cas se présentent :
  - si $m' = k$ on a le résultat directement
  - si $m' \neq k$ et $q_{\alpha'+1}^{m'} = q_{\alpha'}^{k}\varphi(u_{\alpha'})$ alors $m' = c_{\alpha'+1}(k)$ et on a le résultat
  - si $m' \neq k$ et $q_{\alpha'+1}^{m'} = \varphi(u_{\alpha'})$ alors $q_{\alpha'}^{k} \in \{s_1, e_2, e_f\}$ et on a le résultat en ajoutant un élément à la suite des machines et un à la suite des temps.

Maintenant on examine le cas où $\alpha' - \alpha \in \mathit{Lim}$. Puisque $m \in Aff_{\alpha'}^{m'}$, m' et m sont actives à $\alpha' - \alpha$, m n'allume pas une de ses lampes cofinalement à $\alpha' - \alpha$ et m apparait cofinalement à $\alpha' - \alpha$ dans $Aff^{m'}$. Il existe donc un moment α'' à partir duquel m n'allume plus de lampe, m' n'allume plus sa lampe rouge et pour tout α''' tel que $\alpha' - \alpha > \alpha''' > \alpha''$ alors $m \in Aff_{\alpha'''}^{m'}$. Par hypothèse de récurrence on a la résultat à α'', et il suit à $\alpha' - \alpha$.

Finalement, la preuve de l'inclusion de la droite vers la gauche se fait simplement en utilisant les règles qui régissent $\mathcal{A}_{(s,e)}$. ∇

La proposition suivante nous permettra d'obtenir le résultat principal.

Proposition 3.5.29 *Soit m une machine de $\mathcal{A}_{(s,e)}$ démarrée à l'instant α, ou active dès la première lettre du mot ($\alpha = 0$). A chaque instant $\alpha' > \alpha$, il existe une machine m' de $\mathcal{A}_{(s,e)}$ telle que $m' = c_{\alpha'}(m)$ et $q_{\alpha'}^{m'} = \varphi(u[\alpha, \alpha'[)$.*

Preuve L'existence de m' est prouvée par le lemme 3.5.24. Il reste à prouver que $q_{\alpha'}^{m'} = \varphi(u[\alpha, \alpha'[)$, par induction transfinie sur $\alpha' - \alpha$. Comme $q_{\alpha+1}^{m} = \varphi(u_\alpha)_f$ le cas de base de la récurrence est vérifié. On vérifie également très facilement que si l'énoncé est vrai pour $\alpha' - \alpha$ il l'est aussi pour $\alpha' + 1 - \alpha$.

On suppose maintenant que l'énoncé est vrai pour tout $\alpha'' - \alpha < \alpha' - \alpha \in Lim$, et on le montre pour $\alpha' - \alpha$. Si $\alpha' - \alpha \in Lim$, alors $\alpha' \in Lim$. Par construction, à l'instant $\alpha + 1$, pour chaque couple lié (s', e') de S une machine $m_{(s',e')}$ est dans l'état $\varphi(u_\alpha)$ pour la première copie au temps $\alpha + 1$, de façon à ce que $m \in Ass_{\alpha+1}^{m_{(s',e')}}$.

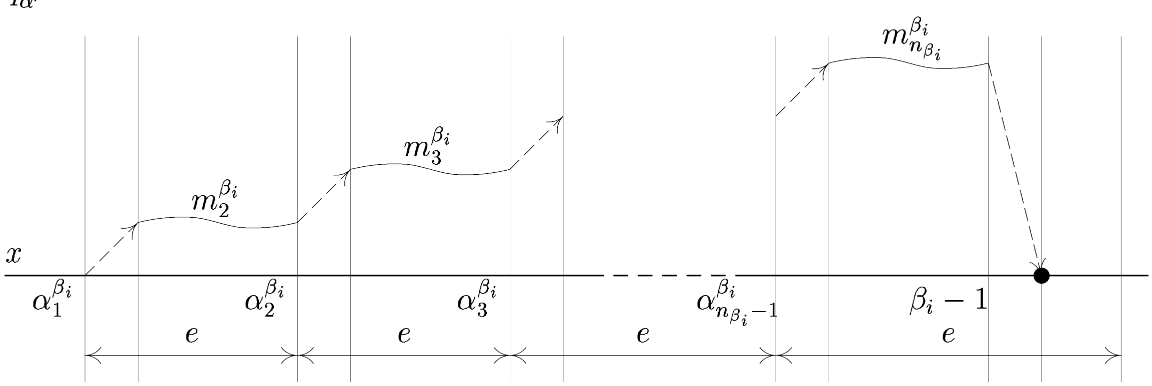
Lemme 3.5.30 *A l'instant α', il existe un couple lié (s', e') et une machine $x \in \mathcal{A}_{(s',e')}$ telle que*

- *x est active cofinalement à α', et n'allume pas sa lampe rouge cofinalement à α'*
- *x allume sa lampe verte cofinalement à α'*
- *il existe $y \in \mathcal{A}_{(s',e')}$ qui est active cofinalement à α' sans allumer sa lampe rouge cofinalement à α', et telle que $y = c_{\alpha'}(m_{(s',e')})$, si $m' = c_{\alpha'}(m)$ alors $m' \in Ass_{\alpha'}^{y}$ et $y \in Aff_{\alpha'}^{x}$ de telle façon que si $(\alpha_i)_{0<i<n}$ est la suite de temps définie au lemme 3.5.28 alors il existe α'' tel que $\alpha'' \leq \alpha_1$ et $y = c_{\alpha''}(m_{(s',e')})$.*

Preuve Le lemme 3.5.24 montre que y existe. D'après le lemme 3.5.27 on a $m' \in Ass_{\alpha'}^{y}$ On montre maintenant l'existence de x. Le facteur $u[\alpha, \alpha'[$ admet un découpage ultimement monocolore $s'e'^{\omega}$. Soit $(\alpha_i)_{i\in\mathbb{N}}$ une suite de temps cofinale à α' telle que $\alpha_0 = \alpha$, $\varphi(u[\alpha_0, \alpha_1[) = s'$ et $\varphi(u[\alpha_i, \alpha_{i+1}[) = e'$ pour tout $i > 0$. Comme (s', e') est un couple lié on peut supposer que $\alpha_{i+1} - \alpha_i > 1$ et que $y = c_{\alpha_1}(m_{(s',e')})$. Par hypothèse de récurrence à chaque α_i pour $i > 0$ on a $q_{\alpha_i}^{y} = s'$ et donc à chaque α_i+1 il existe une machine m_{α_i} démarrée par y. On a $y \in Aff_{\alpha_i+1}^{m_{\alpha_i}}$. Soit $k = c_{\alpha'}(m_{\alpha_1})$. A partir d'un certain moment, k n'allume plus sa lampe rouge, cofinalement à α'. Soit j le plus petit entier qui vérifie : il n'existe pas $\alpha' > \alpha'' > \alpha_j$ tel que k allume sa lampe rouge à α''. Pour chacun des α_i pour $i > j$, puisque $\varphi(u[\alpha_i, \alpha_{i+1}[) = e'$, k démarre une machine k_{α_i}. Soit $k'_{\alpha_i} = c_{\alpha'_{i+1}}(k_{\alpha_i})$, où α'_{i+1} est le plus vieux temps plus petit que α_{i+1} tel que $k'_{\alpha_i} \neq k$. Comme $\varphi(u[\alpha_i, \alpha_{i+1}[) = e' = \varphi(u[\alpha_1, \alpha_{i+1}[)$, et k est plus ancienne que k'_{α_i}, les deux machines vont fusionner de telle sorte que k'_{α_i} allume sa lampe rouge au plus tard au temps $\alpha'_{i+1} + 1 \leq \alpha_{i+1} + 1$. Si k n'a pas allumé sa lampe verte dans l'intervalle de temps $]\alpha_i, \alpha'_{i+1}]$ alors en utilisant le lemme 3.5.28 il vient que $k \in Aff_{\alpha'_{i+1}}^{k'_{\alpha_i}}$ et donc k allume sa lampe verte au temps $\alpha'_{i+1} + 1$. En répétant infiniment ce raisonnement on trouve que k allume sa lampe verte cofinalement à α'. Finalement, en posant $x = k$ et en utilisant le lemme 3.5.28 on a bien $y \in Aff_{\alpha'}^{x}$ car y ne peut pas allumer sa lampe verte dans l'intervalle de temps $[\alpha + 1, \alpha'[$. En effet, comme $q_{\alpha+1}^{m(s',e')} = \varphi(u_\alpha)_1$ et $y = c_{\alpha'}(m_{(s',e')})$, si α_y désigne l'instant où y a été activée tel que y n'allume pas sa lampe rouge au temps α'' pour tout $\alpha' > \alpha'' > \alpha_y$, alors $q_{\alpha''}^{y}$ est un état de la première copie. Or, pour que y allume sa lampe verte au temps $\alpha'' + 1$, il faut qu'il existe une machine m''

active à α'' telle que $q^y_{\alpha''+1} \in \delta(q^{m''}_{\alpha''}, u_{\alpha''}) - F$ et $y \in Aff^{m''}_{\alpha''}$. Il est aisé de montrer que ceci signifie que $\delta(q^{m''}_{\alpha''}, u_{\alpha''}) - F$ est un état de la seconde ou de la troisième copie, or $q^y_{\alpha''+1}$ est un état de la première copie, donc il est impossible que $q^y_{\alpha''+1} \in \delta(q^{m''}_{\alpha''}, u_{\alpha''}) - F$ et donc que y allume sa lampe verte au temps $\alpha''+1$. ∇

Nous montrons maintenant que $\varphi(u[\alpha, \alpha'[) = s'e'^{\omega}$. Comme $y \in Aff^x_{\alpha'}$ en utilisant le lemme 3.5.28 il existe en entier n et deux suites $(m_i)_{0<i\leq n}$ et $(\alpha_i)_{0<i<n}$ qui vérifient l'énoncé du lemme. Comme $y = c_{\alpha'}(m_{(s',e')})$, en utilisant le lemme 3.5.26 il vient que pour tout α'' dans l'intervalle $]\alpha, \alpha']$ on a que $q^y_{\alpha''}$ est un état de la première copie. Par conséquent, $q^y_{\alpha_1} = s_1$. Comme $q^{m_{(s',e')}}_{\alpha+1} = \varphi(u_\alpha)_1$ et $y = c_{\alpha_1}(m_{(s',e')})$ par hypothèse de récurrence on a $\varphi(u[\alpha, \alpha_1[) = s'$. On montre en utilisant des arguments similaires que $\varphi(u[\alpha_i, \alpha_{i+1}[) = e'$ pour $1 \leq i < n-1$ et donc $\varphi(u[\alpha, \alpha_{n-1}[) = s'$. On a $x = c_{\alpha'}(m_n)$, or les états pris par m_n sont de la seconde ou troisième copie. Soit $(\beta_i)_{i<\omega}$ une sous-suite de la suite croissante des temps cofinale à α' où x allume sa lampe verte. D'après la définition de l'automate pour chaque β_i il existe une machine m_{β_i} active à $\beta_i - 1$ telle que $q^x_{\beta_i} = q^{m_{\beta_i}}_{\beta_i-1}$ et $x \in Aff^{m_{\beta_i}}_{\beta_i-1}$. En utilisant toujours le lemme 3.5.28 on prouve qu'il existe des suites $(m^{\beta_i}_j)_{0<j\leq n_{\beta_i}}$ et $(\alpha^{\beta_i}_j)_{0<j<n_{\beta_i}}$ de machines et de temps telles que $m_{\beta_i} = c_{\beta_i-1}(m^{\beta_i}_{n_{\beta_i}})$, $x = m^{\beta_i}_1$, et $q^x_{\alpha^{\beta_i}_1} \in \{e'_2, e'_f\}$. Comme $x = c_{\alpha^{\beta_1}_1}(m_n)$ en utilisant l'hypothèse de récurrence on a $\varphi(u[\alpha_{n-1}, \alpha^{\beta_1}_1[) = e'$. En utilisant des arguments similaires on montre que $\varphi(u[\alpha^{\beta_i}_{n_{\beta_i}-1}, \alpha^{\beta_{i+1}}_1[) = e$ et que $\varphi(u[\alpha^{\beta_i}_1, \alpha^{\beta_i}_{n_{\beta_i}-1}[) = e$ pour chaque i d'où il sort que $\varphi(u[\alpha, \alpha'[) = s'e'^{\omega}$. Par la définition de l'automate, on a bien $q^{m'}_{\alpha'} = s'e'^{\omega}$.



x allume sa lampe verte au temps β_i

∇

En particulier, comme il existe une machine $m_{(s,e)}$ active dès la première lettre du mot pour chaque couple lié (s, e), cette machine n'allume jamais de lampe rouge (puisqu'il n'en existe pas de plus ancienne) et $q^{m_{(s,e)}}_{\alpha} = \varphi(u[0, \alpha[)$ à chaque instant α.

3.5.3 ω_1-semigroupe syntaxique

Soient A un alphabet et X une partie reconnaissable de $A^{<\omega_1}$. Nous montrons maintenant que parmi tous les ω_1-semigroupes finis qui reconnaissent X il en existe un unique qui divise tous les autres, et qui par conséquent est minimal en termes de nombre d'éléments. On peut donc associer à chaque partie reconnaissable X de $A^{<\omega_1}$ un ω_1-semigroupe de façon canonique. Cet ω_1-semigroupe s'appelle l'ω_1-semigroupe syntaxique de X. Ceci étend les théorèmes 3.1.2 et 3.2.6 aux ensembles de mots de longueur dénombrable.

Proposition 3.5.31 *Soient T un ω_1-semigroupe et X une partie reconnaissable de T. Parmi toutes les congruences d'ω_1-semigroupes $\sim_X$ telles que $T/\sim_X$ reconnaisse X, il en existe une unique moins fine que toutes les autres. Le nombre de classes d'équivalences pour cette congruence, qui est minimal, est fini. Cette congruence d'ω_1-semigroupes, appelée* **congruence syntaxique de** *X, est définie par : pour tout $x, y \in T$, $x \sim_X y$ si, pour tout $r, t \in T^1$,*

$$rxt \in X \iff ryt \in X \tag{3.6}$$

et, pour tout entier $m > 1$ et $y_0, y_1, \ldots, y_m \in T^1$,

$$y_0(\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_m \in X \iff y_0(\ldots(((yy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_m \in X \tag{3.7}$$

L'ω_1-semigroupe quotient $S(X) = T/\sim_X$ est appelé l'ω_1**-semigroupe syntaxique** de X, et le morphisme $\varphi : T \to S(X)$ le **morphisme syntaxique** de X.

Exemple 3.5.32 *Soit $\{a, b\}$ un alphabet. L'ω_1-semigroupe de l'exemple 3.5.9 est l'ω_1-semigroupe syntaxique de $(aa + b)^{<\omega_1} - \lambda$.*

Exemple 3.5.33 *Soit $\{a, b\}$ un alphabet. L'ω_1-semigroupe de l'exemple 3.5.10 est l'ω_1-semigroupe syntaxique de $(ab)^{<\omega_1} - \lambda$.*

La preuve de la proposition est semblable au cas des ω^n-semigroupes. Par contre, le nombre d'équivalence à vérifier dans la proposition précédente est infini. La proposition suivante montre que malgré tout le calcul de l'ω_1-semigroupe syntaxique d'une partie reconnaissable X d'un ω_1-semigroupe est effectif à partir d'un ω_1-semigroupe fini qui reconnaît X. Sa preuve utilise le lemme suivant, dont la preuve est similaire à celle du lemme correspondant pour le cas des mots de longueur ω^n (lemme 3.4.29).

Lemme 3.5.34 *Soient S une ω_1-algèbre de Wilke et P un sous ensemble de S. La relation d'équivalence $\sim_P$ définie par, pour tout $x, y \in S$, $x \sim_P y$ si, pour tout $r, t \in S^1$,*

$$rxt \in P \iff ryt \in P \tag{3.8}$$

et, pour tout entier $m > 1$ et $y_0, y_1, \ldots, y_m \in S^1$,

$$y_0(\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_m \in P \iff y_0(\ldots(((yy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_m \in P \tag{3.9}$$

est une congruence d'ω_1-algèbre de Wilke.

Proposition 3.5.35 *Soient S une ω_1-algèbre de Wilke finie, $P \subseteq S$ et $n = |S|^2$. On dénote par $\sim_P^1$ la relation d'équivalence du lemme 3.5.34 et $\sim_P^2$ la relation d'équivalence définie par, pour $x, y \in S$, $x \sim_P^2 y$ si, pour tout $r, t \in S^1$,*

$$rxt \in P \iff ryt \in P$$

et, pour tout entier $1 < m \leq n$ et $y_0, y_1, \ldots, y_m \in S^1$

$$y_0(\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_m \in P \iff y_0(\ldots(((yy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_m \in P$$

Alors $x \sim_P^1 y$ si et seulement si $x \sim_P^2 y$ pour tout $x, y \in S$.

Preuve Evidemment, si $x \sim_P^1 y$ alors $x \sim_P^2 y$. Supposons maintenant que $x \sim_P^2 y$. Bien entendu, l'équivalence 3.8 est vérifiée. On montre que l'équivalence 3.9 est vérifiée pour tout entier $m > 1$ par induction sur m. Si $n = 1$ le résultat est vrai. Sinon, il l'est pour tout entier m inférieur ou égal à n car $x \sim_P^2 y$. Supposons maintenant qu'il est vrai pour m, on le montre pour $m+1$, avec $m+1 > n$. Supposons que $y_0(\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots)^\omega y_{m+1} \in P$. Soit $(c_i)_{0<i\leq m+1}$ la suite des éléments de $S \times S$ définie par

$$c_i = ((\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots y_i)^\omega, (\ldots(((yy_1)^\omega y_2)^\omega y_3)^\omega \ldots y_i)^\omega)$$

Comme $m+1 > n$ il existe i et j deux entiers tels que $i < j$, donc

$$(\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots y_i)^\omega = (\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots y_j)^\omega$$

et

$$(\ldots(((yy_1)^\omega y_2)^\omega y_3)^\omega \ldots y_i)^\omega = (\ldots(((yy_1)^\omega y_2)^\omega y_3)^\omega \ldots y_j)^\omega$$

Il vient que

$$\begin{aligned} &y_0(\ldots((\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots y_j)^\omega y_{j+1})^\omega \ldots)^\omega y_m \\ &\qquad = y_0(\ldots((\ldots(((xy_1)^\omega y_2)^\omega y_3)^\omega \ldots y_i)^\omega y_{j+1})^\omega \ldots)^\omega y_m \end{aligned} \tag{3.10}$$

et

$$\begin{aligned} &y_0(\ldots((\ldots(((yy_1)^\omega y_2)^\omega y_3)^\omega \ldots y_j)^\omega y_{j+1})^\omega \ldots)^\omega y_m \\ &\qquad = y_0(\ldots((\ldots(((yy_1)^\omega y_2)^\omega y_3)^\omega \ldots y_i)^\omega y_{j+1})^\omega \ldots)^\omega y_m \end{aligned} \tag{3.11}$$

Or par hypothèse de récurrence le terme de droite de 3.11 est dans P si et seulement si celui de gauche de 3.11 l'est aussi, ce qui termine la preuve de la proposition. ∇

Comme pour le cas des ω^n-semigroupes, l'ω_1-semigroupe d'une partie reconnaissable X est le plus petit, au sens de la division, qui reconnait X :

Théorème 3.5.36 *Soient A un alphabet et X une partie reconnaissable de $A^{<\omega_1}$. Un ω_1-semigroupe T reconnait X si et seulement si $S(X)$ divise T. De plus, si T divise un troisième ω_1-semigroupe U, alors U reconnait X.*

La preuve est similaire à celle du théorème 3.4.34.

