

Mémoire

Auteur : Rossetto, Marie

Promoteur(s) : Charlier, Emilie; Whiteland, Markus

Faculté : Faculté des Sciences

Diplôme : Master en sciences mathématiques, à finalité didactique

Année académique : 2022-2023

URI/URL : <http://hdl.handle.net/2268.2/17763>

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.



FACULTÉ DES SCIENCES
DÉPARTEMENT DE MATHÉMATIQUE

Décidabilité pour les mots sturmiens

Mémoire de fin d'études présenté en vue de l'obtention du titre de
Master en Sciences Mathématiques, à finalité didactique

Année académique 2022–2023

Auteur :
Marie ROSSETTO

Promotrice :
Émilie CHARLIER

Co-Promoteur :
Markus WHITELAND

Remerciements

Je tiens tout d'abord à remercier chaleureusement ma promotrice Émilie Charlier pour m'avoir donné l'opportunité de travailler sur cet intéressant sujet, ainsi que mon co-promoteur Markus Whitheland pour s'être lancé dans l'aventure avec nous. Ils ont tous les deux su se rendre disponibles pour relire mon mémoire, m'aider à travers nos discussions sur le sujet et me prodiguer de judicieux conseils à chaque fois que j'en avais besoin. Je suis également reconnaissante d'avoir eu la chance de les avoir comme professeurs et d'avoir pu développer mes connaissances en mathématiques discrètes auprès d'eux.

Je remercie également Gentiane Haesbroeck, Michel Rigo et Jean-Pierre Schneiders pour prendre part au jury. Ils ont chacun apporté une contribution importante à ma formation et ont marqué mon parcours universitaire.

Merci aussi à mon frère, Vincent, qui n'a jamais refusé de m'aider quand j'avais besoin de lui. Ses conseils pour m'aider à installer le logiciel Pecan m'ont été précieux. Je pense également à mes parents qui m'ont toujours encouragée à aller au bout de ce que j'entreprends. Leur soutien sans faille m'a réellement aidée tout au long de mes études.

Je remercie également mon amie Mara pour sa relecture et son soutien moral.

Finalement, merci à mes amis du B37 qui ont su égayer ces cinq années d'études, et ce, même dans les moments difficiles. Cette aventure académique n'aurait pas été la même sans eux. Je tiens, en particulier, à remercier Delphine. Mes sessions de travail n'auraient pas été aussi productives sans elle et j'ai la chance de toujours pouvoir compter sur elle.

Table des matières

Remerciements	1
1 Introduction	3
2 Notions de base	6
2.1 ω -régularité	6
2.2 Représentations binaires	8
2.3 Représentations d'Ostrowski	8
3 Codage binaire	17
3.1 Ordre et alignement sur H_∞	17
3.2 Codage binaire des fractions continues	21
3.3 Codage binaire des représentations d'Ostrowski	26
4 Acceptation de l'addition	34
4.1 Addition de représentations d'Ostrowski	34
4.2 Addition de codages binaires de représentations d'Ostrowski	42
5 Structures et décidabilité	49
5.1 Structures ω -régulières	49
5.2 La structure \mathcal{R}_α	50
5.3 Décidabilité de propriétés des mots sturmiens	67
6 Le logiciel Pecan	70
6.1 Addition de codages binaires de représentations d'Ostrowski	72
6.2 Mots sturmiens	74
7 Pour aller plus loin	78
Lexique	80
Bibliographie	82

Chapitre 1

Introduction

Les mots sturmiens sont des objets mathématiques bien connus de la combinatoire des mots. La première personne à s'être intéressée à eux est Jean Bernouilli III en 1771 [4]. Cependant, c'est seulement en 1940 que Gustav Arnold Hedlund et Marston Morse ont réalisé la première étude approfondie de ces mots [18] et les ont nommés en l'honneur du mathématicien Jacques Charles François Sturm. De nombreuses propriétés ont été abordées par Ethan Coven et Gustav Arnold Hedlund [6] en 1973. En 2002, un groupe de mathématiciens, nommé M.Lothaire [17], s'est intéressé aux propriétés sur ces mots, ainsi qu'à l'équivalence entre différentes caractérisations.

Ici, nous définissons les mots sturmiens de la manière suivante : soient un irrationnel α et un réel ρ . Le mot sturmien de pente α et d'intercept ρ est le mot $c_{\alpha,\rho} = c_{\alpha,\rho}(1)c_{\alpha,\rho}(2)\cdots$ défini sur l'alphabet $\{0, 1\}$ tel que

$$c_{\alpha,\rho}(n) = \lfloor (n+1)\alpha + \rho \rfloor - \lfloor n\alpha + \rho \rfloor - \lfloor \alpha \rfloor$$

pour tout $n \in \mathbb{N}$. Quand ρ vaut zéro, on parle du mot caractéristique de pente α .

Nous notons $\mathcal{N}_{\alpha,\rho}$ la structure $(\mathbb{N}, <, +, 0, 1, n \mapsto c_{\alpha,\rho}(n))$ qui est l'extension de l'arithmétique de Presburger [11] par un mot sturmien interprété comme une fonction unaire. Le but de ce mémoire, à l'instar de l'article [13] qui l'a fortement inspiré, est de démontrer que la théorie du premier ordre de la collection de telles extensions est décidable. Autrement dit, nous allons prouver que les théories du premier ordre de

$$\mathcal{K}_{\text{sturm}} = \{\mathcal{N}_{\alpha,\rho} : \alpha \in \text{Irr}, \rho \in \mathbb{R}\} \text{ et } \mathcal{K}_{\text{car}} = \{\mathcal{N}_{\alpha,0} : \alpha \in \text{Irr}\}.$$

sont décidables, où Irr est l'ensemble $]0, 1[\setminus \mathbb{Q}$.

Or, nous verrons que, pour tout $\alpha \in \text{Irr}$, pour tout $\rho \in \mathbb{R}$, la structure $\mathcal{N}_{\alpha,\rho}$ est définissable dans la structure

$$\mathcal{R}_\alpha = (\mathbb{R}, <, +, \mathbb{Z}, \alpha \mathbb{Z}).$$

En toute généralité, \mathcal{R}_α est défini pour $\alpha \in \mathbb{R}_0^+$.

Certains résultats de décidabilité autour de la structure \mathcal{R}_α sont déjà connus. Par exemple, nous savons que la théorie du premier ordre $\text{FO}(\mathcal{R}_\alpha)$ est décidable si α est rationnel [26] ou irrationnel quadratique [12]. Pour prouver ce deuxième résultat, il a en fait été démontré que \mathcal{R}_α est une structure ω -régulière lorsque α est irrationnel quadratique. Or, lorsqu'une structure est ω -régulière, alors la théorie du premier ordre de cette structure est décidable [5]. C'est dans cette même optique que nous allons établir, dans ce travail, un lien entre ω -régularité et décidabilité.

Dans ce mémoire, nous allons prouver que la théorie du premier ordre de

$$\mathcal{K} = \{\mathcal{R}_\alpha : \alpha \in \text{Irr}\}$$

est décidable. Pour cela, nous allons démontrer qu'il existe une famille de structures ω -régulières telle que \mathcal{R}_α est isomorphe à une structure de la famille pour tout $\alpha \in \text{Irr}$. Or, nous verrons également que si $(\mathcal{U}_z)_{z \in Z}$ est une famille uniforme de structures ω -régulières, alors la théorie du premier ordre de $\{\mathcal{U}_z : z \in Z\}$ est décidable.

On dit que $(\mathcal{U}_z)_{z \in Z}$ est une famille uniforme de structures ω -régulières est si

- l'ensemble $\{(z, y) : z \in Z, y \in U_z\}$ est ω -régulier, et
- l'ensemble $\{(z, y_1, \dots, y_{ar(i)}) : z \in Z, (y_1, \dots, y_{ar(i)}) \in R_{i,z}\}$ est ω -régulier pour tout $i \in \{1, \dots, m\}$.

où m est un naturel, Z est un ensemble, ar est une fonction qui à un élément de $\{1, \dots, m\}$ associe un naturel et, pour tout $z \in Z$, \mathcal{U}_z est la structure $(U_z; R_{1,z}, \dots, R_{m,z})$ telle que $R_{i,z} \subseteq U_z^{ar(i)}$.

On parle d' ω -régularité pour des mots infinis qui sont acceptés par des automates de Büchi. Ceux-ci fonctionnent comme des automates classiques, à l'exception près qu'il faut introduire un nouveau critère d'acceptation qui permet de travailler avec des mots infinis. Il est possible de vérifier que le langage accepté par un automate de Büchi (construit sur un alphabet Σ) est vide [2] ou contient l'ensemble de tous les mots infinis sur Σ [9]. Cela permet de vérifier qu'il existe un mot qui vérifie une propriété donnée ou qu'une propriété est vraie pour tous les mots infinis sur Σ .

Il y a un élément clef qui nous permettra d'utiliser cette notion d' ω -régularité à travers nos résultats de décidabilité et cet élément est un automate [3] qui permet de réaliser des additions de naturels dans les systèmes de numération d'Ostrowski. Le but, par après, sera de passer d'une addition et d'un ordre sur les naturels (dans les systèmes de numérations d'Ostrowski) à une addition et un ordre sur les réels (dans \mathcal{R}_α).

C'est pourquoi, nous allons également nous intéresser aux représentations d'Ostrowski [1], ainsi qu'aux fractions continues [24] qui permettent de définir les systèmes de numération d'Ostrowski.

Cependant, un facteur qui pourrait s'avérer être problématique est le fait que les représentations d'Ostrowski sont définies sur un alphabet infini : les naturels. Si nous souhaitons construire un automate qui permet de réaliser des additions dans les systèmes de numération d'Ostrowski, alors cela nous amène à potentiellement travailler avec un nombre infini d'arcs, ce qui, en pratique, nécessiterait des ressources infinies. Ainsi, pour éviter ce problème d'alphabet infini, nous allons introduire une manière de coder en binaire les fractions continues et les représentations d'Ostrowski.

Finalement, nous allons nous intéresser au logiciel Pecan [20] : une implémentation de l'algorithme qui décide $\mathcal{K}_{\text{sturm}}$ et \mathcal{K}_{car} . Pecan se base sur des automates de Büchi afin de représenter des prédicats logiques. Nous nous en servons pour vérifier automatiquement certaines propriétés sur les mots sturmiens et caractéristiques.

Chapitre 2

Notions de base

Dans ce chapitre nous allons introduire les concepts de bases qui nous seront utiles pour la compréhension de ce travail : l' ω -régularité, les représentations binaires et les représentations d'Ostrowski.

2.1 ω -régularité

Nous savons qu'un mot fini peut être accepté par automate fini si, en le lisant, le dernier état visité est final. Lorsque nous commençons à travailler avec des mots infinis, nous devons utiliser un autre critère d'acceptation. C'est pourquoi nous introduisons les automates de Büchi qui fonctionnent comme les automates classiques, mais où le critère d'acceptation nécessite de passer infiniment souvent par des états finals. De plus, des automates de Büchi découlent la notion d' ω -régularité qui est un concept clef de ce travail.

Soit un ensemble non vide Σ appelé **alphabet**. On note Σ^ω l'ensemble des mots infinis sur Σ . Nous notons ε le mot vide.

Définition 2.1.1. Un **automate de Büchi** est un tuple $\mathcal{A} = (Q, \Sigma, \Delta, I, F)$ où Q est un ensemble d'états, Σ est un alphabet fini, $\Delta \subseteq Q \times \Sigma \times Q$ est une relation de transition, $I \subseteq Q$ est l'ensemble d'états initiaux et $F \subseteq Q$ est l'ensemble d'états finals.

Soit $\mathcal{A} = (Q, \Sigma, \Delta, I, F)$ un automate de Büchi.

- Soient $\sigma = \sigma_0\sigma_1\sigma_2\cdots \in \Sigma^\omega$ et $p \in Q$. Un **chemin** de σ à partir de p est une suite $s = (s_i)_{i \geq 0}$ d'états de Q telle que $s_0 = p$ et $(s_n, \sigma_n, s_{n+1}) \in \Delta$ pour tout $n \in \mathbb{N}$.
- On dit que σ est **accepté par \mathcal{A}** s'il existe s un chemin de σ à partir d'un état initial tel que l'ensemble $\{n : s_n \in F\}$ est infini. Dans ce cas, s est appelé un **chemin acceptant**.
- On note $L(\mathcal{A})$ l'ensemble des mots acceptés par \mathcal{A} .

Un sous-ensemble X de Σ^ω est ω -régulier si $X = L(\mathcal{A})$ où \mathcal{A} est un automate de Büchi. Dans ce cas, on dit que X est **accepté** par \mathcal{A} .

Un **automate de Büchi à n bandes** est un automate de Büchi $(Q, \Sigma, \Delta, I, F)$ où la relation de transition Δ est incluse dans $Q \times \Sigma^n \times Q$.

Dans ce cas, si $\sigma = (\sigma_1, \dots, \sigma_n) \in (\Sigma^\omega)^n$ où $\sigma_i = \sigma_{i,0}\sigma_{i,1}\sigma_{i,2}\dots$ pour tout $i \in \{1, \dots, n\}$, et si $p \in Q$, alors un **chemin** de σ à partir de p est une suite $s = (s_i)_{i \geq 0}$ d'états de Q telle que $s_0 = p$ et $(s_k, (\sigma_{1,k}, \dots, \sigma_{n,k}), s_{k+1}) \in \Delta$ pour tout $k \in \mathbb{N}$.

Un sous-ensemble X de $(\Sigma^\omega)^n$ est ω -régulier si $X = L(\mathcal{A})$ où \mathcal{A} est un automate de Büchi à n bandes. Dans ce cas, on dit que X est **accepté** par \mathcal{A} .

Proposition 2.1.2. L' ω -régularité est stable par union, intersection, complémentaire et projection.

Démonstration. Si A et B sont deux ensembles ω -réguliers, alors il existe deux automates de Büchi $\mathcal{A} = (Q_1, \Sigma, \Delta_1, I_1, F_1)$ et $\mathcal{B} = (Q_2, \Sigma, \Delta_2, I_2, F_2)$ qui acceptent respectivement A et B . Nous allons commencer par prouver la stabilité par union. Quitte à renommer les états (pour obtenir deux ensembles d'états distincts), l'automate $(Q_1 \cup Q_2, \Sigma, \Delta_1 \cup \Delta_2, I_1 \cup I_2, F_1 \cup F_2)$ accepte l'ensemble $A \cup B$. Ainsi $A \cup B$ est ω -régulier.

Démontrons maintenant la stabilité par intersection. On considère l'automate $\mathcal{P} = (Q_1 \times Q_2 \times \{1, 2\}, \Sigma, \Delta, I, F)$ où

- $\Delta = \Delta' \cup \Delta''$

où

$$\Delta' = \left\{ \begin{array}{l} ((q_1, q_2, 1), a, (p_1, p_2, i)) \mid \\ (q_1, a, p_1) \in \Delta_1, (q_2, a, p_2) \in \Delta_2, i = \begin{cases} 2 & \text{si } q_1 \in F_1 \\ 1 & \text{sinon} \end{cases} \end{array} \right\},$$

$$\Delta'' = \left\{ \begin{array}{l} ((q_1, q_2, 2), a, (p_1, p_2, i)) \mid \\ (q_1, a, p_1) \in \Delta_1, (q_2, a, p_2) \in \Delta_2, i = \begin{cases} 1 & \text{si } q_2 \in F_2 \\ 2 & \text{sinon} \end{cases} \end{array} \right\},$$

- $I = I_1 \times I_2 \times \{1\}$,
- $F = \{(q_1, q_2, 2) \mid q_2 \in F_2\}$.

