Université Paris Diderot - Paris 7

Laboratoire d'Informatique Algorithmique : Fondements et Applications

Thèse

présentée pour l'obtention du diplôme de

Docteur de l'Université Paris Diderot,
spécialité Informatique

à l'École doctorale de Sciences Mathématiques de Paris Centre

---

Circuits booléens, prédicats modulaires et langages réguliers

---

Par :

Charles Paperman

Soutenue publiquement le 11 décembre 2014 *devant le jury constitué de :*

Marie-Pierre Béal,	Professeur à l'université Paris-Est Marne-la-Vallée	*Examinatrice*
Alexis Bès,	Maître de conférence à l'université Paris-Est Créteil	*Examinateur*
Olivier Carton,	Professeur à l'université de Paris-Diderot	*Directeur de thèse*
Arnaud Durand,	Professeur à l'université de Paris-Diderot	*Examinateur*
Jean-Éric Pin,	Directeur de recherche au CNRS	*Directeur de thèse*
Howard Straubing,	Professor at Boston College	*Rapporteur*
Marc Zeitoun,	Professeur à l'université de Bordeaux.	*Rapporteur*

Cette thèse a été financée par la fondation CFM pour la recherche.

Remerciements

Ce manuscrit conclut trois années de recherche au LIAFA encadrées par mes deux directeurs, Jean-Éric et Olivier que je remercie énormément pour leur accompagnement, leur bienveillance et leurs connaissances. À leur contact j'ai beaucoup appris, et pas seulement en mathématiques [1].

Howard Straubing et Marc Zeitoun ont accepté d'être rapporteurs de ce manuscrit. Je leur suis extrêmement reconnaissant de s'être intéressés à mes travaux et d'avoir grandement contribué à l'amélioration de ce mémoire grâce à leurs commentaires. Je remercie également Marie-Pierre Béal, Alexis Bès et Arnaud Durand de me faire l'honneur de participer à mon jury de thèse.

J'aimerais particulièrement remercier Howard Straubing pour son accueil chaleureux lors de mon séjour au Boston College, ainsi que pour nos nombreux échanges qui ont largement contribué à améliorer ma compréhension de ce très riche domaine.

Ces trois années furent ponctuées de multiples collaborations, travaux de groupes et séminaires qui tous se déroulèrent dans une bonne humeur contagieuse et une ambiance remplie d'humour notamment dans le cadre de l'ANR FREC. Je souhaiterais en remercier tous les participants, de Bordeaux comme de Paris, et en particulier les membres de FREC junior : Sam, Lorjn, Arthur, Laure, Luc, Nathanaël et Denis. Ces quatre derniers ont directement influé le cours de ma thèse :

- Laure, ou devrais-je dire *maman*, qui pour la première fois depuis sept ans vient de m'abandonner à mon triste sort. Je suis maintenant contraint de remplir mes papiers administratifs seul, de trouver les informations sur internet comme un grand, etc... Le sevrage étant difficile, je m'excuse par avance (ou devrais-je dire : *je lui présente mes excuses*©JEP) des centaines de mails paniqués qu'elle recevra dans les mois/années qui viennent. Si je profite et abuse de ses talents administratifs, c'est avant tout ses (très) grandes qualités scientifiques, sa patience et sa gentillesse profinies que je désire saluer. Enfin je la remercie de m'avoir cédé aussi facilement le canapé de Denis qui, il faut bien l'avouer, lui revenait de droit.
- Luc, avec qui j'ai exploré aussi bien les bars de Kiel que la théorie des variétés de catégories. Il est bien plus agréable d'être deux (et en chanson) pour comprendre, étudier et rechercher, que les idées soient les plus foireuses (big-up pour strict-**MSO**) ou les plus belles.

1. je ne pense pas non plus à l'orthographe ou à la grammaire, bien qu'ils m'aient beaucoup apporté sur ce sujet.

- Nath, dont la vivacité, la curiosité et les connaissances sont une source d'admiration. Ses conseils précieux et nos longues discussions m'ont guidé à de nombreuses reprises, jusqu'à m'entraîner avec lui dans les confins de l'Europe de l'Est, où je l'espère, nous résoudrons de belles conjectures.
- Denis-senseï, qui m'a transmis son amour du Go, de la logique, des débats interminables et des belles mathématiques (pas des énigmes, ça j'en ai marre !). Nous sommes allés ensemble au Cameroun, mais ce n'est en rien comparable aux horizons mathématiques qu'il m'a fait découvrir.

J'aimerais en outre remercier l'ensemble du LIAFA, son équipe administrative, Noëlle et Nathalie, Houy et Laifa, mes co-bureaux nouveaux, Sven et Thomas (certainement pas François) et mes co-bureaux anciens, Virginie, Heger et Sam. Nos interminables discussions me manquent déjà. De nombreuses personnes ont toujours eu leur porte ouverte ; Sophie, toujours de bon conseil, m'a appris l'informatique à Orsay et m'a remonté le moral dans les moments les plus difficiles ; Thomas qui m'a littéralement illuminé (oui comme une lanterne) par ses idées brillantes ; Inès et Sylvain toujours présents pour discuter et échanger ; enfin Florian et Arthur pour leur efficace relecture de ma thèse.

Je ne serais jamais arrivé là sans la confiance inébranlable de ma famille, de mes amis, Polo, FaGa, SoMi et Hélène, Moee et toute la BGU mais aussi et surtout d'Ambre. Elle m'a soutenu moralement, écouté chacune de mes présentations, relu chacun de mes textes durant ces trois années. Elle a arpenté et corrigé ce manuscrit jusque dans les cafés amstellodamois et sur les rives du Danube. Je ne lui serais jamais assez reconnaissant pour toute l'énergie qu'elle m'a apportée, pour avoir partagé joies et peines, pour avoir vibré à l'unisson lorsque j'étais persuadé d'avoir une solution (tout théorème de moins de 24 heures est faux$^{©\text{JEP}}$).

Table des matières

Introduction

La très récente histoire de l'informatique prend sa source dans celle, tumultueuse, de la *logique*. Lorsque les fondements des mathématiques ont semblé bancals et les *ensembles* dangereux, l'introduction d'un formalisme rigide et rigoureux s'imposa. Il s'agissait alors d'en explorer les fondements.

Une simple addition, pourtant exécutée par des générations d'écoliers studieux, devint un véritable défi. Il ne suffisait plus simplement de comprendre et convaincre, il fallait également *prouver formellement*. Le premier théorème d'incomplétude [29] de Gödel mit un terme à l'espoir d'emprisonner les mathématiques dans un petit nombre de règles simples, évidentes et mécaniques. Mais de cet échec, on tira la science du calcul automatisé, réalisé par des machines *abstraites* simplement descriptibles : les *machines de Turing* [74].

L'un des résultats les plus surprenants de ce domaine est l'existence d'une frontière de *calculabilité*, c'est-à-dire, l'existence d'une limite intrinsèque à la réalisation des *calculs automatiquement*, et ce quelle que soit la complexité des machines que l'on considère. Cette limitation provient de la *finitude* de nos moyens. En effet, pour résoudre un problème à l'aide d'une machine, il lui est nécessaire d'être descriptible finiment. Cette simple réalité dresse un mur infranchissable quelle que soit la modélisation choisie pour *le calcul*. Bien comprendre comment se dessine cette limite, évaluer exactement ce qui permet à un problème d'être résolu mécaniquement et de disposer d'un *algorithme*, constitue l'un des nombreux domaines de recherche de l'informatique théorique : la *calculabilité*.

Savoir qu'un problème est calculable nous en apprend beaucoup sur sa nature mais n'est pas suffisant pour construire une solution automatique utilisable. Il est également nécessaire que la résolution du problème nécessite un *temps* et une quantité de *mémoire* raisonnables. L'étude de ces contraintes, la classification des problèmes calculables en fonction de leur difficulté, est nommée la *complexité*. Beaucoup de questions, énoncées lors de l'émergence de ce domaine, restent aujourd'hui sans réponses. Cette difficulté peut s'expliquer par leur nature : on parle de *bornes inférieures de complexité* pour un problème lorsqu'on arrive à déterminer une quantité de *ressources indispensables* à sa résolution. Établir de telles bornes pose de grandes difficultés car cela nécessite de prouver la non-existence d'algorithmes efficaces.

Afin d'étudier la notion de calcul, on emprunte au champ lexical de la linguistique et de la théorie des *langages formels*. Un *langage* modélise un problème à résoudre et un *mot* en constitue une instance. Dans cette thèse, nous nous focalisons sur l'interface de deux modèles de calcul : les *automates finis* et les *circuits booléens*. Les automates finis four-

nissent une représentation particulièrement simple d'un calcul réalisé *séquentiellement* ; ils disposent d'une mémoire finie et acceptent ou rejettent un mot après l'avoir parcouru entièrement. Les langages ainsi calculés sont dits *réguliers*. De cette simplicité, on extrait des outils algébriques, logiques et combinatoires permettant d'explorer l'expressivité de ces machines et d'obtenir des notions de *complexité algébrique*.

Les circuits booléens modélisent quant à eux un calcul *parallèle*, acceptant des mots d'une taille fixée, en utilisant des *portes* comme unité de calcul. Il n'est pas vraiment possible de parler de notion de complexité sans être capable de faire varier la taille des entrées. Afin de pallier cette limitation, on considérera des *familles de circuits* ayant pour chaque taille d'entrée un circuit différent. Sans contrainte supplémentaire, les familles de circuits ne possèdent pas de description finie ; on parle alors d'un modèle de calcul *non uniforme*. On s'intéressera principalement à deux notions de complexité : la *profondeur*, qui correspond à une complexité temporelle, et le *nombre de portes* qui correspond à une complexité spatiale ; ces deux notions constituent la *complexité booléenne.*

Tout calcul réalisé à l'aide d'un automate peut l'être également avec une famille de circuits ayant une profondeur logarithmique et un nombre linéaire de portes. Cette traduction est réalisable algorithmiquement et permet une accélération exponentielle de ce calcul, avec en contrepartie une explosion de la mémoire.

Problèmatique : Peut-on déterminer des bornes exactes de complexité booléenne pour les langages réguliers ?

De nombreux outils ont été mis en place pour tenter de répondre à cette question difficile. Le premier résultat en la matière est indéniablement les bornes inférieures de complexité obtenues pour le langage *parité* par Furst, Saxe et Sipser [28], puis généralisé aux langages modulaires par Razborov [56] et étendu à des familles de circuits utilisant des portes modulaires par Smolensky [60]. Une caractérisation algébrique des langages réguliers calculés par des circuits de profondeur bornée et de taille polynomiale ($\mathbf{AC^0}$) a été obtenue par Barrington, Compton, Straubing et Thérien [10].

La logique donne un éclairage particulier à ces résultats puisque des *fragments logiques* permettent d'obtenir des descriptions de classes de langages. Ces fragments représentent une notion de *complexité logique*, ils sont composés de *formules logiques* et équipés d'une *signature*. En fonction de la signature choisie, un même fragment peut être équivalent à une classe de langages réguliers, quand la signature est dite *régulière*, ou à une classe de complexité de circuits booléens, quand elle est dite *arbitraire*.

La *conjecture de Straubing* [66] suggère qu'un langage régulier définissable dans un fragment logique équipé d'une signature arbitraire, est en fait définissable par le même fragment logique mais équipé d'une signature régulière. Cette conjecture reformule logiquement la problématique centrale de cette thèse. Il existe une méthode *générique* permettant de prouver des instances de cette conjecture :

(1) Caractériser algébriquement le fragment logique sur la signature régulière.
(2) En déduire certains langages *témoins* caractérisant, par leur absence, la classe de langages réguliers que l'on étudie.

(3) Prouver des bornes inférieures pour ces langages témoins.

Ainsi, en appliquant cette méthode générique à la classe de circuits $\mathbf{AC^0}$, qui est équivalente à la logique du premier ordre, on reprouve le résultat de Barrington *et al.* Si le troisième point de cette méthode semble le plus difficile, il existe des situations où même le premier point semble hors d'atteinte. Par exemple, le fragment du premier ordre, équipé de *quantifications modulaires* et restreint à deux variables, semble ardu à caractériser, même équipé uniquement de l'ordre linéaire.

- Des caractérisations algébriques décidables d'un certain nombre de fragments équipés de *prédicats réguliers* seront présentées dans de ce manuscrit. Elles sont conséquences de l'étude systématique de l'ajout des *prédicats descriptifs locaux* et des *prédicats réguliers* exspola première partie . Entre autres, on obtiendra une caractérisation algébrique décidable des fragments $\mathbf{FO}^2[<, \mathrm{MOD}]$ et $\mathbf{FO}^2[\mathcal{R}\mathrm{eg}]$ ainsi que de leur hiérarchie d'alternance de quantifications.
- On proposera également une caractérisation algébrique et logique décidable des langages réguliers calculables par des circuits de $\mathbf{AC^0}$ disposant d'un nombre d'arêtes linéaires.
- On prouvera la conjecture de Straubing pour le fragment $\mathbf{FO}^2$ équipée de l'ordre linéaire et de la classe des *prédicats numériques uniformes de degré fini.*
- On prouvera également la conjecture de Straubing pour tous les fragments équipés de prédicats numériques au plus unaires.

Structure du document :

Trois types de résultats sont présentés dans cette thèse : des résultats logiques, des résultats algébriques et des résultats concernant les classes de complexités de circuits. Ces résultats, bien que de natures différentes ne sont pas indépendants. En effet, certains d'entre eux fournissent des arguments clefs dans les preuves d'autres résultats.

Résultats logiques :

- Le théorème *d'ajout des prédicats unaires* (voir Théorème 1.13) établit une description de la classe de langages obtenue lorsque l'on ajoute des prédicats au plus unaires à un fragment. L'un des arguments nécessaires à la preuve de ce théorème est la définition de *fragment logique*, propre à cette thèse, qui englobe les fragments présents dans la littérature. La description obtenue par le théorème d'ajout des prédicats unaires est assez proche de celle donnée par le *principe du produit en couronne*. Elle nous permettra par la suite d'obtenir des caractérisations algébriques de l'ajout des *prédicats modulaires et descriptifs locaux* à un fragment logique.
- Le théorème de substitution des prédicats monadiques (voir Théorème 7.2) établit que si une formule de la logique *monadique du second ordre* définit un langage régulier à l'aide de prédicats monadiques *arbitraires*, alors il est possible de remplacer chaque prédicat par un *prédicat régulier*. Ce résultat permet d'obtenir des caractérisations logiques et algébriques des langages réguliers définis dans un fragment

logique à l'aide de prédicats monadiques arbitraires. On en déduit systématiquement des résultats de séparation pour les fragments équipés de prédicats monadiques arbitraires. Par exemple nous en déduirons que les hiérarchies d'alternances de la logique du premier ordre et de son fragment à deux variables équipés de prédicats numériques unaires sont strictes ; c'est-à-dire que pour tout entier k :

$$\mathcal{B}\mathbf{\Sigma}_k[<, \mathcal{A}\mathrm{rb}_1] \subsetneq \mathcal{B}\mathbf{\Sigma}_{k+1}[<, \mathcal{A}\mathrm{rb}_1]$$
$$\mathbf{FO}^2_k[<, \mathcal{A}\mathrm{rb}_1] \subsetneq \mathbf{FO}^2_{k+1}[<, \mathcal{A}\mathrm{rb}_1]$$

Résultats algébriques :
Nous donnons des descriptions algébriques de l'ajout à un fragment des *prédicats descriptifs locaux* et des *prédicats numériques modulaires*. Cette description algébrique prend la forme d'un *produit en couronne* pour des *variétés de timbres* et nous permet de nous abstraire de la logique. Nos deux principaux résultats sur ce sujet sont les suivantes :

- Le théorème d'ajout des prédicats descriptifs locaux (voir Théorème 3.24) et le théorème d'ajout des prédicats modulaires (voir Théorème 4.15) sont des résultats nouveaux. Dans le cas des prédicats locaux, cela était conjecturé et prouvé pour de nombreux fragments. Ces théorèmes seront présentés comme des conséquences du théorème d'ajout des prédicats unaires (voir Théorème 1.13), qui lui-même repose sur la notion de fragments, propre à cette thèse.
- Les théorèmes *de délai* pour MOD (voir Théorème 4.34 et Théorème 4.39) sont les contributions les plus importantes de cette partie. En effet, on y prouve des *bornes* pour la question dite *de délai* pour le cas des *variétés de rang fini*. Ces deux théorèmes permettent d'obtenir, ou de reprouver, un grand nombre de résultats de décidabilité comme le montrent les tableaux récapitulatifs de la section 4.6. Entre autres, on y trouvera la caractérisation des fragments $\mathbf{FO}^2[<, \mathrm{MOD}]$, $\mathbf{FO}^2[\mathcal{R}\mathrm{eg}]$ ainsi que leur *hiérarchie d'alternance*.

Résultats concernant les circuits booléens :
Les résultats logiques et algébriques vont simplifier en partie les caractérisations algébriques des langages réguliers dans des classes de complexités de circuits. Sur ce sujet, voici les principales contributions de cette thèse :

- En utilisant les résultats algébriques de la première partie ainsi que des bornes inférieures présentes de la littérature, nous caractérisons les langages réguliers appartenant à $\mathbf{WLAC^0}$, c'est-à-dire, des langages reconnus par des circuits de profondeur bornée et possédant un nombre linéaire d'arêtes (voir Théorème 5.13).
- On montre la propriété de *Crane Beach* pour chaque niveau de la hiérarchie d'alternance du fragment à deux variables équipé de *prédicats de degré fini* (voir Théorème 6.10). Cela signifie que les prédicats de degré fini ne sont pas nécessaires pour définir des *langages ayant une lettre neutre*, c'est-à-dire, qu'ils ne permettent pas d'améliorer la *complexité logique à deux variables* de ces langages. De ce résultat, on déduit une caractérisation algébrique des langages réguliers définissables dans la logique à deux variables équipée des prédicats de degré fini ainsi que la séparation

de sa hiérarchie d'alternance.

- On montre également la propriété de Crane Beach (voir Théorème 6.24) pour la logique monadique du second ordre équipée de prédicats numériques monadiques. Cette preuve nous permet par la suite d'obtenir la propriété de Crane Beach pour un grand nombre de fragments vérifiant certaines hypothèses algébriques supplémentaires (voir le corollaire 7.5).

Organisation du manuscrit :
Ce manuscrit est réparti en un chapitre introductif et deux parties principales possédant chacune trois chapitres.

- Chapitre 1 :
  On introduira dans ce chapitre les principales définitions logiques qui seront utilisées dans l'ensemble du document. Les notions de prédicats descriptifs locaux et de fragments logiques sont présentées dans ce chapitre mais ne sont pas usuelles. Le résultat principal de ce chapitre et le théorème d'ajout des prédicats unaires (voir Théorème 1.13).
- **Partie 1 :**
  Dans cette partie, nous étudierons principalement comment l'ajout des prédicats réguliers modifie l'expressivité des fragments logiques. Les outils principaux seront algébriques. Cette partie est décomposée en trois chapitres, chacun correspondant à l'étude d'une signature particulière.

  Chapitre 2 : On étudiera dans ce chapitre les fragments logiques usuels n'utilisant comme prédicats numériques que le prédicat d'ordre ou le prédicat d'égalité. Il y sera présenté les définitions et résultats de la théorie classique des *variétés de monoïdes finis* ainsi que des caractérisations algébriques de ces fragments logiques. Les résultats de cette partie sont principalement issus de la bibliographie.

  Chapitre 3 : On étudiera dans ce chapitre l'ajout des prédicats descriptifs locaux à un fragment logique correspondant à une variété de monoïdes finis. Dans le cas des prédicats numériques locaux, cette opération est connue pour correspondre parfois au produit en couronne par **D**. Ce n'est malheureusement pas tout le temps le cas. En considérant les prédicats descriptifs locaux, et à l'aide du théorème d'ajout des prédicats unaires, il est possible d'obtenir un théorème d'équivalence entre l'ajout de ces prédicats et le produit en couronne par la *variété de semigroupes* **D**. Il s'agit de la principale innovation de ce chapitre (voir Théorème 3.24). Les classes de langages définies dans ce chapitre n'étant pas des *variété de langages*, on introduira les notions de variétés de langages non effaçantes. Pour étudier le produit en couronne par **D**, on utilisera également les outils introduits par Tilson [73], comme par exemple la théorie des *variétés de catégories finies*.

  Chapitre 4 : On étudiera dans ce chapitre l'ajout des prédicats modulaires à un fragment logique. Contrairement aux prédicats numériques locaux, cet ajout correspond exactement au produit en couronne par **MOD** (voir Théorème 4.15).

Les théorèmes de délai (voir Théorème 4.34 et Théorème 4.39) en constituent les principaux résultats. L'étude de ce produit en couronne nécessite l'introduction de *la théorie des variétés multiplicatives*. Afin que les résultats de ce chapitre soient *compatibles* avec ceux du chapitre précédent, on étudiera le produit en couronne par **MOD** à la fois sur les variétés de monoïdes et sur les variétés non effaçantes. Dans ce dernier cas, il sera nécessaire d'introduire la notion de *variété non effaçante de timbres de catégories*, déjà présente dans la thèse de Chaubard [19].

À la fin de chaque chapitre de cette première partie, on trouvera des tableaux récapitulatifs des fragments étudiés, ainsi qu'une description succincte de leur algorithme de décision si celui-ci est connu.

- **Partie 2 :**
  Cette partie se concentrera sur les fragments logiques équipés de prédicats numériques arbitraires. Elle est structurée en trois chapitres.

  Chapitre 5 : Dans ce chapitre, nous présenterons les principales définitions concernant les classes de complexité de circuits booléens, ainsi que des descriptions logiques qui leur sont équivalentes. Le principal résultat de ce chapitre est la caractérisation des langages réguliers de la classe $\mathbf{WLAC^0}$ (voir Théorème 5.13). Un certain nombre de résultats, présents dans la bibliographie, seront également évoqués afin d'exposer un état de l'art sur ce sujet.

  Chapitre 6 : Ce chapitre contient deux résultats concernant des fragments logiques équipés de classe de prédicats numériques non réguliers. Afin de présenter ces résultats, nous introduirons une variante de la conjecture de Straubing, inspirée par celle introduite dans le livre [66] de ce dernier, ainsi que la propriété de Crane Beach, inspirée par la conjecture du même nom réfutée dans l'article [11]. Deux résultats seront exposés dans ce chapitre. Le premier établit que la propriété de Crane Beach est satisfaite pour la hiérarchie d'alternance de la logique à deux variables équipée de prédicats de degré fini (voir Théorème 6.10). De ce théorème, on déduit que ce même fragment satisfait la conjecture de Straubing. Le second résultat établi la propriété de Crane Beach pour la logique monadique du second ordre équipée de prédicat monadique (voir Théorème 6.24).

  Chapitre 7 : Ce chapitre présentera *la propriété substitution*. Nous établirons que cette propriété est vérifiée pour la logique monadique du second ordre équipée de prédicats unaires. Comme corollaires immédiats, nous obtiendrons que tout fragment logique équipé de prédicats monadiques satisfait la conjecture de Straubing. En ajoutant certaines hypothèses nous en déduirons que la propriété de Crane Beach est satisfaite pour tout fragment équipé de prédicats numérique monadique. Enfin, nous conclurons ce manuscrit en étudiant les limites de cette propriété de substitution ainsi que les possibles extensions pour des recherches ultérieures.

Chapitre 1

Prérequis

1.1 Notations classiques

Dans l'ensemble de la thèse, chaque première occurrence d'un terme non défini sera mise en *italique*. Nous utiliserons les notations classiques de la théorie des ensembles.

- $\emptyset$ *l'ensemble vide*,
- $\mathcal{P}(E)$ *l'ensemble des parties* d'un ensemble E,
- $x \in E$ pour x *appartient* à E,
- E^c le *complément* de E,
- $E \cup F$ *l'union* des ensembles E et F,
- $E \cap F$ *l'intersection* des ensembles E et F,
- $E - F$ pour $E \cap F^c$,
- $F \subseteq E$ pour F *inclus non strictement* dans E et $F \subsetneq E$ pour F *inclus strictement* dans E,
- $E \times F$ pour le *produit cartésien* de E par F et E^k le produit cartésien de E par lui-même k fois,
- $|E|$ la *taille* de E, avec E un ensemble fini.

En outre, un k-uplet est un élément de E^k. Par convention, on pose $E^0 = \{\emptyset\}$. Pour $E \subseteq \mathbb{N}$, on notera $\min E$ le plus petit élément de E et $\max E$ son plus grand élément avec $\min \emptyset = +\infty$ et $\max \emptyset = -\infty$.

Une *relation* d'arité n sur un ensemble E est un sous-ensemble de E^n. Soit $\mathcal{R}$ une relation d'arité 2 (ou binaire) sur un ensemble E. Deux éléments x et y de E sont en *relation* par $\mathcal{R}$, si $(x, y) \in \mathcal{R}$, ce que l'on note $x \mathcal{R} y$. La relation $\mathcal{R}$ est dite *réflexive* si, pour tout $x \in E$, on a $x \mathcal{R} x$. Elle est dite *symétrique* si pour tous $x, y \in E$, $x \mathcal{R} y$ implique $y \mathcal{R} x$, et *antisymétrique* si pour tous $x, y \in E$, $x \mathcal{R} y$ et $y \mathcal{R} x$ implique $x = y$. Enfin, $\mathcal{R}$ est dite *transitive* si pour tous $x, y, z \in E$, $x \mathcal{R} y$ et $y \mathcal{R} z$ impliquent $x \mathcal{R} z$.

- Une relation est un *préordre* si elle réflexive et transitive.
- Une relation est un *ordre* si c'est un pré-ordre antisymétrique.
- Une *relation d'équivalence* est une relation réflexive, symétrique et transitive. Si $\mathcal{R}$

est une relation d'équivalence de E et $x \in E$, alors la *classe d'équivalence de* x est l'ensemble des éléments de E équivalents à x selon $\mathcal{R}$. Les classes d'équivalences selon $\mathcal{R}$ forment une partition de E et l'ensemble de ces classes est noté $E/\mathcal{R}$.

1.2 Automates et mots finis

Soit A un ensemble fini. On dit que A est un *alphabet* quand on souhaite souligner que les éléments de A seront utilisés comme des *lettres*. Un *mot fini* $u = (u_0, \ldots, u_{n-1})$ de longueur n est un élément de A^n et 1 est l'unique mot de longueur nulle qu'on appelle le *mot vide*. On note A^* l'ensemble des mots finis sur l'alphabet A et A^+ l'ensemble des mots différents du mot vide sur l'alphabet A. Un *langage* de A^* (ou sur l'alphabet A) est un sous-ensemble de A^*. On utilise la notation $u = u_0 \cdots u_{n-1}$ pour désigner les mots finis au lieu de la notation classique des n-uplets et on note $|u|$ la *longueur* du mot u. Pour $B \subseteq A$, on pose

$$|u|_B = |\{i < |u| \mid u_i \in B\}|.$$

La concaténation d'un mot $u = u_0 \cdots u_{n-1} \in A^*$ par un mot $v = v_0 \cdots v_{p-1} \in A^*$ est le mot $uv = u_0 \cdots u_{n-1} v_0 \cdots v_{p-1}$. On note également u^n la concaténation de u par lui-même n fois. Par convention $u^0 = 1$. Pour $u \in A^*$ et L un langage de A^*, on pose

$$u^{-1}L = \{v \in A^* \mid uv \in L\}$$

ainsi que

$$Lu^{-1} = \{v \in A^* \mid vu \in L\}.$$

On dit qu'un langage L sur l'alphabet A a une *lettre neutre* s'il existe une lettre $c \in A$ telle que pour tous mots $u, v \in A^*$, $uv \in L$ si et seulement si $ucv \in L$.

Un *automate* est un quintuplet $\mathcal{A} = (Q, A, \delta, I, F)$ avec Q un ensemble fini d'*états*, A un alphabet, $\delta \subseteq Q \times A \times Q$, les *transitions*, $I \subseteq Q$ les *états initiaux* et $F \subseteq Q$ les *états finaux*. On note dans la suite $q \xrightarrow{a} q'$ la transition (q, a, q'). Un chemin de $\mathcal{A}$ est un mot $(q_0, a_0, q_1)(q_1, a_1, q_2) \cdots$ sur l'alphabet $(Q \times A \times Q)$ que l'on note

$$q_0 \xrightarrow{a_0} q_1 \xrightarrow{a_1} \cdots q_n \xrightarrow{a_n} q_{n+1} \in (Q \times A \times Q)^{n+1}$$

et tel que pour tout $i \leqslant n$, $(q_i, a_i, q_{i+1}) \in \delta$. Il est dit *acceptant* si $q_0 \in I$ et $q_{n+1} \in F$. Un mot est *accepté* par $\mathcal{A}$ s'il étiquette un chemin acceptant de $\mathcal{A}$. On note $L(\mathcal{A})$ le langage des mots acceptés par $\mathcal{A}$. Un langage L est *reconnaissable* s'il existe un automate $\mathcal{A}$ tel que $L = L(\mathcal{A})$. Pour chaque langage reconnaissable, il existe un *automate minimal déterministe* le reconnaissant (voir le livre [16] pour plus de détails).

Les opérations suivantes sont dites *rationnelles*. Soient L et K deux langages.

- L'union de deux langages,
- La concaténation de deux langages

$$LK = \{uv \mid u \in L \text{ et } v \in K\},$$

- L'*étoile de Kleene*
$$L^* = \{u^n \mid u \in L \text{ et } n \in \mathbb{N}\}.$$

La classe des *langages rationnelles* de A^* est la plus petite classe close par les opérations rationnelles, contenant le langage vide et les langages $\{a\}$ pour $a \in A$.

Théorème 1.1 (Kleene [36]).

Un langage est reconnaissable si et seulement s'il est rationnel.

Les langages reconnaissables (ou rationnels d'après le théorème de Kleene) sont aussi appelés *langages réguliers*. Nous adopterons cette terminologie dans la suite de cette thèse.

1.3 Logique sur les mots finis

Nous allons présenter les définitions logiques usuelles : formules, structures, syntaxe et sémantique de la logique monadique du second ordre, puis nous allons préciser la différence entre *prédicats descriptifs* et *prédicats numériques*. Enfin, nous introduirons une définition formelle de *fragments* afin de pouvoir prouver le théorème 1.13 (*d'ajout des prédicats unaires*) qui sera utilisé à plusieurs reprises dans la suite de la thèse.

1.3.1 Syntaxe de la logique monadique du second ordre

Notation : Par convention, les lettres minuscules $x, y, z, \ldots$ désigneront des variables du *premier ordre* et les lettres majuscules $X, Y, Z, \ldots$ des variables du second ordre.

Pour chaque formule φ, on associera par induction un ensemble de symboles de variables libres $\mathcal{V}\ell_1(\varphi)$ du premier ordre et un ensemble de symboles de variables libres $\mathcal{V}\ell_2(\varphi)$ du second ordre. Les *atomes* de la logique désignent les briques utilisées pour construire les formules. Outre l'atome *d'appartenance*, noté $x \in X$, nous considérons des *prédicats* appartenant une *signature* que l'on note σ.

Remarque : Nous ne considérons que des signatures relationnelles, c'est-à-dire, σ ne contiendra jamais de symbole de fonction.

Quand cela sera nécessaire, les prédicats pourront être notés comme des applications ou comme des ensembles, c'est-à-dire que, pour un prédicat P d'arité n, on utilisera indistinctement les notations $(x_1, \ldots, x_n) \in P$ ou $P(x_1, \ldots, x_n)$. Pour un prédicat abstrait dont l'arité n'est pas précisée, on utilisera également la notation $\vec{x} \in P$ ou $P(\vec{x})$.

Soit σ une signature. Les formules suivantes constituent les atomes de la *logique monadique du second ordre*.

- La formule *vrai* et la formule *faux*.
- La formule $x \in X$ avec $\mathcal{V}\ell_1(x \in X) = \{x\}$ et $\mathcal{V}\ell_2(x \in X) = \{X\}$

- La formule $(x_1, \ldots, x_n) \in P$ pour $P \in \sigma$ d'arité n avec

$$\mathcal{V}\ell_1((x_1, \ldots, x_n) \in P) = \{x_1, \ldots, x_n\} \text{ et } \mathcal{V}\ell_2((x_1, \ldots, x_n) \in P) = \emptyset.$$

Supposons que φ et ψ soient des formules. Nous construisons les *formules* de la logique monadique du second ordre par induction à l'aide des opérations suivantes.

- L'opérateur booléen unaire $\neg\varphi$ (non φ) avec

$$\mathcal{V}\ell_1(\neg\varphi) = \mathcal{V}\ell_1(\varphi) \text{ et } \mathcal{V}\ell_2(\neg\varphi) = \mathcal{V}\ell_2(\varphi).$$

- Les opérateurs booléens binaires $\varphi \wedge \psi$ (φ et ψ) ainsi que $\varphi \vee \psi$ (φ ou ψ) avec

$$\mathcal{V}\ell_1(\varphi \wedge \psi) = \mathcal{V}\ell_1(\varphi \vee \psi) = \mathcal{V}\ell_1(\varphi) \cup \mathcal{V}\ell_1(\psi),$$
$$\mathcal{V}\ell_2(\varphi \wedge \psi) = \mathcal{V}\ell_2(\varphi \vee \psi) = \mathcal{V}\ell_2(\varphi) \cup \mathcal{V}\ell_2(\psi).$$

- Les quantifications du premier ordre $\exists x\ \varphi$ (il existe une position x telle que φ), et $\forall x\ \varphi$ (pour toute position x φ) avec

$$\mathcal{V}\ell_1(\exists x\ \varphi)) = \mathcal{V}\ell_1(\forall x\ \varphi) = \mathcal{V}\ell(\varphi) - \{x\},$$
$$\mathcal{V}\ell_2(\exists x\ \varphi)) = \mathcal{V}\ell_2(\forall x\ \varphi) = \mathcal{V}\ell_2(\varphi).$$

- Les quantifications monadiques du second ordre $\exists X\ \varphi$ (il existe un ensemble de positions X tel que φ), et $\forall X\ \varphi$ (pour tout ensemble de positions X φ) avec

$$\mathcal{V}\ell_1(\exists X\ \varphi)) = \mathcal{V}\ell_1(\forall X\ \varphi) = \mathcal{V}\ell(\varphi),$$
$$\mathcal{V}\ell_2(\exists X\ \varphi)) = \mathcal{V}\ell_2(\forall X\ \varphi) = \mathcal{V}\ell_2(\varphi) - \{X\}.$$

Notations : On utilisera $\varphi \to \psi$ pour la formule $(\neg\varphi) \vee \psi$ et $\varphi \leftrightarrow \psi$ pour $(\varphi \to \psi) \wedge (\psi \to \varphi)$. Lorsqu'on voudra mettre en évidence les variables libres d'une formule φ de **MSO** on pourra utiliser la notation $\varphi(x_1, \ldots, x_k, X_1, \ldots, X_p)$ avec $\mathcal{V}\ell_1(\varphi) = \{x_1, \ldots, x_k\}$ et $\mathcal{V}\ell_2(\varphi) = \{X_1, \ldots, X_p\}$.

Nous introduisons également les priorités usuelles des opérations logiques. La négation ($\neg$) est prioritaire sur les autres opérations, puis dans l'ordre suivant, la conjonction ($\wedge$), la disjonction ($\vee$), les quantifications, l'implication ($\to$) et l'équivalence ($\leftrightarrow$).

Une formule φ de la logique monadique du second ordre est *close* si $\mathcal{V}\ell_1(\varphi) = \mathcal{V}\ell_2(\varphi) = \emptyset$, autrement dit si elle ne possède pas de variable libre. On dit également que φ est un *énoncé*.

1.3.2 Sémantique de la logique monadique du second ordre sur les mots finis

Nous avons défini la syntaxe de la logique monadique du second ordre. Nous allons maintenant en décrire la sémantique sur les mots finis. Avant toute chose, nous allons

proposer un codage d'un mot fini en une *structure*. Soit n un entier, le *segment initial* de taille n est l'ensemble $[n] = \{0, \ldots, n-1\}$. Une *structure* est un couple

$$S = ([n], \sigma_S)$$

avec σ_S une *interprétation* de la signature, c'est-à-dire, pour chaque prédicat $P \in \sigma$ d'arité k on associe un sous-ensemble $P_S \subseteq [n]^k$. Si P est d'arité 0, alors P_S est une valeur de vérité *vrai* ou *faux*. Soit $S = ([n], \sigma_S)$ une structure. Une interprétation dans S des variables de $\mathcal{V}\ell_1$ et $\mathcal{V}\ell_2$ est une paire $\nu = (\mathcal{I}_1, I_2)$, où $\mathcal{I}_1$ est une fonction de $\mathcal{V}\ell_1$ vers $[n]$ et $\mathcal{I}_2$ une fonction de $\mathcal{V}\ell_2$ vers $\mathcal{P}([n])$. Pour $\nu = (\mathcal{I}_1, \mathcal{I}_2)$, a un élément de $[n]$ et x une variable de $\mathcal{V}\ell_1$, on note $\nu\binom{a}{x}$ l'assignation de x à la variable a. Plus précisément, la paire $\nu\binom{a}{x} = (\mathcal{I}'_1, \mathcal{I}_2)$, où

$$\mathcal{I}'_1(y) = \begin{cases} \mathcal{I}_1(y) & \text{si } y \neq x, \\ a & \text{si } y = x. \end{cases}$$

De même, pour $R \subseteq [n]$ et X une variable de $\mathcal{V}\ell_2$, on note $\nu\binom{R}{X}$ la paire $(\mathcal{I}_1, \mathcal{I}'_2)$, où

$$\mathcal{I}'_1(Y) = \begin{cases} \mathcal{I}_1(Y) & \text{si } Y \neq X, \\ R & \text{si } Y = X. \end{cases}$$

Nous définissons maintenant la relation $S \models \varphi[\nu]$ (S vérifie $\varphi[\nu]$) par induction. On suppose dans la suite, que les variables libres des formules que l'on considère sont dans les pré-images des fonctions $\mathcal{I}_1$ et $\mathcal{I}_2$. On définit dans un premier temps cette relation sur les cas de base :

- $S \models \mathit{vrai}[\nu]$ et $S \not\models \mathit{faux}[\nu]$.
- $S \models (x \in X)[\nu]$ si et seulement si $\mathcal{I}_1(x) \in \mathcal{I}_2(X)$.
- $S \models P[\nu]$ avec P un prédicat d'arité 0 si et seulement si P_S est interprété par *vrai*.
- $S \models (P(x_1, \ldots, x_k))[\nu]$ si et seulement si $(\mathcal{I}_1(x_1), \ldots, \mathcal{I}_1(x_k)) \in P_S$.

Supposons que cette relation soit définie pour les formules φ et ψ.

- $S \models (\neg\varphi)[\nu]$ si et seulement si $S \not\models \varphi[\nu]$.
- $S \models (\varphi \wedge \psi)[\nu]$ si et seulement si $S \models \varphi[\nu]$ et $S \models \psi[\nu]$.
- $S \models (\varphi \vee \psi)[\nu]$ si et seulement si $S \models \varphi[\nu]$ ou $S \models \psi[\nu]$.
- $S \models (\exists x\ \varphi)[\nu]$ si et seulement s'il existe un élément $a \in [n]$ tel que $S \models \varphi[\nu\binom{a}{x}]$.
- $S \models (\forall x\ \varphi)[\nu]$ si et seulement s'il pour tout élément $a \in [n]$, on a $S \models \varphi[\nu\binom{a}{x}]$.
- $S \models (\exists X\ \varphi)[\nu]$ si et seulement s'il existe un ensemble $R \subseteq [n]$ tel que $S \models \varphi[\nu\binom{R}{X}]$.
- $S \models (\forall X\ \varphi)[\nu]$ si et seulement s'il pour tout ensemble $R \subseteq [n]$, on a $S \models \varphi[\nu\binom{R}{X}]$.

À un mot de longueur n on associe à une structure de taille n ; précisons l'interprétation des prédicats. On distingue deux cas : si l'interprétation d'un prédicat dépend des lettres du mot, le prédicat est dit *descriptif*, dans le cas contraire, son interprétation est identique sur tous les mots d'une même longueur, il est alors dit *numérique*. Plus précisément, un prédicat numérique $P = (P_n)$ d'arité k est une suite telle que $P_n \subseteq [n]^k$. Un prédicat numérique P est *uniforme* s'il s'agit d'une relation sur les entiers. Plus précisément, (P_n)

est uniforme s'il existe $Q \subseteq \mathbb{N}^k$ tel que $P_n = Q \cap [n]^k$. Pour les prédicats uniformes, nous ne distinguerons plus la relation sur les entiers du prédicat associé.

Notations : On note $\mathcal{A}\mathrm{rb}$ la classe de tous les prédicats numériques et $\mathcal{A}\mathrm{rb}^u$ la classe des prédicats uniformes. Pour k un entier, on note également $\mathcal{A}\mathrm{rb}_k$ et $\mathcal{A}\mathrm{rb}_k^u$ les prédicats numériques (uniformes) d'arité au plus k. On confondra à partir de maintenant les prédicats numériques et leur interprétation.

Exemples : Les prédicats suivants sont des prédicats uniformes.

- Les constantes $x = c$ définies par $\{c\}$ pour $c \in \mathbb{N}$.
- Le prédicat d'égalité, $x = y$ défini par $\{(x, y) \in \mathbb{N}^2 \mid x = y\}$.
- Le prédicat d'ordre linéaire, $x < y$ défini par $\{(x, y) \in \mathbb{N}^2 \mid x < y\}$.
- Les prédicats arithmétiques, $x + y = z$, $xy = z, \ldots$
- Le prédicat $\mathrm{BIT}(x, y)$ défini par

$$\{(x, y) \mid \text{ le } y^{\text{ème}} \text{ bit de la représentation binaire de } x \text{ est un } 1\}.$$

Les prédicats suivants ne sont pas uniformes :

- Le prédicats 0-aires de taille : *la position maximale est première* qui est vrai si et seulement si la dernière position du mot est un nombre premier.
- Les positions constantes par rapport à la position maximale, $x = \max - c$ définies par $(\{n - c\})_n$ pour $c \in \mathbb{N}$.
- La position médiane, $x/2$ définie par (P_n) où $\begin{cases} P_{2n} = \{n\}, \\ P_{2n+1} = \emptyset. \end{cases}$

Les prédicats descriptifs usuels sont les *prédicats de lettres*. À chaque lettre $a \in A$, on associe un prédicat unaire, noté $\mathbf{a}$. Pour le mot $u = u_0 \cdots u_{n-1} \in A^*$, l'interprétation de $\mathbf{a}$ est l'ensemble $\mathbf{a}_u = \{i \mid u_i = a\}$. D'autres prédicats descriptifs existent. Nous utiliserons également les prédicats descriptifs *locaux* qui sont les prédicats qui parlent des lettres *autour* d'une position et pas uniquement de la lettre de la position. On les définit comme suit. Pour chaque lettre $a \in A$ et $k \in \mathbb{N}$:

- Le prédicat unaire translaté à gauche $\mathbf{a_{-k}}$:
  Pour tout mot $u = u_0 \cdots u_{n-1} \in A^*$, l'interprétation de $\mathbf{a_{-k}}$ est l'ensemble

$$(\mathbf{a_{-k}})_u = \{k \leqslant i < n \mid u_{i-k} = a\}.$$

- Le prédicat $\mathbf{a}(\max - k)$:
  Pour tout mot $u = u_0 \cdots u_{n-1} \in A^*$, l'interprétation de $\mathbf{a}(\max - k)$ est *vraie* si et seulement si $u_{n-k} = a$.

Ainsi le prédicat translaté d'une position à gauche $\mathbf{a_{-1}}$ est évalué uniquement en fonction de la lettre directement à la gauche de la position.

Notation : On note $\mathrm{LOC_D}$ l'ensemble des prédicats descriptifs locaux.

Remarques : Les prédicats descriptifs locaux étendent les prédicats usuels puisque le prédicat de lettre $\mathbf{a}$ est exactement le prédicat $\mathbf{a_{-0}}$. Une définition équivalente (prédicats de lettre translatés à droite) est possible, on choisit d'orienter la signature à gauche par commodité.

Exemples :

- L'interprétation du prédicat $\mathbf{a_{-2}}$ pour le mot $u = \underset{0\,1\,2\,3\,4}{abaab}$ est l'ensemble
$$(\mathbf{a_{-2}})_u = \{2, 4\}.$$
- L'interprétation du prédicat $\mathbf{a_{-3}}$ pour le mot $u = aa$ est l'ensemble
$$(\mathbf{a_{-3}})_u = \emptyset.$$

Notations : Soit $\mathcal{C}$ une classe de prédicats. On notera $\mathbf{MSO}[\mathcal{C}]$ les formules utilisant les prédicats dans $\mathcal{C}$ ainsi que les prédicats de lettres. On notera également $\mathbf{MSO}[\mathcal{C}](A^*)$ les langages de A^* reconnus par une formules de $\mathbf{MSO}[\mathcal{C}]$.

Un langage L de A^* est *défini* par un énoncé φ si $L \cap A^+$ est le langage des mots satisfaisant φ sur l'alphabet A. Deux formules sont *équivalentes* si elles définissent les mêmes langages. Il s'agit ici d'une équivalence *sémantique* et non pas de la notion plus usuelle d'*équivalence* en logique.

Remarque : Une même formule peut définir plusieurs langages sur des alphabets différents. Par exemple, $\exists x\ \mathbf{a}(x)$ définit le langage a^+ sur l'alphabet $\{a\}$ ainsi que le langage $\{a{+}b\}^*a\{a{+}b\}^*$ sur l'alphabet $\{a, b\}$.

Le théorème suivant établit le lien entre la logique et les langages réguliers.

Théorème 1.2 (Büchi [15]).

Un langage est régulier si et seulement s'il est définissable par une formule de $\mathbf{MSO}[<]$.

Il existe d'autres équivalences intéressantes entre **MSO** et des modèles de calculs qui sortent du cadre de cette thèse.

Théorème 1.3 (Wrathall [76]).

Un langage est dans la *hiérarchie de temps linéaire* si et seulement s'il est définissable par une formule de $\mathbf{MSO}[+]$.

Remarques : La hiérarchie de temps linéaire correspond à la *clôture par oracles* de la classe des langages calculés par une *machine de Turing* en temps linéaire. Ces langages sont également connus sous le nom de *langages rudimentaires*.

1.3.3 Quelques classes de prédicats numériques

Soit $\varphi(x_1, \ldots, x_k)$ une formule de $\mathbf{MSO}[<]$ sans prédicat descriptif. Le prédicat numérique $P = (P_n)$ est défini par φ si $(p_1, \ldots, p_n) \in P_n$ si et seulement si $([n], <) \models \varphi[\nu]$ où $\nu = (\mathcal{I}_1, \mathcal{I}_2)$ vérifie que $\mathcal{I}_1(x_i) = p_i$ pour $1 \leqslant i \leqslant n$. Un prédicat numérique est *un prédicat numérique régulier* s'il est défini par une formule de $\mathbf{MSO}[<]$. La classe des prédicats numériques réguliers a été introduite par Straubing [65] et étudiée par Péladeau [49].

Notation : On note $\mathcal{R}\text{eg}$ la classe des prédicats numériques réguliers.

Exemple : Les prédicats numériques suivants sont réguliers.

- Le prédicat $<$ est par définition régulier. Il est défini par la formule $x < y$. On note également $x \leqslant y$ pour le prédicat régulier défini par $\neg(y < x)$.
- Les prédicats *numériques locaux*

$$\text{LOC} : \begin{cases} x = y + k \\ x = k \text{ et } x = \max - k \\ \max = k \end{cases} \quad \text{pour } k \in \mathbb{N}$$

- Les prédicats *numériques modulaires*

$$\text{MOD}_q : \begin{cases} x \equiv r \bmod q \\ \max \equiv r \bmod q \end{cases} \quad \text{pour } r < q \text{ deux entiers.}$$

  On notera également $\text{MOD} = \bigcup_{q \in \mathbb{N}} \text{MOD}_q$.

Le théorème suivant établit que tout prédicat régulier est définissable par des combinaisons booléennes d'atomes de la signature numérique $\{<\} \cup \text{LOC} \cup \text{MOD}$. Il a été prouvé simultanément par Péladeau et Straubing.

Théorème 1.4 (Péladeau [49], Straubing [65]).

Un prédicat P est régulier s'il est définissable par une formule de $\mathbf{MSO}[<, \text{LOC}, \text{MOD}]$ sans prédicat descriptif et sans quantificateur.

1.3.4 Les fragments de la logique monadique du second ordre

On dira que deux classes de formules sont *équivalentes* si elles définissent les mêmes classes de langages. Il peut être intéressant d'imposer certaines restrictions syntaxiques sur les classes de formules pour pouvoir prouver des résultats génériques et réutilisables. Cela va motiver notre définition de *fragment logique*.

Définition 1.5 (substitution atomique).

Une classe de formules $\mathbf{F}$ sur une signature σ est stable par substitution atomique si pour toute formule de $\mathbf{F}$, une formule obtenue en substituant un atome par une combinaison booléenne d'atomes de σ ayant le même ensemble de variables libres est toujours dans $\mathbf{F}$.

Dans cette thèse, un *fragment* est une classe d'énoncés, stable par $\wedge$ et par $\vee$, contenant les prédicats d'arité 0 et stable par substitution atomique. Il s'agira donc des hypothèses minimales que nous supposerons vérifiées par les classes de formules. Ces hypothèses ne sont pas très exigeantes ; tous les fragments présents dans la littérature les vérifient.

Notations : On notera les fragments en gras : **F**. Suivant les notations pour **MSO**, pour $\mathcal{C}$ une classe de prédicats, $\mathbf{F}[\mathcal{C}]$ désigne le fragment obtenu en ajoutant les prédicats $\mathcal{C}$ dans la signature. En particulier, si **F** est un fragment, alors $\mathbf{F}[\mathcal{C}]$ est également un fragment. Pour A un alphabet fini, on notera $\mathbf{F}[\mathcal{C}](A^*)$ les langages de A^* définissable par une formule de $\mathbf{F}[\mathcal{C}]$.

La notion de fragments a été abordée sous un angle différent dans l'article de Kufleitner et Lauser [43]. Ils ont donné d'autres restrictions syntaxiques qui garantissent que les fragments définissent des classes de langages possédant des propriétés algébriques intéressantes, par exemple, de définir une *variété de langages*.

La proposition suivante est une conséquence directe du théorème 1.4 et de la définition de fragment. En effet, il est toujours possible de remplacer dans un fragment une occurrence d'un prédicat régulier par une formule sans quantificateur équivalente.

Proposition 1.6.

Soit **F** un fragment. Les fragments $\mathbf{F}[\mathcal{R}\mathrm{eg}]$ et $\mathbf{F}[<, \mathrm{MOD}, \mathrm{LOC}]$ sont équivalents.

La taxonomie des fragments de la logique monadique du second ordre est très riche. De nombreux paramètres et constructions peuvent être utilisés pour définir des fragments pertinents. Nous allons nous intéresser particulièrement à *la théorie du premier ordre*, à la notion *de complexité logique* associée ainsi qu'aux *quantificateurs modulaires*. Toutes les classes de formules ainsi introduites seront des fragments.

La logique du *premier ordre* est l'un des fragments les plus classiques. Il s'agit des formules de **MSO** n'utilisant aucune quantification du second ordre.

Notation : On notera le fragment de la logique du premier ordre **FO** (*first order*).

Introduisons maintenant les *quantificateurs modulaires*. Pour chaque couple d'entiers $0 \leqslant r < q$, on note $\exists^{r,q} x\ \varphi$ (il existe r modulo q positions x vérifiant φ) le symbole de *quantification modulaire d'indices* r, q. La sémantique est présentée dans la définition suivante.

Définition 1.7 (Quantificateurs modulaires).

Soient φ une formule de $\mathbf{MSO}[<]$, $0 \leqslant r < q$ deux entiers, $S = ([n], \sigma_S)$ une structure et $\nu = (\mathcal{I}_1, \mathcal{I}_2)$ une interprétation des variables libres dans S. On a $S \models (\exists^{r,q} x\ \varphi)[\nu]$ si et seulement s'il existe r modulo q élément(s) $a \in [n]$ tel(s) que $S \models \varphi[\nu\binom{a}{x}]$.

Ces quantificateurs sont dits réguliers car *exprimables* dans $\mathbf{MSO}[<]$, comme nous allons le voir dans la proposition suivante.

Proposition 1.8.

Soit φ une formule de $\mathbf{MSO}[<]$. Pour tout entier $0 \leqslant r < q$, il existe une formule ψ de $\mathbf{MSO}[<]$ équivalente à $\exists^{r,q} x\ \varphi(x)$.

Démonstration : Nous allons exhiber une formule de $\mathbf{MSO}[<]$ permettant de calculer la taille d'un ensemble r modulo q. Avant de donner cette formule, introduisons quelques formules intermédiaires. La formule $X = X_0 \uplus \cdots \uplus X_{q-1}$ est vraie si X est l'union disjointe de $X_0, \ldots, X_{q-1}$. Cette formule est définie par :

$$\Big(\forall x\ x \in X \to \Big(\bigvee_{i=0}^{q-1} x \in X_i\Big)\Big) \wedge \left(\bigwedge_{i=0}^{q-1} \Big(\forall x\ x \in X_i \to \Big(\bigwedge_{j \neq i} \neg(x \in X_j)\Big)\Big)\right)$$

La formule $y = \mathrm{suc}_X(x)$ est vraie si $x < y$ sont dans X et qu'il n'existe aucun élément de X entre eux. Cette formule est définie par :

$$\big(x \in X\big) \wedge \big(y \in X\big) \wedge (x < y) \wedge \Big(\forall z\ \Big(\big(z \in X\big) \wedge (x \leqslant z) \wedge (z \leqslant y)\Big) \to \Big((z = y) \vee (z = x)\Big)\Big)$$

La formule $x = \max_X$ est vraie si x est la dernière position de X. Cette formule est définie par :

$$\big(x \in X\big) \wedge \forall y\ \big(y \in X\big) \to (y \leqslant x)$$

Enfin, on donne la formule $|X| \equiv r \bmod q$ qui est vraie si X contient r modulo q éléments :

$$\begin{aligned} \exists X_0 \cdots \exists X_{q-1}\ & (X = X_0 \uplus \cdots \uplus X_{q-1}) \wedge \\ & \bigwedge_{i=0}^{q-1} \forall x, y\ \Big(\big(x \in X_i\big) \wedge y = \mathrm{suc}_X(x)\Big) \to \Big(y \in X_{i+1 \bmod q}\Big) \wedge \\ & \qquad \exists x\ x = \max_X \wedge \big(x \in X_r\big). \end{aligned}$$

Nous concluons la preuve en définissant la formule ψ (équivalente à $\exists^{r,q} x\ \varphi$)) par :

$$\exists X\ \ \big(\forall x\ \big(x \in X\big) \leftrightarrow \varphi(x)\big) \wedge |X| \equiv r \bmod q$$

■

Notations : Soit $Q \subseteq \mathbb{N}$. On notera $\mathbf{FO} + \mathbf{MOD}(Q)$ l'ensemble des formules n'utilisant que des quantifications du premier ordre ou modulaires d'indices r, q avec $q \in Q$. On notera également $\mathbf{MOD}(Q)$ l'ensemble des formules utilisant uniquement des quantifications modulaires d'indices r, q avec $q \in Q$, ainsi que $\mathbf{FO} + \mathbf{MOD}$ le fragment $\mathbf{FO} + \mathbf{MOD}(\mathbb{N})$ et $\mathbf{MOD}$ le fragment $\mathbf{MOD}(\mathbb{N})$.

À l'aide du théorème 1.2 et de la proposition 1.8, on obtient que les langages définissables dans $(\mathbf{FO} + \mathbf{MOD})[<]$ sont tous réguliers.

Complexité logique

Le *nombre de symboles de variables* du premier ordre utilisés dans une formule est un premier paramètre qui va nous intéresser. Soit φ une formule de **FO**. Le nombre de variables de φ est le nombre maximal de variables libres présent dans les sous-formules de φ.

Exemple : Dans l'exemple suivant, la formule n'utilise que deux variables mais trois quantifications :

$$\exists x\ (x = 0) \wedge \Big(\exists y\ (y = x + 1) \wedge \big(\exists x\ (x = y + 1) \wedge \mathbf{a}(x)\big)\Big)$$

Sur l'alphabet $A = \{a, b\}$, cette formule définit du langage A^2aA^*.

Notation : Soit **F** un fragment de **MSO**. On note $\mathbf{F}^k$ la classe des formules de **F** utilisant au plus k variables.

Le théorème suivant établit que dans le contexte des langages réguliers, trois variables sont suffisantes pour décrire les langages définissables dans **FO**.

Théorème 1.9 (Kamp [35]).

Pour tout entier $k \geqslant 3$, $\mathbf{FO}^k[<]$ est un fragment équivalent à $\mathbf{FO}[<]$.

Le dernier paramètre qui nous intéresse sera étudié uniquement dans le cadre de la logique du premier ordre. Il s'agit du nombre d'*alternances de quantifications* ou de la *complexité logique fine* que l'on note $\mathrm{alt}(\varphi)$ pour φ une formule du premier ordre.

Afin de le définir, on introduit deux nouveaux paramètres. Le premier est le nombre d'alternances de quantificateurs commençant par une quantification existentielle, noté $\mathrm{alt}_\exists$. Le second, noté $\mathrm{alt}_\forall$, est son symétrique, c'est-à-dire, le nombre d'alternances de quantificateurs débutant par une quantification universelle. On les définit simultanément par induction. Pour toute formule φ sans quantification, on pose $\mathrm{alt}_\exists(\varphi) = \mathrm{alt}_\forall(\varphi) = 0$. Soient φ et ψ deux formules de **FO**. On pose

$$\begin{aligned}
\mathrm{alt}_\exists(\varphi \wedge \psi) &= \mathrm{alt}_\exists(\varphi \vee \psi) = \max\{\mathrm{alt}_\exists(\varphi), \mathrm{alt}_\exists(\psi)\} \\
\mathrm{alt}_\forall(\varphi \wedge \psi) &= \mathrm{alt}_\forall(\varphi \vee \psi) = \max\{\mathrm{alt}_\forall(\varphi), \mathrm{alt}_\forall(\psi)\} \\
\mathrm{alt}_\exists(\neg\varphi) &= \mathrm{alt}_\forall(\varphi) \\
\mathrm{alt}_\forall(\neg\varphi) &= \mathrm{alt}_\exists(\varphi) \\
\mathrm{alt}_\exists(\exists x\ \varphi) &= \mathrm{alt}_\forall(\varphi) + 1 \\
\mathrm{alt}_\exists(\forall x\ \varphi) &= \mathrm{alt}_\exists(\varphi) \\
\mathrm{alt}_\forall(\exists x\ \varphi) &= \mathrm{alt}_\forall(\varphi) \\
\mathrm{alt}_\forall(\forall x\ \varphi) &= \mathrm{alt}_\exists(\varphi) + 1
\end{aligned}$$

Enfin, on pose $\mathrm{alt}(\varphi) = \max\{\mathrm{alt}_\exists(\varphi), \mathrm{alt}_\forall(\varphi)\}$. Pour **F** un fragment, on note $\mathbf{F}_n$ la classe des formules φ de **F** telles que $\mathrm{alt}(\varphi) \leqslant n$ et $\mathbf{F}_n^k$ la classe des formules de $\mathbf{F}_n$ utilisant au

plus k variables. On note également $\mathbf{\Sigma}_n$ les formules de **FO** équivalente à une formule en *forme normale prénexe* dans laquelle le préfixe de quantification est une suite alternée de blocs de quantificateurs existentiels et universels (possiblement vides), commençant par un bloc de quantificateurs existentiels. On notera également $\mathcal{B}\mathbf{\Sigma}_n$ l'ensemble des combinaisons booléennes des formules de $\mathbf{\Sigma}_n$. Pour plus de précisions sur ces classes de formules on se reportera par exemple à l'article [24].

Proposition 1.10.

Soient $\mathbf{F}$ un fragment, k et n deux entiers. Les classes $\mathcal{B}\mathbf{\Sigma}_n$, $\mathbf{F}^k$ et $\mathbf{F}_n$ sont également des fragments.

Démonstration : Soient φ et ψ appartenant à $\mathbf{F}_n^k$. Les formules $\varphi \wedge \psi$ et $\varphi \vee \psi$ utilisent au plus k symboles de variables et comme

$$\mathrm{alt}(\varphi \wedge \psi) = \mathrm{alt}(\varphi \vee \psi) = \max\{\mathrm{alt}_\exists(\varphi), \mathrm{alt}_\forall(\psi)\}$$

on a $\varphi \wedge \psi$ et $\varphi \vee \psi$ appartiennent à $\mathbf{F}_n^k$. De même, les substitutions atomiques dans l'énoncé φ n'introduisent ni quantification ni symbole de variable supplémentaires. La classe de formules $\mathbf{F}_n^k$ est donc un fragment.

Soient φ et ψ appartenant à $\mathcal{B}\mathbf{\Sigma}_n$. Par définition, les énoncés $\varphi \wedge \psi$ et $\varphi \vee \psi$ appartiennent également à $\mathcal{B}\mathbf{\Sigma}_n$. De même, les substitutions atomiques dans l'énoncé φ n'introduisent aucune quantification supplémentaire. La classe de formules $\mathcal{B}\mathbf{\Sigma}_n$ est donc un fragment. ■

1.3.5 Les jeux d'Ehrenfeucht-Fraïssé

Les *jeux d'Ehrenfeucht-Fraïssé* empruntent au vocabulaire de la théorie des jeux afin de décrire le comportement de fragments logiques classiques. Il s'agit d'un des moyens les plus efficaces pour obtenir des résultats de non-définissabilité d'un langage dans un fragment. Nous allons présenter ces jeux uniquement pour le premier ordre classique ; ils pourraient toutefois être étendus au premier ordre modulaire et même à la logique monadique du second ordre. Pour une exposition plus complète des jeux d'Ehrenfeucht-Fraïssé, on pourra se référer au livre de Libkin [46, page 32].

Le jeu pour **FO** se déroule ainsi : fixons une signature σ comportant un nombre fini de prédicats et prenons deux mots u et v. Le jeu d'Ehrenfeucht-Fraïssé se joue à deux joueurs, *Spoiler* et *Duplicateur*. Ils disposent de jetons numérotés qu'ils déposeront à tour de rôle sur les mots. Spoiler commence le $k^{\text{ème}}$ tour en choisissant un mot, disons u. Sur ce mot, il choisit une position et y place son $k^{\text{ème}}$ jeton. Duplicateur choisit une position sur le mot v et y place également un jeton. En ayant placé ces jetons, Spoiler et Duplicateur ont défini deux triplets $S_u = ([|u|], \sigma_u, \mathcal{I}_u)$ et $S_v = ([|v|], \sigma_v, \mathcal{I}_v)$ avec pour $i \leqslant k$, $\mathcal{I}_u(x_i)$ est la position du jeton étiqueté par i sur u (et de même pour $\mathcal{I}_v$). Ces triplets sont dits

isomorphes si pour tout k-uplet $(y_1, \ldots, y_t)$ d'éléments de la pré-image de $\mathcal{I}_u$ et de $\mathcal{I}_v$ et pour tout prédicat P de la signature,

$$(\mathcal{I}_u(y_1), \ldots, \mathcal{I}_u(y_t)) \in P_u \text{ si et seulement si } (\mathcal{I}_v(y_1), \ldots, \mathcal{I}_v(y_t)) \in P_v.$$

Spoiler gagne le jeu quand les structures ne sont plus isomorphes. Il dispose d'une *stratégie gagnante* en k tours, si quels que soient les choix de Duplicateur, il gagne le jeu en moins de k tours.

Théorème 1.11.

Soit σ une signature finie et L un langage. Les deux conditions suivantes sont équivalentes.

(1) Le langage L est définissable dans **FO** sur la signature σ.
(2) Il existe un entier k tels que pour tout mot $(u, v) \in L \times L^c$, Spoiler dispose d'une stratégie gagnante en k tours pour le jeu d'Ehrenfeucht-Fraïssé sur (u, v) et la signature σ.

Pour étudier la complexité fine de **FO**, on peut restreindre certains paramètres du jeu. Ainsi, le jeu d'Ehrenfeucht-Fraïssé *se joue avec p variables* si chaque joueur dispose de p-jetons étiquetés (indépendamment du nombre de tours). Pour que le nombre de tours ne soit pas borné par le nombre de variables, on suppose qu'au début de chaque tour, si les joueurs ont épuisé leurs jetons, alors ils ramassent deux jetons plus anciens. L'alternance de quantification coïncide, elle, avec une limitation pour Spoiler du nombre de fois où il est autorisé à changer de mots. Le théorème suivant n'est pas énoncé le livre de Libkin [46]. Toutefois, ce résultat est bien connu, et une preuve peut être adaptée de la preuve du théorème précédant.

Théorème 1.12.

Soit σ une signature finie et L un langage. Les deux conditions suivantes sont équivalentes.

(1) Le langage L est définissable dans $\mathbf{FO}_n^p$ sur la signature σ.
(2) Il existe un entier k tels que pour tout mot $(u, v) \in L \times L^c$, Spoiler dispose d'une stratégie gagnante en k tours pour le jeu d'Ehrenfeucht-Fraïssé utilisant p variables et autorisant n alternances sur (u, v) et la signature σ.

Remarque : Dans cette thèse, les jeux d'Ehrenfeucht-Fraïssé seront utilisés dans une unique preuve : celle du théorème 6.10. On y utilisera les jeux à deux jetons.

1.4 Le théorème d'ajout de prédicats au plus unaires

Nous ajouterons à plusieurs reprises (voir Théorèmes 3.24, 4.15 et la proposition 6.23) des prédicats, au plus unaires, à un fragment logique. Le théorème suivant sera notre principale *interface* avec les fragments logiques ; il est énoncé afin de ressembler au *principe du produit en couronne* que nous introduirons dans les chapitres suivants. L'idée principale de ce théorème est que l'ajout de prédicats unaires peut-être géré *localement* en ajoutant de *l'information* supplémentaire directement dans l'alphabet. Ceci utilise fortement le fait que les prédicats sont unaires.

Introduisons maintenant certaines notations afin de formaliser cette idée. Soit $\kappa = (P_0, \dots, P_{k-1})$ un k-uplet de prédicats (pas forcément numériques) unaires et A un alphabet fini. On pose $B_k = A \times \mathcal{P}([k])$. À un mot $u = u_0 \cdots u_{n-1}$ de A^* on associe un mot $\overline{u} = (u_0, \beta_0) \cdots (u_{n-1}, \beta_{n-1})$ de B_k^* avec $j \in \beta_i$ si et seulement si $i \in E_j$ où E_j est l'interprétation de P_j dans u.

Exemple : Prenons $\kappa = (\mathbf{a_{-1}}, \mathbf{b_{-1}})$ et le mot $u = abaa$. On a alors

$$\begin{aligned} E_0 &= \{1, 3\}, \\ E_1 &= \{2\}, \\ \overline{u} &= (a, \emptyset)(b, \{0\})(a, \{1\})(a, \{0\}). \end{aligned}$$

Notations : On appelle les mots de B_k^* de la forme $\overline{u}$ les mots *bien formés*. On notera K_κ le langage des mots bien formés. On appelle également π_k la projection de B_k^* vers A^*.

Soient $\mu = (Q_0, \dots, Q_{t-1})$ un t-uplet de prédicats d'arité 0 et soit $E \subset \{0, \dots, t-1\}$. On note T_E le langage suivant :

$$T_E = \big\{ u \in A^* \mid \ \{i \mid u \text{ satisfait } Q_i\} = E \big\}.$$

En posant $L(Q_i)$ l'ensemble des mots satisfaisant Q_i on obtient que

$$T_E = \bigcap_{i \in E} L(Q_i) - \bigcup_{i \notin E} L(Q_i).$$

Théorème 1.13 (Théorème d'ajout des prédicats unaires).

Soient $\mathbf{F}$ un fragment, A un alphabet fini, $\mathcal{C}$ une classe de prédicats d'arité au plus 1 et L un langage de A^*. Les deux conditions suivantes sont équivalentes.

(1) Le langage L appartient à $\mathbf{F}[\mathcal{C}](A^*)$.