3.5.4 Opérations

Nous généralisons maintenant deux opérations très utilisées sur les semigroupes aux ω_1-semigroupes. Ces opérations ont été étendues dans [Car93] des semigroupes aux ω-semigroupes.

Produit de Schützenberger

Soit A un alphabet. Soient $\varphi : A^+ \to S$ et $\psi : A^+ \to T$ deux morphismes de semigroupes qui reconnaissent respectivement deux parties L_S et L_T de A^+. Le **produit de Schützenberger** $S \diamond T$ est le semigroupe de support $S \times [S^1 \times T^1] \times T$ muni du produit $(s_1, P_1, t_1)(s_2, P_2, t_2) = (s_1 s_2, s_1 P_2 \cup P_1 t_2, t_1 t_2)$ avec

$$\begin{aligned} s_1 P_2 &= \{(s_1 s, t) : (s,t) \in P_2\} \\ P_1 t_2 &= \{(s, t t_2) : (s,t) \in P_1\} \end{aligned}$$

L'élément (s, P, t) du semigroupe $S \diamond T$ peut alors être identifié avec la matrice

$$\begin{pmatrix} t & P \\ 0 & s \end{pmatrix}$$

et le produit du semigroupe au produit matriciel. Le morphisme $\varphi \diamond \psi : A^+ \to S \diamond T$ est obtenu en posant, pour toute lettre a de A,

$$\varphi \diamond \psi(a) = \begin{pmatrix} \varphi(a) & \{(\varphi(a), 1), (1, \psi(a))\} \\ 0 & \psi(a) \end{pmatrix}$$

On a alors

Théorème 3.5.37 (Schützenberger) *Soient A un alphabet, S et T deux semigroupes qui reconnaissent respectivement deux parties L_S et L_T de A^+. Alors $S \diamond T$ reconnait L_S, L_T, $L_S \cup L_T$, $L_S \cap L_T$ et $L_S \cdot L_T$.*

Pour en obtenir la preuve, il suffit de se convaincre que si (s, P, t) est l'image d'un mot u de A^+ par $\varphi \diamond \psi$ alors s et t sont respectivement les images de u par φ et ψ, et P contient exactement les couples $(\varphi(v), \psi(w))$ tels que $u = vw$ avec $v, w \in A^*$.

Carton [Car93] a adapté le produit de Schützenberger aux langages de mots de longueur ω : si S et (T_+, T_ω) sont respectivement un semigroupe et un ω-semigroupe alors $S \diamond T$ est l'ω-semigroupe de support $(S \diamond T_+, [S^1 \times T_\omega] \times T_\omega)$. Les éléments de $[S^1 \times T_\omega] \times T_\omega$ sont identifiables à des matrices colonnes, et le produit d'un élément de $S \diamond T_+$ et d'un élément de $[S^1 \times T_\omega] \times T_\omega$ au produit de matrice habituel. L'application $\omega : S \diamond T_+ \to [S^1 \times T_\omega] \times T_\omega$ est définie par

$$\begin{pmatrix} s_1 & P_1 \\ 0 & t_1 \end{pmatrix}^\omega = \begin{pmatrix} \{(s_1^k s, t t_1^\omega) : k \in \mathbb{N} \text{ et } (s,t) \in P_1\} \\ t_1^\omega \end{pmatrix}$$

avec la convention que $s^0 = 1$. On a alors une généralisation du théorème 3.5.37 :

Théorème 3.5.38 (Carton) *Soient A un alphabet, S et T respectivement un semigroupe et un ω-semigroupe qui reconnaissent $L_S \subseteq A^+$ et $L_T \subseteq A^\omega$. Alors $S \diamond T$ reconnait L_S, L_T, $L_S \cup L_T$, $L_S \cap L_T$ et $L_S \cdot L_T$.*

Nous étendons maintenant le produit de Schützenberger aux ω_1-semigroupes.

Soient $\varphi : A^{[1,\omega_1[} \to S$ et $\psi : A^{[1,\omega_1[} \to T$ deux morphismes d'ω_1-semigroupes. Le **produit de Schützenberger** de S et de T, noté $S \diamond T$, est l'ω_1-semigroupe de support $S \times [S^1 \times T^1] \times T$ dont les éléments sont identifiables à des matrices 2×2, le produit est défini par le produit matriciel et l'application $\omega : S \diamond T \to S \diamond T$ par

$$\begin{pmatrix} s & P \\ 0 & t \end{pmatrix}^\omega = \begin{pmatrix} s^\omega & \{(s^k s', t' t^\omega) : k \in \mathbb{N} \text{ et } (s', t') \in P\} \cup \{(s^\omega, 1)\} \\ \emptyset & t^\omega \end{pmatrix}$$

avec la convention que $s^0 = 1$. On vérifie facilement que le produit est associatif, que $s(ts)^\omega = (st)^\omega$ et $(s^n)^\omega = s^\omega$ pour tout $n \in \mathbb{N}^*$ et $s, t \in S \diamond T$. On définit le morphisme $\varphi \diamond \psi : A^{[1,\omega_1[} \to S \diamond T$ par

$$\varphi \diamond \psi(a) = \begin{pmatrix} \varphi(a) & \{(\varphi(a), 1), (1, \psi(a))\} \\ \emptyset & \psi(a) \end{pmatrix}$$

et par application de la proposition 3.5.7, de manière analogue au cas des mots finis.

Voici l'extension des théorèmes 3.5.37 et 3.5.38 attendue :

Théorème 3.5.39 *Soient A un alphabet, S et T deux ω_1-semigroupes qui reconnaissent respectivement deux parties L_S et L_T de $A^{[1,\omega_1[}$. Alors $S \diamond T$ reconnait L_S, L_T, $L_S \cup L_T$, $L_S \cap L_T$ et $L_S \cdot L_T$.*

Preuve Nous allons montrer que si $u \in A^{[1,\omega_1[}$, alors

$$\varphi \diamond \psi(u) = \begin{pmatrix} \varphi(u) & \{(\varphi(v), \psi(w)) : v, w \in A^{<\omega_1} \text{ et } u = vw\} \\ \emptyset & \psi(u) \end{pmatrix}$$

Le théorème s'en déduit directement. La preuve fonctionne par induction sur $|u|$. Si $|u| = 1$ le résultat vient immédiatement de la définition de $\varphi \diamond \psi$. Supposons maintenant que $u = va$, où a est une lettre, et que le résultat soit vrai pour v. On a alors $\varphi \diamond \psi(u) = \varphi \diamond \psi(v) \cdot \varphi \diamond \psi(a)$ ce qui est égal, par hypothèse de récurrence, à

$$\begin{pmatrix} \varphi(v) & \{(\varphi(v_1), \psi(v_2)) : v_1, v_2 \in A^{<\omega_1} \text{ et } v = v_1 v_2\} \\ \emptyset & \psi(v) \end{pmatrix} \cdot \begin{pmatrix} \varphi(a) & \{(\varphi(a), 1), (1, \psi(a))\} \\ \emptyset & \psi(a) \end{pmatrix}$$

c'est-à-dire, par définition du produit,

$$\begin{pmatrix} \varphi(u) & \{(\varphi(u), 1), (\varphi(v), \psi(a))\} \cup \{(\varphi(v_1), \psi(v_2 a)) : v_1, v_2 \in A^{<\omega_1} \text{ et } v = v_1 v_2\} \\ \emptyset & \psi(u) \end{pmatrix}$$

d'où le résultat. Supposons maintenant que $|u| \in Lim$, et que l'énoncé soit vrai pour tout mot de longueur inférieure à $|u|$. D'après le théorème 3.3.7 il existe une suite $(u_i)_{i<\omega}$ de mots sur A et un couple lié (s,e) de $S \diamond T$ tels que $\varphi \diamond \psi(u_0) = s$, $\varphi \diamond \psi(u_i) = e$ pour tout entier i positif et $u = \prod_{i<\omega} u_i$. Posons

$$s = \begin{pmatrix} s_1 & P_1 \\ 0 & t_1 \end{pmatrix} \qquad e = \begin{pmatrix} s_2 & P_2 \\ 0 & t_2 \end{pmatrix} \qquad e^\omega = \begin{pmatrix} s_3 & P_3 \\ 0 & t_3 \end{pmatrix}$$

Nous allons montrer que

$$P_3 = \{(\varphi(v), \psi(w)) : v, w \in A^{<\omega_1} \text{ et } \prod_{0<i<\omega} u_i = vw\} \tag{3.12}$$

Soient v et w tels que $\prod_{0<i<\omega} u_i = vw$. Si $w = \lambda$ alors $v = \prod_{0<i<\omega} u_i$, et on a $(\varphi(v), \psi(w)) = (e^\omega, 1)$, qui appartient à P_3 par définition. Sinon, $v = (\prod_{0<i\leq k} u_i)v'$ et $w = w'\prod_{k+1<i<\omega} u_i$ pour un certain entier k et $v', w' \in A^{<\omega_1}$ tels que $v'w' = u_{k+1}$. Comme $\varphi \diamond \psi(u_{k+1}) = e$ et $|u_{k+1}| < |u|$, par hypothèse de récurrence il vient $(\varphi(v'), \psi(w')) \in P_2$, et $(s_2^k\varphi(v'), \psi(w')t_2^\omega) \in P_3$ par définition de P_3. Supposons maintenant que $(s,t) \in P_3$. Si $(s,t) = (s_2^\omega, 1)$ alors en posant $v = \prod_{0<i<\omega} u_i$ et $w = 1$ on a $vw = \prod_{0<i<\omega} u_i$ et $(\varphi(v), \psi(w)) = (s,t)$. Sinon, par définition il existe $(s', t') \in P_2$ et un entier k tels que $s = s_2^k s'$ et $t = t't_2^\omega$. Par hypothèse de récurrence, il existe $v, w \in A^{<\omega_1}$ tels que $vw = u_{k+1}$, $s' = \varphi(v)$ et $t' = \psi(w)$. Donc $s = s_2^k s' = \varphi((\prod_{0<i\leq k} u_i)v)$ et $t = t't_2^\omega = \psi(w\prod_{k+1<i<\omega} u_i)$ et par conséquent (s,t) appartient au membre droit de l'égalité 3.12, ce qui finit de montrer 3.12. Comme évidemment $s_3 = \varphi(\prod_{0<i<\omega} u_i)$ et $t_3 = \psi(\prod_{0<i<\omega} u_i)$ il vient que

$$\varphi \diamond \psi(\prod_{0<i<\omega} u_i) = \begin{pmatrix} \varphi(\prod_{0<i<\omega} u_i) & \{(\varphi(v), \psi(w)) : v, w \in A^{<\omega_1} \text{ et } \prod_{0<i<\omega} u_i = vw\} \\ \emptyset & \psi(\prod_{0<i<\omega} u_i) \end{pmatrix}$$

Maintenant,

$$\varphi \diamond \psi(u) = \varphi \diamond \psi(u_0) \cdot \varphi \diamond \psi(\prod_{0<i<\omega} u_i) = \begin{pmatrix} \varphi(u) & s_1P_3 \cup P_1t_3 \\ 0 & \psi(u) \end{pmatrix}$$

Il reste à vérifier que $s_1P_3 \cup P_1t_3 = \{(\varphi(v), \psi(w)) : v, w \in A^{<\omega_1} \text{ et } u = vw\}$. Supposons que (s,t) soit un couple du membre gauche de l'égalité. On a alors $(s,t) \in s_1P_3$ ou $(s,t) \in P_1t_3$. Supposons que $(s,t) \in s_1P_3$, l'autre cas est similaire. Il existe donc $(s', t) \in P_3$ tel que $s = s_1s'$, et donc $v, w \in A^{<\omega_1}$ tels que $vw = \prod_{0<i<\omega} u_i$, $\varphi(v) = s'$ et $\psi(w) = t$. Comme $\varphi(u_0v) = s_1s' = s$ et $u_0vw = u$ le couple (s,t) appartient au membre droit de l'égalité. Passons à la réciproque. Soit $(\varphi(v), \psi(w))$ un couple du membre droit de l'égalité. On a $vw \in A^{<\omega_1}$ et $u = vw$, et donc ou bien $v = u_0v'$ ou bien $u_0 = vv'$ avec $v' \in A^{<\omega_1}$. Supposons que $v = u_0v'$, l'autre cas est similaire. On a alors $(\varphi(v'), \psi(w)) \in P_3$ et $\varphi(v) = \varphi(u_0)\varphi(v') = s_1\varphi(v')$ donc $(\varphi(v), \psi(w)) \in s_1P_3$. ∇

Produit en couronne

Nous généralisons maintenant une autre opération importante sur les ω_1-semigroupes, le produit en couronne de deux ω_1-semigroupes. Cette opération a été généralisée aux mots de longueur ω par Carton [Car93]. Le produit en couronne est lié aux applications séquentielles. Soient A et B deux alphabets finis. Une **application séquentielle** $\sigma : A^{<\omega_1} \to B^{<\omega_1}$ est une application décrite par un transducteur. Un **transducteur** est un sextuplet $< Q, A, B, q_0, \cdot, * >$ où $< Q, A, \cdot, \{q_0\}, \emptyset >$ est un D-automate déterministe complet et $*$ est une application de sortie, c'est-à-dire une application de $Q \times A$ dans $B^{<\omega_1}$ qu'on peut naturellement étendre en une application de $Q \times A^{<\omega_1}$ dans $B^{<\omega_1}$ en posant

- $q * \lambda = \lambda$,
- $q * ua = (q * u)((q \cdot u) * a)$,
- si $|u| \in \mathit{Lim}$ et $u = \prod_{i<\omega} u_i$ alors $q * u = \prod_{i<\omega} (q \cdot (\prod_{j<i} u_j)) * u_i$.

Une application $\sigma : A^{<\omega_1} \to B^{<\omega_1}$ est dite **séquentielle** s'il existe un transducteur $< Q, A, B, q_0, \cdot, * >$ tel que $\sigma(u) = q_0 * u$ pour tout mot $u \in A^{<\omega_1}$.

Si E et E' sont deux ensembles nous notons $E^{E'}$ l'ensemble des applications de E' dans E.

Définition 3.5.40 *Soient S et T deux ω_1-semigroupes finis. Le* **produit en couronne** *$S \circ T$ de S et de T est l'ensemble fini $S^{T^1} \times T$ muni du produit*

$$(f_1, t_1)(f_2, t_2) = (t \to f_1(t) f_2(t t_1), t_1 t_2)$$

et de l'opération ω

$$(f_1, t_1)^\omega = (t \to f_1(t) f_1(t t_1)^\omega, t_1^\omega)$$

que nous ne définissons que sur les idempotents par application de la remarque 3.5.5.

On vérifie facilement que $S \circ T$ est un ω_1-semigroupe.

Théorème 3.5.41 *Soient A et B deux alphabets finis, $\sigma : A^{<\omega_1} \to B^{<\omega_1}$ une application séquentielle réalisée par un transducteur $< Q, A, B, q_0, \cdot, * >$ et $M(\sigma)$ l'ω_1-monoïde construit à partir de $< Q, A, \cdot, \{q_0\}, \emptyset >$ dans la sous-sous-section 3.5.2. Si $L \subseteq B^{<\omega_1}$ est reconnu par un ω_1-monoïde M, alors $\sigma^{-1}(L)$ est reconnu par $M \circ M(\sigma)$.*

Preuve Notons μ le morphisme de $A^{<\omega_1}$ dans $M(\sigma)$ et $\varphi : B^{<\omega_1} \to M$ celui qui reconnait L. Soit $\psi : A^{<\omega_1} \to M \circ M(\sigma)$ le morphisme d'ω_1-semigroupes défini par, pour toute lettre $a \in A$,

$$\psi(a) = (t \to \varphi(q_0 t * a), \mu(a))$$

Le diagramme suivant résume la situation :

$$\begin{tikzcd}
M(\sigma) & A^{<\omega_1} \arrow[l, "\mu"'] \arrow[r, dashed, "\sigma"] \arrow[d, "\psi"'] & B^{<\omega_1} \arrow[r, "\varphi"] & M \\
 & M \circ M(\sigma) & &
\end{tikzcd}$$

Lemme 3.5.42 *Pour tout mot $u \in A^{<\omega_1}$ on a*

$$\psi(u) = (t \to \varphi(q_0 t * u), \mu(u))$$

Preuve Par induction sur $|u|$. Le résultat est évidemment vrai pour $|u| = 1$ par définition de ψ. Si $u = va$ alors

$$\begin{aligned}
\psi(va) &= (t \to \varphi(q_0 t * u)), \mu(u))(t \to \varphi(q_0 t * a), \mu(a)) \\
&= (t \to \varphi(q_0 t * u))\varphi(q_0 t\mu(u) * a), \mu(ua)) \\
&= (t \to \varphi((q_0 t * u)(q_0 t\mu(u) * a)), \mu(ua)) \\
&= (t \to \varphi(q_0 t * ua), \mu(ua))
\end{aligned}$$

Si maintenant $|u| \in \mathit{Lim}$ d'après le théorème 3.3.7 il existe un couple lié (s, e) de $M \circ M(\sigma)$, un couple lié (s', e') de $M(\sigma)$ et une suite $(u_i)_{i<\omega}$ de mots de $A^{<\omega_1}$ tels que $u = \prod_{i<\omega} u_i$, $\psi(u_0) = s$, $\mu(u_0) = s'$ et $\psi(u_i) = e$ et $\mu(u_i) = e'$ pour tout entier i positif. En particulier on a

$$\varphi(q_0 t\mu(u_0 u_1) * u_1) = \varphi(q_0 t\mu(\prod_{j<i} u_j) * u_i)$$

pour tout entier i positif. On a donc, en utilisant l'hypothèse de récurrence,

$$\begin{aligned}
\psi(u) &= \psi(u_0)\psi(u_1)^\omega \\
&= (t \to \varphi(q_0 t * u_0), \mu(u_0))(t \to \varphi(q_0 t * u_1), \mu(u_1))^\omega \\
&= (t \to \varphi(q_0 t * u_0), \mu(u_0))(t \to \varphi(q_0 t * u_1)\varphi(q_0 t\mu(u_1) * u_1)^\omega, \mu(u_1)^\omega) \\
&= (t \to \varphi(q_0 t * u_0)\varphi(q_0 t\mu(u_0) * u_1)\varphi(q_0 t\mu(u_0 u_1) * u_1)^\omega, \mu(u)) \\
&= (t \to \varphi(q_0 t * u_0 u_1)\varphi(q_0 t\mu(u_0 u_1) * u_1)^\omega, \mu(u)) \\
&= (t \to \varphi(q_0 t * u), \mu(u))
\end{aligned}$$

∇

Comme $\sigma(u) \in L$ si et seulement si $\varphi(q_0 * u) \in \varphi(L)$, $M \circ M(\sigma)$ reconnait $\sigma^{-1}(L)$. ∇

3.5.5 Structure des ω_1-semigroupes

Nous donnons maintenant quelques propositions relatives à la structure des ω_1-semigroupes finis. Les résultats présentés ici sont facilement adaptables aux ω^n-semigroupes finis.

Pour ce qui concerne la structure multiplicative du semigroupe nous renvoyons au chapitre 3 de [Pin84]. Tout au long de cette sous-section S est un ω_1-semigroupe fini.