Ainsi, \mathcal{P} accepte l'ensemble $A \cap B$. En effet, on passe un nombre infini de fois par des états de F si et seulement si des états de F_2 et 2 apparaissent infiniment souvent en deuxième et troisième composante respectivement. Or, en passant par un tel état, on transite vers un état avec 1 sur sa troisième composante. De plus, comme 2 apparaît infiniment souvent en troisième composante, on va forcément transiter vers un état ayant un 2 sur sa troisième composante, et cela se produit si et seulement s'il y a un état de F_1 sur la première composante. Le même mécanisme se répète indéfiniment et c'est pourquoi des états de F_1 et des états de F_2 apparaissent infiniment souvent en première et deuxième composante respectivement. Donc $A \cap B$ est ω -régulier.

Pour la preuve de la stabilité par complémentaire, nous nous référons à ce qui a été démontré dans le livre [22].

Finalement, nous prouvons la stabilité par projection. Si C un sous ensemble de $(\Sigma^\omega)^n$ est ω -régulier, alors il existe \mathcal{C} un automate de Büchi à n bandes qui accepte C . Soit $k \in \{1, \dots, n\}$. Considérons l'ensemble C_k qui est une projection de l'ensemble C . Alors, si on prend l'automate \mathcal{C} et qu'on retire la k -ème bande des transitions, cet automate accepte l'ensemble C_k . Donc l' ω -régularité est stable par projection. \square

2.2 Représentations binaires

Nous définissons la représentation binaire des nombres naturels de manière à commencer par le chiffre de poids faible.

Notation 2.2.1. Soit un mot $w = w_0 \cdots w_n$ tel que $w_i \in \{0, 1\}$ pour tout $i \geq 0$. On note $[w]_2$ la valeur $\sum_{i=0}^n w_i 2^i$. De plus, $[w]_2$ est unique pour un w donné.

Exemple 2.2.2. Considérons le mot binaire $w = 1011$. Alors, on a

$$[w]_2 = 1.2^0 + 0.2^1 + 1.2^2 + 1.2^3 = 1 + 4 + 8 = 13.$$

Définition 2.2.3. Soit N un naturel. On dit que $b = b_0 \cdots b_n \in \{0, 1\}^n$ est une **représentation binaire** de N si $N = [b]_2$. Une représentation binaire de N est unique à des zéros de queue près.

Exemple 2.2.4. Considérons le naturel $N = 13$. Alors, une représentation binaire de N est 1011 ou encore 101100.

2.3 Représentations d'Ostrowski

Dans cette section, nous allons introduire le système de numération d'Ostrowski. Il repose sur le développement en fraction continue d'un irrationnel.

Définitions 2.3.1. Une **fraction continue finie** est une expression de la forme

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_k}}}}$$

où $a_0 \in \mathbb{Z}$ et $a_i \in \mathbb{N}_0$ pour tout $i \in \{1, \dots, k\}$. Elle est notée $[a_0; a_1, \dots, a_k]$.

Soit α un réel. On dit que $[a_0; a_1, \dots, a_k, \dots]$ est le **développement en fraction continue (ou la fraction continue)** de α si $\alpha = \lim_{k \rightarrow +\infty} [a_0; a_1, \dots, a_k]$ et si $a_0 \in \mathbb{Z}$ et $a_i \in \mathbb{N}_0$ pour tout $i > 0$. On note $\alpha = [a_0; a_1, \dots]$. Pour tout k , les éléments a_k sont appelés les **coefficients** de la fraction continue.

Nous pourrions nous demander si la définition de fraction continue a du sens. En effet, à priori, nous ne savons pas si la limite converge et si c'est le cas, à quelles conditions. Cependant, nous pouvons assurer la convergence via la proposition [23, Théorème 3.1.1] suivante :

Proposition 2.3.2. Toute fraction continue est convergente.

De plus, chaque nombre irrationnel possède un unique développement en fraction continue et réciproquement, chaque développement en fraction continue correspond à un unique irrationnel [24, Ch. I-§2].

N'importe quel rationnel r peut être écrit sous forme de deux fractions continues finies différentes. Une des deux représentations est plus grande que l'autre d'un terme et les deux représentations diffèrent uniquement sur le dernier terme pour la plus petite et les deux derniers pour la plus grande [24, Ch. I-§2]. En effet, on a

$$r = [a_0; a_1, \dots, a_{k-1}, a_k + 1] = [a_0; a_1, \dots, a_k, 1].$$

Pour trouver les fractions continues finies d'un rationnel, il suffit de réaliser successivement des divisions euclidiennes jusqu'à obtenir un reste égal à zéro.

Exemple 2.3.3. Développons le rationnel $\frac{-1}{3}$ en fraction continue finie. Nous avons

$$\frac{-1}{3} = -1 + \frac{2}{3} = -1 + \frac{1}{\frac{3}{2}} = -1 + \frac{1}{1 + \frac{1}{2}} = -1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}$$

Ainsi, on obtient que $\frac{-1}{3} = [-1; 1, 2] = [-1; 1, 1, 1]$.

Considérons maintenant le nombre irrationnel $\sqrt{2}$. On a

$$\sqrt{2} = 1 + \sqrt{2} - 1 = 1 + \frac{(\sqrt{2} - 1)(\sqrt{2} + 1)}{\sqrt{2} + 1} = 1 + \frac{1}{1 + \sqrt{2}}.$$

Ainsi, nous pouvons substituer $\sqrt{2}$ par $1 + \frac{1}{1 + \sqrt{2}}$.

$$\sqrt{2} = 1 + \frac{1}{1 + \sqrt{2}} = 1 + \frac{1}{1 + 1 + \frac{1}{1 + \sqrt{2}}} = 1 + \frac{1}{2 + \frac{1}{1 + \sqrt{2}}}.$$

En répétant plusieurs fois cette manipulation, on obtient :

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\ddots + \frac{1}{2 + \frac{1}{1 + \sqrt{2}}}}}}$$

Nous pouvons en déduire le développement en fraction continue de $\sqrt{2}$. En effet, on a

$$\sqrt{2} = [1; 2, 2, 2, \dots].$$

Définition 2.3.4. Soit un nombre irrationnel $\alpha = [a_0; a_1, \dots]$. Le développement en fraction continue de α est :

- **ultimement périodique** de période p s'il existe $r \in \mathbb{N}_0$ tel que, pour tout $i \geq r$, on a $a_i = a_{i+p}$. Dans ce cas, on note $\alpha = [a_0; a_1, \dots, a_{r-1}, \overline{a_r, \dots, a_{r+p-1}}]$;
- **purement périodique** de période p si, pour tout $i \geq 0$, on a $a_i = a_{i+p}$. Dans ce cas, on note $\alpha = [\overline{a_0, \dots, a_{p-1}}]$.

Proposition 2.3.5 (Théorème de Lagrange). Si $\alpha \in \mathbb{R}$, alors α est un nombre quadratique irrationnel si et seulement si le développement en fraction continue de a est ultimement périodique.

La proposition ci-dessus a été démontrée dans [14, p. 603–622].

Proposition 2.3.6. Soient des irrationnels α et α' tels que $\alpha = [a_0; a_1, \dots]$ et $\alpha' = [a'_0; a'_1, \dots]$. Soit k le plus petit naturel tel que $a_k \neq a'_k$. On a $\alpha < \alpha'$ si et seulement si

- k est pair et $a_k < a'_k$, ou
- k est impair et $a_k > a'_k$.

Démonstration. Procédons par récurrence sur k . Si $k = 0$, alors $a_0 \neq a'_0$. De plus, puisque $[0; a_1, a_2, \dots], [0; a'_1, a'_2, \dots] < 1$, alors nous avons

$$\begin{aligned} a_0 < a'_0 &\Leftrightarrow [a_0; 0, \dots] < [a'_0; 0, \dots] \\ &\Leftrightarrow [a_0; a_1, \dots] < [a'_0; a'_1, \dots] \\ &\Leftrightarrow \alpha < \alpha'. \end{aligned}$$

Supposons maintenant que $k = 1$. Ainsi, puisque $a_0 = a'_0$ par hypothèse, nous avons

$$\begin{aligned} \alpha < \alpha' &\Leftrightarrow [a_0; a_1, \dots] < [a'_0; a'_1, \dots] \\ &\Leftrightarrow [0; a_1, \dots] < [0; a'_1, \dots] \\ &\Leftrightarrow \frac{1}{[a_1; a_2, \dots]} < \frac{1}{[a'_1; a'_2, \dots]}. \end{aligned}$$

De plus, comme $a_1, a'_1 \in \mathbb{N}_0$, alors $[a_1; a_2, \dots], [a'_1; a'_2, \dots] > 1$. Il en découle que

$$\frac{1}{[a_1; a_2, \dots]} < \frac{1}{[a'_1; a'_2, \dots]} \Leftrightarrow [a_1; a_2, \dots] > [a'_1; a'_2, \dots].$$

Or, nous savons par hypothèse que $a_1 \neq a'_1$. Donc, par le cas précédent, nous pouvons en déduire que

$$[a_1; a_2, \dots] > [a'_1; a'_2, \dots] \Leftrightarrow a_1 > a'_1.$$

Supposons maintenant que $k > 1$ et que la thèse est vérifiée pour tout indice strictement inférieur à k . Par hypothèse, nous savons que $a_0 = a'_0$. Via le même raisonnement qu'au cas précédent, nous pouvons en déduire que

$$\alpha < \alpha' \Leftrightarrow [a_1; a_2, \dots] > [a'_1; a'_2, \dots].$$

Or, nous savons que $a_j = a'_j$ pour tout $j \in \{1, \dots, k-1\}$ et que $a_k \neq a'_k$. En appliquant l'hypothèse de récurrence, nous obtenons

$$\begin{aligned} [a_1; a_2, \dots] > [a'_1; a'_2, \dots] &\Leftrightarrow \begin{cases} a_k > a'_k & \text{si } k-1 \text{ est pair,} \\ a_k < a'_k & \text{si } k-1 \text{ est impair.} \end{cases} \\ &\Leftrightarrow \begin{cases} a_k > a'_k & \text{si } k \text{ est impair,} \\ a_k < a'_k & \text{si } k \text{ est pair.} \end{cases} \end{aligned}$$

□

Définitions 2.3.7. Soit $\alpha = [a_0; a_1, \dots]$ un irrationnel. Pour tout $k \geq 0$, le k -ème convergent de α est donné par

$$[a_0; a_1, \dots, a_k]$$

et peut être réécrit sous forme de fraction irréductible $\frac{p_k}{q_k}$ telle que $p_k \in \mathbb{Z}$, $q_k \in \mathbb{N}_0$. Pour tout $k \geq 0$, la k -ème différence β_k de α est donnée par $\alpha q_k - p_k$.

Posons $p_{-1} = 1$, $p_0 = a_0$, $q_{-1} = 0$ et $q_0 = 1$.

Proposition 2.3.8. Pour tout $n \geq 1$, on a

$$\begin{cases} p_n = a_n p_{n-1} + p_{n-2} \\ q_n = a_n q_{n-1} + q_{n-2} \end{cases}$$

La proposition ci-dessus est démontrée dans [24, Ch. I-§1].

Proposition 2.3.9. Pour tout $n \in \mathbb{N}$, on a

1. $\beta_n > 0$ si et seulement si n est pair.
2. $\beta_0 > -\beta_1 > \beta_2 > -\beta_3 > \dots$
3. $-\beta_n = a_{n+2}\beta_{n+1} + a_{n+4}\beta_{n+3} + a_{n+6}\beta_{n+5} + \dots$

La proposition ci-dessus est démontrée dans [1, Théorème 2.4.5].

Exemple 2.3.10. Prenons l'irrationnel $\sqrt{2} = [1; \bar{2}]$ (voir l'exemple 2.3.3). Alors, nous obtenons les valeurs suivantes :

$p_{-1} = 1$	$q_{-1} = 0$
$p_0 = a_0 = 1$	$q_0 = 1$
$p_1 = 2.1 + 1 = 3$	$q_1 = 2.1 + 0 = 2$
$p_2 = 2.3 + 1 = 7$	$q_2 = 2.2 + 1 = 5$
$p_3 = 2.7 + 3 = 17$	$q_3 = 2.5 + 2 = 12$

Ainsi, en développant la fraction $\frac{p_3}{q_3}$, nous obtenons bien le 3-ème convergent de $\sqrt{2}$. En effet, nous avons

$$\frac{p_3}{q_3} = \frac{17}{12} = 1 + \frac{1}{\frac{12}{5}} = 1 + \frac{1}{2 + \frac{1}{\frac{5}{2}}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}.$$

De plus, nous pouvons calculer les premières k -èmes différences.

$$\begin{aligned}\beta_0 &= \sqrt{2} - 1 \approx 0,414 > 0, \\ \beta_1 &= 2\sqrt{2} - 3 \approx -0,172 < 0, \\ \beta_2 &= 5\sqrt{2} - 7 \approx 0,071 > 0, \\ \beta_3 &= 12\sqrt{2} - 17 \approx -0,029 < 0.\end{aligned}$$

Pour la suite de cette section, nous considérons un irrationnel $\alpha \in]0, 1[$ et nous notons $[0; a_1, a_2, \dots]$ son développement en fraction continue. Nous allons maintenant montrer comment nous pouvons représenter un naturel dans le système de numération d'Ostrowski. Notons que cette représentation commence par le chiffre de poids faible.

La proposition suivante est démontrée dans [1, Théorème 3.9.1].

Proposition 2.3.11. Soit $X \in \mathbb{N}$. Alors, il existe un naturel N tel que X peut être écrit sous la forme

$$X = \sum_{n=0}^N b_{n+1}q_n \tag{2.1}$$

où

1. $0 \leq b_1 < a_1$,
2. $0 \leq b_{n+1} \leq a_{n+1}$ pour tout $n \geq 1$,
3. $b_n = 0$ quand $b_{n+1} = a_{n+1}$ pour tout $n \geq 1$.

La proposition qui précède est démontrée dans [1, Théorème 3.9.1].

Définition 2.3.12. Pour X entier vérifiant l'équation (2.1), on note

$$X = [b_1 b_2 \cdots b_{N+1}]_\alpha$$

et X est appelé **la α -valeur** de $b_1 b_2 \cdots b_{N+1}$. Si, en plus, X est naturel et vérifie les contraintes qui sont associées à l'équation (2.1), alors le mot $b_1 b_2 \cdots b_{N+1}$ est appelé **une α -représentation d'Ostrowski** de X .

Cette représentation est unique à des zéros de queue près. Quand on prend la représentation sans zéro de queue, on parle de **la α -représentation d'Ostrowski** de X .

La représentation sans zéro de queue peut être obtenue par un algorithme glouton en maximisant les b_i un par un (en parcourant les indices i dans l'ordre décroissant et en commençant par un indice plus grand ou égal à k où k est l'indice maximal tel que $q_{k-1} \leq X$) de manière à respecter l'équation (2.1) et les contraintes qui lui sont associées.