(2) Il existe un t-uplet $(Q_0, \dots, Q_{t-1})$ de prédicats d'arité 0 de la classe $\mathcal{C}$, un k-uplet $\kappa = (P_0, \dots, P_{k-1})$ de prédicats unaires de la classe $\mathcal{C}$, et pour tout $E \in \mathcal{P}([t])$, il existe un langage L_E appartenant à $\mathbf{F}(B_k^*)$, tels que

$$L = \bigcup_{E \in \mathcal{P}([t])} T_E \cap \pi_k(L_E \cap K_\kappa). \qquad (*)$$

Démonstration :

(**1**) $\rightarrow$ (**2**). Notons φ la formule de $\mathbf{F}[\mathcal{C}]$ définissant le langage L. Soient $\{Q_0, \ldots, Q_{t-1}\}$ les prédicats d'arité 0 de $\mathcal{C}$ apparaissant dans φ et $\kappa = (P_0, \ldots, P_{k-1})$ le j-uplet des prédicats d'arité 1 de $\mathcal{C}$ apparaissant dans φ. La formule φ est équivalente à la formule

$$\bigvee_{E \in \mathcal{P}([t])} \bigwedge_{i \in E} Q_i \wedge \bigwedge_{i \notin E} \neg Q_i \wedge \varphi_E,$$

où pour chaque E, φ_E est la formule obtenue à partir de φ en remplaçant chaque prédicat Q_i avec $i \in E$ par *vrai* et chaque prédicat Q_i avec $i \notin E$ par *faux*. Comme $\mathbf{F}$ est stable par substitution atomique, la formule φ_E est dans $\mathbf{F}[\mathcal{C}](A^*)$. De plus tous les prédicats d'arité 0 de $\mathcal{C}$ apparaissant dans φ ont été remplacés soit par *vrai* soit par *faux* et n'apparaissent pas dans la formule φ_E. Pour chaque formule φ_E, on construit une formule ψ_E en remplaçant chaque occurrence de $\mathbf{a}(x)$ pour chaque lettre a et chaque symbole de variable du premier ordre x, par la formule atomique

$$\bigvee_{\beta \in \mathcal{P}([t])} \boldsymbol{(\mathbf{a}, \beta)}(x).$$

Pour $i \in [t]$, on remplace chaque occurrence du prédicat $P_i(x)$ par la formule atomique

$$\bigvee_{a \in A \text{ et } \beta \in \mathcal{P}([t]) \text{ tels que } i \in \beta} \boldsymbol{(\mathbf{a}, \beta)}(x).$$

Les prédicats $\boldsymbol{(\mathbf{a}, \beta)}(x)$ sont des prédicats de lettre sur l'alphabet B_k. Comme $\mathbf{F}$ est stable par substitution atomique, la formule ψ_E ainsi créée est dans $\mathbf{F}$. On remarque que pour tout mot $u \in T_E$, le mot u satisfait φ_E si et seulement si $\overline{u}$ satisfait ψ_E. C'est pourquoi

$$L = \bigcup_{E \in \mathcal{P}([t])} T_E \cap \pi_k(L_E \cap K_\kappa)$$

où L_E est le langage défini par la formule ψ_E sur l'alphabet B_k.

(**2**) $\rightarrow$ (**1**). Partons de la formule $(*)$. Pour chaque $E \in \mathcal{P}([t])$, il existe une formule ψ_E de $\mathbf{F}$ définissant le langage L_E. Pour chaque formule ψ_E on définit une formule φ_E en substituant chaque prédicat de lettre $\boldsymbol{(\mathbf{a}, \beta)}(x)$ par la formule atomique

$$\mathbf{a}(x) \wedge \bigwedge_{i \in \beta} P(x) \wedge \bigwedge_{i \notin \beta} \neg P(x).$$

On remarque que pour tout mot $u \in T_E$, le mot u satisfait φ_E si et seulement si $\overline{u}$ satisfait ψ_E. Finalement, on pose :

$$\varphi = \bigvee_{E \in \mathcal{P}([t])} \bigwedge_{i \in E} Q_i \wedge \bigwedge_{i \notin E} \neg Q_i \wedge \varphi_E,$$

Cette formule se trouve dans le fragment $\mathbf{F}[\mathcal{C}]$, et définit le langage L, ce qui conclut la preuve. ■

Première partie

Prédicats réguliers

Introduction

Les fragments logiques sont perçus, dans cette thèse, comme des *langages de programmation* pour automates finis et pour circuits booléens. Les différents fragments coïncident avec certaines notions de complexité. Dans le cas des circuits, il s'agit de *complexité booléenne* tandis que dans le cas des automates, il s'agit de *complexité algébrique*. L'objectif de cette première partie est d'étudier le comportement des fragments lorsque l'on ajoute des prédicats à la signature. 'est-à-dire, lorsque l'on ajoute pouvoir expressif du fragment. Nous nous concentrerons sur des résultats dits de *transfert*, où nous enrichirons la signature d'un fragment tout en propageant des résultats de *séparation* et de *décidabilité*.

La séparation consiste à prouver qu'un fragment est strictement plus expressif qu'un autre. Les questions classiques de séparation concernent, par exemple, la structure fine du premier ordre. De nombreux résultats de séparation sont connus dans le cadre d'une signature contenant uniquement l'ordre. Nous allons montrer qu'il est possible de les transférer à la signature contenant tout ou partie des prédicats réguliers.

De nombreux résultats sont connus lorsque l'on considère uniquement le prédicat numérique d'ordre. Certains résultats de transfert de séparations seront obtenus dans le cadre des langages réguliers mais également, dans les derniers chapitres de cette thèse, pour des classes de langages bien plus expressives (voir chapitre 7).

La décidabilité consiste à *décider algorithmiquement* la définissabilité d'un langage dans un fragment. Ici encore, dans le cas où la signature ne contient que le prédicat numérique d'ordre, de nombreux résultats sont connus. Des résultats de transfert concernant l'ajout de prédicats numériques locaux à la signature ont été étudiés et traités en grande partie par Straubing [63] et Tilson [73]. Toutefois, il n'existe pas de théorème général sur le sujet car l'ajout des prédicats numériques locaux ne semble pas correspondre à une opération algébrique connue. Ce problème peut être contourné en étudiant l'ajout des prédicats descriptifs locaux, qui a le bon goût de correspondre à un *produit en couronne*, grâce au théorème 1.13. Dans la plupart des fragments, l'ajout des prédicats descriptifs locaux définit la même classe de langages que l'ajout des prédicats numériques locaux. Il existe néanmoins un contre-exemple (voir la proposition 3.49).

Il est également possible d'ajouter des prédicats modulaires à la signature. Cela est nécessaire pour étudier les fragments sur la totalité des prédicats numériques réguliers, comme cela a été fait par Maciel, Péladeau et Thérien [47] ainsi que par Straubing [66], dans le contexte de l'étude des langages réguliers dans les restrictions de $\mathbf{NC^1}$. Ce dernier auteur a introduit les notions clefs que sont l'*indice de stabilité* et le *semigroupe stable*. Ces travaux ont été poursuivis par Chaubard, Pin et Straubing [20], dans le cadre de l'ajout des prédicats modulaires au premier niveau de la hiérarchie fine du premier ordre. L'objectif d'obtenir un théorème général qui marcherait pour un grand nombre de fragments semble raisonnable mais se heurte à la question du *délai*.

En effet, que ce soit pour l'ajout des prédicats modulaires ou des prédicats locaux, la question du délai est centrale. Intuitivement il s'agit d'être capable de décider d'un *indice*, en fonction du langage que l'on souhaite définir, qui bornerait la taille de la signature que l'on ajoute au fragment. Dans le cas des prédicats locaux, un indice de délai a été

déterminé par Straubing [63] : la taille du *monoïde syntaxique*. Pour les prédicats modulaires, l'indice de stabilité semble être un bon candidat. Dans un travail conjoint avec Luc Dartois, nous avons établi un certain nombre de conditions suffisantes pour calculer un indice de délai (voir Théorèmes 4.34 et 4.39) recouvrant ainsi de nombreux cas.

Avant de rentrer dans le vif du sujet, discutons de l'organisation de l'introduction des définitions algébriques. Chacun de ces trois chapitres s'ouvre sur une présentation d'un nouvel *objet* algébrique. Ainsi le premier chapitre présentera les définitions propres à la théorie des variétés de monoïdes, le deuxième chapitre celles de la théorie des *ne*-variétés de timbres, enfin le dernier chapitre exposera la moins usuelle théorie des *mu*-variété de timbres. Il eût été possible de tout regrouper dans un chapitre introductif algébrique, allégeant d'autant la présentation des second et troisième chapitres. Toutefois, il y a une cohérence à introduire les objets algébriques au moment ou la théorie présentée n'est plus suffisante pour capturer l'expressivité d'un fragment. Le prix malheureux à payer pour profiter de cette cohérence est une forme de redondance ainsi qu'une certaine lourdeur, dans l'exposition de ces différentes théories.

Les principales contributions présentes dans cette première partie de thèse sont les suivantes :

- Le théorème 3.24 d'ajout des prédicats descriptifs locaux et le théorème 4.15 d'ajout des prédicats modulaires sont des résultats, à ma connaissance, nouveaux. Dans le cas des prédicats locaux, le résultat était suspecté et prouvé pour de nombreux fragments. Ce sont des conséquences du théorème 1.13 d'ajout des prédicats unaires qui lui-même repose sur la notion de fragments, propre à cette thèse.
- Les théorèmes de délai pour MOD : théorèmes 4.34 et 4.39 sont les contributions les plus importantes. Ils permettent d'obtenir, ou de reprouver, un grand nombre de résultats de décidabilité comme le montrent les tableaux récapitulatifs de la section 4.6.

De nombreuses questions intéressantes restent ouvertes. La décidabilité de la complexité fine de **FO** par exemple (ou conjecture de la Dot-Depth). Les questions suivantes ont également été étudié.

- La décidabilité du fragment $(\mathbf{FO} + \mathbf{MOD})^2[<]$: une description algébrique obtenue par Straubing et Thérien [69] est encourageante, mais cette question reste malheureusement ouverte.
- Un théorème de délai pour le produit en couronne par **MOD** : un tel résultat pourrait prendre deux formes, une version forte établirait que l'indice de stabilité convient systématiquement pour toutes les variétés. Une version plus faible se contenterait de donner une borne calculable. Ce résultat permettrait de prouver des résultats de transfert de décidabilité pour de nombreux fragments.
- Il est connu que l'ajout des prédicats descriptifs locaux ne préserve pas la décidabilité, (voir l'article d'Auinger [8]). Obtenir un résultat similaire pour l'ajout des prédicats modulaires pourrait être intéressant. Au vu de la structure du théo-

rème 4.28 de la catégorie dérivée pour le produit en couronne par **MOD**, je suspecte cette question d'être plus difficile qu'il n'y paraît. En effet, la structure des catégories que l'on teste sur le global de la variété est très contrainte, contrairement au cas du produit en couronne par **D**.

Chapitre 2

Le prédicat d'ordre linéaire

et la théorie des variétés de monoïdes finis

Les objectifs de ce chapitre consistent à :

- Introduire dans un premier temps les concepts indispensables de *semigroupes*, de *monoïdes*, de *variétés de monoïdes finis* ainsi que la théorie du *profini* (partie 2.1).
- Puis, nous utiliserons ces concepts afin de caractériser des classes de langages définies par des fragments logiques présentés dans le premier chapitre. Nous nous restreindrons à trois signatures différentes. La signature vide, la signature ne contenant que le prédicat numérique d'égalité et, la plus intéressante, la signature contenant uniquement le prédicat numérique d'ordre linéaire. Plus précisément, nous exposerons dans la partie 2.2 des résultats autour du premier ordre et dans la partie 2.3 des résultats concernant la restriction à deux variables et sa structure fine.

Les résultats introduits dans ce chapitre serviront pour les deux chapitres suivants. En particulier, les équivalences entre fragments logiques et variétés de monoïdes seront exploitées à de nombreuses reprises afin d'étudier l'enrichissement de la signature.

2.1 Variété de monoïdes finis

Rappelons avant toute chose quelques définitions. Un *semigroupe* est un ensemble muni d'une loi de composition interne associative et un *monoïde* est un semigroupe disposant d'un élément neutre noté 1.

Notation : On essayera, autant que possible, de noter un monoïde à l'aide des lettres M et N et les semigroupes à l'aide des lettres S et T.

La loi de composition interne est, de manière usuelle, notée multiplicativement. On rappelle également qu'un idempotent est un élément e vérifiant $e^2 = e$.

Exemple : L'ensemble A^* des mots finis équipé de la concaténation forme un monoïde qu'on appelle le *monoïde libre* sur A et l'ensemble A^+ des mots finis différents du mot vide forme un semigroupe qu'on appelle le *semigroupe libre* sur A .

Soient S et T deux semigroupes. Le produit cartésien $S \times T$, muni de la *loi produit*, est un semigroupe. L'ensemble des parties $\mathcal{P}(S)$ est également un semigroupe si on définit le produit de deux sous-ensembles de S comme le sous-ensemble des produits de leurs éléments. Par abus de notation, pour $E \in \mathcal{P}(S)$ et $x \in S$, on notera xE et Ex les ensembles $\{x\}E$ et $E\{x\}$. Une application $\eta : S \to T$ est un *morphisme de semigroupes* si pour tout élément x et y dans S, alors $\eta(xy) = \eta(x)\eta(y)$. Une application $\eta : M \to N$ est un *morphisme de monoïdes* si c'est un morphisme de semigroupes et si $\eta(1) = 1$. Un *timbre* est un morphisme surjectif d'un monoïde libre finiment engendré vers un monoïde fini. Soit S un semigroupe. L'ensemble T est un *sous-semigroupe* de S si $T \subseteq S$ et si pour tout x et y dans T, xy est également dans T. De même, pour M un monoïde, N est un *sous-monoïde* de M si c'est un sous-semigroupe et si le neutre de M appartient à N. Le semigroupe T est un *quotient* de S s'il existe un morphisme surjectif de S dans T. La notion de quotient s'étend naturellement aux monoïdes. On dit que T *divise* S (noté $T \preccurlyeq S$) si T est un quotient d'un sous-semigroupe de S. La notion de division s'étend naturellement aux monoïdes. Un *morphisme relationnel de monoïdes*, noté $\tau : M \to N$, est une application $\tau : M \to \mathcal{P}(N)$ telle que $1_N \in \tau(1_M)$, $\tau(x) \neq \emptyset$ et $\tau(x)\tau(y) \subseteq \tau(xy)$ pour tout $x, y \in M$. Un morphisme relationnel est *injectif* si pour tout $m, m' \in M$, la condition $m \neq m'$ implique que $\tau(m)$ et $\tau(m')$ sont disjoints. Les résultats suivants sont bien connus.

Proposition 2.1.

- La composition de deux morphismes relationnels est un morphisme relationnel.
- Les morphismes sont des morphismes relationnels.
- Les morphismes inverses de morphismes surjectifs sont des morphismes relationnels.
- Un monoïde N divise un monoïde M si et seulement s'il existe un morphisme relationnel injectif de N vers M.

Une *congruence* d'un semigroupe est une relation d'équivalence stable par produit. Si S est un semigroupe et $\sim$ une congruence de S, alors $S/\sim$ est un semigroupe quotient de S. Enfin, on introduit les notations suivantes.

Notations : Soit S un semigroupe.

- On pose
$$S^1 = \begin{cases} S \text{ si } S \text{ est un monoïde,} \\ S \cup \{1\} \text{ avec 1 vérifiant } 1x = x1 = x \text{ sinon.} \end{cases}$$
- On note $E(S)$ l'ensemble des idempotents de M.
- Pour toute partie P de S, on note $\langle P \rangle$ le sous-semigroupe engendré par P, c'est-à-dire, le plus petit sous-semigroupe de S contenant P.

Si S est un semigroupe fini, alors pour chaque élément x de S, il existe un plus petit entier n tel que x^n soit idempotent. De plus, pour tout m tel que x^m est idempotent, on a $x^m = x^n$. On appelle alors x^n *la puissance d'idempotence* de x et on la note x^ω.

Définition 2.2 (Variété de monoïdes finis).

Une classe de monoïdes finis est une (pseudo-)variété si elle est stable par produit direct et division de monoïdes.

Notation : Le terme *pseudo-variété* ne sera plus, par la suite, utilisé. Les variétés de monoïdes finis seront notées en gras : $\mathbf{V}, \mathbf{W}, \ldots$

Soient A et B deux alphabets finis de même taille et $\sigma : A \to B$ une bijection. On note également $\sigma : A^* \to B^*$ le morphisme de monoïdes libres qui étend σ. Une *classe de langages* est une correspondance $\mathcal{F}$ qui associe à chaque alphabet A un ensemble $\mathcal{F}(A^*)$ de langages de A^* telle que pour toute bijection $\sigma : A \to B$, un langage L appartient à $\mathcal{F}(A^*)$ si et seulement si $\sigma(L)$ appartient à $\mathcal{F}(B^*)$. Il suit que, si on fixe pour chaque entier positif n un alphabet $A_n = \{a_1, \ldots, a_n\}$, alors la classe $\mathcal{F}$ est complètement déterminée par la famille $(\mathcal{F}(A_n^*))_{n\in\mathbb{N}}$.

Une classe $\mathcal{C}$ de langages est stable par *image inverse de morphisme* si pour tout morphisme $\eta : A^* \to B^*$ et tout langage L de B^*, $L \in \mathcal{C}(B^*)$ implique $\eta^{-1}(L) \in \mathcal{C}(A^*)$. Enfin, une classe $\mathcal{C}$ de langages est stable par quotient si pour tout langage L de $\mathcal{C}(A^*)$ et tout mot u de A^*, les langages $u^{-1}L$ et Lu^{-1} sont également dans $\mathcal{C}(A^*)$.

Définition 2.3 (Variété de langages).

Une classe de langages réguliers est une variété de langages si elle est close par opération booléenne, par image inverse de morphisme et par quotient.

Remarque : Les variétés de langages seront souvent notées à l'aide de caractères calligraphiques : $\mathcal{V}, \mathcal{W}, \ldots$.

Un langage L sur l'alphabet A est *reconnu* par un morphisme η s'il existe un un sous-ensemble P de M tels que $L = \eta^{-1}(P)$. Il est *reconnu* par un monoïde M s'il existe un morphisme $\eta : A^* \to M$ tel que η le reconnaît. Soient u et v deux mots de A^*. On dit que u et v sont *L-syntaxiquement équivalents*, ce qui est noté $u \equiv_L v$, si pour tous mots $s, t \in A^*$, *sut* appartient à L si et seulement si *svt* appartient à L. On notera $[u]_L$ la classe de u pour la congruence $\equiv_L$.

Définition 2.4 (Monoïde et morphisme syntaxique).

Soit L un langage. On appelle le monoïde $A^*/\equiv_L$ le monoïde syntaxique de L et l'application $u \mapsto [u]_L$ son morphisme syntaxique.

Le théorème suivant nous sera utile pour la suite. Il résume certaines des relations connues pour les objets que nous avons introduits.

Théorème 2.5 (Folklore).

Soit L un langage. Les conditions suivantes sont équivalentes.

(1) Le langage L est régulier.
(2) Le langage L est reconnu par un monoïde fini.
(3) La congruence $\equiv_L$ est d'indice fini.
(4) Le monoïde syntaxique de L est fini.

Notations : On notera M_L et η_L, respectivement, le monoïde syntaxique et le morphisme syntaxique de L.

La proposition suivante nous sera utile. Elle énonce que le morphisme syntaxique d'un langage régulier L se factorise à travers tout morphisme surjectif reconnaissant L.

Proposition 2.6 (Folklore).

Soient L un langage régulier de A^* et $\eta : A^* \to M$ un morphisme surjectif reconnaissant le langage L. Il existe un morphisme surjectif $\psi : M \to M_L$ tel que

$$\eta_L = \psi \circ \eta.$$

La proposition suivante établit que les langages reconnus par les monoïdes d'une variété de monoïdes finis, forment une variété des langages.

Proposition 2.7.

Soit $\mathbf{V}$ une variété de monoïdes finis. La classe des langages réguliers reconnus par les monoïdes de $\mathbf{V}$ forme une variété de langages.

Il existe une construction réciproque à cette proposition. En effet, à une variété de langages, on peut associer la variété des monoïdes finis engendrée par les monoïdes syntaxiques des langages de cette variété de langages. Le théorème d'Eilenberg [25] (ou théorème de la variété) établit que ces correspondances sont mutuellement bijectives. On dit qu'une variété est *décidable* s'il existe un algorithme permettant de décider si un monoïde fini appartient à une variété. On parle également du *problème de l'appartenance* à une variété de monoïdes.

2.1.1 Représentation des semigroupes et relations de Green

Les relations de Green jouent un rôle particulier dans l'étude de la *structure* des monoïdes. Elles permettent, entre autre, de fournir la représentation en diagramme *boîte-à-œufs*. Soient S un semigroupe et s, t deux éléments de S. Nous définissons les quatre

préordres suivants :

$$s \leqslant_{\mathcal{R}} t \text{ si et seulement si } sS^1 \subseteq tS^1$$
$$s \leqslant_{\mathcal{L}} t \text{ si et seulement si } S^1s \subseteq S^1t$$
$$s \leqslant_{\mathcal{J}} t \text{ si et seulement si } S^1sS^1 \subseteq S^1tS^1$$
$$s \leqslant_{\mathcal{H}} t \text{ si et seulement si } s \leqslant_{\mathcal{R}} t \text{ et } s \leqslant_{\mathcal{L}} t$$

Les relations de Green [30] sont les *clôtures symétriques* de ces préordres :

$$s \mathcal{R} t \text{ si et seulement si } s \leqslant_{\mathcal{R}} t \text{ et } t \leqslant_{\mathcal{R}} s \text{ si et seulement si } sS^1 = tS^1$$
$$s \mathcal{L} t \text{ si et seulement si } s \leqslant_{\mathcal{L}} t \text{ et } t \leqslant_{\mathcal{L}} s \text{ si et seulement si } S^1s = S^1t$$
$$s \mathcal{J} t \text{ si et seulement si } s \leqslant_{\mathcal{J}} t \text{ et } t \leqslant_{\mathcal{J}} s \text{ si et seulement si } S^1sS^1 = S^1tS^1$$
$$s \mathcal{H} t \text{ si et seulement si } s \leqslant_{\mathcal{H}} t \text{ et } t \leqslant_{\mathcal{H}} s \text{ si et seulement si } s \mathcal{R} t \text{ et } s \mathcal{L} t$$

Enfin, la relation $\mathcal{D}$ est la composition de $\mathcal{R}$ et de $\mathcal{L}$. La représentation (graphique) des semigroupes n'est pas toujours aisée. Nous les représenterons à l'aide de leur *diagramme boîte-à-œufs*. Ces derniers seront réalisés à l'aide du logiciel Semigroupe 2 [50]. Chaque $\mathcal{D}$-classe est représentée par une grille où chaque ligne représente une $\mathcal{R}$-classe, chaque colonne représente une $\mathcal{L}$-classe, et les intersections d'une ligne et d'une colonne, c'est-à-dire chaque cellule de la grille, représente une $\mathcal{H}$ classe.

Exemple : Représentations du monoïde syntaxique du langage $A^*(aaba)A^* \cup (aa)^*$:

^{*1}

b	a

ab

$^*a^2$	a^3

$^*ab^2a^2$	$^*ab^2a$	a^2b	$^*ab^2$
aba^2	aba	aba^2b	$^*abab$
ba^2	$^*ba$	$^*ba^2b$	$^*bab$
$^*b^2a^2$	$^*b^2a$	$^*b^2a^2b$	$^*b^2$

$^*a^2ba$

2.1.2 La théorie profinie des variétés de monoïdes finis

La théorie profinie donne une description *topologique* des variétés de monoïdes finis. En particulier, elle permet d'établir que toute variété peut être décrite à l'aide *d'identités*

profinies. De ces identités, on arrive parfois (malheureusement pas toujours) à obtenir des critères de décidabilité pour le problème de l'appartenance à la variété. Présentons maintenant les définitions nécessaires à ces descriptions topologiques.

Complétion d'un espace métrique

Un espace métrique est un couple (X, d) pour X un ensemble et d une *distance* sur X, c'est-à-dire, pour $d : X \times X \to [0, +\infty[$ vérifiant pour tout $x, y, z \in E$:

(1) $d(x, y) = 0$ si et seulement si $x = y$ (séparée),

(2) $d(x, y) = d(y, x)$ (symétrique)

(3) $d(x, z) \leqslant d(x, y) + d(y, z)$ (inégalité triangulaire).

Soit (X, d) un espace métrique. Une *suite de Cauchy* de (X, d) est une suite (u_n) de X vérifiant que pour tout $\varepsilon > 0$ il existe $N \in \mathbb{N}$ tel que pour tous $n, m > N$, $d(u_n, u_m) \leqslant \varepsilon$. La suite (u_n) est *convergente* s'il existe $u \in X$ tel que pour tout $\varepsilon > 0$, il existe $N \in \mathbb{N}$ tel que pour tout $n > N$, $d(u_n, u) < \varepsilon$. On note alors $u = \lim u_n$. Soit (E', d') un autre espace métrique. Une application $f : (E, d) \to (E', d')$ est *uniformément continue* si pour tout $\varepsilon > 0$ il existe $\delta > 0$ tel que pour tout $x, y \in E$, $d(x, y) < \delta$ implique $d(f(x), f(y)) < \varepsilon$. L'image d'une suite de Cauchy par une application uniformément continue est une suite de Cauchy. On dit que deux suites de Cauchy (u_n) et (v_n) sont équivalentes si la suite entremêlée $u_0, v_0, u_1, v_1, \ldots$ est également une suite de Cauchy.

Un espace métrique (X, d) est *complet* si toute suite de Cauchy est convergente. Il est dit *compact* si toute suite possède une sous-suite convergente.

On note $\widehat{X}$ l'ensemble des classes d'équivalence des suites de Cauchy de X. On définit également :

$$\widehat{d} : \begin{cases} \widehat{X} \times \widehat{X} & \to [0, +\infty[\\ ((u_n), (v_n)) & \mapsto \lim d(u_n, v_n). \end{cases}$$

L'application $\widehat{d}$ est bien définie car $(d(u_n, v_n))$ est une suite de Cauchy de $[0, +\infty[$ qui est un espace métrique complet. La proposition suivante est un résultat classique sur les espaces métriques.

Proposition 2.8.

L'espace $(\widehat{X}, \widehat{d})$ est un espace métrique complet.

On appelle $(\widehat{X}, \widehat{d})$ la *complétion* de (X, d).

Notation : Lorsque la distance sera claire selon le contexte, on notera abusivement $\widehat{X}$ l'espace métrique $(\widehat{X}, \widehat{d})$.

On remarque qu'en utilisant des suites constantes, on peut plonger *canoniquement* X dans $\widehat{X}$. On utilisera également le résultat classique suivant.

Proposition 2.9.

Soient (E, d) et (E', d') deux espaces métriques et $f : (E, d) \to (E', d')$ une application uniformément continue. Il existe une unique fonction uniformément continue de $\widehat{E}$ vers $\widehat{E'}$ qui prolonge f. On la note $\widehat{f}$.

Soient (E_1, d_1) et (E_2, d_2) deux espaces métriques. On définit l'*espace métrique produit* $(E_1 \times E_2, d_p)$ par $d_p((u, u'), (v, v')) = \max\{d_1(u, v), d_2(u', v')\}$. On peut vérifier qu'il s'agit bien d'une distance. Un monoïde (M, d) est un *monoïde métrique* s'il s'agit d'un espace métrique complet et si la multiplication est uniformément continue. Soit M un monoïde fini et d l'application telle que pour tout $x, y \in M$, $d(x, y) = 1$ si $x \neq y$ et $d(x, x) = 0$. On peut vérifier que (M, d) est un monoïde métrique.

Le monoïde pro-V libre

Soient $\mathbf{V}$ une variété de monoïde, A un alphabet fini et $u, v \in A^*$. On définit :

$$r_{\mathbf{V}}(u, v) = \min\{|M| \mid \text{ il existe } \eta : A^* \to M, \text{ avec } M \in \mathbf{V} \text{ tel que } \eta(u) \neq \eta(v)\}.$$

Intuitivement, $r_{\mathbf{V}}$ quantifie la difficulté de *séparer deux mots* par des monoïdes de $\mathbf{V}$. On pose $u \sim_{\mathbf{V}} v$ si et seulement si ces deux mots ne sont pas séparables ($r_{\mathbf{V}}(u, v) = +\inf$). Cette relation est une congruence et donc $A^*/\sim_V$ est un monoïde.

Remarque : Dans la plupart des cas qui nous intéressent, la congruence $\sim_{\mathbf{V}}$ sera triviale, c'est-à-dire, tous les mots seront deux-à-deux séparables.

On note $\pi_{\mathbf{V}}$ le morphisme surjectif de A^* vers $A^*/\sim_V$ et on définit l'application

$$d_{\mathbf{V}} : \begin{cases} (A^*/\sim_{\mathbf{V}}) \times (A^*/\sim_{\mathbf{V}}) & \to [0, +\infty[\\ (u, v) & \mapsto 2^{-r_{\mathbf{V}}(u,v)} \end{cases}$$

Proposition 2.10.

L'espace $(A^*/\sim_{\mathbf{V}}, d_{\mathbf{V}})$ est un espace métrique.

Démonstration : Il suffit de vérifier que $d_{\mathbf{V}}$ est une distance. Par définition, il s'agit d'une application symétrique et séparée. Prouvons qu'elle satisfait l'inégalité triangulaire. Soient $u, v, w \in (A^*)$ et $\eta : A^* \to M$ qui sépare u de w. Alors M sépare soit u de v, soit v de w. En particulier,

$$d_{\mathbf{V}}(u, w) \leqslant \max\{d_{\mathbf{V}}(u, v), d_{\mathbf{V}}(v, w)\} \leqslant d_{\mathbf{V}}(u, v) + d_{\mathbf{V}}(v, w).$$

■

Proposition 2.11.

(1) Le produit de $A^*/\sim_{\mathbf{V}}$ est uniformément continu.
(2) Soient $M \in \mathbf{V}$ et $\eta : A^*/\sim_{\mathbf{V}} \to M$ un morphisme. L'application η est uniformément continue.
(3) L'application $\pi_{\mathbf{V}} : A^* \to A^*/\sim_{\mathbf{V}}$ est un morphisme de monoïdes uniformément continu.

On démontre par ailleurs [7, 51] le résultat suivant.

Proposition 2.12.

L'espace $(\widehat{A^*/\sim_{\mathbf{V}}}, \widehat{d_{\mathbf{V}}})$ est un monoïde métrique compact.

Si $\mathbf{V}$ est la variété de tous les monoïdes finis, alors la congruence $\sim_{\mathbf{V}}$ est triviale et on note $\widehat{A^*}$ l'espace $(\widehat{A^*}, \widehat{d_{\mathbf{V}}})$, que l'on appelle le monoïde *profini*. Pour toute autre variété $\mathbf{V}$, on notera $\widehat{F}_{\mathbf{V}}(A)$ cette complétion. Comme l'application $\pi_{\mathbf{V}}$ est uniformément continue, il existe une extension qu'on note abusivement $\pi_{\mathbf{V}} : \widehat{A^*} \to \widehat{F}_{\mathbf{V}}(A)$.

Une *identité profinie* sur l'alphabet A est un couple $(u, v) \in \widehat{A^*}^2$, que l'on note $u = v$. Un morphisme $\eta : A^* \to M$ *vérifie* l'identité profinie $u = v$ si $\widehat{\eta}(u) = \widehat{\eta}(v)$. Un monoïde M *vérifie* l'identité $u = v$ si pour tout morphisme $\eta : A^* \to M$, η vérifie cette identité.

Proposition 2.13.

Soit E un ensemble d'identités profinies. La classe des monoïdes qui vérifient toutes les identités de E est une variété de monoïdes finis.

Démonstration : Soient M et M' deux monoïdes vérifiant les identités de E. Soit $\psi : A^* \to M \times M'$ un morphisme. On note les projections $\pi_1 : M \times M' \to M$ et $\pi_2 : M \times M' \to M'$. Soit $(u = v) \in E$, comme $\widehat{\pi_1 \circ \psi}(u) = \widehat{\pi_1 \circ \psi}(v)$ et $\widehat{\pi_2 \circ \psi}(u) = \widehat{\pi_2 \circ \psi}(v)$, on a $\widehat{\psi}(u) = \widehat{\psi}(v)$.

Supposons maintenant que M vérifie les identités de E et que M' est un sous-monoïde de M et notons Id le morphisme identité de M' vers M. Soit $\psi : A^* \to M'$. Le morphisme $\mathrm{Id} \circ \psi$ de A^* vers M vérifie, par hypothèse, les équations de E, d'où ψ vérifie également les équations de E.

Enfin, supposons qu'il existe $\eta : M \to M'$ surjectif et soit $\psi : A^* \to M'$ un morphisme. Pour chaque lettre $a \in A$, comme η est surjectif, il existe au moins un élément m_a qui appartient à $\eta^{-1}(\psi(a))$. On définit le morphisme $\theta : A^* \to M$ par $\theta(a) = m_a$. Par

construction, $\psi = \eta \circ \theta$. Soit $(u = v) \in E$. Le monoïde M vérifie l'équation $(u = v)$ et donc $\widehat{\theta}(u) = \widehat{\theta}(v)$. Finalement $\widehat{\psi}(u) = \widehat{\psi}(v)$, ce qui conclut la preuve. ■

Notation : Soit E un ensemble d'identités profinies. On note $[\![E]\!]$ la variété des monoïdes qui vérifient ces identités.

Une variété $\mathbf{V}$ de monoïdes finis est définie par un ensemble d'identités profinies E si $\mathbf{V} = [\![E]\!]$.

Les ω-termes

Introduisons maintenant un outil important afin de décrire des ensembles d'identités profinies définissant une variété : les *ω-termes*.

Proposition 2.14.

Soit $u \in A^*$. La suite $(u^{n!})$ est de Cauchy.

Démonstration : Soit M un monoïde de taille n. On remarque que pour tout élément $m \in M$, il existe un entier $n_m \leqslant n$ tel que $m^{n_m} = m^\omega$ est idempotent. En particulier, cet entier divise $n!$ et donc $m^{n!} = m^\omega$. Donc pour tout morphisme $\eta : A^* \to M$, on a $\eta(u^{n!}) = \eta(u)^\omega$. De plus, pour tout $n' > n$, $\eta(u^{n'!}) = \eta(u^{n!})$, donc la suite $(u^{n!})$ est de Cauchy. ■

Notations : La suite $(u^{n!})$ converge dans $\widehat{A^*}$ et on note u^ω sa limite. On note également $u^{\omega+1} = \lim u^{n!+1}$ et $u^{\omega-1} = \lim u^{n!-1}$.

Pour tout morphisme $\eta : A^* \to M$, où M est un monoïde fini, on a $\widehat{\eta}(u^\omega) = \eta(u)^\omega$. En particulier, cela donne que $u^{2\omega} = u^\omega$. Enfin, le monoïde des ω-termes est le plus petit sous-monoïde de $\widehat{A^*}$, contenant A^* et clos par les opérations $u \mapsto u^\omega$, $u \mapsto u^{\omega+1}$ et $u \mapsto u^{\omega-1}$.

Remarques : Il est possible de vérifier algorithmiquement si une identité donnée sous la forme d'ω-termes est satisfaite par un monoïde. Il est donc possible d'en déduire des algorithmes de décision pour le problème de l'appartenance à une variété de monoïdes.

Quelques exemples importants

(1) La variété triviale : $\mathbf{I} = [\![x = 1]\!]$.
(2) La variété des monoïdes idempotents et commutatifs : $\mathbf{J_1} = [\![xy = yx, x^2]\!]$.
(3) La variété des monoïdes commutatifs : $\mathbf{Com} = [\![xy = yx]\!]$.
(4) La variété des groupes finis : $\mathbf{G} = [\![x^\omega = 1]\!]$.
(5) La variété des groupes résolubles : $\mathbf{G}_{\text{sol}}$.
(6) La variété des groupes abéliens : $\mathbf{Ab} = [\![x^\omega = 1, xy = yx]\!]$.

(7) La variété des monoïdes dont tous les groupes qui les divisent sont résolubles : $\mathbf{M}_{\text{sol}}$.
(8) La variété des monoïdes apériodiques : $\mathbf{A} = [\![x^{\omega+1} = x^\omega]\!]$. Il s'agit des monoïdes n'ayant pas de groupes qui les divisent.
(9) La variété des monoïdes apériodiques et commutatifs : $\mathbf{ACom} = [\![xy = yx, x^{\omega+1} = x^\omega]\!]$.
(10) La variété des monoïdes dont les $\mathcal{D}$-*classes* sont des semigroupes apériodiques : $\mathbf{DA} = [\![(xy)^\omega x(xy)^\omega = (xy)^\omega]\!]$.
(11) La variété des monoïdes $\mathcal{J}$-*triviaux* : $\mathbf{J} = [\![y(xy)^\omega = (xy)^\omega = x(yx)^\omega]\!]$.

2.2 Le premier ordre

L'un des intérêts du formalisme des variétés réside dans le fait que, sous réserve de contraintes syntaxiques, des classes de formules logiques seront équivalentes à des variétés de langages. En ce sens, le théorème de Büchi (voir Théorème 1.2) initia l'étude systématique des classes de langages réguliers définies par des fragments logiques. Le théorème suivant établit une caractérisation algébrique des langages définissables dans le premier ordre.

Théorème 2.15 (Schützenberger [58], McNaugton et Papert [48]).

Un langage régulier est définissable dans $\mathbf{FO}[<]$ si et seulement si son monoïde syntaxique est apériodique.

Une des conséquences de cette caractérisation est la possibilité de décider si un langage régulier est définissable par une formule de $\mathbf{FO}[<]$. En effet, il suffit de calculer son monoïde syntaxique (*via* son automate minimal) et de tester l'équation $[\![x^{\omega+1} = x^\omega]\!]$. Lorsqu'on enlève le prédicat d'ordre linéaire, le fragment logique devient beaucoup moins expressif. L'absence de prédicats binaires dans la signature permet de décomposer les formules en des formules n'utilisant qu'une seule variable. On en déduit la proposition suivante.

Proposition 2.16 (Folklore).

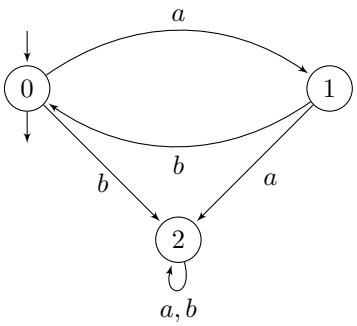
Les fragments $\mathbf{FO}[\emptyset]$ et $\mathbf{FO}^1[<]$ sont équivalents. En particulier, un langage régulier est définissable dans $\mathbf{FO}[\emptyset]$ si et seulement si son monoïde syntaxique est dans $\mathbf{J_1}$.

Étudions maintenant quelques exemples pour illustrer ces résultats.

Applications :

(1) Le langage $(ab)^*$:

Son monoïde syntaxique est apériodique mais n'est pas dans $\mathbf{J_1}$.

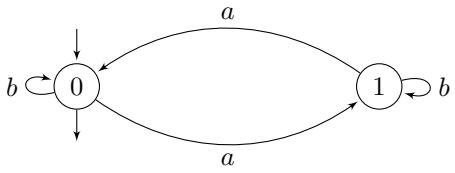


^{*1}

$^*ba$	b
a	$^*ab$

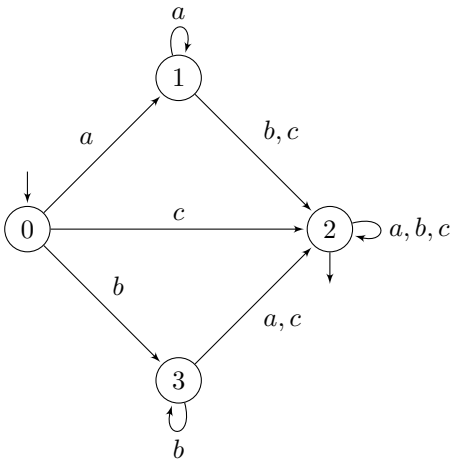
$^*a^2$

(2) Le langage *parité*, des mots ayant un nombre pair de a, ayant pour expression rationnelle $(b^*ab^*a)^*b^*$ a pour automate minimal :



Son monoïde syntaxique n'est donc pas apériodique, il s'agit du groupe $\mathbb{Z}/2\mathbb{Z}$.

(3) On pose $A = \{a, b, c\}$. Le langage des mots contenant soit un c, soit un a et un b $(A^*aA^* \cap A^*bA^*) \cup A^*cA^*$:



^{*1}

$^*b$	$^*a$

$^*c$

Son monoïde syntaxique est dans $\mathbf{J_1}$ et dans $\mathbf{A}$.

Dans son livre de 1994 [66], Howard Straubing a donné des preuves élégantes des caractérisations de la logique du premier ordre équipée de quantifications modulaires. Elles reposent en partie sur le théorème de décomposition de Krohn-Rhodes [42].

Théorème 2.17 (Straubing, Thérien et Thomas [70]).

- Un langage régulier est définissable dans $\mathbf{MOD}[<]$ si et seulement si son monoïde syntaxique est dans $\mathbf{G}_{sol}$.
- Un langage régulier est définissable dans $(\mathbf{FO} + \mathbf{MOD})[<]$ si et seulement si son monoïde syntaxique est dans la variété $\mathbf{M}_{sol}$.

On peut également étudier ces fragments en se restreignant à la signature ne contenant que l'égalité.

Proposition 2.18 (Folklore).

- Un langage régulier est définissable dans $(\mathbf{FO} + \mathbf{MOD})[=]$ si et seulement si son monoïde syntaxique est dans **Com**.
- Un langage régulier est définissable dans $\mathbf{FO}[=]$ si et seulement si son monoïde syntaxique est dans **ACom**.
- Un langage régulier est définissable dans $\mathbf{MOD}[=]$ si et seulement si son monoïde syntaxique est dans **Ab**.

Démonstration : Les deux derniers points sont des conséquences directes du premier point, du théorème 2.15 et du théorème 2.17. En effet, **ACom** est l'intersection de **Com** et de **A** et **Ab** est de plus l'intersection de **Com** et de $\mathbf{G}_{\text{sol}}$. On montre dans un premier temps que tout langage régulier définissable dans $(\mathbf{FO} + \mathbf{MOD})[=]$ a un monoïde syntaxique commutatif. On utilise le jeu d'Ehrenfeucht-Fraïssé associé à $(\mathbf{FO} + \mathbf{MOD})[=]$. Pour tout mot u et pour toute permutation des lettres de u, Duplicateur peut répondre à chaque coup de Spoiler en prenant l'image des choix de Spoiler par la permutation. En particulier, pour tout langage régulier L définissable dans $(\mathbf{FO} + \mathbf{MOD})[=]$, et pour tous mots u, v, on a $uv \equiv_L vu$. Donc le monoïde syntaxique de L est dans **Com**. Pour le sens contraire, on utilise la propriété suivante de la variété **Com**. Un monoïde est *monogène* s'il existe un élément qui l'engendre.

Lemme 2.19.

Un monoïde appartient à **Com** s'il est quotient d'un produit cartésien de monoïdes monogènes.

Démonstration : Soit M un monoïde commutatif fini et $\{f_1, \ldots, f_k\} \subseteq M$ un ensemble de générateurs de M. Pour chaque élément f_i, on note M_{f_i} le sous-monoïde engendré par f. On montre que M est un quotient de $M_{f_1} \times \cdots \times M_{f_k}$. On définit

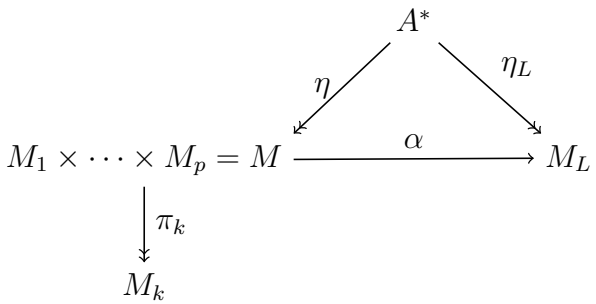
$$\psi : \begin{cases} M_{f_1} \times \cdots \times M_{f_k} & \to M \\ (m_1, \ldots, m_k) & \mapsto m_1 \cdots m_k \end{cases}$$

Tout d'abord M est un monoïde commutatif, donc ψ est un morphisme. De plus ψ est surjectif puisque $f_1, \ldots, f_k$ généré M. ■

Soit L un langage régulier de A^* dont le monoïde syntaxique est dans **Com**. D'après le lemme précédent, il existe des monoïdes monogènes $M_1, \ldots, M_p$ tels que le monoïde syntaxique de L soit un quotient de

$$M = M_1 \times \cdots \times M_p.$$

Il existe donc un morphisme surjectif $\alpha : M \to M_L$. Pour chaque lettre $a \in A$, il existe un élément, que l'on note m_a, dans la pré-image de α tel que $\alpha(m_a) = \eta_L(a)$. Enfin, on définit le morphisme $\eta : A^* \to M$ en posant $\eta(a) = m_a$. Le morphisme η ainsi défini reconnaît le langage L. Posons, pour $1 \leqslant k \leqslant p$, $\pi_k : M \to M_k$ la projection sur la $k^{\text{ème}}$ composante pour $1 \leqslant k \leqslant p$.



Il existe un ensemble $P \subseteq M$ tel que $L = \eta^{-1}(P)$. Pour chaque $x = (x_1, \ldots, x_p) \in P$ et chaque entier $1 \leqslant i \leqslant p$, $\eta^{-1}(x)$ est l'intersection des langages de la forme $(\pi_k \circ \eta)^{-1}(x_k)$, qui sont reconnus par des monoïdes monogènes. De plus,

$$L = \bigcup_{x \in P} \eta^{-1}(x).$$

C'est pourquoi un langage a son monoïde syntaxique dans **Com** si et seulement s'il est une combinaison booléenne (positive) de langages reconnus par des monoïdes monogènes.

Lemme 2.20.

Si un langage L sur l'alphabet A est reconnu par un monoïde monogène, alors il est combinaison booléenne de langages de la forme

$$L_{a,k} = \{u \mid |u|_a = k\},$$

où $a \in A$ et $k \in \mathbb{N}$ et de langages de la forme

$$L_{a,(r,d)} = \{u \mid |u|_a \equiv r \bmod d\}$$

où $a \in A$ et $0 \leqslant r < d$ sont des entiers.

Démonstration : Soit L un langage de A^* reconnu par un monoïde monogène. Montrons qu'il est une combinaison booléenne de langages de la forme $L_{a,P}$, où a et P sont définis comme dans l'énoncé. Par hypothèse, il existe $\eta : A^* \to M$ tel que M est monogène. Soit g un générateur de M et soit

$$T = \{i \in \mathbb{N} \mid g^i \in \eta(L)\}.$$

L'ensemble T est de la forme $K \cup (d\mathbb{N} + R)$ où d est la puissance d'idempotence de g, K un ensemble fini et $R \subseteq \{d, \ldots, 2d-1\}$. Pour chaque lettre a on note i_a, le plus petit entier i tel que $\eta(a) = g^i$. On conclut grâce à l'égalité suivante

$$L = \left(\bigcup_{\sum_{a\in A} i_a k_a \in K} \bigcap_{a\in A} L_{a,k_a} \right) \cup \left(\bigcup_{\sum_{a\in A} i_a r_a \in R'} \bigcap_{a\in A} \left(L_{a,(r_a,d)} \cap L^c_{a,r_a} \right) \right)$$

où $R' = \{i \in \{0, \ldots, d-1\} \mid i + d \in R\}$. ■

Pour terminer la preuve, comme $(\mathbf{FO} + \mathbf{MOD})[=]$ est stable par combinaison booléenne, il suffit de prouver que les langages de la forme $L_{a,k}$ et $L_{a,(r,d)}$ sont définissables dans $(\mathbf{FO} + \mathbf{MOD})[=]$. Le langage $L_{a,k}$ est défini par la formule

$$\left(\bigcup_{k\in K} \psi_k \wedge \neg\psi_{k+1} \right)$$

où

$$\psi_k = \exists x_1 \ldots \exists x_k \left(\bigwedge_{i\neq j} x_i \neq x_j \right) \wedge \bigwedge_{i=1}^{k} \mathbf{a}(x_i).$$

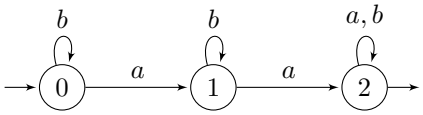
Le langage $L_{a,(r,d)}$ est défini par la formule

$$\exists^{r,d} x\ \mathbf{a}(x),$$

ce qui conclut la preuve. ■

Applications :

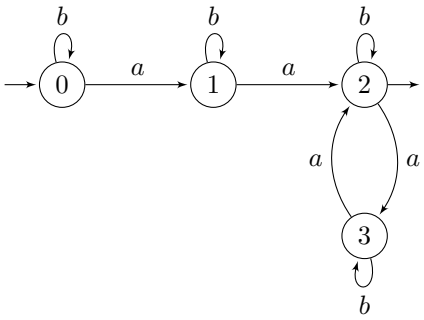
(1) Le langage des mots ayant au moins deux a ($A^*aA^*aA^*$) a pour automate minimal :

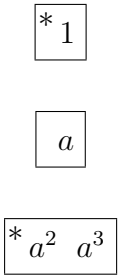


Son monoïde syntaxique est dans **ACom** et pas dans **Ab**.

(2) Le langage parité, $(b^*ab^*a)^*b^*$, a un monoïde syntaxique dans **Ab** et pas dans **A** et donc pas dans **ACom**.

(3) Le langage des mots ayant un nombre pair de a et au moins deux a, $A^*aA^*aA^* \cap (b^*ab^*a)^*b^*$ a pour automate minimal :





Son monoïde syntaxique est dans **Com** mais ni dans **ACom**, ni dans **Ab** et ni dans **A**.

2.2.1 La structure fine du premier ordre

La caractérisation algébrique de la hiérarchie d'alternances de quantifications constitue un problème ouvert depuis longtemps et a fait l'objet de nombreux travaux y compris récemment [54]. Tout en bas de la hiérarchie, on trouve le fragment $\mathcal{B}\mathbf{\Sigma}_1[<]$. Si une opération algébrique pour passer du fragment $\mathcal{B}\mathbf{\Sigma}_k[<]$ au fragment $\mathbf{\Sigma}_{k+1}[<]$ est connue (voir l'article [53]), elle reste mal comprise et non effective.

Théorème 2.21 (Simon [59], Thomas [72]).

Un langage est définissable dans $\mathcal{B}\mathbf{\Sigma}_1[<]$ si et seulement si son monoïde syntaxique est dans la variété **J**.

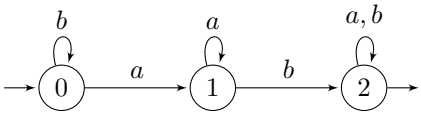
Place et Zeitoun ont annoncé [54] la décidabilité de $\mathcal{B}\mathbf{\Sigma}_2[<]$. Pour $k > 2$, aucun résultat de décidabilité n'est connu pour la hiérarchie $\mathcal{B}\mathbf{\Sigma}_k[<]$. On sait toutefois qu'elle définit une hiérarchie de variétés de monoïdes et qu'elle est infinie. Cela nous sera utile pour la suite.

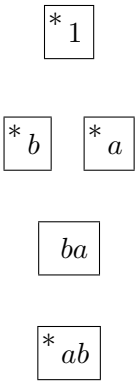
Théorème 2.22 (Brozowsky, Knast [13]).

Pour tout entier k, il existe un langage dans $\mathcal{B}\mathbf{\Sigma}_{k+1}[<]$ qui n'est pas définissable dans $\mathcal{B}\mathbf{\Sigma}_k[<]$.

Applications :

(1) Soit $A = \{a, b\}$. Le langage $A^*aA^*bA^*$ a pour automate minimal :





Son monoïde syntaxique est dans **J**.

(2) Le langage $L_2 = (ab)^*$ est définissable $\mathcal{B}\mathbf{\Sigma}_2[<]$ mais pas dans $\mathcal{B}\mathbf{\Sigma}_1[<]$.

(3) On pose par induction $L_{i+1} = (aL_i^*b)^*$ pour $i \geqslant 2$. Le langage L_{i+1} est définissable dans $\mathcal{B}\mathbf{\Sigma}_{i+1}[<]$ mais pas dans $\mathcal{B}\mathbf{\Sigma}_i[<]$.

2.3 La restriction à deux variables

La restriction à deux variables du premier ordre aura une certaine importance dans la deuxième partie de cette thèse. On introduit ici les résultats de décidabilité connus sur ce sujet.

Théorème 2.23 (Thérien, Wilke [71]).

Un langage est définissable dans $\mathbf{FO}^2[<]$ si et seulement si son monoïde syntaxique est dans **DA**.

Contrairement au cas de **FO**, la décidabilité de la structure fine de $\mathbf{FO}^2$ est maintenant connue. Le résultat a été prouvé indépendamment et presque simultanément par Krebs et Straubing [41] ainsi que par Kufleitner et Weil [45]. On remarquera que le premier niveau de cette hiérarchie, le fragment $\mathbf{FO}^2_1[<]$, est équivalent à $\mathcal{B}\mathbf{\Sigma}_1[<]$.

Définition 2.24 (équations de la structure fine de $\mathbf{FO}^2$).

On définit deux suites d'ω-termes par induction. On note l'ensemble des variables libres $X_0 = \{x_0, x_1\}$ et on pose $u_0 = (x_1x_2)^\omega$ ainsi que $v_0 = (x_2x_1)^\omega$. La définition est itérée sur l'ensemble $X_{n+1} = X_n \cup \{x_{2n+1}, x_{2n+2}\}$ comme suit :

$$u_{n+1} = (x_1 \cdots x_{2n}x_{2n+1})^\omega u_n (x_{2n+2}x_1 \cdots x_{2n})^\omega$$
$$v_{n+1} = (x_1 \cdots x_{2n}x_{2n+1})^\omega v_n (x_{2n+2}x_1 \cdots x_{2n})^\omega$$

Théorème 2.25 (Krebs, Straubing [41]).

Un langage régulier est définissable dans $\mathbf{FO}^2_k[<]$ si et seulement si son monoïde syntaxique est dans la variété définie par $[\![u_k = v_k, x^{\omega+1} = x^\omega]\!]$.

De cette caractérisation on en déduit le corollaire suivant.

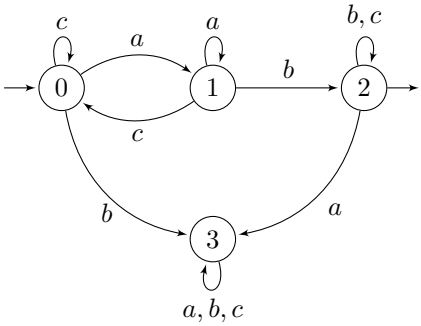
Corollaire 2.26 (Immermann et Weiss [75]).

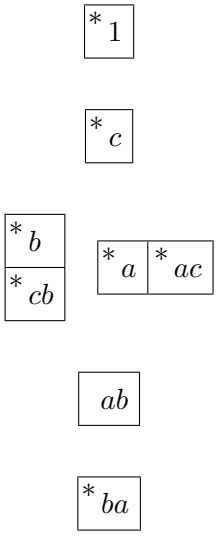
Pour tout entier k, il existe un langage dans $\mathbf{FO}^2_{k+1}[<]$ qui n'est pas définissable dans $\mathbf{FO}^2_k[<]$.

Applications :

(1) Le langage $(ab)^*$ n'est pas définissable dans $\mathbf{FO}^2[<]$.

(2) Le langage $\{a+b\}^*ab\{b+c\}^*$ a pour automate minimal :





Son monoïde syntaxique est dans **DA** mais pas dans **J**.

2.3.1 Restriction à deux variables avec des quantifications modulaires

Les fragments à deux variables avec des quantifications modulaires ont été étudiés par Straubing et Thérien [68, 69]. Des outils algébriques un peu plus avancés sont nécessaires afin d'en exposer ici les résultats.

Le produit semi-direct est une opération algébrique très utilisée en théorie des groupes finis, en particulier pour décomposer les groupes en *briques* élémentaires. Le théorème [42] de décomposition de Krohn-Rodes établit un résultat similaire pour les semigroupes. Le produit en couronne, que nous allons maintenant présenter, dispose d'une littérature riche,

(voir par exemple les articles [64, 73, 2, 6, 61, 19]). Des cas particuliers de ce produit en couronne seront exposés dans les deux chapitres suivants.

Définition 2.27 (produit en couronne).

Soient S et T deux semigroupes finis. Le produit en couronne de S par T, noté $S \circ T$ est le monoïde $S^T \times T$ avec comme loi de composition interne :

$$(f,t)(f',t') = (g,tt'),$$

en posant g la fonction de S vers T définie par $g(x) = f(x)f'(xt)$.

On étend cette définition aux variétés de monoïdes : le produit semidirect de $\mathbf{V}$ par $\mathbf{W}$, noté $\mathbf{V} * \mathbf{W}$, est la variété engendrée par les monoïdes de la forme $M \circ N$ pour $M \in \mathbf{V}$ et $N \in \mathbf{W}$.

Théorème 2.28 (Straubing, Thérien [68, 69]).

Un langage est définissable dans $(\mathbf{FO} + \mathbf{MOD})^2[<]$ si et seulement si son monoïde syntaxique est dans la variété $\mathbf{DA} * \mathbf{G}_{\text{sol}}$.

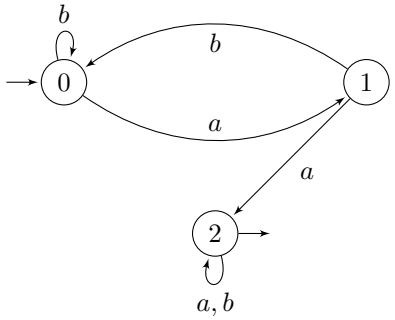
Ce théorème ne permet malheureusement pas d'avoir une caractérisation effective de $(\mathbf{FO} + \mathbf{MOD})^2[<]$. Toutefois, on en déduit une sur-approximation intéressante. On note $\mathcal{E}\mathbf{DA}$ la variété des monoïdes dont les idempotents engendrent un monoïde dans $\mathbf{DA}$.

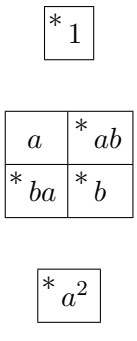
Proposition 2.29 (Almeida et Escada [4]).

$\mathbf{DA} * \mathbf{G}_{\text{sol}} \subsetneq \mathbf{DA} * \mathbf{G} = \mathcal{E}\mathbf{DA}$.

Applications :

- Soit $A = \{a, b\}$. Le langage A^*aaA^* a pour automate minimal :





Le sous-monoïde engendré par les idempotents est le monoïde complet. Or ce monoïde n'est pas dans **DA**. Il n'est donc pas dans $\mathbf{DA} * \mathbf{G}_{\text{sol}} = \mathcal{E}\mathbf{DA}$. Ce langage n'est pas définissable dans $(\mathbf{FO} + \mathbf{MOD})^2[<]$.

- Le langage $(ab)^*$ est définissable dans $(\mathbf{FO} + \mathbf{MOD})^2[<]$ par la formule :

$$(\forall x\ \mathbf{a}(x) \to \exists^{0,2} y < x) \wedge (\forall x\ \mathbf{b}(x) \to \exists^{1,2} y < x)$$

2.4 Résumé

Les tableaux suivants résument les résultats présentés dans cette section.

Fragment	Variété	Équations
$\mathbf{FO}[\emptyset]$ $\mathbf{FO}^1[<]$	$\mathbf{J_1}$	$[\![xy = yx, x^2 = x]\!]$
$\mathbf{FO}[=]$	$\mathbf{ACom}$	$[\![xy = yx, x^{\omega+1} = x^\omega]\!]$
$\mathbf{MOD}[=]$	$\mathbf{Ab}$	$[\![xy = yx, x^\omega = 1]\!]$
$(\mathbf{FO} + \mathbf{MOD})[=]$	$\mathbf{Com}$	$[\![xy = yx]\!]$
$\mathbf{FO}[<]$	$\mathbf{A}$	$[\![x^{\omega+1} = x^\omega]\!]$
$\mathbf{MOD}[<]$	$\mathbf{G}_{\text{sol}}$	
$(\mathbf{FO} + \mathbf{MOD})[<]$	$\mathbf{M}_{\text{sol}}$	

FIGURE 2.1 – Le premier ordre

Fragment	Variété	Équations
$\mathbf{FO}^2_k[<]$	$\mathbf{V}_k$	$[\![x^{\omega+1} = x^\omega, u_k = v_k]\!]$
$\mathbf{FO}^2[<]$	$\mathbf{DA}$	$[\![x^{\omega+1} = x^\omega, (xy)^\omega x (xy)^\omega = (xy)^\omega]\!]$
$(\mathbf{FO} + \mathbf{MOD})^2[<]$	$\mathbf{DA} * \mathbf{G}_{\text{sol}}$	
$\mathbf{MOD}^2[<]$	$\mathbf{G}_{\text{sol}}$	

FIGURE 2.2 – La restriction à deux variables

Chapitre 3

Les prédicats locaux

et la théorie des ne-variétés

Dans le chapitre précédent, nous nous sommes concentrés sur trois types de signatures. La signature vide, la signature ne contenant que le prédicat numérique d'égalité et la signature contenant uniquement le prédicat numérique d'ordre. Nous allons étudier comment l'enrichissement d'un fragment à l'aide de prédicats locaux modifie son expressivité. Il existe deux types de prédicats locaux :

- les prédicats numériques locaux,
- les prédicats descriptifs locaux.

Seul l'ajout des descriptifs locaux correspond systématiquement à une opération algébrique. Toutefois, pour un grand nombre de fragments, ces deux signatures donneront la même classe de langages. L'unique contre-exemple connu est fourni par le fragment $\mathbf{FO}^1$ dont le comportement au contact des prédicats numériques locaux est particulier puisqu'il lui est impossible d'utiliser les prédicats binaires.

Comme on le soulignera dans la première section de ce chapitre, le cadre fourni par la théorie des variétés de monoïdes n'est pas suffisant pour traiter de l'ajout des prédicats locaux. Nous allons donc introduire dans la partie 3.2 les notions de *variétés non effaçantes*. Les parties suivantes vont être consacrées à l'étude d'une opération algébrique (le produit en couronne par $\mathbf{D}$) qui correspond à l'ajout des prédicats descriptifs locaux. Enfin, nous donnerons dans la dernière partie les résultats de transfert de décidabilité et de séparation.

3.1 Le fragment $\mathbf{FO}^2[<, \mathrm{LOC}]$

Dans un premier temps, étudions le cas de $\mathbf{FO}^2$ afin de mettre en évidence que les notions algébriques introduites dans le chapitre précédent ne sont pas suffisantes.

Proposition 3.1.

Le fragment $\mathbf{FO}^2[<, \mathrm{LOC}]$ est strictement plus expressif que le fragment $\mathbf{FO}^2[<]$.

Démonstration : Le langage $(ab)^*$ est définissable dans $\mathbf{FO}[<]$ mais non définissable dans $\mathbf{FO}^2[<]$. La formule suivante permet de définir ce langage dans $\mathbf{FO}^2[<, \mathrm{LOC}]$:

$$\Big(\forall x \forall y \ (x = y + 1) \to \big(\mathbf{a}(x) \wedge \mathbf{b}(y)\big) \vee \big(\mathbf{b}(x) \wedge \mathbf{a}(y)\big)\Big) \wedge \mathbf{a}(0) \wedge \mathbf{b}(\max)).$$

■

La proposition qui suit donne un résultat de non-définissabilité pour un langage dans $\mathbf{FO}^2[<, \mathrm{LOC}]$. Ce type de résultat peut être prouvé *à la main* en utilisant des jeux d'Ehrenfeucht-Fraïssé. Toutefois, il est plus aisé de s'appuyer sur la description algébrique de ce fragment qui sera introduite dans la suite de ce chapitre.

Proposition 3.2.

Le langage $c^*(ac^*bc^*)^*$ n'est pas définissable dans $\mathbf{FO}^2[<, \mathrm{LOC}]$.

Posons $A = \{a, b\}$ et $B = \{a, b, c\}$ ainsi que le morphisme $\eta : B^* \to A^*$ défini par $\eta(a) = a, \eta(b) = b$ et $\eta(c) = 1$. Alors, on a

$$c^*(ac^*bc^*)^* = \eta^{-1}((ab)^*).$$

On en conclut donc que les langages définissables dans $\mathbf{FO}^2[<, \mathrm{LOC}]$ ne forment pas une variété de langages.

3.2 Outils algébriques : *ne*-variétés, variétés de semigroupes

La stabilité par morphisme inverse est une des conditions d'utilisation de la théorie des variétés de monoïdes finis. En son absence, on peut parfois utiliser la théorie des $\mathcal{C}$-variétés de langages introduite par Ésik et Ito [26] ainsi que Straubing [67] puis développée par Pin et Straubing [52]. Dans ce chapitre, on se concentrera sur les variétés *non effaçantes*. On introduira un autre type de $\mathcal{C}$-variétés dans le chapitre suivant.

3.2.1 Définitions

Avant d'introduire les notions de variétés non effaçantes, nous devons expliquer ce qu'est un morphisme non effaçant.

Définition 3.3 (Morphisme non effaçant).

Soient A et B deux alphabets finis. Un morphisme $\psi : A^* \to B^*$ est non effaçant si $\psi(A) \subseteq B^+$. Autrement dit, l'image d'une lettre est un mot de longueur non nulle.

Voici un exemple de morphisme non effaçant.

Exemple : Le morphisme $\psi : \{a, b\}^* \to \{a, b\}^*$ tel que $\psi(a) = a$ et $\psi(b) = bb$. Ce qui donne, par exemple, $\psi(ababa) = abbabba$.

Proposition 3.4.

La classe des morphismes non effaçants est stable par composition.

Définition 3.5 (*ne*-variété de langages).

Une classe de langages réguliers est une *ne*-variété de langages si elle est close par les opérations booléennes, par image inverse de morphisme non effaçants et par les quotients.

Comme pour le cas des variétés de langages, on cherche maintenant à obtenir une correspondance entre les *ne*-variétés de langages et une variété d'objets algébriques finis. Deux possibilités s'offrent à nous. Soit on considère les *variétés de timbres*, soit on considère les *variétés de semigroupes finis*. Les deux ne diffèrent que par leur gestion du mot vide. On rappelle qu'un timbre est un morphisme surjectif d'un monoïde libre dans un monoïde fini (voir la section 2.1).

Un *ne-morphisme* d'un timbre $\eta : A^* \to M$ vers un timbre $\psi : B^* \to N$ est un couple (f, α) où $f : A^* \to B^*$ est un morphisme non effaçant et $\alpha : M \to N$ un morphisme de monoïdes tels que $\psi \circ f = \alpha \circ \eta$. Un *ne*-morphisme (f, α) est un *ne-quotient* si $f(A) = B$.

$$\begin{array}{ccc} A^* & \xrightarrow{\quad f \quad} & B^* \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ M & \xrightarrow{\quad \alpha \quad} & N \end{array}$$

Dans ce cas, les morphismes f et α sont nécessairement surjectifs. Un *ne*-morphisme (f, α) est une *ne-inclusion* si α est un morphisme injectif. Soient $\varphi : A^* \to M_1$ et $\psi : A^* \to M_2$ deux timbres. Le *produit* de φ par ψ est le timbre $\theta : A^* \to N$ défini par

$$\theta(a) = \big(\varphi(a), \psi(a)\big)$$

où N est le sous-monoïde de $M_1 \times M_2$ engendré par $\theta(a)$ pour tout $a \in A$. Un timbre φ *ne-divise* un timbre ψ s'il existe un timbre $\theta : C^* \to K$, une *ne*-inclusion $(f, \alpha) : \theta \to \psi$ et un *ne*-quotient $(g, \beta) : \theta \to \varphi$. La définition suivante, donnée dans l'article [67], est équivalente (voir l'article [52, proposition 2.1]). Un timbre $\varphi : A^* \to M$ *ne-divise* un timbre $\psi : B^* \to N$ si et seulement s'il existe un couple (f, α) tel que $f : A^* \to B^*$ est un morphisme non effaçant, $\alpha : N' \to M$ un morphisme surjectif où N' est l'image de $\psi \circ f$ et

$$\varphi = \alpha \circ \psi \circ f.$$

Comme les morphismes non effaçants sont stables par composition, la relation sur la *ne*-division de timbres est transitive.

Définition 3.6 (*ne*-variété de timbres).

Une classe de timbres est une *ne*-variété de timbres si elle est stable par produit direct et par *ne*-division de timbres.

Il existe une correspondance entre *ne*-variété de langages et *ne*-variété de timbres. En effet, une *ne*-variété de langages peut être naturellement associée à la *ne*-variété de timbres engendrée par ses timbres syntaxiques. La proposition suivante permet d'obtenir une correspondance réciproque.

Proposition 3.7.