Proposition 3.5.43 *Soient e et e' deux idempotents de S. Si $e \mathcal{D} e'$ alors $e^\omega \mathcal{L} e'^\omega$.*

Preuve D'après la proposition 3.3.5 il existe $x, y \in S$ tels que $e = xy$ et $e' = yx$. Donc $e^\omega = (xy)^\omega = x(yx)^\omega = xe'^\omega$ et $e'^\omega = (yx)^\omega = y(xy)^\omega = ye^\omega$ ce qui prouve que $e^\omega \mathcal{L} e'^\omega$. ∇

Proposition 3.5.44 *Soient e et e' deux idempotents de S. Si $e \mathcal{R} e'$ alors $e^\omega = e'^\omega$.*

Preuve Comme $e \mathcal{R} e'$ il existe x tel que $e'x = e$. D'après la proposition 3.3.5 $ee' \mathcal{H} e'$, c'est-à-dire $e'xe' \mathcal{H} e'$. Posons $h = e'xe'$. Comme $\mathcal{H}(e')$ est un groupe de neutre e' d'après la proposition 3.3.4, il existe un entier n positif tel que $h^n = e'$. Posons maintenant $y = h^{n-1}e'v$. On a $e'y = e'(e've')^{n-1}e'v = (e'v)^n = e^n = e$ et $ye' = (e've')^{n-1}e've' = (e've')^n = e'$. Donc $e^\omega = (e'y)^\omega = e'(ye')^\omega = e'e'^\omega = e'^\omega$. ∇

La proposition suivante montre, comme le théorème 2.5.2 en conjonction avec les théorèmes 2.6.1 et 3.5.17, que tout langage reconnaissable par ω_1-semigroupe contient un mot de longueur inférieure à ω^ω :

Proposition 3.5.45 *Soient A un alphabet, S un ω_1-semigroupe fini, $\varphi : A^{<\omega_1} \to S$ un morphisme d'ω_1-semigroupes, $x \in S$ et u le plus court mot de $A^{<\omega_1}$ tel que $\varphi(u) = x$. Alors $|u| = \sum_{j=i}^{0} \omega^j a_j$ avec $a_i > 0$ et $\sum_{j=0}^{i} a_j \leq |S|$.*

Preuve Il suffit d'utiliser les théorèmes 3.5.17 et 2.5.2 pour montrer que $|u| < \omega^\omega$. Posons $|u| = \sum_{j=i}^{0} \omega^j a_j$ avec $a_i > 0$. Supposons que $\sum_{j=0}^{i} a_j > |S|$. Soit $(s_j)_{1 \leq j \leq \sum_{j=0}^{i} a_j}$ la suite d'éléments de S définie par ($l < a_{i-k-1}$)

$$s_{\sum_{j=i-k}^{i} a_j + l} = \varphi(u[0, \sum_{j=i}^{i-k} \omega^j a_j + \omega^{i-k-1} l[)$$

Si $\sum_{j=0}^{i} a_j > |S|$ il existe deux entiers k et l ($k < l$) plus petits ou égaux à $\sum_{j=0}^{i} a_j$ tels que $s_k = s_l$. Soient (avec $l_1 < a_{i-k_1-1}$ et $l_2 < a_{i-k_2-1}$)

$$k = \sum_{j=i-k_1}^{i} a_j + l_1 \qquad \text{et} \qquad l = \sum_{j=i-k_2}^{i} a_j + l_2$$

On pose

$$w = u[0, \sum_{j=i}^{i-k_1} \omega^j a_j + \omega^{i-k_1-1} l_1[\qquad \text{et} \qquad v = u[\sum_{j=i}^{i-k_2} \omega^j a_j + \omega^{i-k_2-1} l_2, |u|[$$

On a $\varphi(w) = s_k$. Posons $\varphi(v) = y$. On a $\varphi(u) = s_k y = x$. Comme

$$|v| = \omega^{i-k_2-1}(a_{i-k_2-1} - l_2) + \sum_{j=i-k_2-2}^{0} \omega^j a_j$$

et comme soit $k_2 > k_1$, soit $k_2 = k_1$ et $l_2 > l_1$ on peut vérifier que $|wv| < |u|$, or $\varphi(wv) = \varphi(w)\varphi(v) = s_k y = x$, ce qui contredit l'hypothèse, donc $\sum_{j=0}^{i} a_j \leq |S|$. ∇

3.5.6 Variétés

Nous étendons maintenant le théorème d'Eilenberg, qui établit une bijection entre les pseudo-variétés de monoïdes et les variétés de langages rationnels de mots finis aux langages de mots reconnaissables par ω_1-monoïdes. Nous renvoyons à [Eil76, Pin84] et [PP97] pour les analogues sur respectivement les mots finis et de longueur ω. Tous les ω_1-monoïdes considérés ici sont finis, exceptés les ω_1-monoïdes libres.

Nous commençons par rappeler que les pseudo-variétés d'ω_1-monoïdes sont définissables par des suites d'identités. Ce résultat est issu de la théorie des algèbres universelles. Pour les preuves, nous renvoyons à [Alm94].

Définition 3.5.46 *Soit V un ensemble de variables. L'ensemble des* **termes** *T sur V est défini récursivement par les règles :*
- *si $x \in V$ alors $x \in T$,*
- *si $x, y \in T$ alors $x \cdot y \in T$,*
- *si $x \in T$ alors $(x) \in T$,*
- *si $x \in T$ alors $x^\omega \in T$.*

On dénote par $p(v_1, \ldots, v_n)$ un terme p sur l'ensemble de variables $\{v_1, \ldots, v_n\}$. Si S est un ω_1-monoïde et $s_1, \ldots, s_n \in S$ on dénote par $p(s_1, \ldots, s_n)$ le terme $p(v_1, \ldots, v_n)$ dans lequel v_i a été remplacé par s_i pour tout $1 \leq i \leq n$.

Définition 3.5.47 *Soit V un ensemble de variables. Une* **identité** *sur V est une égalité $p = q$ où p et q sont des termes sur V. On dit qu'un ω_1-monoïde S* **satisfait** *une identité $p(v_1, \ldots, v_n) = q(v_1, \ldots, v_n)$, et on écrit $S \models p = q$, si $p(s_1, \ldots, s_n) = q(s_1, \ldots, s_n)$ pour tout $s_1, \ldots, s_n \in S$. L'ensemble des ω_1-monoïdes qui satisfont un ensemble I d'identité est dénoté par $[I]$.*

Nous omettrons par la suite d'indiquer l'ensemble V sur lesquels les identités sont construites.

Théorème 3.5.48 (Eilenberg et Schützenberger) *Soit $\boldsymbol{V}$ une pseudo-variété d'ω_1-monoïdes. Il existe une suite $(\iota_n)_{n\in\mathbb{N}}$ d'identités telle que $\boldsymbol{V} = \cup_{k\in\mathbb{N}}[\iota_n : n \geq k]$.*

Nous utilisons maintenant les pseudo-variétés d'ω_1-monoïdes pour classifier les langages D-reconnaissables par les propriétés algébriques de leur ω_1-monoïde syntaxique.

Si $\boldsymbol{V}$ est une pseudo-variété d'ω_1-monoïdes et A un alphabet, on dénote par $A^{<\omega_1}\mathcal{V}$ l'ensemble des langages reconnaissables de $A^{<\omega_1}$ dont l'ω_1-monoïde syntaxique est dans $\boldsymbol{V}$.

Autrement dit,

Proposition 3.5.49 *$A^{<\omega_1}\mathcal{V}$ est l'ensemble des langages de $A^{<\omega_1}$ reconnus par un ω_1-monoïde de $\boldsymbol{V}$.*

Preuve L'inclusion de la gauche vers la droite est triviale. Soit maintenant L un langage de mots de $A^{<\omega_1}$ reconnu par $S \in \boldsymbol{V}$. Comme $S(L) < S$ et que $\boldsymbol{V}$ est fermé par division alors $S(L) \in \boldsymbol{V}$, donc $L \in A^{<\omega_1}\mathcal{V}$. ∇

Définition 3.5.50 *Une* **classe de langages reconnaissables** *est une application $\mathcal{C}$ qui associe à chaque alphabet A un ensemble $A^{<\omega_1}\mathcal{C}$ de langages reconnaissables de $A^{<\omega_1}$.*

Définition 3.5.51 *Une* **variété de langages** *$\mathcal{V}$ est une classe de langages reconnaissables telle que*

- *pour tout alphabet A, si $L, L' \in A^{<\omega_1}\mathcal{V}$ et $u \in A^{<\omega_1}$ alors $L \cup L' \in A^{<\omega_1}\mathcal{V}$, $A^{<\omega_1} - L \in A^{<\omega_1}\mathcal{V}$, $u^{-1}L \in A^{<\omega_1}\mathcal{V}$, $Lu^{-1} \in A^{<\omega_1}\mathcal{V}$ et finalement $Lu^{-\omega} \in A^{<\omega_1}\mathcal{V}$,*
- *si $\varphi : A^{<\omega_1} \to B^{<\omega_1}$ est un morphisme d'ω_1-monoïdes libres et $L \in B^{<\omega_1}\mathcal{V}$ alors $\varphi^{-1}(L) \in A^{<\omega_1}\mathcal{V}$.*

Soit $\boldsymbol{V}$ une pseudo-variété d'ω_1-monoïdes. L'application $\boldsymbol{V} \to \mathcal{V}$ associe à $\boldsymbol{V}$ une classe de langages reconnaissables. Il n'est pas difficile de vérifier que cette classe $\mathcal{V}$ est une variété de langages.

Proposition 3.5.52 *Soient $\boldsymbol{V}$ une pseudo-variété d'ω_1-monoïdes et $\mathcal{V}$ une classe de langages reconnaissables tels que $\boldsymbol{V} \to \mathcal{V}$. Alors $\mathcal{V}$ est une variété de langages.*

Preuve Soient A un alphabet, $L, L' \in A^{<\omega_1}\mathcal{V}$ et $u \in A^{<\omega_1}$. On a $S(L), S(L') \in \boldsymbol{V}$. D'après les propositions 3.5.15 et 3.5.16 le premier point de la définition de variété de langages est vérifié. Soient maintenant A, B, φ et L comme dans le second point. Soit également $\varphi' : B^{<\omega_1} \to S(L)$ un morphisme de ω_1-monoïde qui reconnaît L. On a $S(L) \in \boldsymbol{V}$. Le morphisme $\varphi'' = \varphi\varphi'$ composé reconnaît L, donc $\varphi^{-1}(L) \in A^{<\omega_1}\mathcal{V}$. La situation est résumée par le diagramme suivant :

$$\begin{tikzcd}
B^{<\omega_1} \arrow[r, "\varphi'"] & S(L) \\
A^{<\omega_1} \arrow[u, "\varphi"] \arrow[ur, "\varphi''"'] &
\end{tikzcd}$$

∇

Pour prouver le théorème des variétés

Théorème 3.5.53 *L'application $\boldsymbol{V} \to \mathcal{V}$ est une bijection entre les pseudo-variétés d'ω_1-monoïdes et les variétés de langages.*

Nous avons besoin des deux propositions suivantes :

Proposition 3.5.54 *Soient $\boldsymbol{V}$ une pseudo-variété d'ω_1-monoïdes et $S \in \boldsymbol{V}$. Il existe un alphabet fini A et k langages $L_1, \ldots, L_k \in A^{<\omega_1}\mathcal{V}$ tels que $S < \prod_{1 \leq i \leq k} S(L_i)$.*

Preuve Comme S est fini il existe un alphabet fini A et un morphisme d'ω_1-monoïdes surjectif $\varphi : A^{<\omega_1} \to S$. Pour tout $s \in S$ le langage $L_s = \varphi^{-1}(s)$ est reconnu par S, donc $L_s \in A^{<\omega_1}\mathcal{V}$. Soit maintenant $\sim$ la relation d'équivalence sur $A^{<\omega_1}$ définie par $u \sim v$ si et seulement si $u \sim_{L_s} v$ pour tout $s \in S$. Si $u \sim v$ alors $u \sim_{L_{\varphi(u)}} v$, et comme $u \in L_{\varphi(u)}$ on a aussi $v \in L_{\varphi(u)}$, donc $\varphi(u) = \varphi(v)$. D'après la proposition 3.5.12

$$A^{<\omega_1}/\sim \; < \prod_{s\in S} A^{<\omega_1}/\sim_{L_s} = \prod_{s\in S} S(L_s)$$

Comme $u \sim v \Rightarrow \varphi(u) = \varphi(v)$, $\sim_\varphi$ est moins fine que $\sim$ donc, en utilisant la proposition 3.5.13, $A^{<\omega_1}/\sim_\varphi \, < A^{<\omega_1}/\sim$, et finalement, comme φ est surjective, S est isomorphe à $A^{<\omega_1}/\sim_\varphi$ d'où le résultat. ∇

Proposition 3.5.55 *Soient $\mathcal{V}$ une variété de langages, A un alphabet fini et $L \in A^{<\omega_1}\mathcal{V}$. Soit $\varphi : A^{<\omega_1} \to S(L)$ le morphisme syntaxique de L. Alors $\varphi^{-1}(s) \in A^{<\omega_1}\mathcal{V}$ pour tout $s \in S(L)$.*

Preuve Soient $w \in A^{<\omega_1}$ et

$$C_f^L(w) = \{(u,v) \in A^{<\omega_1} \times A^{<\omega_1} : uwv \in L\}$$

et

$$C_i^L(w) = \{(v_i)_{i\leq m} \in (A^{<\omega_1})^m \text{ pour tout entier } m > 1 : \\ v_0(\ldots(((wv_1)^\omega v_2)^\omega v_3)^\omega \ldots)^\omega v_m \in L\}$$

D'après la définition de la congruence syntaxique $\sim_L$, si $u, v \in A^{<\omega_1}$ on a $u \sim_L v$ si et seulement si $C_f^L(u) = C_f^L(v)$ et $C_i^L(u) = C_i^L(v)$. C'est-à-dire

$$\varphi^{-1}\varphi(w) = \left(\bigcap_{(u,v)\in C_f^L(w)} u^{-1}Lv^{-1} - \bigcup_{(u,v)\notin C_f^L(w)} u^{-1}Lv^{-1} \right)$$
$$\bigcap \bigcap_{1<m<\omega} \left(\bigcap_{(v_i)_{i\leq m}\in C_i^L(w)} v_0^{-1}Lv_m^{-1}v_{m-1}^{-\omega}\ldots v_1^{-\omega} - \bigcup_{(v_i)_{i\leq m}\notin C_i^L(w)} v_0^{-1}Lv_m^{-1}v_{m-1}^{-\omega}\ldots v_1^{-\omega} \right)$$

Comme L est reconnaissable, $S(L)$ est fini d'après la proposition 3.5.31 et comme d'après la proposition 3.5.15 $S(L)$ reconnaît chacun des résiduels ces derniers sont en nombre fini. Finalement, la proposition 3.5.35 montre que le nombre d'opérations booléenes de l'égalité précédente est fini. Le résultat vient des propriétés de fermeture des variétés de langages. ∇

Nous retournons maintenant à la preuve du théorème des variétés :
Preuve du théorème 3.5.53. Nous montrons d'abord que $\boldsymbol{V} \to \mathcal{V}$ est injective, i.e. si $\boldsymbol{V}$ et $\boldsymbol{W}$ sont pseudo-variétés de ω_1-monoïdes et $\boldsymbol{V} \to \mathcal{V}$ et $\boldsymbol{W} \to \mathcal{W}$ alors $\mathcal{V} = \mathcal{W}$

implique $\boldsymbol{V} = \boldsymbol{W}$. Si $S \in \boldsymbol{V}$ d'après la proposition 3.5.54 il existe un alphabet A et $L_1, \ldots, L_k \in A^{<\omega_1}\mathcal{V}$ tels que $S < \prod_{1 \leq i \leq k} S(L_i)$. Comme par hypothèse de récurrence $\mathcal{V} = \mathcal{W}$ on a $L_1, \ldots, L_k \in A^{<\omega_1}\mathcal{W}$, il suit que $S(L_i) \in \boldsymbol{W}$ pour tout $1 \leq i \leq n$, donc $S \in \boldsymbol{W}$ d'après les propriétés de fermeture des pseudo-variétés d'ω_1-monoïdes. Si $S \in \boldsymbol{W}$ on montre que $S \in \boldsymbol{V}$ en utilisant exactement les mêmes arguments. Donc $\mathcal{V} = \mathcal{W}$ implique $\boldsymbol{V} = \boldsymbol{W}$.

Il reste à prouver que $\boldsymbol{V} \to \mathcal{V}$ est surjective. Soit $\mathcal{V}$ une variété de langages, et $\boldsymbol{V}$ l'intersection de toutes les pseudo-variétés d'ω_1-monoïdes qui contiennent les ω_1-monoïdes syntaxiques des langages de $A^{<\omega_1}\mathcal{V}$ pour un alphabet A. Comme l'intersection d'une famille de pseudo-variétés d'ω_1-monoïdes est encore une pseudo-variété d'ω_1-monoïdes, $\boldsymbol{V}$ en est une. Supposons que $\boldsymbol{V} \to \mathcal{W}$; on montre que $\mathcal{V} = \mathcal{W}$. Si $L \in A^{<\omega_1}\mathcal{V}$ alors $S(L) \in \boldsymbol{V}$, donc $L \in A^{<\omega_1}\mathcal{W}$, ce qui prouve que $A^{<\omega_1}\mathcal{V} \subseteq A^{<\omega_1}\mathcal{W}$. Passons à l'inclusion inverse. Si $L \in A^{<\omega_1}\mathcal{W}$ alors $S(L) \in \boldsymbol{V}$, et d'après la définition de $\boldsymbol{V}$ il existe un entier positif n, une famille $(A_i)_{1 \leq i \leq n}$ d'alphabets et $L_i \in A_i^{<\omega_1}\mathcal{V}$ pour tout $1 \leq i \leq n$ tels que $S(L) < \prod_{1 \leq i \leq n} S(L_i) = S$. Soit $\pi_i : S \to S(L_i)$ pour $1 \leq i \leq n$ la famille de morphismes d'ω_1-monoïdes définie par $\pi_i((s_1, \ldots, s_n)) = s_i$. Comme $S(L) < S$ il existe un morphisme $\varphi : A^{<\omega_1} \to S$ et $P \subseteq S$ tels que $P = \varphi^{-1}\varphi(L)$. Soit $\varphi_i = \pi_i \varphi$ pour chaque $1 \leq i \leq n$. Pour tout $1 \leq i \leq n$ on dénote par η_i le morphisme de $A_i^{<\omega_1}$ dans $S(L_i)$. Finallement soit $\psi_i : A^{<\omega_1} \to A_i^{<\omega_1}$ l'application définie par $\psi_i(a) = b$, où b est un élément choisi de $\eta_i^{-1}\varphi_i(a)$. On vérifie facilement que ψ_i est un morphisme d'ω_1-monoïdes. On a le diagramme suivant :

$$\begin{tikzcd}
A^{<\omega_1} \arrow[r, "\psi_i"] \arrow[d, "\varphi"'] \arrow[dr, "\varphi_i"] & A_i^{<\omega_1} \arrow[d, "\eta_i"] \\
S \arrow[r, "\pi_i"] & S(L_i)
\end{tikzcd}$$

Maintenant, comme $L = \varphi^{-1}(P) = \cup_{s \in S} \varphi^{-1}(s)$ et les variétés de langages sont fermées par union, pour prouver que $L \in A^{<\omega_1}\mathcal{V}$ il suffit de montrer que $\varphi^{-1}(s) \in A^{<\omega_1}\mathcal{V}$ pour tout $s \in S$. De plus, si $s = (s_1, \ldots, s_n)$ on a $\varphi^{-1}(s) = \cap_{1 \leq i \leq n} \varphi_i^{-1}(s_i)$, et comme les variétés de langages sont fermées par intersection, il suffit de montrer que chaque composante de l'intersection est dans $A^{<\omega_1}\mathcal{V}$. Finallement, comme $\varphi_i = \eta_i \psi_i$, $\varphi_i^{-1} = \psi_i^{-1}\eta_i^{-1}$, et comme ψ_i est un morphisme d'ω_1-monoïdes libres il suffit de montrer que $\eta_i^{-1}(s_i) \in A_i^{<\omega_1}\mathcal{V}$, ce qui découle directement de la proposition 3.5.55. ∇

Nous donnons maintenant un exemple de variété, qui est une extension de la variété $\boldsymbol{J_1}$ sur les mots finis.