Exemple 2.3.13. Prenons $X = 30$ et $\alpha = [0; 13, 12, \bar{1}] = \frac{3429+\sqrt{5}}{44878}$. Calculons les premiers termes de la suite $(q_i)_{i \geq -1}$.

$$\begin{aligned} q_{-1} &= 0, \\ q_0 &= 1, \\ q_1 &= 13 \cdot 1 + 0 = 13, \\ q_2 &= 12 \cdot 13 + 1 = 157, \\ q_3 &= 1 \cdot 157 + 13 = 170. \end{aligned}$$

Ainsi, on peut écrire X en respectant la décomposition donnée par l'équation (2.1) et ses contraintes :

$$\begin{aligned} X = 30 &= 1 \cdot b_1 + 13 \cdot b_2 + 157 \cdot b_3 + 170 \cdot b_4 + \dots, \\ 0 &\leq b_1 < 13, \\ 0 &\leq b_2 \leq 12, \\ 0 &\leq b_3 \leq 1, \\ 0 &\leq b_4 \leq 1, \dots \end{aligned}$$

Puisque $X < 157$ et $X < 170$, alors $b_3 = 0$ et $b_4 = 0$. Ensuite, on choisit une valeur maximale pour b_2 telle que le terme $13 \cdot b_2$ soit plus petit ou égal à 30 et que $0 \leq b_2 \leq 12$, c'est pourquoi on prend 2 comme valeur pour b_2 . Et finalement, pour que la décomposition soit correcte, il faut que $1 \cdot b_1$ soit égal à 4, on choisit donc $b_1 = 4$. Ainsi, on a que

$$30 = [4 \ 2 \ 0 \ 0]_\alpha$$

et que 4 2 0 0 est une α -représentation d'Ostrowski de 30 et 4 2 est la α -représentation d'Ostrowski de 30.

Définition 2.3.14. Soit \preceq un ordre total sur un alphabet Σ .

- L'**ordre lexicographique** correspondant sur Σ^* est notée \preceq_{lex} . Pour tout $w, v \in \Sigma^*$, on a $w \prec_{\text{lex}} v$ s'il existe un naturel l tel que $w_l \prec v_l$ et que, pour tout $i < l$, on a $w_i = v_i$.
- L'**ordre co-lexicographique** correspondant sur Σ^* est notée \preceq_{colex} . Pour tout $w, v \in \Sigma^*$, on a $w \prec_{\text{colex}} v$ s'il existe un naturel l maximal tel que $w_l \neq v_l$ et $w_l \prec v_l$.

Remarque 2.3.15. Soient $X, Y \in \mathbb{N}$. Il existe N tel que

$$\begin{aligned} X &= [b_1 b_2 \cdots b_{N+1}]_\alpha, \\ Y &= [c_1 c_2 \cdots c_{N+1}]_\alpha. \end{aligned}$$

On a $X < Y$ si et seulement si $b_1 b_2 \cdots b_{N+1} <_{\text{colex}} c_1 c_2 \cdots c_{N+1}$. Cela découle directement de l'algorithme glouton qui permet de déterminer une α -représentation d'Ostrowski d'un nombre naturel.

Nous allons maintenant montrer comment nous pouvons représenter un réel dans le système de numération d'Ostrowski. Cette représentation est très similaire à celle des naturels que nous avons décrite précédemment. Notons que cette représentation, à l'instar de celle des naturels, commence par le chiffre de poids faible. Nous allons restreindre l'ensemble des réels à un intervalle de taille 1 (que nous noterons I_α). Si nous voulions considérer tous les réels, il suffirait d'ajouter un chiffre au début de la représentation et cela nous permettrait de décaler l'intervalle considéré.

Notations 2.3.16. Soit un irrationnel α . Notons

$$I_\alpha = [\lfloor \alpha \rfloor - \alpha, 1 + \lfloor \alpha \rfloor - \alpha[.$$

On remarque que tout réel x peut être associé à un unique élément j de I_α tel que la différence $x - j$ équivaut à un entier. On note

$$f_\alpha : \mathbb{R} \rightarrow I_\alpha$$

la fonction qui, à un réel x , associe $x - u$ où u est l'unique entier tel que $x - u \in I_\alpha$.

La proposition suivante est démontrée dans [24, Ch. II.§6 Théorème 1].

Proposition 2.3.17. Soit $x \in I_\alpha$. Alors x peut être écrit de manière unique sous la forme

$$x = \sum_{n=0}^{+\infty} b_{n+1} \beta_n \tag{2.2}$$

où $b_n \in \mathbb{Z}$, $0 \leq b_n \leq a_n$ et $b_n = 0$ quand $b_{n+1} = a_{n+1}$ pour tout $n \geq 1$, $b_1 \neq a_1$ et $b_n \neq a_n$ pour une infinité de n impairs.

Définition 2.3.18. Pour $x \in I_\alpha$ vérifiant l'équation (2.2), on note

$$x = [b_1 b_2 \cdots]_\alpha$$

et x est appelé **la α -valeur** de $b_1 b_2 \cdots$. Si, en plus, x vérifie les contraintes qui sont associées à l'équation (2.2), alors le mot $b_1 b_2 \cdots$ est appelé la **α -représentation d'Ostrowski** de x .

Cette représentation peut être obtenue par un algorithme glouton en optimisant les b_i un par un (en parcourant les indices i dans l'ordre croissant).

Exemple 2.3.19. Soit $\alpha = \sqrt{2} - 1 = [0; \bar{2}]$ (voir exemple 2.3.3). Alors, on a

$$I_\alpha = \left[1 - \sqrt{2}; 2 - \sqrt{2} \right[.$$

Nous calculons les valeurs suivantes :

k	q_k	p_k	β_k
-1	0	1	
0	1	0	$\sqrt{2} - 1$
1	2	1	$2\sqrt{2} - 3$
2	5	2	$5\sqrt{2} - 7$
3	12	5	$12\sqrt{2} - 17$
4	29	12	$29\sqrt{2} - 41$
5	70	29	$70\sqrt{2} - 99$
6	169	70	$169\sqrt{2} - 239$

Prenons $x = \sqrt{3} - 2 \approx -0,267949 \in I_\alpha$. Ainsi, on peut écrire x en respectant la décomposition donnée par l'équation (2.2) et ses contraintes :

$$x = (\sqrt{2} - 1).b_1 + (2\sqrt{2} - 3).b_2 + (5\sqrt{2} - 7).b_3 + (12\sqrt{2} - 17).b_4 + (29\sqrt{2} - 41).b_5 + (70\sqrt{2} - 99).b_6 + (169\sqrt{2} - 239).b_7 + \dots$$

Au vu des contraintes, nous savons que pour tout $k \in \mathbb{N}_0$, nous avons $b_k \in \{0, 1, 2\}$. Comme $\sqrt{2} - 1$ est positif et que x est négatif, nous prenons b_1 égal à 0 pour minimiser l'erreur entre x et $(\sqrt{2} - 1).b_1$.

Ensuite, nous nous intéressons à b_2 . Nous testons les différentes valeurs possibles pour b_2 et choisissons celle qui minimise l'erreur.

b_2	Valeur de $ x - (\sum_{n=0}^1 b_{n+1}\beta_n) $ (arrondie à 3 décimales)
0	0,268
1	0,096
2	0,075

Nous constatons que l'erreur est minimisée si nous prenons 2 comme valeur pour b_2 . Nous testons maintenant les différentes valeurs pour b_3 .

b_3	Valeur de $ x - (\sum_{n=0}^2 b_{n+1}\beta_n) $ (arrondie à 4 décimales)
0	0,0752
1	0,0041
2	0,0669

Nous constatons que l'erreur est minimisée si nous prenons 1 comme valeur pour b_3 . Nous procédons de manière similaire pour chaque indice et nous pouvons obtenir que les valeurs optimales pour b_4, b_5, b_6 et b_7 son respectivement 0, 0, 0 et 2. Avec ces valeurs, nous avons

$$\sum_{n=0}^6 b_{n+1}\beta_n \approx -0,26789.$$

Nous avons ainsi obtenu que 0 2 1 0 0 0 2 est le début de l' α -représentation d'Ostrowski de $\sqrt{3} - 2$.

La proposition suivante est prouvée dans [12, Lemma 3.4].

Proposition 2.3.20. Soit $X \in \mathbb{N}$ tel que $b_1 b_2 \cdots b_{N+1}$ est une α -représentation d'Ostrowski de X . Alors, on a

$$f_\alpha(\alpha X) = \sum_{k=0}^{+\infty} b_{k+1} \beta_k$$

et $b_1 b_2 \cdots$ est la α -représentation d'Ostrowski de $f_\alpha(\alpha X)$ où $b_k = 0$ pour tout $k > N + 1$.

La proposition suivante est prouvée dans [12, Fact 2.13].

Proposition 2.3.21. Soient deux réels distincts $x, y \in I_\alpha$ tels que

$$x = [b_1 b_2 \dots]_\alpha \quad \text{et} \quad y = [c_1 c_2 \dots]_\alpha.$$

Soit le plus petit naturel k tel que $b_k \neq c_k$. Alors $x < y$ si et seulement si

$$\begin{cases} b_k < c_k & \text{si } k \text{ est pair,} \\ b_k > c_k & \text{si } k \text{ est impair.} \end{cases}$$

Chapitre 3

Codage binaire

Dans ce chapitre, nous allons montrer comment nous pouvons coder en binaire un développement en fraction continue et une représentation d'Ostrowski d'un naturel ou d'un réel. Pour cela, nous allons d'abord introduire l'ensemble H_∞ qui nous permettra de séparer avec un $\#$ les différents coefficients dans notre codage.

3.1 Ordre et alignement sur H_∞

Dans cette section, nous allons discuter de H_∞ et des manières d'ordonner deux mots de cet ensemble. Nous allons aussi nous assurer de préserver une notion d' ω -régularité dans ces différents concepts.

Notons

- $\Sigma_\#$ l'alphabet $\{0, 1, \#\}$ et H_∞ l'ensemble des mots infinis sur $\Sigma_\#$ qui commencent par $\#$ et dans lesquels $\#$ apparaît une infinité de fois,
- $\mathbb{N}_\#$ l'alphabet $\mathbb{N} \cup \{\#\}$ et \mathbb{N}_∞ l'ensemble des mots infinis sur $\mathbb{N}_\#$ qui commencent par $\#$ et dans lesquels $\#$ apparaît une infinité de fois.

Remarquons que H_∞ est ω -régulier. En effet, l'automate représentée par la figure 3.1 accepte les mots de H_∞ . Notons qu'un état final est représenté par un double cercle.

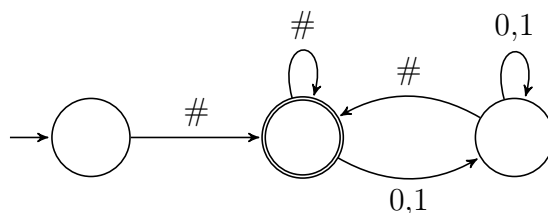


FIGURE 3.1 – Automate de Büchi acceptant H_∞

Définition 3.1.1. Soit $u \in H_\infty$. Alors u est de la forme suivante :

$$\#u_1\#u_2\#u_3\#\dots$$

où $u_i \in \{0, 1\}^*$ pour tout $i > 0$. Définissons la fonction

$$[\cdot]_2 : H_\infty \rightarrow \mathbb{N}_\infty : u = \#u_1\#u_2\#u_3\#\dots \mapsto \#[u_1]_2\#[u_2]_2\#[u_3]_2\#\dots$$

Malgré des notations similaires, le contexte dans lequel on travaille nous permet de distinguer aisément les fonctions $[\cdot]_2 : \{0, 1\}^* \rightarrow \mathbb{N}$ et $[\cdot]_2 : H_\infty \rightarrow \mathbb{N}_\infty$. Le choix d'indicer à partir de 1 les mots entre deux $\#$ permet de simplifier la manière de définir les concepts d'ordre qui suivent.

Exemple 3.1.2. Considérons le mot $w = \#001\#010(\#101)^\omega$. Alors, on a

$$[w]_2 = \#4\#2(\#5)^\omega.$$

Définition 3.1.3. Soit \leq l'ordre sur \mathbb{N} . Soient $u, v \in H_\infty$ tels que

$$u = \#u_1\#u_2\#\dots \quad \text{et} \quad v = \#v_1\#v_2\#\dots$$

- L'**ordre lexicographique binaire** correspondant sur H_∞ est noté $\leq_{\text{lex},2}$. On a $u <_{\text{lex},2} v$ s'il existe un naturel l tel que $[u_l]_2 < [v_l]_2$ et que, pour tout $i < l$, on a $[u_i]_2 = [v_i]_2$;
- L'**ordre co-lexicographique binaire** correspondant sur H_∞ est noté $\leq_{\text{colex},2}$. On a $u <_{\text{colex},2} v$ s'il existe un naturel l maximal tel que $[u_l]_2 \neq [v_l]_2$ et $[u_l]_2 < [v_l]_2$;
- L'**ordre lexicographique alterné binaire** correspondant sur H_∞ est noté $\leq_{\text{alex},2}$. On a $u <_{\text{alex},2} v$ s'il existe un k minimal tel que $[u_k]_2 \neq [v_k]_2$ et que $[u_k]_2 < [v_k]_2$ si k est pair, ou $[u_k]_2 > [v_k]_2$ si k est impair.

Exemple 3.1.4. Soient les mots $u = (\#1110)^\omega$, $v = (\#10110)^\omega$ et $w = \#10\#101(\#1110)^\omega$. Ainsi, on a

$$[u]_2 = (\#7)^\omega, \quad [v]_2 = (\#13)^\omega \quad \text{et} \quad [w]_2 = \#1\#5(\#7)^\omega.$$

Et comme $[u_1]_2 < [v_1]_2$, alors $u <_{\text{lex},2} v$. De plus, $[w_2]_2 < [u_2]_2$, donc $w <_{\text{colex},2} u$. On peut également observer que $u <_{\text{alex},2} w$, car $[u_1]_2 > [w_1]_2$.

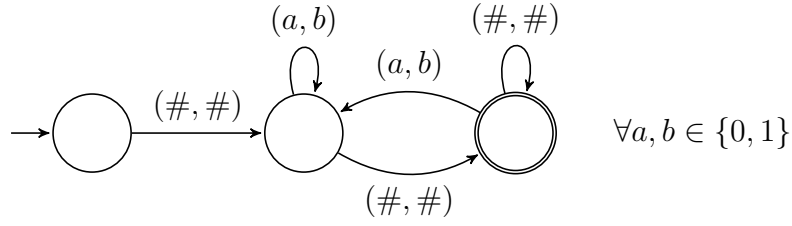
Définition 3.1.5. Soient $u, v \in \Sigma_\#^\omega$. On dit que u et v sont **alignés** si pour tout $i \geq 1$, la i -ème lettre de u est $\#$ si et seulement si la i -ème lettre de v est $\#$.

On dit que le tuple $(w_1, \dots, w_n) \in (\Sigma_\#^\omega)^n$ est **aligné** si les w_i sont deux à deux alignés.

Un ensemble $X \in (\Sigma_\#^\omega)^n$ est dit **aligné** si tous les éléments de X sont alignés.