Soit $\mathbf{V}$ une *ne*-variété de timbres. La classe des langages reconnue par les timbres de $\mathbf{V}$ forme une *ne*-variété de langages.

Comme dans le cas des monoïdes, un équivalent du théorème d'Eilenberg peut être obtenu (voir l'article [52] pour plus de précisions), établissant que ces deux correspondances sont mutuellement bijectives. On introduit la notion de variété de semigroupes finis fortement reliée aux *ne*-variétés de timbres.

Définition 3.8 (Variété de semigroupes).

Une classe de semigroupes finis est une (pseudo-)variété si elle est stable par produit direct et division de semigroupes.

Établissons maintenant le lien entre les notions de *ne*-variété et variété de semigroupes. Dans un premier temps, on remarque que si $\eta : A^* \to M$ est un timbre, alors $\eta(A^+)$ est un semigroupe.

Soit $\mathbf{V}$ une *ne*-variété de timbres. Alors la classe des semigroupes de la forme $\eta(A^+)$ pour η dans $\mathbf{V}$, forme une variété de semigroupes. Réciproquement, si $\mathbf{V}$ est une variété de

semigroupes, alors la classe des timbres de la forme $\eta : A^* \to S^1$ où S est un semigroupe de $\mathbf{V}$, forme une *ne*-variété de timbres. Ces deux correspondances sont des applications bijectives réciproques (voir l'article [52, lemme 7.3]).

3.2.2 La théorie profinie des *ne*-variétés

Comme pour le cas des monoïdes finis, on introduit la notation suivante pour $\mathbf{V}$ une *ne*-variété de timbre et $u, v \in A^*$:

$$r_{\mathbf{V}}(u,v) = \min\{|M| \mid \text{il existe } \eta : A^* \to M \text{ dans } \mathbf{V} \text{ tel que } \eta(u) \neq \eta(v)\}.$$

Ainsi, $u \sim_{\mathbf{V}} v$ si et seulement si ces deux mots ne sont pas séparables ($r_{\mathbf{V}}(u,v) = +\infty$). Cette relation est une congruence et donc $A^*/\sim_V$ est un monoïde. Comme dans le cas des variétés de monoïdes, on définit l'application

$$d_{\mathbf{V}} : \begin{cases} (A^*/\sim_{\mathbf{V}}) \times (A^*/\sim_{\mathbf{V}}) & \to [0, +\infty[\\ (u,v) & \mapsto 2^{-r_{\mathbf{V}}(u,v)} \end{cases}$$

Cette application est une distance sur $A^*/\sim_{\mathbf{V}}$ et on note $\widehat{F}_{\mathbf{V}}(A)$ la complétion de $A^*/\sim_{\mathbf{V}}$ pour cette distance.

Une *ne*-identité profinie sur l'alphabet A est un couple $(u,v) \in \widehat{A^*}^2$. On la note $u =_{\text{ne}} v$. Un timbre $\eta : B^* \to M$ vérifie la *ne*-identité profinie $u =_{\text{ne}} v$ si pour tout morphisme non effaçant $\psi : A^* \to B^*$, le morphisme $\eta \circ \psi$ satisfait l'identité profinie $u = v$. On peut montrer la proposition suivante, similaire à la proposition 2.13.

Proposition 3.9.

Soit E un ensemble de *ne*-identités profinies. La classe des timbres qui vérifient toutes les identités de E est une *ne*-variété de timbres.

Remarque : Pour vérifier qu'une *ne*-identité profinie, donnée par exemple sous la forme d'ω-terme, est satisfaite par un timbre $\eta : A^* \to M$, il suffit de la vérifier pour toute instanciation des variables par des éléments de $\eta(A^+)$.

3.2.3 Des exemples importants

Soit S un semigroupe. Les monoïdes locaux de S sont les monoïdes de la forme eSe où e est un idempotent. Montrons que eSe est effectivement un monoïde. Si on pose $x = eue$ et $y = eve$ dans eSe, alors

$$xy = eueeve = e(uev)e \in eSe,$$
$$ex = xe = x.$$

Soit $\mathbf{V}$ une variété de monoïdes finis. On note $\mathbf{LV}$ la classe des timbres $\eta : A^* \to M$ tels que tous les monoïdes locaux de $\eta(A^+)$ sont dans $\mathbf{V}$.

Proposition 3.10.

Soit **V** une variété de monoïdes finis. La classe de timbres **LV** est une *ne*-variété de timbres.

Démonstration : Il faut montrer que **LV** est stable par produit et *ne*-division.

(1) Soient $\varphi : A^* \to M_1$ et $\psi : A^* \to M_2$ deux timbres de **LV** et $\theta : A^* \to N$ le produit de φ et ψ. Montrons que θ appartient à **LV**. Soit $e = (f_1, f_2)$ un idempotent du semigroupe $S = \theta(A^+)$. L'élément f_1 est un idempotent de M_1 et l'élément f_2 est un idempotent de M_2. Le monoïde eSe est donc un sous-monoïde de $(f_1M_1f_1) \times (f_2M_2f_2)$ qui appartient à **V**. C'est pourquoi eSe appartient à **V**. Finalement, θ appartient à **LV**.

(2) Soient $\psi : B^* \to N$ un timbre de **LV** et $\theta : C^* \to K$ un timbre tels qu'il existe une *ne*-inclusion $(f, \alpha) : \theta \to \psi$. Montrons que θ appartient à **LV**. Soit e un idempotent de $\psi(A^+)$. Par définition, il existe un mot u de longueur non nulle tel que $\psi(u) = e$. L'image de e par α est également un idempotent que l'on note g, et

$$g = \alpha(\psi(u)) = \theta(f(u)).$$

Or $f(u) \in C^+$ et donc $g \in \theta(C^+)$. Par hypothèse gNg appartient à **V** et comme le monoïde $\alpha(eKe)$ est un sous-monoïde de gNg, il appartient également à **V**. Enfin, on conclut puisque $\alpha(eKe)$ est isomorphe à eKe car α est injectif.

(3) Soient $\theta : C^* \to K$ un timbre de **LV** et $\varphi : A^* \to M$ un timbre tels qu'il existe un *ne*-quotient $(f, \alpha) : \theta \to \varphi$. Montrons que φ appartient également à **LV**. Soit e un idempotent du semigroupe $\varphi(A^+)$ et u un mot de longueur non nulle tel que $\eta(u) = e$. Comme f est un morphisme non effaçant surjectif, il existe $v \in C^+$ tel que $f(v) = u$ et notons $x = \theta(v)$. Par définition d'un *ne*-morphisme, nous avons

$$\alpha(x) = \alpha(\theta(v)) = \varphi(f(v)) = \varphi(u) = e.$$

On en déduit que $\alpha(x^\omega) = e$. Par hypothèse, $x^\omega K x^\omega$ appartient à **V**. Or, comme α est surjectif, nous avons

$$\alpha(x^\omega K x^\omega) = eMe$$

et donc eMe est un monoïde quotient de $x^\omega K x^\omega$. C'est pourquoi eMe appartient également à **V**.

On déduit des points (2) et (3) que **LV** est stable par *ne*-division, ce qui termine la preuve. ■

Nous allons maintenant étudier des exemples de *ne*-variété de timbres de la forme **LV**.

Exemple :

- La *ne*-variétés des timbres *localement triviaux*, notée **LI**.
- La *ne*-variétés des timbres *localement* **DA**, notée **LDA**.

À partir d'une description équationnelle d'une variété de monoïdes **V**, sous la forme d'ω-termes, il est possible de construire une description équationnelle de la *ne*-variété **LV**. Nous allons illustrer ceci à l'aide de la proposition suivante.

Proposition 3.11.

- La *ne*-variété des timbres localement triviaux est définie par l'équation

$$\mathbf{LI} = [\![x^\omega y x^\omega =_{\mathrm{ne}} x^\omega]\!]$$

- La *ne*-variété des timbres localement **DA** est définie par l'équation

$$\mathbf{LDA} = [\![(x^\omega y x^\omega z x^\omega)^\omega y (x^\omega y x^\omega z x^\omega)^\omega =_{\mathrm{ne}} (x^\omega y x^\omega z x^\omega)^\omega]\!]$$

Démonstration : Nous allons prouver uniquement le deuxième point. La preuve du premier point est très similaire.

- Soit $\eta : A^* \to M$ un timbre de **LDA** et notons $S = \eta(A^+)$. Montrons que ce timbre vérifie la *ne*-équation

$$(x^\omega y x^\omega z x^\omega)^\omega y (x^\omega y x^\omega z x^\omega)^\omega =_{\mathrm{ne}} (x^\omega y x^\omega z x^\omega)^\omega. \tag{a}$$

Prenons un morphisme non effaçant $\psi : \{x, y, z\}^* \to A^*$ et notons $\theta = \eta \circ \psi : \{x, y, z\}^* \to M$. Pour conclure cette implication, il suffit de montrer que θ vérifie

$$\begin{array}{ccc} \{x,y,z\}^* & \xrightarrow{\psi} & A^* \\ & \searrow^{\theta} & \downarrow \eta \\ & & M \end{array}$$

l'équation profinie

$$(x^\omega y x^\omega z x^\omega)^\omega y (x^\omega y x^\omega z x^\omega)^\omega = (x^\omega y x^\omega z x^\omega)^\omega. \tag{b}$$

Par construction, $\widehat{\theta}(x^\omega)$ est un idempotent de S, et on pose :

$$\begin{aligned} e &= \widehat{\theta}(x^\omega) \in S \\ u &= \widehat{\theta}(x^\omega y x^\omega) \in eSe \\ v &= \widehat{\theta}(x^\omega z x^\omega) \in eSe \end{aligned}$$

Par hypothèse, le monoïde eSe est dans **DA**. C'est pourquoi nous avons que

$$(uv)^\omega u (uv)^\omega = (uv)^\omega$$

et donc

$$\begin{aligned}\widehat{\theta}((x^\omega yx^\omega zx^\omega)^\omega) &= \left(\widehat{\theta}(x^\omega yx^\omega)\widehat{\theta}(x^\omega zx^\omega)\right)^\omega \\ &= (uv)^\omega \\ &= (uv)^\omega u(uv)^\omega \\ &= \widehat{\theta}((x^\omega yx^\omega zx^\omega)^\omega y(x^\omega yx^\omega zx^\omega)^\omega)\end{aligned}$$

Et donc θ vérifie bien l'équation (b).

- Soit $\eta : A^* \to M$ un timbre vérifiant l'équation (a). Montrons que ce timbre est nécessairement dans **LDA**. Soient e un idempotent de $S = \eta(A^+)$ ainsi que u et v deux éléments de eSe. Par définition, il existe des mots $p, s, t \in A^+$ tels que $\eta(p) = e, \eta(s) = u$ et $\eta(t) = v$. On définit $\psi : \{x, y, z\}^* \to A^*$ le morphisme en posant $\psi(x) = p, \eta(y) = s$ et $\eta(z) = t$. On pose également $\theta = \eta \circ \psi : \{x, y, z\}^* \to M$ et on remarque que

$$\begin{aligned}\widehat{\theta}(x^\omega y) = \widehat{\theta}(yx^\omega) = \widehat{\theta}(y) = u, \\ \widehat{\theta}(x^\omega z) = \widehat{\theta}(zx^\omega) = \widehat{\theta}(z) = v,\end{aligned}$$

et donc

$$\widehat{\theta}((x^\omega yx^\omega zx^\omega)^\omega y(x^\omega yx^\omega zx^\omega)^\omega) = (uv)^\omega v(uv)^\omega \;\; \widehat{\theta}((x^\omega yx^\omega zx^\omega)^\omega) \quad = (uv)^\omega.$$

Le morphisme ψ est non effaçant et comme η vérifie la *ne*-équation (a) on a $\theta = \eta \circ \psi : \{x, y, z\}^* \to M$ qui vérifie l'équation profinie (b) et donc

$$(uv)^\omega v(uv)^\omega = (uv)^\omega$$

ce qui conclut la preuve. ■

3.3 Le produit en couronne par D

Le produit en couronne est l'un des outils les plus efficaces pour décrire comment l'ajout de prédicats modifie l'expressivité des fragments. Le produit en couronne de deux semigroupes a été présenté dans le chapitre précédent (voir la définition 2.27). Ce qui nous intéresse dans ce chapitre est le produit en couronne par la *ne*-variété **D**, que nous allons maintenant définir.

Définition 3.12 (Timbres localement triviaux à droites).

Un timbre $\eta : A^* \to M$ est localement trivial à droite si pour tout élément x et y de $\eta(A^+)$ on a $yx^\omega = x^\omega$. On note **D** cette classe de timbres.

Remarque : La classe de timbre **D** correspond également aux timbres vérifiant la *ne*-équation $yx^\omega =_{\text{ne}} x^\omega$.

La *ne*-variété **D** n'est pas une variété de monoïdes finis, on ne peut donc pas directement utiliser la définition donnée dans le chapitre précédent pour le produit en couronne de deux variétés de monoïdes. Nous allons toutefois pouvoir l'adapter à ce contexte par la suite. Avant toutes choses, étudions la *ne*-variété **D**.

Proposition 3.13.

La classe **D** est une *ne*-variété de timbres.

La preuve de cette proposition est semblable à celle de la proposition 3.10.

Soit n un entier positif et A un alphabet fixé. On pose $A^{\leqslant n} = \{u \in A^* \mid |u| \leqslant n\}$ et on définit également la fonction

$$\mathrm{suff}_n : \begin{cases} A^* \to A^{\leqslant n} & \\ u_0 \cdots u_p \mapsto u_{p-n+1} \cdots u_p & \text{si } n \leqslant p \\ u_0 \cdots u_p \mapsto u_0 \cdots u_p & \text{sinon} \end{cases}$$

On équipe l'ensemble $A^{\leqslant n}$ de la loi de composition interne $\cdot$ donnée par

$$\text{pour } u, v \in A^{\leqslant n},\ u \cdot v = \mathrm{suff}_n(uv).$$

L'ensemble $A^{\leqslant n}$ équipé de cette loi est un monoïde et la fonction suff_n, un timbre. Dans la suite le produit de deux éléments de $A^{\leqslant n}$ sera systématiquement le produit dans le monoïde. Il sera parfois nécessaire de réaliser ce produit dans le monoïde libre. Pour ce faire, on définit l'application $\iota : A^{\leqslant n} \to A^*$ en posant $\iota(u) = u$ qui permet d'*oublier* que $A^{\leqslant n}$ est un monoïde. Soient $u, v \in A^{\leqslant n}$, nous avons l'égalité suivante qui est vérifiée :

$$\mathrm{suff}_n(\iota(u)\iota(v)) = uv.$$

Exemple : La fonction suff_n retourne le suffixe de longueur n si le mot est suffisamment grand. Sur les mots de longueur plus petite que n il s'agit de l'identité. Ainsi, $\mathrm{suff}_3(ab) = ab$ et $\mathrm{suff}_3(abababaab) = aab$. Nous avons également $\iota(ab)\iota(ab) = abab$ et $\iota(abab) = ab$.

Remarque : La notation suff_n suppose que l'alphabet est donné implicitement.

Les timbres de la forme suff_n vont jouer un rôle particulier pour la *ne*-variété de timbres **D**. Montrons dans un premier temps qu'ils lui appartiennent.

Proposition 3.14.

Soit n un entier positif. Pour tout alphabet, l'application suff_n est un timbre de **D**.

Démonstration : Montrons que le timbre suff_n est dans **D**. Pour cela, il faut vérifier pour tout élément x, y de $\mathrm{suff}_n(A^+)$ on a $yx^\omega = x^\omega$, où x^ω est la puissance d'idempotence de x dans le monoïde $A^{\leqslant n}$. Soient $x, y \in A^{\leqslant n}$ différent du neutre. Il existe un entier m tel que $x^\omega = \mathrm{suff}_n(\iota(x)^m)$. Par définition de la puissance d'idempotence,

$$x^\omega = \mathrm{suff}_n(\iota(x)^m) = \mathrm{suff}_n(\iota(x)^m)^n = \mathrm{suff}_n(\iota(x)^{nm})$$

et comme $\iota(x)$ n'est pas le mot vide, $\iota(x)^{nm}$ est de longueur au moins n. Or, pour tout mot u de longueur au moins n et tout mot v, on a que

$$\mathrm{suff}_n(vu) = \mathrm{suff}_n(u).$$

On en conclut que

$$yx^\omega = \mathrm{suff}_n(\iota(yx)^{nm}) = \mathrm{suff}_n(\iota(x)^{nm}) = x^\omega.$$

■

Le lemme suivant nous sera utile dans la suite.

Lemme 3.15.

Soient $\eta : A^* \to M$ un timbre de **D** et $n = |M| + 1$. Pour tout mot v de A^+ de longueur au moins n, on a $\eta(v) = \eta(\iota(\mathrm{suff}_n(v)))$.

Démonstration : Soient v un mot de A^+ et $u = u_0 \cdots u_{n-1}$ son suffixe de taille n. Montrons que $\eta(v) = \eta(u)$. Pour tout i, on définit la suite $x_i = \eta(u_0 \cdots u_i)$. Comme $n > |M|$, il existe $i < j < n$ tels que $x_i = x_j$. En posant $y = \eta(u_{i+1} \cdots u_j)$ et $z = \eta(u_{j+1} \cdots u_n)$, on a $x = x_i yz = x_i z$. Par conséquent $x = x_i y^\omega z$. Or, par définition de **D**, pour tout $s \in \eta(A^+)$ on $sy^\omega = y^\omega$. Comme $x_i \in \eta(A^+)$, on a $x = x_i y^\omega z = y^\omega z$ d'où

$$\eta(v) = y^\omega z = \eta(u).$$

■

Nous avons maintenant tous les outils pour décrire complètement la *ne*-variété de langages équivalentes à **D**.

Proposition 3.16.

Soit $\mathcal{D}$ la *ne*-variété de langages associée à **D** et A un alphabet fini. Un langage L appartient à $\mathcal{D}(A^*)$ si et seulement s'il existe deux ensembles finis F et G de A^* tels que $L = A^*F \cup G$.

Démonstration : La preuve de cette proposition se décompose en deux étapes.

(1) Soient F et G deux ensembles finis de mots de A^*. Montrons que le langage $A^*F \cup G$ est dans $\mathcal{D}(A^*)$. Soit $n = \max\{|u| \mid u \in F \cup G\} + 1$. Pour tout mot dans u de longueur au plus $n-1$, nous avons

$$\{u\} = \mathrm{suff}_n^{-1}(\mathrm{suff}_n(u))$$

et donc

$$G = \mathrm{suff}_n^{-1}(\mathrm{suff}_n(G)).$$

De même, pour tout mot u de longueur n,

$$A^*u = \mathrm{suff}_n^{-1}(u).$$

on en déduit que

$$A^*F = \mathrm{suff}_n^{-1}(\mathrm{suff}_n(A^*F)).$$

et donc $A^*F \cup G$ est reconnu par suff_n.

(2) Soient L un langage de $\mathcal{D}(A^*)$ et $\eta_L : A^* \to M$. Comme η_L appartient à **D**, d'après le lemme 3.15, pour tout mot u de A^+ tel que $|u| > |M|$ on a $\eta_L(u) = \eta_L(\mathrm{suff}_n(u))$. On définit l'ensemble

$$F = \{v \in A^n \mid A^*v \cap L \neq \emptyset\}.$$

Pour tout mot $u \in A^*F$, il existe un mot $w \in L$ tel que $\mathrm{suff}_n(u) = \mathrm{suff}_n(w)$ et donc

$$\eta_L(u) = \eta_L(\mathrm{suff}_n(u)) = \eta_L(\mathrm{suff}_n(w)) = \eta_L(w)$$

d'où $u \in L$. On en déduit que $A^*F \subseteq L$. Le langage F est un ensemble de mots de longueurs n. Il est donc fini. On définit également l'ensemble

$$G = L - A^*F.$$

Montrons que les mots de G ont une longueur au plus n. Supposons qu'il existe $u \in G$ tel que $|u| > n$. Par définition, comme $u \in L$, $\mathrm{suff}_n(u) \in F$ d'où $u \in A^*F$ ce qui est absurde. Le langage G est un ensemble de mots de longueurs au plus n. Il est donc fini et par construction

$$L = A^*F \cup G.$$

■

Proposition 3.17.

Soient $\eta : A^* \to M$ un timbre de **D** et $n = |M| + 1$. Le timbre η ne-divise suff_n.

Démonstration : On définit quotient $(f, \alpha) : \mathrm{suff}_n \to \eta$ en posant :

- $f : A^* \to A^*$ est l'identité,
- $\alpha : A^{\leqslant n} \to M$ le morphisme de monoïde défini par $\alpha(u) = \eta(\iota(u))$. Montrons que α est un morphisme surjectif.

- On a $\alpha(1) = 1$ par définition.
- Soient $u, v \in A^{\leqslant n}$. Par définition, $\alpha(uv) = \eta(\iota(uv))$. De même, $\alpha(u)\alpha(v) = \eta(\iota(u))\eta(\iota(v))$. Comme η est un morphisme, $\alpha(u)\alpha(v) = \eta(\iota(u)\iota(v))$. Or en utilisant le lemme 3.15, on obtient

$$\alpha(u)\alpha(v) = \eta(\iota(u)\iota(v)) = \eta(\mathrm{suff}_n(\iota(u)\iota(v)) = \eta(\iota(uv)) = \alpha(uv).$$

- Montrons que α est surjectif. Soit $x \in M$. Comme η est surjectif, il existe un élément $u \in A^*$ tel que $\eta(u) = x$. D'après le lemme 3.15,

$$\eta(u) = \eta(\iota(\mathrm{suff}_n(u)) = \alpha(\mathrm{suff}_n(u)).$$

Ce qui conclut la preuve. ■

Introduisons maintenant le produit en couronne par **D**. En utilisant la proposition précédente, on voit qu'il n'est pas nécessaire de définir ce produit en couronne pour tous les timbres de **D** mais uniquement pour ses générateurs, c'est-à-dire, pour les timbres de la forme suff_n pour un certain n.

Définition 3.18 (Produit en couronne par le timbre suffixe).

Soit $\eta : (A \times A^{\leqslant n})^* \to M$ un timbre. Le produit en couronne de η par suff_n est le timbre

$$\eta \bullet \mathrm{suff}_n : A^* \to N \subseteq M \circ A^{\leqslant n}$$

défini par $\eta \bullet \psi(a) = (f_a, \mathrm{suff}_n(a))$ où

$$f_a : \begin{cases} A^{\leqslant n} & \to M \\ u & \mapsto \eta(a, u) \end{cases}$$

On étend maintenant cette définition au cas particulier du produit en couronne de variétés qui nous intéressent.

Définition 3.19 (produit en couronne par D).

Soit **V** une variété de monoïdes finis. Le produit en couronne de **V** par **D**, noté $\mathbf{V} * \mathbf{D}$, est la *ne*-variété de timbres engendrée par les timbres de la forme $\eta \bullet \mathrm{suff}_n$ où η est un timbre dans un monoïde de **V** et $n \in \mathbb{N}$.

Nous allons maintenant introduire un certain nombre d'outils afin d'étudier ce produit en couronne.

3.3.1 Le principe du produit en couronne

Intuitivement, réaliser un produit en couronne par **D** consiste à rajouter une *information locale à droite*. Le principe du produit en couronne va permettre d'*exhiber*, sous la forme d'un alphabet *enrichi* cette information supplémentaire. Cet enrichissement de l'alphabet va prendre la forme d'un produit direct par $A^{\leqslant n}$, afin de *stocker* dans cette composante supplémentaire cette information locale supplémentaire. En chaque position, la seconde composante va contenir les n lettres qui sont à gauche. Afin de garantir que cette enrichissement soit réalisé correctement, nous allons nous restreindre aux langages des *mots bien formés*, c'est-à-dire, des mots où cet enrichissement est interprété correctement. Introduisons maintenant les définitions précises. Soit n un entier. On associe au timbre suff_n une fonction séquentielle $\sigma_n : A^* \to (A \times A^{\leqslant n})^*$ définie par

$$\sigma_n(a_0 \cdots a_p) = (a_0, 1)(a_1, \mathrm{suff}_n(a_0)) \cdots (a_n, \mathrm{suff}_n(a_0 \cdots a_{p-1})).$$

On associe à ce timbre un langage K_n sur l'alphabet $A_n = A \times A^{\leqslant n}$ défini par

$$K_n = \sigma_n(A^*).$$

Autrement dit, un mot $(a_0, t_0) \cdots (a_n, t_n)$ de A_n^* est dans K_n si $t_0 = 1$ et si $t_i = \mathrm{suff}_n(a_0 \cdots a_{i-1})$. De plus on note π_n la projection canonique de A_n^* vers A^*.

Proposition 3.20.

Les applications $\sigma_n : A^* \to K_n$ et $\pi_n : K_n \to A^*$ sont des applications bijectives réciproques.

Démonstration : Soit $u \in A^*$. Par définition de π_n, nous avons que $\pi_n(\sigma_n(u)) = u$. De plus, par définition $\sigma_n : A^* \to K_n$ est une application surjective. Ces applications sont sont donc bijectives et réciproques. ■

On peut remarquer, pour un langage L de A^*, on a

$$\sigma_n^{-1}(L) = \pi_n(L \cap K_n).$$

On en déduit le lemme suivant.

Lemme 3.21.

Pour L et L' des langages de A_n^*, nous avons les égalités suivantes :

1. $\pi_n((L \cup L') \cap K_n) = \pi_n(L \cap K_n) \cup \pi_n(L' \cap K_n)$,
2. $\pi_n((L \cap L') \cap K_n) = \pi_n(L \cap K_n) \cap \pi_n(L' \cap K_n)$,
3. $\big(\pi_n(L \cap K_n)\big)^c = \pi_n(L^c \cap K_n)$.

Le théorème qui suit constitue l'un des principaux outils pour manipuler les produits en couronnes. Ce théorème fut introduit par Straubing. Il s'agit de fournir une caractérisation de la variété de langages correspondant au produit en couronne de deux variétés. Nous en proposons une version légèrement différente adaptée au cas du produit en couronne par $\mathbf{D}$.

Théorème 3.22 (Principe du produit en couronne, Straubing [62, 65]).

Soient $\mathbf{V}$ une variété de monoïdes, L un langage régulier sur l'alphabet A et $\mathcal{W}$ la *ne*-variété de langages correspondant à $\mathbf{V} * \mathbf{D}$. Les conditions suivantes sont équivalentes.

(1) Le langage L est dans $\mathcal{W}(A^*)$,

(2) il existe un entier $n > 0$ et, pour tout mot $u \in A^{\leqslant n}$, un langage $L_u \in \mathcal{V}\big(A_n^*\big)$ tels que

$$L = \bigcup_{u \in A^{\leqslant n}} \Big(A^* u \cap \pi_n(L_u \cap K_n) \Big). \qquad (*)$$

Démonstration :

(**1**) $\to$ (**2**). Soient L un langage de $\mathcal{W}(A^*)$ et $\eta_L : A^* \to M_L$ son timbre syntaxique. Montrons que ce langage satisfait $(*)$. Par définition, il existe un monoïde M de $\mathbf{V}$ et un entier n tels que L est reconnu par un timbre $\psi : A^* \to N \subseteq M \circ A^{\leqslant n}$. On pose, pour $a \in A$, $\psi(a) = \big(f_a, \mathrm{suff}_n(a)\big)$ où $f_a : A^{\leqslant n} \to M$. On définit un morphisme $\eta : A_n^* \to M^{A^{\leqslant n}}$ en posant

$$\eta(a, u) = \begin{cases} A^{\leqslant n} \to M \\ s \mapsto f_a(su) \end{cases}$$

On pose

$$L_u = \bigcup_{(f,u) \in \psi(L)} \eta^{-1}(f).$$

Comme $M^{A^{\leqslant n}} \in \mathbf{V}$, on a $\eta^{-1}\big(f\big) \in \mathcal{V}(A_n^*)$ et donc $L_u \in \mathcal{V}(A_n^*)$. Montrons qu'avec ces notations l'égalité $(*)$ est satisfaite. Pour la suite on note R le membre droit de $(*)$.

- Montrons d'abord l'inclusion $L \subseteq R$. Soit $v = v_1 \cdots v_p \in L$ et soit $x = \psi(v)$. Par définition $x = (f, \mathrm{suff}_n(v))$ où f est donnée par

$$f : \begin{cases} A^{\leqslant n} \to M \\ s \mapsto f_{v_1}\big(s\big) f_{v_2}\big(\mathrm{suff}_n(sv_1)\big) \cdots f_{v_p}\big(\mathrm{suff}_n(sv_1 \cdots v_{p-1})\big) \end{cases}$$

Posons $u = \mathrm{suff}_n(v)$. On a alors $v \in A^*u$ par construction. De plus il existe un unique mot $v' \in K_n$ tel que $\pi_n(v') = v$. Il suffit donc de démontrer que $v' \in L_u$. Par définition,

$$v' = (v_1, 1)(v_2, \mathrm{suff}_n(v_1)) \cdots (v_p, \mathrm{suff}_n(v_1 \cdots v_{p-1})).$$

Donc,

$$\eta(v') = \begin{cases} A^{\leqslant n} \to M \\ s \mapsto f_{v_1}\big(s\big) f_{v_2}\big(sv_1\big) \cdots f_{v_p}\big(\mathrm{suff}_n(sv_1 \cdots v_{p-1})\big) \end{cases}$$

et donc $\eta(v') = f$. On a donc $v' \in \eta^{-1}(f)$ avec $x = (f, u) \in \psi(L)$ et finalement $v' \in L_u$ et et $v \in \pi_n(L_x \cap K_n)$.

- Montrons maintenant que $R \subseteq L$. Soit $u \in A^{\leqslant n}$ et soit $v \in \pi_n(L_u \cap K_n) \cap A^*u$. Montrons que $v \in L$. Par définition, il existe un unique mot $v' \in L_u \cap K_n$ tel que $\pi_n(v') = v$. Comme ce mot est bien formé, on a

$$v' = (v_1, 1)(v_2, \mathrm{suff}_n(v_1)) \cdots (v_p, \mathrm{suff}_n(v_1 \cdots v_{p-1})).$$

Notons f la fonction

$$f = \eta(v') = \begin{cases} A^{\leqslant n} \to M \\ s \mapsto f_{v_1}\big(s\big) f_{v_2}\big(sv_1\big) \cdots f_{v_p}\big(\mathrm{suff}_n(sv_1 \cdots v_{p-1})\big) \end{cases}$$

Comme $v' \in L_u$, nous avons que $(f, u) \in \psi(L)$ et comme $\psi(v) = (f, u)$ nous avons que $v \in L$.

(**2**) $\to$ (**1**). Soit L un langage régulier tel que (2) soit satisfaite. Montrons que ce langage appartient à $\mathcal{W}(A^*)$. Soit $u \in A^{\leqslant n}$. Comme $L_u \in \mathcal{V}(A_n^*)$, il existe un timbre $\eta : A_n^* \to M$ tel que $M \in \mathbf{V}$ et $P_u \subseteq M$ tel que $L_u = \eta^{-1}(P_u)$. On définit $\psi : A^* \to N \subseteq M \circ A^{\leqslant n}$ en posant $\psi(a) = \big(f_a, \mathrm{suff}_n(a)\big)$, où

$$f_a : \begin{cases} A^{\leqslant n} \to M \\ s \mapsto \eta(a, s) \end{cases}$$

Posons $F_u = \{f \in M^{A^{\leqslant n}} \mid f(1) \in P_u\} \cap N$ et montrons que

$$L \cap A^*u = \bigcup_{f \in F_u} \psi^{-1}(f, u).$$

- Soit $v \in L \cap A^*u$. Comme dans le premier point, nous avons $\psi(v) = (f, \mathrm{suff}_n(v)) = (f, u)$ où

$$f : \begin{cases} A^{\leqslant n} \to M \\ s \mapsto f_{v_1}\big(s\big) f_{v_2}\big(\mathrm{suff}_n(sv_1)\big) \cdots f_{v_p}\big(\mathrm{suff}_n(sv_1 \cdots v_{p-1})\big) \end{cases}$$

Par hypothèse, il existe un unique $v' \in L_u \cap K_n$ tel que

$$\eta(v') = \eta(v_1, 1)\eta(v_2, \mathrm{suff}_n(v_1)) \cdots \eta(v_p, \mathrm{suff}_n(v_1 \cdots v_{p-1})) \in P_u.$$

Or $\eta(v') = f(1)$ donc $f \in F_u$ et

$$v \in \bigcup_{f \in F_u} \psi^{-1}(f, u).$$

- Réciproquement, supposons

$$v \in \bigcup_{f \in F_u} \psi^{-1}(f, u).$$

Donc $\psi(v) = (f, u)$ où $f(1)$ est dans P_u. Or en prenant v' l'unique mot bien formé tel que $\pi(v') = v$, on a

$$\eta(v') = \eta(v_1, 1)\eta(v_2, \mathrm{suff}_n(v_1)) \cdots \eta(v_p, \mathrm{suff}_n(v_1 \cdots v_{p-1})) = f(1) \in P_u.$$

Donc $v' \in L_u$, ce qui conclut la preuve. ■

Remarques : La distinction entre cet énoncé du principe du produit en couronne et l'original est principalement cosmétique. Elle sera toutefois utile dans la suite pour faire le lien avec le problème de *séparation* (voir la section 3.6), ainsi qu'avec le théorème d'ajout des prédicats unaires (voir Théorème 1.13).

3.4 L'ajout des prédicats locaux

Il y dans la littérature un certain nombre de résultats concernant l'ajout de la relation successeur, c'est-à-dire du prédicat $x = y+1$. Un tel enrichissement correspond souvent à un produit en couronne par $\mathbf{D}$. Il n'existe néanmoins pas de théorème unifiant ce type de résultats. Ceci s'explique par l'existence de contre-exemples désagréables. Par exemple, dans le cas du fragment $\mathbf{FO}^1$, ajouter une relation binaire ne va pas modifier l'expressivité car celle-ci ne sera pas utilisable. Ajouter la relation successeur à $\mathbf{FO}^1$ ne correspond donc pas à un produit en couronne par $\mathbf{D}$. Afin de contourner ces difficultés désagréables, nous allons considérer les prédicats descriptifs locaux $\mathrm{LOC_D}$. Ceux-ci étant unaires, ils sont plus aisés à gérer. De plus, dans la plupart des cas raisonnables, ajouter les prédicats numériques locaux (LOC) équivaut à ajouter les prédicats descriptifs locaux ($\mathrm{LOC_D}$). Comme nous l'avons déjà évoqué, ce ne sera pas toujours le cas (voir la proposition 3.49).

Proposition 3.23 (Folklore).

Soient $k > 1$ et $n \geqslant 1$. Le fragment $\mathcal{B}\mathbf{\Sigma}_n[<, \mathrm{LOC_D}]$ est équivalent à $\mathcal{B}\mathbf{\Sigma}_n[<, \mathrm{LOC}]$. De même, le fragment $\mathbf{FO}^2_n[<, \mathrm{LOC_D}]$ est équivalent à $\mathbf{FO}^2_n[<, \mathrm{LOC}]$.

La preuve d'une telle proposition est très classique. Elle peut être réalisée par exemple à l'aide d'opérations syntaxiques élémentaires sur les formules ou à l'aide de jeux d'Ehrenfeucht-Fraïssé. On peut en effet remplacer les prédicats numériques de la forme $x = y + k$ par le prédicat d'égalité et propager syntaxiquement l'information de localité aux prédicats de lettres. Réciproquement, on code un prédicat descriptif local à l'aide d'une quantification soit existentielle, soit universelle. On préserve ainsi à la fois le nombre de variables utilisées et l'alternance de quantifications.

Grâce au théorème 1.13, nous savons ajouter des prédicats unaires. Comme les prédicats numériques locaux contiennent des prédicats binaires ($x = y + k$), ils ne tombent pas sous le coup de ce théorème. Quoi qu'il en soit, nous pouvons l'appliquer à l'ajout des prédicats descriptifs locaux.

Théorème 3.24.

Soient $\mathbf{F}$ un fragment de $\mathbf{MSO}[<]$, équivalent à une variété de monoïdes $\mathbf{V}$, L un langage régulier sur l'alphabet A et $\mathcal{W}$ la *ne*-variété de langages correspondant à $\mathbf{V} * \mathbf{D}$. Les conditions suivantes sont équivalentes.

(1) Le langage L est dans $\mathcal{W}(A^*)$,

(2) il existe un entier $n > 0$ et, pour tout mot $u \in A^{\leqslant n}$, un langage $L_u \in \mathcal{V}(A_n^*)$ tel que
$$L = \bigcup_{u \in A^{\leqslant n}} \Big(A^* u \cap \pi_n(L_u \cap K_n) \Big),$$

(3) le langage L est définissable dans $\mathbf{F}[\mathrm{LOC_D}]$.

Démonstration :

(**1**) $\leftrightarrow$ (**2**). Cette équivalence est donnée directement par le théorème du produit en couronne (voir Théorème 3.22).

(**2**) $\leftrightarrow$ (**3**). Afin de prouver cette équivalence, nous allons utiliser le théorème d'ajout des prédicats unaires (voir Théorème 1.13). Ce dernier établit, en reprenant les mêmes notations, qu'un langage L est définissable dans $\mathbf{F}[\mathrm{LOC_D}]$ si et seulement s'il existe un t-uplet $(Q_0, \ldots, Q_{t-1})$ de prédicats d'arité 0 de la classe $\mathrm{LOC_D}$, $\kappa = (P_0, \ldots, P_{k-1})$ un k-uplet de prédicats unaires de la classe $\mathrm{LOC_D}$, et pour tout $E \in \mathcal{P}([t])$, il existe un langage L_E appartenant à $\mathbf{F}(B_k^*)$, tels que
$$L = \bigcup_{E \in \mathcal{P}([t])} T_E \cap \pi_k(L_E \cap K_\kappa).$$

Or les prédicats $Q_0, \ldots, Q_{t-1}$ sont de la forme $\mathbf{a}(\max - k)$ pour $a \in A$ et k un entier. De même les prédicats $P_1(x), \ldots, P_{k-1}(x)$ sont de la forme $\mathbf{a}(x - k)$ pour $a \in A$ et k un entier. On note dans la suite n le plus grand entier k tel que soit $\mathbf{a}(\max - k)$ soit $\mathbf{a}(x - k)$ soit l'un des prédicats que l'on a introduit. Sans perte de généralité, quitte à ajouter artificiellement des prédicats, on peut supposer que μ contienne tous les prédicats de la forme $\mathbf{a}(\max - k)$ pour $k \leqslant n$ et $a \in A$. De même, sans perte de généralité, on suppose que κ contienne tous les prédicats de la forme $\mathbf{a}(x - k)$ pour $k \leqslant n$ et $a \in A$. On note pour la suite $i_{a,k}$ l'indice du prédicat $\mathbf{a}(x - k)$ dans le k-uplet κ, c'est-à-dire, $P_{i_{a,k}}(x) = \mathbf{a}(x - k)$.
Pour $a, b \in A$ deux lettres différentes, les prédicats $\mathbf{a}(\max - k)$ et $\mathbf{b}(\max - k)$ ne peuvent pas être tous deux évalués à *vrai* sur un même mot. On les dira alors *incompatibles*. Pour $E \in \mathcal{P}([t])$, soit T_E est vide, si E contient des entiers représentant deux prédicats 0-aires qui sont incompatibles, soit T_E est de la forme $A^* u$ pour $u \in A^{\leqslant n}$.

Il s'agit maintenant d'expliquer comment passer du langage L_E au langage L_u et réciproquement. Ces deux langages ne sont pas sur le même alphabet mais nous allons utiliser la stabilité par morphisme inverse des langages définissables dans le fragment $\mathbf{F}$ pour conclure.

(1) Supposons qu'on dispose d'un langage $L_E \in \mathbf{F}(B_k^*)$. Nous devons construire un langage L_u vérifiant les hypothèses du théorème. On définit le morphisme $\psi : A_n^* \to B_k^*$ en posant pour $a \in A$ et $v = v_0 \cdots v_p \in A^{\leqslant n}$, $\psi(a, v) = (a, \beta_v)$ où

$$\beta_v = \{i_{a,k} \mid a = u_{p-k+1}\}.$$

Le morphisme ainsi défini vérifie que l'image inverse d'un mot bien formé contient un unique mot qui est lui même bien formé. On pose $L_u = \psi^{-1}(L_E) \in \mathbf{F}(A_n^*)$ et nous avons $L \cap A^*u = \pi_n(L_u \cap K_n)$.

(2) Supposons maintenant qu'on dispose d'un langage $L_u \in \mathbf{F}(A_n^*)$. Nous devons construire un langage L_E vérifiant les hypothèses du théorème. Notons Ω l'ensemble des lettres qui apparaissent dans les mots du langage K_κ.
On définit le morphisme $\theta : B_k^* \to A_n^*$ en posant $\theta(a, E) = (a, 1)(a, 1)$ si (a, E) n'appartient pas à Ω et dans le cas contraire, $\theta(a, E) = (a, u_E)$ où $u_E = u_0 \cdots u_p$ est défini par

$$u_k = a \text{ si et seulement si } i_{a,p-k+1} \in E.$$

Le morphisme ainsi défini vérifie que l'image inverse d'un mot bien formé contient un unique mot qui est lui même bien formé. On pose $L_E = \theta^{-1}(L_u) \in \mathbf{F}(A_n^*)$ et nous avons $L \cap A^*u = \pi_k(L_E \cap K_\kappa)$. ■

Dans la définition des prédicats descriptifs locaux, nous avons choisi d'orienter la translation des prédicats de lettre vers la gauche. On pourrait également ajouter les prédicats de lettres translatés vers la droite. On obtiendrait alors la *ne*-variété $\mathbf{V} * \mathbf{LI}$ égale à $\mathbf{V} * \mathbf{D}$ (sauf pour $\mathbf{V} = \mathbf{I}$, voir l'article de Straubing [63]).

3.5 Le théorème de délai

Avant d'introduire la problématique du *délai* nous allons devoir introduire le formalisme des *variétés de catégories finies*. Une grande partie de ce que nous allons présenter provient l'article de Tilson [73]. Bien que nous utiliserons systématiquement la terminologie des catégories finies, il est parfois plus aisé de penser une catégorie finie comme un monoïde fini disposant d'une loi interne qui n'est pas définie sur toutes les paires d'éléments. Les catégories finies émergent relativement naturellement quand on étudie les produits en couronnes de variétés, et en particulier quand il s'agit de variétés *peu expressives*. Ainsi, si une variété contient le monoïde syntaxique du langage $(ab)^*$, il n'est plus nécessaire de recourir aux catégories finies. En effet, si ce monoïde est présent, alors il est toujours possible de réaliser une opération, appelée la *consolidation* de la catégorie, qui la transforme en un monoïde (ou semigroupe).

Une autre intuition permettant de saisir l'importance du langage $(ab)^*$ sera donnée dans la section suivante. En effet, dés que ce langage est présent dans une variété de langages, alors le langage des mots bien formés l'est également (voir la proposition 3.40).

3.5.1 Catégories finies

L'ensemble des définitions que nous allons présentés maintenant proviennent de l'article de Tilson [73]. *Un graphe* C est un ensemble d'*objets* noté $\mathrm{Ob}(C)$ tel qu'à chaque paire d'objets $(x, y) \in \mathrm{Ob}(C)$, on associe un ensemble $C(x, y)$ de *flèches* de x vers y.

Notation : Pour tout graphe C, on notera $|C|$ le nombre de flèches de C. Un graphe est fini si $|C|$ est fini et un graphe est à support fini si $|\mathrm{Ob}(C)|$ est fini.

Deux flèches e, f sont co-terminales s'il existe $x, y \in \mathrm{Ob}(C)$ telles que $e, f \in C(x, y)$. Elles sont dites consécutives s'il existe $x, y, z \in \mathrm{Ob}(C)$ telles que $e \in C(x, y)$ et $f \in C(y, z)$. Enfin, une flèche e est une boucle de l'objet x si $e \in C(x, x)$. Une loi de composition assigne à chaque couple de flèches consécutives, e, f une flèche ef. Cette loi est dite associative si pour des flèches consécutives e, f, g on a $(ef)g = e(fg)$. Soit C un graphe muni d'une loi de composition associative. Pour tout objet x de C, l'ensemble des boucles de x est un semigroupe que l'on appelle *le semigroupe* local de x. On dit qu'une flèche e est *l'élément neutre* en x si pour tout objet y, flèche $f \in C(y, x)$ et $g \in C(x, y)$, on a $fe = f$ et $ef = f$. On notera un tel élément 1_x.

Définition 3.25 (Catégories).

Une catégorie C est un graphe muni d'une loi de composition interne associative et possédant un élément neutre en x pour chaque objet x.

Si C est une catégorie, alors les semigroupes locaux sont des monoïdes que l'on appelle les *monoïdes locaux*.

Il est utile de penser les catégories comme des monoïdes dont la loi de composition interne n'est pas définie partout. Ainsi, un monoïde est une catégorie qui ne possède qu'un seul objet. Les notions de morphisme, morphisme relationnel, quotient, sous-monoïde, congruence aux catégories finies.

Nous donnons maintenant une notion de division de catégories. La catégorie C divise la catégorie D s'il existe une application $\tau : \mathrm{Ob}(C) \to \mathrm{Ob}(D)$ et pour chaque couple $(x, y) \in \mathrm{Ob}(C)^2$, une relation $\tau : C(x, y) \to D(x, y)$ telle que :

- Pour chaque flèche e, $\tau(e)$ est non vide.
- Pour chaque paire de flèches e et f consécutives, $\tau(e)\tau(f) \subseteq \tau(ef)$.
- Pour chaque paire flèches co-terminales e et f, $\tau(e) \cap \tau(f) = \emptyset$.
- Pour chaque objet x, $1_{\tau(x)} \in \tau(1_x)$.

On appelle *division* l'application $\tau : C \to D$. On remarque qu'il s'agit d'un morphisme relationnel injectif de catégories et donc cette condition de division généralise celle donnée

dans la proposition 2.1. Soient C et D deux catégories. Si C est une sous-catégorie de D ou si C est une catégorie quotient de D, alors C divise D.

On remarque qu'un monoïde M divise un monoïde N si M vu comme une catégorie divise N également vu comme une catégorie.

Définition 3.26 (Variété de catégories finies).

Une classe de catégories finies est une variété si elle est stable par produit direct et par division de catégories.

Une variété de monoïdes $\mathbf{V}$ engendre une variété de catégories finies que l'on note $\mathbf{gV}$. L'étude du global d'une variété de monoïdes a été l'objet de nombreuses études (voir par exemple l'article [5]). On note également $\boldsymbol{\ell}\mathbf{V}$ la classe des catégories dont les monoïdes locaux sont dans $\mathbf{V}$. La classe $\boldsymbol{\ell}\mathbf{V}$ est également une variété de catégories finies. Une variété de monoïdes est *locale* si $\boldsymbol{\ell}\mathbf{V} = \mathbf{gV}$. La localité est un outil efficace pour décider les produits semi-directs. Elle est cependant parfois difficile à démontrer, par exemple dans le cas de la variété $\mathbf{DA}$. Le théorème suivant résume certains des cas de variétés locales connues.

Théorème 3.27 (Simon [14], Tilson [73], Almeida [1]).

Les variétés $\mathbf{J_1}$, $\mathbf{DA}$, $\mathbf{A}$ et $\mathbf{G}$ ainsi que toutes les variétés de groupes non triviales sont locales.

L'étude de la localité des variétés de monoïdes demeure l'objet de travaux (par exemple les articles [34, 22]).

3.5.2 Le théorème de la catégorie dérivée pour D

Après avoir introduit les variétés de catégories finies, nous allons les utiliser afin de mieux comprendre le produit en couronne par $\mathbf{D}$. Une première étape consiste à définir la n-catégorie dérivée d'un langage pour $\mathbf{D}$.

Étant donné un entier n, on définit la catégorie D_n sur l'alphabet A en prenant pour ensemble d'objets l'ensemble $A^{\leqslant n}$ et pour ensemble de flèches de u à v l'ensemble

$$D_n(u, v) = \{w \in A^* \mid \mathrm{suff}_n(uw) = v\}.$$

Ainsi la catégorie D_2 est représentée dans la figure 3.5.2. Afin d'améliorer la lisibilité, les flèches de 1 vers aa, ab, ba et bb sont volontairement omises ainsi que les langages étiquetant les flèches qui ne sont pas des boucles. L'ensemble des flèches de aa vers ba est composé des mots dans le langage A^*ba alors que l'ensemble des flèches de ba vers bb est

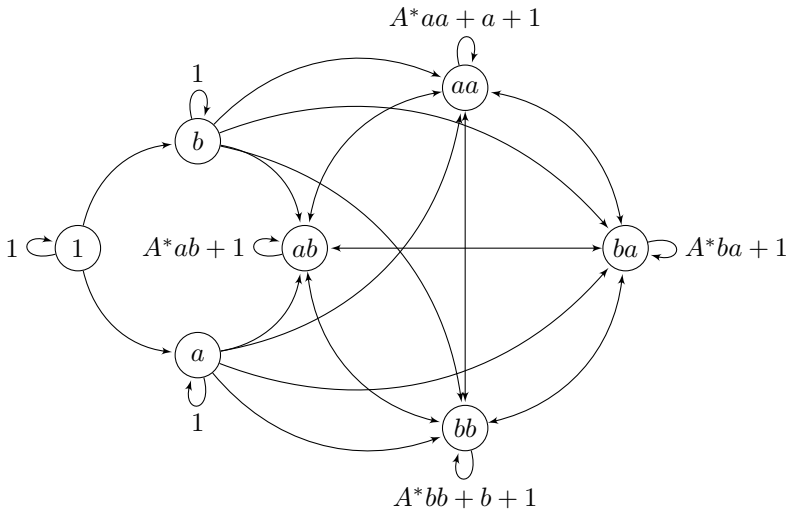


FIGURE 3.1 – La catégorie D_2 de $\{a, b\}$

composé des mots dans le langage $A^*aa + a$.

Soient L un langage régulier, $\eta : A^* \to M$ son timbre syntaxique et $u, v \in A^{\leqslant n}$. On définit une relation $\sim$ sur D_n en posant, pour $p, q \in D_n(u, v)$, $p \sim q$ si pour tout mot $r \in D_n(1, u)$, $\eta(rp) = \eta(rq)$. On montre que cette relation est une congruence de D_n et pour chaque paire de flèches le nombre de classes d'équivalences pour cette relation est bornée par la taille de M. On en déduit donc que cette relation est une congruence d'indice fini de D_n.

Remarque : Pour $p, q \in D_n(u, v)$ si $\eta(p) = \eta(q)$, alors $p \sim q$.

On note $D_n(L)$ la catégorie finie $D_n/\sim$ et $\theta_n : D_n \to D_n(L)$ le morphisme surjectif associé. On note de plus $\theta_n^{(u,v)} : D_n(u, v) \to D_n(L)(u, v)$ l'application surjective qui à une flèche de $D_n(u, v)$ associe sa classe d'équivalence. Comme θ_n est un morphisme, nous avons

$$\theta_n^{(u,v)}(p)\theta_n^{(v,w)}(q) = \theta_n^{(u,w)}(pq)$$

pour $u, v, w \in A^{\leqslant n}$, $p \in D_n(u, v)$ et $q \in D_n(v, w)$.

Le théorème suivant justifie l'introduction des notions de variétés de catégories finies dans l'étude du produit en couronne. Pour un langage régulier L, il établit que la catégorie $D_n(L)$, pour un certain entier n, appartient à $\mathbf{gV}$ si et seulement si le timbre syntaxique de ce dernier appartient à $\mathbf{V} * \mathbf{D}$. Comme le théorème du produit en couronne, il peut être prouvé dans un cadre plus général, qui sort du cadre de cette thèse.

Théorème 3.28 (Théorème de la catégorie dérivée, Tilson [73]).

Soient $\mathbf{V}$ une variété de monoïdes, L un langage régulier sur l'alphabet A et $\mathcal{W}$ la *ne*-variété de langages correspondant à $\mathbf{V}*\mathbf{D}$. Les conditions suivantes sont équivalentes.

(1) Le langage L est dans $\mathcal{W}(A^*)$,

(2) il existe un entier $n > 0$ et, pour tout mot $u \in A^{\leqslant n}$, un langage $L_u \in \mathcal{V}\big(A_n^*\big)$ tel que

$$L = \bigcup_{u \in A^{\leqslant n}} \Big(A^* u \cap \pi_n(L_u \cap K_n) \Big) \qquad (*)$$

(3) il existe un entier $n > 0$ tel que $D_n(L)$ appartient à $\mathbf{gV}$.

De plus, le même entier convient pour les points (2) et (3).

Démonstration : Dans la suite de la preuve, $\eta : A^* \to M$ est le timbre syntaxique de L. Soit $u \in A^{\leqslant n}$. On définit $\sigma_n^u : A^* \to A_n^*$ la *fonction séquentielle d'enrichissement décalée* telle que l'image d'un mot est un facteur bien formé décalé par le mot u. Plus précisément, pour tout mot p, $\sigma_n^u(p) = \mathrm{suff}_{|p|}(\sigma_n(up))$. Par exemple,

$$\sigma_2^a(abba) = (a,a)(b,aa)(b,ab)(a,bb)$$

(**1**) $\leftrightarrow$ (**2**). C'est exactement le théorème du produit en couronne (voir Théorème 3.22).

(**2**) $\rightarrow$ (**3**). Supposons que L vérifie (2). Il existe donc un entier n entier et pour tout $u \in A^{\leqslant n}$ des langages L_u tels que tel que L vérifie le membre droit de $(*)$. Montrons que $D_n(L)$ appartient à $\mathbf{gV}$. Soit $\psi : A_n^* \to N$ un timbre où N est un monoïde dans $\mathbf{V}$ tel que pour tout $u \in A^{\leqslant n}$, L_u est reconnu par ψ. Montrons que $D_n(L)$ divise N. On va construire une division $\tau : D_n(L) \to N$. Comme N est une catégorie disposant d'un seul objet, l'application entre objets de τ est triviale. Nous devons définir une relation sur les flèches. Soient $u, v \in A^{\leqslant n}$, on définit $\tau : D_n(L)(u,v) \to N$ en posant

$$\tau(m) = \psi\Big(\sigma_n^u\big(\theta_n^{(u,v)^{-1}}(m)\big)\Big).$$

On remarque que pour tout objet, l'image du neutre local contient le neutre de N et comme θ_n est un morphisme surjectif de catégories, l'image de chaque flèche est non vide. Soient $w \in A^{\leqslant n}$, $m \in D_n(L)(u,v)$ et $n \in D_n(L)(v,w)$.

- Montrons que $\tau(m)\tau(n) \subseteq \tau(mn)$. Soient $x \in \tau(m)$ et $y \in \tau(n)$. Par définition, il existe deux mots s et t dans A^* tels que $s \in \theta_n^{(u,v)^{-1}}(m)$ et $t = \theta_n^{(v,w)^{-1}}(n)$ et donc,

$$st = \theta_n^{(u,w)^{-1}}(mn).$$

Posons $\psi(\sigma_n^u(s)) = x$ et $\psi(\sigma_n^v(t)) = y$. Comme $\sigma_n^u(st) = \sigma_n^u(s)\sigma_n^v(t)$, nous avons $\psi(\sigma_n^u(st)) = xy$. On en déduit que

$$xy \in \psi\Big(\sigma_n^u\big(\theta_n^{(u,w)^{-1}}(mn)\big)\Big) = \tau(mn).$$

- Supposons maintenant que $m' \in D_n(L)(u,v)$ tel que $\tau(m) \cap \tau(m') \neq \emptyset$. Il existe donc $p \in {\theta_n^{(u,v)}}^{-1}(m)$ et $q \in {\theta_n^{(u,v)}}^{-1}(m')$ tel que $\psi(\sigma_n^u(p)) = \psi(\sigma_n^u(q))$. On en déduit que $\sigma_n^u(p) \sim_{L_w} \sigma_n^u(q)$ pour tout $w \in A^{\leqslant n}$. En particulier, pour tout mot $r \in A^*u$ et tout mot $t \in A^*$, $rpt \in L$ si et seulement si $rqt \in L$. Par définition de $D_n(L)$, on a $m = m'$.

L'application $\tau : D_n \to N$ est bien une division d'où $D_n(L)$ divise N et donc $D_n(L) \in \mathbf{gV}$.

(**3**) $\to$ (**2**). On suppose qu'il existe un entier n tel que la catégorie $D_n(L)$ appartienne à $\mathbf{gV}$. Montrons que L vérifie (2). Soit $\tau : D_n(L) \to N$ une division où N est un monoïde de V. Pour tout $u \in A^{\leqslant n}$, et toute lettre a, on pose $m_a^u = \theta_n^{(u,\mathrm{suff}_n(ua))}(a)$ et on choisit un élément $n_{(a,u)} \in \tau(m_a^u)$. On peut alors définir le morphisme $\psi : A_n^* \to N$ en posant $\psi(a,u) = n_{(a,u)}$ pour chaque lettre $a \in A$ et chaque mot $u \in A^{\leqslant n}$. On note également

$$P_u = \bigcup_{v \in D_n(1,u) \cap L} \tau(\theta_n^{(1,v)}(v)).$$

Pour conclure la preuve, il est suffisant de montrer que

$$L \cap A^*u = \pi_n(\psi^{-1}(P_u) \cap K_n) \cap A^*u.$$

- Soit $p \in L \cap A^*u$. Montrons que $p \in \pi_n(\psi^{-1}(P_u) \cap K_n)$. Pour cela, il suffit de montrer que $\psi(\sigma_n(p))$ appartient à P_u. Posons

$$\sigma_n(p) = (p_1, v_1)(p_2, v_2) \cdots (p_k, v_k).$$

Par construction

$$\psi(\sigma_n(p)) = n_{(p_1,v_1)} \cdots n_{(p_k,v_k)}$$

où $n_{(p_i,v_i)} \in \tau(m_{p_i}^{v_i})$. Comme τ est une division, nous avons

$$\begin{aligned} \psi(\sigma_n(p)) = n_{(p_1,v_1)} \cdots n_{(p_k,v_k)} &\in \tau(m_{p_1}^{v_1}) \cdots \tau(m_{p_k}^{v_k}) \\ &\subseteq \tau(m_{p_1}^{v_1} \cdots m_{p_k}^{v_k}) = \tau(\theta_n^{(u,v)}(p)) \subseteq P_u. \end{aligned}$$

- Réciproquement, supposons que $p \in \pi_n(\psi^{-1}(P_u) \cap K_n) \cap A^*u$. Nous avons donc $\psi(\sigma_n(p)) \in P_u$. Ce qui implique qu'il existe $q \in D_n(1,u)$ tel que $q \in L$ et

$$\psi(\sigma_n(p)) \in \tau(\theta_n^{(1,u)}(q)).$$

De plus, on a vu que

$$\psi(\sigma_n(p)) \in \tau(\theta_n^{(1,u)}(p)).$$

Comme $\tau(\theta_n^{(1,u)}(p)) \cap \tau(\theta_n^{(1,u)}(q)) \neq \emptyset$ et que τ est une division, on a $\theta_n^{(1,u)}(p) = \theta_n^{(1,u)}(q)$ et, comme $q \in L$, on a $p \in L$. Ce qui conclut la preuve. ■

La proposition suivante va nous permettre d'introduire la question du délai pour le produit en couronne par $\mathbf{D}$.

Proposition 3.29.

Soit L un langage régulier de A^*. Pour tout entier $n \leqslant n'$, la catégorie $D_{n'}(L)$ divise la catégorie $D_n(L)$.

Démonstration : Afin de prouver ce lemme, nous construisons une division $\tau : D_{n'}(L) \to D_n(L)$. Pour tout mot $u \in A^{\leqslant n'}$, on pose $\tau(u) = \mathrm{suff}_n(u)$. Pour $u, v \in A^{\leqslant n'}$, et $m \in D_n(L)(u, v)$, on définit

$$\tau(m) = \theta_n^{(\mathrm{suff}_n(u),\mathrm{suff}_n(v))}\Big(\theta_{n'}^{(u,v)^{-1}}(m)\Big).$$

Montrons que la relation τ ainsi construite est bien une division. L'image de chaque flèche est non vide et l'image du neutre local contient au moins le neutre local.

- Soient $w \in A^{\leqslant n'}$ et $m' \in D_{n'}(L)(v, w)$. Montrons que

$$\tau(m)\tau(m') \subseteq \tau(mm').$$

Soient $x \in \tau(m)$ et $y \in \tau(m')$. Par définition, il existe deux mots $p \in D_{n'}(u, v)$ et $q \in D_{n'}(v, w)$ tels que

$$\theta_{n'}^{(u,v)}(p) = m \text{ et } \theta_n^{(\mathrm{suff}_n(u),\mathrm{suff}_n(v))}(p) = x$$
$$\theta_{n'}^{(v,w)}(q) = m' \text{ et } \theta_n^{(\mathrm{suff}_n(v),\mathrm{suff}_n(w))}(q) = y.$$

Par conséquent

$$\theta_{n'}^{(u,w)}(pq) = mm' \text{ et } \theta_n^{(\mathrm{suff}_n(u),\mathrm{suff}_n(w))}(pq) = xy$$

et donc $xy \in \tau(mm')$

- Soit $m' \in D_{n'}(L)(u, v)$ tel que $\tau(m) \cap \tau(m') \neq \emptyset$. Montrons que $m = m'$. Soit $x \in \tau(m) \cap \tau(m')$. Par définition, il existe deux mots $p, q \in D_{n'}(u, v)$ tels que

$$\theta_{n'}^{(u,v)}(p) = m \text{ et } \theta_n^{(\mathrm{suff}_n(u),\mathrm{suff}_n(v))}(p) = x$$
$$\theta_{n'}^{(u,v)}(q) = m' \text{ et } \theta_n^{(\mathrm{suff}_n(u),\mathrm{suff}_n(v))}(q) = x.$$

Soit $r \in A^*u$. En particulier $r \in A^*\mathrm{suff}_n(u)$ et comme

$$\theta_n^{(\mathrm{suff}_n(u),\mathrm{suff}_n(v))}(p) = \theta_n^{(\mathrm{suff}_n(u),\mathrm{suff}_n(v))}(q),$$

on a que $\eta(rp) = \eta(rq)$. On en déduit que

$$m = \theta_{n'}^{(u,v)}(p) = \theta_{n'}^{(u,v)}(q) = m'.$$

Ce qui conclut la démonstration. ■

3.5.3 Le théorème de délai

Le théorème de la catégorie dérivée et la proposition 3.29 montre que décider le problème d'appartenance pour le produit en couronne $\mathbf{V} * \mathbf{D}$ se réduit à trouver une borne et à décider la variété de catégories $\mathbf{gV}$. En effet, un langage L à son timbre syntaxique qui à appartient à $\mathbf{V} * \mathbf{D}$ si et seulement s'il existe un entier N tel que pour tout $n \geqslant N$, la catégorie $D_n(L)$ appartient à $\mathbf{gV}$. La question du délai pour le produit en couronne par $\mathbf{D}$ consiste à calculer un tel entier N.

La question du délai va se simplifier légèrement en introduisant la catégorie suivant qui est constructible à partir du monoïde syntaxique.

Définition 3.30.

Soit S un semigroupe. On définit la catégorie S_E ainsi :

- Les objets de S_E sont les idempotents de S,
- Pour $e, f \in E(S)$, $S_E(e, f) = eSf$.

Remarque : Soient S un semigroupe, $e, f, g \in E(S)$ ainsi que $m \in S_E(e, f)$ et $m' \in S_E(f, g)$. Nous avons que

$$mm' \in eSffSg \subseteq eSg$$

et donc $mm' \in S_E(e, g)$. De plus, pour chaque idempotent $e \in E(S)$, $S_E(e, e)$ est bien un monoïde en posant e son élément neutre.

La catégorie S_E contient toute l'information nécessaire pour décider l'appartenance à $\mathbf{V} * \mathbf{D}$, grâce au théorème de délai que nous présentons maintenant. La première version de ce théorème a été établie par Straubing [63].

Théorème 3.31 (Le théorème de délai, Straubing [63], Tilson [73]).

Soit $\mathbf{V}$ une variété de monoïdes finis, L un langage régulier sur l'alphabet A et $\mathcal{W}$ la ne-variété de langages correspondant à $\mathbf{V} * \mathbf{D}$. Les conditions suivantes sont équivalentes.

(1) Le langage L est dans $\mathcal{W}(A^*)$,
(2) il existe un entier $n > 0$ tel que $D_n(L)$ appartient à $\mathbf{gV}$,
(3) la catégorie S_E appartient à $\mathbf{gV}$, où S est le semigroupe syntaxique de L,
(4) la catégorie $D_n(L)$ appartient à $\mathbf{gV}$, où $n \geqslant |M| + 1$.

Il s'agit d'un résultat difficile à prouver. Il va nous permettre d'obtenir un certain nombre de résultats de décidabilité, une fois que nous aurons des outils afin de décider l'appartenance d'une catégorie à une variété de catégories. Comme le montre le corollaire suivant, le cas des variétés locales se simplifie grandement. Dans ce cas, la décidabilité de $\mathbf{V} * \mathbf{D}$ se réduit à la décidabilité de $\mathbf{V}$.

Corollaire 3.32.

Soit $\mathbf{V}$ variété de monoïdes finis. Alors $\mathbf{V} * \mathbf{D} \subseteq \mathbf{LV}$. Si $\mathbf{V}$ est une variété locale, alors $\mathbf{V} * \mathbf{D} = \mathbf{LV}$. En particulier, pour tout langage disposant d'une lettre neutre l'appartenance de son timbre syntaxique à $\mathbf{V} * \mathbf{D}$ est équivalente à l'appartenance à $\mathbf{V}$.

Démonstration : Soient $\eta : A^* \to M$ un timbre et $S = \eta(A^+)$. Le timbre η appartient à $\mathbf{LV}$ si et seulement si S_E appartient à $\boldsymbol{\ell}\mathbf{V}$. De plus nous avons que $\mathbf{gV} \subseteq \boldsymbol{\ell}\mathbf{V}$ par définition de ces deux classes de catégories. D'après le théorème du délai, le timbre η appartient à $\mathbf{V} * \mathbf{D}$ si et seulement si S_E appartient à $\mathbf{gV}$ ce qui implique que S_E appartient à $\boldsymbol{\ell}\mathbf{V}$ et donc η appartient à $\mathbf{LV}$. On a bien que $\mathbf{V} * \mathbf{D} \subseteq \mathbf{LV}$. Si la variété est locale, nous avons la réciproque puisque par définition $\mathbf{gV} = \boldsymbol{\ell}\mathbf{V}$.

Si S est un monoïde, le timbre η appartient à $\mathbf{LV}$ si et seulement si S appartient à $\mathbf{V}$. Or, pour tout langage L de A^* disposant d'une lettre neutre, son timbre syntaxique η_L vérifie que $\eta_L(A^+)$ est un monoïde. On en conclut qu'un langage à lettre neutre appartient à $\mathbf{V} * \mathbf{D}$ si et seulement s'il appartient à $\mathbf{V}$. ■

Du corollaire précédent, on déduit la proposition suivante qui nous sera utile à plusieurs reprises dans le chapitre suivant.

Proposition 3.33.

Le langage $(ab)^*$ a son timbre syntaxique dans $\mathbf{J_1} * \mathbf{D}$.

Démonstration : On rappelle que la variété $\mathbf{J_1}$ est locale. D'après le corollaire 3.32, $\mathbf{J_1} * \mathbf{D} = \mathbf{LJ_1}$. Il suffit donc de vérifier que le timbre syntaxique de $(ab)^*$ est dans $\mathbf{LJ_1}$. On rappelle également que ce timbre est le morphisme $\psi : \{a, b\}^* \to B_2^1$ avec B_2^1 le monoïde de Brandt ayant la représentation en $\mathcal{D}$-classe suivante :

^{*1}

$^*ba$	b
a	$^*ab$

$^*a^2$

Il y a donc trois monoïdes locaux abB_2^1ab, baB_2^1ba et aaB_2^1aa. Les deux premiers sont isomorphes au monoïde $\{0, 1\}$ et le dernier au monoïde trivial. Ils appartiennent donc tous à $\mathbf{J_1}$, ce qui conclut la preuve. ■

Le corollaire suivant résume la conséquence principale du théorème de délai.

Corollaire 3.34.

Soit $\mathbf{V}$ une variété de monoïdes finis telle que l'appartenance à $\mathbf{gV}$ est décidable. Alors, l'appartenance d'un timbre à $\mathbf{V} * \mathbf{D}$ est décidable.

La réciproque de ce corollaire, conséquence des travaux de Tilson [73] et énoncée par Auinger [8], est également vraie mais sort du cadre de cette thèse. Nous allons maintenant étudier différents critères de décidabilité pour l'appartenance d'une catégorie à $\mathbf{gV}$.