Théorème 3.5.56 *Soient A un alphabet et $u \in A^{<\omega_1}$. Posons $C(u) = \{a \in A : u \in A^{<\omega_1} a A^{<\omega_1}\}$. Soit $\boldsymbol{V} = [x^2 = x, xy = yx, x^\omega = x]$, et supposons que $\boldsymbol{V} \to \mathcal{V}$. Alors*

$$A^{<\omega_1}\mathcal{V} = \{L \in Rec(A^{<\omega_1}) : \forall u \in L \ \forall v \in A^{<\omega_1} \quad C(u) = C(v) \Rightarrow v \in L\}$$

où $Rec(A^{<\omega_1})$ dénote l'ensemble des langages reconnaissables de mots de longueur dénombrable sur A.

Preuve Soit L appartenant au membre droit de l'égalité et $\varphi : A^{<\omega_1} \to S(L)$ le morphisme syntaxique de L. Soit $u \in A^{<\omega_1}$. Comme $C(uu) = C(u)$ on a nécessairement $\varphi(uu) = \varphi(u)$, donc $x^2 = x$ pour tout $x \in S(L)$. On utilise le même argument pour montrer que $xy = yx$ et $x^\omega = x$ pour tout $x, y \in S(L)$. Soit maintenant L dans le membre gauche de l'égalité, et $\varphi : A^{<\omega_1} \to S$ un morphisme d'ω_1-monoïdes qui reconnait L et tel que $S \in \boldsymbol{V}$. Soit deux mots $u, v \in A^{<\omega_1}$ tels que $C(u) = C(v)$. On montre que $\varphi(v) = \prod_{a\in C(v)} \varphi(a)$ par induction sur $|v|$. Remarquons que l'ordre des lettres pour le produit n'a pas d'importance puisque $xy = yx$. Si $|v| = 1$ le résultat est immediat. Supposons le résultat vrai pour tout mot de longueur α et que $|v| = \alpha + 1$. On a $v = v'a$ avec $a \in A$ et $|v'| = \alpha$, donc $\varphi(v) = \varphi(v'a) = (\prod_{a\in C(v')} \varphi(a))\varphi(a)$. Si $a \in C(v')$, on a $C(v) = C(v')$, et $\varphi(v) = (\prod_{a\in C(v')} \varphi(a))$ comme $xy = yx$ et $x^2 = x$. Sinon, $\varphi(v) = \varphi(v')\varphi(a) = (\prod_{a\in C(v')} \varphi(a))\varphi(a) = \prod_{a\in C(v)} \varphi(a)$. Donc le résultat est vrai pour $|v| = \alpha + 1$. Supposons maintenant que $|v| = \xi \in \mathit{Lim}$. Si A est fini, d'après le théorème 3.3.7 il existe un couple lié (s, e) de S et $(v_i)_{i\in\mathbb{N}}$ tels que $v = v_0v_1v_2\ldots$, $\varphi(v_0) = s$ et $\varphi(v_i) = e$ pour tout entier i positif. Comme $se = s$ et $e^2 = e$ et A est fini on peut choisir $(v_i)_{i\in\mathbb{N}}$ de telle façon que toute lettre qui apparait dans $v_1v_2\ldots$ apparaisse aussi dans v_0, et $C(v_i) = C(v_j)$ pour tout entiers i et j positifs. En utilisant l'hypothèse de récurrence et l'égalité $e^\omega = e$ on obtient $\varphi(v) = se^\omega = se = \prod_{a\in C(v_0)\cup C(v_1)} \varphi(a) = \prod_{a\in C(v)} \varphi(a)$. Si A est infini on obtient le résultat à partir du cas fini de la manière suivante : si $a \in A$, pour tout $\varphi(a)$ on choisit $\overline{a} \in A$ tel que $\overline{a} \in \varphi^{-1}\varphi(a)$. Si $v = a_0a_1a_2\ldots$ on pose $\overline{v} = \overline{a_0a_1a_2}\ldots$. On a $\varphi(v) = \varphi(\overline{v})$ et $C(\overline{v})$ est fini. Le cas où A est fini prouve que $\varphi(\overline{v}) = \prod_{a\in C(\overline{v})} \varphi(a)$. Il suffit donc de prouver que $\prod_{a\in C(\overline{v})} \varphi(a) = \prod_{a\in C(v)} \varphi(a)$. Soit $(i_j)_{j\in\mathbb{N}}$ la suite des indices de première apparition de chaque lettre dans v. On a que $C(v) = \cup_{j\in\mathbb{N}}\{a_{i_j}\}$. Maintenant, si $a \in C(\overline{v})$ il existe i tel que $\overline{a_i} = a$. Choisissons i le plus petit possible. Alors a_i apparait pour la première fois dans v, donc il existe j tel que $i = i_j$, et $a \in \cup_{j\in\mathbb{N}}\{\overline{a_{i_j}}\}$. Il vient donc $C(\overline{v}) = \cup_{j\in\mathbb{N}}\{\overline{a_{i_j}}\}$ comme $\overline{a_{i_j}} \in C(\overline{v})$. Donc $\prod_{a\in C(\overline{v})} \varphi(a) = \prod_{a\in C(v)} \varphi(a)$. ∇

On remarque que comme pour le cas des mots finis, on peut donner une version du théorème des variétés qui traite les ω_1-semigroupes plutôt que les ω_1-monoïdes. Il faut alors partout remplacer le terme "ω_1-monoïde" par "ω_1-semigroupe", et $A^{<\omega_1}$ par $A^{[1,\omega_1[}$. Seule la définition de la congruence syntaxique reste inchangée.

Chapitre 4

Logique

Nous définissons maintenant des langages en formalisant les propriétés des mots qui les composent à l'aide de formules de logique. La logique que nous allons utiliser, appelée calcul séquentiel, a été introduite par Büchi en 1962 [Büc62].

Dans ce chapitre nous redonnons une preuve d'un résultat de Büchi : les langages définissables par des énoncés de logique du second ordre monadique de l'ordre linéaire sont exactement les langages D-reconnaissables. Ensuite, nous étendons le théorème d'équivalence entre langages (de mots finis) reconnus par semigroupes finis apériodiques, langages sans étoile et langages définis par énoncé de logique du premier ordre aux mots de longueur inférieure à ω^n en utilisant les jeux d'Ehrenfeucht-Fraïssé. Nous donnons en particulier une preuve que les langages définis par des formules de logique du premier ordre de l'ordre linéaire sont exactement les langages sans étoile, et ceci indépendamment de la longueur des mots sur lesquels sont interprétés ces deux modèles. Les jeux d'Ehrenfeucht-Fraïssé sont notamment utilisés pour passer d'un énoncé de logique du premier ordre de l'ordre linéaire à un ω^n-semigroupe apériodique qui reconnaît le même langage. La méthode employée, très simple, permet également de passer d'un énoncé de logique du premier ordre à un semigroupe apériodique, un ω-semigroupe apériodique ou un ω_1-semigroupe apériodique suivant la longueur des mots sur lesquels sont interprétées les formules de logique. Finalement, le passage d'un ω^n-semigroupe apériodique à une expression sans étoile se fait par induction sur la structure en $\mathcal{D}$-classes de l'ω^n-semigroupe.

Nous commençons par décrire la syntaxe des formules de logique que nous utilisons, nous en verrons ensuite leur sémantique, c'est-à-dire le sens que nous leur donnons. Dans la troisième section nous redonnons la preuve du théorème de Büchi. La quatrième section est dédiée aux langages sans étoile de mots de longueur inférieure à ω^n. Elle est divisée en cinq sous-sections. La première est une présentation des jeux d'Ehrenfeucht-Fraïssé. Dans la seconde nous donnons un algorithme pour construire un énoncé ϕ du premier ordre (de l'ordre linéaire) à partir d'un ensemble E, tel que $\mathcal{L}(\phi) = E$, en procédant par induction sur les règles de construction de E. Dans la troisième nous montrons que l'ω^n-semigroupe syntaxique d'un langage défini par un énoncé du premier ordre est apériodique en utilisant les jeux. Dans la quatrième nous prouvons que la classe d'équivalence d'un mot pour les jeux d'Ehrenfeucht-Fraïssé en n coups s'obtient par induction sur n en utilisant des combinaisons booléennes et des produits de concaténation en nombre fini. Comme les langages défini par énoncé du premier ordre sont union de telles classes, et que ces dernières sont en nombre fini, ils sont sans étoile. Enfin dans la dernière nous montrons que les langages reconnus par ω^n-semigroupes finis et apériodiques sont sans étoile.

Tout au long de ce chapitre les alphabets sont supposés finis.

4.1 Syntaxe

Soit A un alphabet. Les formules de logique du second ordre que nous allons employer sont construites à partir de variables d'individus, de variables d'ensembles, de prédicats binaires, de formules atomiques, d'un quantificateur et de deux opérateurs booléens. Les variables d'individu, qu'on appelle aussi variables du premier ordre sont notées par des lettres minuscules $x, y, z, x_1, y_1, z_1, \ldots$. Les variables d'ensemble, aussi appelées variables du second ordre, sont dénotées par des lettres majuscules $X, Y, Z, X_1, Y_1, Z_1, \ldots$. Un prédicat binaire P est une relation entre deux variables d'individus. Les formules atomiques sont soit un prédicat binaire P appliqué à deux variables d'individus x et y, et la formule atomique correspondante est alors xPy, soit de la forme $R_a(x)$, où x est une variable d'individu et a une lettre de l'alphabet, soit de la forme $X(x)$, où x est une variable d'individu et X une variable d'ensemble. L'unique quantificateur que nous utiliserons est le quantificateur $\exists$. Finalement, nous emploierons les deux opérateurs booléens de négation $\neg$ et de disjonction $\vee$. En général, les formules de logiques seront notées par les lettres grecques ϕ et ψ.

Les formules de logique du second ordre sont définies par induction en suivant les règles :

- toute formule atomique est une formule,
- si ϕ et ψ sont des formules, alors $\psi \vee \phi$ aussi,
- si ϕ est une formule, alors $\neg\phi$ aussi,
- si ϕ est une formule et x une variable du premier ordre, alors $\exists x \phi$ aussi,
- si ϕ est une formule et X une variable du second ordre, alors $\exists X \phi$ aussi.

Une formule ψ qui apparaît dans la formation par les règles précédentes d'une autre formule ϕ est une **sous-formule** de ϕ. En particulier ϕ est une sous-formule de ϕ.

Nous nous servirons de formules de logique du second ordre particulières, où l'utilisation de variables du second ordre est interdite. Ces formules sont dites formules de logique du premier ordre. Ainsi, si X et x sont respectivement des variables du second et du premier ordre, alors $X(x)$ n'est pas une formule atomique du premier ordre et si ϕ est une formule de logique, alors $\exists X \phi$ n'est pas une formule du premier ordre. Si ψ n'est pas une formule du premier ordre, alors $\neg\psi$, $\psi \vee \phi$, $\phi \vee \psi$ et $\exists x \psi$, où x est une variable du premier ordre, ne le sont pas non plus.

Définition 4.1.1 *La* **hauteur de quantificateur** *$hq(\phi)$ d'une formule de logique ϕ est définie par induction sur les règles de formation des formules :*

- *$hq(xRy) = 0$,*

- $hq(R_a(x)) = 0$,
- $hq(\phi \vee \psi) = max(hq(\phi), hq(\psi))$,
- $hq(\neg\phi) = hq(\phi)$,
- $hq(\exists x\phi) = 1 + hq(\phi)$,
- $hq(\exists X\phi) = 1 + hq(\phi)$.

Définition 4.1.2 *L'ensemble $FV(\psi)$ des* **variables libres** *d'une formule de logique ϕ est également défini par induction sur les règles de formation des formules :*

- $FV(xRy) = \{x, y\}$,
- $FV(R_a(x)) = \{x\}$,
- $FV(\phi \vee \psi) = FV(\phi) \cup FV(\psi)$,
- $FV(\neg\phi) = FV(\phi)$,
- $FV(\exists x\phi) = FV(\phi) - \{x\}$,
- $FV(\exists X\phi) = FV(\phi) - \{X\}$.

Nous noterons $FVS(\psi)$ (resp. $FVF(\psi)$) l'ensemble des variables du second (resp. premier) ordre de ψ.

Une occurrence d'une variable du premier ou du second ordre de nom x dans une formule ϕ est **liée** s'il existe une sous-formule ψ de ϕ qui contient l'occurrence et telle que $x \notin FV(\psi)$, elle est **libre** sinon. Un **énoncé** est une formule qui ne contient pas de variables libres. Quitte à renommer des variables, nous supposerons que pour chaque nom de variable x (resp. X), $\exists x$ (resp. $\exists X$) apparaît au plus une seule fois dans une formule, et que si ϕ est une formule telle que $x \in FV(\phi)$ (resp. $X \in FV(\phi)$), alors $\exists x\psi$ (resp. $\exists X\psi$) n'est pas une sous-formule de ϕ. En d'autres termes, nous supposerons que toutes les occurrences d'un même nom de variable dans une formule font référence à la même variable.

Nous n'utiliserons qu'un prédicat binaire, noté $<$. Nous notons $SO[<]$ (resp. $FO[<]$) la classe des formules du second (resp. premier) ordre qui n'utilisent que le prédicat $<$ (resp. $<$).

Nous ajoutons les parenthèses à la syntaxe pour plus de clarté. De plus, pour simplifier l'écriture des formules nous définissons les abréviations suivantes :

- $\psi \wedge \phi$ pour $\neg(\neg\psi \vee \neg\phi)$,
- $\psi \to \phi$ pour $\neg\psi \vee \phi$,
- $\psi \leftrightarrow \phi$ pour $(\psi \to \phi) \wedge (\phi \to \psi)$,
- $x = y$ pour $(\neg x < y) \wedge (\neg y < x)$,
- $x = y+1$ pour $y < x \wedge (\neg \exists z\ y < z \wedge z < x)$,
- $x \leq y$ pour $x < y \vee x = y$,
- $\forall x\psi$ pour $\neg\exists x\neg\psi$,
- $\forall_z^y x\ \psi$ pour $\forall x((z \leq x \wedge x < y) \to \psi)$,
- $\exists_z^y x\ \psi$ pour $\exists x(z \leq x \wedge x < y \wedge \psi)$,
- $Succ(x)$ pour $\exists y\ x = y + 1$,
- $Lim(x)$ pour $\neg Succ(x)$.

Exemple 4.1.3 *Soit $A = \{a, b\}$ un alphabet. La formule*

$$\begin{aligned} &\exists X \exists Y \forall x (\forall y (x \leq y) \to X(x)) \\ &\qquad \wedge \forall x_1\ X(x_1) \to (R_a(x_1) \wedge \exists y_1\ y_1 = x_1 + 1 \wedge Y(y_1)) \\ &\qquad \wedge \forall x_2\ Y(x_2) \to (R_b(x_2) \wedge \forall y_2\ y_2 = x_2 + 1 \to X(y_2)) \end{aligned}$$

est un énoncé du second ordre.

Exemple 4.1.4 *Soit $A = \{a, b\}$ un alphabet. La formule*

$$\Big(\forall x\big(\neg\exists y\ x = y + 1 \to R_a(x)\big)\Big)\wedge\Big(\forall x_1 R_a(x_1) \to \big(\exists y_1\ y_1 = x_1 + 1 \wedge R_b(y_1)\big)\Big)$$
$$\wedge\Big(\forall x_2\big(\exists y_2\ x_2 < y_2 \wedge R_b(x_2)\big)\to \exists z\ z = x_2 + 1 \wedge R_a(z)\Big)$$

est un énoncé du premier ordre.

4.2 Sémantique

Nous expliquons maintenant l'interprétation de ces formules de logique. Nous utilisons pour cela la notion de mot marqué introduite par Perrin et Pin [PP86], que nous présentons comme dans [Str94].

Définition 4.2.1 *Soient V et V' respectivement des ensembles finis de variables du premier et du second ordre, A un alphabet et α un ordinal. Un (V, V')-**mot marqué** de longueur α sur A est un mot $u = ((a_\beta, V_\beta, V'_\beta))_{\beta<\alpha}$ de longueur α sur $A \times ([V] \cup \emptyset) \times ([V'] \cup \emptyset)$ tel pour chaque élément x de V il existe une et une seule lettre de u qui contient x dans sa seconde composante. Plus formellement, $\cup_{\beta<\alpha} V_\beta = V$ et $V_\beta \cap V\gamma = \emptyset$ pour tout $\beta, \gamma < \alpha$ avec $\beta \neq \gamma$. On ne pose pas de condition sur la troisième composante des lettres.*

Soit maintenant ψ une formule de logique du second ordre, A un alphabet, V et V' respectivement deux ensembles finis de variables du premier et second ordre et $u = ((a_\beta, V_\beta, V'_\beta))_{\beta<\alpha}$ un (V, V')-mot marqué de longueur α. On définit $u \models \psi$ (lire u est un **modèle** pour ψ) par induction sur la construction de ψ de la façon suivante :

- $u \models R_a(x)$ si et seulement si il existe une lettre de u de la forme $(a_\beta, V_\beta, V'_\beta)$ avec $x \in V_\beta$ et $a_\beta = a$,
- $u \models x < y$ si et seulement si il existe deux lettres $(a_\beta, V_\beta, V'_\beta)$ et $(a_\gamma, V_\gamma, V'_\gamma)$ de u telles que $x \in V_\beta$, $y \in V_\gamma$ et $\beta < \gamma$,
- $u \models X(x)$ si et seulement si il existe $\beta < \alpha$ tel que la lettre $(a_\beta, V_\beta, V'_\beta)$ d'indice β de u vérifie $x \in V_\beta$ et $X \in V'_\beta$,
- $u \models \neg\phi$ si et seulement si $u \not\models \phi$,
- $u \models \phi \vee \psi$ si et seulement si $u \models \phi$ ou $u \models \psi$,
- $u \models \exists x\phi$ si et seulement si il existe $\beta < \alpha$ tel que le mot u dans lequel la lettre $(a_\beta, V_\beta, V'_\beta)$ d'indice β est remplacée par $(a_\beta, V_\beta \cup \{x\}, V'_\beta)$ est un modèle pour ϕ,
- $u \models \exists X\phi$ si et seulement si il existe un ensemble B éventuellement vide d'ordinaux plus petits que α tel que le mot u dans lequel chaque lettre $(a_\beta, V_\beta, V'_\beta)$ dont l'indice est un élément de B est remplacée par $(a_\beta, V_\beta, V'_\beta \cup \{X\})$ est un modèle pour ϕ.