Définition 3.1.6. On définit la relation $\sim_\#$ sur $\Sigma_\#^\omega$ telle que, pour tout $u, v \in \Sigma_\#^\omega$,

$$u \sim_\# v \text{ si } u \text{ et } v \text{ sont alignés.}$$

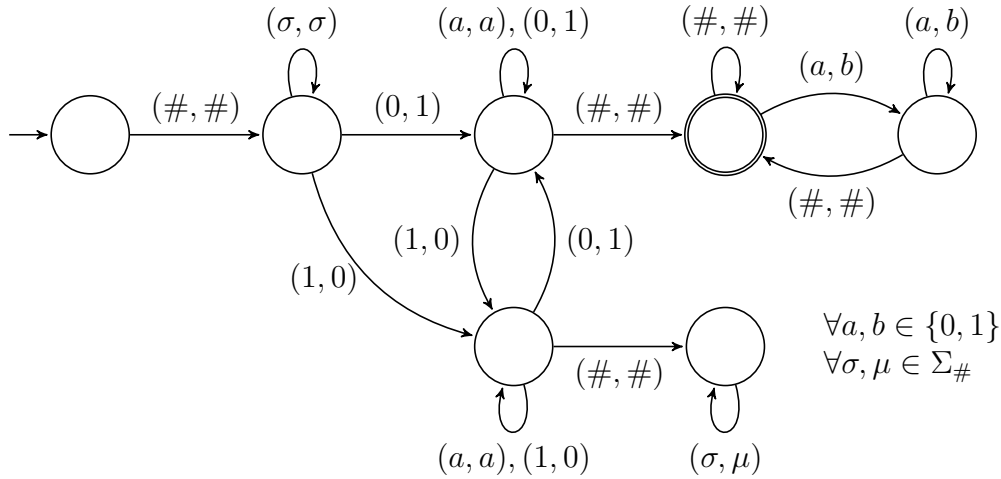

 FIGURE 3.2 – Automate de Büchi acceptant l'ensemble des couples de mots de H_∞ alignés

Remarquons que $\sim_\#$ est une relation d'équivalence. De plus, cette relation est ω -régulière. En effet, l'automate représenté dans la figure 3.2 accepte les couples $(u, v) \in H_\infty^2$ si et seulement si u et v sont alignés.

Proposition 3.1.7. Les ensembles suivants sont ω -réguliers :

1. $\{(u, v) \in H_\infty^2 : u \sim_\# v, u <_{\text{lex},2} v\}$,
2. $\{(u, v) \in H_\infty^2 : u \sim_\# v, u <_{\text{colex},2} v\}$,
3. $\{(u, v) \in H_\infty^2 : u \sim_\# v, u <_{\text{alex},2} v\}$.

Démonstration. Prouvons que le premier ensemble est ω -régulier. Il suffit de construire un automate de Büchi qui accepte l'ensemble des couples de mots alignés (u, v) de H_∞^2 si $u <_{\text{lex},2} v$. Or, l'automate représenté dans la figure 3.3 accepte exactement l'ensemble de ces couples de mots.


 FIGURE 3.3 – Automate de Büchi acceptant l'ensemble des couples de mots alignés (u, v) de H_∞ si $u <_{\text{lex},2} v$

Prouvons que le deuxième ensemble est ω -régulier. L'automate représenté dans la figure 3.4 accepte l'ensemble des couples de mots alignés (u, v) de H_∞^2 si $u <_{\text{colex},2} v$.

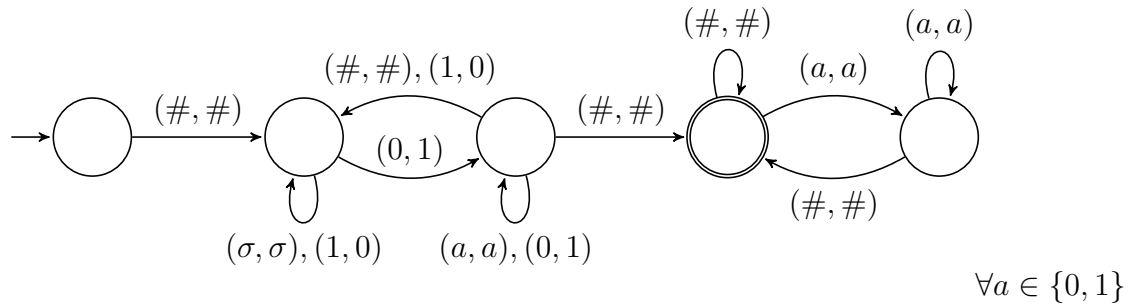


FIGURE 3.4 – Automate de Büchi acceptant l'ensemble des couples de mots alignés (u, v) de H_∞ si $u <_{\text{colex}, 2} v$

Finalement démontrons que le troisième ensemble est ω -régulier. L'automate représenté dans la figure 3.5 accepte l'ensemble des couples de mots alignés (u, v) de H_∞^2 si $u <_{\text{alex}, 2} v$.

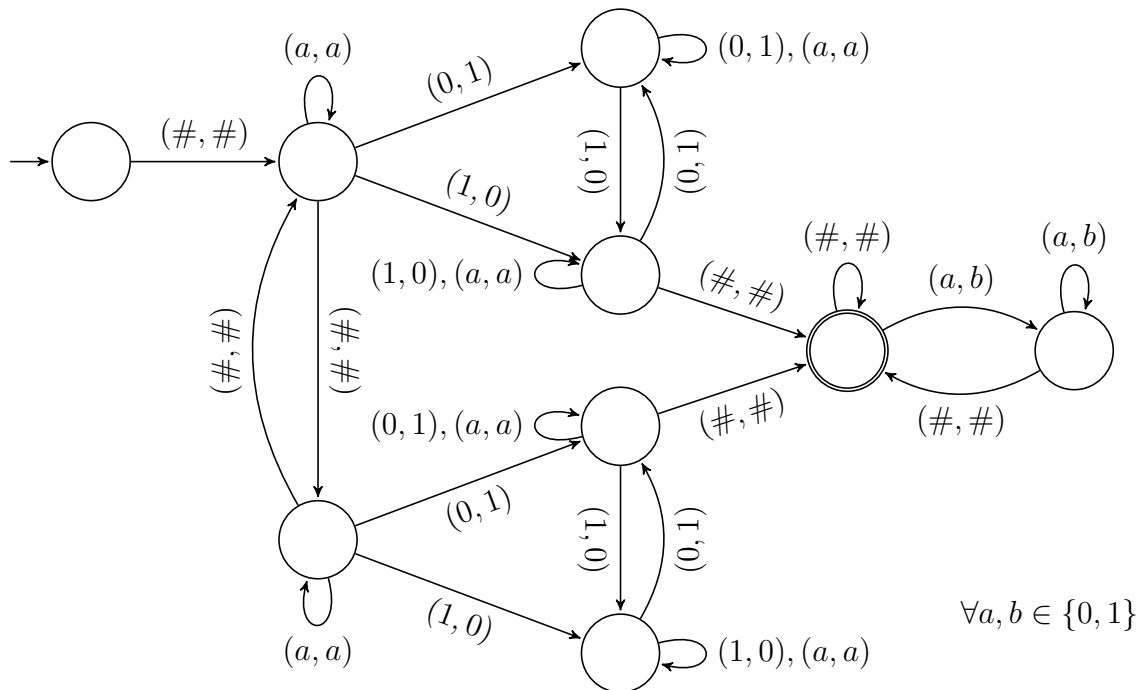


FIGURE 3.5 – Automate de Büchi acceptant l'ensemble des couples de mots alignés (u, v) de H_∞ si $u <_{\text{alex}, 2} v$

□

3.2 Codage binaire des fractions continues

Dans cette section, nous allons montrer de quelle manière nous pouvons coder en binaire des développements en fraction continue d'irrationnels. Afin de distinguer les codages de chaque coefficient de la fraction continue, nous les séparons par le symbole #. Ainsi, nous transformons nos fractions continues en mots de H_∞ .

Définition 3.2.1. Soit un nombre irrationnel $\alpha \in]0, 1[$ tel que son développement en fraction continue est $[0; a_1, a_2, \dots]$. On dit que

$$\#u_1\#u_2\#u_3\#\dots$$

est un **#-codage binaire du développement en fraction continue** de α si $[u_i]_2 = a_i$ pour tout $i \geq 1$.

Puisque, pour tout $i \geq 1$, les coefficients a_i d'une fraction continue $[0; a_1, a_2, \dots]$ sont des naturels non nuls, alors les codages en binaire de ces coefficients doivent au moins contenir chacun un 1. C'est pour cela que nous allons introduire l'ensemble R .

Notation 3.2.2. Notons R l'ensemble des mots infinis sur $\Sigma_\#$ de la forme $(\#(0|1)^*1(0|1)^*)^\omega$.

Remarquons que l'ensemble R est ω -régulier. En effet, l'automate de Büchi représenté dans la figure 3.6 accepte R .

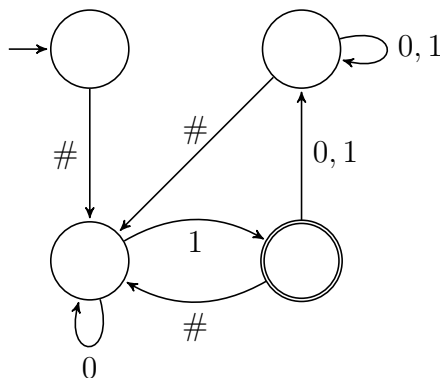


FIGURE 3.6 – Automate de Büchi acceptant R

Nous allons démontrer que chaque mot de R est en fait le codage binaire d'un irrationnel de $]0, 1[$.

Lemme 3.2.3. Si $w \in R$, alors il existe un unique irrationnel $\alpha \in]0, 1[$ tel que w est un #-codage binaire de la fraction continue de α .

Démonstration. Si $w \in R$, alors

$$w = \#w_1\#w_2\#\dots$$

où $w_i \in \{0, 1\}^*$ tel que w_i contienne au moins un 1 pour tout $i \geq 1$.

Posons $a_i = [w_i]_2$ pour tout $i \geq 1$. Comme les w_i contiennent au moins un 1, alors les a_i diffèrent de zéro.

Ainsi, si on prend $\alpha = [0; a_1, a_2, \dots]$, alors α existe par convergence des fractions continues (Proposition 2.3.2) et w est un $\#$ -codage binaire du développement en fraction continue de α .

De plus, l'unicité de α découle directement de l'unicité de la valeur d'une représentation binaire et de l'unicité du développement en fraction continue d'un nombre irrationnel. \square

Définition 3.2.4. Pour $w \in R$, on définit $\alpha(w)$ l'unique irrationnel $\alpha \in]0, 1[$ tel que w est un $\#$ -codage binaire de la fraction continue de α .

Si $v = (v_1, \dots, v_n) \in R^n$, alors on note $\alpha(v)$ pour désigner $(\alpha(v_1), \dots, \alpha(v_n))$.

Exemple 3.2.5. Si $w = \#1101\#001010(\#1)^\omega$, alors $\alpha(w) = [0; 11, 20, \bar{1}]$.

Nous pouvons remarquer que, pour un irrationnel α donné, il existe plusieurs codages binaires de α . En effet, chaque coefficient du développement en fraction continue de α peut être codé en binaire de manière unique à des zéros de queue près. Donc, la représentation binaire va dépendre du nombre de caractères qu'on veut allouer à chaque coefficient. Dans certains cas, on veut pouvoir travailler avec l'ensemble des représentations d'un irrationnel (qui ne diffèrent que par des zéros de queue pour chaque coefficient). C'est pourquoi nous allons introduire le concept de zéro-fermeture.

Définition 3.2.6. Soit $X \subseteq R^n$. La **zéro-fermeture** de X est donnée par l'ensemble

$$\{u \in R^n : \exists v \in X : \alpha(u) = \alpha(v)\}.$$

Exemple 3.2.7. Considérons le singleton $X = \{\#100(\#101)^\omega\}$. Alors, la zéro fermeture de X est l'ensemble des mots de la forme suivante :

$$\#10^*(\#1010^*)^\omega.$$

Lemme 3.2.8. Soit un ensemble $X \subseteq R^n$ aligné. Si X est ω -régulier, alors la zéro-fermeture de X est ω -régulière.

Démonstration. Comme X est ω -régulier, il existe un automate de Büchi \mathcal{A} qui accepte X . Notons Q les états de \mathcal{A} et Δ l'ensemble des transitions.

Modifions l'automate \mathcal{A} pour construire un automate \mathcal{B} qui accepte la zéro-fermeture de X .

1. Pour toutes les transitions $(p, (\#, \dots, \#), q) \in \Delta$, on ajoute un nouvel état $\mu(p, q)$, ainsi que les transitions

$$(p, (0, \dots, 0), \mu(p, q)), (\mu(p, q), (0, \dots, 0), \mu(p, q)) \text{ et } (\mu(p, q), (\#, \dots, \#), q).$$

2. Si un état q est accessible à partir d'un état p en lisant $(0, \dots, 0)^m(\#, \dots, \#)$ où $m > 0$, alors on ajoute un état $\nu(p, q)$ ainsi que les transitions $(p, (\#, \dots, \#), \nu(p, q))$. Pour tout mot $t \in (\Sigma_{\#})^n$ et pour tout état $r \in Q$ tels que $(q, t, r) \in \Delta$, on ajoute la transition $(\nu(p, q), t, r)$.

De plus, si le chemin emprunté pour aller de p à q contient un état final, alors, on ajoute $\nu(p, q)$ aux états finals.

Notons \mathcal{B} ce nouvel automate, Q' ses états et Δ' ses transitions.

Montrons que la zéro-fermeture de X est $L(\mathcal{B})$. Procédons par double inclusion.

Soit $v \in X$, alors v est aligné et v est accepté par \mathcal{A} . Soit $w \in R^n$ tel que w est aligné et $\alpha(v) = \alpha(w)$. Ainsi w appartient à la zéro-fermeture de X .

On sait que v et w sont respectivement de la forme

$$\begin{pmatrix} \#v_{1,1}\#v_{1,2}\#\cdots \\ \#v_{2,1}\#v_{2,2}\#\cdots \\ \vdots \\ \#v_{n,1}\#v_{n,2}\#\cdots \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \#w_{1,1}\#w_{1,2}\#\cdots \\ \#w_{2,1}\#w_{2,2}\#\cdots \\ \vdots \\ \#w_{n,1}\#w_{n,2}\#\cdots \end{pmatrix}.$$

où $v_{i,j}, w_{i,j} \in \{0, 1\}^*$ pour tout $i \in \{1, \dots, n\}$ et pour tout $j > 0$.

Nous pouvons remarquer que, comme v est aligné, alors $|v_{1,j}| = |v_{i,j}|$ pour tout $i \in \{1, \dots, n\}$ et pour tout $j > 0$. De même manière, puisque w est aligné, alors $|w_{1,j}| = |w_{i,j}|$ pour tout $i \in \{1, \dots, n\}$ et pour tout $j > 0$.

De plus, puisque $\alpha(v) = \alpha(w)$, alors on a $[v_{i,j}]_2 = [w_{i,j}]_2$ pour tout $i \in \{1, \dots, n\}$ et pour tout $j > 0$. Ainsi, pour tout $i \in \{1, \dots, n\}$ et pour tout $j > 0$, nous avons que $v_{i,j}$ et $w_{i,j}$ diffèrent uniquement par des zéros de queue.