3.6 Digression sur la séparation et les monoïdes de Brandt

Dans cette partie, nous allons revenir sur la preuve du théorème de la catégorie dérivée, en utilisant la séparation par des variétés de langages. On notera que le théorème de la catégorie dérivée sera redémontré dans le troisième chapitre (voir Théorème 4.28) en utilisant les outils introduits ici.

Intuitivement une catégorie peut être vue comme un *monoïde partiel* : un monoïde dont la loi interne n'est pas définie sur l'ensemble de ses éléments. Assez naturellement, on peut associer un semigroupe à une catégorie en ajoutant un zero. On appelle cette opération la *consolidation* de la catégorie.

Définition 3.35.

Soit C une catégorie. On définit le *semigroupe* consolidé

$$C_{\mathrm{cd}} = \left(\bigcup_{e,f \in \mathrm{Ob}(C)} \{e\} \times C(e,f) \times \{f\} \right) \cup \{0\}$$

où le produit est défini par

$$(e,m,f)(g,n,h) = \begin{cases} (e,mn,h) \text{ si } f = g, \\ 0 \text{ sinon.} \end{cases}$$

Remarques : On peut vérifier que le consolidé d'une catégorie est effectivement un semigroupe. En effet, le produit est bien défini car si m et n sont des flèches consécutives, alors mn est également une flèche de la catégorie. De même l'associativité découle de l'associativité du produit des flèches de la catégorie.

La proposition suivante, tirée de l'article [73, Proposition 16.1], donne un lien intéressant entre la catégorie S_E et le consolidé C_{cd}.

Proposition 3.36.

Soit C une catégorie finie. Les catégories C et $(C_{\mathrm{cd}})_E$ se divisent mutuellement.

La proposition suivante nous sera utile par la suite, pour connecter la question de la séparation aux monoïdes de la forme $D_n(L)^1_{\mathrm{cd}}$.

Proposition 3.37.

Soient L un langage régulier et $n \geqslant 1$ un entier. Pour tout mot $u \in A^{\leqslant n}$, les langages $\pi_n^{-1}(L \cap A^*u) \cap K_n$ et $\pi_n^{-1}(L^c \cap A^*u) \cap K_n$ sont reconnus par $D_n(L)^1_{\mathrm{cd}}$.

Démonstration : On définit $\eta : A_n^* \to D_n(L)^1_{\mathrm{cd}}$ en posant, pour $a \in A$ et $u \in A^{\leqslant n}$,

$$\eta(a,u) = (u, \theta^{(u,\mathrm{suff}_n(ua))}(a), \mathrm{suff}_n(ua)).$$

On remarque dans un premier temps qu'un mot qui n'est pas bien formé va nécessairement être envoyé sur 0. En effet, pour tout mot $(a_0,u_0)\cdots(a_p,u_p) \in A_n^* - K_n$, il existe un entier $i < p$ tel que $u_{i+1} \neq \mathrm{suff}_n(u_ia_i)$. Dans ce cas, en omettant la partie centrale

$$\eta\big((a_i,u_i)\big)\eta\big((a_{i+1},u_{i+1})\big) = \big(u_i, \_, \mathrm{suff}(u_ia_i)\big)\big(u_{i+1}, \_, \mathrm{suff}(u_{i+1}a_{i+1})\big) = 0.$$

En particulier, chaque élément de la forme $(1, \_, u) \in D_n(L)^1_{\mathrm{cd}}$ ne reconnaît que des éléments de K_n dont la première composante termine par le facteur u. Prenons un mot $v \in L \cap D_n(1,u)$ et un mot $w \in D_n(1,u)$ tels que $\theta_n^{(1,u)}(v) = \theta_n^{(1,u)}(w)$. Par construction de $\theta_n^{(1,u)}$, on a $w \in L$. On en déduit les égalités suivantes qui concluent la preuve :

$$\pi_n^{-1}(L \cap A^*u) \cap K_n = \bigcup_{m \in \theta_n^{(1,u)}\left(L \cap D_n(1,u)\right)} \eta^{-1}(1,m,u)$$
$$\pi_n^{-1}(L^c \cap A^*u) \cap K_n = \bigcup_{m \in \theta_n^{(1,u)}\left(L^c \cap D_n(1,u)\right)} \eta^{-1}(1,m,u)$$

■

Le problème de la *séparation* de deux langages par une classe de langages peut être énoncé ainsi. Soient $\mathcal{L}$ une classe de langages, L_1 et L_2 deux langages de A^*. On dit que L_1 est $\mathcal{L}$*-séparable* de L_2 s'il existe un langage $L \in \mathcal{L}(A^*)$ tel que $L_1 \subseteq L$ et $L_2 \cap L = \emptyset$. Le problème de la séparation par des (ne)-variétés de langages est une instance d'un problème algébrique plus général, le calcul des *point-like*. Le théorème suivant établit une caractérisation des langages séparables par une (ne)-variété de langages.

Théorème 3.38 (Théorème de séparation, Almeida [3]).

Soient $\mathbf{V}$ une variété de monoïdes ou une *ne*-variété de timbres, L_1 et L_2 deux langages réguliers sur l'alphabet A et $\eta : A^* \to M$ un timbre reconnaissant L_1 et L_2. Les deux conditions sont équivalentes.

(1) Le langage L_1 est $\mathcal{V}$-séparable de L_2.

(2) Il existe un timbre $\psi : A^* \to N \in \mathbf{V}$ tel que pour tout $(x, y) \in \eta(L_1) \times \eta(L_2)$,

$$\psi(\eta^{-1}(x)) \cap \psi(\eta^{-1}(x)) = \emptyset.$$

Ce théorème peut être un outil intéressant pour établir des théorèmes comme le théorème de la catégorie dérivée.

Théorème 3.39 (Théorème de la catégorie dérivée, *via* la $\mathcal{V}$-séparation).

Soient $\mathbf{V}$ une variété de monoïdes, L un langage régulier sur l'alphabet A et $\mathcal{W}$ la *ne*-variété de langages correspondant à $\mathbf{V} * \mathbf{D}$. Les conditions suivantes sont équivalentes.

(1) Le langage L est dans $\mathcal{W}(A^*)$,

(2) il existe un entier $n > 0$ tel que pour tout mot $u \in A^{\leqslant n}$ un langage $L_u \in \mathcal{V}\big(A_n^*\big)$ tel que

$$L = \bigcup_{u \in A^{\leqslant n}} \Big(A^* u \cap \pi_n(L_u \cap K_n) \Big),$$

(3) il existe un entier $n > 0$ tel que pour tout mot $u \in A^{\leqslant n}$ les langages $\pi_n^{-1}(L \cap A^* u) \cap K_n$ et $\pi_n^{-1}(L^c \cap A^* u) \cap K_n$ sont $\mathcal{V}$-séparables.

(4) il existe un entier $n > 0$ tel que $D_n(L)$ appartient à $\mathbf{gV}$.

De plus, le même entier convient pour les points (2), (3) et (4).

Reprouver le théorème de la catégorie dérivée en utilisant la séparation comme outil de preuve ne serait qu'une reformulation de la preuve classique. Toutefois, cette formulation permet d'obtenir une preuve facilement adaptable à d'autres contextes, comme par exemple aux cas des *ne*-variétés de timbres ou des *variétés positives*. En effet, le théorème central de cette approche, le théorème 3.38, est aisément adaptable à ces différents contextes. Nous utiliserons cette approche pour prouver le théorème de la catégorie dérivée dans le chapitre suivant (voir Théorème 4.28).

Le langage $(ab)^*$ et son monoïde syntaxique jouent un rôle particulier dans l'étude des produits en couronne. Son monoïde syntaxique, le monoïde de Brandt d'ordre 2, possède 6 éléments. On le note B_2^1.

^{*1}

$^*ba$	b
a	$^*ab$

$^*a^2$

FIGURE 3.2 – $\mathcal{D}$-classes du monoïde syntaxique du langage $(ab)^*$.

Proposition 3.40.

Soit $\mathcal{V}$ une *ne*-variété de langages contenant le langage $(ab)^*$. Pour tout alphabet A et tout entier n, le langage K_n de A_n^* est dans $\mathcal{V}(A_n^*)$.

Démonstration : Par hypothèse, le langage $(ab)^* \in \mathcal{V}(\{a,b\})$. On pose $A = \{c_1, \ldots, c_p\}$. On définit $\psi : A_n^* \to \{a,b\}^*$, le morphisme tel que pour toute lettre $c \in A$ et pour tout mot $u \in A^{\leqslant n}$ de longueur non nulle $\psi(c,u) = ab$ et $\psi(c,1) = a$. À l'aide d'un tel morphisme, on peut obtenir le langage des mots qui possèdent une lettre de la forme $(c,1)$, c'est-à-dire

$$\bigcup_{c\in A} A_n^*(c,1)A_n^* = \psi^{-1}((ab)^*)^c \in \mathcal{V}(A_n^*)$$

On définit également le morphisme suivant

$$\psi_{(c,u)} : \begin{cases} A_n^* & \to \{a,b\}^* \\ (c,u) & \mapsto a \\ (c', \mathrm{suff}_n(uc)) & \mapsto b \text{ pour tout } c' \in A \\ (c',v) & \mapsto ab \text{ pour } c \neq c' \text{ et } v \notin A^*c \end{cases}$$

À l'aide de ce morphisme on obtient le langage des mots tels que juste derrière chaque occurrence de la lettre (c,u) on retrouve la lettre $(c', \mathrm{suff}_n(uc))$, c'est-à-dire

$$L_{(c,u)} = \psi_{(c,u)}^{-1}((ab)^*) = B_{(c,u)}^*\Big((c,u)(c',\mathrm{suff}(uc))B_{(c,u)}^*\Big)^*$$

où $B_{(c,u)} = A - \{(c,u)\}$. Enfin,

$$K_n = \Big(\bigcap_{(c,u)\in A_n} L_{(c,u)}\Big) \cap \Big(\bigcup_{c\in A} A_n^*(c,1)A_n^*\Big).$$

En effet, l'intersection des langages de la forme $L_{(c,u)}$ garantit que les mots sont des facteurs de mots bien formés et le langage

$$\bigcup_{a\in A} A_n^*(c,1)A_n^*$$

garantit que au moins une lettre aura 1 comme deuxième composante. Comme les mots sont des facteurs de mots bien formés, cela impose qu'ils soient tous bien formés. Ce qui conclut la preuve. ■

Remarque : Une variété de langages étant en particulier une *ne*-variété de langages, la proposition précédente est également vraie pour les variétés de langages.

On en déduit le corollaire suivant.

Corollaire 3.41.

Soient $\mathbf{V}$ une variété de monoïdes contenant B_2^1, L un langage régulier sur l'alphabet A, $n \geqslant 1$ un entier et $u \in A^{\leqslant n}$. Les langages $\pi_n^{-1}(L \cap A^*u) \cap K_n$ et $\pi_n^{-1}(L^c \cap A^*u) \cap K_n$ sont $\mathcal{V}$-séparables si et seulement si

$$\pi_n^{-1}(L \cap A^*u) \cap K_n \in \mathcal{V}(A_n^*).$$

Démonstration : Comme la variété $\mathbf{V}$ contient B_2^1, nous avons que $(ab)^*$ appartient à $\mathcal{V}(\{a,b\}^*)$. D'après la proposition 3.40, cela implique que $K_n \in \mathcal{V}(A_n^*)$. Les langages $L_1 = \pi_n^{-1}(L \cap A^*u) \cap K_n$ et $L_2 = \pi_n^{-1}(L^c \cap A^*u) \cap K_n$ sont $\mathcal{V}$-séparables si et seulement s'il existe un langage $L' \in \mathcal{V}(A_n^*)$ tel que

- $L_1 \subseteq L'$,
- $L_2 \cap L' = \emptyset$.

Or $\mathcal{W}(A_n^*)$ est stable par intersection et donc

$$L'' = K_n \cap L' \in \mathcal{V}(A_n^*).$$

Le langage L'', qui est inclus dans K_n, est également un $\mathcal{V}$-séparateur des langages L_1 et L_2. Remarquons que $L_1 \cup L_2 = K_n$ et donc nécessairement, nous avons

$$L'' = L_1 = \pi_n^{-1}(L \cap A^*u) \cap K_n\big).$$

On en déduit que les langages L_1 et L_2 sont $\mathcal{V}$-séparables si et seulement si le langage $L_1 = \pi_n^{-1}(L \cap A^*u) \cap K_n$ appartient à $\mathcal{V}(A_n^*)$. Ce qui conclut la preuve. ■

Une approche équivalente utilisant la division de catégories peut être trouvée dans l'article de Tilson [73, Proposition 8.4]. En effet, il y est montré la proposition suivante.

Proposition 3.42.

Soient $\mathbf{V}$ une variété de monoïdes contenant B_2^1 et C une catégorie finie. La catégorie finie C appartient à $\mathbf{gV}$ si et seulement si le monoïde C_{cd}^1 appartient à $\mathbf{V}$

De ces propositions, on obtient la simplification immédiate du théorème de délai.

Corollaire 3.43.

Soient $\mathbf{V}$ une variété de monoïdes finis contenant le monoïde B_2^1, L un langage régulier sur l'alphabet A, S son semigroupe syntaxique et $\mathcal{W}$ la ne-variété de langages correspondant à $\mathbf{V} * \mathbf{D}$. Les conditions suivantes sont équivalentes.

(1) Le langage L est dans $\mathcal{W}(A^*)$,

(2) pour tout mot $u \in A^{\leqslant n}$ les langages $\pi_n^{-1}(L \cap A^*u) \cap K_n$ sont dans $\mathcal{V}(A_n^*)$, où $n = |S| + 2$.

(3) $(S_E)^1_{\mathrm{cd}}$ appartient à $\mathbf{V}$.

3.7 Le problème de l'appartenance à une variété de catégories finies

Dans les sections précédentes, nous avons montré que décider le problème de l'appartenance au produit en couronne $\mathbf{V} * \mathbf{D}$ se réduisait à décider l'appartenance d'une catégorie à la variété de catégories finies $\mathbf{gV}$. Dans le cas où B_2^1 appartient à $\mathbf{V}$ ou dans le cas où $\mathbf{V}$ est une variété locale, la décidabilité de $\mathbf{V}$ se transfert à la décidabilité de $\mathbf{V} * \mathbf{D}$

Dans les autres cas, la décidabilité de $\mathbf{V} * \mathbf{D}$ n'est pas nécessairement préservée, (par exemple voir [8]). L'objectif de cette section est d'introduire la théorie profinie équationnelle des variétés de catégories finies et de donner des résultats de décidabilité. La plupart des preuves seront omises.

3.7.1 Équations profinies pour les variétés de catégories finies

Il est nécessaire d'introduire des outils spécifiques pour décider le global des variétés de monoïdes ne contenant pas B_2^1 et n'étant pas locales. C'est pourquoi nous allons maintenant étendre aux catégories finies les notions d'équations profinies. Soient X un graphe fini et A l'ensemble de ces arêtes. Un mot de $u = u_1 \cdots u_n \in A^*$ est bien formé si pour tout $1 \leqslant i < n$, u_i et u_{i+1} sont des arêtes consécutives, on dit alors que u est un chemin. Pour $e, f \in \mathrm{Ob}(X)$, on pose $K_X(e, f)$, l'ensemble des chemins (potentiellement vides) de e vers f. Il s'agit d'un langage régulier de A^*. On note X^δ la *catégorie libre* engendrée par X. C'est une catégorie ayant les mêmes objets que X et telle que, pour tout $e, f \in \mathrm{Ob}(X)$, on ait $X^\delta(e, f) = K_X(e, f)$. Enfin, on note X^Δ la catégorie ayant les mêmes objets que X et dans laquelle, pour tout $e, f \in \mathrm{Ob}(X)$, l'ensemble $X^\Delta(e, f) = \overline{K_X(e, f)}$ est la complétion profinie du langage $K_X(e, f)$.

Soit C une catégorie finie. Une application de $h : X \to C$ est donnée par une application des objets de $h : \mathrm{Ob}(X) \to \mathrm{Ob}(C)$ et pour toute paire d'objets $e, f \in \mathrm{Ob}(X)$, une application $h : X(e, f) \to C(h(e), h(f))$.

Proposition 3.44.

Soient X un graphe et C une catégorie finie. Toute application $h : X \to C$, s'étend uniquement en un morphisme de catégories uniformément continu $\overline{h} : X^{\Delta} \to C$.

Cette proposition est une conséquence de la proposition 2.9.

Définition 3.45 (Équation de catégories).

Une équation de catégories est un couple $(X, u = v)$ où X est un graphe fini et $u, v \in X^{\Delta}(e, f)$ pour $e, f \in \mathrm{Ob}(X)$. Une catégorie finie C vérifie l'équation $(X, u = v)$ si pour toute application $h : X \to C$, l'unique morphisme de catégories uniformément continu $\overline{h} : X^{\Delta} \to C$ vérifie $\overline{h}(u) = \overline{h}(v)$.

Comme pour les théories équationnelles des variétés de monoïdes et de semigroupes, les variétés de catégories sont exactement les classes de catégories définissables par des équations profinies.

Notation : Soit E un ensemble d'équations de catégories. On note $[\![E]\!]$ la classe des catégories qui vérifient toutes les équations de E.

Le résultat principal de cette section est donc le théorème suivant, tiré de l'article de Tilson [73, Proposition 14.2]. Il établit que pour toute variété de catégories finies, il existe un ensemble d'équations de catégories qui la décrit.

Théorème 3.46 (Tilson [73]).

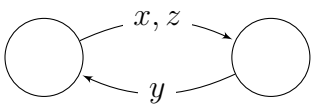
Soit $\mathbf{V}$ une variété de de catégories finies. Il existe un ensemble E d'équations de catégories tel que $\mathbf{V} = [\![E]\!]$.

Nous allons maintenant illustrer ce théorème en présentant des exemples de caractérisations à l'aide d'équations de catégories présents dans la littérature.

3.7.2 Décision pour le problème d'appartenance au global

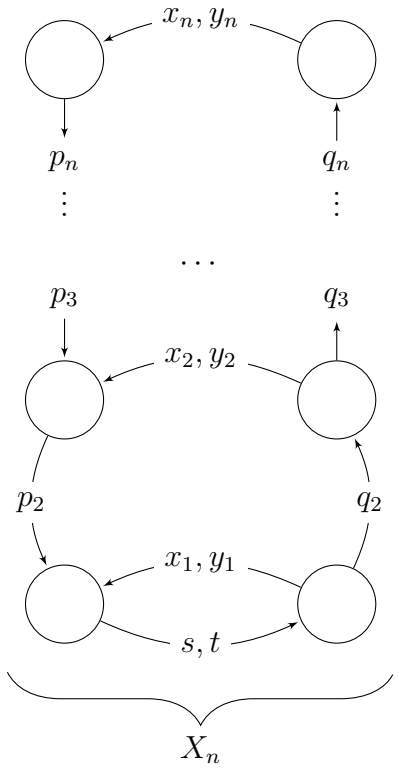
Pour toutes les variétés ci-dessous, le global est décidable. On en déduit que le produit en couronne par $\mathbf{D}$ (et donc l'ajout des prédicats descriptifs locaux au fragment logique correspondant) préserve la décidabilité.

- Les variétés suivantes sont locales : $\mathbf{J_1}, \mathbf{DA}, \mathbf{A}, \mathbf{G}_{\mathrm{sol}}$ et $\mathbf{G}$.
- Les variétés suivantes contiennent B_2^1 : $\mathbf{DA} * \mathbf{G}_{\mathrm{sol}}$, $\mathbf{A}$, $\mathbf{M}_{\mathrm{sol}}$.
- La variété $\mathbf{Com}$:



$xyz = zyx$

- Les équations du global de la variété $\mathbf{V}_n = [\![x^{\omega+1} = x^\omega, u_n = v_n]\!]$ (qui définissent $\mathbf{FO}^2_n[<]$) peuvent être dérivées de l'article de Kufleitner et Lauser [44] :



On pose

$$U_1 = (sx_1)^\omega s(y_1 t)^\omega$$
$$V_1 = (sx_1)^\omega t(y_1 t)^\omega$$

et par induction

$$U_m = (p_m U_{m-1} q_m x_m)^\omega p_m U_{m-1} q_m (y_m p_m U_{m-1} q_m)^\omega$$
$$V_m = (p_m U_{m-1} q_m x_m)^\omega p_m V_{m-1} q_m (y_m p_m U_{m-1} q_m)^\omega$$

Finalement :

$$\mathbf{gV}_n = [\![(X_n, U_n = V_n), x^{\omega+1} = x^\omega]\!]$$

Pour $n = 1$ on obtient également l'équation de Knast (voir l'article [37]) :

$$\mathbf{gJ} = \mathbf{gV}_1 = [\![(X_1, U_1 = V_1), x^{\omega+1} = x^\omega]\!].$$

3.8 Retour à la logique

Nous allons maintenant utiliser le théorème de la catégorie dérivée, le théorème de délai et les caractérisations équationnelles de la section précédentes pour fournir des algorithmes de décidabilité d'un certain nombre de fragments logiques équipés de prédicats descriptifs locaux.

Application : le premier ordre

Dans le chapitre précédent, nous avons étudié le fragment **FO** sur plusieurs signatures numériques. Nous pouvons enrichir cette signature d'une information locale. Le tableau suivant résume les résultats de ce chapitre, il y est décrit la procédure de décidabilité pour un langage L dont le semigroupe syntaxique est noté S.

Fragment	Variété	Équations	Testé sur
$\mathbf{FO}[\mathrm{LOC_D}]$ $\mathbf{FO}^1[\mathrm{LOC_D}]$	$\mathbf{LJ_1}$ corollaire 3.32	$[\![xy = yx, x^2 = x]\!]$	les monoïdes locaux de S
$\mathbf{FO}[\mathrm{LOC}]$ $\mathbf{FO}[=, \mathrm{LOC_D}]$	$\mathbf{ACom} * \mathbf{D}$ corollaire 3.34	de **gCom** et **A**	la catégorie S_E
$(\mathbf{FO} + \mathbf{MOD})[\mathrm{LOC}]$ $(\mathbf{FO} + \mathbf{MOD})[=, \mathrm{LOC_D}]$	$\mathbf{Com} * \mathbf{D}$ corollaire 3.34	de **gCom**	la catégorie S_E
$\mathbf{MOD}[\mathrm{LOC}]$ $\mathbf{MOD}[=, \mathrm{LOC_D}]$	$\mathbf{LAb}$ corollaire 3.32	$[\![xy = yx, x^\omega = 1]\!]$	les monoïdes locaux de S
$\mathbf{MOD}[<, \mathrm{LOC}]$ $\mathbf{MOD}[<, \mathrm{LOC_D}]$	$\mathbf{LG_{sol}}$ corollaire 3.32		
$\mathbf{FO}[<, \mathrm{LOC}]$ $\mathbf{FO}[<], \mathbf{FO}[<, \mathrm{LOC_D}]$	$\mathbf{A}$ corollaire 4.31	$[\![x^{\omega+1} = x^\omega]\!]$	le semigroupe S

FIGURE 3.3 – Le premier ordre

La décidabilité de l'appartenance à la hiérarchie d'alternance du premier ordre n'est pas connue, à l'exception du premier niveau et second niveau (voir la section 2.2.1). À partir du niveau 2 de cette hiérarchie, le langage $(ab)^*$ est définissable et donc la décidabilité de $\mathcal{B}\mathbf{\Sigma}_k[<]$ est équivalente à la décidabilité de $\mathcal{B}\mathbf{\Sigma}_k[<, \mathrm{LOC_D}]$ qui est un fragment équivalent à $\mathcal{B}\mathbf{\Sigma}_k[<, \mathrm{LOC}]$. On obtient également des résultats de séparation.

Proposition 3.47.

Pour tout entier k, il existe un langage dans $\mathcal{B}\mathbf{\Sigma}_{k+1}[<, \mathrm{LOC_D}]$ qui n'est pas définissable dans $\mathcal{B}\mathbf{\Sigma}_k[<, \mathrm{LOC_D}]$.

Démonstration : Fixons un entier $k > 0$. Le fragment $\mathcal{B}\mathbf{\Sigma}_k[<]$ est équivalent à une variété de langages et on note $\mathbf{V}$ la variété de monoïdes correspondant. On peut donc appliquer le théorème d'ajout des prédicats unaires (voir Théorème 1.13) et on obtient qu'un langage L appartient à $\mathcal{B}\mathbf{\Sigma}_k[<, \mathrm{LOC_D}]$ si et seulement si son timbre syntaxique appartient à $\mathbf{V} * \mathbf{D}$. Prenons un langage L_k sur un alphabet A qui appartient à $\mathcal{B}\mathbf{\Sigma}_{k+1}[<]$ mais pas à $\mathcal{B}\mathbf{\Sigma}_k[<]$. Soit c une lettre n'appartenant pas à A et $B = A \cup \{c\}$. On définit le morphisme $\psi : B^* \to A^*$ en posant $\psi(a) = a$ pour $a \in A$ et $\psi(c) = 1$ sinon. Le langage $L' = \psi^{-1}(L)$ a le même monoïde syntaxique que le langage L. C'est pourquoi, L' est définissable dans $\mathcal{B}\mathbf{\Sigma}_{k+1}[<]$ et n'est pas définissable dans $\mathcal{B}\mathbf{\Sigma}_k[<]$. Or, le langage L' a une lettre

neutre, donc d'après le corollaire 3.32, pour tout entier $t > 0$, il est définissable dans $\mathcal{B}\mathbf{\Sigma}_t[<, \mathrm{LOC_D}]$ si et seulement s'il est définissable dans $\mathcal{B}\mathbf{\Sigma}_t[<]$. ■

Application : La restriction à deux variables

Résumons les résultats connus pour l'ajout de prédicats locaux aux fragments de **FO** à deux variables.

Fragment	Variété	Équations	Testé sur
$\mathbf{FO}^2_k[<, \mathrm{LOC}]$ $\mathbf{FO}^2_k[<, \mathrm{LOC_D}]$	$\mathbf{V}_k * \mathbf{D} * \mathbf{MOD}$ corollaire 3.34	de $\mathbf{gV}_k$	la catégorie S_E
$\mathbf{FO}^2[<, \mathrm{LOC}]$ $\mathbf{FO}^2[<, \mathrm{LOC_D}]$	**LDA** corollaire 3.32	de **DA**	les monoïde locaux de S
$(\mathbf{FO} + \mathbf{MOD})^2[<, \mathrm{LOC}]$ $(\mathbf{FO} + \mathbf{MOD})^2[<, \mathrm{LOC_D}]$	$\mathbf{DA} * \mathbf{G}_{\mathrm{sol}} * \mathbf{D}$		

FIGURE 3.4 – La restriction à deux variables

Comme cela fut énoncé dans la proposition 3.2 le langage $c^*(ac^*bc^*)^*$ n'est pas définissable dans $\mathbf{FO}^2[<, \mathrm{LOC}]$ (**LDA**). La proposition suivante conséquence du corollaire 2.26 et du corollaire 3.32 peut être prouvée exactement comme la proposition 3.47.

Proposition 3.48.

Pour tout entier k, il existe un langage dans $\mathbf{FO}^2_{k+1}[<, \mathrm{LOC}]$ qui n'est pas définissable dans $\mathbf{FO}^2_k[<, \mathrm{LOC}]$.

Application : Le cas désagréable à une variable

Le cas à une variable est un peu particulier. C'est un exemple illustrant la différence entre ajouter des prédicats numériques locaux et ajouter des prédicats locaux non numériques.

Proposition 3.49.

$\mathbf{FO}^1[\mathrm{LOC}] \subsetneq \mathbf{FO}^1[\mathrm{LOC_D}]$.

Démonstration : les prédicats de la forme $x = y + k$ ne sont pas utilisables avec une seule variable. Donc, en particulier,

$$\mathbf{FO}^1[\mathrm{LOC}] = \mathbf{FO}^1[\{x = k, x = \max - k, \max = k \text{ pour } k \in \mathbb{N}\}].$$

On rappelle que **LI** est la variété des timbres localement triviaux. En particulier, $\mathbf{LI} = [\![x^\omega y x^\omega =_{\mathrm{ne}} x^\omega]\!]$. Les langages localement triviaux sont de la forme $FA^*G \cup K$ où F, G, K sont des ensembles finis de mots. On remarque qu'un langage est définissable dans $\mathbf{FO}^1[\mathrm{LOC}]$ si et seulement si son semigroupe syntaxique appartient à **LI**.

Le langage $(ab)^*$ est dans $\mathbf{LJ_1}$ mais n'est pas dans **LI**, car

$$(ab)^\omega a(ab)^\omega = (aa)^\omega \neq (ab)^\omega.$$

Ce qui prouve la proposition 3.49. ■

Chapitre 4

Les prédicats modulaires

et la théorie des mu-variétés

Ce chapitre va conclure la partie de cette thèse consacrée à l'enrichissement d'un fragment par des prédicats numériques réguliers. Contrairement au cas des prédicats locaux, la distinction entre prédicats numériques et descriptifs n'est ici pas pertinente. En effet, les prédicats modulaires sont unaires et tombent directement sous le coup du théorème 1.13. Comme pour les prédicats descriptifs locaux, leur ajout va correspondre à une opération algébrique que nous introduirons.

Comme cela sera souligné par la première section de ce chapitre, le cadre fourni par les théories des variétés de monoïdes et des *ne*-variétés n'est pas suffisant pour traiter de l'ajout des prédicats modulaires. Nous allons donc présenter dans la partie 4.2 la notion de *variété de timbres multiplicatifs*. Les parties suivantes vont être consacrées à l'étude du produit en couronne par **MOD**. Les outils introduits dans le chapitre précédent nous seront utiles : nous allons par exemple ré-utiliser le vocabulaire des variétés de catégories finies ainsi que le théorème de la catégorie dérivée. Nous avons évoqué la possibilité de démontrer ce théorème en utilisant la notion, très flexible, de séparation dans la section 3.6. Nous allons l'illustrer en le démontrant dans le contexte du produit en couronne par **MOD**. Il est à noter que le théorème de la catégorie dérivée, adapté au contexte des $\mathcal{C}$-variétés, a été prouvé dans un cadre plus général par Chaubard, Pin et Straubing [20, 19]. En outre, dans l'article [21], ils ont caractérisé effectivement le fragment $\mathcal{B}\mathbf{\Sigma}^1[<, \mathrm{MOD}]$.

Par ailleurs, des théorèmes *de délai partiels* seront présentés ; c'est-à-dire des théorèmes similaires au théorème de délai pour le produit en couronne par **D** (voir Théorème 3.31). Il est regrettable qu'aucun résultat du même ordre que le théorème de délai pour $\mathbf{V}*\mathbf{D}$ ne soit connu (voir Théorème 3.31). Toutefois, une grande partie des fragments présentés dans la partie précédente seront couverts par les hypothèses des délais partiels. Enfin, nous donnerons dans la dernière partie les résultats de transfert de décidabilité et de séparation. Deux tableaux récapitulatifs sont présents à la fin de ce chapitre pour résumer les principaux résultats de décidabilité. Ces travaux ont été réalisés avec Luc Dartois (voir l'article [23]).

4.1 Le cas du premier ordre

Contrairement aux prédicats locaux, l'ajout des prédicats modulaires au premier ordre le rend plus expressif.

Proposition 4.1.

Le langage $(aa)^*$ est exprimable dans $\mathbf{FO}[<, \mathrm{MOD}]$ mais pas dans $\mathbf{FO}[<]$.

Démonstration : La formule

$$(\forall x\ \mathbf{a}(x)) \wedge \max \equiv 0 \bmod 2$$

définit le langage $(aa)^*$. De plus, si on note η le timbre syntaxique de $(aa)^*$,

$$\eta(aa) = \eta(a)^\omega \neq \eta(a)^{\omega+1} = \eta(a),$$

le monoïde syntaxique de ce langage n'est pas apériodique. Il n'est pas définissable dans $\mathbf{FO}[<]$. ■

Les concepts algébriques introduits dans les parties précédentes ne permettent pas de capturer la classe des langages définissables par $\mathbf{FO}[<, \mathrm{MOD}]$. En effet, comme le montre la proposition suivante, cette classe de langages n'est pas stable par *ne*-morphisme inverse. Cela va nous conduire à introduire la notion de variété stable par morphisme inverse multiplicatif.

Proposition 4.2.

Soit $\psi : \{a, c\}^* \to \{a\}^*$ un morphisme non effaçant tel que $\psi(a) = a$ et $\psi(c) = aa$. Le langage $c^*(ac^*ac^*)^* = \psi^{-1}((aa)^*)$ n'est pas définissable dans $\mathbf{FO}[<, \mathrm{MOD}]$.

Nous pourrions donner une preuve de cette proposition *à la main*, en ayant recours uniquement aux jeux d'Ehrenfeucht-Fraïssé. Toutefois, utiliser les descriptions algébriques que nous allons obtenir dans ce chapitre est plus aisé.

4.2 Outils algébriques : mu-variétés de timbres

La stabilité par morphisme inverse constitue l'une des conditions d'utilisation de la théorie des variétés de monoïdes finis. La stabilité par morphisme inverse non effaçant est une condition d'utilisation de la théorie des *ne*-variétés, ou de manière équivalente, des variétés de semigroupes finis. Dans ce chapitre, on se concentrera sur les *variétés de langages multiplicatives*, c'est-à-dire des classes de langages stables par image inverse de morphisme *multiplicatifs*. Introduisons maintenant les définitions nécessaires à l'étude de cette nouvelle sorte de variétés.

4.2.1 Définitions

Définition 4.3 (Morphisme multiplicatif).

Soient A et B deux alphabets finis. Un morphisme $\eta : A^* \to B^*$ est multiplicatif s'il existe un entier k tel que $\eta(A) \subseteq B^k$. Autrement dit, l'image d'une lettre est un mot de longueur k.

Proposition 4.4.

La classe des morphismes multiplicatifs est stable par composition.

Comme pour les *ne*-variétés de langages (voir la définition 3.5), nous introduisons la notion de *mu-variété de langages*.

Définition 4.5 (*mu*-variété de langages).

Une classe de langages réguliers est une *mu*-variété de langages si elle est close par les opérations booléennes, par image inverse de morphisme multiplicatif et par quotient.

Un *mu-morphisme* d'un timbre $\eta : A^* \to M$ vers un timbre $\psi : B^* \to N$ est un couple (f, α) où $f : A^* \to B^*$ est un morphisme multiplicatif et $\alpha : M \to N$ un morphisme de monoïdes tels que $\psi \circ f = \alpha \circ \eta$. Un *mu*-morphisme (f, α) est un *mu-quotient* si

$$\begin{array}{ccc} A^* & \xrightarrow{\quad f \quad} & B^* \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ M & \xrightarrow{\quad \alpha \quad} & N \end{array}$$

$f(A) = B$. Dans ce cas, les morphismes f et α sont nécessairement surjectifs. Un *mu*-morphisme (f, α) est une *mu-inclusion* si α est un morphisme injectif. Un timbre φ *mu-divise* un timbre ψ s'il existe un timbre $\theta : C^* \to K$, une *mu*-inclusion $(f, \alpha) : \theta \to \psi$ et un *mu*-quotient de $(g, \beta) : \theta \to \varphi$. La définition suivante, donnée dans l'article [67], est équivalente (voir l'article [52, proposition 2.1]). Un timbre $\varphi : A^* \to M$ *mu-divise* le timbre $\psi : B^* \to N$ si et seulement s'il existe un couple (f, α) tel que $f : A^* \to B^*$ est un morphisme multiplicatif, $\alpha : N' \to M$ un morphisme surjectif où N' est l'image de $\psi \circ f$ et

$$\varphi = \alpha \circ \psi \circ f.$$

Comme les morphismes multiplicatifs sont stables par composition, la relation sur la *mu*-division de timbres est transitive.

Définition 4.6 (*mu*-variété de timbres).

Une classe de timbres est une *mu*-variété de timbres si elle est stable par produit et *mu*-division de timbres.

Il existe une correspondance entre *mu*-variété de langages et *mu*-variété de timbres. En effet, une *mu*-variété de langages peut être naturellement associée à la *mu*-variété de timbres engendrée par ses timbres syntaxiques. La proposition suivante permet d'obtenir une correspondance réciproque.

Proposition 4.7.

Soit **V** une *mu*-variété de timbres. La classe des langages reconnue par les timbres de **V** forme une *mu*-variété de langages.

Comme dans le cas des variétés de monoïdes et des *ne*-variété de timbres, un équivalent du théorème d'Eilenberg peut être obtenu, établissant que ces deux correspondances sont mutuellement bijectives [67, 26]. Nous introduisons maintenant deux exemples importants pour la suite :

- Les *mu*-variétés de timbres de la forme **QV**.
- La *mu*-variété de timbres **MOD**.

4.2.2 Les *mu*-variétés QV

Soit un timbre $\eta : A^* \to M$. L'ensemble $\eta(A)$ est un élément du monoïde des parties de M. Comme ce monoïde est fini, il existe un entier n, tel que $\eta(A)^n = \eta(A)^{2n}$. On appelle le plus petit entier s vérifiant cette propriété l'*indice de stabilité* de η. On remarque que $\eta(A^s) = \eta((A^s)^+)$ et en particulier, $\eta(A^s)$ est un semigroupe. On l'appelle le *semigroupe stable* de η, on nomme $\eta((A^s)^*)$ le *monoïde stable* et le timbre $\psi : (A^s)^* \to \eta(A^s)^1$ le *timbre stable* de η. Par extension, l'indice de stabilité d'un langage est l'indice de stabilité de son timbre syntaxique et le semigroupe [monoïde, timbre] stable d'un langage est le semigroupe [monoïde, timbre] stable de son timbre syntaxique.

Soit **V** une variété de monoïdes, on note **QV** la classe des timbres dont le monoïde stable est dans **V**.

Exemples :

- Le langage $(aa)^*$ a pour monoïde syntaxique le groupe cyclique $\mathbb{Z}/2\mathbb{Z}$ et pour monoïde stable le monoïde trivial. Son timbre syntaxique appartient donc à **QI**.
- Le langage $(b^*ab^*ab^*)^*$, des mots ayant un nombre pair de a, a pour monoïde syntaxique le groupe cyclique $\mathbb{Z}/2\mathbb{Z}$ et pour monoïde et semigroupe stable toujours le groupe cyclique $\mathbb{Z}/2\mathbb{Z}$. Son timbre syntaxique appartient donc à **QAb**.

- Le langage $(ab)^*$ a pour monoïde syntaxique le monoïde B_2^1 et pour monoïde stable le monoïde à quatre éléments $\{1, ab, ba, 0\}$ dont tous les éléments sont idempotents et $abba = baab = 0$. Son timbre syntaxique appartient donc à $\mathbf{QJ_1}$.

De manière similaire, si $\mathbf{V}$ est une *ne*-variété de timbres, on note $\mathbf{QV}$ la classe des timbres dont le timbre stable est dans $\mathbf{V}$.

Remarque : La classe de timbres $\mathbf{QV}$ est une *mu*-variété de timbres (voir l'article [52] pour plus de précision sur ce sujet).

La *mu*-variété $\mathbf{QV}$ ainsi introduite est connue pour correspondre dans certains cas à l'ajout des prédicats modulaires. Nous verrons dans la suite que que cela correspond au cas local mais que ce n'est pas vrai dans le cas général (voir la proposition 4.32).

4.2.3 La *mu*-variété MOD

Comme pour l'ajout des prédicats descriptifs locaux, l'ajout des prédicats modulaires va correspondre à un produit en couronne. Avant de présenter ce produit en couronne, nous allons étudier la *mu*-variété $\mathbf{MOD}$ qui jouera un rôle similaire à la *ne*-variété $\mathbf{D}$ du chapitre précédent.

Soit d un entier. On définit

$$\psi_d : \begin{cases} \{a\}^* & \to \mathbb{Z}/d\mathbb{Z} \\ a & \mapsto 1 \end{cases}$$

On note $\mathbf{MOD}_d$ la *mu*-variété des timbres engendrés par ψ_d et $\mathbf{MOD} = \bigcup_{d\in\mathbb{N}} \mathbf{MOD}_d$. La classe de timbres $\mathbf{MOD}$ est par définition une *mu*-variété de timbres. Nous allons maintenant décrire la *mu*-variété de langages qui lui est équivalente. Soit A un alphabet. On pose

$$\mathcal{M}_d(A^*) = \left\{ \bigcup_{r\in I} (A^d)^* A^r \mid I \subseteq [d] \right\}.$$

Nous allons montrer l'équivalence entre la *mu*-variété de timbres $\mathbf{MOD}_d$ et la classe de langages $\mathcal{M}_d$.

Proposition 4.8.

Pour d un entier, la classe $\mathcal{M}_d$ est la *mu*-variété de langages équivalente à $\mathbf{MOD}_d$.

Démonstration : Montrons dans un premier temps que $\mathcal{M}_d$ est une *mu*-variété de langages.

Soit I_1 et I_2 des sous-ensembles de $[d]$. On remarque que

$$\left(\bigcup_{r\in I_1}(A^d)^*A^r\right)^c = \bigcup_{r\in[d]-I_1}(A^d)^*A^r,$$
$$\left(\bigcup_{r\in I_1}(A^d)^*A^r\right)\cup\left(\bigcup_{r\in I_2}(A^d)^*A^r\right) = \bigcup_{r\in I_1\cup I_2}(A^d)^*A^r,$$
$$\left(\bigcup_{r\in I_1}(A^d)^*A^r\right)\cap\left(\bigcup_{r\in I_2}(A^d)^*A^r\right) = \bigcup_{r\in I_1\cap I_2}(A^d)^*A^r.$$

De plus, pour a une lettre et $r > 0$,

$$a^{-1}(A^d)^*A^r = (A^d)^*A^ra^{-1} = (A^d)^*A^{r-1}$$
$$a^{-1}(A^d)^* = (A^d)^*a^{-1} = (A^d)^*A^{d-1}.$$

La classe de langages $\mathcal{M}_d$ est donc stable par opérations booléennes et quotients. Montrons qu'elle est également stable par image inverse de morphisme multiplicatif. Prenons également un morphisme multiplicatif $\mu : B^* \to A^*$ et un entier p tels que $\mu(B) \subseteq A^p$ ainsi qu'un entier $r < d$. Posons $\ell = \text{pgcd}(d, p)$. Pour u un mot de B^*, si $\mu(u) \in (A^d)^*A^r$ alors $|\mu(u)| \equiv p|u| \equiv r \bmod d$. De plus, ℓ divise nécessairement r et donc,

$$\frac{p}{\ell}|u| \equiv \frac{r}{\ell} \bmod \frac{d}{\ell}.$$

Comme $\frac{p}{\ell}$ et $\frac{d}{\ell}$ sont premiers entre eux, alors $\frac{p}{\ell}$ est inversible dans $\mathbb{Z}/d\mathbb{Z}$ et on pose

$$r' \equiv r(\frac{p}{\ell})^{-1} \bmod \frac{d}{\ell}.$$

Finalement,

$$\mu^{-1}((A^d)^*A^r) = (B^{\frac{d}{\ell}})^*B^{r'} = \bigcup_{s\in I}(B^d)^*B^s \in \mathbf{M}_d(B^*)$$

pour

$$I = \{s \in \mathbb{Z}/d\mathbb{Z} \mid s \equiv r' \bmod \frac{d}{\ell}\},$$

ce qui conclut la preuve que $\mathcal{M}_d$ est une *mu*-variété de langages.

Montrons maintenant que $\mathcal{M}_d = \mathcal{MOD}_d$. On remarque que les langages reconnus par le timbre ψ_d sont dans $\mathcal{M}_d(\{a\}^*)$ et on a donc que $\mathcal{MOD}_d \subseteq \mathcal{M}_d$. Montrons l'inclusion réciproque. On remarque que le $(A^d)^*A^r$ est l'image inverse du langage $(a^d)^*a^r$ pour le morphisme $\theta : A^* \to \{a\}^*$ défini par $\eta(b) = a$ pour toute lettre $b \in A$. Le morphisme θ étant multiplicatif, on conclut que $(A^d)^*A^r$ appartient à $\mathcal{MOD}_d$ et donc que $\mathcal{M}_d \subseteq \mathcal{MOD}_d$. De chacune de ces inclusions, on obtient $\mathcal{MOD}_d = \mathcal{M}_d$, ce qui conclut la preuve. ■

4.3 Le produit en couronne par MOD

Nous allons utiliser le produit en couronne par **MOD** pour décrire l'ajout des prédicats modulaires. Une fois défini, nous introduirons le principe du produit en couronne puis le théorème d'ajout des prédicats unaires.

4.3.1 Définition

Nous introduisons le produit en couronne adapté au contexte des timbres de **MOD**.

Définition 4.9 (Produit en couronne par un timbre de MOD).

Soient d un entier et $\eta : (A \times \mathbb{Z}/d\mathbb{Z})^* \to N$ un timbre de $\mathbf{V}$. On note $\eta \bullet \psi_d : A^* \to M \circ \mathbb{Z}/d\mathbb{Z}$ le produit en couronne de η par ψ_d défini par $\eta \bullet \psi_d(a) = (f_a, 1)$ pour $f_a : \mathbb{Z}/d\mathbb{Z} \to M$ tel que $f_a(k) = \eta(a, k)$.

Soit $\mathbf{V}$ une variété de monoïdes finis ou une *ne*-variété de timbres. Le produit en couronne de $\mathbf{V}$ par $\mathbf{MOD}_d$, noté $\mathbf{V} * \mathbf{MOD}_d$, est la variété de timbres engendrée par les timbres de la forme $\eta \bullet \psi$ où η est dans $\mathbf{V}$ et $\psi \in \mathbf{MOD}_d$. Le produit en couronne de $\mathbf{V}$ par **MOD**, noté $\mathbf{V} * \mathbf{MOD}$, est la variété de timbres engendrée par les timbres de la forme $\eta \bullet \psi$ où η est dans $\mathbf{V}$ et $\psi \in \mathbf{MOD}$. La proposition suivante est une conséquence de ces définitions.

Proposition 4.10.

Soit $\mathbf{V}$ une variété de monoïdes finis ou une *ne*-variété de timbres. Un timbre η appartient à $\mathbf{V} * \mathbf{MOD}$ si et seulement s'il existe un entier d tel que η appartient à $\mathbf{V} * \mathbf{MOD}_d$.

Remarque : La proposition précédente peut se réécrire plus simplement *via* la formule

$$\mathbf{V} * \mathbf{MOD} = \bigcup_{d \in \mathbb{N}} \mathbf{V} * \mathbf{MOD}_d.$$

4.3.2 Le principe du produit en couronne pour MOD

Le produit en couronne par **MOD** va correspondre exactement à l'opération d'ajout des prédicats modulaires. Intuitivement, ces deux opérations rajoutent une information supplémentaire qui peut être retranscrite directement sur l'alphabet. Pour assurer la *cohérence* de cet enrichissement, nous allons considérer des mots que nous appellerons *bien formés*.

Introduisons les notations nécessaires pour énoncer le principe du produit en couronne. Soit d un entier et A un alphabet. On associe au timbre $\psi_d : A^* \to \mathbb{Z}/d\mathbb{Z}$ une fonction séquentielle $\sigma_d : A^* \to (A \times \mathbb{Z}/d\mathbb{Z})^*$ définie par

$$\sigma_d(a_0 \cdots a_n) = (a_0, 0)(a_1, 1) \cdots (a_n, \psi_d(a_0 \cdots a_n)).$$

À ce timbre est associé un langage K_d sur l'alphabet $A_d = A \times \mathbb{Z}/d\mathbb{Z}$ défini par

$$K_d = \sigma_d(A^*).$$

Autrement dit, un mot $(a_0, t_0) \cdots (a_n, t_n)$ de A_d^* est dans K_d si et seulement si, pour $1 \leqslant i \leqslant n$, $t_i \equiv i \bmod d$. De plus on note π_d la projection canonique de A_d^* vers A^*.

Proposition 4.11.

Les applications $\sigma_d : A^* \to K_d$ et $\pi_d : K_d \to A^*$ sont des applications bijectives réciproques.

La preuve de cette dernière proposition est une simple vérification. On peut remarquer, pour un langage L, que

$$\sigma_d^{-1}(L) = \pi_d(L \cap K_d).$$

Le principe du produit en couronne permet de manipuler le produit en couronne en utilisant directement des opérations sur les langages.

Théorème 4.12 (Principe du produit en couronne revisité).

Soient $\mathbf{V}$ une variété de monoïdes ou une *ne*-variété de timbres, L un langage régulier sur l'alphabet A, d un entier et $\mathcal{W}_d$ la *mu*-variété de langages correspondant à $\mathbf{V} * \mathbf{MOD}_d$. Les conditions suivantes sont équivalentes.

(1) Le langage L est dans $\mathcal{W}_d(A^*)$,

(2) pour tout entier $r \in \mathbb{Z}/d\mathbb{Z}$, il existe un langage $L_r \in \mathcal{V}(A_d^*)$ tel que

$$L = \bigcup_{r \in \mathbb{Z}/d\mathbb{Z}} \Big((A^d)^* A^r \cap \pi_d(L_r \cap K_d) \Big).$$

La preuve de ce théorème est identique à celle du théorème 3.22.

Le principe du produit en couronne se simplifie pour les *ne*-variétés de la forme $\mathbf{V} * \mathbf{D}$ telles que $\mathbf{J_1} \subseteq \mathbf{V}$. En effet, sous ces conditions :

- Le langage A^*a appartient à $\mathcal{D}$ et donc son timbre syntaxique appartient à $\mathbf{V} * \mathbf{D}$.
- Le timbre syntaxique du langage $(ab)^*$ appartient à $\mathbf{LJ_1} = \mathbf{J_1} * \mathbf{D} \subseteq \mathbf{V} * \mathbf{D}$ (voir Proposition 3.33).

La présence du langage $(ab)^*$ dans la *ne*-variété de langages équivalente à $\mathbf{V}*\mathbf{D}$ va garantir la présence du langage des mots bien formés.

Proposition 4.13.

Soit $\mathcal{V}$ est une (*ne*-)variété de langages. Si $\mathcal{V}$ contient le langage $(ab)^*$ alors elle contient le langage K_d pour tout entier d.

La preuve de cette proposition est identique à celle de la proposition 3.40.

Sous ces hypothèses, le principe du produit en couronne se simplifie. Le problème de l'appartenance à $\mathbf{V} * \mathbf{D} * \mathbf{MOD}_d$ se réduit alors à celui de l'appartenance à $\mathbf{V} * \mathbf{D}$.

Proposition 4.14.

Soient $\mathbf{V}$ une variété de monoïdes contenant $\mathbf{J_1}$, $\mathcal{W}$ la *ne*-variété de langage correspondant à $\mathbf{V} * \mathbf{D}$, L un langage régulier sur l'alphabet A, d un entier et $\mathcal{W}_d$ la *mu*-variété de langages correspondant à $\mathbf{V} * \mathbf{D} * \mathbf{MOD}_d$. Les conditions suivantes sont équivalentes.

(1) Le langage L est dans $\mathcal{W}_d(A^*)$,

(2) le langage $\pi_d^{-1}(L) \cap K_d$ appartient à $\mathcal{W}\big(A_d^*\big)$.

Démonstration :

(**2**) $\to$ (**1**). Supposons que

$$L' = \pi_d^{-1}(L) \cap K_d \in \mathcal{W}(A_d^*)$$

et montrons que L est un langage de $\mathcal{W}_d(A^*)$. Comme L' est un langage de mots bien formés on a que $L' = L' \cap K_d$. D'après la proposition 4.11,

$$L = \pi_d(L') = \pi_d(L' \cap K_d)$$

On en déduit que

$$L = \bigcup_{r \in \mathbb{Z}/d\mathbb{Z}} (A^d)^* A^r \cap \pi_d(L_r \cap K_d)$$

en posant $L_r = L'$ pour tout $r \in \mathbb{Z}/d\mathbb{Z}$. Il suffit de conclure en utilisant le principe du produit en couronne.

(**1**) $\to$ (**2**). Supposons que L est un langage de $\mathcal{W}_d(A^*)$. Montrons que

$$\pi_d^{-1}(L) \cap K_d \in \mathcal{W}(A_d^*).$$

Les langages $(ab)^*$ et A^*a ont leur timbre syntaxique dans $\mathbf{V}*\mathbf{D}$ (voir le paragraphe ci-dessus). D'après le principe du produit en couronne, L appartient à $\mathcal{W}_d(A^*)$ si et seulement si pour tout $r \in \mathbb{Z}/d\mathbb{Z}$ il existe un langage $L_r \in \mathcal{W}\big(A_d^*\big)$ tel que

$$L = \bigcup_{r \in \mathbb{Z}/d\mathbb{Z}} \Big((A^d)^* A^r \cap \pi_d(L_r \cap K_d) \Big).$$

De plus,

$$(A^d)^* A^r \cap \pi_d(L_r \cap K_d) = \pi_d((A_d)^*(a,r) \cap L_r \cap K_d). \qquad (*)$$

Comme $(A_d)^*(a,r) \in \mathcal{W}(A_d^*)$ et en posant $L'_r = (A_d)^*(a,r) \cap L_r \in \mathcal{W}(A_d^*)$ on obtient en utilisant l'équation $(*)$ que

$$L = \bigcup_{r \in \mathbb{Z}/d\mathbb{Z}} \pi_d(L'_r \cap K_d).$$

D'après le lemme 3.21,

$$\bigcup_{r \in \mathbb{Z}/d\mathbb{Z}} \pi_d(L'_r \cap K_d) = \pi_d((\bigcup_{r \in \mathbb{Z}/d\mathbb{Z}} L'_r) \cap K_d).$$

Quitte à poser $L' = \bigcup_{r \in \mathbb{Z}/d\mathbb{Z}} L'_r \in \mathcal{W}(A_d^*)$, on obtient que

$$L = \pi_d(L' \cap K_d).$$

Or, le timbre syntaxique du langage $(ab)^*$ appartient à $\mathbf{V} * \mathbf{D}$ et donc d'après le proposition 4.13, $K_d \in \mathcal{W}(A_d^*)$, d'où $\pi_d^{-1}(L) \cap K_d = L' \cap K_d \in \mathcal{W}(A_d^*)$ et donc

$$\pi_d^{-1}(L) \cap K_d \in \mathcal{W}(A_d^*).$$

Ce qui conclut la preuve. ■

4.3.3 L'ajout des prédicats numériques modulaires

Contrairement au cas des prédicats numériques locaux, les prédicats numériques modulaires ne contiennent pas de relations binaires, il n'est donc pas nécessaire dans ce cas de se ramener à des prédicats descriptifs unaires. La preuve du théorème suivant est presque identique à celle du théorème 3.24, il s'agit d'une d'application du théorème 1.13 L'unique différence provient des hypothèses considérées pour le fragment **F**. Dans le théorème 3.24, le fragment est supposé être équivalent à une variété de monoïdes. Dans le théorème suivant, nous allons le supposer équivalent à une variété de monoïdes ou à une *ne*-variété de timbres. L'argument central de la preuve du théorème 3.24 utilise la stabilité par morphisme inverse de la classe de langages associée à **F**. Or, les morphismes utilisés sont non effaçants et cet argument n'induit pas de technicité supplémentaire. La preuve s'adapte donc directement. Ces morphismes n'étant pas multiplicatifs, le cas des *mu*-variétés ne serait pas aussi simple, mais cela sort du cadre de cette thèse.

Théorème 4.15.

Soient **F** un fragment de **MSO**[<] équivalent à une variété de monoïdes ou une *ne*-variété de timbres **V**, L un langage régulier sur l'alphabet A et d un entier. On note $\mathcal{W}_d$ la *mu*-variété de langages correspondant à $\mathbf{V} * \mathbf{MOD}_d$. Les trois conditions suivantes sont équivalentes.

(1) Le langage L est dans $\mathcal{W}_d(A^*)$.

(2) Pour tout $r \in \mathbb{Z}/d\mathbb{Z}$, il existe un langage $L_r \in \mathcal{V}\big(A_d^*\big)$ tel que

$$L = \bigcup_{r \in \mathbb{Z}/d\mathbb{Z}} \Big((A^d)^* A^r \cap \pi_d(L_r \cap K_d) \Big).$$

(3) Le langage L est définissable dans $\mathbf{F}[\mathrm{MOD}_d]$.

Le théorème précédent ne donne pas exactement une caractérisation pour l'ajout des prédicats modulaires, mais uniquement pour l'ajout des prédicats modulaires pour un d fixé. Nous généralisons ce résultat à l'ajout de tous les prédicats modulaires simultanément.

Corollaire 4.16.

Soient **F** un fragment équivalent à une variété de monoïdes ou une *ne*-variété de timbres **V**, L un langage régulier sur l'alphabet A. On note $\mathcal{W}$ la *mu*-variété de langages correspondant à $\mathbf{V} * \mathbf{MOD}$. Les deux conditions suivantes sont équivalentes.

(1) Le langage L est dans $\mathcal{W}(A^*)$.

(2) Le langage L est définissable dans $\mathbf{F}[\mathrm{MOD}]$.

Démonstration : Pour la suite de cette preuve, nous notons $\mathcal{W}_d(A^*)$ la *mu*-variété de langages associée à $\mathbf{V} * \mathbf{MOD}_d$.

(**1**) $\to$ (**2**). Soit L un langage appartenant à $\mathcal{W}(A^*)$. D'après la proposition 4.10, il existe un entier d tel que L appartient à $\mathcal{W}_d(A^*)$. D'après le théorème 4.15, L est définissable dans $\mathbf{F}[\mathrm{MOD}_d]$ et donc dans $\mathbf{F}[\mathrm{MOD}]$.

(**2**) $\to$ (**1**). Supposons que L soit définissable dans $\mathbf{F}[\mathrm{MOD}]$. Par définition, il existe un ensemble fini de prédicats $\mathcal{P} \subseteq \mathrm{MOD}$ tel que L soit définissable dans $\mathbf{F}[\mathcal{P}]$. Les prédicats dans $\mathcal{P}$ sont de la forme $x \equiv r \bmod q$ ou $\max \equiv r \bmod q$ où q est l'indice de congruence de ces prédicats. Notons d le plus petit multiple commun de tous les indices de congruences des prédicats apparaissant dans $\mathcal{P}$. Montrons que chaque prédicat de $\mathcal{P}$ est équivalent à une combinaison booléenne de prédicats de MOD_d. Supposons que $x \equiv r \bmod q$ appartienne à $\mathcal{P}$. Par définition, q divise d. On pose

$$I_r = \{r' \in \mathbb{Z}/d\mathbb{Z} \mid r' \equiv r \bmod q\}.$$

Nous avons alors, pour tout entier $x \geqslant 0$ que le prédicat $x \equiv r \bmod q$ est équivalent à la formule atomique

$$\bigvee_{r' \in I_r} (x \equiv r' \bmod d).$$

De même, si $\max \equiv r \bmod q$ appartient à $\mathcal{P}$, alors le prédicat $\max \equiv r \bmod q$ est équivalent à la formule atomique

$$\bigvee_{r' \in I_r} (\max \equiv r' \bmod d).$$

Pour conclure, il suffit d'utiliser l'hypothèse de substitution atomique du fragment **F**. ■

On appelle *indice modulaire* d'un langage régulier L par rapport à une variété de monoïdes ou une *ne*-variété de timbres $\mathbf{V}$, un entier d tel que le timbre syntaxique de L appartient à $\mathbf{V} * \mathbf{MOD}_d$. Si $\mathbf{V}$ est équivalent à un fragment $\mathbf{F}$, alors L est définissable dans $\mathbf{F}[\mathrm{MOD}_d]$. On note $\mathcal{I}d_{\mathbf{V}}(L)$ l'ensemble des indices modulaires de L par rapport à $\mathbf{V}$. Si le timbre syntaxique de L est dans $\mathbf{V}$, alors $\mathcal{I}d_{\mathbf{V}}(L) = \mathbb{N} - \{0\}$ et si le timbre syntaxique de L n'est pas dans $\mathbf{V} * \mathbf{MOD}$, alors $\mathcal{I}d_{\mathbf{V}}(L) = \emptyset$.
Introduisons maintenant la problématique du *calcul du délai*.

Question 4.17.

Peut-on calculer un indice $s_{\mathbf{V},L}$ tel que si $\mathcal{I}d_{\mathbf{V}}(L)$ est non vide, alors $s_{\mathbf{V},L} \in \mathcal{I}d_{\mathbf{V}}(L)$?

Cette question est centrale dans l'étude du produit en couronne par **MOD**. En effet, dans de nombreux cas, la question du délai est le seul obstacle à la décidabilité de ce produit en couronne. Il n'existe malheureusement pas de résultat général bien que la conjecture suivante semble raisonnable.

Conjecture 4.18.

Si $\mathcal{I}d_{\mathbf{V}}(L)$ est non vide, alors l'indice de stabilité du langage L appartient à $\mathcal{I}d_V(L)$.

Cette conjecture sera prouvée dans la suite pour les variétés et *ne*-variétés locales (avec une notion de localité adaptée aux *ne*-variétés). Nous allons maintenant étudier la structure de l'ensemble $\mathcal{I}d_{\mathbf{V}}(L)$, ce qui nous sera utile pour la suite. On rappelle qu'un sous-ensemble E de $\mathbb{N} - \{0\}$ est un *idéal* du monoïde $\mathbb{N} - \{0\}$ si pour tout $x \in E$ et $y \in \mathbb{N} - \{0\}$, $xy \in E$. On remarque que pour tout entier d et tout entier q, nous avons $\mathbf{MOD}_d \subseteq \mathbf{MOD}_{dq}$. On en déduit que $\mathbf{V} * \mathbf{MOD}_d \subseteq \mathbf{V} * \mathbf{MOD}_{dq}$ et donc nous en déduisons la proposition suivante.

Proposition 4.19.

Soient $\mathbf{V}$ une variété de monoïdes ou une *ne*-variété de timbres et L un langage régulier. L'ensemble $\mathcal{I}d_{\mathbf{V}}(L)$ est un idéal du monoïde $\mathbb{N} - \{0\}$.

Il est possible d'interpréter cette dernière proposition d'un point de vue plus logique. Il n'est pas vraiment étonnant qu'un langage qui soit définissable dans $\mathbf{F}[\mathrm{MOD}_d]$ soit définissable dans $\mathbf{F}[\mathrm{MOD}_{dk}]$ pour tout entier k. En effet, les prédicats de MOD_d sont équivalents a des formules sans quantificateurs n'utilisant que des prédicats MOD_{kd} (voir la preuve du corollaire 4.16).

4.4 Le théorème de catégorie dérivée pour MOD

Cette section est largement inspirée de la thèse de Chaubard [19]. La principale distinction provient de l'utilisation de la séparation comme outil de preuve pour le théorème de la catégorie dérivée (voir la section 3.6). Comme nous étudions l'ajout des prédicats modulaires pour des variétés de monoïdes finis mais aussi pour des *ne*-variétés de timbres, il va être nécessaire de généraliser la notion de variété de catégories. C'est pourquoi nous introduisons maintenant les *ne-variétés de catégories*. On rappelle qu'une *ne*-variété est équivalente à une variété de semigroupes. Il eût été possible d'introduire les *variétés de semigroupoïdes* au lieu des *ne*-variétés de timbres de catégories. La relation entre variété de semigrouïdes et *ne*-variété de timbres est identique à la relation entre variété de semigroupes et *ne*-variété de timbres (voir le paragraphe en dessous de la définition 3.8).

4.4.1 Les *ne*-variétés de catégories

Soit X un graphe fini. On rappelle que X^δ est la catégorie libre engendrée par X (voir la section 3.7.1).

Définition 4.20 (*ne*-morphisme de catégories libres).

Soient X et Y deux graphes finis. Un *ne*-morphisme de catégories libres est un morphisme de catégories $\eta : X^\delta \to Y^\delta$ tel que pour chaque flèche f de X, $\eta(f)$ est un chemin de Y de taille non nulle.

Soit X un graphe fini. Un timbre de catégories est un morphisme surjectif de X^δ vers une catégorie finie C. Nous allons maintenant généraliser les notions de produits, quotients et inclusions au cas des classes de timbres de catégories.

Soient $\varphi : X^\delta \to C_1$ et $\psi : X^\delta \to C_2$ deux timbres de catégories. Le *produit* de φ par ψ est le timbre de catégories $\theta : X^\delta \to F$ défini par

$$\theta(a) = \big(\varphi(a), \psi(a)\big)$$

où F est la sous-catégorie de $C_1 \times C_2$ engendrée par $\theta(a)$ pour tout $a \in A$.

Un *ne-morphisme* d'un timbre de catégories $\varphi : X^\delta \to C$ vers un timbre de catégories $\psi : Y^\delta \to F$ est un couple (f, α) où $f : X^\delta \to Y^\delta$ est un morphisme non effaçant de catégories libres et $\alpha : C \to F$ un morphisme de catégories tels que $\psi \circ f = \alpha \circ \eta$. Un *ne*-morphisme (f, α) est un *ne-quotient* si f est surjectif. Dans ce cas, le morphisme α est nécessairement surjectif. Un *ne*-morphisme (f, α) est une *ne-inclusion* si α est un morphisme injectif. Un timbre de catégories $\varphi : X^\delta \to C$ *ne-divise* un timbre de catégories $\psi : Y^\delta \to F$ si et seulement s'il existe un couple (f, τ) tel que $f : X^\delta \to Y^\delta$ est un morphisme non effaçant et $\tau : C \to F$ est une division de catégories tels que pour tout $u \in X^\delta$

$$\psi(f(u)) \in \tau(\varphi(u)).$$

Soient φ et ψ deux timbres de catégories. S'il existe une *ne*-inclusion de η dans ψ ou s'il existe un *ne*-quotient de ψ vers η, alors η divise ψ.

Comme les morphismes non effaçants de catégories libres sont stables par composition, la relation de *ne*-division de timbres est transitive. Ces notions étendent la notion de catégorie finie de la même manière qu'un timbre étend la notion de monoïde fini. À un timbre de catégorie, on peut associer un *semigroupoïde* qui est l'image des chemins de taille non nulle. La théorie des semigroupoïdes généralise également la théorie des catégories de la même manière que la théorie des semigroupes généralise celle des monoïdes.

Soit $\eta : X^\delta \to C$ un timbre de catégories. Si x est un objet de C, un timbre $\psi : A^* \to M \subseteq C(x, x)$ est un *timbre local* de η s'il existe un morphisme de catégories libres $\theta : A^* \to X^\delta$ tel que $\psi = \eta \circ \theta$ où le monoïde libre A^* est vu comme une catégorie possédant un unique objet. Nous introduisons maintenant la notion de *ne*-variété de timbres de catégories.

Définition 4.21 (*ne*-variété (de timbres) de catégories).

Une classe de timbres de catégories est une *ne*-variété si elle est stable par produit et *ne*-division de timbres de catégories.

Notation : On parlera dorénavant de *ne*-variété catégories au lieu de *ne*-variété de timbres de catégories.

Une *ne*-variété de timbres $\mathbf{V}$ engendre une *ne*-variété de catégories que l'on note $\mathbf{gV}$. De plus on note $\boldsymbol{\ell}\mathbf{V}$ la classe des timbres de catégories dont les timbres locaux sont dans $\mathbf{V}$.

Définition 4.22 (localité).

Une *ne*-variété de timbres est locale si $\mathbf{gV} = \boldsymbol{\ell}\mathbf{V}$.

La notion de localité pour les *ne*-variétés de timbres (ou de manière équivalente des variétés de semigroupes) fait l'objet de nombreuses recherches. Cette notion de localité

est différente de celle présentée dans le chapitre précédent (localité pour les variétés de monoïdes). Par exemple, les variétés de groupes peuvent être vues comme des variétés de monoïdes ou comme des variétés de semigroupes (et donc des *ne*-variétés). Ces dernières sont locales en tant que variétés de monoïdes mais pas nécessairement locales en tant que variétés de semigroupes (voir [57, page 104]). Ainsi, Costa et Escada ont récemment établi un certain nombre d'opérations algébriques préservant la localité des variétés de semigroupes [22].

Soit $\eta : X^\delta \to C$, un timbre de catégories. On note E l'ensemble

$$\{(x, m, y) \mid m \in X(x, y), x, y, \text{ sont des objets de } X\}$$

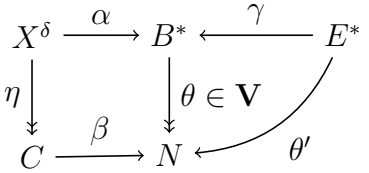
et on appelle *timbre consolidé* de η, le timbre $\eta_{\mathrm{cd}} : E^* \to C^1_{\mathrm{cd}}$ tel que pour tout mot u de E^*, $\eta_{\mathrm{cd}}(u) = \tau(u)$ si u est une arête de X^δ et $\eta_{\mathrm{cd}}(u) = 0$ dans le cas contraire. La proposition suivante est une adaptation de la proposition 3.42 qui provient de l'article de Tilson [73]. Nous la prouvons dans le cadre des *ne*-variétés de timbres.