Exemple 4.2.2

$$(a, \{y\}, \emptyset)(b, \{x\}, \{X, Y\})(c, \emptyset, \{Z\}) \models R_a(y) \wedge y < x \wedge X(x) \wedge (\exists z\ x < z \wedge Z(z))$$

Remarque 4.2.3 *On note que*

1. *Quelle que soit la formule ϕ, et si x dénote une variable du premier ordre, $\lambda \not\models \exists x\phi$, donc $\lambda \models \neg\exists x\phi$, i.e. $\lambda \models \forall x\neg\phi$.*
2. *Si u est un (V, V')-mot marqué et que $u \models \phi$, alors nécessairement $FVF(\phi) \subseteq V$ et $FVS(\phi) \subseteq V'$.*

Notons qu'un $(\emptyset, \emptyset)$-mot marqué sur un alphabet A peut être vu comme un mot de A, et réciproquement. Pour alléger les notations par la suite nous confondrons donc les deux notions. Soit finalement ϕ un énoncé. L'ensemble des mots de longueur finie sur A défini par ϕ, noté $\mathcal{L}^{<\omega}(\phi)$ est

$$\mathcal{L}^{<\omega}(\phi) = \{u \in A^{<\omega} : u \models \phi\}$$

Plus généralement, si ϕ est une formule de logique, alors $\mathcal{L}^{<\omega}(\phi)$ est l'ensemble des $(FVF(\phi), FVS(\phi))$-mots marqués finis sur A qui sont un modèle pour ϕ, et $\mathcal{L}(\phi)$ est l'ensemble des $(FVF(\phi), FVS(\phi))$-mots marqués sur A qui sont un modèle pour ϕ.

Deux formules de logique ϕ et ψ sont **logiquement équivalentes**, et on note $\phi \equiv \psi$, si $\mathcal{L}^{<\omega}(\phi) = \mathcal{L}^{<\omega}(\psi)$.

La proposition suivante est au cœur de l'effectivité des résultats que nous allons présenter :

Proposition 4.2.4 *Soit V et V' respectivement des ensembles finis de variables du premier et du second ordre, A un alphabet fini et n un entier naturel. A l'équivalence logique près il n'existe qu'un nombre fini de formules de logique de hauteur de quantificateur n.*

On dit qu'une classe de formules de logique est **décidable** si, pour chaque formule ϕ de la classe, la question “existe t-il un mot marqué u qui soit un modèle pour ϕ ?” est décidable.

Ce théorème marque le lien entre les langages reconnaissables et les langages définis par formules de logiques :

Théorème 4.2.5 (Büchi) *Soit A un alphabet fini. Une partie L de A^* est rationnelle si et seulement si il existe une formule ϕ de logique du second ordre tel que $\mathcal{L}^{<\omega}(\phi) = L$.*

Pour une preuve nous renvoyons par exemple à [Str94]. Le théorème montre en particulier, avec le corollaire 2.1.8, que la logique du second ordre (et donc aussi celle du premier ordre) est décidable.

Exemple 4.2.6 *Soient $A = \{a, b\}$ et ϕ l'énoncé de l'exemple 4.1.3. Alors $\mathcal{L}^{<\omega}(\phi) = (ab)^*$. Le premier terme de l'énoncé indique que l'indice de la première lettre du mot, s'il y a en une, est dans X. Le second terme spécifie que tout élément de X est l'indice d'une lettre a dans le mot, qui est suivie d'une lettre dont l'indice est élément de Y. Enfin, le dernier terme indique que tout élément de Y est l'indice d'une lettre b dans le mot, et que si cette lettre n'est pas la dernière, alors l'indice de la suivante est un élément de X.*

Plus particulièrement, on a l'analogue du théorème précédent pour les formules du premier ordre :

Théorème 4.2.7 (McNaughton et Papert) *Soit A un alphabet fini. Une partie L de A^* reconnaissable est sans étoile si et seulement si il existe un énoncé ϕ de $FO[<]$ tel que $\mathcal{L}^{<\omega}(\phi) = L$.*

Exemple 4.2.8 *Soient $A = \{a, b\}$ et ϕ l'énoncé de l'exemple 4.1.4. Alors $\mathcal{L}^{<\omega}(\phi) = (ab)^*$. Le premier terme indique que toute lettre dont l'indice n'est pas successeur est un a. Le second spécifie que tout a est suivi d'un b. Enfin, le dernier indique que si un b n'est pas la dernière lettre alors il est suivi d'un a.*
Or, $(ab)^* = (ab)^+ \cup \{\lambda\}$. Comme $\{\lambda\} = \overline{\emptyset} - \cup_{a\in A} a\overline{\emptyset}$ et comme $(ab)^+$ est sans étoile (cf. exemple 3.1.4), $(ab)^*$ l'est aussi.

En utilisant le théorème 3.1.5 il vient :

Théorème 4.2.9 *Soit ϕ une formule de logique du second ordre. La question "existe t-il une formule ψ de logique du premier ordre telle que $\mathcal{L}^{<\omega}(\phi) = \mathcal{L}^{<\omega}(\psi)$?" est décidable.*

La logique sur les mots de longueur ω est exactement la même que celle sur les mots finis, exception faite que les mots marqués ne sont plus de longueur finie mais de longueur ω. Les résultats énoncés sur les mots finis s'étendent aux mots de longueur ω. L'utilisation des automates sur les mots finis est remplacée par celle des automates de Büchi, ou indifféremment ceux de Muller, et les semigroupes par les ω-semigroupes. Si ϕ est une formule de logique, l'ensemble des mots marqués de longueur ω qui sont un modèle pour ϕ est dénoté par $\mathcal{L}^{\omega}(\phi)$.

L'analogue du théorème 4.2.5 pour les mots de longueur ω est encore dû à Büchi. L'adaptation du théorème 4.2.7 aux mots de longueur ω est de Ladner [Lad77] et Thomas [Tho79].

Exemple 4.2.10 *Soient $A = \{a, b\}$, ϕ et ψ respectivement les énoncés des exemples 4.1.3 et 4.1.4. Alors $\mathcal{L}^{\omega}(\phi) = \mathcal{L}^{\omega}(\psi) = (ab)^{\omega}$.*

4.3 Equivalence entre D-automates et logique du second ordre

Nous redonnons dans cette section une preuve du théorème 4.2.5 étendu aux mots de longueur dénombrable en en adaptant simplement la preuve de [Str94], qui traite le cas des mots finis.

On dénote par $\mathcal{L}^{<\omega_1}(\phi)$ l'ensemble des mots marqués de longueur dénombrable qui sont un modèle pour ϕ. Nous redonnons maintenant une preuve du théorème suivant :

Théorème 4.3.1 (Büchi) *Soit A un alphabet fini. Une partie L de $A^{<\omega_1}$ est D-rationnelle si et seulement si il existe une formule ϕ de logique du second ordre tel que $\mathcal{L}^{<\omega_1}(\phi) = L$.*

Le sens de la preuve qui va des ensembles D-reconnaissables vers un énoncé du second ordre utilise des arguments classiques. Plutôt que d'un D-automate on peut partir d'un B-automate : à partir d'un B-automate $\mathcal{A} =< Q, A, E, I, F >$, on construit un énoncé qui définit le même langage en codant les états par des variables du second ordre et en utilisant des formules qui traduisent qu'un mot u est reconnu par le B-automate si et seulement si il est l'étiquette d'un chemin réussi dans $\mathcal{A}$, c'est-à-dire si et seulement si il existe des ensembles $(X_s)_{s\in[Q]_0^1}$ d'ordinaux inférieurs à $|u|$ tels que (on suppose d'abord que $\lambda \notin \mathcal{L}(\mathcal{A})$)

1. $0 \in \cup_{i\in I} X_i$,
2. une des deux conditions suivantes est vraie :
   (a) si $|u| \in \mathit{Succ}$ et $|u| - 1 \in X_s$ alors il existe $f \in F$ tel que $(s, u_{|u|-1}, f) \in E$,
   (b) si $|u| \in \mathit{Lim}$ il existe $\{s_1, \ldots, s_p\} \in F$ tel que les X_{s_i} sont exactement ceux qui contiennent une suite d'ordinaux cofinale avec $|u|$,
3. $\alpha \in X_s$ pour $s \in [Q]$ si et seulement si $\alpha \in \mathit{Lim}$,
4. si $\alpha \in X_s$ et $\alpha + 1 \in X_t$ alors $(s, u_\alpha, t) \in E$,
5. $\alpha \in X_{\{s_1,\ldots,s_p\}}$ si et seulement si les X_{s_i} sont exactement ceux qui contiennent une suite d'ordinaux cofinale avec α,
6. tout ordinal inférieur à $|u|$ est dans un X_s,
7. tous ces ensembles soient deux à deux disjoints.

On code chacune de ces propriétés par des formules du second ordre :

1. $\psi_1 \equiv \forall x(\neg\exists y\ y < x) \to \vee_{i\in I} X_i(x)$,
2. $\psi_2 \equiv \psi_{2a} \wedge \psi_{2b}$ où
   (a) $\psi_{2a} \equiv (\exists x(\forall y\ y \leq x)) \to \exists z((\forall y\ y \leq z) \wedge_{s\in[Q]_0^1} (X_s(z) \to \bigvee_{\substack{(s',a,f)\in E\\ s'=s\\ f\in F}} R_a(z)))$,
   (b)
$$\psi_{2b} \equiv (\neg\exists x(\forall y\ y \leq x)) \to \bigvee_{\{s_1,\ldots,s_p\}\in F} \Bigg(\Big(\bigwedge_{s_i\in\{s_1,\ldots,s_p\}} \forall y \exists z\ y < z \wedge X_{s_i}(z)\Big)$$
$$\bigwedge_{t\in Q-\{s_1,\ldots,s_p\}} \neg\forall y\exists z\ y < z \wedge X_t(z)\Bigg),$$
3. $\psi_3 \equiv \forall x((\mathit{Lim}(x) \wedge \exists y\ y < x) \leftrightarrow \vee_{s\in[Q]} X_s(x))$,
4. $\psi_4 \equiv \forall x \forall y(y = x + 1 \to \wedge_{(s,t)\in[Q]_0^1\times Q, s\neq t}(X_s(x) \wedge X_t(y) \to \vee_{(s',a,t')\in E, s'=s, t'=t} R_a(x))$,
5.
$$\psi_5 \equiv \bigwedge_{\{s_1,\ldots,s_p\}\in[Q]} \forall x(X_{\{s_1,\ldots,s_p\}}(x) \leftrightarrow$$
$$((\wedge_{s_i\in\{s_1,\ldots,s_p\}} \forall_0^x y\ \exists_y^x z\ X_{s_i}(z)) \wedge_{t\in Q-\{s_1,\ldots,s_p\}} \neg\forall_0^x y\ \exists_y^x z\ X_t(z))),$$
6. $\psi_6 \equiv \forall x \vee_{s\in[Q]_0^1} X_s(x)$,

7. $\psi_7 \equiv \wedge_{s\neq t,(s,t)\in([Q]_0^1)^2} \neg\exists x(X_s(x) \wedge X_t(x))$.

Si $[Q]_0^1 = \{s_1, \ldots, s_p\}$ et $\lambda \notin \mathcal{L}(\mathcal{A})$ on a alors

$$\mathcal{L}(\mathcal{A}) = \mathcal{L}(\exists X_{s_1} \cdots \exists X_{s_p} \wedge_{1\leq i\leq 7} \psi_i)$$

Si $\lambda \in \mathcal{L}(\mathcal{A})$ on a

$$\mathcal{L}(\mathcal{A}) = \mathcal{L}((\forall x\ \neg x = x) \vee (\exists X_{s_1} \cdots \exists X_{s_p} \wedge_{1\leq i\leq 7} \psi_i))$$

Nous allons maintenant prouver la réciproque du théorème. Soient A un alphabet et ϕ une formule du second ordre. Nous allons construire un D-automate $\mathcal{A}$ tel que $\mathcal{L}(\mathcal{A}) = \mathcal{L}^{<\omega_1}(\phi)$ par induction sur la structure de ϕ. Soient V_1 et V_2 respectivement l'ensemble des variables du premier et du second ordre qui apparaissent dans ϕ, et L l'ensemble des (V_1, V_2)-mots marqués de longueur dénombrable sur A. Si $a \in A$ et $x \in V_1$, il est aisé de construire un D-automate qui accepte uniquement les (V_1, V_2)-mots marqués de L dont la lettre dont x est membre de la seconde composante a a pour première composante. En d'autres termes les mots $u \in L$ tels que $u \models R_a(x)$. De même pour les autres formules atomiques. Comme le théorème 2.4.4 montre que la classe des langages D-reconnaissables est fermée par les opérations booléennes, il ne nous reste qu'à montrer que si ϕ est de la forme $\exists x\psi$ (ou bien $\exists X\psi$), alors on peut construire un D-automate $\mathcal{A}$ tel que $\mathcal{L}(\mathcal{A}) = \mathcal{L}^{<\omega_1}(\phi)$. Par hypothèse de récurrence on peut construire un D-automate $\mathcal{B} =< Q, A \times V_1' \times V_2', E, I, F >$ tel que $\mathcal{L}(\mathcal{B}) = \mathcal{L}^{<\omega_1}(\psi)$. Soit $\mathcal{A} =< Q', A \times V_1' - \{x\} \times V_2', E', I', F' >$ le D-automate défini par :

- $Q' = Q \times \{0, 1\}$,
-

$$E' = \cup \begin{cases} \{(q, (a, W_1, W_2), p) \in [Q']_0^1 \times (A \times V_1' \times V_2') \times Q' : \\ \qquad (\mathcal{P}_1(q), (a, W_1, W_2), \mathcal{P}_1(p)) \in E \text{ et } \mathcal{P}_2(p) = \mathcal{P}_2(q) \text{ et } x \notin W_1\} \\ \{(q, (a, W_1 - \{x\}, W_2), p) \in [Q']_0^1 \times (A \times V_1' \times V_2') \times Q' : \\ \qquad (\mathcal{P}_1(q), (a, W_1, W_2), \mathcal{P}_1(p)) \in E \text{ et } \mathcal{P}_2(p) = 1, \mathcal{P}_2(q) = 0 \text{ et } x \in W_1\} \end{cases}$$

- $I' = \{(p, 0) : p \in I\}$,
- $F' = \{p \in [Q']_0^1 : \mathcal{P}_1(p) \in F \text{ et } \mathcal{P}_2(p) = 1\}$.

où $\mathcal{P}_1$ est l'application de $[Q']_0^1$ dans $[Q]_0^1$ définie par

- $\mathcal{P}_1(\{p_1, \ldots, p_k\}) = \{\mathcal{P}_1(p_1), \ldots, \mathcal{P}_1(p_k)\}$
- $\mathcal{P}_1((p, q)) = p$

et $\mathcal{P}_2$ est l'application de $[Q']_0^1$ dans $\{0, 1\}$ définie par

- $\mathcal{P}_2(\{p_1, \ldots, p_k\}) = 1$ si et seulement si il existe $i \in 1 \ldots k$ tel que $\mathcal{P}_2(p_i) = 1$
- $\mathcal{P}_2((p, q)) = q$

Intuitivement, la seconde composante des éléments de Q' marque le passage dans $\mathcal{B}$ par une transition étiquetée par une lettre dont x appartient à la seconde composante. On vérifie alors facilement que $\mathcal{L}(\mathcal{A}) = \mathcal{L}^{<\omega_1}(\exists x\psi)$. La construction pour $\exists X\psi$ utilise des arguments similaires. Ceci termine la preuve du théorème 4.3.1.

4.4 Equivalence entre langages sans étoile et logique du premier ordre

Nous allons maintenant étendre les théorèmes 4.2.7 et 3.1.5 qui établissent l'équivalence entre énoncés de logique du premier ordre, semigroupes finis apériodiques et langages sans étoile aux mots de longueur inférieure à ω^{n+1}. Plus formellement,

Définition 4.4.1 *Soient A un alphabet fini et n un entier. L'ensemble $SF(A, [1, \omega^{n+1}[)$ des langages* **sans étoile** *de mots de longueur inférieure à ω^{n+1} sur A est le plus petit ensemble qui contient $\{a\}$ pour chaque lettre $a \in A$ fermé par les opérations booléennes, où la complémentation est prise par rapport à $A^{[1,\omega^{n+1}[}$, et le produit de concaténation, en nombre fini.*

Exemple 4.4.2 *Le langage $(ab)^{<\omega^2} - \lambda$ de $\{a,b\}^{<\omega^2}$ est sans étoile, puisque*

$$(ab)^{<\omega^2} - \lambda = (ab\overline{\emptyset}) - (Lb\overline{\emptyset} \cup \overline{\emptyset}a \cup \overline{\emptyset}aa\overline{\emptyset} \cup \overline{\emptyset}bb\overline{\emptyset})$$

où $L = \overline{\emptyset} - (\overline{\emptyset}A)$ est l'ensemble des mots de longueur limite, non nulle et inférieure à ω^2 sur A.

On dit qu'un ω^n-semigroupe est **apériodique** si son semigroupe de support est apériodique.

Proposition 4.4.3 *Soient A un alphabet, n un entier, S un ω^n-semigroupe qui reconnaît une partie L de $A^{[1,\omega^{n+1}[}$. Si S est apériodique, alors $S(L)$ l'est aussi.*

Preuve D'après le théorème 3.4.34 $S(L)$ divise S. Il existe donc un sous-ω^n-semigroupe T de S et un morphisme surjectif $\varphi : T \to S(L)$. Si S est apériodique T l'est aussi donc il existe un entier k tel que $t^k = t^{k+1}$ pour tout $t \in T$. Soient $x \in S(L)$, et $t \in T$ tel que $\varphi(t) = x$. On a

$$x^k = \varphi(t)^k = \varphi(t^k) = \varphi(t^{k+1}) = \varphi(t)^{k+1} = x^{k+1}$$

ce qui montre l'apériodicité de $S(L)$. ∇

Si ϕ est une formule de logique, l'ensemble des mots marqués dont la longueur appartient à $[1, \omega^{n+1}[$ qui sont un modèle pour ϕ est dénoté par $\mathcal{L}^{[1,\omega^{n+1}[}(\phi)$.

Le reste du chapitre est consacré à la preuve de ce théorème :

Théorème 4.4.4 *Soient A un alphabet fini, n un entier et L une partie reconnaissable de $A^{[1,\omega^{n+1}[}$. Les conditions suivantes sont équivalentes :*
- *$L \in SF(A, [1, \omega^{n+1}[)$,*
- *L'ω^n-semigroupe $S(L)$ est apériodique,*
- *$L = \mathcal{L}^{[1,\omega^{n+1}[}(\phi)$ pour un énoncé $\phi \in FO[<]$.*

Exemple 4.4.5 *Soit $A = \{a,b\}$ un alphabet et $L = (ab)^{<\omega^2} - \lambda$. Alors $S(L)$, donné dans l'exemple 3.4.10, est apériodique, et $L = \mathcal{L}^{[1,\omega^2[}(\phi)$, où ϕ est l'énoncé du premier ordre de l'exemple 4.1.4. De plus, l'exemple 4.4.2 montre que L est sans étoile.*

Exemple 4.4.6 *Soit $A = \{a, b\}$ un alphabet et $L = (aa+b)^{<\omega^2} - \lambda$. Puisque l'exemple 3.4.9 montre que $S(L)$ n'est pas apériodique, L n'est pas sans étoile et il n'existe pas d'énoncé ϕ du premier ordre tel que $L = \mathcal{L}^{[1,\omega^2[}(\phi)$.*

Comme les constructions que nous donnons dans la preuve du théorème 4.4.4 sont effectives,

Théorème 4.4.7 *Soient ϕ une formule de logique du second ordre et n un entier. La question "existe t-il une formule ψ de logique du premier ordre telle que $\mathcal{L}^{[1,\omega^{n+1}[}(\phi) = \mathcal{L}^{[1,\omega^{n+1}[}(\psi)$?" est décidable.*

Pour éviter des manipulations de formules de logique complexes dans la preuve nous avons besoin des jeux d'Ehrenfeucht-Fraïssé. Nous ne manipulons dans cette section que des formules du premier ordre. La partie qui concerne les variables du second ordre dans les mots marqués sera donc inutilisée.