Comme $v \in X$, il existe $s = s_1s_2\cdots \in Q^\omega$ un chemin de v qui est un chemin acceptant dans \mathcal{A} . Construisons $s' = s'_1s'_2\cdots \in (Q')^\omega$ un chemin de w qui est un chemin acceptant dans \mathcal{B} .

Pour tout $i > 0$, posons

$$\begin{aligned} y(i) &= \text{position du } i\text{-ème } (\#, \dots, \#) \text{ dans } v, \\ z(i) &= \text{position du } i\text{-ème } (\#, \dots, \#) \text{ dans } w. \end{aligned}$$

Pour tout $i > 0$, on va définir la suite d'états $s'_{z(i)+1} \cdots s'_{z(i+1)}$ de la manière suivante :

Si $|w_{1,i}| = |v_{1,i}|$: alors $w_{j,i} = v_{j,i}$ pour tout $j \in \{1, \dots, n\}$. Posons

$$s'_{z(i)+1} \cdots s'_{z(i+1)} = s_{y(i)+1} \cdots s_{y(i+1)}.$$

Si $|w_{1,i}| > |v_{1,i}|$: alors $w_{j,i} = v_{j,i}0^{|w_{1,i}|-|v_{1,i}|}$ pour tout $j \in \{1, \dots, n\}$. Posons

$$s'_{z(i)+1} \cdots s'_{z(i+1)} = s_{y(i)+1} \cdots s_{y(i+1)-1} (\mu(s_{y(i+1)-1}, s_{y(i+1)}))^{|w_{1,i}|-|v_{1,i}|} s_{y(i+1)}.$$

Si $|w_{1,i}| < |v_{1,i}|$: alors $v_{j,i} = w_{j,i}0^{|v_{1,i}|-|w_{1,i}|}$ pour tout $j \in \{1, \dots, n\}$. Posons

$$s'_{z(i)+1} \cdots s'_{z(i+1)} = s_{y(i)+1} \cdots s_{y(i)+|w_{1,i}|} \nu(s_{y(i)+|w_{1,i}|}, s_{y(i+1)}).$$

Nous avons ainsi construit s' un chemin de w qui est un chemin acceptant dans \mathcal{B} . C'est pourquoi $w \in L(\mathcal{B})$ et la zéro-fermeture de X est incluse dans $L(\mathcal{B})$.

Pour la deuxième inclusion, prenons $w = w_1 w_2 \cdots \in L(\mathcal{B})$ et démontrons que w appartient à la zéro-fermeture de X . Comme $w \in L(\mathcal{B})$, il existe $s' = s'_1 s'_2 \cdots \in (Q')^\omega$ un chemin de w qui est un chemin acceptant dans l'automate \mathcal{B} .

Construisons un mot $v \in X$ tel que $\alpha(v) = \alpha(w)$ et une suite d'états $s = s_1 s_2 \cdots \in Q^\omega$ telle que s est un chemin de w qui est un chemin acceptant dans \mathcal{A} .

Nous initialisons $v = w_1 w_2 \cdots$ et $s = s'_1 s'_2 \cdots$ et, pour tout $i > 0$, nous remplaçons w_i dans v et s'_i dans s de la manière suivante :

Si $s'_i \in Q$: on ne change ni s'_i , ni w_i .

Si $s'_i = \mu(p, q)$: pour un certain p et un certain q dans Q , alors on supprime w_i dans v et s'_i dans s .

Si $s'_i = \nu(p, q)$: pour un certain p et un certain q dans Q , alors on remplace s'_i par un chemin $t_1 \cdots t_{m+1} \in Q^{m+1}$ allant de p à q quand on lit le mot $(0, \dots, 0)^m(\#, \dots, \#)$, et on remplace w_i par $(0, \dots, 0)^m(\#, \dots, \#)$.

De plus, si $\nu(p, q)$ est un état final, on fait en sorte de choisir le chemin $t_1 \cdots t_{m+1}$ pour qu'il passe par un état final.

Ainsi, on a construit un chemin $s \in Q^\omega$ de v qui est un chemin acceptant dans \mathcal{A} , ce qui implique que $v \in X$. De plus, par construction, on a $\alpha(v) = \alpha(w)$. De là, en découle que w appartient à la zéro-fermeture de X , et donc, que $L(\mathcal{B})$ est inclus dans la zéro-fermeture de X . □

Lemme 3.2.9. L'ensemble

$$\{(w_1, w_2) \in R^2 : w_1 \sim_{\#} w_2, \alpha(w_1) < \alpha(w_2)\}$$

est ω -régulier.

Démonstration. Notons E l'ensemble considéré dans l'énoncé.

Soient $w_1, w_2 \in R$ deux mots alignés. Donc w_1 est de la forme $\#w_{1,1}\#w_{1,2}\#\cdots$ et w_2 est de la forme $\#w_{2,1}\#w_{2,2}\#\cdots$. Donc on a

$$\alpha(w_1) = [0; [w_{1,1}]_2, [w_{1,2}]_2, \cdots] \text{ et } \alpha(w_2) = [0; [w_{2,1}]_2, [w_{2,2}]_2, \cdots].$$

Par la proposition 2.3.6, on a que $\alpha(w_1) < \alpha(w_2)$ si et seulement s'il existe k minimal tel que $[w_{1,k}]_2 \neq [w_{2,k}]_2$ et que $[w_{1,k}]_2 < [w_{2,k}]_2$ si k est pair, ou $[w_{1,k}]_2 > [w_{2,k}]_2$ si k est

impair.

Or, par définition de l'ordre lexicographique alterné binaire, cela est équivalent à

$$w_1 <_{\text{alex},2} w_2.$$

De plus, puisque $R \subseteq H_\infty$, alors $w_1, w_2 \in H_\infty$. On peut donc réécrire E comme étant une intersection d'ensembles ω -réguliers. En effet, on a

$$E = \{(u, v) \in H_\infty^2 : u \sim_{\#} v, u <_{\text{alex},2} v\} \cap R^2$$

Or, le premier ensemble est ω -régulier via la proposition 3.1.7 et R est également ω -régulier (cf. Figure 3.6). Ainsi, on peut conclure par stabilité de l' ω -régularité par intersection (cf. Proposition 2.1.2). \square

Lemme 3.2.10. Soit un nombre quadratique irrationnel $a \in]0, 1[$. L'ensemble

$$\{w \in R : \alpha(w) = a\}$$

est ω -régulier.

Démonstration. Par la proposition 2.3.5, on sait que a est un nombre quadratique irrationnel si et seulement si le développement en fraction continue de a est ultimement périodique. On peut donc noter

$$a = [a_0; a_1, \dots, a_{r-1}, \overline{a_r, \dots, a_{r+p}}].$$

De plus, il existe un mot $u = \#u_1\#u_2\#\dots \in R$ tel que $[u_i]_2 = a_i$ pour tout $i > 0$. Ainsi, on a que u est un $\#$ -codage binaire de la fraction continue de a . D'où $\alpha(u) = a$.

Et comme a est ultimement périodique, alors nous pouvons choisir u de telle manière à ce qu'il le soit aussi. Il est facile de construire un automate de Büchi acceptant un mot ultimement périodique, ce pourquoi le singleton

$$\{u\} \subset R$$

est ω -régulier.

Ainsi par le lemme 3.2.8, la zéro-fermeture de $\{u\}$ est ω -régulière. Cette zéro-fermeture correspond exactement à l'ensemble $\{w \in R : \alpha(w) = a\}$. \square

Lemme 3.2.11. L'ensemble

$$\{w \in R : \alpha(w) < \frac{1}{2}\}$$

est ω -régulier.

Démonstration. Notons E l'ensemble considéré dans l'énoncé. Soit un mot $w \in E$. On a $\alpha(w) = [0; a_1, a_2, \dots]$ où $a_i \in \mathbb{N}_0$ pour tout $i > 0$.

Remarquons que $\alpha(w) < \frac{1}{2}$ si et seulement si $a_1 > 1$. Ainsi nous pouvons réécrire l'ensemble

$$E = \{w \in R : \alpha(w) = [0; a_1, a_2, \dots], a_1 \neq 1\}.$$

Posons $Y = \#10^*(\#(0|1)^*)^\omega$. Nous remarquons que $E = R \setminus Y = R \cap Y^c$. L'automate de Büchi représenté à la figure 3.7 accepte Y , ainsi Y est ω -régulier. Ainsi, comme Y et R sont ω -réguliers, on peut conclure que E l'est aussi via la proposition 2.1.2.

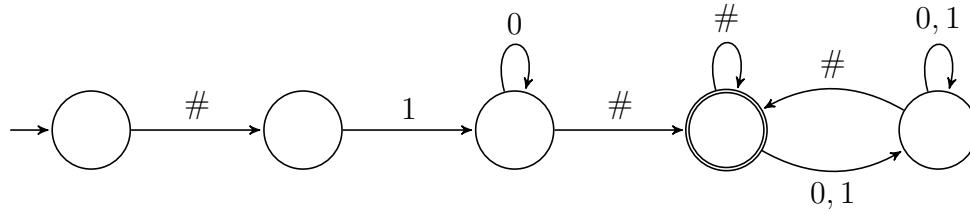


FIGURE 3.7 – Automate de Büchi acceptant Y

□

3.3 Codage binaire des représentations d'Ostrowski

Dans cette section, nous allons montrer une manière de coder en binaire les représentations d'Ostrowski de naturels et de réels. Puisque les représentations binaires des naturels peuvent varier de taille en fonction du nombre de zéros de queue, nous allons fixer les tailles des représentations en alignant le codage sur un mot v de R . Ensuite, nous définirons des ensembles A^{fin} et A qui contiennent l'entièreté de ces codages et établirons une notion d'ordre sur ces ensembles, tout en conservant l' ω -régularité à travers nos concepts.

Définition 3.3.1. Soit $v \in R$. Soient

$$x = x_1x_2 \dots \in \mathbb{N}^\omega \quad \text{et} \quad w = \#w_1\#w_2\#\dots \in H_\infty$$

tels que $[w_i]_2 = x_i$ pour tout $i > 0$.

- Soit $N \in \mathbb{N}$. On dit que w est la **$\#$ - v -représentation d'Ostrowski** de N si v et w sont alignés et si x est la concaténation de la $\alpha(v)$ -représentation d'Ostrowski de N et de 0^ω .
- Soit $c \in I_{\alpha(v)}$. On dit que w est la **$\#$ - v -représentation d'Ostrowski** de c si v et w sont alignés et si x est la $\alpha(v)$ -représentation d'Ostrowski de c .

Ces représentations sont uniques pour un $v \in R$ donné. Cela découle du fait de devoir être aligné avec v ainsi que de l'unicité des α -représentations d'Ostrowski. Nous verrons dans la preuve du lemme 3.3.10 qu'il est toujours possible de coder une représentation d'Ostrowski en respectant l'alignement.

Exemple 3.3.2. Prenons $N = 30$ et $v = \#1011\#0011(\#1)^\omega$. Alors

$$\begin{aligned}\alpha(v) &= [0; [1011]_2, [0011]_2, \overline{[1]_2}] \\ &= [0; 13, 12, \overline{1}].\end{aligned}$$

Au vu de ce qui a été développé dans l'exemple 2.3.13, on a

$$30 = [4 \ 2 \ 0 \ 0]_{\alpha(v)}$$

et donc, si on pose $x = (4)(2)(0)^\omega$, alors x est la concaténation d'une $\alpha(v)$ -représentation d'Ostrowski de 30 et de 0^ω .

Choisissons $w = \#w_1\#w_2\#\dots \in H_\infty$ de telle manière à avoir $[w_i]_2 = x_i$ pour tout $i > 0$ et tel que w soit aligné avec v . Prenons

$$w = \#0010\#0100(\#0)^\omega.$$

Ainsi, le mot w est la $\#$ - v -représentation d'Ostrowski de 30.

Exemple 3.3.3. Prenons $x = \sqrt{3} - 2$ et $v = (\#01)^\omega$. Alors

$$\alpha(v) = [0; \overline{2}].$$

Au vu de ce qui a été développé dans l'exemple 2.3.19, on sait que 0 2 1 0 0 0 2 est le début de l' $\alpha(v)$ -représentation d'Ostrowski de $\sqrt{3} - 2$. Pour obtenir le début de w la $\#$ - v -représentation d'Ostrowski de $\sqrt{3} - 2$, il suffit de coder en binaire 0 2 1 0 0 0 2 et d'aligner le résultat sur v . Ainsi,

$$w = \#00\#01\#10\#00\#00\#00\#01\#\dots$$

Notation 3.3.4. Soit $v \in R$. Notons

- A_v^{fin} l'ensemble des mots $w \in H_\infty$ tels que w est la $\#$ - v -représentation d'Ostrowski d'un nombre naturel,
- A_v l'ensemble des mots $w \in H_\infty$ tels que w est la $\#$ - v -représentation d'Ostrowski d'un réel $c \in I_{\alpha(v)}$.

Notation 3.3.5. Notons les ensembles

$$A^{\text{fin}} = \{(v, w) : v \in R, w \in A_v^{\text{fin}}\} \quad \text{et} \quad A = \{(v, w) : v \in R, w \in A_v\}.$$

De manière générale, dans ce travail, la notation suivante sera régulièrement employée pour parler d'un ensemble qu'on souhaiterait considérer sans une de ses composantes.

Notation 3.3.6. Soient X, Y deux ensembles. Soit $Z \subseteq X \times Y$. Pour tout $x \in X$, nous notons Z_x l'ensemble $\{y \in Y : (x, y) \in Z\}$.

Lemme 3.3.7. Les ensembles A^{fin} et A sont ω -réguliers. De plus, $A^{\text{fin}} \subseteq A$.

Démonstration. Démontrons que $A^{\text{fin}} \subseteq A$. Soit $(v, w) \in A^{\text{fin}}$. Alors $v \in R$ et $w \in A_v^{\text{fin}}$. Ainsi, $w = \#w_1\#w_2\#\dots \in H_\infty$ est la $\#$ - v -représentation d'Ostrowski d'un certain N naturel. Autrement dit, w et v sont alignés; et il existe $x = x_1x_2\cdots \in \mathbb{N}^\omega$ tel que $[w_i]_2 = x_i$ pour tout $i > 0$ et tel que x est la concaténation d'une $\alpha(v)$ -représentation d'Ostrowski de N et de 0^ω .

Par la proposition 2.3.20, on a que x est la $\alpha(v)$ -représentation d'Ostrowski de

$$f_{\alpha(v)}(\alpha(v)N).$$

Or $f_{\alpha(v)}(\alpha(v)N) \in I_{\alpha(v)}$.

Donc, w est la $\#$ - v -représentation d'Ostrowski d'un certain réel appartenant à $I_{\alpha(v)}$, ce qui est équivalent à dire que $w \in A_v$. Donc $(v, w) \in A$.

Démontrons maintenant que A^{fin} et A sont ω -réguliers. Posons

$$B = \{(v, w) : v \in R, v \sim_{\#} w\}.$$

On a $A^{\text{fin}} \subseteq B$. Comme R est ω -régulier et que $\sim_{\#}$ est une relation ω -régulière, alors B est également ω -régulier.