Proposition 4.23.

Soit $\mathbf{V}$ une *ne*-variété contenant le timbre syntaxique de $(ab)^*$. Un timbre de catégorie appartient à $\mathbf{gV}$ si et seulement si son timbre consolidé appartient à $\mathbf{V}$.

Démonstration : Soit $\eta : X^\delta \to C$ un timbre de catégorie, dont le timbre consolidé appartient à $\mathbf{V}$ et montrons que η *ne*-divise η_{cd} en tant que timbres de catégories. Puisque C^1_{cd} est un monoïde, c'est une catégorie à un élément. On définit la division de catégorie $\beta : C \to C^1_{\mathrm{cd}}$ en posant $\beta(m) = (e, m, f)$ pour chaque arête $m \in C(e, f)$. Soit $\alpha : X^\delta \to E^*$ le morphisme défini par $\alpha(x) = (e, x, f)$ pour $x \in X(e, f)$. On obtient alors que $(\alpha, \beta) : \eta \to \eta_{\mathrm{cd}}$ est une *ne*-division de catégorie et donc η appartient à $\mathbf{gV}$.

Réciproquement, supposons que $\eta : X^\delta \to C$ appartienne à $\mathbf{gV}$ et notons d le nombre d'objets de C. Il existe donc un timbre $\theta : B^* \to N$ dans $\mathbf{V}$ et une *ne*-division $(\alpha, \beta) : \eta \to \psi$ où $\alpha : X^\delta \to B^*$ est un morphisme de catégorie libre non effaçant et $\beta : C \to N$ une division de catégories. Soit E l'ensemble des arêtes de X. Le morphisme α s'étend naturellement en un morphisme $\gamma : E^* \to B^*$ en posant pour chaque flèche $x \in X(e, f)$, $\gamma(e, x, f) = \alpha(x)$. Le morphisme γ est non effaçant car α non effaçant et donc le morphisme $\theta' = \theta \circ \gamma$ est un timbre de $\mathbf{V}$. Malheureusement le timbre η_{cd} ne *ne*-divise pas forcément le timbre θ' car certains mots de E^* ne sont pas des chemins de X^δ.



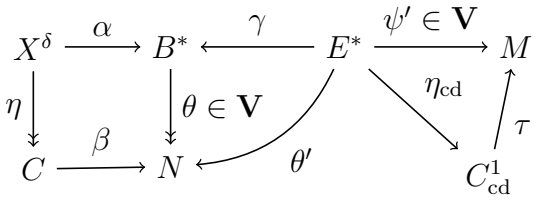
Par hypothèse le timbre syntaxique de $(ab)^*$, que l'on note ψ, appartient à $\mathbf{V}$. Pour

chaque couple $(e, f) \in \mathrm{Ob}(X)$, on définit le morphisme

$$\kappa_{(e,f)} : \begin{cases} E^* \to A^* \\ \qquad\quad a \text{ si } m \in X(e,f) \\ m \mapsto \quad b \text{ si } m \in X(f,e) \\ \qquad\quad ab \text{ sinon} \end{cases}$$

Les morphismes ainsi définis sont tous non effaçants et on obtient que le timbre $\kappa : E^* \to (B_2^1)^d$ produit de tous les timbres de la forme $\psi \circ \kappa_{(e,f)}$ est dans $\mathbf{V}$. Par construction un mot de E^* est un chemin de X si et seulement si son image par κ n'est pas 0. Finalement, on définit le timbre $\psi' : E^* \to M \subseteq (B_2^1)^d \times N$ comme le produit du timbre κ et du timbre θ'. Nous montrons maintenant que le timbre η_{cd} ne-divise le timbre ψ' qui appartient à $\mathbf{V}$. Nous construisons pour cela une ne-division $(f, \tau) : \eta_{\mathrm{cd}} \to \psi'$. On prend pour $f : A^* \to A^*$ l'identité (qui est un bien un ne-morphisme) et on pose $\tau = \psi' \circ \eta_{\mathrm{cd}}^{-1}$. Pour $u \in A^*$, on a

$$\psi'(f(u)) = \psi'(u) \in \tau(\eta_{\mathrm{cd}}(u)).$$



Il reste à prouver que $\tau : C^1_{\mathrm{cd}} \to M$ est une division de monoïdes. Les propriétés $(1) - (3)$ montrent que τ est un morphisme relationnel. Les propriétés $(4) - (5)$ montrent qu'il est injectif.

(1) On a clairement $1 \in \tau(1)$.

(2) Pour $x \in C^1_{\mathrm{cd}}$, comme η_{cd} est surjectif, il existe $u \in A^*$ tel que $\eta_{\mathrm{cd}}(u) = x$, donc $\psi'(u) \in \tau(x)$ et donc $\tau(x) \neq \emptyset$,

(3) Pour $x, y \in C^1_{\mathrm{cd}}$, $m \in \tau(x)$ et $n \in \tau(y)$, il existe u, v tels que $\eta_{\mathrm{cd}}(u) = x$, $\psi'(u) = m$ et $\eta_{\mathrm{cd}}(v) = y$, $\psi'(v) = n$. C'est pourquoi $\eta_{\mathrm{cd}}(uv) = xy$ et $\psi'(uv) = mn$ et donc on a bien $mn \in \tau'(xy)$.

(4) Soient $x, y \in C^1_{\mathrm{cd}}$ des éléments différents de 0 tel que $\tau(x) \cap \tau(y) \neq \emptyset$. Par définition de la catégorie consolidée, il existe des objets e, f et e', f' de C ainsi que $m \in C(e, f)$ et $m' \in C(e', f')$ tels que $x = (e, m, f)$ et $y = (e', m', f')$. Soit $n \in \tau(x) \cap \tau(y)$. Il existe $u, v \in E^*$ tels que

$$\begin{aligned} \eta_{\mathrm{cd}}(u) &= x \\ \eta_{\mathrm{cd}}(v) &= y \\ \psi'(u) = \psi'(v) &= \kappa \times \theta'(u) = \kappa \times \theta'(v) = (n_1, n_2) \end{aligned}$$

Comme x et y sont différents de 0, u et v sont des chemins de X et on note $u', v' \in X^\delta$ les flèches de X^δ associées. En en déduit que $\gamma(u) = \alpha(u')$ et $\gamma(v) = \alpha(v')$. Or

comme $\psi'(u) = \psi'(v)$ nous avons que

$$\beta(m) \ni \theta(\alpha(u)) = \theta(\gamma(u)) = \theta'(u) = n_2 = \theta'(v) = \theta(\gamma(v)) = \theta(\alpha(v)) \in \beta(m').$$

Enfin, on en déduit que $n_2 \in \beta(m) \cap \beta(m')$ et comme β est une division, $m = m'$, d'où $x = y$.

(5) Soit $x \in C_{\text{cd}}^1$ tel qu'il existe un élément n dans $\tau(x) \cap \tau(0)$. Il existe donc $u, v \in E^*$ tel

$$\begin{aligned}\eta_{\text{cd}}(u) &= x\\ \eta_{\text{cd}}(v) &= 0\\ \psi'(u) = \psi'(v) = \kappa \times \theta'(u) &= \kappa \times \theta'(v) = (n_1, n_2)\end{aligned}$$

Le mot v n'est pas un chemin de X. Le morphisme κ reconnaît par construction le langage des chemins de X et comme $n_1 = \kappa(u) = \kappa(v) = 0$, u n'est pas non plus un chemin de X et donc $x = \eta_{\text{cd}}(u) = 0$. Ce qui conclut la preuve. ■

À l'aide de la proposition précédente, on prouve qu'une grande partie des *ne*-variétés de timbre de la forme **LV** sont locales.

Proposition 4.24.

Si **V** est une variété locale de monoïdes finis contenant la variété $\mathbf{J_1}$, alors **LV** est une *ne*-variété de timbres locale.

Démonstration : Si **V** contient $\mathbf{J_1}$, alors le timbre du langage $(ab)^*$ appartient à **LV** (voir la proposition 3.33) et donc d'après la proposition précédente, l'appartenance d'un timbre de catégories à **gLV** se réduit à l'appartenance d'un timbre de monoïdes à **LV**. Soit $\eta : X^\delta \to C$ un timbre de catégorie appartenant à ℓ**LV**. Montrons qu'il appartient à **gLV**. Le timbre η appartient à **gLV** si et seulement si η_{cd} appartient à **LV**. Or le timbre $\eta_{\text{cd}} : E^* \to C_{\text{cd}}^1$ appartient à **LV** si et seulement si les monoïdes locaux de $\eta_{\text{cd}}(E^+)$ sont dans **V**. On remarque qu'un idempotent de $\eta_{\text{cd}}(E^+)$ est soit 0 soit de la forme (x, f, x) où f est un idempotent. Pour 0, le monoïde local est trivial. Prenons (x, f, x) un idempotent de $\eta_{\text{cd}}(E^+)$ et posons

$$M_f = (x, f, x)C_{\text{cd}}^1(x, f, x)$$

le monoïde local associé. On remarque que M_f est isomorphe à $N_f \cup \{0\}$ où $N_f = fC(x, x)f$ est un monoïde de **V**. Par hypothèse, **V** contient $\mathbf{J_1}$ et donc le monoïde $\{0, 1\}$. Le monoïde $N_f \times \{0, 1\}$ est donc également dans **V**. On conclut la preuve en définissant

$$\theta : \begin{cases} N_f \times \{0,1\} & \to N_f \cup \{0\} \\ (x, 1) & \mapsto x \\ (x, 0) & \mapsto 0 \end{cases}$$

L'application θ est un morphisme surjectif donc M_f est isomorphe à un quotient d'un monoïde de **V**. Le monoïde M_f appartient donc à **V**. ■

4.4.2 Le théorème de la catégorie dérivée pour MOD

Introduisons maintenant le théorème de la catégorie dérivée pour **MOD**. Soit d un entier et A un alphabet, on définit le graphe X_d ayant pour ensemble d'objets l'ensemble $\mathbb{Z}/d\mathbb{Z}$ et tel que pour $r \in \mathbb{Z}/d\mathbb{Z}$, et pour a une lettre de A, $(r, a, r+1)$ est une flèche de $X_d(r, r+1)$. On pose $F_d = X_d^\delta$.

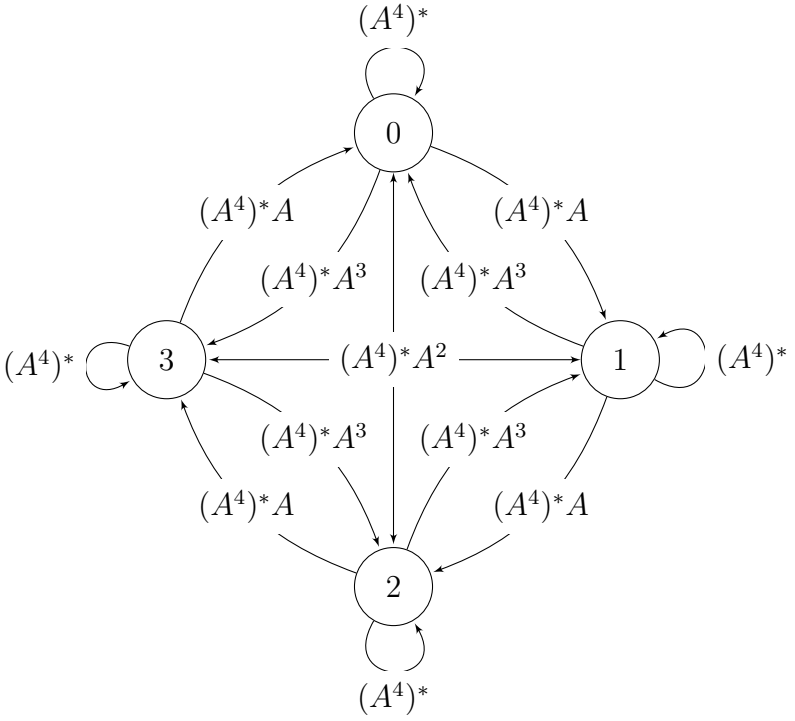


FIGURE 4.1 – La catégorie F_4 sur l'alphabet A

Soient L un langage régulier, $\eta : A^* \to M$ son timbre syntaxique et $r, q \in \mathbb{Z}/d\mathbb{Z}$. On définit une relation d'équivalence $\sim_{(r,q)}$ sur $F_d(r, q)$ en posant, pour $u, v \in F_d(r, q)$, $u \sim_{(r,q)} v$ si pour tout mot $p \in F_d(0, r)$, $\eta(pu) = \eta(pv)$. Cette relation induit une congruence sur F_d, notée $\sim$.

Remarques : Pour $u, v \in F_d(r, q)$ si $\eta(u) = \eta(v)$, alors $u \sim_{(r,q)} v$. Réciproquement, si $u \sim_{(0,q)} v$, alors $\eta(u) = \eta(v)$.

On introduit les catégories et timbres de catégories suivantes :

- On note $F_d(L)$ la catégorie finie $F_d/\sim$ et Θ_d le timbre de catégories de F_d vers $F_d(L)$.
- On note $C_d(L)$ la catégorie ayant pour ensemble d'objets $\mathbb{Z}/d\mathbb{Z}$ et dont les flèches sont définies ainsi. Pour $r, q \in \mathbb{Z}/d\mathbb{Z}$, l'ensemble des flèches de r vers q de $C_d(L)$ est l'ensemble $\eta(\psi_d^{-1}(q - r))$ où ψ_d est le timbre de A^* vers $\mathbb{Z}/d\mathbb{Z}$ tel que $\psi(a) = 1$ pour toute lettre $a \in A$. On note également Γ_d le timbre de F_d vers $C_d(L)$.

$$\begin{array}{ccc} F_d & \xrightarrow{\Gamma_d} & C_d(L) \\ {\scriptstyle \Theta_d}\big\downarrow & & \\ F_d(L) & & \end{array}$$

La catégorie finie $F_d(L)$ a un rôle similaire à la catégorie $D_n(L)$ introduite au chapitre précédent. La proposition suivante montre qu'il est suffisant de considérer la catégorie $C_d(L)$. Cette dernière est bien plus simple à décrire et à manipuler. Cela simplifiera un certain nombre de preuves.

Proposition 4.25.

Les timbres de catégories Θ_d et Γ_d vérifient les propriétés suivantes.

(1) Pour tout entier d, le timbre de catégories Θ_d est un ne-quotient du timbre de catégories Γ_d. En particulier la catégorie $F_d(L)$ est un quotient de la catégorie $C_d(L)$.

(2) Pour tout entier d, le timbre de catégories Γ_d ne-divise un produit du timbre Θ_d par lui même d fois.

Démonstration :

(1) On montre dans un premier temps que le timbre Θ_d se *factorise* à travers le timbre Γ_d. En effet, nous allons construire un morphisme de catégories $\alpha : C_d(L) \to F_d(L)$ tel que $\Theta_d = \alpha \circ \Gamma_d$. Un tel morphisme est nécessairement surjectif puisque Θ_d et Γ_d

$$\begin{array}{ccc} F_d & \xrightarrow{\Gamma_d} & C_d(L) \\ & {\scriptstyle \Theta_d}\searrow & \big\downarrow{\scriptstyle \alpha} \\ & & F_d(L) \end{array}$$

sont surjectifs. On définit l'application entre objets $\alpha : \mathrm{Ob}(C_d(L)) \to \mathrm{Ob}(F_d(L))$ comme étant l'identité. Il reste à définir α sur les flèches. Soit $r, q \in \mathbb{Z}/d\mathbb{Z}$ et $m \in C_d(L)(r, q)$. Montrons que l'ensemble $\Theta_d \circ {\Gamma_d}^{-1}(m)$ contient un unique élément. Soit $u, v \in {\Gamma_d}^{-1}(m)$. Par définition de $C_d(L)$, nous avons $\eta(u) = \eta(v)$ et donc $u \sim_{(r,q)} v$, d'où $\Theta_d(u) = \Theta_d(v)$. On note $\alpha(m)$ l'unique élément de

$$\Theta_d \circ {\Gamma_d}^{-1}(m).$$

Pour tout $u \in F_d(r, q)$, nous avons

$$\Theta_d(u) = \alpha \circ \Gamma_d(u)$$

et donc comme Θ_d et Γ_d sont des morphismes surjectifs, α est surjectif.

Montrons que α est un morphisme. Soit m, n deux flèches consécutives de $C_d(L)$. Il existe donc deux mots u et v tels que $\Gamma_d(u) = m$ et $\Gamma_d(v) = n$ et $\Gamma_d(uv) = mn$. Par définition $\alpha(m) = \Theta_d(u)$, $\alpha(n) = \Theta_d(v)$ et $\alpha(mn) = \Theta_d(uv)$. Nous avons donc

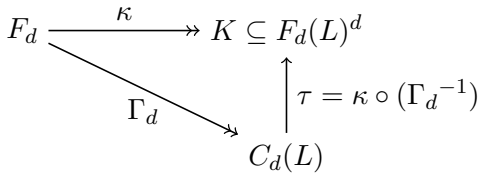
$$\alpha(m)\alpha(n) = \alpha(mn).$$

Enfin, le morphisme $\alpha : C_d(L) \to F_d(L)$ définit un quotient de catégories finies et $(f, \alpha) : \Gamma_d \to \Theta_d$, où f est l'identité, définit un *ne*-quotient de timbres de catégories.

(2) Introduisons dans un premier temps le *ne*-morphisme $r : F_d \to F_d$ qui réalise la *rotation* des objets. Plus précisément, pour tout objet $q \in \mathbb{Z}/d\mathbb{Z}$, $r(q) = q+1 \bmod d$. De plus, pour $t \in \mathbb{Z}/d\mathbb{Z}$, la flèche u de $F_d(q,t)$ est envoyée par r sur la flèche u de $F_d(r(q), r(t))$. On définit $\kappa : F_d \to K \subseteq F_d(L)^d$ un timbre en posant

$$\kappa(u) = (\Theta_d(u), \Theta_d(r(u)), \Theta_d(r^2(u)) \ldots, \Theta_d(r^{d-1}(u))).$$

Nous allons construire une *ne*-division $(f, \tau) : \Gamma_d \to \kappa$, où $f : F_d \to F_d$ est l'identité. On pose le morphisme relationnel de catégories $\tau = \kappa \circ ({\Gamma_d}^{-1})$.



Vérifions que τ est bien une division de catégories. Soient $r, q \in \mathbb{Z}/d\mathbb{Z}$ et $m, m' \in C_d(L)(r,q)$. Supposons que $\tau(m) \cap \tau(m') \neq \emptyset$. Il existe donc $u, v \in F_d(r,q)$ tels que $\kappa(u) = \kappa(v)$. On en déduit que $\Theta_d(r^i(u)) = \Theta_d(r^i(v))$ pour tout $i \in \mathbb{Z}/d\mathbb{Z}$. En particulier $\Theta_d(r^{d-r}(u)) = \Theta_d(r^{d-r}(v))$ et en posant $q' = q - r \bmod d$ on obtient que $u \sim_{(0,q')} v$ et donc, d'après la remarque 4.4.2, $\eta(u) = \eta(v)$. Ce qui conclut cette démonstration. ■

De cette proposition, on en déduit immédiatement la proposition suivante.

Proposition 4.26.

(1) Pour toute variété de catégories finies $\mathbf{V}$, la catégorie $C_d(L)$ appartient à $\mathbf{gV}$ si et seulement la catégorie $F_d(L)$ appartient à $\mathbf{V}$.
(2) Pour toute *ne*-variété de timbres de catégories $\mathbf{V}$, le timbre Γ_d appartient $\mathbf{V}$ si et seulement si le timbre Θ_d appartient à $\mathbf{V}$.

Nous allons de nouveau établir le théorème de la catégorie dérivée mais pour le produit en couronne par **MOD**. La preuve donnée pour le cas du produit en couronne par **D** est classique et dans la partie 3.6, une preuve alternative passant par la séparation a été évoquée. Nous allons utiliser cette autre approche ici.

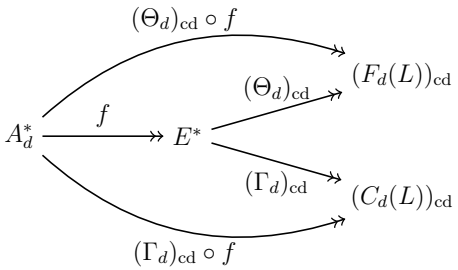
La proposition suivante est nécessaire à la preuve, *via* la séparation, du théorème de la catégorie dérivée.

Proposition 4.27.

Soient L un langage régulier et $d \geqslant 1$ un entier. Pour tout entier $d \in \mathbb{Z}/d\mathbb{Z}$, les langages $\pi_d^{-1}(L \cap (A^d)^* A^r) \cap K_d$ et $\pi_d^{-1}(L \cap (A^d)^* A^r) \cap K_d$ sont reconnus par les timbres :

- $(\Theta_d)_{\mathrm{cd}} \circ f : A_d^* \to F_d(L)^1_{\mathrm{cd}}$,
- $(\Gamma_d)_{\mathrm{cd}} \circ f : A_d^* \to C_d(L)^1_{\mathrm{cd}}$

où $f : A_d^* \to E^*$ est le ne-morphisme défini par $f(a, i) = (i, a, i + 1)$.



La preuve de cette proposition est très similaire à celle de la proposition 3.37.

On rappelle que le théorème de la catégorie dérivée, établi dans l'article de Tilson [73], est plus général. De nombreuses généralisations sont possibles pour être adaptés à différents contextes. Nous n'établissons ici ce théorème que dans le cas qui nous intéresse, mais une preuve d'un théorème général ne serait pas différente.

Théorème 4.28 (La catégorie dérivée pour MOD, Chaubard *et al.* [20]).

Soient $\mathbf{V}$ une variété de monoïdes ou une ne-variété de timbres, L un langage régulier sur l'alphabet A, d un entier et $\mathcal{W}_d$ la mu-variété de langages correspondant à $\mathbf{V} * \mathbf{MOD}_d$. Les conditions suivantes sont équivalentes.

(1) Le langage L est dans $\mathcal{W}_d(A^*)$,

(2) pour tout $r \in \mathbb{Z}/d\mathbb{Z}$, il existe un langage $L_r \in \mathcal{V}\big(A_d^*\big)$ tel que

$$L = \bigcup_{r \in \mathbb{Z}/d\mathbb{Z}} \Big((A^d)^* A^r \cap \pi_d(L_r \cap K_d) \Big),$$

(3) pour tout $r \in \mathbb{Z}/d\mathbb{Z}$ les langages

$$\pi_d^{-1}(L \cap (A^d)^* A^r) \cap K_d$$
$$\pi_n^{-1}(L^c \cap (A^d)^* A^r) \cap K_d$$

sont $\mathcal{V}$-séparables,

(4) la catégorie $C_d(L)$ (resp. le timbre de catégories Γ_d) appartient à $\mathbf{gV}$.

Démonstration : On ne prouve le théorème que pour les *ne*-variétés de timbres. Le cas des variétés de monoïdes peut être traités similairement ou en reprenant la preuve du chapitre précédent.

(**1**) $\leftrightarrow$ (**2**). C'est exactement le principe du produit en couronne.

(**2**) $\leftrightarrow$ (**3**). Le langage L_r est un séparateur pour $\pi_d^{-1}(L \cap (A^d)^* A^r) \cap K_d$ et $\pi_d^{-1}(L^c \cap (A^d)^* A^r) \cap K_d$ et réciproquement, un séparateur est un langage L_r donnant l'équivalence entre ces deux points.

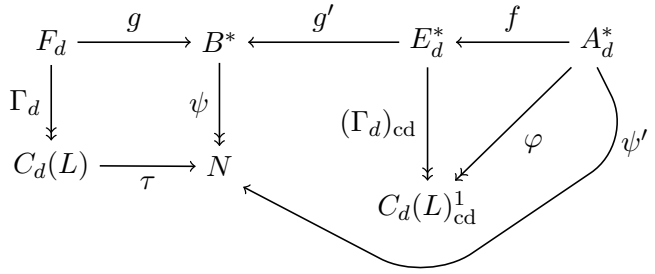
(**4**) $\rightarrow$ (**3**). Supposons que Γ_d appartient à $\mathbf{gV}$. Il existe donc une *ne*-division $(g, \tau) : \Gamma_d \to \psi$ où $\psi : B^* \to N$ est un timbre de $\mathbf{V}$, g est un morphisme de F_d vers B^*. On rappelle que $F_d = X_d^\delta$ et on note E_d l'ensemble des flèches de X_d. Dans ce cas, g s'étend en un morphisme $g' : E_d^* \to B^*$ en posant

$$g'(i, a, i+1) = g(i, a, i+1).$$

Comme le morphisme de catégories libre g est non effaçant, le morphisme de monoïdes libres g' est aussi non effaçant. On définit $f : A_d^* \to E_d^*$ en posant $f(a, i) = (i, a, i+1)$ (comme dans la proposition 4.27), on obtient deux timbres $\varphi = (\Gamma_d)_{\mathrm{cd}} \circ f : A_n^* \to C_d(L)_{\mathrm{cd}}^1$ et

$$\psi' = \psi \circ g' \circ f : A_n^* \to N \in \mathbf{V}.$$

D'après la proposition 4.27, le timbre φ reconnaît les langages $L_r = \pi_d^{-1}(L \cap (A^d)^* A^r) \cap K_d$ et $L'_r = \pi_n^{-1}(L^c \cap (A^d)^* A^r) \cap K_d$.



Soient $x \in \varphi(L_r)$ et $y \in \varphi(L'_r)$. Montrons que

$$\psi'(\varphi^{-1}(x)) \cap \psi'(\varphi^{-1}(x)) = \emptyset.$$

On rappelle que $x = (0, m, r)$ et $y = (0, m', r)$ sont des éléments distincts de $C_d(L)_{\mathrm{cd}}$. En notant x' la flèche de $C_d(0, r)$ correspondant à x et y' la flèche de $C_d(0, r)$ correspondant à y, nous avons par construction

$$\tau(x') = \psi'(\varphi^{-1}(x)) \text{ et } \tau(y') = \psi'(\varphi^{-1}(y)).$$

Par hypothèse, τ est une division ce qui permet de conclure en utilisant le théorème de séparation (voir Théorème 3.38).

(**3**) $\rightarrow$ (**4**). On note $\eta : A^* \to M$, le timbre syntaxique de L. Soit $d > 0$, tel que pour tout $r \in \mathbb{Z}/d\mathbb{Z}$ les langages

$$\pi_d^{-1}(L \cap (A^d)^* A^r) \cap K_d \text{ et } \pi_d^{-1}(L^c \cap (A^d)^* A^r) \cap K_d$$

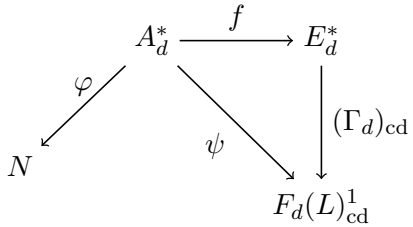
sont $\mathcal{V}$-séparables. Grâce à la proposition 4.26, il suffit de prouver que $F_d(L)$ appartient à $\mathbf{gV}$. D'après la proposition 4.27, les langages

$$\pi_d^{-1}(L \cap (A^d)^* A^r) \cap K_d \text{ et } \pi_d^{-1}(L^c \cap (A^d)^* A^r) \cap K_d$$

sont reconnus par

$$\psi = (\Theta_d)_{\mathrm{cd}} \circ f : A_d^* \to F_d(L)^1_{\mathrm{cd}}$$

où $f : A_d^* \to E^*$ est le ne-morphisme défini par $f(a,i) = (i, a, i+1)$.



Puisque ces langages sont $\mathcal{V}$-séparables, d'après le théorème 3.38, il existe un timbre $\varphi : A_d^* \to N \in V$ tel que

$$\varphi(\psi^{-1}(m)) \cap \varphi(\psi^{-1}(m')) = \emptyset$$
$$m \in \varphi(\pi_d^{-1}(L \cap (A^d)^* A^r) \cap K_d)$$
$$m' \in \varphi(\pi_d^{-1}(L^c \cap (A^d)^* A^r) \cap K_d)$$

On définit la division $\tau : F_d(L) \to N$ en posant, pour $r, q \in \mathbb{Z}/d\mathbb{Z}$ et $m \in F_d(L)(r,q)$,

$$\tau(m) = \varphi(\psi^{-1}(r, m, q)).$$

Montrons que τ est bien une division.

- Pour chaque $m \in F_d(L)$, $\tau(m)$ est non vide par construction.
- Pour chaque objet $r \in \mathbb{Z}/d\mathbb{Z}$, l'image du neutre de $F_d(r,r)$ contient le neutre de N.
- Soient $r, p, q \in \mathbb{Z}/d\mathbb{Z}$, $m \in F_d(L)(r,q)$, $m' \in F_d(L)(q,p)$, $x \in \tau(m)$ et $y \in \tau(m')$. Montrons que $xy \in \tau(mm')$. Par définition, il existe $u, v \in A_d^*$ tels que $\psi(u) = (r, m, q)$, $\psi(v) = (q, m', p)$, $\varphi(u) = x$ et $\varphi(v) = y$. Dans ce cas, le mot uv vérifie que $\psi(uv) = (r, mm', p)$ et $\varphi(uv) = xy$. Par conséquent $xy \in \tau(mm')$.
- Soient $r, q \in \mathbb{Z}/d\mathbb{Z}$ et $m, m' \in F_d(L)(r,q)$. Montrons que $m \neq m'$ implique que $\tau(m) \cap \tau(m') = \emptyset$. Par définition de $F_d(L)$, si $m \neq m'$, alors il existe des mots $s \in F_d(0,r)$, $u, v \in F_d(r,q)$, $p \in \mathbb{Z}/d\mathbb{Z}$ et $t \in F_d(q,p)$ tels que $\Theta_d(u) = m$, $\Theta_d(v) = m'$ et $sut \in L$ si et seulement si $svt \notin L$. Supposons, sans perte de généralité, que $sut \in L$. Par conséquent,

$$\psi^{-1}(0, \Theta_d(sut), p) \subseteq \pi_d^{-1}(L \cap (A^d)^* A^r) \cap K_d$$
$$\psi^{-1}(0, \Theta_d(svt), p) \subseteq \pi_d^{-1}(L^c \cap (A^d)^* A^r) \cap K_d$$

et donc $\tau(\Theta_d(sut)) \cap \tau(\Theta_d(svt)) = \emptyset$. Or, en posant $n = \Theta_d(s)$ et $n' = \Theta_d(t)$, nous avons

$$\tau(n)\tau(m)\tau(n') \subseteq \tau(nmn') = \tau(\Theta_d(sut))$$
$$\tau(n)\tau(m')\tau(n') \subseteq \tau(nm'n') = \tau(\Theta_d(svt))$$

Supposons qu'il existe $x \in \tau(m) \cap \tau(m')$ et prenons $y \in \tau(n)$ et $z \in \tau(n')$. D'après les deux équations précédentes, nous avons

$$yxz \in \tau(nmn') \cap \tau(nm'n') = \tau(\Theta_d(sut)) \cap \tau(\Theta_d(svt)),$$

ce qui est impossible. On en déduit que $\tau(m) \cap \tau(m') = \emptyset$.

Le couple $(h, \tau) : \Theta_d \to \varphi$ est une *ne*-division de timbres de catégories où $h : F_d \to B^*$ est le *ne*-morphisme de catégorie libre défini par $h(i, a, i+1) = (a, i)$. Ce qui conclut la preuve. ■

De ce théorème, on peut obtenir le corollaire suivant, qui va nous servir à plusieurs reprises.

Corollaire 4.29.

Soit $\mathbf{V}$ une variété de monoïdes finis ou une *ne*-variété de timbres. Alors,

$$\mathbf{V} * \mathbf{MOD} \subseteq \mathbf{QV}.$$

En outre, pour tout langage disposant d'une lettre neutre l'appartenance de son timbre syntaxique à $\mathbf{V} * \mathbf{MOD}$ est équivalente à l'appartenance à $\mathbf{V}$.

Démonstration : Supposons que $\mathbf{V}$ est une variété de monoïdes finis. On rappelle que $\mathcal{V}$ désigne la variété de langages correspondante. Notons également $\mathcal{W}$ la *mu*-variété de langages correspondant à $\mathbf{V} * \mathbf{MOD}$ et $\mathcal{W}_d$ la *mu*-variété de langages correspondant à $\mathbf{V} * \mathbf{MOD}_d$ pour tout entier d. Soit L un langage régulier de A^*. Supposons que L appartienne à $\mathcal{W}(A^*)$. Par définition il existe un entier d tel que $L \in \mathcal{W}_d(A^*)$. D'après la proposition 4.19, $L \in \mathcal{W}_{sd}(A^*)$, où s est l'indice de stabilité de L. D'après le théorème 4.28, la catégorie $C_{sd}(L)$ appartient à $\mathbf{gV}$. On remarque que les monoïdes locaux de $C_{sd}(L)$ sont isomorphes au monoïde stable de L. Donc le monoïde stable de L appartient à $\mathbf{V}$ et donc le timbre syntaxique de L appartient à $\mathbf{QV}$.

Supposons qu'un langage régulier L dispose d'une lettre neutre et appartient à $\mathcal{W}$. D'après le point précédent, son timbre syntaxique appartient à $\mathbf{QV}$. Or, le monoïde stable d'un langage à lettre neutre est exactement son monoïde syntaxique. En particulier, s'il appartient à $\mathbf{QV}$, alors il appartient à $\mathbf{V}$.

Le cas où $\mathbf{V}$ est une *ne*-variété de timbres est traité de la même manière. ■

4.5 Les théorèmes de delai

Dans la section précédente, nous avons établi un certain nombres de résultat de décidabilité pour le produit en couronne de la forme $\mathbf{V} * \mathbf{MOD}_d$ où d est un entier fixé. L'objectif ici est d'établir un résultat similaire au théorème du délai pour le produit en couronne par $\mathbf{D}$, c'est-à-dire, d'obtenir une caractérisation de $\mathbf{V} * \mathbf{MOD}$ en testant une unique catégorie sur la variété de catégories $\mathbf{gV}$. De manière équivalente, il s'agit d'être capable de calculer un entier qui appartient à $\mathcal{I}d_{\mathbf{V}}(L)$ si le timbre syntaxique de L est dans $\mathbf{V} * \mathbf{MOD}$. Un candidat pour un tel entier est l'indice de stabilité. Malheureusement, savoir si cet indice convient toujours constitue une question ouverte. En ajoutant des contraintes supplémentaires (mais raisonnables) sur les variétés, nous parviendrons à obtenir une méthode s'appliquant à certaine variétés.

4.5.1 Le cas des variétés locales

Nous allons étudier dans un premier temps le cas des variétés locales. En effet, dans ce cas précis, la décidabilité du global se simplifie suffisamment pour qu'il soit possible de prouver simplement un théorème de délai. Celui-ci conviendra aux variétés de monoïdes et aux *ne*-variétés de timbres.

Proposition 4.30.

Soient $\mathbf{V}$ une variété locale de monoïdes ou une *ne*-variété locale de timbres et L un langage régulier. Le timbre syntaxique de L appartient à $\mathbf{V} * \mathbf{MOD}$ si et seulement si l'indice de stabilité de L appartient à $\mathcal{I}d_{\mathbf{V}}(L)$.

Cette proposition peut être reformulée en disant qu'un timbre syntaxique appartient à $\mathbf{V} * \mathbf{MOD}$ si et seulement s'il appartient à $\mathbf{V} * \mathbf{MOD}_s$, où s est son indice de stabilité.

Démonstration : Soient $\eta : A^* \to L$ le timbre syntaxique de L et s son indice de stabilité. Par définition si l'indice de stabilité de L appartient à $\mathcal{I}d_{\mathbf{V}}(L)$ alors le timbre syntaxique de L appartient à $\mathbf{V} * \mathbf{MOD}$.

Supposons que $\eta \in \mathbf{V} * \mathbf{MOD}$. Par définition, il existe un entier d tel que $d \in \mathcal{I}d_{\mathbf{V}}(L)$. Comme $\mathcal{I}d_{\mathbf{V}}(L)$ est un idéal (voir proposition 4.19), $ds \in \mathcal{I}d_{\mathbf{V}}(L)$. Remarquons que les monoïdes locaux de $C_{ds}(L)$ et de $C_s(L)$ sont isomorphes à $\eta(A^{ds})^1 = \eta(A^s)^1$. Donc, si $\mathbf{V}$ est une variété locale de monoïdes finis, alors C_{ds} appartient à $\mathbf{gV}$ si et seulement si les monoïde locaux de $C_{ds}(L)$ appartiennent à $\mathbf{V}$ si et seulement si les monoïdes locaux de $C_s(L)$ appartiennent à $\mathbf{V}$ si et seulement si $C_s(L)$ appartient à $\boldsymbol{\ell}\mathbf{V} = \mathbf{gV}$. On peut conclure grâce au théorème de la catégorie dérivée pour $\mathbf{MOD}$ (voir Théorème 4.28).

Supposons que $\mathbf{V}$ est une *ne*-variété de timbres et que $\eta \in \mathbf{V} * \mathbf{MOD}$. Par définition, il existe un entier d tel que $d \in \mathcal{I}d_{\mathbf{V}}(L)$. Comme $\mathcal{I}d_{\mathbf{V}}(L)$ est idéal, alors $ds \in \mathcal{I}d_{\mathbf{V}}(L)$. D'après le théorème 4.28, $\Gamma_{ds} \in \mathbf{gV} = \boldsymbol{\ell}\mathbf{V}$. Donc, tous les timbres locaux de Γ_{ds} sont dans $\mathbf{V}$. Montrons que c'est également le cas pour les timbres locaux de Γ_s. Soient $i \in \mathbb{Z}/s\mathbb{Z}$ et $\psi : B^* \to N \subseteq C_s(L)(i,i)$ un timbre local de Γ_s. Nous allons montrer que ψ appartient à $\mathbf{V}$ en prouvant qu'il s'agit d'un timbre local de Γ_{ds}.

Par définition des timbres locaux, il existe un morphisme non effaçant $\theta : B^* \to F_s$ tel que $\psi = \Gamma_s \circ \theta$. Pour chaque lettre $b \in B$, $\theta(b)$ est une flèche $F_s(i,i)$. Par définition, il existe un mot u_b de longueur multiple de s étiquetant la flèche $\theta(b)$. Par définition de l'indice de stabilité, il existe un mot v_b de longueur multiple de ds et tel que $\eta(u_b) = \eta(v_b)$. On définit $\theta' : B^* \to F_{ds}$ en posant $\theta'(b) = v_b \in F_{ds}(i,i)$ et on note N' l'image du morphisme $\Gamma_{ds} \circ \theta'$. Le timbre $\psi' = \Gamma_{ds} \circ \theta' : B^* \to N \subseteq C_{ds}(L)(i,i)$ est un timbre local de Γ_{ds} et appartient donc à $\mathbf{V}$. Or par construction, pour chaque mot $u \in B^*$, $\psi(u) = \psi(u')$. Donc, ψ appartient à $\mathbf{V}$. On en déduit que Γ_s appartient à $\boldsymbol{\ell}\mathbf{V} = \mathbf{gV}$, et par conséquent $s \in \mathcal{I}d_{\mathbf{V}}(L)$. ■

Si on part d'une variété de monoïdes locale, nous allons pouvoir composer les résultats connus pour **D** et pour **MOD**.

Corollaire 4.31.

Soit $\mathbf{V}$ une variété locale de monoïdes finis. Alors $\mathbf{V} * \mathbf{MOD} = \mathbf{QV}$ et si $\mathbf{V}$ contient $\mathbf{J_1}$, alors $\mathbf{V} * \mathbf{D} * \mathbf{MOD} = \mathbf{QLV}$.

Démonstration : Soient $\mathbf{V}$ une variété locale de monoïdes finis et L un langage régulier de timbre syntaxique η et d'indice de stabilité s.

- D'après la proposition 4.30, $\eta \in \mathbf{V} * \mathbf{MOD}$ si et seulement si $C_s(L) \in \mathbf{gV} = \boldsymbol{\ell}\mathbf{V}$. Or, les monoïdes locaux de $C_s(L)$ sont isomorphes au monoïde stable. Donc $C_s(L) \in \boldsymbol{\ell}\mathbf{V}$ si et seulement si le monoïde stable de L est dans $\mathbf{V}$ si et seulement si $\eta \in \mathbf{QV}$.
- D'après le corollaire 3.32, $\mathbf{V} * \mathbf{D} = \mathbf{LV}$. De plus, comme $\mathbf{V}$ contient $\mathbf{J_1}$ par hypothèse, d'après la proposition 4.24, la *ne*-variété de timbres $\mathbf{LV}$ est locale.
  Montrons que si Γ_s appartient à $\ell\mathbf{LV}$, alors η appartient à $\mathbf{QV}$. Soit ψ le timbre stable de L. Ce timbre est un timbre local de Γ_s. En effet, soit $f : (A^s)^* \to F_s$ le morphisme de catégories libres qui a un mot $u \in A^s$ associe la flèche autour de l'objet 0 correspondante. On a alors que $\psi = \Gamma_s \circ f$. Comme $\Gamma_s \in \ell\mathbf{LV}$, nous avons que $\psi \in \mathbf{LV}$ et donc $\eta \in \mathbf{QLV}$.
  Réciproquement, montrons que si $\eta \in \mathbf{QLV}$, alors $\Gamma_s \in \mathbf{gLV} = \ell\mathbf{LV}$. Soit $\kappa : B^* \to N$ un timbre local de Γ_s. Montrons qu'il appartient à $\mathbf{LV}$. Par définition il existe un morphisme de catégories libres non effaçant $f : B^* \to F_s$ tel que $\kappa = \Gamma_s \circ f$. On note i l'image l'unique objet de B^* par f. On a donc que N est un sous-monoïde de $C_s(L)(i,i)$ qui est le monoïde stable de L. De plus, l'image de chaque lettre b est un mot de $F_s(i,i)$ de longueur multiple de s. On note $h : B^* \to (A^s)^*$ tel que $h(b) = f(b)$. En en déduit que $(h, \iota) : \kappa \to \psi$ où $\iota : N \to M$ est le morphisme injectif d'inclusion, est une *ne*-inclusion de timbre. Comme ψ appartient à $\mathbf{LV}$ qui est une *ne*-variété de timbres, on en déduit que κ appartient également à $\mathbf{LV}$.
  Donc, $\eta \in \mathbf{V} * \mathbf{D} * \mathbf{MOD}$ si et seulement si le timbre stable de L est dans $\mathbf{LV}$, c'est-à-dire, si et seulement si $\eta \in \mathbf{QLV}$. ■

Remarques : Depuis un timbre, il est toujours possible de calculer le timbre ou monoïde stable. Par conséquence, si l'appartenance à $\mathbf{V}$ est décidable alors l'appartenance à $\mathbf{QV}$ et à $\mathbf{QLV}$ est également décidable.

Il est tentant de conjecturer que l'opération **QV** est toujours égale à $\mathbf{V} * \mathbf{MOD}$ et pas uniquement dans le cas local. Cela n'est malheureusement pas vrai, comme nous pouvons maintenant le montrer.

Proposition 4.32.

Il existe un langage dont le timbre syntaxique est dans **QJ** mais n'appartient pas à $\mathbf{J} * \mathbf{MOD}$.

Démonstration : Nous allons montrer que le langage $L = (aa)^*(bb)^*$ a son monoïde stable dans **J**, puis que son timbre syntaxique n'appartient pas à $\mathbf{J} * \mathbf{MOD}$. Pour ce faire, nous allons utiliser le théorème de délai partiel prouvé dans la section suivante (voir Théorème 4.34). On pourrait également utiliser le résultat [21, Théorème 4.5].

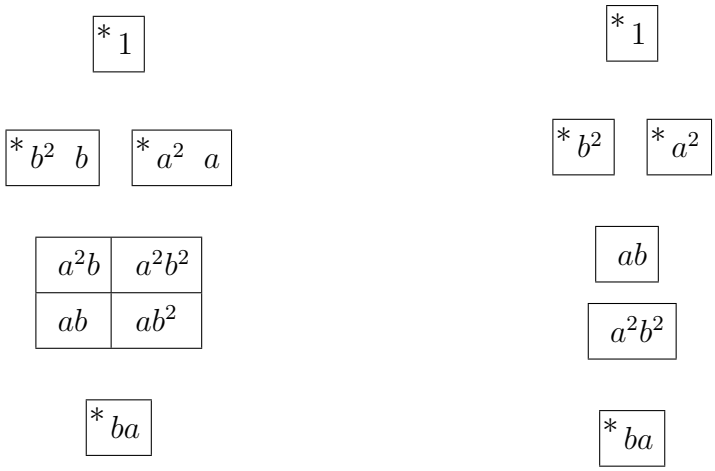
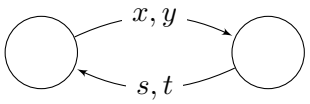


FIGURE 4.2 – Représentation en diagramme *boite-à-œuf* du monoïde et monoïde stable du langage $(aa)^*(bb)^*$

Ce langage a pour indice de stabilité 4 et son monoïde stable est $\mathcal{J}$-trivial. Ce langage appartient bien à **QJ**. Montrons qu'il n'appartient pas à $\mathbf{J} * \mathbf{MOD}$. D'après le théorème du délai partiel (voir Théorème 4.34), il suffit de montrer que $C_8(L)$ n'appartient pas à **gJ**. On utilise pour ça l'équation de **gJ** :



$$(sx)^\omega s(yt)^\omega = (sx)^\omega t(yt)^\omega$$

En posant $s = \eta_L(a)$, $x = \eta_L(a^7)$, $t = \eta_L(b)$ et $y = \eta_L(b^7)$ on a

$$(sx)^\omega s(yt)^\omega = \eta_L(a^8ab^8) = \eta_L(abb)$$
$$(sx)^\omega t(yt)^\omega = \eta_L(a^8bb^8) = \eta_L(aab)$$

Et comme $\eta_L(abb) \neq \eta_L(aab)$, nous avons bien que $C_8(L) \notin \mathbf{gJ}$. Ce qui conclut la preuve. ■

4.5.2 Le cas des variétés de monoïdes de rang borné

Nous allons donner le résultat principal de ce chapitre. Avant toute chose, il est nécessaire d'expliquer les deux différentes notions de *rang* qui nous seront utiles afin de prouver un théorème de délai.

Définition 4.33 (Rang d'une variété).

Soit V une variété de monoïdes finis. On dit que $\mathbf{V}$ est de rang k s'il existe un ensemble d'équations E tel que $\mathbf{gV} = [\![E]\!]$ et vérifiant que pour $(X, u = v) \in E$, la taille de $\mathrm{Ob}(X)$ est plus petite que k.

Exemples : Introduisons quelques exemples :

- Toute variété locale $\mathbf{V}$ est de rang 1.
- Les variétés $\mathbf{J}$ et $\mathbf{Com}$ sont de rang 2.
- La variété $\mathbf{V}_k$, équivalente à $\mathbf{FO}^2_k[<]$, est de rang $2k$.

Nous allons maintenant présenter un résultat de délai partiel pour $\mathbf{MOD}$ pour les variétés dont le rang est fini. Nous utiliserons cette hypothèse pour réaliser une sorte de *pompage* des équations de catégories de petit rang. Nous montrerons ainsi que si une équation de rang k est satisfaite par $C_{ds}(L)$, alors elle est satisfaite par $C_{ks}(L)$, ce qui nous permettra de conclure.

Théorème 4.34 (Le théorème de délai partiel pour MOD).

Soient $\mathbf{V}$ une variété de monoïdes de rang inférieur à k et L un langage régulier d'indice de stabilité s. Si $\mathcal{I}d_{\mathbf{V}}(L)$ est non vide, alors $ks \in \mathcal{I}d_{\mathbf{V}}(L)$.

Ce théorème peut être reformulée en disant qu'un timbre syntaxique appartient à $\mathbf{V} * \mathbf{MOD}$ si et seulement s'il appartient à $\mathbf{V} * \mathbf{MOD}_{ks}$, où s est son indice de stabilité.

Avant de présenter la preuve de ce théorème, en voici la principale conséquence.

Corollaire 4.35.

Soit $\mathbf{V}$ une variété de monoïdes de rang k et telle que l'appartenance à $\mathbf{gV}$ est décidable et $\mathcal{W}$ la *mu*-variété de langages correspondant à $\mathbf{V} * \mathbf{MOD}$. L'appartenance d'un langage régulier à $\mathcal{W}$ est décidable.

Démonstration : D'après le théorème de la catégorie dérivée, un langage L a son timbre syntaxique dans $\mathbf{V} * \mathbf{MOD}$ si et seulement s'il existe un entier d tel que $C_d(L)$ appartient à $\mathbf{gV}$. D'après le théorème du délai, il suffit alors de tester l'appartenance de la catégorie $C_{ks}(L)$ à $\mathbf{gV}$ pour conclure. ■

Preuve du théorème 4.34

Soient L un langage régulier et η son timbre syntaxique. On suppose que $d \in \mathcal{I}d_{\mathbf{V}}(L)$. D'après le théorème de la catégorie dérivée pour **MOD**, il existe d tel que $C_d(L) \in \mathbf{gV}$. D'après la proposition 4.19, on a donc $ds \in \mathcal{I}d_{\mathbf{V}}(L)$. Quitte à remplacer d par un de ces multiples, on peut supposer que $d > k$. D'après le théorème de la catégorie dérivée pour **MOD**, $C_{ds}(L)$ appartient à $\mathbf{gV}$.

Montrons que $C_{ks}(L)$ appartient également à $\mathbf{gV}$. Les équations de rang $p < k$ étant des cas particuliers d'équations de rang k, il suffit de montrer que $C_{ks}(L)$ vérifie toutes les équations de catégories de $\mathbf{gV}$ de rang k. Raisonnons par l'absurde. Supposons qu'il existe une équation de catégories $(X, u = v)$ de $\mathbf{gV}$ non satisfaite par $C_{ks}(L)$ et de rang k. Comme on définit $h : X \to C_{ks}(L)$ tel que $\overline{h}(u) \neq \overline{h}(v)$ pour $\overline{h}$ l'unique prolongement de h en un morphisme uniformément continu de X^{Δ} vers $C_{ks}(L)$. On pose également $E = h(\mathrm{Ob}(X)) \subseteq \mathbb{Z}/ks\mathbb{Z}$. Le lemme suivant est une conséquence du lemme des tiroirs.

Lemme 4.36.

Il existe $i_s \in \mathbb{Z}/ks\mathbb{Z}$ tel que $\{i_s + 1, \ldots, i_s + s - 1\} \cap E = \emptyset$.

Démonstration : On note $e_1 < \ldots < e_k$ les éléments de E et

$$\begin{aligned} I_1 &= \{e_1, e_1 + 1, \ldots, e_2 - 1\}, \\ I_2 &= \{e_2, e_2 + 1 \ldots, e_3 - 1\}, \\ &\ldots \\ I_k &= \{e_k, e_k + 1, \ldots, e_1\}, \end{aligned}$$

où l'addition est réalisée dans $\mathbb{Z}/ks\mathbb{Z}$. Par construction, les ensembles $I_1, \ldots, I_k$ forment une partition de $\mathbb{Z}/ks\mathbb{Z}$ et chacun d'entre d'eux contient exactement un élément de E. Nécessairement, il existe j tel que la taille de I_j soit de taille au moins s et, en posant $i_s = e_j$, on a $\{i_s + 1, \ldots, i_s + s - 1\} \subseteq I_j$, d'où $\{i_s + 1, \ldots, i_s + s - 1\} \cap E = \emptyset$. ■

On pose maintenant

$$\theta : \begin{cases} E \to \mathrm{Ob}(C_{ds}(L)) & \\ j \mapsto j & \text{si } j \leqslant i_s \text{ en tant qu'entier} \\ j \mapsto ds + j - ks & \text{sinon} \end{cases}$$

L'application θ ainsi définie vérifie que pour $i, j \in E$ $j - i \equiv \theta(j) - \theta(i) \bmod s$. Cela nous sera utile pour la preuve suivante. On rappelle que les flèches de $C_{ds}(L)$ et de $C_{ks}(L)$ sont des éléments du monoïde syntaxique de L.

Lemme 4.37.

Soient $i, j \in E$ et $m \in C_{ks}(L)(i, j)$. Alors $m \in C_{ds}(L)(\theta(i), \theta(j))$.

Démonstration : On remarque d'abord que comme $m \in C_{ks}(L)(i,j)$, alors il existe un mot u tel que $\eta(u) = m$ et $i + |u| \equiv j \bmod ks$. On distingue plusieurs cas possibles.

- Si $|u| \geqslant s$, alors par définition de l'indice de stabilité, pour tout entier ℓ, il existe un mot u_ℓ tel que $\eta(u) = \eta(u_\ell)$, $\ell s \leqslant |u_\ell| \leqslant (\ell+1)s$ et $|u_\ell| \equiv |u| \bmod s$. En particulier, comme $\theta(i) - \theta(j) \equiv i - j \bmod s$, on a que $m \in C_{ds}(\theta(i), \theta(j))$.
- Supposons que $|u| < s$. On distingue les quatre cas suivants.
  - Si $\theta(i) = i$ et $\theta(j) = j$, alors puisque $|u| < s$ et que $\theta(i) + |u| \equiv \theta(j) \bmod ds$ et donc $m \in C_{ds}(L)(\theta(i), \theta(j))$.
  - Si $\theta(i) = ds + i - ks$ et $\theta(j) = ds + j - ks$, alors comme $\theta(j) - \theta(i) = j - i$, en particulier, $\theta(i) + |u| \equiv \theta(j) \bmod ds$ et donc $m \in C_{ds}(L)(\theta(i), \theta(j))$.
  - Si $\theta(i) = ds + i - ks$ et $\theta(j) = j$, alors $i + |u| = j + ks$. C'est pourquoi $\theta(i) + |u| = ds + i - ks + |u| = j + ds$ et finalement, $m \in C_{ds}(L)(\theta(i), \theta(j))$.
  - Le cas $\theta(i) = i$ et $\theta(j) = ds + i - ks$ est impossible car, $i \leqslant i_s$ et $j > i_s + s$. En particulier, $|u| = j - i \geqslant s$, or par hypothèse $|u| < s$. ■

On définit une application $T : X \to C_{ds}(L)$ telle que pour tout objet e de X, $T(e) = \theta(h(e))$, pour tout objet f et pour toute flèche $x \in X(e,f)$, $T(x) = h(x)$. D'après le lemme précédent, l'application T est bien définie car $h(x) \in C_{ds}(L)(T(e), T(f))$.

Par hypothèse, $C_{ds}(L)$ vérifie l'équation $(X, u = v)$ et donc $\overline{T}(u) = \overline{T}(v)$. Mais, par construction de T,

$$\overline{T}(u) = \overline{h}(u) \neq \overline{h}(v) = \overline{T}(v).$$

Ce qui est absurde. C'est pourquoi $C_{ks}(L)$ satisfait toutes les identités de $\mathbf{gV}$ et donc appartient à $\mathbf{gV}$. Ce qui conclut cette preuve.

4.5.3 Le cas des variétés de monoïdes de rang axiomatique borné

Nous allons adapter la preuve précédente afin d'obtenir un résultat similaire pour les variétés de la forme $\mathbf{V} * \mathbf{D}$ quand $\mathbf{J_1} \subseteq \mathbf{V}$.

Définition 4.38 (Rang axiomatique d'une *ne*-variété).

Soit V une *ne*-variété de timbres. On dit que $\mathbf{V}$ est de rang axiomatique k s'il existe un ensemble de *ne*-équations E sur un alphabet de taille k tel que $V = [\![E]\!]$.

Le rang axiomatique d'une *ne*-variété de la forme $\mathbf{V} * \mathbf{D}$ peut se calculer (quand il est fini) à partir des équations du global. En effet, si une variété est de rang k (et donc son global utilise des équations de catégories sur au plus k objets) et si toutes les équations de catégories du global sont sur un alphabet de taille au plus p, alors $\mathbf{V} * \mathbf{D}$ est de rang axiomatique $k + p$.

Exemples :

- La *ne*-variété $\mathbf{Com} * \mathbf{D}$ est de rang axiomatique 5.

- La *ne*-variété $\mathbf{V}_k * \mathbf{D}$, équivalente à $\mathbf{FO}^2_k[<, \mathrm{LOC}]$, est de rang axiomatique $2k+4k = 6k$.

À l'aide de cette hypothèse de rang axiomatique, nous allons prouver un théorème du délai en reprenant les idées de preuves utilisées pour le théorème 4.34.

Théorème 4.39 (Le théorème de délai partiel pour $\mathbf{D} * \mathbf{MOD}$).

Soient $\mathbf{V}$ une variété de monoïdes contenant $\mathbf{J_1}$ et telle que $\mathbf{V} * \mathbf{D}$ soit de rang axiomatique k et L un langage régulier d'indice de stabilité s. Si $\mathcal{I}d_{\mathbf{V}*\mathbf{D}}(L)$ est non vide, alors $(2k+1)s \in \mathcal{I}d_{\mathbf{V}*\mathbf{D}}(L)$.

Ce théorème peut être reformulée en disant qu'un timbre syntaxique appartient à $\mathbf{V} * \mathbf{MOD}$ si et seulement s'il appartient à $\mathbf{V} * \mathbf{MOD}_{(2k+1)s}$, où s est son indice de stabilité.

La principale conséquence de ce théorème est le corollaire suivant.

Corollaire 4.40.

Soient $\mathbf{V}$ une variété de monoïdes contenant $\mathbf{J_1}$ et telle que $\mathbf{V} * \mathbf{D}$ soit décidable et de rang axiomatique k. L'appartenance d'un langage régulier à la *mu*-variété de langages correspondant à $\mathbf{V} * \mathbf{D} * \mathbf{MOD}$ est décidable.

Démonstration : Notons $\mathcal{W}$ (resp. $\mathcal{W}_d$) la *mu*-variété de langages correspondant à $\mathbf{V} * \mathbf{D} * \mathbf{MOD}$ (resp. $\mathbf{V} * \mathbf{D} * \mathrm{MOD}_d$) et $\mathcal{Z}$ la *ne*-variété de langage correspondant à $\mathbf{V} * \mathbf{D}$. Prenons L un langage régulier de A^* d'indice de stabilité s. D'après le théorème 4.39, si $L \in \mathcal{W}(A^*)$, alors $L \in \mathcal{W}_{(2k+1)s}(A^*)$. Or d'après la proposition 4.14, $L \in \mathcal{W}_{(2k+1)s}(A^*)$ si et seulement si le langage

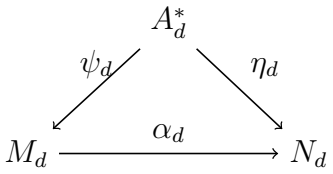
$$\pi^{-1}_{(2k+1)s}(L) \cap K_{(2k+1)s} \in \mathcal{Z}(A^*_{(2k+1)s}).$$

Or par hypothèse, l'appartenance d'un langage régulier à $\mathcal{Z}$ est décidable. Ce qui conclut la preuve. ■

Preuve du théorème 4.39

Avant de présenter la preuve, nous introduisons les quelques notations suivantes.

- On note $\mathcal{W}$ la *ne*-variété de langages associée à $\mathbf{V} * \mathbf{D}$.
- On note $\eta : A^* \to M$ le timbre syntaxique du langage L et s son indice de stabilité.
- On note $L_d = \pi_d^{-1}(L) \cap K_d$.
- On note $\eta_d : A_d^* \to N_d$ le timbre syntaxique du langage L_d.
- On pose également le timbre $\psi_d : A_d^* \to C_d(L)^1_{\mathrm{cd}}$ défini par $\psi_d(a, i) = (i, \eta(a), i+1)$. Dans la suite on notera M_d le monoïde $C_d(L)^1_{\mathrm{cd}}$. On rappelle que ce monoïde est un sous-monoïde de $\mathbb{Z}/d\mathbb{Z} \times M \times \mathbb{Z}/d\mathbb{Z}$. On rappelle également que ce timbre reconnaît le langage L_d (voir Proposition 4.27). On en déduit qu'il existe un morphisme surjectif $\alpha_d : M_d \to N_d$ tel que $\eta_d = \alpha_d \circ \psi_d$ (voir la proposition 2.6).



Nous allons pouvoir maintenant présenter le cœur de la preuve du théorème. Posons $d \in \mathcal{I}d_{\mathbf{V}*\mathbf{D}}(L)$. Comme $\mathcal{I}d_{\mathbf{V}*\mathbf{D}}(L)$ est un idéal, nous avons également $ds \in \mathcal{I}d_{\mathbf{V}*\mathbf{D}}(L)$. Quitte à multiplier d par un entier, on peut supposer que $(2k+1)s \leqslant ds$. Dans la suite, on pose $t = 2k+1$. D'après la proposition 3.33, le langage $L_{ds} = \pi_d^{-1}(L) \cap K_d$ a son timbre syntaxique dans $\mathbf{V} * \mathbf{D}$. Nous allons suivre le schéma de preuve du théorème 4.34 et prouver que L_{ts} a également son timbre syntaxique dans $\mathbf{V} * \mathbf{D}$.

Pour ce faire, nous allons prouver que L_{ts} satisfait toutes les équations définies sur un alphabet de taille au plus k de $\mathbf{V} * \mathbf{D}$. Soit $u =_{\mathrm{ne}} v$ une équation profinie sur un alphabet B de taille k satisfaite par la variété $\mathbf{V} * \mathbf{D}$. Montrons que η_{ts} vérifie cette *ne*-équation. On raisonne par l'absurde. On suppose qu'il existe un morphisme non effaçant $\kappa : B^* \to A_{ts}^*$ tel que le morphisme $\gamma = \eta_{ts} \circ \kappa$ vérifie que $\widehat{\gamma}(u) \neq \widehat{\gamma}(v)$. Pour chaque lettre $b \in B$, son image peut être un facteur bien formé ou non. Nous allons noter B_0 l'ensemble des lettres s'envoyant sur un mot qui n'est pas un facteur bien formé. Plus précisément, une lettre $b \in B$ telle que

$$\kappa(b) = (a_0, i_0) \cdots (a_n, i_n)$$

appartient à B_0 si et seulement s'il existe $0 \leqslant j < n$ vérifiant $i_{j+1} \not\equiv i_j + 1 \bmod ts$. On remarquera que nous avons $\gamma(B_0) = \{0\}$.

Soit $b \in B - B_0$ telle que

$$\kappa(b) = (a_0, i_0) \cdots (a_n, i_n),$$

on pose $i_b = i_0$ et $j_b \equiv i_n + 1 \bmod ts$. En utilisant ces notations, on obtient qu'il existe $m \in M$ tel que $\psi_d(\kappa(b)) = (i_b, m, j_b)$. Enfin on définit l'ensemble suivant dont le rôle va être central pour la suite :

$$E = \{i_b \mid b \in B - B_0\} \cup \{j_b \mid b \in B - B_0\} \cup \{0\} \subseteq \mathbb{Z}/ts\mathbb{Z}.$$

Comme B dispose d'au plus k lettres, E contient au plus t éléments.

Le monoïde N_d a un peu plus de structure que la catégorie $C_d(L)$ utilisée dans la preuve du théorème 4.34, nous allons utiliser par la suite la présence du 0 dans l'ensemble E pour passer outre. Le lemme suivante peut être prouvé exactement comme dans la preuve du théorème 4.34. Nous omettons donc la preuve.

Lemme 4.41.

Il existe $i_s \in \mathbb{Z}/ts\mathbb{Z}$ tel que $\{i_s + 1, \ldots, i_s + s - 1\} \cap E = \emptyset$.

On pose maintenant

$$\theta : \begin{cases} E \to \mathbb{Z}/ds\mathbb{Z} & \\ j \mapsto j & \text{si } j \leqslant i_s \text{ en tant qu'entier} \\ j \mapsto ds + j - ts & \text{sinon} \end{cases}$$

On remarque que l'application θ ainsi définie vérifie que $\theta(0) = 0$. Ce fait nous sera utile pour la suite. On rappelle que les flèches de $C_{ds}(L)$ et de $C_{ts}(L)$ sont des éléments du monoïde syntaxique de L. La preuve du lemme suivant est identique à celle du lemme 4.37

Lemme 4.42.

Soient $i, j \in E$ et $m \in C_{ts}(L)(i, j)$. Alors $m \in C_{ds}(L)(\theta(i), \theta(j))$.

La principale différence entre les deux preuves réside dans l'ajout du 0 dans l'ensemble E qui s'explique par la nécessité de prouver le lemme suivant. Celui-ci établit que si deux éléments de M_d ne sont pas équivalent pour α_d, alors leur image par l'opération θ seront des éléments également non-équivalents.

Lemme 4.43.

Soient $i, j, j' \in E$ et $(i, m, j), (i, m', j') \in M_{ts}$.

- Si $\alpha_{ts}(i, m, j) \neq \alpha_{ts}(i, m', j')$, alors
$$\alpha_{ds}(\theta(i), m, \theta(j)) \neq \alpha_{ds}(\theta(i), m', \theta(j')).$$
- Si $\alpha_{ts}(i, m, j) \neq 0$, alors
$$\alpha_{ds}(\theta(i), m, \theta(j)) \neq 0.$$

Démonstration : Nous allons prouver les deux points simultanément. Soient $i, j, j' \in E$ et $(i, m, j), (i, m', j') \in M_{ts}$.

Supposons que $\alpha_{ts}(i, m, j) \neq \alpha_{ts}(i, m', j')$. Sans perte de généralité, quitte à échanger le rôle de (i, m, j) et de (i, m', j), on peut supposer que $\alpha_{ts}(i, m, j) \neq 0$ et qu'il existe $(0, x, i), (j, y, \ell) \in M_{ts}$ tels que $xmy \in \eta(L)$ et

$$(0, x, i)(i, m', j')(j, y, \ell) \notin \psi_{ks}(L).$$

D'après le lemme 4.42,

$$(0, x, \theta(i)), (\theta(i), m, \theta(j)), (\theta(i), m', \theta(j)) \in M_{ds},$$

car $0 \in E$ et $\theta(0) = 0$. De plus, il existe $\ell' \in \mathbb{Z}/ds\mathbb{Z}$ tel que $(\theta(j), y, \ell')$ appartienne à M_{ds}. Nous avons donc que

$$(0, x, \theta(i))(\theta(i), m, \theta(j))(\theta(j), y, \ell') = (0, xmy, \ell') \in \psi_{ds}(L_{ds})$$

car $xmy \in \eta(L)$.

(1) Si $j' \neq j$, alors

$$(0, x, \theta(i))(\theta(i), m', \theta(j'))(\theta(j), y, \ell') = 0 \notin \psi_{ds}(L_{ds}).$$

(2) Si $j' = j$, alors

$$(0, x, \theta(i))(\theta(i), m', \theta(j'))(\theta(j), y, \ell') = (0, xmy, \ell').$$

Or

$$(0, x, i)(i, m', j)(j, y, \ell) = (0, xmy, \ell) \notin \psi_{ks}(L)$$

et donc $xm'y \notin \eta(L)$, d'où

$$\alpha_{ds}(\theta(i), m, \theta(j)) \neq \alpha_{ds}(\theta(i), m', \theta(j)).$$

De plus, on en déduit que

$$\alpha_{ds}(\theta(i), m, \theta(j)) \neq 0.$$

■

Nous allons maintenant construire un morphisme non effaçant $\kappa' : B^* \to A_{ds}^*$ permettant de rendre l'équation $u =_{\mathrm{ne}} v$ fausse sur η_{ds}.

Pour $b \in B_0$, on pose $\kappa'(b) = (a, 0)(a, 0)$ où $a \in A$. Ainsi, l'image des lettres de B_0 seront des facteurs mal formés et s'enverront sur 0,

Pour $b \in B - B_0$, on pose $\psi_{ts}(b) = (i_b, m_b, j_b) \in C_{ts}(L)^1_{\mathrm{cd}}$. D'après le lemme 4.42,

$$(\theta(i_b), m_b, \theta(j_b)) \in C_{ds}(L)^1_{\mathrm{cd}}.$$

On choisit un mot $u_b \in A_{ds}^+$ tel que $\psi_{ds}(u_b) = (\theta(i_b), m_b, \theta(j_b))$ et on pose $\kappa'(b) = u_b$.