4.4.1 Jeux d'Ehrenfeucht-Fraïssé

Les jeux que nous présentons dans cette section ont été définis par Ehrenfeucht [Ehr61] pour analyser les propriétés logiques de l'arithmétique des ordinaux. Des techniques similaires, mais qui n'utilisent pas la terminologie des jeux, ont été développées indépendamment, et antérieurement, par Fraïssé [Fra54].

Soient u et v deux $(\emptyset, \emptyset)$-mots marqués, et n un entier. Les **jeux** d'Ehrenfeucht-Fraïssé se jouent à deux joueurs, $\mathfrak{A}$ et $\mathfrak{B}$. Les deux mots u et v constituent le terrain de jeu. Chacun des deux joueurs a à sa disposition une pile de n jetons étiquetés $x_1, \ldots, x_n$. Les deux joueurs disposent d'exactement les mêmes jetons. L'objectif de $\mathfrak{A}$ est de montrer que u et v ne vérifient pas les mêmes formules atomiques, où les noms de variables sont pris dans $\{x_1, \ldots, x_n\}$, en plaçant des jetons sur des lettres de u ou de v. $\mathfrak{B}$ essaie de contrarier son adversaire. Le jeu se déroule de la façon suivante : $\mathfrak{A}$ commence ; il choisit un mot et prend un jeton, qu'il pose sur une lettre du mot choisi. $\mathfrak{B}$ joue alors sur l'autre mot en copiant l'étiquette du jeton précédemment joué par $\mathfrak{A}$. Ceci constitue un tour. Le jeu se termine quand les deux joueurs n'ont plus de jetons. A la fin du jeu, on obtient évidemment deux $(\{x_1, \ldots, x_n\}, \emptyset)$-mots marqués. On note $G(u, v, n)$ l'ensemble des jeux sur u et v avec n jetons. Un joueur a une **stratégie gagnante** dans un jeu de $G(u, v, n)$ s'il gagne, quels que soient les coups de l'adversaire.

Pour les preuves des trois propositions suivantes nous renvoyons par exemple à [Str94, Lad77] ou [Ros82].

Proposition 4.4.8 *Soient u, v deux $(\emptyset, \emptyset)$-mots marqués, et n un entier. Pour tout jeu de $G(u, v, n)$, un des deux joueurs a une stratégie gagnante.*

Si $\mathfrak{A}$ a une stratégie gagnante, elle permet de construire une formule de logique ψ de hauteur de quantificateurs le nombre de coups du jeu telle que $u \models \psi$ mais $v \not\models \psi$. D'autre part, il est clair que si $\mathfrak{B}$ (resp. $\mathfrak{A}$) a une stratégie gagnante en n coups, il en a également une en k coups pour $k \leq n$ (resp. $k \geq n$). Dans la suite, on note $u \sim_n v$ si et seulement si $\mathfrak{B}$ a une stratégie gagnante en n coups sur les mots u et v. La proposition suivante donne le lien entre la logique et les jeux, et montre en particulier que $\sim$ est une relation d'équivalence.

Proposition 4.4.9 *$u \sim_n v$ si et seulement si u et v satisfont exactement les mêmes formules de logique de hauteur de quantificateur au plus n.*

Proposition 4.4.10 *Le nombre de classes d'équivalence de $\sim_n$ pour une hauteur de quantification donnée n est fini.*

Proposition 4.4.11 *Soient A un alphabet, α un ordinal, $(u_\beta)_{\beta<\alpha}$ et $(v_\beta)_{\beta<\alpha}$ deux suites de mots de A. Si $u_\beta \sim_n v_\beta$ pour tout $\beta < \alpha$ alors $\prod_{\beta<\alpha} u_\beta \sim_n \prod_{\beta<\alpha} v_\beta$.*

Preuve S'il reste m coups à jouer et que $\mathfrak{A}$ joue sur u_β ou v_β, la stratégie de $\mathfrak{B}$ consiste à appliquer sa stratégie gagnante sur $G(u_\beta, v_\beta, m)$. ∇

Les ordinaux peuvent être vus comme des mots sur une seule lettre. La logique sur les ordinaux ne contient donc pas les prédicats $R_a(x)$. Par exemple, l'ordinal ω peut être identifié au mot a^ω. Les résultats qui suivent sont des classiques de la théorie des jeux sur les ordinaux.

Proposition 4.4.12 *Soit n un entier. Pour tout $k \geq 2^n - 1$ on a $k \sim_n k+1$.*

Pour une preuve nous renvoyons à [Str94], page 45. On renvoie à [Ros82] pour la preuve de la proposition suivante :

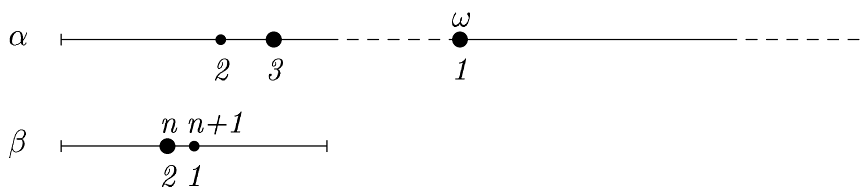
Proposition 4.4.13 *Soit n un entier. Si $\alpha < \omega^{n+1} < \beta$, alors*

1. $\alpha \not\sim_{2n+2} \omega^{n+1}$
2. $\alpha \not\sim_{2n+3} \beta$

En particulier, si $\gamma \neq \omega^{n+1}$ alors $\gamma \not\sim_{2n+3} \omega^{n+1}$.

Proposition 4.4.14 *Soient n un entier, α et β deux ordinaux tels que $\alpha < \omega^{n+1} \leq \beta$. Alors $\alpha \not\sim_{2n+3} \beta$.*

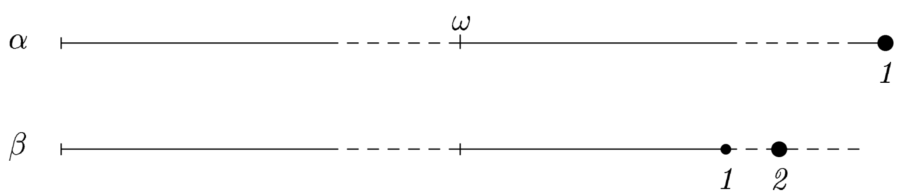
Exemple 4.4.15 *Soit $\alpha = a_0 a_1 \ldots a_\omega \ldots$ un ordinal tel que $\alpha > \omega$ et $\beta = a_0 a_1 \ldots a_{\beta-1}$ tel que $\beta < \omega$. On montre que $\mathfrak{A}$ a une stratégie gagnante en 3 coups en mettant en évidence le point limite. Il joue d'abord sur α au point limite a_ω. $\mathfrak{B}$ répond sur β n'importe où (a_γ), mais pas sur la première lettre, sinon il perd au tour suivant. $\mathfrak{A}$ joue alors dans β sur $a_{\gamma-1}$, et $\mathfrak{B}$ répond sur α à une position finie a_δ. Le dernier coup de $\mathfrak{A}$ est dans $\alpha]\delta, \omega[$, et il a gagné.*



Dans la figure, les gros points sont le jeu de $\mathfrak{A}$, les petits ceux de $\mathfrak{B}$, en dessous du point on trouve le numéro du coup et au dessus éventuellement l'indice de l'élément sur lequel on joue.

Les ordinaux limite sont séparables des ordinaux successeur en 2 coups :

Exemple 4.4.16 *Soient α un ordinal successeur et β un ordinal limite. $\mathfrak{A}$ joue dans α sur $a_{\alpha-1}$. $\mathfrak{B}$ joue dans β sur a_γ. Comme $\beta \in Lim$, il existe $\gamma < \delta < \beta$. $\mathfrak{A}$ joue dans β sur a_δ et il gagne.*



4.4.2 Des langages sans étoile aux énoncés

Soient $L \in SF(A, [1, \omega^{n+1}[)$ et $u = a_0 a_1 \dots$ un mot de $A^{[1,\omega^{n+1}[}$. Nous allons prouver qu'il existe un énoncé de $FO[<]$ dont u est un modèle si et seulement si u est un mot de L. La méthode utilisée est classique. On commence par construire par induction sur les règles de construction du langage sans étoile L une formule ϕ_L de $FO[<]$ qui possède exactement deux variables libres x et y et telle que

$$(a_0, \emptyset) \dots (a_\alpha, \{x\}) \dots (a_\beta, \{y\}) \dots (\$, \emptyset) \models \phi_L \iff u[\alpha, \beta[\in L \tag{4.1}$$

où \$ est une lettre qui n'est pas dans A qui n'apparaît qu'à la fin du mot marqué et $(\$, \emptyset)$ est d'indice $|u|$ dans la structure de support u de l'égalité ci-dessus. Si r est un nom de variable libre d'une formule ϕ on dénote par $\phi\{r \leftarrow s\}$ la formule ϕ dans laquelle le nom r a été remplacé par s. Pour une lettre $a \in A$ on pose

$$\phi_{\{a\}} \equiv y = x + 1 \wedge R_a(x)$$

Supposons maintenant que pour deux langages sans étoile quelconque L_1 et L_2 on puisse construire ϕ_{L_1} et ϕ_{L_2} telles que 4.1 soit vérifiée. Alors

$$\phi_{L_1 L_2} \equiv \exists r(\phi_A\{y \leftarrow r\} \wedge (\phi_B\{x \leftarrow r\}))$$

et

$$\phi_{A\cup B} \equiv \phi_A \vee \phi_B$$

Passons maintenant à la complémentation. D'après la proposition 4.4.13 il existe un énoncé du premier ordre $\phi_{\omega^{n+1}}$ tel que $\mathcal{L}(\phi_{\omega^{n+1}}) = X$ où X est l'ensemble des mots de longueur ω^{n+1} sur A. A partir de cet énoncé on peut construire une formule $\phi'_{\omega^{n+1}}$ qui possède exactement deux variables libres x et y telle que pour tout mot $v = a_0a_1\ldots$,

$$(a_0,\emptyset)\ldots(a_\alpha,\{x\})\ldots(a_\beta,\{y\})\ldots(\$,\emptyset) \models \phi'_{\omega^n} \iff v[\alpha,\beta[\models \phi_{\omega^n}$$

Il suffit de remplacer dans $\phi_{\omega^{n+1}}$ chaque occurrence de $\exists z_i\psi$, où z_i est une variable et ψ une sous-formule de $\phi_{\omega^{n+1}}$, par $\exists^y_x z_1\ \psi$ et $\forall z_i$ par $\forall^y_x z_1\ \psi$. Comme les mots de longueur inférieure à ω^{n+1} sont ceux qui ne contiennent aucun facteur de longueur ω^{n+1}

$$\phi_{\neg L_1} \equiv x < y \wedge (\neg\phi_{L_1}) \wedge (\neg\exists^y_x z_1\ \exists^y_x z_2\ (\phi'_{\omega^{n+1}}\{x \leftarrow z_1\}\{y \leftarrow z_2\})) \wedge \neg\phi'_{\omega^{n+1}}$$

Nous avons donc construit ϕ_L pour tout langage sans étoile L. Nous supprimons maintenant les deux variables libres x et y de ϕ_L. On pose $\phi'_L \equiv \exists z[(\forall x\ z \leq x) \wedge (\phi_L\{x \leftarrow z\})]$, où z est un nom de variable qui n'apparaît pas dans ϕ_L. La seule variable libre de ϕ'_E est y. On peut facilement montrer par récurrence que ϕ'_L ne contient aucune sous-formule de la forme $R_a(y)$, où a est une lettre de l'alphabet. Soit ϕ''_E l'énoncé obtenu à partir de ϕ'_E en substituant les sous-formules de la forme $r < y$ par $r = r$, et $y < r$ par $r \neq r$, où r est n'importe quelle variable de ϕ'_E. On a alors

$$u \in E \iff u \models \phi''_E$$

4.4.3 Des énoncés aux ω^n-semigroupes apériodiques

Nous avons donné dans la section 4.3 un algorithme qui permet de passer d'une formule de logique du second ordre à un D-automate qui reconnaît exactement les mêmes mots de longueur dénombrable, dans le chapitre 2 une construction pour obtenir un n-automate qui reconnaît exactement les mêmes mots de longueur inférieure à ω^{n+1} que ce D-automate et dans le chapitre 3 un algorithme pour construire un ω^n-semigroupe fini qui reconnaît le même langage que le n-automate.

Nous pouvons remontrer ce résultat pour le cas particulier des formules de logique du premier ordre en utilisant simplement la proposition 4.4.11, qui montre que la relation d'équivalence $\sim_m$ est une congruence d'ω^n-semigroupes, la proposition 4.4.10 qui montre que $A^{[1,\omega^{n+1}[}/\sim_m$ est fini et la proposition 4.4.9 qui montre que $A^{[1,\omega^{n+1}[}/\sim_m$ reconnaît $\mathcal{L}^{[1,\omega^{n+1}[}(\phi)$ pour une formule ϕ de hauteur de quantificateur au plus m.

Il reste à montrer que, si ϕ est un énoncé du premier ordre, $S(\mathcal{L}^{[1,\omega^{n+1}[}(\phi))$ est apériodique. Or $A^{[1,\omega^{n+1}[}/\sim_m$ l'est quel que soit m d'après la proposition 4.4.12. En particulier, $A^{[1,\omega^{n+1}[}/\sim_{hq(\phi)}$ l'est et comme il reconnaît $\mathcal{L}^{[1,\omega^{n+1}[}(\phi)$ d'après la proposition 4.4.3 $S(\mathcal{L}^{[1,\omega^{n+1}[}(\phi))$ l'est aussi.

4.4.4 Des énoncés aux langages sans étoile

Soient ϕ un énoncé, n un entier et A un alphabet. Nous allons montrer en nous appuyant sur les jeux que $\mathcal{L}^{[1,\omega^{n+1}[}(\phi) \in SF(A, [1, \omega^{n+1}[)$. Outre sa simplicité, l'intérêt de cette preuve est qu'elle fournit en particulier des arguments pour montrer que les langages de mots définis par des énoncés du premier ordre sont dans le plus petit ensemble qui contient $\{a\}$ pour chaque lettre $a \in A$ fermé par les opérations booléennes et le produit de concaténation en nombre fini, et ceci indépendamment de la longueur des mots considérés. Cependant, la construction n'est effective que si on se restreint aux mots de longueur dénombrable.

Soient ϕ un énoncé, n un entier et A un alphabet. D'après la proposition 4.4.9, l'ensemble des mots $u \in A^{[1,\omega^{n+1}[}$ tels que $u \models \phi$ est union de classes d'équivalence pour $\sim_m$ avec $m \geq hq(\phi)$. Cette union est finie car le nombre de telles classes d'équivalence est fini d'après la proposition 4.4.10. Nous allons maintenant prouver que chaque classe d'équivalence pour les jeux en m coups sont obtenables par combinaisons booléennes et produit de concaténation en nombre fini à partir des classes d'équivalence pour les jeux en $m-1$ coups. Ceci montre que $\mathcal{L}^{[1,\omega^{n+1}[}(\phi) \in SF(A, [1, \omega^{n+1}[)$.

La proposition suivante est issue d'une communication personnelle de Ladner. Elle montre en particulier que les ensembles de mots infinis définissables par des formules du premier ordre sont sans étoile, ce qu'il manquait à [Lad77] et qu'il a découvert peu après sa publication, indépendamment de [Tho79].

Si u est un mot sur A alors $< u >_n$ dénote la classe d'équivalence de u pour les jeux d'Ehrenfeucht-Fraïssé en n coups.

Proposition 4.4.17 *Soient m, n deux entiers et x un mot tel que $0 < |x| < \omega^m$. Alors*

$$< x >_n = \Big(\bigcap_{(u,a,v)\in P} < u >_{n-1} a < v >_{n-1} \Big) - \Big(\bigcup_{(u,a,v)\in Q} < u >_{n-1} a < v >_{n-1} \Big)$$

où $P = \{(u, a, v) \in A^{<\omega^m} \times A \times A^{<\omega^m} : uav = x\}$ et $Q = \{(u, a, v) \in A^{<\omega^m} \times A \times A^{<\omega^m}$ tels que pour toute factorisation $x = u'a'v'$ alors $u \not\sim_{n-1} u'$ ou $a \neq a'$ ou $v \not\sim_{n-1} v'\}$.

Lemme 4.4.18 *Soient x et y deux mots tels que $x \not\sim_n y$. Si x_1, x_2, y_1, y_2 sont quatre mots et a et b deux lettres déterminés par le premier tour du jeu tels que $x_1 a x_2 = x$ et $y_1 b y_2 = y$, alors $x_1 \not\sim_{n-1} y_1$ ou $x_2 \not\sim_{n-1} y_2$ ou $a \neq b$.*

Preuve On note x^i et y^i l'indice des lettres jouées sur x et y au tour i. Dans sa stratégie gagnante, $\mathfrak{A}$ joue son premier coup, $\mathfrak{B}$ répond, définissant ainsi les factorisations de x et de y du lemme. Si $\mathfrak{B}$ n'a pas put répondre sur la même lettre que $\mathfrak{A}$, on a $a \neq b$. Supposons que ça ne soit pas le cas. Comme $\mathfrak{A}$ gagne, il existe des entiers $i, j \leq n$ tels qu'une des deux conditions suivantes soit vérifiée :

1. $R_c(x^i)$, $R_d(y^i)$ et $c \neq d$
2. $x^i < x^j$ et non $y^i < y^j$

Comme jouer deux fois à la même position n'avance pas le jeu de $\mathfrak{A}$, puisque $\mathfrak{B}$ peut toujours faire la même chose, on peut supposer que tout ses coups sont distincts. Regardons le cas 1, et supposons que $\mathfrak{A}$ ait joué à gauche du premier coup au coup i (la droite est similaire). Comme $\mathfrak{B}$ n'a pas trouvé une bonne lettre à gauche aussi, et puisque les coups joués à droite du premier coup ne servent pas à la stratégie gagnante de $\mathfrak{A}$, il possède une stratégie gagnante sur les facteurs $x[0, x^1[$ et $y[0, y^1[$ en $n-1$ coups. Le cas 2 est similaire. ∇

Voici la preuve de la proposition :
Preuve Soit $y \in < x >_n$. On commence par montrer que pour toute factorisation $x = uav$, où u, v sont des mots et a une lettre, alors il existe deux mots u' et v' tels que $y = u'av'$ avec $u' \sim_{n-1} u$ et $v' \sim_{n-1} v$. Supposons que ce soit faux, c'est-à-dire que pour tout u', v' on ait $u' \not\sim_{n-1} u$ ou $v' \not\sim_{n-1} v$. Dans ce cas, $\mathfrak{A}$ a une stratégie gagnante sur les mots x et y en n coups : il joue a sur x, $\mathfrak{B}$ répond n'importe où sur y. S'il n'arrive pas à trouver la lettre a, il a perdu en un coup. Sinon, il a choisi une factorisation $u'av'$ de y, et comme $u' \not\sim_{n-1} u$ ou $v' \not\sim_{n-1} v$ $\mathfrak{A}$ n'a plus qu'a appliquer sa stratégie gagnante en $n-1$ coups soit à gauche soit à droite du premier coup. Montrons maintenant qu'il n'existe pas u, a et v tels que pour toute factorisation $x = u'av'$ on ait $y \in < u >_{n-1} a < v >_{n-1}$ et $u \not\sim_{n-1} u'$ ou $v \not\sim_{n-1} v'$ ou $a \neq a'$. Supposons que u, a et v existent, et posons $uav = z$. La stratégie gagnante de $\mathfrak{A}$ consiste à jouer sur a dans y, choisissant ainsi une factorisation $y = u''av''$. $\mathfrak{B}$ répond dans x et détermine ainsi une factorisation $x = u'a'v'$. Si $a' \neq a$, $\mathfrak{A}$ a gagné en un seul coup. Sinon, comme $u'' \sim_{n-1} u \not\sim_{n-1} u'$ ou $v'' \sim_{n-1} v \not\sim_{n-1} v'$, $\mathfrak{A}$ applique sa stratégie gagnante soit sur les u, soit sur les v. Nous avons obtenu la contradiction $x \not\sim_n y$.