Soit $(v, w) \in B$. Les mots v et w peuvent être écrits de la manière suivante :

$$v = \#v_1\#v_2\#\dots \quad \text{et} \quad w = \#w_1\#w_2\#\dots$$

où $v_i, w_i \in \{0, 1\}^*$ pour tout $i > 0$. Ainsi, on a $\alpha(v) = [0; [v_1]_2, [v_2]_2, \dots]$. De plus, comme v et w sont alignés, on a $|v_i| = |w_i|$ pour tout $i > 0$.

Démontrons que A^{fin} est ω -régulier. Le couple $(v, w) \in A^{\text{fin}}$ si et seulement si le mot w est la $\#$ - v -représentation d'Ostrowski d'un certain nombre naturel N . Cela est vrai si et seulement s'il existe un naturel M tel que $[w_1]_2[w_2]_2\cdots[w_{M+1}]_2$ est une $\alpha(v)$ -représentation d'Ostrowski de N . Par la proposition 2.3.11, cette dernière affirmation est équivalente à ces conditions :

1. $[w_1]_2 < [v_1]_2$
2. $[w_i]_2 \leq [v_i]_2$ pour tout $i > 1$.
3. Si $[w_i]_2 = [v_i]_2$, alors $[w_{i-1}]_2 = 0$, pour tout $i > 1$.
4. w a un nombre fini de 1.

Par définition de l'ordre co-lexicographique, les conditions (1) et (2) peuvent respectivement se réécrire $w_1 <_{\text{colex}} v_1$ et $w_i \leq_{\text{colex}} v_i$ pour tout $i > 1$.

Comme $|w_i| = |v_i|$ pour tout $i > 0$, alors la condition (3) peut se réécrire : si $w_i = v_i$, alors $w_{i-1} = 0^{|v_{i-1}|}$, pour tout $i > 1$.

On peut facilement construire un automate de Büchi acceptant l'ensemble des couples de mots respectant chacune de ces conditions, celles-ci sont donc ω -régulières. D'où l' ω -régularité de A^{fin} .

Démontrons que A est ω -régulier.

$$(v, w) \in A \Leftrightarrow w \text{ est la } \#-v\text{-représentation d'Ostrowski d'un certain réel } c \in I_{\alpha(v)}.$$

$$\Leftrightarrow [w_1]_2[w_2]_2 \cdots \text{ est la } \alpha(v)\text{-représentation d'Ostrowski de } c.$$

Par la proposition 2.3.17, cette dernière affirmation est équivalente à ces conditions :

1. $[w_1]_2 < [v_1]_2$
2. $[w_i]_2 \leq [v_i]_2$ pour tout $i > 1$.
3. Si $[w_i]_2 = [v_i]_2$, alors $[w_{i-1}]_2 = 0$, pour tout $i > 1$.
4. $[w_i]_2 \neq [v_i]_2$ pour une infinité de i impairs.

Par définition de l'ordre co-lexicographique, les conditions (1) et (2) peuvent respectivement se réécrire $w_1 <_{\text{colex}} v_1$ et $w_i \leq_{\text{colex}} v_i$ pour tout $i > 1$.

Comme $|w_i| = |v_i|$ pour tout $i > 0$, alors les conditions (3) et (4) peuvent se réécrire : si $w_i = v_i$, alors $w_{i-1} = 0^{|v_{i-1}|}$, pour tout $i > 1$; et $w_i \neq v_i$ pour une infinité de i impairs.

On peut facilement construire un automate de Büchi acceptant l'ensemble des couples de mots respectant chacune de ces conditions, celles-ci sont donc ω -régulières. D'où l' ω -régularité de A . \square

Nous allons maintenant établir, pour un $v \in R$ donné, une bijection entre les codages binaires des représentations d'Ostrowski des naturels (resp. des réels de $I_{\alpha(v)}$) et l'ensemble des naturels (resp. l'ensemble $I_{\alpha(v)}$).

Définition 3.3.8. Soit $v \in R$. Définissons les fonctions suivantes :

$$Z_v : A_v^{\text{fin}} \rightarrow \mathbb{N} : w \mapsto N \text{ tel que } w \text{ est la } \#-v\text{-représentation d'Ostrowski de } N;$$

$$O_v : A_v \rightarrow I_{\alpha(v)} : w \mapsto c \text{ tel que } w \text{ est la } \#-v\text{-représentation d'Ostrowski de } c.$$

Exemple 3.3.9. Soient

$$v = \#1011\#0011(\#1)^\omega,$$

$$w = \#0010\#0100(\#0)^\omega.$$

Ainsi, vu ce qui a été développé dans l'exemple 3.3.2, on a

$$Z_v(w) = 30.$$

Lemme 3.3.10. Soit $v \in R$. Les fonctions Z_v et O_v sont bijectives.

Démonstration. Soit $v \in R$. Par les propositions 2.3.11 et 2.3.17, il existe une seule $\alpha(v)$ -représentation d'Ostrowski d'un naturel N ou d'un réel $c \in I_{\alpha(v)}$ donné (à des zéros de queue près pour le cas naturel).

Démontrons d'abord que les fonctions sont injectives. Il suffit de montrer qu'une $\alpha(v)$ -représentation d'Ostrowski ne correspond qu'à un seul codage dans A_v^{fin} ou dans A_v . Cela découle directement de l'unicité des représentations binaires pour une taille donnée ; et du fait que w et v doivent être alignés, ainsi, v détermine les longueurs des représentations binaires.

Démontrons que les fonctions sont surjectives. Il suffit de montrer que $b_1 b_2 \dots$ la concaténation d'une $\alpha(v)$ -représentation d'Ostrowski de $N \in \mathbb{N}$ et de 0^ω ou la $\alpha(v)$ -représentation d'Ostrowski de $c \in I_{\alpha(v)}$ peut toujours être encodée par un mot w respectivement de A_v^{fin} ou de A_v . Montrons que le fait de devoir être aligné avec v ne fait jamais en sorte qu'on manque de place pour encoder les nombres b_i en binaire pour tout $i > 0$.

Pour encoder un nombre naturel n en binaire, nous avons besoin de $1 + \lfloor \log_2 n \rfloor$ caractères. Puisque la fonction $n \mapsto 1 + \lfloor \log_2 n \rfloor$ est strictement croissante, alors, si on peut encoder n en k caractères, tout naturel plus petit ou égal à n peut être encodé en k caractères.

Or, comme v est de la forme $\#v_1\#v_2\#\dots$, alors $\alpha(v) = [0; [v_1]_2, [v_2]_2, \dots]$. De plus, par les propositions 2.3.11 et 2.3.17, on a $b_n \leq [v_n]_2$ pour tout $n > 1$. Ainsi, comme w doit être aligné avec v , si $[v_n]_2$ est codé en binaire en k caractères, alors b_n peut aussi être codé en k caractères. \square

Définition 3.3.11. Soit $v \in R$. On définit

$$0_v = Z_v^{-1}(0) \quad \text{et} \quad 1_v = Z_v^{-1}(1).$$

Exemple 3.3.12. Si $v = \#1011\#0011(\#1)^\omega$, alors

$$\alpha(v) = [0; 13, 12, \bar{1}] = \frac{3429 + \sqrt{5}}{44878}.$$

Dans l'exemple 2.3.13, on a montré que le début de la décomposition d'un naturel X donnée par l'équation (2.1) est

$$X = 1.b_1 + 13.b_2 + 157.b_3 + 170.b_4 + \dots$$

Ainsi, si X vaut 0, alors

$$X = [0 \dots 0]_{\alpha(v)}.$$

Si on pose $x = (0)^\omega$, alors x est la concaténation d'une $\alpha(v)$ -représentation d'Ostrowski de 0 et de 0^ω . D'où

$$0_v = \#0000\#0000(\#0)^\omega.$$

De plus, si X vaut 1, alors

$$X = [1 \ 0 \dots 0]_{\alpha(v)}$$

et on peut prendre $x = 1(0)^\omega$ comme $\alpha(v)$ -représentation d'Ostrowski de 1. D'où

$$1_v = \#1000\#0000(\#0)^\omega.$$

Définition 3.3.13. Nous définissons les ensembles suivants :

$$0_* = \{(v, 0_v) : v \in R\} \quad \text{et} \quad 1_* = \{(v, 1_v) : v \in R\}.$$

Lemme 3.3.14. Les ensembles 0_* et 1_* sont ω -réguliers.

Démonstration. Démontrons que 0_* est ω -régulier. Une α -représentation d'Ostrowski de 0 est $0 \dots 0$ pour tout α irrationnel. De plus, le codage de 0 en binaire est uniquement composé de 0. Ainsi, on peut réexprimer la relation 0_* de la manière suivante :

$$0_* = \{(v, w) : v \in R, w \text{ est } v \text{ où les } 1 \text{ ont été remplacés par des } 0 \}.$$

Or, il est facile de construire un automate de Büchi qui reconnaît cet ensemble, donc 0_* est ω -régulier.

Démontrons que 1_* est ω -régulier. Soit un nombre irrationnel $\alpha = [0; a_1, a_2, \dots]$ où $a_i \in \mathbb{N}_0$ pour tout $i > 0$. Par la proposition 2.3.11, on sait qu'il existe un naturel N tel que nous pouvons décomposer 1 de la manière unique (à des zéros de queue près) suivante :

$$1 = \sum_{n=0}^N b_{n+1}q_n$$

où $0 \leq b_1 < a_1$, $0 \leq b_{n+1} \leq a_{n+1}$ et $b_n = 0$ quand $b_{n+1} = a_{n+1}$ pour tout $n \geq 1$. De plus, par la proposition 2.3.8, on a $q_n = a_n q_{n-1} + q_{n-2}$ pour tout $n > 0$ (en posant $q_{-1} = 0$ et $q_0 = 1$).

Si $a_1 > 1$: alors $q_1 = a_1 q_0 + q_{-1} = a_1 > 1$. Donc, nous obtenons la décomposition

$$1 = b_1 \underbrace{q_0}_{=1} + b_2 \underbrace{q_1}_{>1} + \dots$$

Ainsi, nous avons $b_2 = 0$, $b_1 = 1$ et $1 = [1 \ 0 \dots 0]_\alpha$.

Si $a_1 = 1$: alors $q_1 = a_1 q_0 + q_{-1} = a_1 = 1$ et $q_2 = a_2 q_1 + q_0 = a_2 + 1 > 1$. De plus, $0 \leq b_1 < a_1 = 1$. Donc, nous obtenons la décomposition

$$1 = \underbrace{b_1}_{=0} \underbrace{q_0}_{=1} + b_2 \underbrace{q_1}_{=1} + b_3 \underbrace{q_2}_{>1} + \dots$$

Ainsi, nous avons $b_3 = 0$, $b_2 = 1$ et $1 = [0 \ 1 \ 0 \dots 0]_\alpha$.

Donc, pour un mot $v = \#v_1\#v_2\#\dots \in R$ donné, on a

$$1_v = \#10^{|v_1-1|}\#0^{|v_2|}\#0^{|v_3|}\#\dots \quad \text{ou} \quad 1_v = \#0^{|v_1|}\#10^{|v_2-1|}\#0^{|v_3|}\#0^{|v_4|}\#\dots$$

On peut facilement construire un automate de Büchi qui accepte des mots de cette forme, ainsi 1_* est ω -régulier. \square

Lemme 3.3.15. Soit $v \in R$. Soit $s \in A_v^{\text{fin}}$. Alors $O_v(s) = f_{\alpha(v)}(\alpha(v)Z_v(s))$. Autrement dit,

$$\alpha(v)Z_v(s) - O_v(s) \in \mathbb{Z}.$$

De plus, nous avons

$$O_v(1_v) = \begin{cases} \alpha(v) & \text{si } \alpha(v) < \frac{1}{2}, \\ \alpha(v) - 1 & \text{sinon.} \end{cases}$$

Démonstration. Soit $v \in R$. Soit $s \in A_v^{\text{fin}}$. On a $Z_v(s) \in \mathbb{N}$. Soit $b_1 \cdots b_{N+1}$ une $\alpha(v)$ -représentation d'Ostrowski de $Z_v(s)$. Autrement dit, il existe un naturel N tel que

$$Z_v(s) = \sum_{k=0}^N b_{k+1}q_k$$

où $0 \leq b_1 < a_1$, $0 \leq b_{n+1} \leq a_{n+1}$ pour tout $n \geq 1$, $b_n = 0$ quand $b_{n+1} = a_{n+1}$ pour tout $n \geq 1$ et $b_{n+1} = 0$ pour tout $n > N$. Par la proposition 2.3.20, on a que $b_1 \cdots b_{N+1}0^\omega$ est la $\alpha(v)$ -représentation d'Ostrowski de

$$f_{\alpha(v)}(\alpha(v)Z_v(s)) \in I_{\alpha(v)}.$$

Autrement dit, il existe un unique u entier tel que $f_{\alpha(v)}(\alpha(v)Z_v(s)) = \alpha(v)Z_v(s) - u$ et on a

$$f_{\alpha(v)}(\alpha(v)Z_v(s)) = \sum_{k \geq 0} b_{k+1}\beta_k$$

où $b_k = 0$ pour tout $k > N + 1$. Or $O_v(s) = \sum_{k \geq 0} b_{k+1}\beta_k$. Ainsi, nous avons

$$O_v(s) = f_{\alpha(v)}(\alpha(v)Z_v(s)).$$

Autrement dit, on a

$$\alpha(v)Z_v(s) - O_v(s) = \alpha(v)Z_v(s) - \underbrace{f_{\alpha(v)}(\alpha(v)Z_v(s))}_{\alpha(v)Z_v(s) - u} = u \in \mathbb{Z}.$$

Démontrons maintenant la deuxième partie de l'énoncé. Vu ce que nous venons de prouver et par définition de 1_v , nous obtenons

$$O_v(1_v) = f_{\alpha(v)}(\alpha(v)Z_v(1_v)) = f_{\alpha(v)}(\alpha(v)) = \alpha(v) - u \in I_{\alpha(v)}.$$

Comme $\alpha(v) \in]0, 1[$, alors $I_{\alpha(v)} = [-\alpha(v), 1 - \alpha(v)[$.

Si $0 < \alpha(v) < \frac{1}{2}$: alors $\alpha(v) \in I_{\alpha(v)}$. Par conséquent, $O_v(1_v) = \alpha(v)$.

Si $\frac{1}{2} < \alpha(v) < 1$: alors $-\frac{1}{2} < \alpha(v) - 1 < 0$. Donc $\alpha(v) - 1 \in I_{\alpha(v)}$. Par conséquent, $O_v(1_v) = \alpha(v) - 1$.

□

Nous introduisons maintenant une notion d'ordre sur l'ensemble des codages binaires des représentations d'Ostrowski.

Notation 3.3.16. Soit $v \in R$. Notons les ensembles suivants :

$$\begin{aligned} \prec^{\text{fin}} &= \{(v, s, t) \in R \times (A_v^{\text{fin}})^2 : Z_v(s) < Z_v(t)\}, \\ \prec_v^{\text{fin}} &= \{(s, t) \in (A_v^{\text{fin}})^2 : Z_v(s) < Z_v(t)\}, \\ \prec &= \{(v, s, t) \in R \times (A_v)^2 : O_v(s) < O_v(t)\}, \\ \prec_v &= \{(s, t) \in (A_v)^2 : O_v(s) < O_v(t)\}. \end{aligned}$$

Lemme 3.3.17. Les ensembles \prec^{fin} et \prec sont ω -réguliers.