Le morphisme κ' ainsi défini est non effaçant. On pose $\gamma' = \eta_{ds} \circ \kappa'$. Par définition de α_{ds} $\gamma'(b) = \alpha_{ds}(\theta(i_b), m_b, \theta(j_b))$. Comme η_{ds} appartient à $\mathbf{V} * \mathbf{D}$, ce timbre satisfait la *ne*-équation $u =_{\mathrm{ne}} v$ et donc $\widehat{\gamma'}(u) = \widehat{\gamma'}(v)$. Comme u et v sont des mots profinis, il existe (u_n) et (v_n) deux suites telles que $u = \lim u_n$ et $v = \lim v_n$. Pour n assez grand on aura donc

$$\widehat{\gamma}(u) = \gamma(u_n) \neq \widehat{\gamma}(v_n) = \gamma(v_n) \tag{4.1}$$

$$\widehat{\gamma'}(u) = \gamma'(u_n) = \widehat{\gamma'}(v_n) = \gamma'(v_n) \tag{4.2}$$

Posons $u_n = b_0 \cdots b_p$ et $v_n = c_0 \cdots c_q$. Nous allons distinguer plusieurs cas.

- Supposons que $\kappa(u_n)$ et $\kappa(v_n)$ sont des facteurs bien formés. Nous avons alors par construction

$$\begin{aligned}
\gamma(u_n) &= \alpha_{ts}\big(i_{b_0}, m_{b_0} \cdots m_{b_p}, j_{b_p}\big) \\
\gamma(v_n) &= \alpha_{ts}\big(i_{c_0}, m_{c_0} \cdots m_{c_q}, j_{c_q}\big) \\
\gamma'(u_n) &= \alpha_{ds}\big(\theta(i_{b_0}), m_{b_0} \cdots m_{b_p}, \theta(j_{b_p})\big) \\
\gamma'(v_n) &= \alpha_{ds}\big(\theta(i_{c_0}), m_{c_0} \cdots m_{c_q}, \theta(j_{c_q})\big)
\end{aligned}$$

D'après l'équation (4.2), nous avons

$$\alpha_{ds}\big(\theta(i_{b_0}), m_{b_0}\cdots m_{b_p}, \theta(j_{b_p})\big) = \alpha_{ds}\big(\theta(i_{c_0}), m_{c_0}\cdots m_{c_q}, \theta(j_{c_q})\big)$$

et donc nécessairement que $\theta(i_{b_0}) = \theta(i_{c_0})$ donc $i_{b_0} = i_{c_0}$. D'après l'équation (4.1),

$$\alpha_{ts}\big(i_{b_0}, m_{b_0}\cdots m_{b_p}, j_{b_p}\big) \neq \alpha_{ts}\big(i_{c_0}, m_{c_0}\cdots m_{c_q}, j_{c_q}\big)$$

et d'après le lemme 4.43, on obtient alors

$$\alpha_{ds}\big(\theta(i), m_{b_0}\cdots m_{b_p}, \theta(j)\big) \neq \alpha_{ds}\big(\theta(i), m_{c_0}\cdots m_{c_q}, \theta(j)\big)$$

ce qui est en contradiction avec l'équation (4.2). L'équation $u =_{\text{ne}} v$ est donc satisfaite par η_{ts}.

- Supposons que $\kappa(u_n)$ est un facteur mal formé. On a donc et $\gamma(u_n) = 0$. Si $\kappa(v_n)$ était également un facteur mal formé, alors $\gamma(v_n) = \gamma(u_n) = 0$ ce qui est impossible d'après l'équation (4.1). De plus, par construction de κ', $\kappa'(u_n)$ est également un facteur mal formé et donc $\gamma'(u_n) = 0$. D'après l'équation (4.2), on a $\gamma'(v_n) = 0$. Or, comme dans le point précédent,

  $$\gamma(v_n) = \alpha_{ts}\big(i_{c_0}, m_{c_0}\cdots m_{c_q}, j_{c_q}\big)$$

  et

  $$\gamma'(v_n) = \alpha_{ds}\big(\theta(i_{c_0}), m_{c_0}\cdots m_{c_q}, \theta(j_{c_q})\big).$$

  D'après le lemme 4.43, $\alpha_{ts}\big(i_{c_0}, m_{c_0}\cdots m_{c_q}, j_{c_q}\big) \neq 0$ implique que

  $$\alpha_{ds}\big(\theta(i_{c_0}), m_{c_0}\cdots m_{c_q}, \theta(j_{c_q})\big) \neq 0$$

  Ce qui est absurde.
- Le cas restant, c'est-à-dire où $\kappa(v_n)$ est mal formé, est symétrique au point précédent.

Ce qui conclut la preuve.

4.6 Retour à la logique

Contrairement au cas de l'ajout des prédicats locaux, nous n'avons pas prouvé que l'ajout des prédicats modulaires conservait la décidabilité de la hiérarchie d'alternances de **FO**. En effet, rien ne laisse à penser que les hypothèses des théorèmes de délai précédents soient satisfaites par cette hiérarchie.

Conjecture 4.44.

Pour tout entier n, les fragments $\mathcal{B}\mathbf{\Sigma}_n[<, \mathrm{MOD}]$ et $\mathcal{B}\mathbf{\Sigma}_n[\mathcal{R}\mathrm{eg}]$ sont décidables si et seulement si le fragment $\mathcal{B}\mathbf{\Sigma}_n[<]$ est décidable.

Application : le premier ordre

Dans les chapitres précédents, nous avons étudié le fragment **FO** sur plusieurs signatures numériques. Nous pouvons enrichir ces signatures à l'aide de prédicats modulaires. Le tableau 4.3 récapitule l'ensemble des résultats de décidabilité concernant le premier ordre obtenus à l'aide des théorèmes des chapitres précédents. Dans ce tableau L désigne un langage régulier et s son indice de stabilité.

Fragment	Variété	Équations	Testé sur
$\mathbf{FO}[\mathrm{MOD}]$	$\mathbf{QJ_1}$ corollaire 4.31	$[\![xy = yx, x^2 = x]\!]$	le monoïde stable
$\mathbf{FO}[\mathrm{LOC_D}, \mathrm{MOD}]$ $\mathbf{FO}^1[\mathrm{LOC_D}, \mathrm{MOD}]$	$\mathbf{QLJ_1}$ corollaire 4.31	$\left[\!\!\left[\begin{array}{l} x^\omega yzx^\omega = x^\omega zyx^\omega \\ x^\omega y^2 x^\omega = x^\omega yx^\omega \end{array} \right]\!\!\right]$	le semigroupe stable
$\mathbf{FO}[\mathrm{LOC}, \mathrm{MOD}]$ $\mathbf{FO}[=, \mathrm{LOC_D}, \mathrm{MOD}]$	$\mathbf{ACom} * \mathbf{D} * \mathbf{MOD}$ corollaire 4.40	de $\mathbf{ACom} * \mathbf{D}$	le langage $\pi_{11s}^{-1}(L) \cap K_{11s}$
$\mathbf{FO}[<, \mathrm{MOD}]$ $\mathbf{FO}[\mathcal{R}\mathrm{eg}]$	$\mathbf{QA}$ corollaire 4.31	$[\![x^{\omega+1} = x^\omega]\!]$	le monoïde stable
$\mathbf{MOD}[=, \mathrm{MOD}]$	$\mathbf{QAb}$ corollaire 4.31	$[\![x^\omega = 1, xy = yx]\!]$	le monoïde stable
$(\mathbf{FO} + \mathbf{MOD})[=, \mathrm{MOD}]$	$\mathbf{Com} * \mathbf{MOD}$ corollaire 4.35	de $\mathbf{gCOM}$	la catégorie $C_{2s}(L)$
$(\mathbf{FO} + \mathbf{MOD})[\mathrm{LOC}, \mathrm{MOD}]$ $(\mathbf{FO} + \mathbf{MOD})[=, \mathrm{LOC_D}, \mathrm{MOD}]$	$\mathbf{Com} * \mathbf{D} * \mathbf{MOD}$ corollaire 4.40	de $\mathbf{Com} * \mathbf{D}$	le langage $\pi_{11s}^{-1}(L) \cap K_{11s}$

FIGURE 4.3 – Le premier ordre.

Comme pour le chapitre précédent, le résultat de transfert suivant est immédiat, grâce à l'inclusion $\mathbf{V} * \mathbf{MOD} \subseteq \mathbf{QV}$ (voir Corollaire 4.29).

Proposition 4.45.

Pour tout entier k, il existe un langage dans $\mathcal{B}\mathbf{\Sigma}_{k+1}[\mathcal{R}\mathrm{eg}]$ qui n'est pas définissable dans $\mathcal{B}\mathbf{\Sigma}_k[\mathcal{R}\mathrm{eg}]$.

De la dernière ligne du tableau, on déduit la proposition suivante. On appelle *langages modulaires* les langages de la forme $L_{a,d} = \{u \in \{a,b\}^* \mid |u|_a \equiv 0 \bmod d\}$.

Proposition 4.46.

Soit $\mathcal{QA}$ la *mu*-variété de langages correspondant à **QA**. La *mu*-variété $\mathcal{QA}$ est la plus grosse *mu*-variété ne contenant aucun langage de la forme $L_{a,n}$ pour tout entier $n \in \mathbb{N}$.

Démonstration : Soit $\mathcal{V}$ une *mu*-variété de langages ne contenant aucun langage modulaire. On rappelle que **V** est la *mu*-variété de timbres correspondant à $\mathcal{V}$. Supposons par l'absurde que $\mathcal{V}$ ne soit pas incluse dans $\mathcal{QA}$.

En particulier, il existe un timbre $\eta : A^* \to M$ dans **V** qui n'est pas dans **QA**. Posons s son indice de stabilité et M_s son monoïde stable. Comme M_s n'est pas dans **A**, il existe un élément $x \in M_s$ tel que

$$x^\omega \neq x^{\omega+1}.$$

Soit $B = \{a, b\}$ et u un mot de longueur s tel que $\eta(u) = x^{\omega+1}$ et v un mot de longueur s tel que $\eta(v) = x^\omega$. On pose $\psi : B^* \to A^*$ défini par $\psi(a) = u$ et $\psi(b) = v$. Le morphisme ψ est multiplicatif donc le langage $\psi^{-1}(\eta^{-1}(x^\omega))$ est dans $\mathcal{V}$. Or, par construction, il s'agit du langage $L_{a,d}$ pour $d > 1$ la puissance d'idempotence de $x^{\omega+1}$. Ce qui absurde. ■

Application : La restriction à deux variables

Résumons les résultats connus pour l'ajout de prédicats modulaires aux fragments de **FO** à deux variables. On note $\mathbf{V}_k = [\![u_k = v_k, x^{\omega+1} = x^\omega]\!]$ la variété équivalente au fragment $\mathbf{FO}^2_k[<]$. Comme précédemment, L désigne un langage régulier et s son indice de stabilité.

Fragment	Variété	Équations	Testé sur
$\mathbf{FO}^2_k[<, \mathrm{MOD}]$	$\mathbf{V}_k * \mathbf{MOD}$ corollaire 4.35	de $\mathbf{gV}_k$	la catégorie $C_{2ks}(L)$
$\mathbf{FO}^2_k[<, \mathrm{LOC}, \mathrm{MOD}]$ $\mathbf{FO}^2_k[\mathcal{R}\mathrm{eg}]$	$\mathbf{V}_k * \mathbf{D} * \mathbf{MOD}$ corollaire 4.40	de $\mathbf{V}_k * \mathbf{D}$	le langage $\pi^{-1}_{(12k+1)s}(L) \cap K_{(12k+1)s}$
$\mathbf{FO}^2[<, \mathrm{MOD}]$	**QDA** corollaire 4.31	de **DA**	le monoïde stable
$\mathbf{FO}^2[<, \mathrm{LOC}, \mathrm{MOD}]$ $\mathbf{FO}^2[\mathcal{R}\mathrm{eg}]$	**QLDA** corollaire 4.31	de **LDA**	le timbre stable

FIGURE 4.4 – La restriction à deux variables.

En particulier, on obtient que le langage $c^*(ac^*bc^*)^*$, qui a une lettre neutre, n'est pas dans **QLDA**, comme énoncé dans la proposition 3.2. Comme pour le chapitre précédent, le résultat de transfert suivant est immédiat, grâce à l'inclusion $\mathbf{V} * \mathbf{MOD} \subseteq \mathbf{QV}$ (voir Corollaire 4.29).

Proposition 4.47.

Pour tout entier k, il existe un langage dans $\mathbf{FO}^2_{k+1}[\mathcal{R}\mathrm{eg}]$ qui n'est pas définissable dans $\mathbf{FO}^2_k[\mathcal{R}\mathrm{eg}]$.

De la dernière ligne du tableau, on déduit la proposition suivante.

Proposition 4.48.

Soit $\mathbf{V}$ une *mu*-variété de timbres. Si $\mathbf{QLDA} \subseteq \mathbf{V} \subseteq \mathbf{QA}$ et si le timbre syntaxique du langage $c^*(ac^*bc^*)^*$ n'appartient pas à $\mathbf{V}$, alors $\mathbf{V} = \mathbf{QLDA}$.

Démonstration : On pose dans la suite l'alphabet $A = \{a, b, c\}$ et $\mathcal{V}$ la *mu*-variété de langages correspondant à $\mathbf{V}$. Par hypothèse le langage $L = c^*(ac^*bc^*)^*$ n'appartient pas à $\mathcal{V}$.

On remarque dans un premier temps que si $\mathcal{V}(A^*)$ contient le langage $K = A^*ac^*aA^*$, alors $\mathcal{V}(A^*)$ contient

$$L = c^*aA^* \cap A^*bc^* \cap (A^*ac^*aA^*)^c \cap (A^*bc^*bA^*)^c.$$

Supposons que **V** contienne strictement **QLDA**. Il existe donc un timbre $\eta : A^* \to M$ dans **V** qui n'est pas dans **QLDA**. Posons s son indice de stabilité et S_s son semigroupe stable. Le timbre η appartient à **QA** et donc S_s vérifie l'équation

$$x^{\omega+1} = x^\omega.$$

Nous l'utiliserons à plusieurs reprises.

Comme S_s n'est pas dans **LDA**, il existe un idempotent $e \in S_s$ tel que $M_e = eS_se$ n'est pas dans **DA**. Il existe donc deux éléments x, y de M_e tels que

$$(xy)^\omega x(xy)^\omega \neq (xy)^\omega \tag{4.3}$$

Notons u, v et w trois mots de longueurs s tels que

$$\begin{aligned}\eta(u) &= (xy)^\omega x\\ \eta(v) &= y(xy)^\omega\\ \eta(w) &= e\end{aligned}$$

Soit $\psi : \{a, b, c\}^* \to A^*$ un morphisme défini par $\psi(a) = u$, $\psi(b) = v$ et $\psi(c) = w$. On remarque que ψ est un morphisme multiplicatif.

On pose $\tau = \eta \circ \psi \in \mathbf{V}$. On remarque que d'après l'équation (4.3) τ vérifie

$$\tau(aab) = (xy)^\omega x(xy)^\omega xy(xy)^\omega = (xy)^\omega x(xy)^\omega \neq (xy)^\omega = (xy)^\omega xy(xy)^\omega = \tau(ab)$$

et donc

$$\tau(aab) \neq \tau(ab) \tag{4.4}$$

On distingue deux cas.

- Supposons que η vérifie
$$(xy)^w y(xy)^w = (xy)^w.$$
Nous avons alors
$$\begin{aligned}\tau(bb) &= y(xy)^w y(xy)^w\\ &= \tau(b)\\ &= \tau(bab)\end{aligned}$$
On en déduit que $\tau(aba) = \tau(a)$. Posons $P = \tau(K)$. Nous allons montrer que $\tau^{-1}(P) = K$.
Soit $u = u_0 \cdots u_n$ un mot n'appartenant pas à K. Montrons que $\tau(u) \notin P$. Sans perte de généralité, nous pouvons supposer qu'aucune lettre c n'apparaisse dans u. Par définition du langage K, nous avons que chaque lettre a apparaissant dans u est soit en première position, soit en dernière position soit précédée et suivie d'une

lettre b. Comme $\tau(bab) = bbb$, le mot v où chaque facteur bab de u a été remplacé par un facteur bbb vérifie que $\tau(v) = \tau(u)$. Or $v \in (a+1)b^*(a+1)$ et donc

$$\tau(u) = \tau(v) \in \{\tau(b), \tau(ab), \tau(ba), \tau(a)\}.$$

De plus, comme eS_se est apériodique $\tau(aa) <_{\mathcal{J}} \tau(a)$ ou $\tau(a) = \tau(aa)$. Or d'après l'équation (4.4), $\tau(a) \neq \tau(aa)$ et donc $\tau(aa) <_{\mathcal{J}} \tau(a)$. Par définition

$$P = \{x \in eS_se \mid x \leqslant_{\mathcal{J}} \tau(aa)\}$$

et donc nous avons que $\tau(u) \notin P$. Ce qui conclut la preuve.

- Supposons que η vérifie

$$(xy)^w y (xy)^w \neq (xy)^w.$$

On en déduit que

$$\tau(aab) \neq \tau(ab) \tag{4.5}$$

Nous avons alors

$$\begin{aligned}\tau(aba) &= \tau(a)\\ \tau(bab) &= \tau(b)\\ \tau(abab) &= \tau(ab)\\ \tau(baba) &= \tau(ba)\end{aligned}$$

Posons $P = \tau(L)$. D'après les équations précédentes nous avons que $P = \{1, \tau(ab)\}$. Montrons que $L = \tau^{-1}(P)$. Prenons un mot $u \notin L$ et montrons que $\tau(u) \notin P$. Sans pertes de généralité on peut supposer qu'aucune lettre c n'apparaisse dans le mot u.
Le mot u n'appartient pas à L donc soit il possède un facteur aa, soit il possède un facteur bb soit il débute par b soit il termine par un a.
Comme eS_se est apériodique nous avons $\tau(aa) = \tau(a)$ ou $\tau(aa) <_{\mathcal{J}} \tau(a)$ ainsi que $\tau(aa) = \tau(a)$ ou $\tau(aa) <_{\mathcal{J}} \tau(a)$. D'après (4.4) et (4.5), on a que $\tau(aa) <_{\mathcal{J}} \tau(a)$ et $\tau(bb) <_{\mathcal{J}} \tau(b)$. Si le mot u possède un facteur aa ou bb, nous avons donc que $\tau(u) \notin P$.
Supposons que le mot u ne possède pas de tels facteurs et débute par un b. Nous avons alors que $u \in (ba)^*(a+1)$, d'où $\tau(u) \in \{b, ba\}$ et donc $\tau(u) \notin P$.
Symétriquement supposons que u ne possède pas de facteurs aa et bb et termine par un a. Nous avons alors que $u \in (1+a)(ba)^*$, d'où $\tau(u) \in \{a, ba\}$ et donc $\tau(u) \notin P$.
Ce qui conclut la preuve. ■

Deuxième partie

Prédicats numériques arbitraires

Introduction

Dans la partie précédente, nous avons étudié comment l'ajout de prédicats à un fragment modifie son expressivité. L'objectif étant de décrire des classes de langages réguliers, on s'est limité à des prédicats dont on pouvait garantir qu'ils ne permettraient pas de sortir des langages réguliers. Dans cette partie, nous allons nous concentrer sur des classes de langages définies par des fragments logiques, mais sans imposer de restriction aux prédicats numériques.

Les fragments ainsi définis correspondent à des classes de *complexité booléenne* que nous présenterons dans le chapitre qui suit. Puisque les classes de prédicats numériques arbitraires permettent de sortir des langages réguliers, nous ne pouvons plus utiliser les outils algébriques de la première partie. Afin d'évaluer l'expressivité de ces fragments, nous allons nous pencher sur deux questions :

- Peut-on transférer des résultats de séparations des fragments utilisant des prédicats réguliers vers des fragments utilisant des prédicats numériques arbitraires ?
- Peut-on caractériser les langages réguliers définissables dans un fragment utilisant des prédicats numériques arbitraires ?

La première question semble, en terme de *complexité*, la plus pertinente. En effet, être capable de séparer des classes de complexité constitue un problème récurrent et difficile. Puisqu'il est plus aisé de séparer des classes de langages réguliers, un théorème de transfert serait intéressant. Toutefois, il parait utopique d'en obtenir un en toute généralité. Nous présenterons deux résultats de transfert de séparation. L'un concerne la structure fine du fragment à deux variables du premier ordre auquel on ajoute des prédicats de *degré fini* (voir corollaire 6.12). Le second, présenté dans le dernier chapitre, est un résultat de transfert général pour l'ajout des prédicats arbitraires unaires (voir corollaire 7.6).

La seconde question est connue sous le nom de *conjecture de Straubing*. Cette conjecture, énoncée dans le livre [66], propose que l'ajout des prédicats numériques arbitraires n'augmente qu'*à la marge* l'expressivité des fragments. Plus précisément, ils ne permettent pas de définir plus de langages réguliers que les prédicats numériques réguliers. Il devient alors possible de caractériser effectivement les langages réguliers dans ces fragments enrichis de prédicats numériques arbitraires, à l'aide notamment des résultats de la première partie de ce manuscrit.

Cette conjecture est connue pour des fragments comme par exemple la logique du premier ordre. Les preuves reposent principalement sur des résultats de bornes inférieures pour les langages modulaires (voir Théorème 5.5). Ainsi, on obtient que ces langages ne sont pas définissables dans le premier ordre enrichi des prédicats numériques arbitraires. Les propositions 4.46 et 6.2 permettent alors de conclure.

La conjecture de Straubing a été majoritairement étudiée dans le contexte des fragments ($\mathbf{FO} + \mathbf{MOD}(Q)$). L'objectif était alors de reformuler logiquement la conjecture, toujours ouverte, de séparation entre les classes $\mathbf{ACC}$ et $\mathbf{NC^1}$. On l'énoncera sur des fragments quelconques équipés d'une classe de prédicats numériques (voir la conjecture 6.1).

Une autre conjecture, dite de *Crane Beach*, a tenté des reformulations purement logiques de ces questions. Cette dernière, suivant l'intuition apportée par la conjecture de

Straubing, proposait que les langages à lettre neutre définissables dans le premier ordre à l'aide de prédicats numériques arbitraires pouvaient être définis uniquement à l'aide de l'ordre. Elle a malheureusement été réfutée dans l'article [11], mais les concepts qu'elle introduit restent pertinents pour d'autres fragments, moins expressifs. Puisqu'il ne s'agit plus d'une conjecture, on y fera dorénavant référence en tant que la *propriété de Crane Beach* (voir la définition 6.7).

Enfin, le dernier chapitre de cette thèse présentera une nouvelle conjecture plus forte (et optimiste) que celle de Straubing : la conjecture de *substitution*. Cette dernière propose que si un langage régulier est définissable à l'aide de prédicats numériques non réguliers, alors il est possible de *substituer* ces prédicats syntaxiquement dans la formule par des prédicats réguliers, tout en définissant le même langage. Les principales contributions de cette partie sont les suivantes :

- La présentation de caractérisations logiques des classes de complexité linéaire (voir Théorème 5.9). Ce résultat qui était connu pour la restriction linéaire de $\mathbf{AC^0}$ sera étendu aux classes disposant de portes modulaires.
- La caractérisation algébrique des langages réguliers de $\mathbf{WLAC^0}$ (voir Théorème 5.13). Les points clefs de ce résultat sont fournis par l'article [40] ainsi que par la caractérisation algébrique de $\mathbf{FO}^2[\mathcal{R}\mathrm{eg}]$ (voir la proposition 4.48).
- La preuve de la propriété Crane Beach pour la hiérarchie fine de $\mathbf{FO}^2$ équipée de l'ordre et des prédicats de *degré fini* (voir Théorème 6.10). Cette preuve est la plus difficile de cette thèse. Elle repose principalement sur la propriété de *Crane Beach*, sur les jeux d'Ehrenfeucht-Fraïssé ainsi que sur l'utilisation du *théorème de Ramsey*. On en déduit la séparation de cette hiérarchie ainsi qu'une preuve de la conjecture de Straubing sur ce fragment.
- La fin de cette thèse est consacrée à l'étude systématique de l'ajout des prédicats unaires. En effet, cette restriction rend le problème bien plus simple. Ainsi, on prouvera que **MSO** équipée de l'ordre et des prédicats monadiques vérifie la propriété de Crane Beach (voir Théorème 6.24). On montrera également la conjecture de substitution pour ce fragment (voir Théorème 7.2). On donnera un contre-exemple à la substitution pour le cas binaire (voir la section 7.3) et l'on sera amené à énoncer une version affaiblie de la substitution (voir la définition 7.10) qui ne tombera pas sous le coup du contre-exemple de la proposition 7.11. Ces travaux on été réalisés en collaboration avec Nathanaël Fijalkow (voir l'article [27]).

De nombreuses questions intéressantes de ce domaine restent ouvertes. La plus emblématique est probablement la séparation de **ACC** et $\mathbf{NC^1}$. J'ai porté une attention particulière aux questions suivantes :

- La caractérisation effective des langages réguliers de $\mathbf{LAC^0}$. En effet, si la conjecture de Straubing était vérifiée pour le fragment logique équivalent, on obtiendrait plusieurs résultats, notamment, que les langages réguliers de $\mathbf{LAC^0}$ sont exactement ceux de $\mathbf{WLAC^0}$. Une autre conséquence pertinente concerne le calcul des bornes inférieures pour le circuit de l'addition de deux entiers. La difficulté de ces questions est illustrée par le théorème 5.20.

- La propriété de substitution faible. Au vu des implications, il ne serait pas étonnant que ce soit un problème difficile ou tout simplement qu'il existe des fragments peu expressifs l'infirmant. Quoi qu'il en soit, les contraintes syntaxiques ainsi imposées forcent à un point de vue nouveau sur ces questions et pourraient apporter un angle d'attaque innovant. Le cas le plus simple, des formules disposant d'une unique occurrence d'un unique prédicat numérique, semble déjà difficile.

Chapitre 5

Les circuits booléens

5.1 Définitions

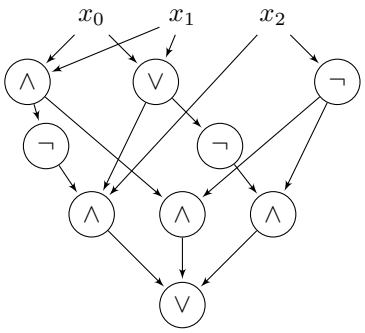
Un *circuit booléen* est un *graphe fini orienté acyclique* avec un ensemble de portes de degré entrant nul, que l'on désigne comme *les entrées*, et un ensemble de portes de degré sortant nul que l'on désigne comme *les sorties*. Le circuit *calcule* les sorties en fonction des entrées. Les entrées sont numérotées de 0 à $n-1$ pour un circuit ayant n entrées et les sorties de 0 à $p-1$ pour un circuit ayant p sorties.

Les portes autres que les entrées sont étiquetées par des fonctions booléennes commutative dont l'arité est égale au degré entrant. La *profondeur* d'une porte est le plus long chemin qui relie cette porte à une des entrées. Un circuit calcule les sorties avec comme entrée un mot $u_0 \cdots u_{n-1} \in \{0,1\}^n$ en remplaçant l'entrée numérotée par i par la valeur de la lettre u_i. On évalue ensuite chaque porte, profondeur par profondeur, en remplaçant les fonctions booléennes par leur valeur avec comme entrée les portes antécédentes ; ces fonctions étant commutatives l'ordre des entrées n'a pas d'importance. La sortie du circuit est un mot $v_0 \cdots v_{p-1} \in \{0,1\}^p$ avec v_i la valeur de la porte de sortie numérotée par i.

Ainsi, un circuit avec n portes d'entrée et p portes de sortie calcule une fonction de $\{0,1\}^n$ vers $\{0,1\}^p$. Si $p=1$, alors le circuit *accepte* un mot en entrée si celui-ci est évalué à 1 et le rejette sinon.

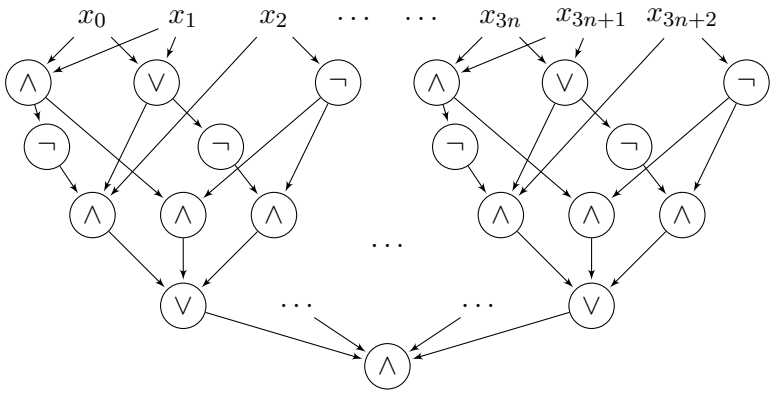
Dans cette thèse, on se contentera des portes $\wedge^r$, $\vee^r$, d'arité r, de la porte $\neg$ d'arité 1, ainsi que des portes MOD_n, pour $n \in \mathbb{N}$ d'arité quelconque telles que, pour $u \in \{0,1\}^*$, on a $\mathrm{MOD}_n(u) = 1$ si et seulement si $|u|_1 \equiv 0 \bmod n$.

Exemple : Le circuit suivant à trois entrées x_1, x_2 et x_3 et accepte si et seulement si $x_0 \oplus x_1 = x_2$.



Un circuit booléen *calcule* des mots d'une longueur fixée. Pour comparer la puissance d'expression des circuits booléens par rapport aux autres modèles de calculs, comme les automates finis, il est nécessaire de leur faire calculer des langages dont les mots ne sont pas nécessairement d'une taille fixée. Afin de palier à cette limitation, on introduit la notion de *famille de circuits* ; il s'agit d'une suite de circuits $(C_n)_{n\in\mathbb{N}}$ avec C_n un circuit ayant n portes d'entrée. Un mot u est *accepté* par $(C_n)_{n\in\mathbb{N}}$ si le mot u est accepté par le circuit $C_{|u|}$.

Exemple : La figure suivante représente une famille de circuits $(C_n)_{n\in\mathbb{N}}$. Les circuits d'indice non divisible par 3 sont triviaux et valent 0. Le circuit C_{3n} dispose de $3(n+1)$ entrées que l'on note $x_0x_1x_2\cdots x_{3n}x_{3n+1}x_{3n+2}$ et accepte si et seulement si pour tout $0 \leqslant i < n$ on a $x_{3i} \oplus x_{3i+1} = x_{3i+2}$.



Un langage est *calculé* par une famille de circuits s'il s'agit de l'ensemble des mots qui sont acceptés par cette famille.

Les circuits sont définis uniquement sur des alphabets binaires. Pour se ramener à des alphabets de taille supérieure on peut utiliser un encodage *unaire*. Par exemple si $A = \{a_1, \ldots, a_k\}$ est un alphabet de taille k, alors on représentera a_1 par $10\cdots0$, a_2 par $010\cdots0$, jusqu'à a_k qui sera représenté par $0\cdots01$. Ainsi le langage $(abc)^*$ sera représenté par le langage sur l'alphabet binaire $(100010001)^*$. Il s'agit ici d'une convention propre à cette thèse, il est possible d'encoder plus efficacement les lettres supplémentaires. On utilisera toujours la convention que le $n^{\text{ème}}$ circuit reconnaît les mots de taille n. Le $n^{\text{ème}}$ circuit de $(ac)^*$ aura donc $3n$ portes d'entrée dans l'alphabet binaires.

Une famille de circuits est caractérisée par deux paramètres importants :

(1) La *profondeur* : c'est-à-dire la fonction qui à l'entier n associe le plus long chemin d'une entrée vers une sortie dans le $n^{\text{ème}}$ circuit.
(2) La *taille* : c'est-à-dire la fonction qui à l'entier n associe le nombre de portes du $n^{\text{ème}}$ circuit.

Sans condition sur la taille du circuit, il est très facile de calculer tous les langages. En effet, il suffit d'énumérer tous les mots du langages et de tester si le mot en entrée est l'un d'entre eux. Une telle construction nécessite au pire un nombre exponentielle de portes et une profondeur bornée. On obtient donc la proposition suivante.

Proposition 5.1 (Folklore).

Tout langage est calculé par une famille de circuits de profondeur 3 et de taille exponentielle.

Afin d'obtenir une notion de complexité pertinente, nous choisissons de nous restreindre aux familles de circuits de taille polynomiale. En jouant sur les différents paramètres, profondeur, taille et type de portes, nous obtenons de nombreuses classes intéressantes.

Notations : Les paramètres que nous avons introduits définissent la *complexité booléenne* d'un langage.

- On note $\mathbf{AC^0}$ la classe des familles de circuits de profondeur bornée, de taille polynomiale et utilisant les portes $\wedge^r$, $\vee^r$ pour tout entier r ainsi que les portes $\neg$. On note également $\mathbf{AC^0_k}$ les familles ayant une taille bornée par un polynôme de degré k.
- On note $\mathbf{NC^1}$ la classe des familles de circuits de profondeur logarithmique, de taille polynomiale, et utilisant les portes $\wedge^2$, $\vee^2$ ainsi que les portes $\neg$.
- Pour n un entier non nul quelconque, on note $\mathbf{ACC}(n)$ la classe des familles de circuits de profondeur bornée, de taille polynomiale et utilisant les portes $\wedge^r$, $\vee^r$, pour tout r, MOD_n d'arité quelconque ainsi que les portes $\neg$. On note également $\mathbf{ACC_k}(m)$ les circuits ayant une taille bornée par un polynôme de degré k.
- Enfin on note également
$$\mathbf{ACC} = \bigcup_{m>0} \mathbf{ACC}(m)$$
ainsi que
$$\mathbf{ACC_k} = \bigcup_{m>0} \mathbf{ACC_k}(m).$$

Dans la suite, on ne distinguera pas les classes de familles de circuits des classes de langages qu'ils calculent. Par exemple, $\mathbf{AC^0}$ correspond aussi bien aux circuits dans $\mathbf{AC^0}$ qu'aux langages calculés par des circuits dans $\mathbf{AC^0}$.

Dans le cadre de l'étude de la complexité des langages réguliers, il n'est pas nécessaire d'aller au delà de $\mathbf{NC^1}$, comme le montre la proposition classique suivante (voir par exemple les articles [9, 18]).

Proposition 5.2.

Les langages réguliers appartiennent à $\mathbf{NC^1}$.

La preuve de ce dernier théorème peut être faite à l'aide d'une simple construction à partir des automates finis déterministes. En effet, il suffit de calculer pour chaque lettre en entrée les différents comportements possibles de l'automate, et de reconstruire son exécution, ce qui peut être réalisé à l'aide d'un circuit de profondeur logarithmique. Une attention particulière sera apportée aux *restriction linéaire* des classes de complexité plus classiques introduites ci-dessus.

Notations : Soit $\mathbf{C}$ une classe de familles de circuits.

- On note $\mathbf{LC}$ l'ensemble des familles de circuits de $\mathbf{C}$ dont le nombre de portes est linéaire.
- On note $\mathbf{WLC}$ l'ensemble des familles de circuits de $\mathbf{C}$ dont le nombre d'arêtes est linéaire.

On remarque que les notations sont (un peu) redondantes. Par exemple, la classe $\mathbf{LAC^0} = \mathbf{AC^0_1}$. De toutes ces définitions, on peut tirer des inclusions simples. On les résume à l'aide du schéma suivant, où les flèches représentent les inclusions entre les classes.

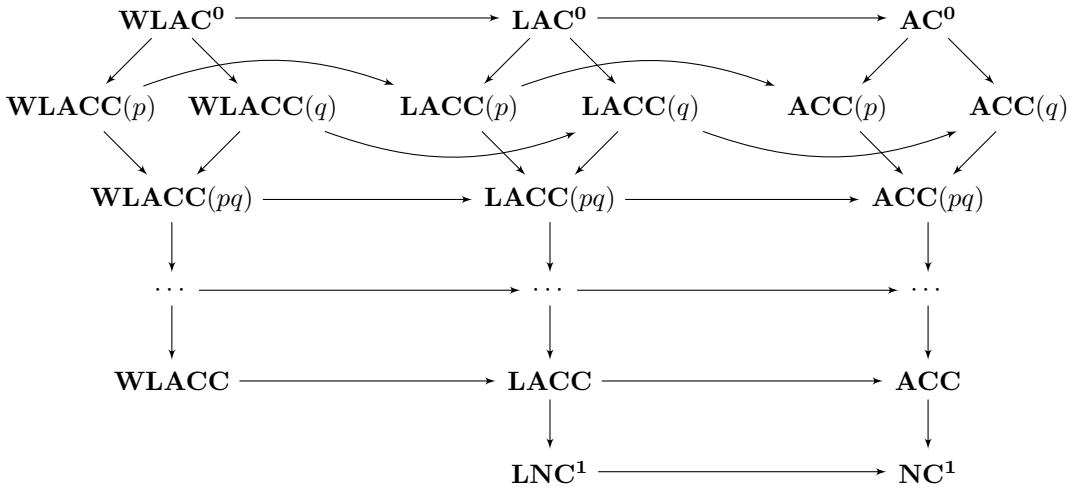


FIGURE 5.1 – Inclusions des classes de complexité de circuits

Nous savons que les langages réguliers appartiennent à $\mathbf{NC^1}$. Nous allons tenter de donner une intuition sur l'expressivité de ces différentes classes. Dans certains cas, il sera possible de décider à laquelle de ces classes appartient un langage régulier. Ce genre de résultats peut être obtenu à l'aide de caractérisations algébriques, du même ordre que celles obtenues dans la première partie de cette thèse, mais surtout de bornes inférieures de complexité, parfois très difficiles à obtenir.

5.2 Séparation de classes de circuits

Dans le cadre de l'étude de la complexité des circuits booléens, il est intéressant de savoir si certaines inclusions sont strictes. En effet, cela nous permet alors d'évaluer la puissance relative des classes de complexité. Nous appellerons un résultat de *séparation* de classes de circuits lorsqu'on prouvera qu'une inclusion est stricte. Les séparations de ces classes de complexité sont des questions difficiles, intéressantes et, pour certaines instances, ouvertes de longues dates. Nous allons maintenant présenter, sans donner de preuve, un certain nombre de résultats connus sur ce sujet.

Proposition 5.3 (Koucký, Lipton, Pudlák et Thérien [39]).

$$\mathbf{LAC^0} \subsetneq \mathbf{AC^0}.$$

Cette proposition se prouve en utilisant des arguments dits *de comptages*. Les familles de circuits linéaires sont donc strictement moins expressives que les familles de la classe $\mathbf{AC^0}$. Malheureusement, le seul langage séparateur connu n'est pas agréable à manipuler et est construit de manière *ad hoc*. Il n'éclaire qu'assez peu sur l'expressivité réelle de la classe $\mathbf{LAC^0}$. Déterminer exactement les langages réguliers de $\mathbf{LAC^0}$ fournirait beaucoup plus d'informations, mais il s'agit d'une question ouverte. Comme nous le verrons dans la suite de ce manuscrit, déterminer ces langages réguliers est relié à des questions difficiles concernant des bornes inférieures de complexité pour la fonction d'*addition*.

Le théorème suivant est un des résultats fondateurs de ce domaine. Non seulement il établit la séparation de la classe $\mathbf{AC^0}$ de $\mathbf{NC^1}$, mais en plus le séparateur est un langage régulier. De ce théorème, on peut comprendre l'intérêt d'étudier l'intersection des langages réguliers et des classes de complexité de circuit.

Théorème 5.4 (Furst, Saxe et Sipser [28]).

Les langages modulaires ne sont pas définissables dans $\mathbf{AC^0}$.

On rappelle que les langages modulaires sont de la forme

$$L_{a,n} = \{u \in A^* \mid |u|_a \equiv 0 \bmod n\}.$$

Ce théorème a été prouvé dans un premier temps en utilisant des méthodes probabilistes. Il a été par la suite reprouver à l'aide de résultat sur la combinatoire des circuits ; *via* le *switching lemma* d'Haståd (voir [32]). Enfin, ce théorème est un argument clef permettant de caractériser exactement les langages réguliers d'$\mathbf{AC^0}$ (voir théorème 6.3).

Le langage $L_{a,n}$ est définissable dans $\mathbf{ACC}(n)$ puisqu'il s'agit de l'utilisation d'une unique porte modulaire. On peut par contre se demander s'il est définissable dans $\mathbf{ACC}(p)$, avec p et n premiers entre eux, c'est-à-dire, si l'on peut utiliser un nombre polynomial de portes modulo p pour simuler une porte modulo n. Le théorème suivant permet de montrer que cela est impossible dans certains cas.

Théorème 5.5 (Razborov [56] et Smolensky [60]).

Pour tout entier premier p, tout entier k et tout entier n premier avec p, le langage modulaire $L_{a,n}$ n'appartient pas à $\mathbf{ACC}(p^k)$.

La preuve de ce résultat est difficile. Elle utilise des *approximations* de la fonction calculée par le circuit à l'aide de *polynômes à plusieurs variables dans un corps fini*.

Le théorème suivant est plus récent. Sa preuve utilise des notions de *complexité de la communication*. Elle peut être vue comme une généralisation d'un résultat similaire établissant l'impossibilité de réaliser l'addition dans $\mathbf{WLAC^0}$ [17]. Il nous sera utile pour établir la caractérisation des langages réguliers de $\mathbf{WLAC^0}$ (voir théorème 5.13).

Théorème 5.6 (Koucký, Pudlák et Thérien [40]).

Le langage $c^*(ac^*bc^*)^*$ n'appartient pas à $\mathbf{WLACC}$.

Finalement, ces résultats nous permettent d'obtenir la figure 5.2 qui résume l'ensemble des résultats de séparation connus. Les flèches en pointillées représentent des inclusions strictes qui sont conjecturées mais non prouvées. Les autres flèches représentent des inclusions strictes conséquences des théorèmes que nous venons d'exposer.

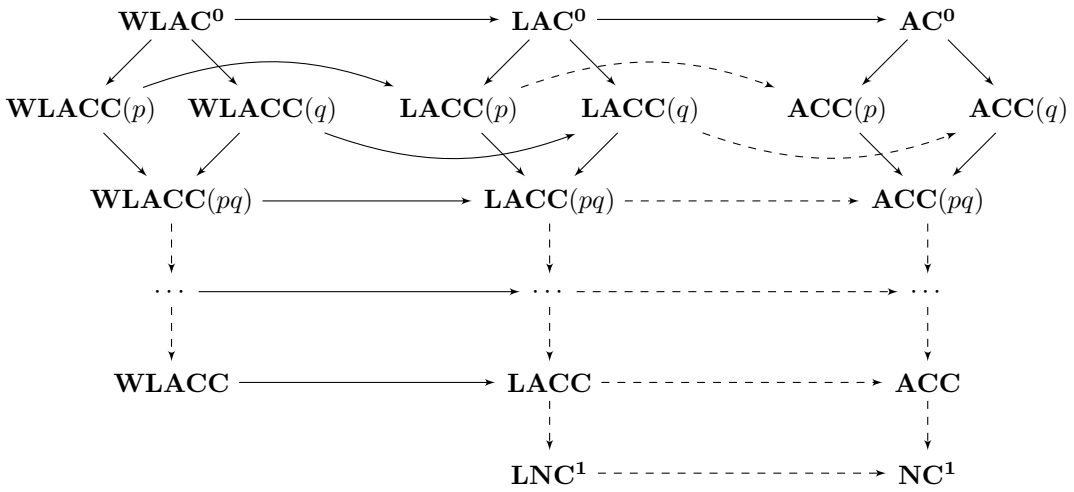


FIGURE 5.2 – Séparations connues des classes de circuits en dessous de $\mathbf{NC^1}$

5.3 Caractérisations logiques

La logique est un outil important pour obtenir une certaine intuition de l'expressivité de ces classes de complexité. Il s'agira également de notre principal outil afin d'établir

des correspondances avec les langages réguliers.

Théorème 5.7 (Immerman [33], Gurevich et Lewis [31]).

Un langage appartient à $\mathbf{AC^0}$ si et seulement s'il est définissable dans $\mathbf{FO}[\mathcal{A}\mathrm{rb}]$.

Le second théorème étend le résultat précédent au classe de circuits possédant des portes modulaires.

Théorème 5.8 (Barrington, Compton Straubing et Thérien [10]).

Soit m un entier strictement positif. Un langage appartient à $\mathbf{ACC}(m)$ si et seulement s'il est définissable dans $(\mathbf{FO} + \mathbf{MOD})(m)[\mathcal{A}\mathrm{rb}]$.

La preuve de ce théorème se fait en réalisant des traductions syntaxiques des familles de circuits vers les formules et réciproquement. Un résultat similaire est connu pour les classes de familles de circuits linéaires.

Théorème 5.9 (Koucký, Lipton, Pudlák et Thérien [39]).

Un langage appartient à $\mathbf{LAC^0}$ si et seulement s'il est définissable dans $\mathbf{FO}^2[\mathcal{A}\mathrm{rb}]$,

Ce résultat ne parle pas des autres classes de circuits linéaires que nous avons présenté. Nous allons donc l'étendre au cas du premier ordre enrichi de quantificateurs modulaires.

Théorème 5.10.

Soit m un entier strictement positif. Un langage appartient à $\mathbf{LACC}(m)$ si et seulement s'il est définissable dans $((\mathbf{FO} + \mathbf{MOD})(m))^2[\mathcal{A}\mathrm{rb}]$.

Nous décomposons la preuve en deux propositions. Il s'agit d'une adaptation issue de l'article [39], qui ne traite que du premier ordre sans quantifications modulaires.

Montrons dans un premier temps que les familles de circuits booléens de taille linéaires peuvent être traduites en formules logiques à deux variables.

Proposition 5.11.

Si un langage appartient à $\mathbf{LACC}(m)$, alors il est définissable dans $(\mathbf{FO} + \mathbf{MOD}(m))^2[\mathcal{A}\mathrm{rb}]$.

Démonstration : Soit $(C_n)_{n\in\mathbb{N}}$ une famille de circuits de $\mathbf{LACC}(m)$ et K la constante telle que la taille de C_n est au plus Kn. Quitte à ajouter un nombre linéaire de portes, il est possible de se ramener à un circuit où les portes de profondeur $i+1$ sont reliées uniquement à des portes de profondeur i . Comme le circuit a une profondeur constante, on suppose que le nombre de portes de chaque profondeur est borné par Kn. Chaque porte du circuit de profondeur ℓ, peut être uniquement décrit par le couple (x,c) avec $c \in [0; K-1]$ et $0 < x < n$. Chaque porte est étiquetée par une fonction $\wedge$, $\vee$, $\neg$ ou MOD_m. Donc, pour chaque entier $c \in [0; K-1]$ et chaque profondeur ℓ, on introduit les quatre prédicats suivants, $P_{\ell,c,\wedge}(x)$, $P_{\ell,c,\vee}(x)$, $P_{\ell,c,\neg}(x)$ et $P_{c,\mathrm{MOD}(m)}(x)$ d'arité k tels que la porte décrite par (x,c) est étiquetée par la fonction f avec $f \in \{\wedge,\vee,\neg,\mathrm{MOD}_m\}$ alors $P_{f,c,\ell}(x)$ est vrai et les trois autres prédicats sont faux.

On construit la formule que l'on recherche par induction sur la profondeur du circuit. On en déduira ainsi une unique formule pour la famille de circuits. En effet, on rappelle que les prédicats numériques ne sont pas uniformes, et dépendent donc de la taille des mots considérés. Cela va nous permettre ainsi d'encoder une unique formule pour une famille de circuits.

Les portes de profondeur 0 sont des portes d'entrée ; il suffit de prendre les prédicats de lettres comme formules. On définit K formules $\psi_{1,c}(x)$ avec $c \in [0; K-1]$ pour décrire les portes de profondeur 1. On introduit également les prédicats $Q_{1,c}$ tel que $Q_{1,c}(x,y)$ est vrai si et seulement si la porte décrite par (x,c) est reliée à la $y^{\text{ème}}$ entrée. On définit les formules suivantes.

$$\begin{aligned}
\psi_{1,c,\wedge}(x) &\equiv \forall y\ Q_{1,c}(x,y) \to \mathbf{1}(y),\\
\psi_{1,c,\vee}(x) &\equiv \exists y\ Q_{1,c}(x,y) \wedge \mathbf{1}(y),\\
\psi_{1,c,\neg}(x) &\equiv \neg\exists y\ Q_{1,c}(x,y) \wedge \mathbf{1}(y),\\
\psi_{1,c,\mathrm{MOD}_m}(x) &\equiv \exists^{(0,m)} y\ Q_{1,c}(x,y) \wedge \mathbf{1}(y).
\end{aligned}$$

Enfin, on pose

$$\psi_{1,c}(x) \ \equiv \bigvee_{f\in\{\wedge,\vee,\neg,\mathrm{MOD}(m)\}} \Big(P_{1,c,f}(x) \wedge \psi_{1,c,f}(x)\Big).$$

Pour $u \in A^n$ et $0 \leqslant j < n$ un entier, le mot u satisfait la formule $\psi_{1,c}(j)$ si et seulement si la porte de profondeur 1 encodée par (j,c) est évaluée à 1 sur l'entrée u.

On suppose qu'on a construit des formules $\psi_{i,c}(x)$ pour tout $c \in [0; K-1]$ tel que pour tout mot $u \in A^n$, et tout entier $0 \leqslant j < n$, le mot u satisfait la formule $\psi_{i,c}(j)$ si et seulement si la porte de profondeur i encodée par (j,c) est évaluée à 1 dans le circuit sur l'entrée u. On construit maintenant les formules $\psi_{i+1,c}(x)$.

On remarque que si on peut construire une formule $\psi_{i+1,c,f}(x)$ définissant la valeur de la porte de profondeur $i+1$ encodée par (x,c) si elle est étiquetée par une fonction f, alors la formule suivante convient

$$\psi_{i+1,c}(x) \ \equiv \bigvee_{f\in\{\wedge,\vee,\neg,\mathrm{MOD}(m)\}} \Big(P_{i+1,c,f}(x) \wedge \psi_{i+1,c,f}(x)\Big).$$

On construit maintenant les formules $\psi_{i+1,c,f}(x)$. Comme dans le cas de base, on introduit les prédicats $Q_{(i,c',c)}(x,y)$ d'arité 2 vérifiant que la porte de profondeur i est encodée par (y,c') et est reliée à la porte de profondeur $i+1$ encodée (x,c).

$$\psi_{i+1,c,\wedge}(x) \equiv \bigwedge_{c'\in[0;K-1]} \forall y\ Q_{(i,c',c)}(x,y) \to \psi_{i,c'}(y),$$
$$\psi_{i+1,c,\vee}(x) \equiv \bigvee_{c'\in[0;K-1]} \exists y\ Q_{(i,c',c)}(x,y) \wedge \psi_{i,c'}(y),$$
$$\psi_{i+1,c,\neg}(x) \equiv \neg \bigvee_{c'\in[0;K-1]} \exists y\ Q_{(i,c',c)}(x,y) \wedge \psi_{i,c'}(y),$$
$$\psi_{i+1,c,\mathrm{MOD}(m)}(x) \equiv \bigvee_{\substack{\vec{r}\in[0;m-1]^K \\ \sum_{c'=0}^{K-1} r_{c'}\equiv 0 \bmod m}} \bigwedge_{c'\in[0;K-1]} \exists^{(r_{c'},m)} y\ Q_{(i,c',c)}(x,y) \wedge \psi_{i,c'}(y).$$

■

Montrons maintenant que les formules logiques peuvent être traduites en circuits booléens.

Proposition 5.12.

Si un langage est définissable dans $(\mathbf{FO}+\mathbf{MOD}(m))^2[\mathcal{A}\mathrm{rb}]$, alors il appartient à $\mathbf{LACC}(m)$.

Démonstration : La preuve se fait par induction sur la structure de la formule. Il est donc nécessaire de gérer les variables libres, et donc de prouver un résultat légèrement plus fort. Comme nous étudions une logique à deux variables, il ne va pas être nécessaire de gérer plus qu'une variable libre à la fois.

Un circuit C va calculer une formule $\varphi(x)$ sur les mots de tailles n s'il possède n portes de sorties $s_0,\dots,s_{n-1}$ telles que pour tout mot $u\in A^n$ et tout entier $0\leqslant j<n$, $u\models\varphi(j)$ si et seulement si la porte s_j du circuit C est évaluée à 1 sur entrée u.

Les cas de base, des prédicats de lettres et des prédicats numériques unaires, sont trivialement gérés. Le cas des prédicats d'arité supérieur sera, quant à lui, géré à l'aide de l'induction. En effet, nous allons voir qu'ils vont coder la manière dont les portes sont reliées entre elles.

Dans un premier temps, remarquons que si deux formules, avec ou sans variable libre, vérifient l'hypothèse d'induction, alors leurs combinaisons booléennes la vérifient également. En effet, il suffit de reproduire les opérations booléennes avec les familles de circuits obtenues par l'hypothèse d'induction. Cela n'introduira qu'un nombre constant de portes si les formules sont closes, et un nombre linéaire de portes si elles ont une variable libre.

Pour terminer la preuve, il faut traiter le cas des quantifications.

- Soit φ une formule sans variable libre de la forme $Qy\ \psi(y)$ où $\psi(y)$ vérifie l'hypothèse d'induction et $Q \in \{\exists, \forall, \exists^{r,m}\}$. Dans le cas où $Q = \forall$, il suffit d'ajouter une unique porte $\wedge$ reliée aux sorties du circuit obtenu pour $\psi(y)$ par l'hypothèse d'induction. De même dans le cas où $Q = \exists$, il suffit d'ajouter une unique porte $\vee$ reliée à ces mêmes sorties. Enfin, dans le cas où $Q = \exists^{r,m}$, il suffit d'ajouter une unique porte MOD_m et la relier aux sorties du circuit obtenu pour $\psi(y)$ ainsi qu'à $m-r$ portes constantes égales à 1. De telles opérations n'introduisent qu'un nombre constant de portes. Le circuit ainsi construit vérifie bien l'hypothèse d'induction.
- Éxaminons le cas où $\varphi(x)$ est de la forme $\forall y\ \psi(x, y)$. Avant d'appliquer l'hypothèse d'induction, il est nécessaire de modifier la forme de la formule. Nous allons utiliser le fait que ψ n'utilise que deux variables pour la transformer en une formule plus agréable. Dans un premier temps, mettons la formule ψ en forme normal conjonctive

$$\psi(x, y) \equiv \bigwedge_{i \leqslant \ell} \Big(\gamma_i(x) \vee \delta_i(x, y) \vee \theta_i(y)\Big)$$

  où ℓ est un entier ne dépendant que de la formule et δ_i, γ_i et $\theta_{i,j}$ vérifient les conditions suivantes :
  - Les formules δ_i sont des combinaisons booléennes de prédicats numériques. En particulier δ_i ne contient aucun quantificateur ou prédicats de lettres.
  - Les formules de la forme $\gamma_i(x)$ n'ont pas de quantifications ou commencent par un quantificateur de la forme Qy où $Q \in \{\exists^{r,m}, \exists, \forall\}$. En particulier, les formules γ_i regroupent les formules indépendantes de la variable y.
  - Les formules $\theta_i(y)$ commencent par un quantificateur de la forme Qx où $Q \in \{\exists^{r,m}, \exists, \forall\}$.

  En distribuant la quantification $\forall y$ nous obtenons que

$$\forall y\ \psi(x, y) \equiv \bigwedge_{i \leqslant \ell} \Big(\gamma_i(x) \vee \forall y\ \big(\theta_i(y) \vee \delta_i(x, y)\big)\Big).$$

  Et donc,

$$\forall y\ \psi(x, y) \equiv \bigwedge_{i \leqslant \ell} \Big(\gamma_i(x) \vee \forall y\ \big(\neg\delta_i(x, y) \to \theta_i(y)\big)\Big).$$

  Les formules $\gamma_i(x)$ et $\theta_i(y)$ vérifient l'hypothèse d'induction. Nous allons en déduire que la formule $\varphi(x)$ la vérifie également. Soit Γ_i un circuit disposant de n entrées et n sorties équivalent à γ_i et Θ_i un circuit de n entrées et n sorties équivalents à θ_i. Nous allons construire un circuit C qui reconnaît la formule $\varphi(x)$. Posons $g_0, \ldots, g_{n-1}$ les n sorties du circuit C. Chacune d'entre elles est étiquetée par $\vee$. Pour tout entier $0 \leqslant t < n$, on relie la porte g_t à la $t^{\text{ème}}$ sortie du circuit Γ_i. Nous introduisons également n nouvelles portes $s_0, \ldots, s_{n-1}$ étiquetées par $\wedge$. Pour tout entier $0 \leqslant t < n$, la porte s_t est reliée à la $j^{\text{ème}}$ sortie du circuit Θ_i si et seulement si la formule $\delta_i(t, j)$ n'est pas satisfaite. Comme δ_i est une combinaison booléenne de prédicats numériques, son interprétation ne dépend pas du mot en entrée (par définition) et donc ce raccordement est bien défini. Pour conclure, il suffit de relier la porte s_t à la porte g_t.
- Le cas où $\varphi(x) \equiv \exists y\ \psi(x, y)$ peut être traité exactement de la même manière.

- Le cas où $\varphi(x) \equiv \exists^{r,m} y\ \psi(x,y)$ est légèrement différent. Pour des raisons analogues et en gardant les mêmes notations, nous pouvons obtenir la forme suivante :

$$\exists^{r,m} y\ \psi(x,y) \equiv \exists^{r,m} y \bigvee_{i \leqslant \ell} \gamma_i(x) \wedge \theta_i(y) \wedge \delta_i(x,y)$$

Ce qui donne en distribuant la quantification :

$$\exists^{r,m} y\ \psi(x,y) \equiv \bigvee_{\substack{\vec{r} \in [0;m-1]^\ell \\ \sum_{i=0}^{\ell} r_i \equiv r \bmod m}} \bigwedge_{i \leqslant \ell} \exists^{r_i,m} y \left(\gamma_i(x) \wedge \theta_i(y) \wedge \delta_i(x,y)\right)$$

Il n'est pas possible de simplement sortir la formule $\gamma_i(x)$ de la quantification à cause du cas $r = 0$. En effet, il est possible que $\exists^{0,m} y \left(\theta_i(y) \wedge \delta_i(x,y)\right)$ soit évaluée à *faux* ainsi que $\gamma_i(x)$. Leur conjonction sera donc également évaluée à *faux* mais la formule $\exists^{0,m} y \left(\gamma_i(x) \wedge \theta_i(y) \wedge \delta_i(x,y)\right)$ sera quant à elle évaluée à *vrai*. C'est pourquoi on obtient la forme suivante :

$$\exists^{r_i,m} y\ \gamma_i(x) \wedge \theta_i(y) \wedge \delta_i(x,y) \equiv \begin{cases} \gamma_i(x) \to \exists^{0,m} y\ \delta_i(x,y) \wedge \theta_i(y) \text{ si } r_i = 0 \\ \\ \gamma_i(x) \wedge \exists^{r_i,m} y\ \delta_i(x,y) \wedge \theta_i(x,y) \text{ sinon} \end{cases}$$

Dans les deux cas, une construction similaire à celle des points précédents permet de conclure cette preuve. ■

De ces résultats, on obtient des descriptions logiques résumées par la figure 5.3, où les flèches en pointillées représentent des inclusions et les doubles flèches représentent des égalités.

5.4 Les langages réguliers de $\mathbf{WLAC^0}$

À l'aide des théorèmes précédents, établissant des bornes inférieures de complexité, il est possible de déduire des caractérisations algébriques des langages réguliers dans les classes de complexité étudiées. Nous allons maintenant étudier le cas de $\mathbf{WLAC^0}$ qui a la particularité de ne pas avoir de reformulation logique agréable. Ce résultat est une amélioration de celui sur présenté dans l'article [40] établissant que les langages réguliers à lettre neutre de $\mathbf{WLAC^0}$ sont exactement ceux définissables dans $\mathbf{FO}^2[<]$. L'amélioration que nous proposons peut être obtenue grâce à la caractérisation algébrique de $\mathbf{FO}^2[\mathcal{R}\mathrm{eg}]$ obtenue dans la première partie de cette thèse.

Théorème 5.13.

Un langage régulier est dans $\mathbf{WLAC^0}$ si et seulement s'il est définissable dans $\mathbf{FO}^2[\mathcal{R}\mathrm{eg}]$.

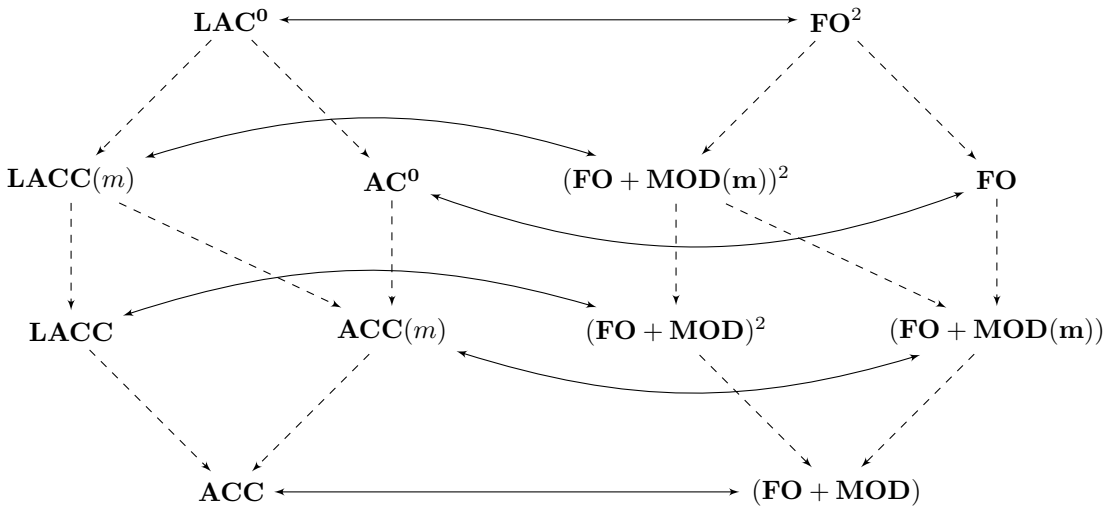


FIGURE 5.3 – Équivalence circuits-logique

La preuve se décompose en deux parties. On utilise le théorème 5.6, le lemme suivant ainsi que la proposition 4.48 pour prouver que les langages réguliers de $\mathbf{WLAC^0}$ sont dans $\mathbf{FO}^2[\mathcal{R}\mathrm{eg}]$.

Lemme 5.14.

La classe des langages réguliers de $\mathbf{WLAC^0}$ est une *mu*-variété de langages réguliers.

Démonstration : Il suffit de prouver que $\mathbf{WLAC^0}$ est stable par opération booléenne, quotient et morphisme inverse multiplicatif. La stabilité par opération booléenne est immédiate. Nous allons donner une construction pour la stabilité par quotient et par morphisme inverse multiplicatif. Soit L un langage régulier de A^* et (C_n) son circuit de $\mathbf{WLAC^0}$.

- Pour la stabilité par quotient, il suffit de le faire pour une lettre : nous allons montrer que $a^{-1}L$ est également dans $\mathbf{WLAC^0}$. Une construction symétrique donne que La^{-1} est dans $\mathbf{WLAC^0}$. Supposons que A soit un alphabet de taille k et que a est encodé par un mot $u \in \{0,1\}^k$. Pour chaque entier n, nous construisons le circuit (C'_n) ainsi. Nous ajoutons des portes constantes afin d'introduire u artificiellement au début du mot d'entrée. Nous utilisons le circuit C_{n+1} qui dispose de $k(n+1)$ entrées binaires. Les kn dernières entrées sont reliées aux n entrées de notre circuit. Les k premières sont reliées aux portes constituant u. Ainsi, le mot v est accepté si et seulement si av est accepté. Le nombre d'arêtes de C'_n est égal au nombre d'arêtes de C_{n+1}. Le circuit ainsi construit est bien dans $\mathbf{WLAC^0}$.
- Prenons $\mu : B^* \to A^*$ un morphisme multiplicatif avec B un alphabet de taille t et A un alphabet de taille k. Nous allons dans un premier temps construire une famille de circuits $(C^\mu_n)_{n\in\mathbb{N}}$ de $\mathbf{WLAC^0}$ sur l'alphabet A *calculant* le morphisme

μ. On rappelle qu'on encode chaque lettre de A par un mot de $\{0,1\}^k$ et chaque lettre de B par un mot de $\{0,1\}^t$. Ainsi, le $n^{\text{ème}}$ circuit (C_n^μ) dispose de tn entrées en binaires et kpn sorties. Ce circuit est réalisable simplement, car il suffit de relier correctement les sorties, étiquetée par des $\vee$, aux entrées. En particulier, il ne possède pas d'autres portes que ses entrées et ses sorties. il faut néanmoins prouver qu'il est bien dans $\mathbf{WLAC^0}$:
Soient $0 \leqslant i < tpn$ et $0 \leqslant r < qp$ et $0 \leqslant q < n$ tels que $i = qtp + r$. La $i^{\text{ème}}$ porte va participer à l'encodage de l'image de la $q^{\text{ème}}$ lettre du mot en entrée. Nous allons donc la raccorder uniquement aux portes d'entrée dont la numérotation est comprise entre qt et $(q+1)t$. Pour chaque porte de sortie, on introduit donc un nombre d'arêtes borné par t. Le nombre total d'arête de ce circuit est donc borné par $tkpn$. Ce circuit est bien dans $\mathbf{WLAC^0}$.
Finalement, nous allons construire une famille de circuits qui va calculer le langage $\mu^{-1}(L)$. Soit $u \in B^n$. Le mot u appartient à $\mu^{-1}(L)$ si et seulement si $\mu(u)$ appartient à L. Il suffit donc de réaliser son image par μ et d'appliquer le circuit C_{pn} au résultat. Le nombre d'arêtes ainsi introduits est le nombre d'arêtes du le circuit C_n^μ et le nombre d'arêtes du circuit C_{pn}. On construit bien un circuit de $\mathbf{WLAC^0}$. ■

Remarque : Ce lemme se généraliserais sans difficulté à toutes les classes de complexité que l'on a introduite. Cela sera prouvé, à l'aide des caractérisation logique de ces classes, dans la proposition 6.2. On remarque également que pour des morphismes qui ne sont pas multiplicatifs cette construction n'est pas réalisable.

Ainsi, la classe des langages réguliers de $\mathbf{WLAC^0}$ est une *mu*-variété de langages réguliers ne contenant ni les langages modulaires, ni le langage $c^*(ac^*bc^*)^*$. D'après la proposition 4.48, cette classe est donc incluse dans la *mu*-variété des langages définissables dans $\mathbf{FO}^2[\mathcal{R}\text{eg}]$.

Le sens contraire repose sur les constructions des *fonctions booléennes préfixes et suffixes* données dans l'article [17]. Pour chaque fonction $f : \{0,1\}^* \to \{0,1\}$ d'arité n, on définit les fonctions suivantes.

- La fonction préfixe-f,

$$\text{p-f} : \begin{cases} \{0,1\}^n \to \{0,1\}^n \\ (x_1,\dots,x_n) \mapsto (y_1,\dots,y_n) \end{cases} \qquad \text{avec } y_i = f(x_1,\dots,x_i).$$

- La fonction suffixe-f,

$$\text{s-f} : \begin{cases} \{0,1\}^n \to \{0,1\}^n \\ (x_1,\dots,x_n) \mapsto (y_1,\dots,y_n) \end{cases} \qquad \text{avec } y_i = f(x_i,\dots,x_n).$$

On s'intéresse uniquement aux fonctions préfixes et suffixes booléennes p-$\wedge$, s-$\wedge$, p-$\vee$ et s-$\vee$.

Proposition 5.15 (Chandra, Fortune et Lipton [17]).

Pour chaque fonction booléenne préfixe et suffixe, il existe un circuit de $\mathbf{WLAC^0}$ qui la réalise.

La preuve suivante est inspirée par les preuves des articles [39, Theorem 2] et [40, Lemma 16].

Proposition 5.16.

Soit $\varphi(x)$ une formule de $\mathbf{FO}^2[\mathcal{R}\mathrm{eg}]$. Pour tout entier n, il existe un circuit C_n de $\mathbf{WLAC^0}$, avec n portes de sortie $y_1, \ldots, y_n$ tel que pour tout mot u, u est accepté par la formule $\varphi(i)$ si et seulement si la porte y_i de C_n est évaluée à 1 avec u comme entrée.

Démonstration : Nous allons réaliser cette preuve par induction sur la structure de la formule. Nous allons prouver un résultat un peu plus difficile en montrant que les formules avec ou sans variable libre sont calculable par un circuit.

On rappelle q'un circuit C va calculer une formule $\varphi(x)$ sur les mots de tailles n s'il possède n portes de sorties $s_0, \ldots, s_{n-1}$ telles que pour tout mot $u \in A^n$ et tout entier $0 \leqslant j < n$, $u \models \varphi(j)$ si et seulement si la porte s_j du circuit C est évaluée à 1 sur entrée u.