Soit maintenant un mot y appartenant au membre droit de l'égalité de la proposition. On montre que $\mathfrak{B}$ gagne le jeu $G(x, y, n)$. Supposons que ça ne soit pas le cas, c'est-à-dire que $x \not\sim_n y$. $\mathfrak{A}$ joue le premier coup de sa stratégie gagnante, $\mathfrak{B}$ répond. Si $\mathfrak{A}$ a joué sur x, il a déterminé une factorisation de $x = uav$ telle qu'il gagne pour toute factorisation de $y = u'a'v'$ déterminée par le premier coup de $\mathfrak{B}$. Si $a \neq a'$, $\mathfrak{A}$ a gagné en un coup. Sinon, en utilisant le lemme précédent, soit $u \not\sim_{n-1} u'$ soit $v \not\sim_{n-1} v'$, c'est-à-dire, il n'existe pas de factorisation $y = u'a'v'$ telle que $u \sim_{n-1} u'$ et $v \sim_{n-1} v'$ et $a = a'$, ce qui implique que y n'appartient pas à l'intersection du membre droit, contradiction. Si $\mathfrak{A}$ a joué sur y, il en a déterminé une factorisation telle que pour toute factorisation de $x = u'a'v'$ déterminée par le premier coup de $\mathfrak{B}$ on ait soit $a \neq a'$ ou $u \not\sim_{n-1} u'$ ou $v \not\sim_{n-1} v'$, et donc y est dans l'union du membre droit, ce qui contredit aussi le fait que y soit dans le membre droit de l'égalité. ∇

4.4.5 Des ω^n-semigroupes apériodiques aux langages sans étoile

Soient A un alphabet, n un entier, S un ω^n-semigroupe fini apériodique et $\varphi : A^{[1,\omega^{n+1}[} \to S$ un morphisme d'ω^n-semigroupes qui reconnaît une partie L de $A^{[1,\omega^{n+1}[}$. Nous montrons dans cette section que L est sans étoile.

Avant de commencer nous montrons trois résultats sur les ω^n-semigroupes intéressants par eux-mêmes :

Proposition 4.4.19 *Soient A un alphabet, n un entier, S un ω^n-semigroupe fini et $\varphi : A^{[1,\omega^{n+1}[} \to S$ un morphisme d'ω^n-semigroupes. Si $0 < i \leq n$ alors pour tout $m \in S_i$,*

$$\varphi^{-1}(m) \cap A^{\omega^i} = \bigcup_{(s,e)\in P} \varphi^{-1}(s)\varphi^{-1}(e)^\omega$$

avec $P = \{(s,e) \in S_{i-1} \times S_{i-1} \ : \ se = s, \ e^2 = e \ and \ se^\omega = m\}$.

Preuve D'abord soit $u \in \varphi^{-1}(s)\varphi^{-1}(e)^\omega$ tel que $(s,e) \in P$. u s'écrit $u = \prod_{i<\omega} u_i$ avec $\varphi(u_0) = s$ et $\varphi(u_j) = e$ pour tout entier j positif. Comme $\omega^{i-1} \leq |u_j| < \omega^i$ pour tout j on a $|u| = \omega^i$. L'inclusion de la droite vers la gauche en découle puisque $\varphi(u) = se^\omega = m$. Passons à la réciproque. Supposons que $u \in \varphi^{-1}(m) \cap A^{\omega^i}$. D'après le théorème 3.3.7, il existe une suite $(u_i)_{i<\omega}$ de mots sur A et un couple lié (s,e) de S tels que $u = \prod_{i<\omega} u_i$ avec $\varphi(u_0) = s$ et $\varphi(u_j) = e$ pour tout entier j positif. On peut choisir u_j de telle façon que $\omega^{i-1} \leq |u_j| < \omega^i$ pour tout entier j. Donc u est aussi dans le membre droit de l'égalité. ∇

Si X et Y sont des ensembles de mots on dénote par $\overrightarrow{X \cdot Y}$ l'ensemble des mots u vérifiant : pour tout $0 < \alpha < |u|$ il existe $\alpha \leq \beta < |u|$ et $\beta < \gamma < |u|$ tels que $u[0,\beta[\in X$ et $u[\beta,\gamma[\in Y$.

Proposition 4.4.20 *Soient A un alphabet, n un entier, S un ω^n-semigroupe fini, (s,e) un couple lié de S et $\varphi : A^{[1,\omega^{n+1}[} \to S$ un morphisme d'ω^n-semigroupes. Alors*

$$\varphi^{-1}(s)\varphi^{-1}(e)^\omega \subseteq \overrightarrow{\varphi^{-1}(s) \cdot \varphi^{-1}(e)} \subseteq \bigcup_{f\in P_{s,e}} \varphi^{-1}(s)\varphi^{-1}(f)^\omega$$

où $P_{s,e} = \{f \in S_i \ : \ sf = s, \ ef = f \ \ et \ f^2 = f\}$.

Preuve L'inclusion de gauche est immédiate. Passons à celle de droite. Supposons que $u \in \overrightarrow{\varphi^{-1}(s) \cdot \varphi^{-1}(e)}$. Soit $(x_jy_j)_{j<\omega}$ une suite de préfixes de u telle que $x_j \in \varphi^{-1}(s)$, $y_j \in \varphi^{-1}(e)$, $|x_j| > |x_{j-1}y_{j-1}|$ pour tout entier j positif et telle que $(|x_jy_j|)_{j<\omega}$ soit cofinale avec $|u|$. Soit aussi $(z_j)_{j<\omega}$ la suite de mots définie par $x_{j+1} = x_jz_j$ pour tout entier j. Le corollaire 3.3.8 montre que u, qui est égal à $x_0\prod_{j<\omega} z_j$ s'écrit $u = (x_0z_0\ldots z_{n_0-1})\prod_{j<\omega}(z_{n_j}\ldots z_{n_{j+1}-1})$ pour une certaine suite strictement croissante d'entiers $(n_j)_{j<\omega}$ et de telle manière que $\varphi(x_0z_0\ldots z_{n_0-1}) = r$ et $\varphi(z_{n_j}\ldots z_{n_j-1}) = f$ pour un couple lié (r,f) de S_i. Comme $\varphi(x_0z_0\ldots z_{n_0-1}) = \varphi(x_{n_0})$ on a $r = s$. Comme d'autre part $\varphi(z_{n_0}\ldots z_{n_1-1}) = f$, y_{n_0} est préfixe de $z_{n_0}\ldots z_{n_1-1}$ et que $\varphi(y_{n_0}) = e$ il vient $f = eg$ pour $g \in \cup_{0\leq j\leq i}S_j$, donc $ef = eeg = eg = f$, ce qui prouve l'inclusion de droite. ∇

Corollaire 4.4.21 $\varphi^{-1}(e)^\omega = \overrightarrow{\varphi^{-1}(e) \cdot \varphi^{-1}(e)}$

Preuve Il suffit de se servir de la proposition précédente en posant $s = e$. Comme $ef = e$ et $ef = f$ alors $e = f$. ∇

Nous aurons également besoin des deux petites propositions suivantes :

Proposition 4.4.22 *Soient p, q et r trois éléments d'un semigroupe S apériodique. Si $p = qpr$ alors $p = qp = pr$.*

Preuve Si S est apériodique il existe un entier m tel que $q^m = q^{m+1}$, donc $p = qpr = q^m pr^m = q^{m+1}pr^m = qp$. La preuve que si $p = qpr$ alors $p = pr$ est similaire. ∇

Proposition 4.4.23 *Soit p un élément d'un semigroupe S apériodique. Alors $p = pS^1 \cap S^1p - \{r : p \notin S^1rS^1\}$.*

Preuve Clairement p est dans le membre droit de l'égalité. Soit maintenant n dans le membre droit de l'égalité. Il existe x, y, r et s dans S^1 tel que $n = px = yp$ et $p = rns$. Donc $n = rnsx$ et et donc $n = rn$ d'après la proposition 4.4.22. On prouve que $n = ns$ en utilisant le même argument. Donc $n = rns = p$. ∇

Nous retournons maintenant à la preuve du résultat principal de cette section : Posons $P = \varphi(L) = \{p_1, \ldots, p_k\}$. Comme $L = \varphi^{-1}(P) = \cup_{i=1\ldots k}\varphi^{-1}(p_k)$ et que $SF(A, [1, \omega^{n+1}[)$ est fermée par union finie il suffit de montrer que $\varphi^{-1}(p_i) \in SF(A, [1, \omega^{n+1}[)$ pour n'importe quel $i \in 1 \ldots k$. Nous pouvons donc supposer que P ne contient qu'un élément p, et que $ty(p) = i$ pour $i \in 0 \ldots n$. Nous prouvons le résultat par induction sur i. Si $i = 0$ le résultat vient directement de la théorie des mots finis. Supposons le résultat vrai pour i inférieur à n, et montrons-le pour $i + 1$.

Lemme 4.4.24 *Si $m \in S_{i+1}$ alors $\varphi^{-1}(m) \cap A^{\omega^{i+1}} \in SF(A, [1, \omega^{n+1}[)$.*

Preuve D'après la proposition 4.4.19,

$$\varphi^{-1}(m) \cap A^{\omega^{i+1}} = \bigcup_{(s,e)\in P} \varphi^{-1}(s)\varphi^{-1}(e)^{\omega}$$

avec $P = \{(s, e) \in S_i \times S_i \ : se = s, \ e^2 = e \text{ et } se^{\omega} = m\}$. L'utilisation du corollaire 4.4.21 donne

$$\varphi^{-1}(m) \cap A^{\omega^{i+1}} = \bigcup_{(s,e)\in P} \varphi^{-1}(s)\overrightarrow{\varphi^{-1}(e) \cdot \varphi^{-1}(e)}$$

Par hypothèse de récurrence, $\varphi^{-1}(s)$ et $\varphi^{-1}(e)$ sont tout deux dans $SF(A, [1, \omega^{i+1}[)$, et d'après les résultats de la sous-section 4.4.2 équivalent à deux formules du premier ordre ϕ_s et ϕ_e qui ont exactement deux variables libres x et y telles que (ce qui suit est également valable pour ϕ_e) :

$$(a_0, \emptyset) \ldots (a_{\alpha}, \{x\}) \ldots (a_{\beta}, \{y\}) \ldots (\$, \emptyset) \models \phi_s \iff u[\alpha, \beta[\in \varphi^{-1}(s)$$

où \$ est une lettre qui n'est pas dans A qui n'apparaît qu'à la fin du mot marqué et $(\$, \emptyset)$ est d'indice $|u|$ dans la structure de support u de l'égalité ci-dessus, et $u = \prod_{\alpha<|u|} a_{\alpha}$. La formule

$$\phi \equiv \forall r \ x < r \rightarrow \exists l \ \exists f \ r \leq l \wedge l < f \wedge \phi_e\{y \leftarrow l\} \wedge (\phi_e\{x \leftarrow l\}\{y \leftarrow f\})$$

n'a plus qu'une variable libre x, et vérifie $(a_0, \emptyset)\dots(a_\alpha, \{x\})\cdots \models \phi$ si et seulement si $u[\alpha, |u|[\in \overrightarrow{\varphi^{-1}(e)\cdot\varphi^{-1}(e)}$ si $u = \prod_{\alpha<|u|} a_\alpha$. En utilisant les arguments de la sous-section 4.4.2 on peut construire un énoncé ϕ_m tel que pour tout mot $u \in A^{[1,\omega^{n+1}[}$, $u \models \phi_m$ si et seulement si $u \in \varphi^{-1}(m) \cap A^{\omega^{i+1}}$. D'après les résultats de la sous-section 4.4.4 $\mathcal{L}^{[1,\omega^{n+1}[}(\phi_m) \in SF(A, [1, \omega^{n+1}[)$. ∇

Le reste de la preuve s'obtient en adaptant la preuve du théorème 3.1.5 de [Per90]. Nous introduisons une nouvelle notation : si $s \in S_j$ on dénote $\varphi^{-1}(s) \cap A^{\omega^j}$ par $\overline{\varphi^{-1}(s)}$. Si S ne possède pas d'élément neutre on en ajoute un qu'on note 1. Remarquons que cet ajout ne modifie en rien l'apériodicité de S, ni $\varphi^{-1}(s)$ pour aucun $s \in S$. Supposons maintenant que $p \in S_{i+1}$. Nous commençons par montrer que

$$\varphi^{-1}(p) = (UA^{\omega^{<n+1}} \cap A^{\omega^{<n+1}}V) - (A^{\omega^{<n+1}}WA^{\omega^{<n+1}}) \tag{4.2}$$

où

$$U = \Big(\bigcup_{\substack{s\in S\\ s\mathcal{R}p}} \overline{\varphi^{-1}(s)}\Big) \cup \Big(\bigcup_{\substack{r,s\in S\\ rs\mathcal{R}p\\ p\not\mathcal{R}r}} \varphi^{-1}(r)\overline{\varphi^{-1}(s)}\Big)$$

$$V = \Big(\bigcup_{\substack{s\in S\\ s\mathcal{L}p}} \overline{\varphi^{-1}(s)}\Big) \cup \Big(\bigcup_{\substack{r,s\in S\\ sr\mathcal{L}p\\ p\not\mathcal{L}r}} \overline{\varphi^{-1}(s)}\varphi^{-1}(r)\Big)$$

et

$$W = \Big(\bigcup_{\substack{s\in S\\ ty(s)\leq ty(p)\\ p\not\leq_{\mathcal{J}} s}} \overline{\varphi^{-1}(s)}\Big) \cup \Big(\bigcup_{ty(p)<j\leq n} A^{\omega^j}\Big)$$
$$\cup \Big(\bigcup_{\substack{s,t\in S\\ p\leq_{\mathcal{J}} s\\ p\leq_{\mathcal{J}} t\\ p\not\leq_{\mathcal{J}} st}} \overline{\varphi^{-1}(s)\varphi^{-1}(t)}\Big) \cup \Big(\bigcup_{\substack{r,s,t\in S\\ p\leq_{\mathcal{J}} rs\\ p\leq_{\mathcal{J}} st\\ p\not\leq_{\mathcal{J}} rst}} \overline{\varphi^{-1}(r)}\varphi^{-1}(s)\overline{\varphi^{-1}(t)}\Big)$$

et nous montrons ensuite que $\varphi^{-1}(p) \in SF(A, [1, \omega^{n+1}[)$ en prouvant que $U, V, W \in SF(A, [1, \omega^{n+1}[)$ par induction sur la structure en $\mathcal{D}$-classes de S. Le résultat final vient alors de la fermeture de $SF(A, [1, \omega^{n+1}[)$ par opérations booléennes et produit de concaténation en nombre fini.

Commençons par montrer l'inclusion de la gauche vers la droite de l'égalité 4.2. Soient $x \in \varphi^{-1}(p)$ et w un facteur gauche de x tel que $\varphi(w) \leq_{\mathcal{R}} p$ et tel qu'il n'existe pas de facteur gauche w' de x tel que $\varphi(w') \leq_{\mathcal{R}} p$ et $|w'| < |w|$. Si $|w| = \omega^m$ pour un entier m alors $w \in \overline{\varphi^{-1}(\varphi(w))}$ et $\varphi(w)\ \mathcal{R}\ p$, donc $w \in U$, et $x \in UA^{<\omega^{n+1}}$. Ecrivons sinon $|w|$ en forme normale de Cantor : $|w| = \omega^{m_1}\cdot n_1 + \omega^{m_2}\cdot n_2 + \cdots + \omega^{m_k}\cdot n_k$ et écrivons w en yz tels que $|z| = \omega^{m_k}$. Comme $|y| < |w|$ on a $\varphi(y) \not\leq_{\mathcal{R}} p$, donc $x \in UA^{<\omega^{n+1}}$. La preuve que $x \in A^{<\omega^{n+1}}V$ est similaire, mais cette fois-ci on impose que la longueur de y (plutôt que celle de z) soit ω^{m_1} (plutôt que ω^{m_k}). Si $x \in A^{<\omega^{n+1}}WA^{<\omega^{n+1}}$ on ne peut pas avoir

$\varphi(x) = p$, ce qui termine la preuve de l'inclusion du membre gauche de l'égalité 4.2 dans celui de droite.

Soit maintenant x un mot du membre droit de cette égalité. Comme $x \in UA^{<\omega^{n+1}}$ et $\varphi(U) \leq_{\mathcal{R}} p$ alors $\varphi(x) \leq_{\mathcal{R}} p$. On montre de façon similaire que $\varphi(x) \leq_{\mathcal{L}} p$. D'après la proposition 4.4.23 il reste à montrer que $p \leq_{\mathcal{J}} \varphi(x)$ pour prouver l'inclusion. Supposons que ce soit faux et soit w un facteur de x tel que $p \not\leq_{\mathcal{J}} \varphi(w)$ et il n'existe pas d'autre facteur w' de x qui vérifie $|w'| < |w|$ et $p \not\leq_{\mathcal{J}} \varphi(w')$. Si $|w| = \omega^m$ pour un entier m alors $w \in \overline{\varphi^{-1}(\varphi(w))}$ et comme $p \not\leq_{\mathcal{J}} \varphi(w)$ il vient $w \in W$, ce qui est une contradiction. Sinon écrivons $|w|$ en forme normale de Cantor : $|w| = \omega^{m_1} \cdot n_1 + \omega^{m_2} \cdot n_2 + \cdots + \omega^{m_k} \cdot n_k$ et factorisons w en $w_1w_2w_3$, avec $|w_1| = \omega^{m_1}$, $|w_3| = \omega^{m_k}$ et w_2 éventuellement vide. Si w_2 n'est pas le mot vide alors $w \in \overline{\varphi^{-1}(\varphi(w_1))}\varphi^{-1}(w_2)\overline{\varphi^{-1}(\varphi(w_3))}$, $p \not\leq_{\mathcal{J}} \varphi(w_1)\varphi(w_2)\varphi(w_3)$, mais $p \leq_{\mathcal{J}} \varphi(w_1)\varphi(w_2)$ et $p \leq_{\mathcal{J}} \varphi(w_2)\varphi(w_3)$, donc $w \in W$. On obtient la même contradiction si w_2 est le mot vide. Ceci termine la preuve de l'égalité 4.2.