Démonstration. Commençons par démontrer que \prec^{fin} est ω -régulier. Soient $v \in R$ et $s, t \in A_v^{\text{fin}}$. Ainsi, s et t sont alignés, puisqu'ils sont alignés avec v . De plus, par la remarque 2.3.15, on a que $Z_v(s) < Z_v(t)$ si et seulement si une $\alpha(v)$ -représentation d'Ostrowski de $Z_v(s)$ est co-lexicographiquement plus petite qu'une de $Z_v(t)$. Cela est équivalent à

$$s <_{\text{colex},2} t$$

et cette condition est ω -régulière vu la proposition 3.1.7.

Démontrons que l'ensemble \prec est ω -régulier. Soient $v \in R$ et $s, t \in A_v$. Ainsi, s et t sont alignés, puisqu'ils sont alignés avec v . De plus, par la proposition 2.3.21, on a que $O_v(s) < O_v(t)$ si et seulement si

$$s <_{\text{alex},2} t$$

et cette condition est ω -régulière vu la proposition 3.1.7. □

Notation 3.3.18. Soit $v \in R$. Notons les ensembles

$$\begin{aligned} \preceq^{\text{fin}} &= \{(v, s, t) \in R \times (A_v^{\text{fin}})^2 : Z_v(s) \leq Z_v(t)\}, \\ \preceq_v^{\text{fin}} &= \{(s, t) \in (A_v^{\text{fin}})^2 : Z_v(s) \leq Z_v(t)\}, \\ \preceq &= \{(v, s, t) \in R \times (A_v)^2 : O_v(s) \leq O_v(t)\}, \\ \preceq_v &= \{(s, t) \in (A_v)^2 : O_v(s) \leq O_v(t)\}. \end{aligned}$$

Remarquons que les ensembles \preceq^{fin} et \preceq sont ω -réguliers vu l' ω -régularité de \prec^{fin} et de \prec , et puisqu'il est facile de construire un automate de Büchi acceptant l'ensemble des couples (s, t) de H_∞^2 tels que $s = t$.

Notations 3.3.19. Soit $v \in R$. Soient $s_1, s_2 \in A_v^{\text{fin}}$. Soient $t_1, t_2 \in A_v$.

- Si $(s_1, s_2) \in \prec_v^{\text{fin}}$, nous notons $s_1 \prec_v^{\text{fin}} s_2$.
- Si $(s_1, s_2) \in \preceq_v^{\text{fin}}$, nous notons $s_1 \preceq_v^{\text{fin}} s_2$.
- Si $(t_1, t_2) \in \prec_v$, nous notons $t_1 \prec_v t_2$.
- Si $(t_1, t_2) \in \preceq_v$, nous notons $t_1 \preceq_v t_2$.

Chapitre 4

Acceptation de l'addition

Dans ce chapitre, nous allons discuter de quelle manière nous pouvons construire un automate qui accepte l'addition de représentations d'Ostrowski. C'est un élément qui nous sera indispensable pour établir nos résultats de décidabilité dans le chapitre suivant. Ici, nous allons d'abord utiliser les représentations d'Ostrowski et dans un second temps, nous passerons aux codages binaires de ces représentations afin de travailler sur un alphabet fini.

4.1 Addition de représentations d'Ostrowski

Dans cette section, nous allons construire un automate qui accepte l'addition de représentations d'Ostrowski de naturels.

Pour tout $k > 1$, nous disons qu'un automate à k bandes accepte un tuple de la forme

$$(a_{1,1} \cdots a_{1,m}, a_{2,1} \cdots a_{2,m}, \cdots, a_{k,1} \cdots a_{k,m})$$

si et seulement si, en partant d'un état initial, puis en lisant successivement les tuples $(a_{1,1}, a_{2,1}, \cdots, a_{k,1})$, $(a_{1,2}, a_{2,2}, \cdots, a_{k,2})$, \cdots , $(a_{1,m}, a_{2,m}, \cdots, a_{k,m})$, il est possible d'arriver dans un état final.

Nous voulons construire un automate fini à 4 bandes sur un alphabet \mathbb{N} tel que

$$(d_1 \cdots d_m, x_1 \cdots x_m, y_1 \cdots y_m, z_1 \cdots z_m) \in (\mathbb{N}^m)^4$$

est accepté si et seulement si, pour tout irrationnel α tel que $\alpha = [0; d_1, \dots, d_m, \dots]$, les mots $x_1 \cdots x_m$, $y_1 \cdots y_m$ et $z_1 \cdots z_m$ sont trois α -représentations d'Ostrowski de nombres naturels telles que

$$[x_1 \cdots x_m]_\alpha + [y_1 \cdots y_m]_\alpha = [z_1 \cdots z_m]_\alpha.$$

Notons que si les trois représentations ne sont pas de la même taille, nous pouvons ajouter des zéros de queue aux représentations des plus petites pour travailler avec des

mots de même taille.

Pour cela, à l'instar de ce qui a été conçu dans l'article [3], nous allons construire un automate fini (mais potentiellement avec un nombre infini d'arcs) déterministe à 2 bandes sur un alphabet \mathbb{N} qui accepte $(d_m \cdots d_1, w_m \cdots w_1) \in \mathbb{N}^m \times \mathbb{Z}^m$ si et seulement si, pour tout irrationnel α tel que $\alpha = [0; d_1, \dots, d_m, \dots]$, on a

$$[w_1 \cdots w_m]_\alpha = 0.$$

En effet, si on pose

$$w_i = z_i - x_i - y_i$$

pour tout $i \in \{1, \dots, m\}$, alors, par définition des α -valeurs, on a

$$\begin{aligned} [x_1 \cdots x_m]_\alpha + [y_1 \cdots y_m]_\alpha = [z_1 \cdots z_m]_\alpha &\Leftrightarrow \sum_{i=0}^{m-1} x_{i+1} q_i + \sum_{i=0}^{m-1} y_{i+1} q_i = \sum_{i=0}^{m-1} z_{i+1} q_i \\ &\Leftrightarrow \sum_{i=0}^{m-1} (z_{i+1} - x_{i+1} - y_{i+1}) q_i = 0 \\ &\Leftrightarrow \sum_{i=0}^{m-1} w_{i+1} q_i = 0 \\ &\Leftrightarrow [w_1 \cdots w_m]_\alpha = 0. \end{aligned}$$

Nous pourrions alors considérer l'automate miroir (c'est à dire l'automate où les arcs ont été retournés et pour lequel les états initiaux deviennent finals et vice versa) pour obtenir l'automate initialement désiré.

Construisons un automate fini déterministe à double bande $\mathcal{A} = (Q \cup \{\perp\}, \mathbb{Z}, (r_0, s_0), F, \delta)$ où $Q \cup \{\perp\}$ est l'ensemble des états, \mathbb{Z} est l'alphabet, (r_0, s_0) l'état initial, F l'ensemble des états finals et $\delta : Q \cup \{\perp\} \times (\mathbb{N} \times \mathbb{Z}) \rightarrow Q \cup \{\perp\}$ la fonction de transition. Chaque état est un couple d'entiers (r, s) , à l'exception du puits que nous notons \perp . Nous allons construire \mathcal{A} pour qu'il satisfasse l'invariant suivant : si on part d'un état (r, s) , alors, pour $k \geq 0$, l'automate accepte une entrée de longueur k $(d_k \cdots d_1, w_k \cdots w_1) \in \mathbb{N}^k \times \mathbb{Z}^k$ si et seulement si

$$\sum_{j=0}^{k-1} w_{j+1} q_j = r q_{k-1} + s q_k. \quad (4.1)$$

L'invariant va nous permettre de déterminer la structure de l'automate \mathcal{A} . En effet, si nous voulons construire un additionneur, il faut qu'une entrée de longueur k soit acceptée uniquement si

$$[w_1 \cdots w_k]_\alpha = \sum_{j=0}^{k-1} w_{j+1} q_j = 0. \quad (4.2)$$

Ainsi, si on prend $(0, 0)$ comme état initial pour \mathcal{A} , alors l'invariant respecte la condition (4.2). De plus, l'invariant nous dit que si on part d'un état (r, s) , alors l'automate accepte une entrée de longueur 0 (c'est à dire quand on reste dans le même état) si et seulement si

$$0 = \sum_{j=0}^{-1} w_{j+1}q_j = rq_{-1} + sq_0 = 0.r + 1.s = s.$$

Ainsi, nous pouvons en déduire que les états finals de \mathcal{A} sont de la forme $(r, 0)$. L'invariant permet également de déterminer les transitions de l'automate.

Lemme 4.1.1. Pour qu'un automate fini déterministe à deux bandes satisfasse l'invariant (4.1), il est suffisant d'avoir $s' = s$ et $t = r + sd - w$ pour toute transition allant de l'état (r, s) à l'état (s', t) en lisant l'entrée (d, w) .

Démonstration. Soit un automate satisfaisant l'invariant (4.1). Soit un naturel $i \geq 0$. Soit

$$(d_{i+1}d_i \cdots d_1, w_{i+1}w_i \cdots w_1) \in \mathbb{N}^{i+1} \times \mathbb{Z}^{i+1}$$

une entrée acceptée par l'automate en partant de l'état (r, s) . Puisque l'invariant (4.1) est satisfait par l'automate, alors, nous avons

$$\sum_{j=0}^i w_{j+1}q_j = rq_i + sq_{i+1}.$$

Soit (s', t) l'état dans lequel on se retrouve en partant de (r, s) et en lisant l'entrée (d_{i+1}, w_{i+1}) . Ainsi, $(d_i \cdots d_1, w_i \cdots w_1)$ est une entrée acceptée par l'automate en partant de l'état (s', t) et l'invariant nous dit que

$$\sum_{j=0}^{i-1} w_{j+1}q_j = s'q_{i-1} + tq_i.$$

Nous pouvons déduire des deux équations précédentes que

$$rq_i + sq_{i+1} = \sum_{j=0}^i w_{j+1}q_j = \sum_{j=0}^{i-1} w_{j+1}q_j + w_{i+1}q_i = s'q_{i-1} + tq_i + w_{i+1}q_i.$$

Or, nous avons

$$\begin{aligned} rq_i + sq_{i+1} &= s'q_{i-1} + tq_i + w_{i+1}q_i \\ \Leftrightarrow w_{i+1}q_i &= rq_i + sq_{i+1} - s'q_{i-1} - tq_i. \end{aligned}$$

Par la propriété 2.3.8, nous savons que $q_{i+1} = d_{i+1}q_i + q_{i-1}$. En substituant q_{i+1} dans l'équation précédente, nous obtenons :

$$w_{i+1}q_i = rq_i + sd_{i+1}q_i + sq_{i-1} - s'q_{i-1} - tq_i.$$

En réordonnant les termes, nous avons l'équation suivante :

$$q_i(w_{i+1} - r - sd_{i+1} + t) = q_{i-1}(s - s').$$

Ainsi, il est suffisant de choisir

$$t = r + sd_{i+1} - w_{i+1} \quad \text{et} \quad s' = s$$

pour satisfaire l'équation précédente. \square

Nous avons trouvé quelles transitions étaient nécessaires pour construire l'automate \mathcal{A} , il ne reste plus qu'à déterminer les états requis.

Proposition 4.1.2. Soit un irrationnel $\alpha = [0; d_1, d_2, \dots]$. Si $(d_k \cdots d_1, w_k \cdots w_1) \in \mathbb{N}^k \times \mathbb{Z}^k$ est une entrée acceptée par \mathcal{A} telle que $w_i = z_i - x_i - y_i$ pour tout $i \in \{1, \dots, k\}$ où $x_1 \cdots x_k$, $y_1 \cdots y_k$ et $z_1 \cdots z_k$ sont des α -représentations d'Ostrowski de naturels telles que

$$[x_1 \cdots x_k]_\alpha + [y_1 \cdots y_k]_\alpha = [z_1 \cdots z_k]_\alpha,$$

alors le chemin parcouru en lisant cette entrée ne passe que par des états dans $\{-1, 0, 1\} \times \{-1, 0, 1\}$.

Démonstration. Notons $S = \{-1, 0, 1\} \times \{-1, 0, 1\}$. Démontrons par récurrence sur n que le n -ème état d'un chemin acceptant de taille k de A appartient à S pour tout $n \in \{0, \dots, k\}$.

Pour le cas de base, si $n = 0$, alors on se trouve dans l'état initial $(0, 0)$ qui est bien dans S .

Pour l'induction, si $n > 0$, supposons que (r, s) le $n - 1$ -ème état visité soit dans S et montrons que le n -ème état appartient aussi à S . En partant de l'état (r, s) , on lit l'entrée (d_j, w_j) où $j = k - n + 1$, alors, par le lemme 4.1.1, on sait qu'on transite vers l'état $(s, r + sd_j - w_j)$. Posons $t = r + sd_j - w_j$. Il suffit de montrer que t appartient à $\{-1, 0, 1\}$.

De plus, comme $[0^{j-1}1]_\alpha = q_{j-1}$ et comme $x_1 \cdots x_k$, $y_1 \cdots y_k$ et $z_1 \cdots z_k$ sont des α -représentations d'Ostrowski de nombres naturels, alors

$$\begin{aligned} 0 &\leq [z_1 \cdots z_{j-1}]_\alpha \leq q_{j-1} - 1, \\ 1 - q_{j-1} &\leq -[x_1 \cdots x_{j-1}]_\alpha \leq 0, \\ 1 - q_{j-1} &\leq -[y_1 \cdots y_{j-1}]_\alpha \leq 0. \end{aligned}$$

Ainsi, on obtient les bornes suivantes :

$$-2q_{j-1} + 2 \leq [w_1 \cdots w_{j-1}]_\alpha \leq q_{j-1} - 1.$$

Or, puisque l'automate satisfait l'invariant (4.1), nous avons

$$[w_1 \cdots w_{j-1}]_\alpha = \sum_{i=0}^{j-2} w_{i+1} q_i = \sum_{i=0}^{j-1} w_{i+1} q_i - q_{j-1} w_j = r q_{j-1} + s q_j - q_{j-1} w_j.$$

Nous pouvons en déduire les inégalités suivantes :

$$-2q_{j-1} + 2 \leq rq_{j-1} + sq_j - q_{j-1}w_j \leq q_{j-1} - 1.$$

Intéressons-nous à la première inégalité. Nous avons

$$\begin{aligned} q_{j-1}w_j &\leq rq_{j-1} + sq_j + 2q_{j-1} - 2 \\ &= rq_{j-1} + s(d_jq_{j-1} + q_{j-2}) + 2q_{j-1} - 2 \\ &= q_{j-1}(r + sd_j + 2) + sq_{j-2} - 2. \end{aligned}$$

Or, par hypothèse de récurrence, nous avons $s \in \{-1, 0, 1\}$.