Les cas de base, des prédicats de lettres et des prédicats numériques unaires, sont trivialement gérés. Le cas des prédicats d'arité supérieur sera, quant à lui, géré à l'aide de l'induction. En effet, nous allons voir qu'ils vont coder comment les portes sont reliées entre elles.

Dans un premier temps, remarquons que si deux formules, avec ou sans variable libre, vérifient l'hypothèse d'induction, alors leurs combinaisons booléennes la vérifient également. En effet, il suffit de reproduire les opérations booléennes avec les familles de circuits obtenues par l'hypothèse d'induction. Cela n'introduira qu'un nombre constant de portes et d'arêtes si les formules sont closes, et un nombre linéaire de portes et d'arêtes si elles ont une variable libre.

Il reste à traiter le cas des quantifications. Soit φ une formule sans variable libre de la forme $Qy\ \psi(y)$ où $\psi(y)$ vérifie l'hypothèse d'induction et $Q \in \{\exists, \forall\}$. Dans le cas où $Q = \forall$, il suffit d'ajouter une unique porte $\wedge$ reliée aux sorties du circuit obtenu pour $\psi(y)$ par l'hypothèse d'induction. De même dans le cas où $Q = \exists$, il suffit d'ajouter une unique porte $\vee$ reliée à ces mêmes sorties. De telles opérations n'introduisent qu'un nombre linéaire d'arêtes. Le circuit ainsi construit vérifie bien l'hypothèse d'induction.

Supposons que $\varphi(x) \equiv \exists y\ \psi(x, y)$. Nous allons réutiliser la forme normale présentée dans la preuve de la proposition 5.12 . On peut donc supposer, sans perte de généralité, que $\varphi(x) = \exists y\ \delta(x, y) \wedge \theta(y)$ avec $\delta(x, y)$ qui est une combinaison booléenne des prédicats de la forme $x \leqslant y$, $x = y + p$ pour $p \in \mathbb{N}$, et $\theta(y)$ qui vérifie l'hypothèse d'induction.

On note que tous les prédicats unaires (prédicats modulaires et prédicats de lettre) sont traités par l'hypothèse d'induction, il ne reste donc que les prédicats réguliers binaires à gérer. δ peut être vu comme une application $\mathbb{N}^2$ vers $\{0,1\}$ car tous les prédicats qui la compose sont *uniformes*.

Montrons maintenant l'hypothèse d'induction. Remarquons dans un premier temps qu'il existe un entier k et $(b^-, b^+) \in \{0,1\}^2$ tels que

- pour tout couple d'entiers (x,y) vérifiant $x < y - k$, $\delta(x,y) = b^-$,
- pour tout couple d'entiers (x,y) vérifiant $x > y + k$, $\delta(x,y) = b^+$.

En effet, chaque prédicat $x \leqslant y$ et $x = y + p$ pour $p \in \mathbb{N}$ vérifie cette propriété et elle est stable par combinaison booléenne.

D'après l'hypothèse d'induction, il existe un circuit C_n de $\mathbf{WLAC^0}$ et n portes de sortie $y_0, \ldots, y_{n-1}$ tels que pour tout mot u, u est accepté par la formule $\theta(i)$ si et seulement si la porte y_i de C_n est évaluée à 1 avec u comme entrée. On construit un nouveau circuit en ajoutant des portes et des arêtes afin de reconnaître la formule $\varphi(x)$. On ajoute n portes de sortie, que l'on nomme $o_0, \ldots, o_{n-1}$, étiquetées par $\vee$, au circuit C_n. D'après ce qui précède, il existe un entier k et $(b^-, b^+) \in \{0,1\}^2$ vérifiant que

- pour tout entier (x,y) vérifiant $x < y - k$, $\delta(x,y) = b^-$,
- pour tout entier (x,y) vérifiant $x > y + k$, $\delta(x,y) = b^+$.

Pour un entier $i \in \{0, \ldots, n-1\}$, et un entier j tels que $|i - j| \leqslant k$, on relie chaque porte o_i aux portes y_j telles que $\delta(i,j)$ est vérifiée. Pour chaque entier i, il existe au plus $2k$ portes j vérifiant ceci et donc nous avons introduit au plus $2kn$ nouvelles arêtes.

Si $b^- = b^+ = 0$, alors la construction est terminée. Supposons que $b^- = 1$. On compose alors le circuit C_n avec le circuit de $\mathbf{WLAC^0}$ de la fonction préfixe-$\vee$, on obtient alors un circuit, que l'on note $C_n^{\text{p-}\vee}$, qui est toujours dans $\mathbf{WLAC^0}$.

Notons ${y_0}^p, \ldots, {y_{n-1}}^p$ les portes de sortie de ce circuit. Pour un entier $i \in \{k+1, \ldots, n-1\}$, on relie o_i à la porte y^p_{i-k}. On remarque que si l'une des portes y_j est évaluée à 1 pour $i < j - k$, alors y^p_{i-k} sera également évaluée à 1 et donc la porte o_i également.

De même, si $b^+ = 1$, on compose le circuit C_n avec une fonction suffixe-$\vee$, et on obtient alors un circuit $C_n^{\text{s-}\vee}$, toujours dans $\mathbf{WLAC^0}$. Notons $y^s_0, \ldots, y^s_{n-1}$ les portes de sorties de ce circuit. On relie, pour un entier $i \in \{0, \ldots, n-1-k\}$, la porte o_i à la porte y^s_{i+k}. Le nombre de portes et le nombre d'arêtes sont toujours linéaires, ce qui conclut la preuve. ■

5.5 Questions ouvertes

Un certain nombre de conjectures ont été émises sur la complexité booléenne des langages réguliers. Nous allons en présenter deux.

Conjecture 5.17.

Il existe un langage régulier qui n'est pas définissable dans **ACC**.

Cette conjecture est équivalente à la séparation de **ACC** et de $\mathbf{NC^1}$ car les langages réguliers sont complets pour $\mathbf{NC^1}$. Ces résultats sont dus aux travaux de Barrington [9] et de Barrington et Thérien [12].

Nous l'avons vu, les classes $\mathbf{LAC^0}$ et $\mathbf{AC^0}$ sont séparées. Toutefois aucun séparateur régulier de ces classes n'est connu. Nous allons montrer par la suite que le langage $c^*(ac^*bc^*)^*$ est, comme évoqué dans les articles [40, 39], un séparateur potentiel de ces deux classes.

Conjecture 5.18.

Le langage $c^*(ac^*bc^*)^*$ n'appartient pas à $\mathbf{LAC^0}$.

Si cette conjecture est vraie, alors en particulier les langages réguliers de $\mathbf{LAC^0}$ sont exactement ceux de $\mathbf{WLAC^0}$ (voir théorème 5.13). On pose la *relation d'addition* définie par

$$\{x_1y_1z_1\cdots x_ny_nz_n \in \{0,1\}^{3n} \mid x,y,z \in \{0,1\}^n \text{ tels que } n_x + n_y = n_z\},$$

où n_x, n_y et n_z sont les entiers ayant les mots x, y et z comme représentations binaires (en prenant le bit de poids le plus faible à droite). Ce langage correspond au langage $d^*(ac^*bd^*)^*$ où la lettre b marque le début d'une propagation de retenue vers la gauche, la présence de la lettre c marque la retenue est correctement propagée et la lettre a marque la fin de la propagation. Plus précisément, on utilise l'application suivante :

$$\begin{cases} \{0,1\}^3 & \to \{a,b,c,d\} \\ 001 & \mapsto a \\ 110 & \mapsto b \\ 100, 010 & \mapsto c \\ 101, 011, 000 & \mapsto d \end{cases}$$

Le timbre syntaxique de ce langage appartient à **QLDA**, donc ce langage est définissable dans $\mathbf{FO}^2[\mathcal{R}\mathrm{eg}]$ et appartient à $\mathbf{WLAC^0}$.

La *fonction d'addition* est l'application $f : \{0,1\}^{2n} \to \{0,1\}^{n+1}$ telle que pour les mots $x, y \in \{0,1\}^n$, $f(x_0y_0\cdots x_{n-1}y_{n-1}) = z_0\cdots z_n$ est la représentation binaire de l'addition de n_x et n_y. Cette fonction est réalisable dans $\mathbf{AC^0}$ et il est conjecturé qu'elle n'est pas faisable dans $\mathbf{LAC^0}$. Comme le montre la proposition suivante, cette question est reliée fortement à la conjecture 5.18.

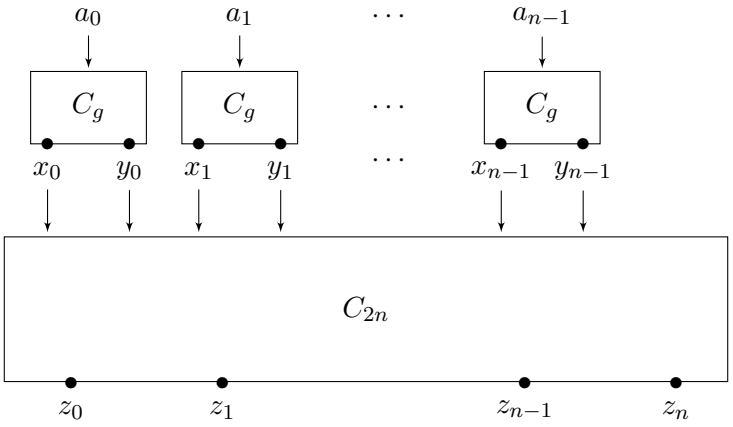
Proposition 5.19.

Si la fonction d'addition appartient à $\mathbf{LAC^0}$, alors le langage $c^*(ac^*bc^*)^*$ appartient également à $\mathbf{LAC^0}$.

Démonstration : Supposons que la fonction d'addition appartient à $\mathbf{LAC^0}$, et notons $(C_n)_{n\in\mathbb{N}}$ la famille de circuit de $\mathbf{LAC^0}$ qui la réalise. Posons la fonction suivante

$$g : \begin{cases} \{a,b,c\} & \to \{0,1\}^2 \\ a & \mapsto 00 \\ b & \mapsto 11 \\ c & \mapsto 10 \end{cases}$$

et notons C_g le circuit qui la calcule. Nous réalisons alors la construction suivante :



Notons $(C'_n)_{n\in\mathbb{N}}$ la famille de circuits ainsi construite. Par hypothèse, il existe un entier $0 \leqslant k$ tel la taille de C_n est bornée par kn et un entier $0 \leqslant p$ tel que la taille de C_g est au plus p. La famille de circuits $(C'_n)_{n\in\mathbb{N}}$ est dans $\mathbf{LAC^0}$ puisque C'_n a une taille au plus $(p+2k)n$. ■

La proposition suivante illustre la difficulté de prouver cette conjecture.

Notation : On pose $g_0(n) = n^{\frac{1}{4}}$, et pour $d \geqslant 0$:

$$g_{d+1} : \begin{cases} \mathbb{N} \to \mathbb{N} \\ n \mapsto \min\{i \mid g_d^{(i)}(n) \leqslant 1\} \end{cases}$$

avec $g_d^{(i)}$ la fonction g_d composée par elle-même i fois.

Théorème 5.20 (Chandra, Fortune et Lipton [18], Kouckỳ [38]).

Soit L un langage régulier de $\mathbf{AC^0}$ et d un entier. Le langage L est calculable par un circuit de $\mathbf{AC^0}$ de profondeur d et de taille bornée par $Kng_d(n)^2$ avec $K \in \mathbb{N}$.

Enfin, comme le montre l'application de la section 2.3.1, le langage $(ab)^*$ et donc le langage $c^*(ac^*bc^*)^*$, sont définissables dans $(\mathbf{FO} + \mathbf{MOD})^2[<]$. De fait, ils appartiennent à **LACC**. On conjecture néanmoins le résultat suivant.

Conjecture 5.21.

Soit $A = \{a, b, c\}$. Le langage $A^*ac^*aA^*$ n'est pas définissable dans **LACC**.

Remarque : Comme le langage $A^*ac^*aA^*$ est définissable dans $\mathbf{AC^0}$, cette conjecture fournirait un témoin régulier de la séparation des classes $\mathbf{LAC^0}$ et de $\mathbf{AC^0}$ mais ne permettrait pas de caractériser les langages réguliers de $\mathbf{LAC^0}$.

Chapitre 6

Conjecture de Straubing

et la propriété de Crane-Beach

Dans le livre [66], Straubing a conjecturé que tout langage régulier définissable dans un fragment de **MSO** à l'aide de prédicats numériques arbitraires, devrait être définissable à l'aide de prédicats numériques réguliers uniquement. Cette conjecture a été formulée pour certains fragments dont $(\mathbf{FO} + \mathbf{MOD})[\mathcal{A}\mathrm{rb}]$ et $\mathcal{B}\mathbf{\Sigma}_k[\mathcal{A}\mathrm{rb}]$ et nous la généralisons à tout fragment.

Conjecture 6.1 (Straubing [66]).

Soit $\mathbf{F}$ un fragment de **MSO**, et $\mathcal{C}$ une classe de prédicats numériques. Les langages réguliers définissables dans $\mathbf{F}[\mathcal{C}]$ sont définissables dans $\mathbf{F}[\mathcal{R}\mathrm{eg}]$.

Pour $\mathbf{F} = (\mathbf{FO} + \mathbf{MOD})$, il s'agit d'une reformulation logique de la conjecture de séparation de **ACC** et de $\mathbf{NC^1}$ (voir conjecture 5.17). Nous allons voir que c'est également le cas pour $\mathbf{FO}^2$ et la conjecture établissant que langage $c^*(ac^*bc^*)^*$ n'appartient pas à $\mathbf{LAC^0}$ (voir conjecture 5.18). La conjecture de Straubing justifie également le choix du langage séparateur de la conjecture établissant que le langage $A^*ac^*aA^*$ n'est pas dans **LACC** (voir conjecture 5.21). En effet, ce langage $A^*ac^*aA^*$ n'est pas définissable dans $(\mathbf{FO} + \mathbf{MOD})^2[\mathcal{R}\mathrm{eg}]$.

La conjecture de Straubing est donc une question difficile quand on la considère sur la classe des prédicats arbitraires. Nous allons néanmoins en prouver certaines instances en restreignant la classe des prédicats. Les preuves que nous proposons pour les cas particuliers de ces conjectures se décomposent en trois étapes distinctes :

(1) Caractériser algébriquement le fragment logique équipée de prédicats réguliers.
(2) En déduire certains langages *témoins* caractérisant, par leur absence, la classe de langages réguliers que l'on étudie.
(3) Prouver des bornes inférieures pour ces langages témoins.

Pour les deux premières étapes, il est utile que la classe de prédicats considérée vérifie certaines hypothèses de stabilité que nous allons introduire maintenant. Les classes de langages ainsi définies seront stables par quotient et morphisme inverse multiplicatifs.

Une classe de prédicats numériques $\mathcal{C}$ est dite *stable multiplicativement* (où *mu*-stable) si elle est stable par les opérations suivantes :

- Projection d'une composante : si le prédicat (P_n) d'arité k est dans $\mathcal{C}$ et $1 \leqslant i \leqslant k$ et en définissant

$$Q_n = \{(x_1, \ldots, x_{k-1}) \in [n] \mid (x_1, \ldots x_{i-1}, 0, x_i, \ldots, x_{k-1}) \in P_{n+1}\},$$

  alors le prédicat (Q_n) est également dans $\mathcal{C}$.
- Addition par une constante : si le prédicat (P_n) d'arité k est dans $\mathcal{C}$, en posant $p \in \mathbb{N}$, ainsi que

$$Q_n = \{(x_1, \ldots, x_k) \in [n] \mid (x_1 + p, \ldots, x_k + p) \in P_{n+p}\},$$

  alors le prédicat (Q_n) est également dans $\mathcal{C}$.
- Multiplication par une constante : si le prédicat (P_n) d'arité k est dans $\mathcal{C}$, en posant $p \in \mathbb{N}$ et $t_1, \ldots, t_k$ des entiers strictement plus petits que p, ainsi que

$$Q_n = \{(x_1, \ldots, x_k) \in [n] \mid (px_1 + t_1, \ldots, px_k + t_k) \in P_{pn}\},$$

  alors le prédicat (Q_n) est également dans $\mathcal{C}$.

Exemples : Voici quelques exemples de classes de prédicats *mu*-stables :

- La classe de tous les prédicats numériques $\mathcal{A}\mathrm{rb}$.
- La classe des prédicats numériques au plus unaires $\mathcal{A}\mathrm{rb}_1$.
- La classe des prédicats réguliers $\mathcal{R}\mathrm{eg}$.

Nous allons justifier le choix de la notation *mu*-stable en montrant qu'un fragment logique du premier ordre équipé d'une classe de prédicats *mu*-stable est stable par quotient et morphisme inverse multiplicatif. Ainsi, la classe des langages réguliers qui y sont définissables forme une *mu*-variété de langages. Cela va nous permettre d'utiliser les outils algébriques introduits dans la première partie de cette thèse.

Proposition 6.2.

Soit $\mathbf{F}$ un fragment du premier ordre et $\mathcal{C}$ une classe de prédicats *mu*-stable. La classe des langages réguliers définissables dans $\mathbf{F}[\mathcal{C}]$ est stable par quotient et par morphisme inverse multiplicatif.

Démonstration : Soit L un langage régulier de A^* et φ sa formule de $\mathbf{F}[\mathcal{C}]$.

- Pour la stabilité par quotient, il suffit de le faire pour une lettre à gauche (le quotient à droite est traité par la construction symétrique). Nous allons *simuler* la présence de la lettre a et *décaler* les autres positions en étiquetant les symboles de variables. Ainsi, pour x une variable du premier ordre, on notera x^{+1} la variable dont la valeur est translatée d'une position à droite et $x^{=0}$ la variable dont la valeur est 0. Ces informations seront *éliminées* une fois arrivées aux atomes. On obtiendra ainsi une formule classique, sans étiquetages supplémentaires. Chaque quantification existentielle et universelle du premier ordre est traitée ainsi :

$$\forall x\ \psi(x) \rightsquigarrow (\forall x\ \psi(x^{+1})) \wedge \psi(x^{=0})$$
$$\exists x\ \psi(x) \rightsquigarrow (\exists x\ \psi(x^{+1})) \vee \psi(x^{=0})$$

  Pour chaque lettre $b \in A$, on remplace $\mathbf{b}(x^{+1})$ par $\mathbf{b}(x)$ et $\mathbf{b}(x^{=0})$ par la formule *vrai* si et seulement si $b = a$. Pour un prédicat numérique P, on va remplacer $P(x_1^{\ell_1}, \ldots, x_k^{\ell_k})$ par un prédicat Q mais certaines variables sont assignées à 0, nous allons devoir les *instancier*. On pose $i_1 < \ldots < i_t$ les indices tels que $\ell_1 = +1$. On remplace alors $P(x_1^{\ell_1}, \ldots, x_k^{\ell_k})$ par le prédicat $Q(x_{i_1}, \ldots, x_{i_t})$ avec i_1 le premier indice tel que $\ell_{i_1} = +1$, i_2 le second et ainsi de suite et avec

$$Q_n = \{(x_1, \ldots, x_t) \in [n]^t \mid (0, \ldots 0 \underbrace{x_1 + 1}_{\text{indice } i_1} 0, \ldots, 0 \underbrace{x_t + 1}_{\text{indice } i_t}, 0 \ldots, 0) \in P_{n+1}\}$$

- Traitons le cas de la stabilité par morphisme inverse. Prenons un morphisme multiplicatif $\mu : B^* \to A^*$ ainsi qu'un entier p tels que $\mu(B) \subseteq A^p$. Comme pour le point précédent nous allons ajouter des informations sur les variables qui seront ensuite éliminées sur les atomes. Ainsi, pour x une variable du premier ordre, on notera x^t la variable encodant la position $px+t$ (avec $t < p$). Chaque quantification existentielle et universelle du premier ordre est traitée ainsi :

$$\forall x\ \psi(x) \rightsquigarrow \forall x \bigwedge_{t=0}^{p-1} \psi(x^t)$$
$$\exists x\ \psi(x) \rightsquigarrow \exists x \bigvee_{t=0}^{p-1} \psi(x^t)$$

  On remplace chaque prédicat $\mathbf{a}(x^t)$ avec a une lettre de A, par

$$\bigvee_{b \mid \mu(b)_t = a} \mathbf{b}(x)$$

  où $\mu(b)_t$ la $t^{\text{ème}}$ lettre de $\mu(b)$. On remplace également le prédicat $P(x_1^{t_1}, \ldots, x_k^{t_k})$ par le prédicat $Q(x_1, \ldots, x_k)$ avec

$$Q_n = \{(x_1, \ldots, x_k) \in [n] \mid (px_1 + t_1, \ldots, px_k + t_k) \in P_{pn}\}.$$

Quitte à factoriser les conjonctions et disjonctions afin de les mettre à l'extérieur de la formule, on obtient bien des formules de $\mathbf{F}$, puisque $\mathbf{F}$ est un fragment (stable par $\wedge$ et $\vee$

et par substitution atomique). Comme la classe de prédicats est *mu*-stable, en particulier les nouveaux atomes introduits sont bien dans la signature. Ce qui conclut la preuve. ■

Nous avions évoqué après la preuve du lemme 5.14, que les autres classes de circuits étaient également stables par opération booléenne, par morphisme inverse multiplicatif et par quotient. Cette proposition fournit une preuve de ceci, puisqu'il suffit de considérer les fragments logiques équivalents équipés de la classe *mu*-stable $\mathcal{A}\text{rb}$. Il est maintenant possible en utilisant des résultats de bornes inférieures et les descriptions algébriques de la première partie de prouver des cas particuliers de la conjecture Straubing.

Nous rappelons que l'objectif de cette thèse est de caractériser la complexité booléenne des langages réguliers. Le résultat suivant, prouvé par Barrington, Compton, Straubing et Thérien (voir l'article [10]) caractérise exactement les langages réguliers de $\mathbf{AC^0}$. En effet, comme nous l'avons vu $\mathbf{FO}[\mathcal{A}\text{rb}]$ est équivalent à $\mathbf{AC^0}$. On remarquera également qu'il s'agit d'une instance de la conjecture de Straubing.

Théorème 6.3 (Barrington, Compton, Straubing et Thérien [10]).

Les langages réguliers définissables dans $\mathbf{FO}[\mathcal{A}\text{rb}]$ sont exactement les langages réguliers de $\mathbf{FO}[\mathcal{R}\text{eg}]$.

Démonstration : D'après la proposition 4.46, la *mu*-variété des langages définissables dans $\mathbf{FO}[\mathcal{R}\text{eg}]$ est la plus grosse *mu*-variété de langages ne contenant pas les langages modulaires. D'après le théorème 5.5, les langages modulaires ne sont pas définissables dans $\mathbf{FO}[\mathcal{A}\text{rb}]$, et d'après la proposition 6.2, la classe des langages réguliers définissables dans $\mathbf{FO}[\mathcal{A}\text{rb}]$ est une *mu*-variété. Les langages réguliers de $\mathbf{FO}[\mathcal{A}\text{rb}]$ appartiennent donc à $\mathbf{FO}[\mathcal{R}\text{eg}]$. La réciproque est triviale car $\mathcal{R}\text{eg} \subsetneq \mathcal{A}\text{rb}$. ■

Dans le cas de $\mathbf{LAC^0}$, le manque de borne inférieure nous empêche d'établir de tels résultats. Toutefois, grâce aux résultats algébriques de la première partie, nous allons montrer que la conjecture 5.18 implique la conjecture de Straubing pour $\mathbf{FO}^2[\mathcal{A}\text{rb}]$.

Proposition 6.4.

Si le langage $c^*(ac^*bc^*)^*$ n'est pas définissable dans $\mathbf{FO}^2[\mathcal{A}\text{rb}]$, alors les langages réguliers définissables dans $\mathbf{FO}^2[\mathcal{A}\text{rb}]$ sont exactement ceux définissables dans $\mathbf{FO}^2[\mathcal{R}\text{eg}]$.

Démonstration : D'après la proposition 4.48, la *mu*-variété des langages définissables dans $\mathbf{FO}^2[\mathcal{R}\text{eg}]$ est l'unique *mu*-variété de langages ne contenant pas les langages modulaires, ne contenant pas le langage $c^*(ac^*bc^*)^*$ et contenant $\mathbf{FO}^2[\mathcal{R}\text{eg}]$. D'après la proposition 6.2, la classe des langages réguliers définissables dans $\mathbf{FO}^2[\mathcal{A}\text{rb}]$ est une *mu*-variété. Si $c^*(ac^*bc^*)^*$ n'est pas définissable dans $\mathbf{FO}^2[\mathcal{A}\text{rb}]$, alors la *mu*-variété des langages réguliers définissables dans $\mathbf{FO}[\mathcal{A}\text{rb}]$ est exactement $\mathbf{FO}^2[\mathcal{R}\text{eg}]$. ■

On remarquera que la conjecture de Straubing pour $\mathbf{FO}^2[\mathcal{A}\mathrm{rb}]$ implique également la conjecture 5.18. En effet, le langage $c^*(ac^*bc^*)^*$ n'est pas définissable dans $\mathbf{FO}^2[\mathcal{R}\mathrm{eg}]$. Ces deux conjectures sont donc équivalentes.

Corollaire 6.5.

Le langage $c^*(ac^*bc^*)^*$ n'est pas définissable dans $\mathbf{FO}^2[\mathcal{A}\mathrm{rb}]$ si et seulement si $\mathbf{FO}^2[\mathcal{A}\mathrm{rb}]$ vérifie la conjecture de Straubing.

On rappelle qu'un langage régulier a une lettre neutre s'il existe une lettre syntaxiquement équivalente au mot vide. La plupart des langages réguliers qui nous intéressent pour séparer des classes de complexité, ont la propriété de posséder une lettre neutre.

Exemples :

- Les langages modulaires ont une lettre neutre.
- Le langage $c^*(ac^*bc^*)^*$ a une lettre neutre (la lettre c).
- Le langage $A^*ac^*aA^*$, où $A = \{a, b, c\}$, a une lettre neutre (la lettre c)

Il serait donc intéressant d'obtenir des bornes inférieurs pour les langages à lettre neutre. Cela pourrait être utile afin de prouver les conjectures de Straubing.

Ainsi il a été conjecturé que les langages à lettre neutre de $\mathbf{FO}[\mathcal{A}\mathrm{rb}]$ étaient réguliers et leur monoïde syntaxique apériodique. L'objectif était alors de reprouver le théorème 5.4 en utilisant des outils logiques. Ceci est malheureusement faux, comme le montre le théorème suivant.

Théorème 6.6 (Barrington *et al.* [11]).

Il existe un langage à lettre neutre non régulier définissable dans $\mathbf{FO}[+, \times]$.

La *propriété de Crane Beach* est une généralisation de la conjecture précédente. Bien que fausse pour $\mathbf{FO}[\mathcal{A}\mathrm{rb}]$, elle pourrait permettre de mieux comprendre certains fragments plus faibles, comme $\mathbf{FO}^2[\mathcal{A}\mathrm{rb}]$.

Définition 6.7 (Propriété de Crane Beach).

Un couple $(\mathbf{F}, \mathcal{P})$, où $\mathbf{F}$ est un fragment et $\mathcal{P}$ une classe de prédicats numériques, vérifie la propriété de Crane Beach si tout langage à lettre neutre définissable dans $\mathbf{F}[\mathcal{P}]$ est définissable dans $\mathbf{F}$.

Notation : Soient $\mathbf{F}$ un fragment et $\mathcal{P}$ une classe de prédicats numériques. On dira que le fragment $\mathbf{F}[\mathcal{P}]$ vérifie la propriété de Crane Beach si le couple $(\mathbf{F}, \mathcal{P})$ vérifie la propriété de Crane Beach.

Le nom *Crane Beach* provient de l'endroit où la conjecture, réfutée par le théorème 6.6, a été énoncée.

Prouver que $\mathbf{FO}^2[\mathcal{A}\mathrm{rb}]$ possède la propriété de Crane Beach montre, grâce à la proposition 6.4 que $\mathbf{FO}^2[\mathcal{A}\mathrm{rb}]$ vérifie la conjecture de Straubing. Le contre-exemple utilisé dans la preuve du théorème 6.6 ne semble pas être définissable dans $\mathbf{FO}^2[\mathcal{A}\mathrm{rb}]$, ce qui peut laisser espérer que la propriété de Crane Beach est vraie pour $\mathbf{FO}^2[\mathcal{A}\mathrm{rb}]$. On peut noter que la propriété de Crane Beach et la conjecture de Straubing établissent que les prédicats supplémentaires numériques ne sont pas réellement *utiles* pour définir des langages réguliers. La proposition suivante établit la propriété de Crane beach pour les prédicats réguliers, en utilisant les résultats de la première partie de cette thèse.

Proposition 6.8.

Soit $\mathbf{F}$ un fragment équivalent à une variété de langages $\mathbf{V}$ tel que $\mathbf{F}[\mathcal{R}\mathrm{eg}]$ est équivalent à $\mathbf{F}[\mathrm{MOD}, \mathrm{LOC_D}]$. Le fragment $\mathbf{F}[\mathcal{R}\mathrm{eg}]$ vérifie la propriété de Crane Beach.

Démonstration : D'après la proposition 6.2, la classe des langages définissables dans $\mathbf{F}[\mathcal{R}\mathrm{eg}]$ est la *mu*-variété de langages $\mathbf{V} * \mathbf{D} * \mathbf{MOD}$. Or nous avons vu dans les corollaires 3.32 et 4.29 que $\mathbf{V} * \mathbf{D} * \mathbf{MOD} \subseteq \mathbf{QLV}$. De plus, d'après les mêmes corollaires, si un langage à lettre neutre est dans $\mathbf{QLV}$, alors il est dans $\mathbf{V}$. Il est donc définissable dans $\mathbf{F}$. ■

Prouver que la propriété de Crane Beach est satisfaite est une question difficile, et peu de méthodes de preuves sont connues. Nous allons présenter deux approches nouvelles à ces questions. La première va utiliser les jeux d'Ehrenfeucht-Fraïssé ainsi que le théorème de Ramsey alors que la seconde utilise des arguments simples de théories des automates. La fin de ce chapitre est dédiée à ces deux exemples.

(1) Nous allons étudier la propriété de Crane Beach pour $\mathbf{FO}^2$ équipé des prédicats de degré fini. En particulier nous allons prouver que cette propriété est satisfaite pour chaque niveau de la hiérarchie d'alternance de $\mathbf{FO}^2$.

(2) Nous allons prouver la propriété de Crane Beach pour $\mathbf{MSO}$ équipé de prédicats unaires.

6.1 Les prédicats de degré fini

Nous allons maintenant étudier la propriété de Crane Beach dans le cas particulier de $\mathbf{FO}^2$ équipé de prédicats numériques de degré fini et en déduire une preuve de la conjecture de Straubing dans ce cas particulier. Dans la suite de cette partie, nous allons emprunter au vocabulaire de la théorie des graphes afin d'exprimer des propriétés sur la *structure* des prédicats numériques. En effet, un prédicat numérique binaire peut être vu comme une suite de graphes. Si, de plus, le prédicat est uniforme, il s'agit en fait d'un graphe sur les entiers.

Notations : Soient $P = (P_n)$ un prédicat numérique binaire et t un entier. Le *degré relativement à t* d'une position $k \leqslant t$ pour P, noté $d_P(k,t)$, est la taille de l'ensemble des positions *reliées* à k via P_t. Formellement,

$$d_P(k,t) = |\{j \mid (k,j) \in P_t \text{ ou } (j,k) \in P_t\}|.$$

Si le prédicat est uniforme, alors on parle de *degré* d'une position $k \in \mathbb{N}$, défini par

$$d_P(k) = |\{j \mid (k,j) \in P \text{ ou } (j,k) \in P\}|.$$

La notion de *localité* est l'un des outils les plus efficaces pour utiliser les jeux d'Ehrenfeucht-Fraïssé. Une des manières d'introduire de la localité est de restreindre le degré de la signature.

Définition 6.9 (Prédicats numériques de degré fini).

Un prédicat uniforme binaire P est de degré fini si toute position est de degré fini.

Notation : On note $\mathcal{F}$ la classe des prédicats de degré fini.

Remarque : Il s'agit d'une classe de prédicats *mu*-stable.

Exemples :

- Les prédicats locaux LOC sont de degré fini.
- Pour toute fonction croissante $f : \mathbb{N} \to \mathbb{N}$, le graphe de f est de degré fini (et même borné). Si pour toute position x on a $f(x) \geqslant x$, alors le prédicat défini par

  $$P = \{(x,y) \mid x \leqslant y \leqslant f(x)\}\}$$

  est de degré fini mais non borné.

Co-exemples :

- L'ordre n'est pas un prédicat de degré fini.
- Le prédicat BIT n'est pas de degré fini.

Les prédicats de degré fini ne contiennent pas les prédicats unaires. Toutefois, tout prédicat unaire uniforme peut s'encoder comme un prédicat de degré fini. En effet, si on pose P, un prédicat uniforme unaire, alors $Q = \{(x,x) \mid P(x)\}$ est un prédicat de degré fini. Dans la suite on supposera que la classe $\mathcal{F}$ contient les prédicats unaires uniformes, quitte à les encoder à l'aide de prédicats de degré fini. La *localité* est un outil efficace permettant d'obtenir de nombreux résultats de non-définissabilité à l'aide de jeux d'Ehrenfeucht-Fraïssé. Dès que l'ordre est présent dans la signature, il n'est malheureusement plus possible d'utiliser des résultats de localité et l'absence de l'ordre rend le fragment peu expressif. Nous allons voir maintenant qu'il est possible d'ajouter l'ordre tout en conservant une *forme de localité* dans le cas ou les autres prédicats sont de degré fini. On rappelle que $\mathbf{FO}^2_m$ est le fragment des formules de $\mathbf{FO}^2$ alternant au plus m fois entre des quantifications existentielles et universelles.

Théorème 6.10.

Soit m un entier. Le fragment $\mathbf{FO}^2_m[<, \mathcal{F}]$ vérifie la propriété de Crane Beach.

Ce théorème établit que les prédicats numériques ne sont pas utiles pour définir des formules des langages réguliers à l'aide de formules de $\mathbf{FO}^2$ et plus précisément, qu'ils ne permettent même pas d'améliorer la complexité fine du langage. De ce résultat, on déduit directement que le fragment $\mathbf{FO}^2[<, \mathcal{F}]$ vérifie la propriété de Crane Beach et grâce à la proposition 4.48, du fait que $\mathcal{F}$ soit une classe mu-stable et de la proposition 6.2, qu'il vérifie également la conjecture de Straubing.

Corollaire 6.11.

Le fragment $\mathbf{FO}^2[<, \mathcal{F}]$ vérifie la conjecture de Straubing.

De ce théorème, on déduit également que la hiérarchie $\mathbf{FO}_m[<, \mathcal{F}]$ est séparée.

Corollaire 6.12.

Pour tout entier m, il existe un langage dans $\mathbf{FO}^2_{m+1}[<, \mathcal{F}]$ qui n'est pas définissable dans $\mathbf{FO}^2_m[<, \mathcal{F}]$.

Démonstration : D'après le corollaire 2.26, il existe un langage régulier L sur un alphabet A définissable dans $\mathbf{FO}^2_{k+1}[<]$ qui n'est pas définissable dans $\mathbf{FO}^2_k[<, \mathcal{F}]$. Soit c une lettre qui n'appartient pas à A et posons $B = A \cup \{c\}$. On définit le morphisme $\psi : B^* \to A^*$ en posant $\psi(a) = a$ pour $a \in A$ et $\psi(c) = 1$. Le langage $\psi^{-1}(L)$ est également définissable dans $\mathbf{FO}^2_{k+1}[<]$ et n'est pas définissable dans $\mathbf{FO}^2_k[<]$. Comme c est une lettre neutre, il n'est pas définissable dans $\mathbf{FO}^2_k[<, \mathcal{F}]$. ■

6.1.1 Préliminaire à la preuve du théorème 6.10

Résumons la preuve du théorème 6.10. Les ingrédients principaux sont une *notion de localité*, les jeux d'Ehrenfeucht-Fraïssé et le théorème de Ramsey.

Notation : On fixe pour la suite de la preuve $P^1, \ldots, P^t$ des prédicats de $\mathcal{F}$.

L'objectif est de prouver que pour tout langage L avec une lettre neutre définissable dans $\mathbf{FO}^2_m[<, P^1, \ldots P^t]$, tout entier s et tous mots $u \in L$ et $v \notin L$, Spoiler a une stratégie gagnante pour le jeu à deux jetons, à s tours et m alternances sur (u, v) et la signature $\{<, +1\}$. La preuve se décompose comme suit.

(1) D'abord, nous introduisons la notion de *voisinage d'une position.*

(2) Puis, nous définissons une relation d'équivalence sur les triplets de voisinages disjoints qui va nous permettre d'identifier les différents rôles que peuvent prendre ces triplets durant le jeu.
(3) À l'aide du théorème de Ramsey sur les 3-hypergraphes, on extrait des triplets de positions dits *bien typées*.
(4) Enfin on construit par induction une stratégie gagnante pour Spoiler sur la signature $\{<, +1\}$. La proposition 6.8 permet alors de conclure.

Soit E défini par $\{x, y\} \in E$ si et seulement si x et y sont deux positions reliées par l'un des prédicats. Plus précisément, $\{x, y\} \in E$ si et seulement si $P^1(x, y) \vee P^1(y, x) \vee \cdots \vee P^t(x, y) \vee P^t(y, x)$. Le graphe $(\mathbb{N}, E)$ est le graphe support de notre raisonnement. Comme chaque prédicat est de degré fini, le graphe $(\mathbb{N}, E)$ est également de degré fini. À partir de maintenant on considère que : l'entier s (le nombre de tours dans le jeux) est fixé.

Définition de voisinage.

Nous allons introduire une notion de voisinage adaptée à notre problème. Avant cela, on introduit la notation suivante, qui nous sera utile.

Notation : Soit F un ensemble fini d'entiers. On note $\mathrm{Cl}(F)$ l'ensemble des éléments compris entre la position minimale et la position maximale de F, c'est-à-dire dans le plus petit intervalle contenant F :

$$\mathrm{Cl}(F) = \{\min F, \min F + 1 \ldots, \max F\}.$$

La notion de voisinage doit capturer l'idée que deux points dont les voisinages ne s'intersectent pas vont être suffisamment *éloignés* pour qu'il soit impossible d'utiliser l'information apportée par les prédicats supplémentaires. Pour chaque entier i, l'ensemble des entiers dans le 0-*voisinage* de de i est défini par

$$V(i, 0) = \mathrm{Cl}(\{i\} \cup \bigcup_{\substack{k' \leqslant i \leqslant k \\ \{k', k\} \in E}} \{k', k\}).$$

On étend cette définition par induction :

$$V(i, r + 1) = \mathrm{Cl}(\bigcup_{j \in V(i,0)} V(j, r)).$$

La figure 6.1 donne une représentation de la construction de ces ensembles.

Remarques : Moins formellement, le 0-voisinage de i est l'ensemble des positions j tel qu'en déplaçant un jeton il soit possible d'atteindre i ou d'encadrer i. On remarque également que, par une induction immédiate, $V(i, r) \subseteq V(i, r + 1)$.

Nous allons montrer dans un premier temps que les k-voisinages sont tous finis.

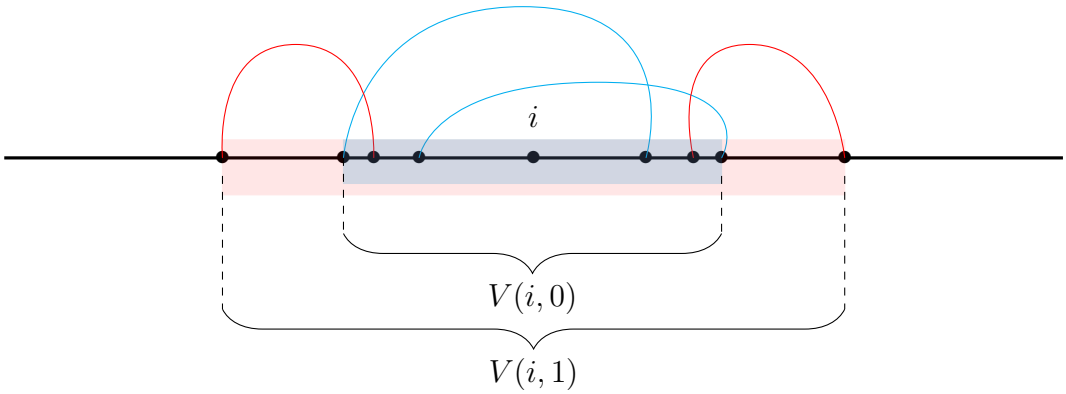


FIGURE 6.1 – Construction des voisinages.

Lemme 6.13.

Pour tout entier i et k, $V(i,k)$ est un segment fini d'entiers.

Démonstration : Nous allons montrer le résultat par induction sur k. Pour j un entier, on note dans la suite de cette preuve E_j l'ensemble des voisins de j pour le graphe $(\mathbb{N}, E)$. On remarque également que pour P un ensemble fini, $\mathrm{Cl}(P)$ est également un ensemble fini.

- Montrons que le 0-voisinage de i est fini. Pour tout $0 \leqslant j \leqslant i$, l'ensemble E_j est fini et on pose
$$m = \max \bigcup_{j=0}^{i} E_j.$$
Alors le 0-voisinage de i est inclus dans le segment $\{0, \ldots, m\}$ qui est fini.
- On suppose que pour tout j le r-voisinage de j est fini et on montre que le $(r+1)$-voisinage de i est également fini. Par définition
$$V(i, r+1) = \mathrm{Cl}(\bigcup_{j \in V(i,0)} V(j,r)).$$
Or par hypothèse d'induction $V(i,0)$ et $V(j,r)$ sont des ensembles finis. L'ensemble
$$E = \bigcup_{j \in V(i,0)} V(j,r)$$
est une union finie d'ensembles finis, il est donc fini. Donc $V(i,r+1) = \mathrm{Cl}(E)$ est fini. ■

Enfin, le lemme suivant va nous être également utile pour la suite.

Lemme 6.14.

Soient r, i et j des entiers. Nous avons $j \in V(i,r)$ si et seulement si $i \in V(j,r)$.

Démonstration : Par symétrie, il est suffisant de montrer que si $j \in V(i,r)$, alors $i \in V(j,r)$. On montre le résultat par induction sur r.

- Supposons que $j \in V(i,0)$. Par définition, il existe $k \leqslant i \leqslant k'$ tels que $k \leqslant j \leqslant k'$ et $k, k' \in E$ et donc, par définition $i \in V(j,0)$.
- Supposons que le résultat est vrai pour r. Nous allons le montrer pour $r+1$. Soit $j \in V(i,r+1)$. Si $j \in V(i,r)$, alors d'après l'hypothèse d'induction, $i \in V(j,r)$ et donc $j \in V(i,r+1)$. Dans le cas contraire, il existe $k \in V(i,r)$ et k' tels que $k, k' \in E$ et soit $k' \leqslant j \leqslant k$ soit $k \leqslant j \leqslant k'$. L'autre cas étant symétrique, supposons que $k' \leqslant j \leqslant k$. En utilisant l'hypothèse d'induction on obtient que $i \in V(k,r)$. Or $k \in V(j,0)$ et donc $i \in V(j,r+1)$. ■

On définit la fonction $g_s : \mathbb{N} \to \mathbb{N}$ par $g_s(i) = \min V(i,s)$ pour i un entier.

Lemme 6.15.

On a $\lim_i g_s(i) = +\infty$.

Démonstration : Supposons par l'absurde qu'il existe $M \in \mathbb{N}$ et $I \subseteq \mathbb{N}$ de taille infinie tels que pour tout entier $i \in I$, $g_s(i) \leqslant M$. Comme l'ensemble I n'est pas fini, il existe un entier $n \leqslant M$ et un ensemble $I' \subseteq I$ de taille infinie tels que pour tout entier $i \in I'$, on a $g_s(i) = n$. D'après le lemme 6.14, $I' \subseteq V(n,s)$, or I' est infini et $V(n,s)$ est un ensemble fini d'après le lemme 6.13. Ce qui conclut la preuve. ■

On en déduit immédiatement le corollaire suivant qui établit qu'il est possible d'obtenir un nombre arbitrairement grand de positions dont les voisinages sont disjoints.

Corollaire 6.16.

Pour tout entier p, il existe $X \subseteq \mathbb{N}$ de taille p tel que pour tout $i, j \in X$ les s-voisinages de i et j sont disjoints et il existe au moins un élément entre eux.

Notation : On appelle une *s-extraction* un sous-ensemble des entiers tels que leur s-voisinages soient disjoints et séparés par au moins un entier ; c'est-à-dire vérifiant les conditions du corollaire 6.16.

Les positions données par le corollaire sont distantes et isolées les unes des autres. L'objectif est donc d'y mettre les lettres non neutres (l'information pertinente). Toutefois, la présence de l'ordre complique ceci. C'est pourquoi nous allons devoir introduire une notion de *type* adaptée à ce contexte et donc l'objectif est de gérer l'interaction de l'ordre et des prédicats de degrés finis.

Une relation d'équivalence sur les triplets.

Nous allons maintenant essayer de quantifier la *ressemblance* des voisinages et des ensembles entre eux pour le jeu à deux jetons. La difficulté de cette notion de ressemblance que nous allons introduire provient des interactions possibles entre les prédicats supplémentaires et l'ordre. Introduisons quelques notations supplémentaires.

Soit (i_-, i, i_+) un triplet d'entiers qui est une s-extraction. Plus précisément, ce triplet vérifie que :

- $i_- < i < i_+$,
- leur s-voisinage sont disjoints et il existe au moins une position entre eux.

D'après le corollaire 6.16, un tel triplet existe. On pose $J_s(i, i_+)$ l'intervalle entre la position minimale du s-voisinage de i et la position minimale du s-voisinage de i_+. Plus formellement

$$J_s(i, i_+) = \{\min V(i, s), \ldots, \min V(i_+, s) - 1\}.$$

On pose $I_{(r,s)}(i_-, i_+)$ l'intervalle entre la position maximale du $(s-r)$-voisinage de i_- et la position minimale du $(s-r)$-voisinage de k. Plus formellement

$$I_{(r,s)}(i_-, i_+) = \{\max V(i_-, s-r) + 1, \ldots, \min V(i_+, s-r) - 1\}.$$

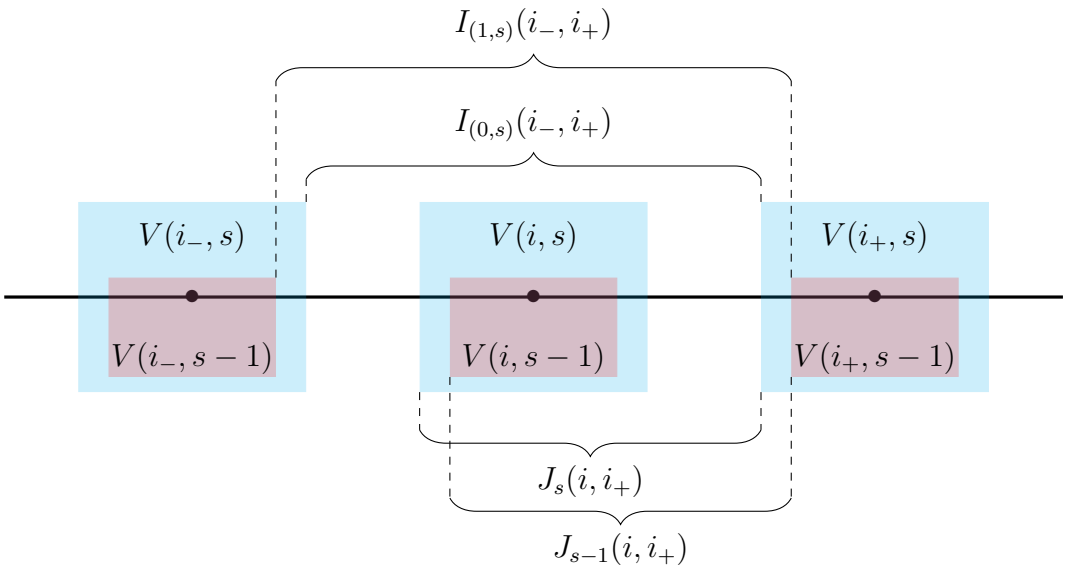


FIGURE 6.2 – Voisinages et segments.

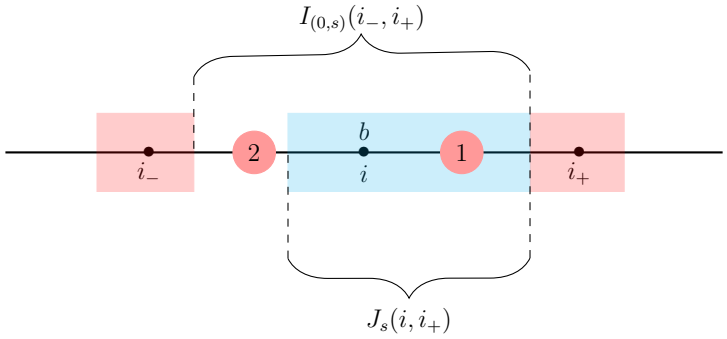
Nous allons maintenant introduire une notion de *similarité* sur les triplets de voisinages prenant sa source dans le jeu d'Ehrenfeucht-Fraïssé à deux jetons (voir théorème 1.12). Prenons deux triplets $(i_-, i, i_+), (j_-, j, j_+)$ qui forment deux s-extractions avec $i_- < i < i_+$ et $j_- < j < j_+$. Ces deux triplets de voisinages vont être *similaires* si les jeux à deux jetons qui y sont *contraints* sont similaires. Nous allons utiliser deux notions différentes de jeux contraints qui ne sont distincts que par l'ensemble de départ. Ces jeux

n'utilisent que deux jetons qui sont contraints d'appartenir aux $r^{\text{ème}}$ tours aux ensembles $I_{(r,s)}(i_-, i_+)$ et $I_{(r,s)}(j_-, j_+)$. Pour le premier jeu, le premier jeton doit être positionné pour Spoiler et Duplicateur dans l'ensemble $J_s(i, i_+)$. Pour le second jeu le premier jeton doit est positionné pour Spoiler et Duplicateur dans l'ensemble $V(i, s)$. Si Duplicateur gagne pour ces deux jeux on dit alors que ces deux triplets sont équivalents, ce que l'on note $(i_-, i, i_+) \sim_s (j_-, j, j_+)$.

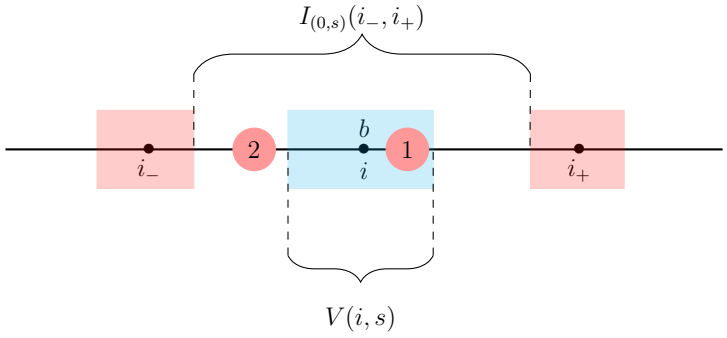
Introduisons formellement cette définition. Nous avons $(i_-, i, i_+) \sim_s (j_-, j, j_+)$. si pour tout $s' \leqslant s$ Duplicateur gagne les deux jeux suivants.

Ce sont des jeux à deux jetons, à s' tours et s' alternances (on considère que Spoiler peut alterner autant qu'il veut entre les deux structures) avec pour signature les prédicats $<, P^1, \ldots, P^t$ et toutes les positions sont étiquetées par la même lettre a à l'exception des positions i et j qui sont étiquetées par la même lettre $b \neq a$. En voici la description :

(1) Pour le premier jeu, le premier jeton de Spoiler et le premier jeton de Duplicateur sont restreints à l'ensemble $J_{s'}(i, i_+)$ et à l'ensemble $J_{s'}(j, j_+)$. Au $r^{\text{ème}}$ tour, les joueurs sont contraints de jouer dans l'ensemble $I_{(r,s')}(i_-, i_+)$ et dans l'ensemble $I_{(r,s')}(j_-, j_+)$.



(2) Pour le second jeu, le premier jeton de Spoiler et le premier jeton de Duplicateur sont restreints à $V(i, s')$ et $V(j, s')$. Au $r^{\text{ème}}$ tour, les joueurs sont contraints de jouer dans l'ensemble $I_{(r,s')}(i_-, i_+)$ et dans l'ensemble $I_{(r,s')}(j_-, j_+)$.



Dans la suite, on dira qu'une position $x \in I_{(r,s')}(i_-, i_+)$ et $y \in I_{(r,s')}(j_-, j_+)$ sont *localement équivalentes* si Duplicateur peut gagner les deux jeux contraints quand les jetons sont sur ces positions. Le lemme suivant, dont la preuve est immédiate, énonce une propriété qui nous sera utile pour la suite.

Lemme 6.17.

Soit (i_-, i, i_+) une s-extraction. Pour tout entier $0 \leqslant r \leqslant s$, nous avons l'égalité suivante qui est satisfaite

$$J_{s-r}(i_-, i) \cup J_{s-r}(i, i_+) = V(i, s-r) \cup I_{(r,s)}(i_-, i_+)$$

Nous allons maintenant prouver que la relation $\sim_s$ est une relation d'équivalence d'indice fini, ce qui est un résultat classique pour ce type d'objet en théorie des modèles finis. On notera que cette relation peut être vue comme l'ensemble des formules vrai pour chaque triplet dans une logique adaptée aux deux jeux contraints. Ainsi deux triplets seraient équivalents s'ils satisfont les mêmes formules logiques de profondeur de quantification au plus s. Comme le nombre de formules est fini, on en déduirait aisément qu'il s'agit d'une relation d'équivalence d'indice fini. Nous présentons maintenant les preuves formelles.

Lemme 6.18.

La relation $\sim_s$ est une relation d'équivalence.

Démonstration : La relation $\sim_s$ est clairement symétrique et réflexive. Soient x, y et z des triplets formant des s-extractions et tels que $x \sim_s y$ et $y \sim_s z$. Prouvons que $x \sim_s z$. On note $S_r(x)$, $S_r(y)$ et $S_r(z)$ les positions autorisées données par ces triplets au $r^{\text{ème}}$ tour. Nous allons jouer simultanément les 3 jeux pour $s' \leqslant s$.

(1) Le premier sur $S_{s'}(x)$ et $S_{s'}(y)$.
(2) Le second sur $S_{s'}(y)$ et $S_{s'}(z)$.
(3) Le troisième sur $S_{s'}(x)$ et $S_{s'}(z)$.

Pour les deux premiers Duplicateur a une stratégie gagnante. Nous allons l'utiliser pour construire une stratégie gagnante pour le troisième jeu. À chaque tour $r \leqslant s'$, supposons que Spoiler joue une position s_1 de $S_r(x)$ dans le troisième jeu. On simule alors le choix de Spoiler en jouant s_1 dans $S_r(x)$ dans le premier jeu. Duplicateur va répondre en suivant sa stratégie gagnante et en choisissant une position s_2 de $S_r(y)$ pour le premier jeu. On simule alors un choix de Spoiler en position s_2 de $S_r(y)$ pour le deuxième jeu. Ici encore, Duplicateur va répondre en suivant sa stratégie gagnante et va choisir une position s_3 dans $S_r(z)$. Enfin, on va choisir cette position s_3 pour répondre au choix de Spoiler dans le troisième jeu.

En suivant les stratégies de Duplicateur, on obtient immédiatement par induction que Duplicateur a également une stratégie pour le troisième jeu. ■

Plutôt qu'introduire une notion assez artificielle de logique adaptée aux jeux contraints, nous allons nous reposer sur une notion de *type* pour prouver que cette relation d'équivalence est d'indice fini. Il s'agit seulement d'un choix de présentation.

Lemme 6.19.

La relation d'équivalence $\sim_s$ est d'indice fini.

Démonstration : Soit $S = (i_-, i, i_+)$ une s-extraction où $i_- < i < i_+$. Nous allons construire par induction une notion de *type* adaptée à notre contexte. On pose r-$\tau_S(x)$ le r-type d'une position x dans $I_{(r,s)}(i_-, i_+)$, défini par induction.

- Pour tout x dans $I_{(0,s)}(i_-, i_+)$ on pose 0-$\tau_S(x)$ le $(t+2)$-uplet de valeurs binaires des prédicats dans la signature. Plus précisément nous avons

$$0\text{-}\tau_S(x) = \big(x < i, x > i, P^1(x,x), \ldots, P^t(x,x)\big) \in \{0,1\}^{t+2}$$

- Pour $s > r > 0$ et tout x dans $I_{(r+1,s)}(i_-, i_+)$ on pose

$$(r+1)\text{-}\tau_S(x) = \Big\{ \Big(C(x,y), r\text{-}\tau(y) \Big) \mid y \in I_{(r,s)} \Big\}$$

avec $C(x,y)$ la valeur des prédicats P^i entre x et y, c'est-à-dire,

$$C(x,y) = \big(x < y, x > y, P^1(x,y), P^1(y,x), \ldots, P^t(x,y), P^t(y,x)\big) \in \{0,1\}^{2t+2}.$$

Le s'-type d'un triplet S est la paire

$$\Big(\{s'\text{-}\tau_S(x) \mid x \in J_{s'}(i, i_+)\}, \{s'\text{-}\tau_S(x) \mid x \in V(i,s)\} \Big).$$

Par construction, il existe un nombre fini de s'-types de positions et donc un nombre fini de s'-types d'un triplet. La définition inductive des types étant calquée sur le jeu à deux jetons et à r-tours défini ci-dessus, il en découle immédiatement que pour tout $s' \leqslant s$ les 2 s-extractions à 3 éléments suivantes (i_-, i, i_+) et (j_-, j, j_+) ont le même s'-type alors $(i_-, i, i_+) \sim_s (j_-, j, j_+)$. Donc $\sim_s$ est d'indice fini. ■

Le théorème de Ramsey est un résultat combinatoire de la théorie des graphes souvent utilisé en théorie des modèles finis. Nous utilisons ici une version adaptée aux *hypergraphes*. Nous l'énonçons dans le contexte des triplets, ce qui est une reformulation directe des 3-*hypergraphes*. Ce théorème établit que pour tout hypergraphe *de grande taille* dont les arêtes sont coloriées, il est possible d'extraire un sous-hypergraphe *de taille suffisamment grande* monochrome. Ce théorème va nous permettre dans la suite de trouver un ensemble de taille arbitrairement grande de triplets de positions tous deux-à-deux équivalents pour la relation $\sim_s$.

Théorème 6.20 (Théorème de Ramsey pour les 3-hypergraphes [55]).

Soit c un entier. Pour chaque entier p il existe un entier n tel que pour tout ensemble E de taille n et pour chaque fonction $h : \mathcal{P}_3(E) \to \{1, \ldots, c\}$ il existe un ensemble $F \subseteq E$ de taille p tel que h est constante sur $\mathcal{P}_3(F)$.

Une *s-extraction bien typée* est un ensemble X qui est une s-extraction et tel que tous les triplets de X sont équivalents pour $\sim_s$. Le théorème suivant est un corollaire immédiat du théorème de Ramsey en posant c le nombre de s-types de triplets et h la fonction qui à triplet associe le s-type.

Corollaire 6.21.

Pour tout entier p il existe une s-extraction bien typée de taille p.

Nous avons maintenant introduit tous les outils pour prouver le théorème 6.10.

6.1.2 Preuve du théorème 6.10.

Soit L un langage avec c comme lettre neutre et définissable dans $\mathbf{FO}^2_m[<, P^1, \ldots, P^t]$. D'après le théorème 1.12, il existe un entier s tel que pour toute paire de mots $(u, v) \in L \times L^c$, Spoiler a une stratégie gagnante pour le jeu à 2-jetons, s-tours et m-alternances sur la signature $\{<, P^1, \ldots, P^t\}$. Prenons une paire (u, v) dans $L \times L^c$. Nous allons maintenant construire une stratégie pour Spoiler n'utilisant que l'ordre et le successeur. Soit $p = \max(|u|, |v|) + 1$. D'après le corollaire 6.21, il existe un entier n et un ensemble $X = \{i_0 < i_1 \cdots < i_p\}$ qui est une s-extraction bien typée de taille p avec $i_p < n$. Soient u' et v' deux mots de longueurs n ainsi que $i_0 < f_0 < f_1 < \cdots < f_{|u|-1} < f_{|u|} = i_p$ et $i_0 < g_0 < g_1 < \cdots < g_{|v|-1} < g_{|v|} = i_p$ vérifiant les conditions suivantes (voir figure 6.3) :

- pour tout entier i les positions f_i et g_i appartiennent à X,
- $u'_{f_i} = u_i$, $v'_{g_i} = v_i$,
- $f_0 = g_0$ et $f_{|u|-1} = g_{|v|-1}$,
- toutes les autres positions de u' et v' sont étiquetées par la lettre c.

Si les mots u et v n'ont pas la même taille, nous pouvons avoir que $f_i \neq g_i$. Les mots u'

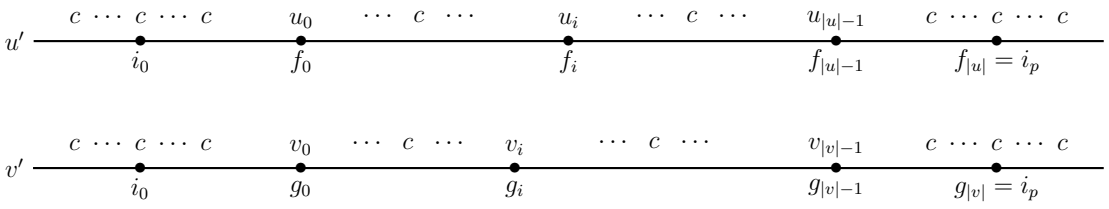
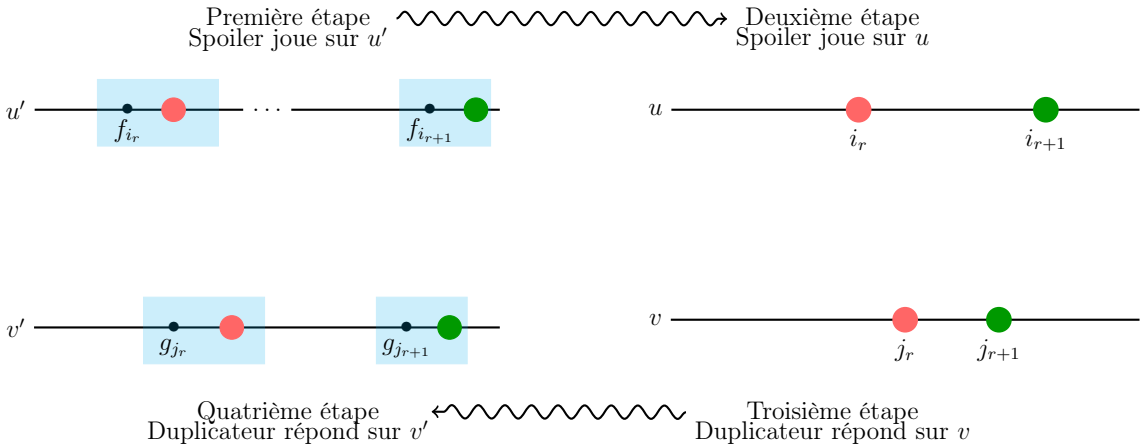


FIGURE 6.3 – Répartition des lettres de u' et v'

et v' ne sont rien d'autre que les mots u et v après avoir inséré suffisamment de lettres neutres pour que les lettres non neutres soient sur les positions de X. On a également forcé les premières et dernières lettres non neutres à être sur les mêmes positions.

Comme c est une lettre neutre, on remarque que (u', v') est dans $L \times L^c$. Donc Spoiler a une stratégie gagnante pour le jeu à 2-jetons, s-tours et m-alternances sur la signature $\{<, P^1, \ldots, P^t\}$. On construit maintenant la nouvelle stratégie pour Spoiler sur (u, v). Pour

ce faire, nous allons *simuler* le jeu sur (u', v') et et construire par induction la stratégie gagnante pour Spoiler sur (u, v). Pour ce faire nous allons exploiter un mécanisme de *va-et-vient* entre le jeu sur (u, v) et le jeu sur (u', v'). En effet, Spoiler va choisir une position sur (u', v') en suivant sa stratégie gagnante que nous allons traduire en une position sur (u, v), puis Duplicateur va choisir une position sur (u, v) que nous allons traduire sur (u', v') et recommencer jusqu'à ce que Duplicateur ne puisse plus répondre sur (u, v). Afin que les choix de Spoiler sur (u', v') conduisent à une stratégie gagnante sur (u, v) nous devons le *forcer* à jouer des coups très distants les uns-des-autres. Si le nouveau jeton de Spoiler est sur un voisinage distincts de l'ancien jeton, alors par construction des voisinages, hormis le prédicat d'ordre, les prédicats numériques ne permettent pas de relier les deux positions ; ils ne *transportent pas* d'informations. Par la suite nous allons toujours noté par i_r la position du $r^{\text{ème}}$ jeton sur u et par j_r la position du $r^{\text{ème}}$ jeton sur v. De même nous noterons à l'aide i'_r la position du $r^{\text{ème}}$ jeton sur u' et par j'_r la position du $r^{\text{ème}}$ jeton sur v'. Le schéma suivant récapitule le fonctionnement du va-et-vient entre les deux jeux.



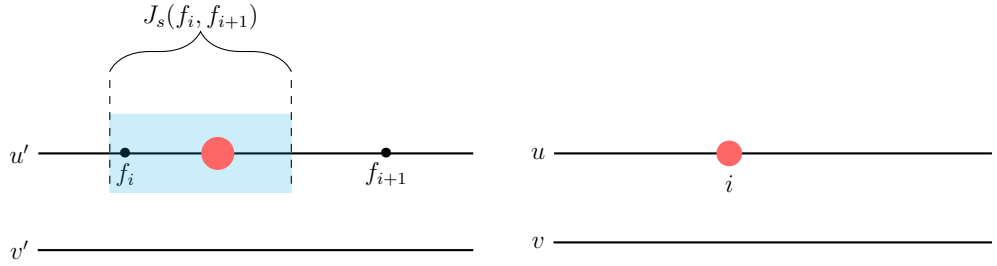
Pour que cette construction fonctionne, il ne faut pas que Spoiler gagne le jeu sur (u', v') avant qu'il ne gagne le jeu sur (u, v). Cela pourrait arriver si les choix de Duplicateur sur (u', v') ne sont pas pertinents. Nous allons empêcher cela en choisissant des positions localement équivalentes, c'est-à-dire des positions où Duplicateur gagne les jeux contraints introduit dans la partie précédente. Spoiler ne pourra pas gagner en choisissant des coups à proximité de l'ancien jeton ; il sera donc obligé de jouer des coups distants.

Lorsque Spoiler joue sur une position extrême du jeu sur (u', v'), Duplicateur peut toujours répondre à la même position sur l'autre mot. Ces coups n'ont donc aucun intérêt dans la stratégie de Spoiler. Ils ne sont pas utilisés pour la construction de la stratégie du jeu sur (u, v). À chaque fois que Spoiler joue un tel coup, le jeu sur (u, v) reste donc figé. En particulier, si le jeu n'a pas encore commencé, les jetons ne sont pas posés, et si les jetons sont déjà positionnés, ils ne sont pas déplacés.

Nous allons commencer par décrire le premier tour du jeu, puis nous donnerons une construction par induction pour les tours suivants. Pour le premier coup, la stratégie gagnante de Spoiler désigne une position pour le jeu sur (u', v'). Par symétrie, nous allons

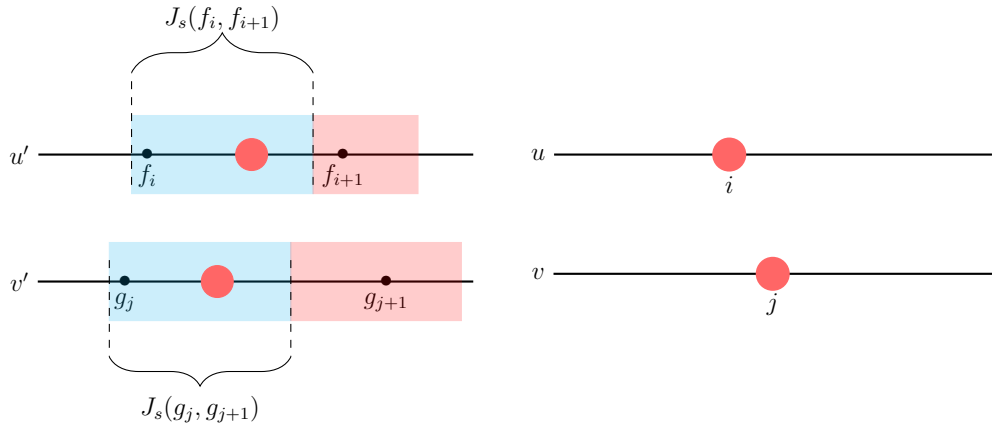
supposer qu'il s'agit d'une position sur u'. On distingue alors deux cas :

(1) Ce premier coup est à l'intérieur d'un segment de la forme $J_s(f_i, f_{i+1})$ pour un entier $0 \leqslant i < |u|$. Dans ce cas, nous allons choisir de jouer sur la position i dans le jeu sur (u, v).