Il reste à prouver que $\varphi^{-1}(p) \in SF(A, [1, \omega^{n+1}[)$. Nous procédons par induction sur la structure en $\mathcal{D}$-classes de S. Observons d'abord que $x \leq_{\mathcal{J}} 1$ pour tout $x \in S$. Comme S est apériodique, en utilisant la proposition 4.4.22, si $1 \leq_{\mathcal{J}} y$ alors $1 = xyz = xy1z = 1z = z = x1y = x = y$, donc si $x \neq 1$ alors $x \not\mathcal{D}\, 1$. En utilisant le même genre d'argument, et comme $1 \in S_0$, il vient

$$\varphi^{-1}(1) = A^+ - A^*(\bigcup_{\substack{a \in A \\ \varphi(a) \neq 1}} a)A^*$$

qui appartient à $SF(A, [1, \omega^{n+1}[)$. Supposons que $p \neq 1$. On commence par montrer que $U \in SF(A, [1, \omega^{n+1}[)$ en utilisant l'hypothèse de récurrence, qui est que si $p \leq_{\mathcal{J}} r$ et $p \not\mathcal{D}\, r$ alors $\varphi^{-1}(r) \in SF(A, [1, \omega^{n+1}[)$. Le lemme 4.4.24 montre que $\overline{\varphi^{-1}(s)} \in SF(A, [1, \omega^{n+1}[)$ pour tout $s \in S$ tel que $ty(s) \leq ty(p)$. La proposition 4.4.13, en conjonction avec le résultat de la sous-section 4.4.4, prouve que $A^{\omega^j} \in SF(A, [1, \omega^{n+1}[)$ quel que soit j. D'autre part, si $s \,\mathcal{R}\, p$, $s \,\mathcal{L}\, p$ ou $rs \,\mathcal{R}\, p$ on peut aisément vérifier que $ty(s) \leq ty(p)$. Soient maintenant r et s tels que $rs \,\mathcal{R}\, p$ et $r \not\mathcal{R}\, p$. Il existe $x \in S$ tel que $p = rsx$, donc $p \leq_{\mathcal{J}} r$ et $p \leq_{\mathcal{R}} r$. Si $p \,\mathcal{D}\, r$ il existe $y, z \in S$ tels que $r = ypz = y(rsx)z = pz$ d'après la proposition 4.4.22, donc $r \leq_{\mathcal{R}} p$ et donc $r \,\mathcal{R}\, p$, ce qui est une contradiction. La preuve que $V \in SF(A, [1, \omega^{n+1}[)$ est similaire. Supposons maintenant que $p \leq_{\mathcal{J}} rs$, $p \leq_{\mathcal{J}} st$ et $p \not\leq_{\mathcal{J}} rst$. Il existe $a, b, c, d \in S$ tels que $p = arsb = cstd$, donc $p \leq_{\mathcal{J}} s$. Si $p \,\mathcal{D}\, s$ alors $s = xpy$ pour $p, y \in S$, et en utilisant la proposition 4.4.22 $s = xarsby = xars$, donc $p = cxarstd$, i.e. $p \leq_{\mathcal{J}} rst$ ce qui est une contradiction, donc $W \in SF(A, [1, \omega^{n+1}[)$.

Conclusion

Nous avons présenté dans cette thèse plusieurs classes d'automates, qui diffèrent par la longueur des mots reconnus. Données deux de ces classes, et en restreignant la longueur des mots reconnus de la classe d'automates qui reconnaît les mots les plus grands à celle de l'autre, les deux classes sont équivalentes.

L'algorithme de déterminisation des D-automates que nous avons exhibé donne une présentation unifiée de la partie difficile de la déterminisation pour les différentes classes d'automates qui ne reconnaissent que des mots de longueur dénombrable. En effet, les automates sur les mots finis ou de longueur ω sont des cas particuliers des automates sur les mots de longueur dénombrable, l'inclusion des langages n-rationnels dans les langages D-rationnels donne un algorithme permettant de construire un D-automate équivalent à un n-automate donné, et nous avons donné un algorithme pour construire un n-automate déterministe à partir d'un D-automate déterministe. L'algorithme de déterminisation que nous avons proposé est une adaptation de celui de McNaughton sur les mots de longueur ω. Sur ces mots, Safra [Saf88] a réduit la complexité de l'algorithme de McNaughton d'une exponentielle double de l'automate de départ à une exponentielle simple. L'algorithme de Safra devrait également être adaptable au cas des mots de longueur dénombrable.

Nous avons présenté deux structures algébriques dont chacune est équivalente à une classe d'automates particulière, et utilisé ces structures pour commencer l'extension des résultats de classification des langages de mots finis par les propriétés algébriques de leur semigroupe syntaxique aux langages de mots de longueur dénombrable. Le prolongement naturel de ce travail de thèse est de continuer l'extension de la classification des langages reconnaissables de mots finis par les propriétés de leur semigroupe syntaxique.

L'extension du théorème d'équivalence entre langages sans étoile, langages reconnus par semigroupes finis apériodiques et langages définis par énoncé de logique du premier ordre utilise des arguments qui montrent l'équivalence entre langages définis par énoncé de logique du premier ordre et langages sans étoile, et que la structure algébrique finie associée à un langage défini par énoncé de logique du premier ordre est apériodique, ceci indépendamment de la longueur des mots considérés :

$$\begin{tikzcd} & \text{algèbre finie apériodique} & \\ \text{sans étoile} \arrow[rr, leftrightarrow] & & \text{logique du premier ordre} \arrow[ul] \end{tikzcd}$$

La généralisation du théorème d'équivalence entre langages reconnus par semigroupes finis apériodiques et langages sans étoile (le sens de la gauche vers la droite) aux langages de mots de longueur inférieure à ω^{n+1} est une adaptation simple de la preuve sur les mots finis de [Per90], qui fonctionne par induction sur la structure en $\mathcal{D}$-classes du semigroupe. La simplicité de l'adaptation provient du fait que les ω^n-semigroupes sont des algèbres graduées de telle façon que l'opérateur ω fait descendre dans les $\mathcal{D}$-classes. Ceci n'est plus vrai dans un ω_1-semigroupe : on peut avoir $s \mathcal{D} s^\omega$. La question “les langages reconnus par ω_1-semigroupes finis apériodiques sont-ils sans étoile ?” reste ouverte.

La logique temporelle introduite par Pnueli [Pnu77] en 1977 est utilisée pour décrire les propriétés des processus, notamment en parallélisme. Il s'agit d'une logique sans quantificateurs, où les seules formules atomiques sont de la forme R_a pour chaque lettre a de l'alphabet, et les formules sont formées par induction à partir des connecteurs booléens habituels et d'opérateurs temporels, $\mathbf{N}$, $\Diamond$ et $\mathbb{U}$, de la manière suivante : si φ et ψ sont deux formules de logique temporelle, alors $\varphi \vee \psi$, $\neg\varphi$, $\mathbf{N}\varphi$, $\Diamond\varphi$ et $\varphi\mathbb{U}\psi$ le sont aussi. Les modèles de cette logique sont des mots sur un alphabet fini. Les indices des lettres du mot représentent le temps. La sémantique est définie de la façon suivante :

- $u \models R_a$ si la première lettre de u est un a,
- $u \models \varphi \vee \psi$ si $u \models \varphi$ ou $u \models \psi$,
- $u \models \neg\varphi$ si $u \not\models \varphi$,
- $u \models \mathbf{N}\varphi$ si $u[1, |u|[\models \varphi$,
- $u \models \Diamond\varphi$ s'il existe $\beta < |u|$ tel que $u[\beta, |u|[\models \varphi$,
- $u \models \varphi\mathbb{U}\psi$ s'il existe $\beta < |u|$ tel que $u[\beta, |u|[\models \psi$ et $u[\alpha, |u|[\models \varphi$ pour tout $\alpha < \beta$.

Il existe de nombreuses preuves de l'équivalence entre cette logique et celle du premier ordre de l'ordre linéaire quand on s'intéresse aux mots dont la longueur ne dépasse pas ω [Kam68, GPSS80, CPP93, CC91]. Rohde a montré récemment [Roh97] que la logique temporelle est strictement incluse dans la logique du premier ordre de l'ordre linéaire dès qu'on considère des modèles de longueur supérieure à ω. L'idée générale de cette non-équivalence est qu'on ne peut spécifier en logique temporelle que l'indice d'une lettre d'un mot est un ordinal limite (les ordinaux limite étant ceux qui sont non nul et non successeur, la propriété “être limite” dépend du passé, or en logique temporelle on ne considère que le futur), mais cette propriété s'exprime facilement en logique du premier ordre de l'ordre linéaire, et même du successeur. Par exemple, le langage $L = (ab)^{<\omega_1} - \lambda$ sur l'alphabet $\{a, b\}$ n'est pas exprimable en logique temporelle, mais est défini par l'énoncé de logique du premier ordre de l'exemple 4.1.4 page 114. Son ω_1-semigroupe syntaxique, donné dans l'exemple 3.5.10 page 83, est donc apériodique. Carton a montré que l'ω_1-semigroupe syntaxique d'un langage de logique temporelle vérifie l'équation $s^\omega s^\pi = s^\pi$, mais on ne sait pas encore caractériser les langages de logique temporelle par les propriétés de leur ω_1-semigroupe syntaxique.

Bibliographie

[ACM80] *Conference Record of the Seventh Annual ACM Symposium on Principles of Programming Languages*, Las Vegas, Nevada, january 1980.

[Alm94] Jorge Almeida. *Finite semigroups and universal algebra*, volume 3 of *Series in algebra*. World Scientific, 1994.

[Arn85] André Arnold. A syntactic congruence for rational ω-languages. *Theoretical Computer Science*, 39 :333–335, 1985.

[BC98] Nicolas Bedon and Olivier Carton. An Eilenberg theorem for words on countable ordinals. In Cláudio L. Lucchesi and Arnaldo V. Moura, editors, *Latin'98 : Theoretical Informatics*, volume 1380 of *Lecture Notes in Computer Science*, pages 53–64, Campinas, Brazil, April 1998. Springer.

[Beda] Nicolas Bedon. Logic over words on denumerable ordinals. To appear.

[Bedb] Nicolas Bedon. Star-free sets of words on ordinals. IGM report 97-8, to appear in Information and Computation.

[Bed96] Nicolas Bedon. Finite automata and ordinals. *Theoretical Computer Science*, 156 :119–144, March 1996.

[Bed98a] Nicolas Bedon. Automata, semigroups and recognizability of words on ordinals. *International Journal of Algebra and Computation*, 8(1) :1–21, February 1998.

[Bed98b] Nicolas Bedon. *Langages reconnaissables de mots indexés par des ordinaux*. PhD thesis, Université de Marne-la-Vallée, Cité Descartes, 5, boulevard Descartes, Champs-sur-Marne, 77454 Marne-la-Vallée Cedex 2, France, January 1998. http ://www-igm.univ-mlv.fr/~bedon/Recherche/These/these.shtml.

[BS73] J. Richard Büchi and Dirk Siefkes. *The monadic second order theory of all countable ordinals*, volume 328 of *Lecture notes in mathematics*. Springer, 1973.

[Büc60] J. Richard Büchi. Weak second-order arithmetic and finite automata. *Zeit. Math. Logik. Grund. Math.*, 6 :66–92, 1960.

[Büc62] J. Richard Büchi. On a decision method in the restricted second-order arithmetic. In *Logic, Methodology and Philosophy of science : Proc. Intern. Congr.*, pages 1–11, Stanford, California, 1962. Stanford University Press.

[Büc64] J. Richard Büchi. Transfinite automata recursions and weak second order theory of ordinals. In *Proc. Int. Congress Logic, Methodology, and Philosophy of Science*, pages 2–23, Jerusalem, 1964. North-Holland Publ. Co. Invited address.

[Büc65] J. Richard Büchi. Decision methods in the theory of ordinals. *Bull. Am. Math. Soc.*, 71 :767–770, 1965.

[Büc90] J. Richard Büchi. *The collected works of J. R. Büchi.* Springer, 1990.

[Car93] Olivier Carton. *Mots infinis, ω-semigroupes et topologie.* PhD thesis, Université Paris 7, Paris (France), 1993.

[CC91] Joëlle Cohen-Chesnot. On the expressive power of temporal logic for infinite words. *Theoretical Computer Science*, 83(2) :301–312, 28 june 1991. Note.

[Cho74] Yaacov Choueka. Theories of automata on ω-tapes : a simplified approach. *Journal of Computer and System Sciences*, 8 :117–141, 1974.

[Cho78] Yaacov Choueka. Finite automata, definable sets, and regular expressions over ω^n-tapes. *Journal of Computer and System Sciences*, 17 :81–97, 1978.

[CPP93] Joëlle Cohen, Dominique Perrin, and Jean-Eric Pin. On the expressive power of temporal logic. *Journal of Computer and System Sciences*, 46(3) :271–294, June 1993.

[Ehr61] A. Ehrenfeucht. An application of games to the completeness problem for formalized theories. *Fund. Math.*, 49 :129–141, 1961. [MR 23, #3666].

[Eil76] Samuel Eilenberg. *Automata, languages and machines*, volume B. Academic press, 1976.

[FR79] J. Ferrante and C. W. Rackoff. *The computational complexity of logical theories*, volume 718 of *Lecture notes in mathematics.* Springer-Verlag, 1979.

[Fra54] R. Fraïssé. Sur quelques classifications des systèmes de relations. *Publications Scientifiques de l'université d'Alger*, 1(A) :35–182, 1954.

[GPSS80] Dov M. Gabbay, Amir Pnueli, Saharon Shelah, and Jonathan Stavi. On the temporal basis of fairness. In ACM [ACM80], pages 163–173.

[HU79] J. E. Hopcroft and J. D. Ullman. *Introduction to automata theory, languages, and computation.* Addison-Wesley, Reading, 1979.

[HW92] Jean-Claude Hemmer and Pierre Wolper. Ordinal finite automata and languages. Technical report, University of Liège, 1992.

[IEE77] IEEE. *18th Annual Symposium on Foundations of Computer Science*, Providence, Rhode Island, 31 october – 2 november 1977.

[IEE88] IEEE. *29th Annual Symposium on Foundations of Computer Science*, White Plains, New York, 24–26 october 1988.

[Kam64] Erich Kamke. *Théorie des ensembles.* 1964. Réédité chez Jacques Gabay.

[Kam68] J. Kamp. *Tense logic and the theory of linear order.* PhD thesis, University of California, Los Angeles, 1968.

[Kle56] Stephen C. Kleene. Representation of events in nerve nets and finite automata. In Shannon and McCarthy, editors, *Automata studies*, pages 3–42, Princeton, New Jersey, 1956. Princeton University Press.

[Kle67] Stephen C. Kleene. *Mathematical logic*. John Wiley and Sons, New York, 1967. French translation : Logique mathématique, J. Gabay eds.

[Lad77] Richard E. Ladner. Application of model theoretic games to discrete linear orders and finite automata. *Information and Control*, 33 :281–303, 1977.

[McN66] Robert McNaughton. Testing and generating infinite sequences by a finite automaton. *Information and Control*, 9 :521–530, 1966.

[Mey69] A. R. Meyer. A note on star free events. *J. Assoc. Comput. Mach.*, 16(2) :220–225, 1969.

[MP71] Robert McNaughton and Seymour Papert. *Counter free automata*. MIT Press, Cambridge, MA, 1971.

[Mul63] D. Muller. Infinite sequences and finite machines. In *Switching circuit theory and logical design : Proc. Fourth Annual Symp. IEEE*, pages 3–16, 1963.

[Péc86a] Jean-Pierre Pécuchet. Etude syntaxique des parties reconnaissables de mots infinis. *Lecture Notes in Computer Science*, 226 :294–303, 1986.

[Péc86b] Jean-Pierre Pécuchet. Variétés de semigroupes et mots infinis. *Lecture Notes in Computer Science*, 210 :180–191, 1986.

[Per84] Dominique Perrin. Recent results on automata and infinite words. In M. P. Chytil and V. Koubek, editors, *Mathematical foundations of computer science*, volume 176 of *Lecture Notes in Computer Science*, pages 134–148, Berlin, 1984. Springer.

[Per90] Dominique Perrin. *Handbook of theoretical computer science*, volume B, chapter Finite automata, pages 1–53. Elsevier, 1990.

[Pin84] Jean-Eric Pin. *Variétés de langages formels*. Masson, Paris, France, 1984. English version : Varieties of formal languages, Plenum Press, New-York, 1986.

[Pin94] Jean-Eric Pin. Logic, semigroups and automata on words. In *Mathematics and Artificial Intelligence*, 1994.

[Pin96] Jean-Eric Pin. Logic, semigroups and automata on words. *Ann. Math. Artificial Intelligence*, 16(1-4) :343–384, 1996.

[Pin97] Jean-Eric Pin. *Handbook of formal languages*, volume 1, chapter Syntactic semigroups, pages 679–746. Springer, 1997.

[Pnu77] Amir Pnueli. The temporal logic of programs. In *18th Annual Symposium on Foundations of Computer Science* [IEE77], pages 46–57.

[PP86] Dominique Perrin and Jean-Eric Pin. First order logic and star-free sets. *Journal of Computer and System Sciences*, 32 :393–406, 1986.

[PP95] Dominique Perrin and Jean-Eric Pin. Semigroups and automata on infinite words. In J. Fountain and V. A. R. Gould, editors, *NATO Advanced Study Institute : Semigroups, Formal Languages and Groups*, pages 49–72. Kluwer Academic Publishers, 1995.

[PP97] Dominique Perrin and Jean-Eric Pin. *Mots infinis (Infinite words).* 1997. To appear (LITP report 97-04), http ://www.liafa.jussieu.fr/~jep/Resumes/InfiniteWords.html. English version : "Infinite words".

[Roh97] Scott Rohde. *Alternating automata and the temporal logic of ordinals.* PhD thesis, University of Illinois, Urbana-Champaign, USA, 1997.

[Ros82] J. G. Rosenstein. *Linear ordering.* Academic Press, New York, 1982.

[RS59] M. O. Rabin and D. Scott. Finite automata and their decision problems. *IBM Journal of Research and Development*, pages 114–125, 1959.

[Saf88] Shmuel Safra. On the complexity of ω-automata. In *29th Annual Symposium on Foundations of Computer Science* [IEE88], pages 319–327.

[Sch56] Marcel-Paul Schützenberger. Une théorie algébrique du codage. In *Séminaire Dubreil-Pisot*, Paris, Février 1956. Institut Henri Pointcaré.

[Sch65] Marcel-Paul Schützenberger. On finite monoids having only trivial subgroups. *Information and Control*, 8 :190–194, 1965.

[Sie50] Waclaw Sierpiński. *Leçons sur les nombres transfinis.* Gauthier-Villars, Paris, 1950.

[Sie65] Waclaw Sierpiński. *Cardinal and ordinal numbers.* Polish Scientific Publishers, Varsovie, 1965.

[Str94] Howard Straubing. *Finite automata, formal logic and circuit complexity.* Birkhäuser, 1994.

[Tho79] Wolfgang Thomas. Star free regular sets of ω-sequences. *Information and Control*, 42 :148–156, 1979.

[Tho90] Wolfgang Thomas. *Handbook of theoretical computer science*, volume B, chapter Automata on infinite objects, pages 135–191. Elsevier, 1990.

[Wil91] Thomas Wilke. An Eilenberg theorem for ∞-languages. In *Automata, Languages and Programming : Proc. of 18th ICALP Conference*, pages 588–599. Springer, 1991.

[Wil93] Thomas Wilke. An algebraic theory for regular languages of finite and infinite words. *International Journal of Algebra and Computation*, 3(4) :447–489, 1993.

[Woj83] Jerzy Wojciechowski. The ordinals less than ω^ω are definable by finite automata. In J. Demetrovics, G. Katona, and A. Salomaa, editors, *Proc. Colloquium on "Algebra, Combinatorics and Logic in Computer Science"*, volume 2, pages 871–887, Amsterdam, 1983. North Holland.

[Woj84] Jerzy Wojciechowski. Classes of transfinite sequences accepted by finite automata. *Fundamenta informaticæ*, 7(2) :191–223, 1984.

[Woj85] Jerzy Wojciechowski. Finite automata on transfinite sequences and regular expressions. *Fundamenta informaticæ*, 8(3-4) :379–396, 1985.

Table des matières

Index des notations

Index