Duplicateur répond alors au jeu sur (u, v) en jouant sur v à une position j. Si la lettre qui étiquette j est différente de celle qui étiquette i, alors Duplicateur perd le jeu. Dans le cas contraire, nous allons pouvoir simuler la réponse de Duplicateur dans le jeu sur (u', v') en choisissant une position dans $J_s(f_j, f_{j+1})$ localement équivalente à celle du premier jeton de Spoiler sur u. Ceci est possible car les lettres qui étiquettent f_i sur u' et g_j sur v' sont identiques et que

$$\{f_{i-1}, f_i, f_{i+1}\} \sim_s \{g_{j-1}, g_j, g_{j+1}\}.$$



(2) Ce premier coup est sur une position extrême, c'est-à-dire, plus petite que

$$\min J_s(f_0, f_1) = \min J_s(g_0, g_1)$$

ou plus grande que

$$\max J_s(f_{|u|-1}, f_{|u|}) = \max J_s(g_{|v|-1}, g_{|v|}).$$

Dans ce cas, le processus de va-et-vient est *dégénéré* car le jeu sur u et v n'a pas encore débuté. Celui-ci ne débutera que quand Spoiler jouera une position *pertinente* sur u' ou v', c'est-à-dire, une position non-extrême. Tous les choix de Spoiler non pertinents sont inutiles ; il suffit pour Duplicateur de répondre dans le jeu sur (u', v') en choisissant la même position que Spoiler mais sur l'autre mot. Tant que Spoiler

répond sur ces positions extrêmes Duplicateur répond en jouant l'exacte même position. Comme Spoiler suit une stratégie gagnante, il va nécessairement finir par jouer à l'intérieur d'un segment de la forme $J_s(f_i, f_{i+1})$ pour un entier $0 \leqslant i < |u|$. En effet, les positions extrêmes et les segments de la forme $J_s(f_i, f_{i+1})$ forment une partition de toutes les positions du mots (voir la figure 6.2). On se ramène alors au cas ci-dessus.

Nous allons maintenant expliquer comment on construit la stratégie de Spoiler sur (u, v) dans les tours suivants. Nous la construisons par induction. Pour ce faire, on suppose que nous avons joué $1 \leqslant r < s$ tours et que les jetons du tour précédent sont sur des positions i_r sur u et j_r sur v ainsi que i'_r sur u' et j'_r sur v'. C'est maintenant à Spoiler de jouer. Nous supposons, par induction, que les propriétés suivantes sont satisfaites :

- Les positions i'_r et j'_r appartiennent à

$$I_{(r,s)}(f_{i_r-1}, f_{i_r+1})$$
$$I_{(r,s)}(g_{j_r-1}, g_{j_r+1})$$

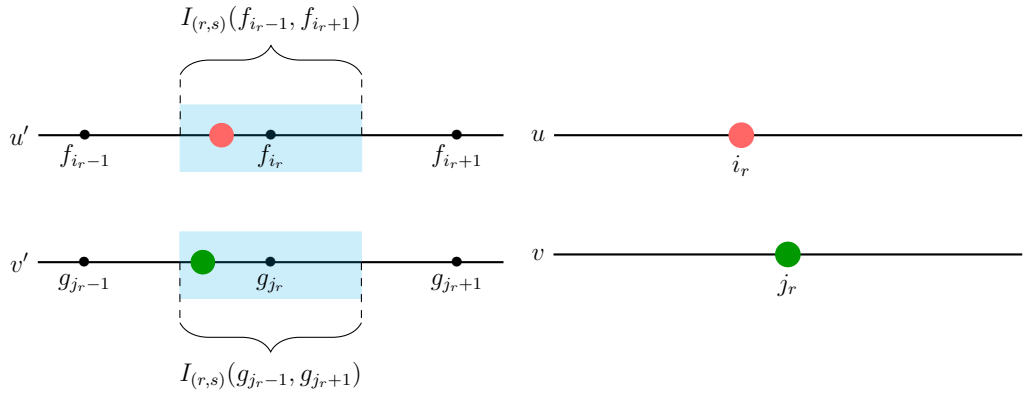
  et sont des positions localement équivalentes pour l'un des deux jeux contraints à $s-r$ tours. Le premier jeu contraint va être utilisé dans le cas numéro 2, et le second jeu contraint va être utilisé dans le cas numéro 3 (voir figure 6.4).
- Si cela n'est pas satisfait, alors les des deux jetons ont la même valeurs qui est une position extrême sur (u', v'). Plus précisément, $i'_r = j'_r$ et soit

$$i'_r < \min J_{s-r}(f_0, f_1) = \min J_{s-r}(g_0, g_1)$$

  ou

$$i'_r > \max J_{s-r}(f_{|u|-1}, f_{|u|}) = \max J_{s-r}(g_{|v|-1}, g_{|v|}).$$

- La configuration du jeux sur (u', v') est gagnante pour Spoiler, c'est-à-dire, qu'il dispose d'une stratégie gagnante en moins de $s - r$ tours (le nombre de tours restant).



Nous allons distinguer deux cas dans ce qui suit. Soit Duplicateur va pouvoir répondre au dernier jeton de Spoiler pour le jeu sur (u, v) soit Duplicateur ne peut pas répondre et Spoiler gagne. Puisqu'on désire construire une stratégie gagnante pour Spoiler, nous allons supposer que Duplicateur répond correctement sur (u, v). Si cela est possible, alors

nous allons construire une réponse correcte pour Duplicateur dans le jeu sur (u', v'). Comme Spoiler possède une stratégie gagnante sur le jeu (u', v') que nous suivons, nous arriverons nécessairement en une position perdante pour Duplicateur pour le jeu (u', v') et donc pour le jeu (u, v). Ce qui permet de conclure la preuve. Il reste néanmoins à expliquer comment construire la nouvelle position de Spoiler sur (u, v) et de déduire de la réponse de Duplicateur sur (u, v) la réponse adéquate de Duplicateur sur (u', v').

Nous allons utiliser la stratégie gagnante de Spoiler sur le jeu sur (u', v') pour construire le nouveau coup de Spoiler sur (u, v). Par symétrie, on peut supposer que ce nouveau coup se fait sur u' et on note i'_{r+1} la position de ce coup sur u'. Nous allons distinguer les quatre cas en fonction de la valeur de i'_{r+1} (voir figure 6.4). En effet, le segment $\{0, \ldots, n-1\}$ est décomposée en quatre parties qui vont chacune correspondre à un des quatre cas suivants :

(1) le premier cas correspond aux segments de la forme $J_{s-r-1}(f_k, f_{k+1})$ pour $k \neq i_r$ et $k \neq i_{r-1}$. Il recouvre pratiquement tout le segment $\{0, \ldots, n\}$ à exception des positions aux extrêmes ainsi que d'un *trou* autours des points i'_r et i'_{r-1}.

(2) Le second cas correspond au segment initial *tronqué* à gauche de l'ancien jeton sur u'. Il s'agit du segment initial du second jeu contraint pour cette position ; plus précisément, c'est le segment $V(f_{i_r-1}, s-r-1)$.

(3) Le troisième cas correspond à l'arène des jeux contraints autours de i'_r ; plus précisément il s'agit du segment $I_{(r+1,s)}(f_{i_r-1}, f_{i_r+1})$.

(4) Le dernier cas correspond aux positions extrêmes qui sont les dernières positions qui n'ont pas été traité par le cas d'avant. Elles sont à droite ou à gauche du segment $\{0, \ldots, n\}$.

Les quatre cas couvrent bien toutes les positions possibles du jeton car d'une part les intervalles $J_{s-r-1}(f_k, f_{k+1})$ forment une partition des positions non-extrêmes et que d'autre part, d'après le lemme 6.17, on a l'égalité

$$J_{s-r-1}(f_{i_r-1}, f_{i_r}) \cup J_{s-r-1}(f_{i_r}, f_{i_r+1}) = V(f_{i_r-1}, s-r-1) \cup I_{(r+1,s)}(f_{i_r-1}, f_{i_r+1}).$$

Nous allons maintenant présenter la stratégie de va-et-vient pour chacun des cas que nous avons exposés ci-dessus.

(1) Il existe un entier k différent de i_r et $i_r - 1$ tel que la position i'_{r+1} appartient à

$$J_{s-r-1}(f_k, f_{k+1}).$$

Il suffit alors à Spoiler de choisir $i_{r+1} = k$ comme position sur (u, v). On remarque que les prédicats autres que l'ordre sont tous évalués à *faux* entre i'_r et i'_{r+1}. Supposons que Duplicateur répond correctement en j_{r+1}, nous choisissons la position j'_{r+1} sur v' dans l'ensemble

$$J_{s-r-1}(g_{j_{r+1}}, g_{j_{r+1}} + 1)$$

de sorte que les positions i'_{r+1} et j'_{r+1} soient localement équivalentes pour le premier jeu contraint. Ceci est possible car les positions $f_{i_{r+1}}$ et $g_{j_{r+1}}$ sont étiquetées par la

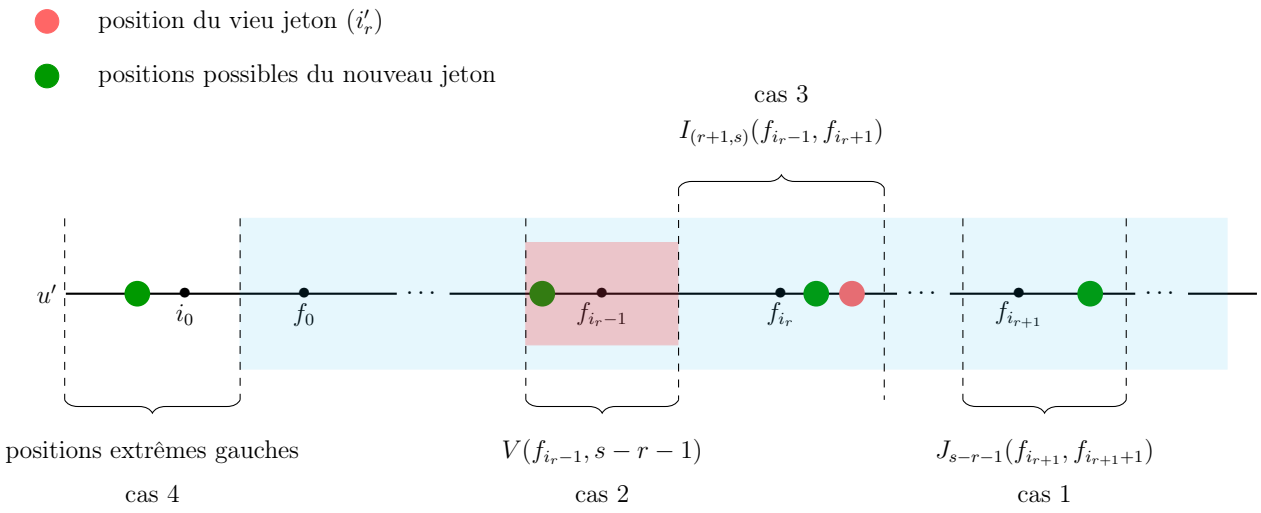


FIGURE 6.4 – Les quatre cas à traiter

même lettre et que

$$\{f_{i_{r+1}-1}, f_{i_{r+1}}, f_{i_{r+1}+1}\} \sim_s \{g_{j_{r+1}-1}, g_{j_{r+1}}, g_{j_{r+1}+1}\}.$$

On remarque que tous les prédicats autres que l'ordre sont évalués à *faux* entre j'_r et j'_{r+1}. La valeur du prédicat d'ordre entre i'_r et i'_{r+1} est la même qu'entre i_r et i_{r+1} qui est la même qu'entre j_r et j_{r+1} qui est la même qu'entre j'_r et j'_{r+1} et puisque les lettres qui étiquettent i_{r+1} sur u et j_{r+1} sur v sont égales nous avons que les lettres qui étiquettent $f_{i_{r+1}}$ et $g_{j_{r+1}}$ sont également égales et donc le choix de j'_{r+1} est correcte pour Duplicateur. Finalement, la nouvelle configuration respecte bien l'hypothèse d'induction.

(2) Supposons que i'_{r+1} appartient à $V(f_{i_r-1}, s-r-1)$. Dans ce cas, on choisit $i_{r+1} = i_r - 1$, c'est-à-dire que Spoiler joue sur la position juste à gauche de i_r. La relation successeur faisant partie de signature, Duplicateur est contraint de jouer également à la position juste à gauche. Les mêmes arguments qu'au cas 1 permettent de construire une position j'_{r+1} telle que la nouvelle configuration respecte bien l'hypothèse d'induction, en utilisant cette fois-ci le second jeu contraint.

(3) Si i'_{r+1} appartient à

$$I_{(r+1,s)}(f_{i_r-1}, f_{i_r+1}),$$

alors par hypothèse d'induction Duplicateur possède une position j'_{r+1} dans

$$I_{(r+1,s)}(g_{j_r-1}, g_{j_r+1})$$

qui est localement équivalente à i'_{r+1}. En jouant cette position, et en posant $i_{r+1} = i_r$ et $j_{r+1} = j_r$ on obtient une nouvelle configuration qui respecte bien l'hypothèse d'induction.
On remarque que dans ce cas la configuration du jeu sur (u, v) n'évolue pas.

(4) Le dernier cas restant est si i'_{r+1} ne vérifie aucun des cas précédents. Par construction des segments, les segments de la forme $J_s(f_k, f_{k+1})$ (resp. $J_s(g_k, g_{k+1})$) forment une partition de l'ensemble des positions non extrême. Si l'entier i_{r+1} n'est traité par aucun des cas précédents, alors nécessairement cette position appartient à une position extrême ; c'est-à-dire

$$i'_{r+1} < \min J_{s-r-1}(f_0, f_1) = \min J_{s-r-1}(g_0, g_1)$$

ou

$$i'_{r+1} > \max J_{s-r-1}(f_{|u|-1}, f_{|u|}) = \max J_{s-r-1}(g_{|v|-1}, g_{|v|}).$$

On choisit $j'_{r+1} = i'_{r+1}$ pour Duplicateur sur le mot v', ainsi que $i_{r+1} = i_r$ et $j_{r+1} = j_r$; la situation sur (u, v) n'évolue pas et la nouvelle configuration respecte bien l'hypothèse d'induction. On remarque qu'il est possible que i'_{r+1} soit sur une position extrême et soit géré par l'un des cas précédents. Par exemple si i_r appartient à $J_{s-r}(f_0, f_1)$ et si

$$i_{r+1} \in I_{(r+1,s)}(i_0, f_1) \cap \{0, \dots, \min J_{s-r-1}(f_0, f_1)\},$$

alors Duplicateur va suivre le premier jeu contraint et il est possible que $i_{r+1} \neq j_{r+1}$. Dans ce cas précis, comme i'_{r+1} et j'_{r+1} sont choisit localement équivalents, nous respectons bien l'hypothèse d'induction.

Tous les cas sont traités, nous avons donc montré que tant que Duplicateur répond correctement sur (u, v), il va pouvoir répondre correctement sur (u', v'). Comme Spoiler a une stratégie gagnante sur (u', v') que l'on suit, Duplicateur va nécessairement être incapable de répondre sur (u, v), ce qui conclut la preuve.

6.2 Le cas des prédicats unaires

Les prédicats unaires, uniformes ou non uniformes, sont bien plus simples à traiter que les prédicats binaires. On remarque néanmoins que de nombreux langages non réguliers classiques sont facilement définissables dans $\mathbf{MSO}[<, \mathcal{A}\mathrm{rb}_1]$.

Exemple : Le langage $\{a^n b^n \mid n > 0\}$ est définissable dans $\mathbf{MSO}[<, \mathcal{A}\mathrm{rb}_1]$ à l'aide de la formule

$$\max \equiv 1 \bmod 2 \wedge \forall x \left(\left(x \leqslant \frac{\max -1}{2} \right) \leftrightarrow \mathbf{a}(x) \right).$$

Notation : Soit $P = (P_n)_{n \in \mathbb{N}}$ un prédicat unaire. Pour n un entier et $x < n$, on notera $P(x, n) = P_n(x)$.

Nous allons introduire un certain nombre de notations qui vont nous permettre d'étudier **MSO** équipé de prédicats unaires. L'objectif est de transférer l'information portée par les prédicats unaires directement sur l'alphabet et décomposer ainsi tout langage défini par des prédicats unaires en deux parties distinctes :

- Une partie contenant une information régulière donnée sous la forme d'un langage régulier sur un alphabet *enrichi*.
- Une partie non régulière contraignant l'alphabet enrichi à respecter la *sémantique* des prédicats numériques unaires.

Soient k un entier et $\kappa = (P_1, \ldots, P_k)$ un k-uplet de prédicats unaires. On définit B_k l'ensemble des parties de $\{1, \ldots, k\}$. Un mot $u \in B_k^n$ est *bien formé* par rapport à κ si et seulement si pour tout entier $i < n$, $u_i = \{j \mid P_j(i, n) = 1\}$. Soit A un alphabet et π_k la projection de $(A \times B_k)^* \to B_k^*$. Un mot de $(A \times B_k)^*$ est *bien formé* si son image par π_k est bien formée. On note K_κ l'ensemble des mots bien formés de $(A \times B_k)^*$

Quand le contexte sera clair, on notera π la projection de $(A \times B_k)^*$ vers A^*. Pour tout mot u de A^*, on notera également $\sigma(u)$ l'unique mot de K_σ tel que $\pi(\overline{u}) = u$ et pour i un entier, on notera $\sigma_n^i(u)$ le *mot bien formé translaté* d'un facteur i de u, c'est-à-dire, l'unique suffixe de longueur $|u|$ du préfixe de longueur $i + |u|$ de $\sigma(vuw)$ pour $v \in A^i$ et $w \in A^{n-i-|u|}$. On remarque que $\sigma_n^i(u)$ n'est bien défini que pour $n \geqslant i + |u|$ et que dans ces conditions, $\sigma_n^i(u)$ ne dépend pas du choix de v et de w.

Exemple : Si on pose $\kappa = (x \leqslant \frac{\max -1}{2})$. On obtient

$$\sigma(aaba) = (a, \emptyset)(a, \emptyset)(b, \{1\})(a, \{1\}) \text{ et } \sigma_6^2(aaba) = (a, \emptyset)(a, \{1\})(b, \{1\})(a, \{1\}).$$

Enfin on remarque que $\sigma(u) = \sigma_n^0(u)$. Le lemme suivant, qui nous sera utile, est une conséquence immédiate de ces définitions.

Lemme 6.22.

Soient u, v, w des mots de A^*. On pose $i = |u|$ et $n = |uvw|$. On a alors $\sigma(uvw) = \sigma_n^0(u)\sigma_n^i(v)\sigma_n^{i+|v|}(w)$.

Comme dans le cas de l'ajout de la signature locale (voir théorème 3.24) et l'ajout des prédicats modulaires (voir théorème 4.15), le théorème 1.13 permet de mettre les langages de $\mathbf{MSO}[<, \mathcal{A}\mathrm{rb}_1]$ sous une forme agréable à utiliser. On remarque qu'il n'est pas nécessaire de prendre en compte le cas des prédicats 0-aires, ceux-ci pouvant être gérés à l'aide de prédicats unaires dans **MSO**. Le théorème d'ajout des prédicats unaires se simplifie donc en la proposition suivante, qui va nous être utile pour la suite. Cette proposition établit qu'un langage défini par une formule de $\mathbf{MSO}[<, \mathcal{A}\mathrm{rb}_1]$ possède une *forme* de régularité.

Proposition 6.23.

Soient L un langage de A^* et $\kappa = (P_1, \ldots, P_k)$ un k-uplet de prédicats unaires. Les deux conditions suivantes sont équivalentes.

(1) Le langage L est dans $\mathbf{MSO}[<, \kappa]$,

(2) il existe un langage régulier L' de $(A \times B_k)^*$ tel que

$$L = \pi(L' \cap K_\kappa).$$

Le théorème suivant constitue le résultat central de cette section.

Théorème 6.24.

Le fragment $\mathbf{MSO}[<, \mathcal{A}\mathrm{rb}_1]$ vérifie la propriété de Crane Beach.

Démonstration : Pour vérifier la propriété de Crane Beach pour $\mathbf{MSO}[<, \mathcal{A}\mathrm{rb}_1]$, il suffit de prouver que tout langage à lettre neutre définissable dans $\mathbf{MSO}[<, \mathcal{A}\mathrm{rb}_1]$ est régulier. Soient $\kappa = (P_1, \ldots, P_k)$ un k-uplet de prédicats unaires et L un langage de A^* définissable dans $\mathbf{MSO}[<, P_1, \ldots, P_k]$ ayant c comme lettre neutre. D'après la proposition 6.23, il existe un langage régulier L' de $(A \times B_k)^*$ tel que $L = \pi(L' \cap K_\kappa)$. On note $\equiv_L$ la congruence syntaxique de L et $\equiv_{L'}$ la congruence syntaxique de L'. D'après le théorème 2.5, il suffit de montrer que $\equiv_L$ est une congruence d'indice fini. Par définition de lettre neutre, pour tout mot $u \in A^*$, $u \equiv_L uc \equiv_L cu$. Soit K le nombre de classes de la congruence $\equiv_{L'}$.

Montrons que le nombre de classes de $\equiv_L$ est borné par K. Pour ce faire, nous allons raisonner par l'absurde, et supposer qu'il existe $K+1$ mots $u_1, \ldots, u_{K+1}$, deux à deux non équivalents pour la congruence $\equiv_L$. Quitte à ajouter des lettres c, on peut supposer que tous ces mots sont tous de même longueur k. Soient u, v deux mots non équivalents. On peut donc supposer qu'il existe s, t tels que $sut \in L$ et $svt \notin L$. Pour chaque paire d'entiers distincts $i, j \in \{1, \ldots, K+1\}^2$ il existe donc deux mots $s_{i,j}$ et $t_{i,j}$ qui témoignent que u_i et u_j ne sont pas équivalents pour $\equiv_L$. Comme il est possible d'ajouter des lettres neutres à ces témoins, on peut supposer qu'il existe p et q tels que pour tous i, j distincts, $s_{i,j}$ est de longueur p et $t_{i,j}$ est de longueur q. Comme il existe au plus K classes d'équivalences pour la congruence $\equiv_{L'}$, nécessairement, il existe deux entiers distincts i, j tels que $\sigma_n^p(u_i) \equiv_{L'} \sigma_n^p(u_j)$, en posant $n = p + k + n$. Or par le lemme 6.22,

$$\sigma(s_{i,j}u_it_{i,j}) = \sigma_n^0(s_{i,j})\sigma_n^p(u_i)\sigma_n^{p+k}(t_{i,j}) \text{ et } \sigma(s_{i,j}u_jt_{i,j}) = \sigma_n^0(s_{i,j})\sigma_n^p(u_j)\sigma_n^{p+k}(t_{i,j})$$

En particulier, on obtient que $\sigma(s_{i,j}u_it_{i,j}) \in L'$ si et seulement si $\sigma(s_{i,j}u_jit_{i,j}) \in L'$ et donc que $s_{i,j}u_it_{i,j} \in L$ si et seulement si $s_{i,j}u_jt_{i,j} \in L$. Or par construction des mots $s_{i,j}$ et $t_{i,j}$, cela est impossible, ce qui conclut la preuve. ■

Chapitre 7

Les propriétés de substitutions

L'objectif de cette partie est d'introduire des outils génériques pour étudier les langages réguliers et à lettre neutre définissables dans un fragment enrichi par des prédicats numériques arbitraires unaires. En effet, des résultats autour de la conjecture de Straubing ou de la propriété de Crane Beach sont connus quand on se restreint aux prédicats unaires. Par exemple la conjecture de Straubing est prouvée pour le fragment $(\mathbf{FO} + \mathbf{MOD})[<, \mathcal{A}\mathrm{rb}_1]$ [66] et le fragment $\mathbf{FO}[<, \mathcal{A}\mathrm{rb}_1]$ vérifie la propriété de Crane Beach [11]. Ces résultats sont difficiles à montrer, par exemple, pour le premier fragment la preuve repose sur le théorème de Ramsey et sur une description algébrique (*one-scan program*). Pour le second fragment, la preuve utilise directement les jeux d'Ehrenfeucht-Fraïssé. Dans ce chapitre, nous allons étudier une propriété plus forte que la conjecture de Straubing : la *substitution*. Il s'agit de montrer que si un langage régulier est défini par une formule à l'aide de prédicats numériques, alors la même formule permet de le définir en substituant les prédicats numériques par des prédicats réguliers. C'est ce que nous appellerons la *propriété de substitution*. Les résultats de ce chapitre sont les suivants :

- La propriété de substitution est vraie pour les prédicats unaires. La preuve repose sur des opérations logiques élémentaires ainsi que sur un résultat de *sélection* (voir le lemme 7.3).
- Nous allons ensuite montrer que la propriété de substitution est fausse quand on considère des prédicats binaires. Nous allons exhiber un contre-exemple construit à partir de l'exécution d'une machine de Turing.
- La propriété de substitution est contraignante car elle requiert qu'un même prédicat qui apparaîtrait à plusieurs endroits dans la formule soit remplacé par un même prédicat régulier. Cette cohérence entre les différentes occurrences du prédicat n'est pas nécessaire pour prouver des résultats du type de la conjecture de Straubing. Nous allons donc redéfinir une propriété de substitution *affaiblie* pour prendre en compte cette remarque. Le contre-exemple à la substitution n'en est plus un lorsqu'on considère la substitution affaiblie.

7.1 Introduction

Dans cette section, nous étudierons, formule par formule, le comportement des prédicats numériques. Pour ce faire, nous allons substituer les prédicats par des variables du second ordre de même arité. Pour ce faire, on introduit brièvement la syntaxe de *logique du second ordre* sur une signature relationnelle σ. Il s'agit des formules construites à partir des opérations booléennes, des quantifications du premier ordre, des quantifications du second ordre d'arité quelconques et à partir des atomes $(x_1, \ldots, x_k) \in P$ où P est un prédicat de σ, $(x_1, \ldots, x_k) \in X$ où X est un symbole de *variable du second ordre* d'arité k. La sémantique de la logique du second ordre peut être définie exactement comme pour $\mathbf{MSO}[\sigma]$ (voir la sous-section 1.3.2).

Nous allons être intéressé qu'à une petite classe des formules du second ordre qu'on appelle *les formules pré-closes de* $\mathbf{MSO}[\sigma]$. Il s'agit des formules de la logique du second ordre sur la signature σ telles que :

- Toutes les quantifications sont des quantifications de la logique monadique du second ordre.
- Toutes les variables libres sont des variables libres du second ordre d'arité quelconques.

On remarque qu'il est possible dans cette logique d'avoir des variables du second ordre d'arité quelconques mais impossible d'utiliser des quantifications du second ordre autres qu'unaire. Le terme *pré-clos* provient de la sémantique que l'on va attribuer à ces formules. En effet, elles peuvent être pensées comme des formules closes dont les prédicats n'ont pas encore d'interprétation. Ainsi, les variables libres du second ordre désignent les *trous* dans lesquels nous allons mettre les prédicats (pas nécessairement numériques).

On notera dans la suite $\mathrm{Ar}(X)$ l'arité d'une variable du second ordre X. Soient $\psi(X_1, \ldots, X_k)$ une formule pré-close de $\mathbf{MSO}[\sigma]$ et $P_1, \ldots, P_k$ des prédicats tels que P_i est d'arité $\mathrm{Ar}(X_i)$. On note $\psi(P_1, \ldots, P_k)$ la formule où la variable X_i est remplacée par le prédicat P_i (on dit également que la variable X_i est *instanciée* par le prédicat P_i). La formule $\psi(P_1, \ldots, P_k)$ devient alors une formule de $\mathbf{MSO}[\sigma, P_1, \ldots, P_k]$. Dans la suite on utilisera la notion d'*équivalence syntaxique*, pour désigner une opération d'instanciation qui rend deux formules syntaxiquement égales, ainsi que la notion d'*équivalence sémantique*, si deux formules définissent les mêmes langages de mots finis.

Exemples :

- Prenons l'énoncé φ :

$$\forall x \left(\left(x \leqslant \frac{\max -1}{2} \right) \leftrightarrow \mathbf{a}(x) \right) \wedge \max \equiv 1 \bmod 2$$

qui définit le langage $\{a^n b^n \mid n > 0\}$. En remplaçant les prédicats par des variables nous obtenons la formule suivante :

$$\psi(X, Y) = \forall x \left(\left(x \in X \right) \leftrightarrow x \in Y \right) \wedge \max \equiv 1 \bmod 2.$$

On a alors que $\psi(x \leqslant \frac{\max -1}{2}, \mathbf{a})$ est syntaxiquement équivalente à φ.

- Soit $A = \{a_1, \ldots, a_p\}$. Prenons l'énoncé φ :

$$\left(\forall x \forall y \; x + y = \max \rightarrow \bigvee_{a \in A} a(x) \wedge a(y)\right) \wedge \max \equiv 1 \bmod 2$$

qui définit le langage $\{u\overline{u} \mid u \in A^*\}$ où $\overline{u}$ est le mot *miroir* de u ; c'est-à-dire pour $u = u_0 \cdots u_n$, on a $\overline{u} = u_n \cdots u_0$. En remplaçant les prédicats par des variables nous obtenons la formule $\psi(X, Y_1, \ldots Y_p)$:

$$\left(\forall x \forall y \; (x, y) \in X \max \rightarrow \bigvee_{i=1}^{p} x \in Y_i \wedge y \in Y_i\right) \wedge \max \equiv 1 \bmod 2$$

On a alors que $\psi(x + y = \max, \mathbf{a_1}, \ldots, \mathbf{a_p})$ est syntaxiquement équivalente à φ.

Nous allons introduire la *propriété de substitution* que nous allons étudier dans ce chapitre. Intuitivement, une formule vérifie la propriété de substitution si quand elle définit un langage régulier à l'aide de prédicats arbitraires, alors il est possible de remplacer les prédicats arbitraires par des prédicats réguliers (et définir le même langage).

Définition 7.1 (Propriété de substitution).

Soit $\psi(X_1, \ldots, X_k)$ une formule pré-close. Cette formule vérifie la propriété de substitution si pour tous prédicats $P_1, \ldots, P_k$ tels que le langage L défini par $\varphi(P_1, \ldots, P_k)$ est régulier, il existe des prédicats réguliers $Q_1, \ldots Q_k$ tels que $\varphi(Q_1, \ldots, Q_k)$ définit également le langage L.

7.2 Le théorème de substitution

Nous allons prouver que la propriété de substitution est vérifiée dans le cas des prédicats monadiques.

Théorème 7.2 (substitution des formules pré-closes monadiques).

Soit φ une formule pré-close de **MSO**[<] dont toutes les variables libres sont unaires. Alors, la formule φ vérifie la propriété de substitution.

Introduisons dans un premier temps quelques notations. La formule Part exprime que les variables monadiques du second ordre $X_1, \ldots, X_1$ forment une partition :

$$\mathrm{Part}(X_1, \ldots, X_k) = \left(\forall x \bigvee_{i=1}^{k} (x \in X_1)\right) \wedge \left(\bigwedge_{i \neq j} \forall x \;\; (x \in X_i \rightarrow x \notin X_j)\right).$$

À plusieurs reprises les variables libres du second ordre auront une sémantique supplémentaire. Afin de faciliter la lecture, nous ajouterons cette information en indice des symboles de variables libres du second. Par exemple, pour un langage régulier L sur un alphabet $A = \{a_1, \ldots, a_t\}$ et φ une formule pré-close tels que $\varphi(\mathbf{a_1}, \ldots, \mathbf{a_t})$ définit le langage L, on notera $\varphi(X_{\mathbf{a_1}}, \ldots, X_{\mathbf{a_t}})$ la formule φ avec ses variables libres du second ordre.

Pour prouver le théorème de substitution nous allons avoir besoin d'un lemme de *sélection*. Le lemme suivant établi que pour un langage régulier ayant au moins un mot de chaque longueur il est possible de construire un langage régulier ayant exactement un mot de chaque longueur.

Lemme 7.3 (Lemme de sélection régulière).

Soit L un langage régulier de A^* tel que pour tout n, $L \cap A^n \neq \emptyset$. Il existe un langage régulier K de A^* inclus dans L et tel que pour chaque entier n, $K \cap B^n$ contient exactement un mot.

Démonstration : On choisit un ordre total $<$ sur les lettres de $A = \{a_1, \ldots, a_p\}$, nous allons montrer que l'ensemble des mots minimaux pour l'ordre lexicographique forme un langage régulier. Nous allons construire une formule de **MSO**[$<$] qui accepte ce langage. Une construction directement sur les automates est également possible. Soient n un entier, $u = u_1 \cdots u_n$ et $v = v_1 \cdots v_n$ deux mots de A^n.

Il est possible de représenter les mots de A^n à l'aide de p prédicats unaires formant une partition du domaine. Par exemple les variables $X_1, \ldots, X_p$ représente un mot $u_0 \cdots u_{n-1}$ de A^* si elles forment une partition de $\{0, \ldots, n-1\}$ et si pour $1 \leqslant i \leqslant p$ l'ensemble représentée par la variable X_i est exactement l'ensemble des positions étiquetées par a_i.

On dit que $u <_{\text{lex}} v$ si le plus petit entier i tel que $u_i \neq v_i$ vérifie $u_i < v_j$. Définissons la formule $\text{lex}(X_{a_1}, \ldots, X_{a_p}, Y_{a_1}, \ldots, Y_{a_p})$, qui accepte si le mot encodé par $X_{a_1}, \ldots, X_{a_p}$ est plus petit pour $<_{\text{lex}}$ que le mot encodé par $Y_{a_1}, \ldots, Y_{a_p}$:

$$\left(\exists x \ \left(\forall y \ y < x \to \bigwedge_a (y \in X_a \leftrightarrow y \in Y_a)\right) \wedge \left(\bigwedge_{a<a'} (x \in X_a \wedge x \in Y_{a'})\right)\right).$$

Soient L un langage régulier de A^* et θ une formule pré-close de **MSO**[$<$] tels que L est défini par $\theta(\mathbf{a_1}, \ldots, \mathbf{a_p})$. On définit la formule $\text{Sel}_L(X_{a_1}, \ldots, X_{a_p})$ par

$$\theta(X_{a_1}, \ldots, X_{a_p}) \wedge$$
$$\forall Y_1 \cdots \forall Y_{a_p} \Big(\text{Part}(Y_{a_1}, \ldots, Y_{a_p}) \wedge \theta(Y_{a_1}, \ldots, Y_{a_p})\Big) \to \text{lex}(X_{a_1}, \ldots, X_{a_p}, Y_{a_1}, \ldots, Y_{a_p})$$

Enfin, la formule $\text{Sel}_L(\mathbf{a_1}, \ldots, \mathbf{a_p})$ est un énoncé de **MSO**[$<$]. Elle définit un langage régulier de A^* contenant les mots de L minimaux pour l'ordre lexicographique. Il y en a exactement un par longueur de mot. ■

Démonstration du théorème 7.2 : Nous allons dans un premier temps montrer que la classe des prédicats qui conviennent pour la formule peut être représentée par un langage régulier. Puis nous allons construire un prédicat à l'aide du lemme de sélection.

Soient $A = \{a_1, \ldots, a_k\}$ un alphabet, L un langage régulier de A^* et $P_1, \ldots, P_n$ des prédicats numériques unaires. On suppose qu'il existe

$$\varphi(X_1, \ldots, X_n, X_{\mathbf{a_1}}, \ldots, X_{\mathbf{a_k}})$$

une formule pré-close de $\mathbf{MSO}[<]$ telle que L est défini par la formule

$$\varphi(P_1, \ldots, P_n, \mathbf{a_1}, \ldots, \mathbf{a_k})$$

Comme L est un langage régulier, il existe également une formule pré-close $\psi(X_{\mathbf{a_1}}, \ldots, X_{\mathbf{a_k}})$ telle que $\psi(\mathbf{a_1}, \ldots, \mathbf{a_k})$ définit le langage régulier L.

On peut quantifier sur tous les mots de longueur identique à celle de la structure. On note $\forall u\ \varphi(X_1, \ldots, X_n) \leftrightarrow \psi$ la formule

$$\forall X_{\mathbf{a_1}} \cdots \forall X_{\mathbf{a_k}}\ \mathrm{Part}(X_{\mathbf{a_1}}, \ldots, X_{\mathbf{a_k}}) \rightarrow \Big(\varphi(X_1, \ldots, X_n, X_{\mathbf{a_1}}, \ldots, X_{\mathbf{a_k}}) \leftrightarrow \psi(X_{\mathbf{a_1}}, \ldots, X_{\mathbf{a_k}})\Big).$$

On pose $B = \{b_1, \ldots, b_{2^n}\}$ l'ensemble des parties de $\{1, \ldots, n\}$. Ces lettres vont nous permettre de représenter l'ensemble des valeurs de vérités des n prédicats présents dans la signature. Ainsi si le $i^{\text{ème}}$ prédicat est vrai à la position j, alors j doit appartenir à la lettre b en position j. Plus précisément, Un mot de B^n permet de représenter un n-uplet de prédicats $(Q_1, \ldots, Q_n)$ de $\{0, \ldots, n-1\}$ à l'aide de la formule suivante, que l'on note $\mathrm{Repr}(X_{b_1}, \ldots, X_{b_{2^n}}, Q_1, \ldots, Q_n)$:

$$\bigwedge_i^{2^n} \forall x \left((x \in X_{b_i}) \rightarrow \Big(\Big(\bigwedge_{j \in b_i} (x \in Q_j) \Big) \wedge \Big(\bigwedge_{j \notin b_i} (x \notin Q_j) \Big) \Big) \right).$$

Posons la formule pré-close $\theta(X_{b_1}, \ldots, X_{b_{2^n}})$:

$$\forall Q_1 \cdots \forall Q_n\ \mathrm{Repr}(X_{b_1}, \ldots, X_{b_{2^n}}, Q_1, \ldots, Q_n) \rightarrow (\forall u\ \varphi(Q_1, \ldots, Q_n) \leftrightarrow \psi).$$

En particulier, la formule $\theta(\mathbf{b_1}, \ldots, \mathbf{b_{2^n}})$ est un énoncé de $\mathbf{MSO}[<]$ utilisant des prédicats de lettres dans B^*. Elle définit donc un langage régulier K de B^* qui représente tous les prédicats numériques permettant de définir L. De plus, comme $P_1, \ldots, P_n$ définissent K via la formule φ on a que pour tout entier n, $K \cap B^n \neq \emptyset$. On utilise le lemme de sélection régulière (voir le lemme 7.3) pour extraire un langage régulier $C \subseteq K$ tel que pour tout entier n, $C \cap B^n$ contient exactement un élément. On pose $\mathrm{Sel}(X_{b_1}, \ldots, X_{b_{2^n}})$ la formule pré-close telle que le langage C est défini par la formule $\mathrm{Sel}(\mathbf{b_1}, \ldots, \mathbf{b_{2^n}})$. On conclut en posant, pour $i \in \{1, \ldots, n\}$, la formule suivante qui *décode* le $i^{\text{ème}}$ prédicat du langage C :

$$R_i(x) = \forall X_1 \cdots \forall X_{b_{2^n}}\ \mathrm{Sel}(X_{b_1}, \ldots, X_{b_{2^n}}) \rightarrow \bigvee_{i \in b} x \in X_b.$$

Par définition, ces prédicats sont réguliers car définis par une formule de $\mathbf{MSO}[<]$, et la formule $\varphi(R_1, \ldots, R_n)$ définit le langage L par construction. Ce qui conclut la preuve. ■

De ce théorème, on déduit le corollaire suivant qui généralise ce qui est connu pour $\mathbf{FO}[<, \mathcal{A}\mathrm{rb}_1]$ et $(\mathbf{FO} + \mathbf{MOD})[<, \mathcal{A}\mathrm{rb}_1]$.

Corollaire 7.4.

Soit $\mathbf{F}$ un fragment de $\mathbf{MSO}[<]$. Le fragment $\mathbf{F}[\mathcal{A}\mathrm{rb}_1]$ vérifie la conjecture de Straubing.

Démonstration : Soit L un langage régulier définissable dans $\mathbf{F}[\mathcal{A}\mathrm{rb}_1]$. Par définition, il existe des prédicats numériques monadiques $P_1, \ldots, P_n$ et $\varphi(X_1, \ldots, X_n)$ une formule pré-close telle que la formule $\varphi(P_1, \ldots, P_n)$ définit le langage L et appartient au fragment $\mathbf{F}[P_1, \ldots, P_n]$. D'après le théorème précédant, elle vérifie la propriété de substitution. Il existe $R_1, \ldots, R_n$ des prédicats réguliers tels que L est définie par la formule $\varphi(R_1, \ldots, R_n)$. Or comme $\mathbf{F}$ est un fragment, il est stable par substitution atomique (voir la définition 1.5) et donc $\varphi(R_1, \ldots, R_n)$ appartient à $\mathbf{F}[\mathcal{R}\mathrm{eg}]$. Ce qui conclut la preuve. ■

La propriété de substitution implique donc la conjecture de Straubing. Du théorème de Crane Beach pour $\mathbf{MSO}[<, \mathcal{A}\mathrm{rb}_1]$ (voir Théorème 6.24) et de la proposition 6.8, on en déduit le corollaire suivant qui généralise le résultat connu pour $\mathbf{FO}[<, \mathcal{A}\mathrm{rb}_1]$.

Corollaire 7.5.

Soit $\mathbf{F}$ un fragment tel que $\mathbf{F}[\mathcal{R}\mathrm{eg}]$ est équivalent à $\mathbf{F}[\mathrm{LOC}, \mathrm{MOD}]$. Le fragment $\mathbf{F}[\mathcal{A}\mathrm{rb}_1]$ vérifie la propriété de Crane Beach.

Enfin, on déduit également du théorème 7.2 le résultat de transfert suivant.

Corollaire 7.6.

Soient $\mathbf{F}$ et $\mathbf{F}'$ deux fragments de $\mathbf{MSO}$ tels qu'il existe un langage définissable dans $\mathbf{F}[\mathcal{R}\mathrm{eg}]$ qui n'est pas définissable dans $\mathbf{F}'[\mathcal{R}\mathrm{eg}]$. Alors il existe un langage définissable dans $\mathbf{F}[\mathcal{R}\mathrm{eg}, \mathcal{A}\mathrm{rb}_1]$ qui n'est pas définissable dans $\mathbf{F}'[\mathcal{R}\mathrm{eg}, \mathcal{A}\mathrm{rb}_1]$.

D'après la proposition 4.45 et la proposition 4.47, les hiérarchies $\mathcal{B}\mathbf{\Sigma}_k[\mathcal{R}\mathrm{eg}]$ et $\mathbf{FO}^2_k[\mathcal{R}\mathrm{eg}]$ sont strictes. Ce résultat permet donc d'obtenir que les hiérarchies définies par $\mathcal{B}\mathbf{\Sigma}_k[\mathcal{R}\mathrm{eg}, \mathcal{A}\mathrm{rb}_1]$ et $\mathbf{FO}^2_k[\mathcal{R}\mathrm{eg}, \mathcal{A}\mathrm{rb}_1]$ sont strictes.

7.3 Le cas des prédicats non unaires

La propriété de substitution n'est malheureusement pas extensible au cas des prédicats binaires. En effet, la classe de prédicats binaires qui convient pour la formule n'a pas

forcément d'hypothèse de régularité. Nous allons le justifier dans cette section en exhibant un contre-exemple tel qu'un seul choix de prédicats convient. Ce dernier est construit en considérant des formules de **MSO** encodant une *machine de Turing*. Avant d'introduire ces outils et ce contre-exemple, nous allons exposer un problème algorithmique un peu différent de la propriété de substitution mais qui lui est fortement reliée : la *reconnaissance par formule pré-close*

Définition 7.7 (Reconnaissance par formule pré-close).

Soit $\varphi(X_1, \ldots, X_k)$ une formule pré-close de $\mathbf{MSO}[<]$ et L un langage régulier. Le langage L est reconnu par φ s'il existe des prédicats $P_1, \ldots, P_k$ tels que :

(1) Le prédicat P_i à la même arité que la variable X_i pour $1 \leqslant i \leqslant k$.

(2) Le langage L est défini par la formule $\varphi(P_1, \ldots, P_k)$.

De plus si les prédicats $P_1, \ldots, P_k$ sont réguliers, alors on dit que L est reconnu régulièrement par φ.

Le problème de reconnaissance régulière pour un couple (φ, L) consiste à décider si le langage L est reconnu régulièrement par φ.

Nous allons réduire ce problème à celui de *l'arrêt d'une machine de Turing déterministe* [74]. Le modèle des machines de Turing qui va nous intéresser est sans entrée, dispose d'un ruban *infini à droite*, termine sur un ruban vide avec le curseur en position 0, et l'alphabet de bande est binaire (sans compter le symbole blanc). La bande est étiquetée par les entiers et le curseur est initialement en position 0. Soit $\mathcal{M}$ une telle machine de Turing. On note $Q = \{q_0, \ldots, q_p\}$ son ensemble d'états, q_0 son état initial et

$$\delta \subseteq Q \times \{0,1\}^2 \times \{\leftarrow, \rightarrow\} \times Q$$

ses transitions. Le quadruplet $(q, b, b', \rightarrow, q') \in \delta$ signifie que si on lit b sur le ruban en étant dans l'état q, alors on écrit b' et on se déplace à droite. Il en est de même pour la transition $(q, b, b', \leftarrow, q')$ à part qu'on se déplace à gauche. Nous allons pouvoir représenter à l'aide d'une formule l'exécution de la machine de Turing $\mathcal{M}$. Deux informations seront représentées à l'aide de deux prédicats numériques uniformes binaires :

- un prédicat B qui représente le contenu du ruban,
- un prédicat C qui représente la position du curseur.

Plus précisément, $(x, y) \in B$ si la $y^{\text{ème}}$ case du ruban au bout de x itérations contient un 1 ; de même $(x, y) \in C$ si le ruban est en position y au bout de x itérations. Donnons la formule vérifiant que les prédicats B et C représentent l'exécution de $\mathcal{M}$. Les variables monadiques $X_0, \ldots, X_p$ forment une partition telle que $x \in X_i$ si au bout de x itérations la machine de Turing est dans l'état q_i.

Notation : Soit $b \in \{0,1\}$, on pose $\varepsilon_b\varphi$ la formule telle que $\begin{cases} \varepsilon_0\varphi = \neg\varphi \\ \varepsilon_1\varphi = \varphi \end{cases}$.

Les deux formules suivantes forcent les paramètres à bien vérifier les règles imposées par la table de transitions :

$$\varphi_{(q,b,b',\rightarrow,q')}(X_q, X_{q'}) = \forall x\ \exists y\ \Big((x,y) \in C \wedge \varepsilon_b\big((x,y) \in B\big) \wedge x \in X_q\Big) \rightarrow \Big(\varepsilon_{b'}\big((x+1,y) \in B\big) \wedge \big((x+1,x+1) \in C\big) \wedge \big((x+1) \in X_{q'}\big)\Big)$$

$$\varphi_{(q,b,b',\leftarrow,q')}(X_q, X_{q'}) = \forall x\ \exists y\ \Big((x,y) \in C \wedge \varepsilon_b\big((x,y) \in B\big) \wedge x \in X_q)\Big) \rightarrow \Big(\varepsilon_{b'}\big((x+1,y) \in B\big)\big) \wedge \big((x+1,x-1) \in C\big) \wedge \big((x+1) \in X_{q'}\big)\Big)$$

On rappelle que la formule $\mathrm{Part}(X_1, \ldots, X_k)$ vérifie que les variables $X_1, \ldots, X_k$ forment une partition (voir preuve du théorème 7.2). Nous pouvons maintenant donner la formule en question :

$$\varphi_{\mathcal{M}}(B,C) = \forall x \exists y\ \Big((x,y) \in C\Big) \wedge \Big(\forall z\ \big((x,z) \in C\big) \rightarrow (z = y)\Big) \wedge \exists X_0 \cdots \exists X_p\ \Big(\mathrm{Part}(X_0, \ldots, X_p)\Big) \wedge \Big(\min \in X_0\Big) \wedge \Big(\bigwedge_{d \in \delta} \varphi_d(X_q, X_{q'})\Big)$$

Proposition 7.8.

Il existe une machine de Turing $\mathcal{M}$ et des prédicats non réguliers B et C tels que le langage A^* soit défini par $\varphi_{\mathcal{M}}(B,C)$ et tels que pour tout prédicat régulier R, Q le langage défini par $\varphi_{\mathcal{M}}(R,Q)$ soit différent de A^*.

Démonstration : La formule φ accepte tous les mots de A^n si et seulement si les prédicats B, C représentent correctement l'exécution de $\mathcal{M}$ jusqu'à la $n^{\text{ème}}$ itération de $\mathcal{M}$. Le langage A^* est reconnu par φ si et seulement si C, M représentent l'exécution de $\mathcal{M}$. On applique ce résultat à une machine un peu particulière. Pour $\mathcal{M}$ une machine de Turing, on pose $\mathcal{M}'$ la machine de Turing qui à l'exécution de la $x^{\text{ème}}$ itération de $\mathcal{M}$ déplace son curseur sur le $x^{\text{ème}}$ nombre premier puis se replace à sa position initiale. Cette petite modification contraint le prédicat C à être régulier si et seulement si la machine de Turing $\mathcal{M}'$ termine.

Il suffit de prendre une machine de Turing qui ne termine pas pour conclure la preuve. ■

De ce résultat, on déduit également la proposition suivante, d'intérêt indépendant.

Proposition 7.9.

Le problème de reconnaissance régulière est indécidable.

Démonstration : Supposons que le problème de reconnaissance régulière soit décidable et prenons $\mathcal{M}$ une machine de Turing. En reprenant les notations de la preuve de la proposition 7.8, on remarque que $\mathcal{M}$ termine si et seulement si $\mathcal{M}'$ termine. Or $\mathcal{M}'$ termine si et seulement si le prédicat C est régulier. Donc décider le problème de reconnaissance régulière implique que l'on pourrait décider si la machine de Turing $\mathcal{M}$ s'arrête. ■

7.4 La substitution affaiblie

Le principal intérêt de la propriété de substitution est qu'elle permet de prouver la conjecture de Straubing sans passer par les arguments habituels de complexité de circuits. En ce sens, remplacer chaque prédicat par une variable libre du second ordre est un peu exigeant. Un même prédicat peut apparaître à plusieurs endroits dans la formule et communiquer une information à un autre endroit. C'est exactement ce qu'il se passe dans la section précédente. La propriété de *substitution faible* relâche la contrainte de cohérence entre les différentes occurrences d'un même prédicat. Soit $\varphi(X_1, \ldots, X_k)$ une formule pré-close. Une *occurrence* de X_i dans φ est une position de φ où X_i apparaît. On note $\varphi^f(Y_1, \ldots, Y_p)$ la formule pré-close obtenue en renommant par une variable différente chaque occurrence d'une variable libre du second ordre dans φ. On remarque que le nombre de variable augmente nécessairement (mais pas forcément strictement).

Définition 7.10 (Propriété de substitution faible).

Soit $\varphi(X_1, \ldots, X_n)$ une formule pré-close. Cette formule vérifie la propriété de substitution faible si pour tous prédicats $P_1, \ldots, P_n$ tels que le langage L défini par $\varphi(P_1, \ldots, P_n)$ est régulier, il existe des prédicats réguliers $Q_1, \ldots Q_t$ tels que le langage L est également défini par la formule $\varphi^f(Q_1, \ldots, Q_p)$.

La condition ne semble pas beaucoup plus restrictive, et pourtant le contre-exemple de la section précédente ne fonctionne plus. En effet, comme chaque variable libre du second ordre apparaît au plus une fois, il est possible de lui attribuer un *signe*. Si une variable est de *signe positif*, alors en grossissant le nombre d'uplets dans le prédicat on acceptera plus de mots. De même, *si le signe est négatif*, en diminuant le nombre d'uplets dans le prédicat on acceptera plus de mots. Si une formule reconnaît le langage A^*, alors il devient possible de remplacer chaque prédicat par le prédicat qui contient tous les uplets ou par le prédicat qui en contient aucun. Cette simple idée nous donne la proposition ci-dessous.

Proposition 7.11.

Soient φ une formule pré-close et $P_1, \ldots, P_n$ des prédicats numériques. Si le langage A^* est défini par la formule $\varphi(P_1, \ldots, P_n)$, alors il existe des prédicats numériques réguliers $R_1, \ldots, R_p$ tels qu'il est défini par $\varphi^f(Q_1, \ldots Q_p)$.

Il n'est donc pas possible d'obtenir un contre-exemple à la substitution faible de la même manière qu'on en a obtenu un pour la substitution.

7.5 Conjecture de substitution faible

La propriété de substitution faible semble plus raisonnable que la propriété de substitution initiale. Elle traduit l'intuition, peut-être faussée, qu'une formule logique qui définit un langage régulier le fait de *manière régulière.* C'est pourquoi on énonce la conjecture très optimiste suivante :

Conjecture 7.12 (Conjecture de substitution faible).

Toutes les formules pré-closes de **MSO** vérifient la propriété de substitution faible.

La conjecture de substitution faible est très forte (ironiquement) par rapport aux autres conjectures de cette seconde partie de thèse. En particulier, elle implique que tout fragment de **MSO** vérifie la conjecture de Straubing. Elle donnerait également des *preuves logiques* des théorèmes 5.4 et 5.5, ainsi que des preuves pour les conjectures 5.18 et 5.17. Cette question nous oblige à penser des preuves dans un contexte radicalement différent de celui des circuits. Les contraintes syntaxiques semblent difficiles à gérer mais pourraient permettre d'obtenir de nouvelles intuitions sur ces conjectures difficiles. Enfin, on remarquera qu'il n'est pas nécessaire de montrer cette conjecture sur toutes les formules pré-closes de **MSO** afin d'obtenir des résultats intéressants. Par exemple, pour prouver la conjecture 5.18, il suffirait de considérer les formules pré-closes de $\mathbf{FO}^2$.

Bibliographie

[1] Jorge Almeida. A syntactical proof of locality of DA. *Internat. J. Algebra Comput.*, 6(2) :165–177, 1996.

[2] Jorge Almeida. Hyperdecidable pseudovarieties and the calculation of semidirect products. *Internat. J. Algebra Comput.*, 9(3-4) :241–261, 1999.

[3] Jorge Almeida. Some algorithmic problems for pseudovarieties. *Publ. Math. Debrecen*, 54(suppl.) :531–552, 1999. Automata and formal languages, VIII (Salgótarján, 1996).

[4] Jorge Almeida and Ana Escada. On the equation $\mathbf{V} * \mathbf{G} = \mathcal{E}\mathbf{V}$. *J. Pure Appl. Algebra*, 166(1-2) :1–28, 2002.

[5] Jorge Almeida and Pedro V. Silva. On the hyperdecidability of semidirect products of pseudovarieties. *J. Pure Appl. Algebra*, 60 :113–128, 1997.

[6] Jorge Almeida and Benjamin Steinberg. Syntactic and global semigroup theory : a synthesis approach. In *Algorithmic problems in groups and semigroups (Lincoln, NE, 1998)*, Trends Math., pages 1–23. Birkhäuser Boston, Boston, MA, 2000.

[7] Jorge Almeida and Pascal Weil. Relatively free profinite monoids : an introduction and examples. In *Semigroups, formal languages and groups (York, 1993)*, volume 466 of *NATO Sci. Ser. II Math. Phys. Chem.*, pages 73–117. Kluwer Acad. Publ., Dordrecht, 1995.

[8] Karl Auinger. On the decidability of membership in the global of a monoid pseudovariety. *Internat. J. Algebra Comput.*, 20(2) :181–188, 2010.

[9] David A. Mix Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1. *J. Comput. System Sci.*, 38(1) :150 – 164, 1989.

[10] David A. Mix Barrington, Kevin Compton, Howard Straubing, and Denis Thérien. Regular languages in NC^1. *J. Comput. System Sci.*, 44(3) :478–499, 1992.

[11] David A. Mix Barrington, Neil Immerman, Clemens Lautemann, Nicole Schweikardt, and Denis Thérien. First-order expressibility of languages with neutral letters or : The Crane Beach conjecture. *J. Comput. System Sci.*, 70(2) :101–127, 2005.

[12] David A. Mix Barrington and Denis Thérien. Finite monoids and the fine structure of nc^1. *J. ACM*, 35(4) :941–952, 1988.

[13] Janusz A. Brzozowski and Robert Knast. The dot-depth hierarchy of star-free languages is infinite. *J. Comput. System Sci.*, 16(1) :37–55, 1978.

[14] Janusz A. Brzozowski and Imre Simon. Characterizations of locally testable events. *Discrete Math.*, 4 :243–271, 1973.

[15] Julius R. Büchi. Weak second-order arithmetic and finite automata. *Z. Math. Logik Grundlagen Math.*, 6 :66–92, 1960.

[16] Olivier Carton. *Langages formels, calculabilité et complexité*. Vuibert, 2008. 240 pages.

[17] Ashok K. Chandra, Steven Fortune, and Richard J. Lipton. Lower bounds for constant depth circuits for prefix problems. In Josep Diaz, editor, *Automata, Languages and Programming*, volume 154 of *Lect. Notes Comp. Sci.*, pages 109–117. Springer Berlin Heidelberg, 1983.

[18] Ashok K. Chandra, Steven Fortune, and Richard J. Lipton. Unbounded fan-in circuits and associative functions. *J. Comput. Syst. Sci.*, 30(2) :222–234, 1985.

[19] Laura Chaubard. *Méthodes algébriques pour les langages formels*. Phd dissertation, Université Paris Diderot, 2007.

[20] Laura Chaubard, Jean-Eric Pin, and Howard Straubing. Actions, Wreath Products of C-varieties and Concatenation Product. *Theoret. Comput. Sci.*, 356 :73–89, 2006.

[21] Laura Chaubard, Jean-Éric Pin, and Howard Straubing. First order formulas with modular predicates. In *21st Annual IEEE Symposium on Logic in Computer Science (LICS 2006)*, pages 211–220. IEEE, 2006.

[22] Alfredo Costa and Ana Escada. Some operators that preserve the locality of a pseudovariety of semigroups. *Internat. J. Algebra Comput.*, 23(3) :583–610, 2013.

[23] Luc Dartois and Charles Paperman. Two-variable first order logic with modular predicates over words. In Natacha Portier and Thomas Wilke, editors, *International Symposium on Theoretical Aspects of Computer Science (STACS)*, LIPIcs, pages 329–340, Dagstuhl, Germany, 2013. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik.

[24] Volker Diekert, Paul Gastin, and Manfred Kufleitner. A survey on small fragments of first-order logic over finite words. *Internat. J. Found. Comput. Sci.*, 19(3) :513–548, 2008.

[25] Samuel Eilenberg. *Automata, languages, and machines. Vol. B*. Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976. With two chapters by Bret Tilson, Pure and Applied Mathematics, Vol. 59.

[26] Zoltán Ésik and Masami Ito. Temporal logic with cyclic counting and the degree of aperiodicity of finite automata. *Acta Cybernet.*, 16(1) :1–28, 2003.

[27] Nathanaël Fijalkow and Charles Paperman. Monadic second-order logic with arbitrary monadic predicates. In *Mathematical Foundations of Computer Science 2014 - 39th International Symposium, MFCS 2014, Budapest, Hungary, August 25-29, 2014. Proceedings, Part I*, pages 279–290, 2014.

[28] Merrick L. Furst, James B. Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. *J. Math. Systems Theory*, 17(1) :13–27, 1984.

[29] Kurt Gödel. Über formal unentscheidbare Sätze der *principia mathematica* und verwandter Systeme. I. *Monatsh. Math.*, 149(1) :1–30, 2006. Reprinted from Monatsh. Math. Phys. **3**8 (1931), 173–198 [MR1549910], With an introduction by Sy-David Friedman.

[30] James A. Green. On the structure of semigroups. *Ann. of Math. (2)*, pages 163–172, 1951.

[31] Yuri Gurevich and Harry R. Lewis. A logic for constant-depth circuits. *Information and Control*, 61(1) :65–74, 1984.

[32] Johan T. Hastad. *Computational limitations of small depth circuits*. PhD thesis, Massachusetts Institute of Technology, 1986.

[33] Neil Immerman. Languages that capture complexity classes. *SIAM J. Comput.*, 16(4) :760–778, 1987.

[34] Jiří Kaďourek. On the locality of the pseudovariety **dg**. *J. Inst. Math. Jussieu*, 7(1) :93–180, 2008.

[35] Hans W. Kamp. *Tense Logic and the Theory of Linear Order*. University Microfilms, 1968.

[36] Stephen C. Kleene. Representation of events in nerve nets and finite automata. In *Automata studies*, Ann. of Math. Stud, no. 34, pages 3–41. Princeton University Press, Princeton, N. J., 1956.

[37] Robert Knast. A semigroup characterization of dot-depth one languages. *RAIRO Theor. Inform. Appl.*, 17(4) :321–330, 1983.

[38] Michal Koucký. Circuit complexity of regular languages. *Theory Comput. Syst.*, 45(4) :865–879, 2009.

[39] Michal Koucký, Clemens Lautemann, Sebastian Poloczek, and Denis Thérien. Circuit Lower Bounds via Ehrenfeucht-Fraissé Games. In *IEEE Conference on Computational Complexity*, pages 190–201, 2006.

[40] Michal Koucký, Pavel Pudlák, and Denis Thérien. Bounded-depth circuits : Separating wires from gates. In *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, STOC '05, pages 257–265, New York, NY, USA, 2005. ACM.

[41] Andreas Krebs and Howard Straubing. An effective characterization of the alternation hierarchy in two-variable logic. In Deepak D'Souza, Telikepalli Kavitha, and Jaikumar Radhakrishnan, editors, *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2012)*, volume 18 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 86–98, Dagstuhl, Germany, 2012. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[42] Kenneth Krohn and John Rhodes. Algebraic theory of machines. I. Prime decomposition theorem for finite semigroups and machines. *Trans. Amer. Math. Soc.*, 116 :450–464, 1965.

[43] Manfred Kufleitner and Alexander Lauser. Lattices of logical fragments over words. In Artur Czumaj, Kurt Mehlhorn, Andrew Pitts, and Roger Wattenhofer, editors, *Automata, Languages, and Programming*, volume 7392 of *Lect. Notes Comp. Sci.*, pages 275–286. Springer Berlin Heidelberg, 2012.

[44] Manfred Kufleitner and Alexander Lauser. Quantifier alternation in two-variable first-order logic with successor is decidable. In *International Symposium on Theoretical Aspects of Computer Science (STACS)*, pages 305–316, 2013.

[45] Manfred Kufleitner and Pascal Weil. The FO^2 alternation hierarchy is decidable. In *Computer science logic 2012*, volume 16 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages 426–439. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2012.

[46] Leonid Libkin. *Elements of Finite Model Theory.* Springer, 2004.

[47] Alexis Maciel, Pierre Péladeau, and Denis Thérien. Programs over semigroups of dot-depth one. *Theoret. Comput. Sci.*, 245(1) :135–148, 2000. Semigroups and algebraic engineering (Fukushima, 1997).

[48] Robert McNaughton and Seymour Papert. *Counter-free automata.* The M.I.T. Press, Cambridge, Mass.-London, 1971.

[49] Pierre Péladeau. Logically defined subsets of $\mathbf{N}^k$. *Theoret. Comput. Sci.*, 93(2) :169–183, 1992.

[50] Jean-Éric Pin. *Semigroup2.* `http://www.liafa.univ-paris-diderot.fr/~jep/Logiciels/Semigroupe2.0/semigroupe2.html`.

[51] Jean-Éric Pin. *Mathematical Foundations of Automata Theory.* Unpublished manuscript, `http://www.liafa.univ-paris-diderot.fr/~jep/PDF/MPRI/MPRI.pdf`, 2014.

[52] Jean-Éric Pin and Howard Straubing. Some results on $\mathcal{C}$-varieties. *Theoret. Informatics Appl.*, 39(1) :239–262, 2005.

[53] Jean-Éric Pin and Pascal Weil. Polynomial closure and unambiguous product. *Theory Comput. Syst.*, 30(4) :383–422, 1997.

[54] Thomas Place and Marc Zeitoun. Going higher in the first-order quantifier alternation hierarchy on words. In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *Automata, Languages, and Programming*, volume 8573 of *Lect. Notes Comp. Sci.*, pages 342–353. Springer Berlin Heidelberg, 2014.

[55] Frank P. Ramsey. On a Problem of Formal Logic. *Proc. London Math. Soc.*, S2-30(1) :264, 1930.

[56] Alexander A. Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Math. Notes of the Soviet Academy of Sciences*, 41(4) :333–338, 1987.

[57] John Rhodes and Benjamin Steinberg. *The q-theory of finite semigroups.* Springer Monographs in Mathematics. Springer, New York, 2009.

[58] Marcel-Paul Schützenberger. On finite monoids having only trivial subgroups. *Information and Control*, 8 :190–194, 1965.

[59] Imre Simon. Piecewise testable events. In *Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975)*, volume 33 of *Lect. Notes Comp. Sci.*, pages 214–222. Springer, Berlin, 1975.

[60] Roman Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, STOC '87, pages 77–82, New York, NY, USA, 1987. ACM.

[61] Benjamin Steinberg. Finite state automata : a geometric approach. *Trans. Amer. Math. Soc.*, 353(9) :3409–3464 (electronic), 2001.

[62] Howard Straubing. Families of recognizable sets corresponding to certain varieties of finite monoids. *J. Pure Appl. Algebra*, 15(3) :305–318, 1979.

[63] Howard Straubing. Finite semigroup varieties of the form $V * D$. *J. Pure Appl. Algebra*, 36(1) :53–94, 1985.

[64] Howard Straubing. The wreath product and its applications. In *Formal properties of finite automata and applications (Ramatuelle, 1988)*, volume 386 of *Lect. Notes Comp. Sci.*, pages 15–24, Berlin, 1989. Springer.

[65] Howard Straubing. Constant-depth periodic circuits. *Internat. J. Algebra Comput.*, 1(1) :49–87, 1991.

[66] Howard Straubing. *Finite automata, formal logic, and circuit complexity.* Birkhäuser Boston Inc., Boston, MA, 1994.

[67] Howard Straubing. On logical descriptions of regular languages. In *LATIN 2002 : Theoretical informatics*, volume 2286 of *Lect. Notes Comp. Sci.*, pages 528–538. Springer, Berlin, 2002.

[68] Howard Straubing and Denis Thérien. Weakly iterated block products of finite monoids. In *LATIN 2002 : Theoretical informatics (Cancun)*, volume 2286 of *Lect. Notes Comp. Sci.*, pages 91–104. Springer, Berlin, 2002.

[69] Howard Straubing and Denis Thérien. Regular languages defined by generalized first-order formulas with a bounded number of bound variables. *Theory Comput. Syst.*, 36(1) :29–69, 2003.

[70] Howard Straubing, Denis Thérien, and Wolfgang Thomas. Regular languages defined with generalized quanifiers. *Inf. Comput.*, 118(2) :289–301, 1995.

[71] Denis Thérien and Thomas Wilke. Over words, two variables are as powerful as one quantifier alternation. In *STOC '98 (Dallas, TX)*, pages 234–240. ACM, New York, 1999.

[72] Wolfgang Thomas. Classifying regular events in symbolic logic. *J. Comput. System Sci.*, 25(3) :360–376, 1982.

[73] Bret Tilson. Categories as algebra : an essential ingredient in the theory of monoids. *J. Pure Appl. Algebra*, 48(1-2) :83–198, 1987.

[74] Alan M. Turing. On Computable Numbers, with an Application to the Entscheidungsproblem. *Proc. London Math. Soc.*, S2-42(1) :230, 30.

[75] Philipp Weis and Neil Immerman. Structure theorem and strict alternation hierarchy for FO^2 on words. *Log. Methods Comput. Sci.*, 5(3) :3 :4, 23, 2009.

[76] Celia Wrathall. Rudimentary predicates and relative computation. *SIAM J. Comput.*, 7(2) :194–209, 1978.