Si $s \in \{-1, 0\}$: alors, comme $q_{j-2} \geq 0$, on a $sq_{j-2} - 2 < 0$. Donc, il en découle

$$q_{j-1}w_j < q_{j-1}(r + sd_j + 2).$$

Puisque $q_{j-1} \geq 1$, alors nous obtenons

$$w_j < r + sd_j + 2.$$

Si $s = 1$: Comme $x_j, y_j \geq 0$ et au vu de la proposition 2.3.11, on a

$$w_j = z_j - x_j - y_j \leq z_j \leq d_j = sd_j.$$

De plus, on a $r \in \{-1, 0, 1\}$ par hypothèse de récurrence. Nous pouvons en déduire que

$$w_j \leq sd_j \leq r + sd_j + 1.$$

Dans les deux cas, nous obtenons l'inégalité suivante :

$$w_j \leq r + sd_j + 1.$$

Intéressons-nous maintenant à la deuxième inégalité. Nous avons

$$\begin{aligned} q_{j-1}w_j &\geq rq_{j-1} + sq_j - q_{j-1} + 1 \\ &= rq_{j-1} + s(d_jq_{j-1} + q_{j-2}) - q_{j-1} + 1 \\ &= q_{j-1}(r + sd_j - 1) + sq_{j-2} + 1. \end{aligned}$$

Par hypothèse de récurrence, nous avons $s \in \{-1, 0, 1\}$. Donc, il en découle

$$q_{j-1}w_j \geq q_{j-1}(r + sd_j - 1) - q_{j-2} + 1.$$

De plus, comme $q_{j-1} \geq q_{j-2}$, alors $-q_{j-2} + 1 > -q_{j-1}$. Ainsi, nous obtenons

$$q_{j-1}w_j > q_{j-1}(r + sd_j - 1) - q_{j-1} = q_{j-1}(r + sd_j - 2).$$

Puisque $q_{j-1} \geq 1$, alors l'inégalité devient

$$w_j > r + sd_j - 2.$$

Regroupons les deux inégalités, nous obtenons :

$$\begin{aligned} r + sd_j - 2 < w_j &\leq r + sd_j + 1 \\ r + sd_j - 2 < r + sd_j - t &\leq r + sd_j + 1 \\ -2 < -t &\leq 1. \end{aligned}$$

Nous pouvons en conclure que $t \in \{-1, 0, 1\}$. □

L'automate représenté dans la figure 4.1 (version modifiée de [3, Fig. 2]) est en fait l'automate \mathcal{A} . En effet, il a été construit de la manière suivante :

- L'ensemble des états est $\{-1, 0, 1\} \times \{-1, 0, 1\}$ (le puits est implicite).
- L'état initial est $(0, 0)$.
- Les états finals sont $(-1, 0)$, $(0, 0)$ et $(1, 0)$.
- Pour chaque état (r, s) , pour tout $d \in \mathbb{N}$, il y a trois arcs sortants vers les états (s, t) (où $t \in \{-1, 0, 1\}$) en lisant respectivement les entrées $(d, r + sd - t)$ (où $t \in \{-1, 0, 1\}$). Il y a donc une infinité d'arcs.

De plus, cet automate a été construit de manière à ce qu'il respecte bien l'invariant (4.1).

Corollaire 4.1.3. Soit $\alpha = [0; d_1, d_2, \dots]$. L'automate \mathcal{A} accepte l'entrée

$$(d_k \cdots d_1, w_k \cdots w_1) \in \mathbb{N}^k \times \mathbb{Z}^k$$

si et seulement si $[w_1 \dots w_k]_\alpha = 0$.

Démonstration. Supposons que l'entrée $(d_k \cdots d_1, w_k \cdots w_1)$ est acceptée par \mathcal{A} . Puisque \mathcal{A} satisfait l'invariant (4.1) et que l'état initial de \mathcal{A} est $(0, 0)$, alors on a

$$[w_1 \dots w_k]_\alpha = \sum_{j=0}^{k-1} w_{j+1} q_j = 0 \cdot q_{k-1} + 0 \cdot q_k = 0.$$

Supposons maintenant que $[w_1, \dots, w_k]_\alpha = 0$. Alors, puisque l'automate \mathcal{A} satisfait l'invariant, l'entrée $(d_k \cdots d_1, w_k \cdots w_1)$ est acceptée par \mathcal{A} si on part de l'état $(0, 0)$. Or, l'état $(0, 0)$ est l'état initial donc l'entrée est bien acceptée par \mathcal{A} . □

Rappelons que l'objectif de cette section est de construire l'automate fini à 4 bandes sur un alphabet \mathbb{N} tel que

$$(d_1 \cdots d_m, x_1 \cdots x_m, y_1 \cdots y_m, z_1 \cdots z_m) \in (\mathbb{N}^m)^4$$

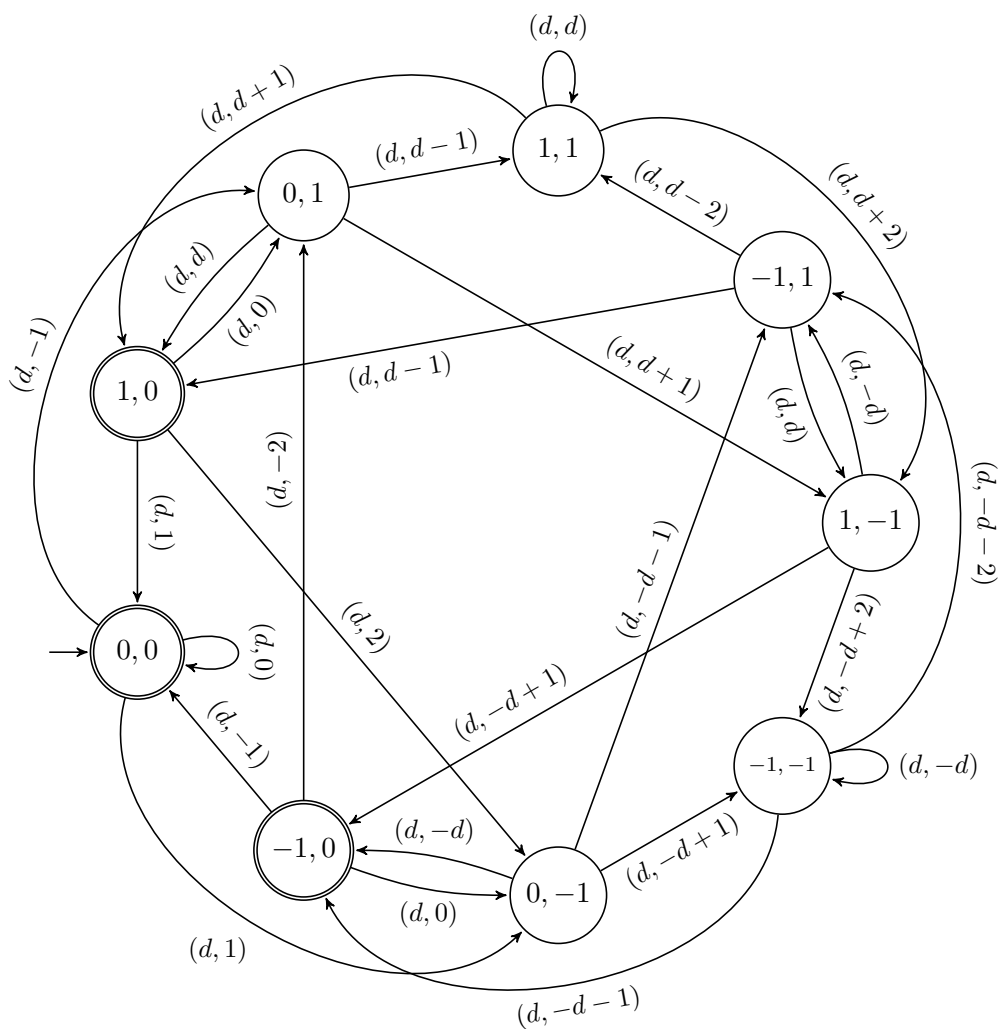


FIGURE 4.1 – L'automate \mathcal{A} qui accepte l'entrée $(d_k \cdots d_1, w_k \cdots w_1) \in \mathbb{N}^k \times \mathbb{Z}^k$ si et seulement si, pour tout irrationnel $\alpha = [0; d_1, d_2, \dots]$, on a $[w_1 \dots w_k]_\alpha = 0$

soit accepté si et seulement si, pour tout irrationnel α tel que $\alpha = [0; d_1, \dots, d_m, \dots]$, les mots $x_1 \cdots x_m$, $y_1 \cdots y_m$ et $z_1 \cdots z_m$ sont trois α -représentations d'Ostrowski de nombres naturels telles que

$$[x_1 \cdots x_m]_\alpha + [y_1 \cdots y_m]_\alpha = [z_1 \cdots z_m]_\alpha.$$

Maintenant que nous avons construit l'automate \mathcal{A} , nous pouvons le modifier afin d'obtenir l'automate voulu. Nous partons de \mathcal{A} et nous transformons tous ses états finals en états initiaux (et vice versa). Ensuite, nous prenons chaque transition partant d'un état (r, s) et arrivant dans l'état $(s, r + sd - w)$ en lisant une entrée (d, w) , et nous la remplaçons par la transition qui part de l'état $(s, r + sd - w)$ et arrive dans l'état (r, s) en lisant l'entrée $(d, x, y, x + y - w)$. Ainsi, l'automate obtenu est exactement l'automate fini à 4 bandes que nous désirions.

Exemple 4.1.4. Soient $x = 51$, $y = 102$ et $z = 153$. Ainsi $x + y = z$. Soit

$$\alpha = [0; d_1, d_2, \dots] = [0; 2, 3, 4, 5, \dots].$$

Alors, tout naturel X peut être écrit selon la décomposition donnée par l'équation (2.1). Les premiers termes de la décomposition sont

$$X = 1b_1 + 2b_2 + 7b_3 + 30b_4 + 157b_5 + \dots$$

où $b_1 < 2$, $b_2 \leq 3$, $b_3 \leq 4$, $b_4 \leq 5$ et $b_5 \leq 6$. Nous pouvons en déduire les α -représentations d'Ostrowski de x, y et z . Nous avons

$$\begin{aligned} x = 51 &= 1.30 + 3.7 = [0031]_\alpha, \\ y = 102 &= 3.30 + 1.7 + 2.2 + 1.1 = [1213]_\alpha, \\ z = 153 &= 5.30 + 1.2 + 1.1 = [1105]_\alpha. \end{aligned}$$

Posons $w_i = z_i - x_i - y_i$ pour tout $i \in \{1, \dots, 4\}$. D'où

$$\begin{aligned} w_1 &= 1 - 1 - 0 = 0, \\ w_2 &= 1 - 2 - 0 = -1, \\ w_3 &= 0 - 1 - 3 = -4, \\ w_4 &= 5 - 3 - 1 = 1. \end{aligned}$$

Par le corollaire 4.1.3, nous savons que l'entrée $(d_4 d_3 d_2 d_1, w_4 w_3 w_2 w_1)$ est acceptée par l'automate \mathcal{A} (représenté dans la figure 4.1) si et seulement si $[w_1 w_2 w_3 w_4]_\alpha = 0$, ce qui est vrai si et seulement si $x + y = z$. Donc, l'automate \mathcal{A} devrait accepter l'entrée

$$(5 \ 4 \ 3 \ 2, 1 \ -4 \ -1 \ 0).$$

Vérifions que c'est bien le cas. On part de l'état $(0, 0)$. En lisant $(5, 1)$, on arrive dans l'état $(0, -1)$. Puis, on lit $(4, -4)$ et on arrive dans l'état $(-1, 0)$. Ensuite, en lisant $(3, -1)$, on

retourne dans l'état $(0, 0)$. Et finalement, on lit $(2, 0)$ et on reste dans l'état $(0, 0)$ qui est bien un état final.

De plus, l'automate à 4 bandes accepte l'entrée $(2\ 3\ 4\ 5, 0\ 0\ 3\ 1, 1\ 2\ 1\ 3, 1\ 1\ 0\ 5)$. En effet, si nous partons de l'état $(0, 0)$, en lisant l'entrée $(2, 0, 1, 1)$, nous arrivons dans l'état $(0, 0)$. Puis, nous lisons l'entrée $(3, 0, 2, 1)$ et arrivons dans l'état $(-1, 0)$. Ensuite, en lisant l'entrée $(4, 3, 1, 0)$, nous nous retrouvons dans l'état $(0, -1)$. Finalement, nous lisons l'entrée $(5, 1, 3, 5)$ et retournons dans l'état $(0, 0)$ qui est bien un état final de l'automate à 4 bandes.

4.2 Addition de codages binaires de représentations d'Ostrowski

Dans cette section, nous allons construire un automate de Büchi qui accepte l'addition de codages binaires de représentations d'Ostrowski de naturels. Nous avons construit dans la section précédente un automate qui accepte l'addition de représentations d'Ostrowski de naturels. Le problème de cet automate est qu'il possède un nombre infini d'arcs puisqu'il est défini sur les naturels. En pratique, cela nécessiterait donc des ressources infinies pour implémenter cet automate. C'est pourquoi, dans cette section, nous allons modifier cet automate afin qu'il soit défini sur l'alphabet fini $\Sigma_{\#}$. Nous allons ensuite étendre ce résultat pour qu'un automate de Büchi accepte l'addition modulo 1 sur I_{α} pour tout irrationnel $\alpha \in]0, 1[$.

Définition 4.2.1. Soit $v \in R$. Nous définissons les ensembles suivants :

$$\begin{aligned} \oplus^{\text{fin}} &= \{(v, s_1, s_2, s_3) : v \in R, s_1, s_2, s_3 \in A_v^{\text{fin}}, Z_v(s_1) + Z_v(s_2) = Z_v(s_3)\}, \\ \oplus_v^{\text{fin}} &= \{(s_1, s_2, s_3) : s_1, s_2, s_3 \in A_v^{\text{fin}}, Z_v(s_1) + Z_v(s_2) = Z_v(s_3)\}. \end{aligned}$$

Théorème 4.2.2. L'ensemble \oplus^{fin} est ω -régulier.

Démonstration. Dans la section précédente, nous avons construit un automate à 4 bandes sur un alphabet \mathbb{N} tel que l'entrée $(d_1 \cdots d_m, x_1 \cdots x_m, y_1 \cdots y_m, z_1 \cdots z_m) \in (\mathbb{N}^m)^4$ est accepté par l'automate si et seulement si, pour tout irrationnel α tel que $\alpha = [0; d_1, \dots, d_m, \dots]$, les mots $x_1 \cdots x_m$, $y_1 \cdots y_m$ et $z_1 \cdots z_m$ sont trois α -représentations d'Ostrowski de nombres naturels telles que

$$[x_1 \cdots x_m]_{\alpha} + [y_1 \cdots y_m]_{\alpha} = [z_1 \cdots z_m]_{\alpha}.$$

Notons \mathcal{A}' cet automate à 4 bandes et construisons \mathcal{B} un automate de Büchi à 4 bandes à partir de \mathcal{A}' pour prouver que \oplus^{fin} est ω -régulier. On prend $\Sigma_{\#}$ comme alphabet pour le nouvel automate. Pour la construction de \mathcal{B} , on procède de la manière suivante :

1. On part de \mathcal{A}' .

2. On crée un nouvel état i qui sera l'unique état initial de \mathcal{B} . On ajoute également les transitions $(i, (\#, \#, \#, \#), j)$ pour tout j appartenant aux états initiaux de \mathcal{A}' . Ainsi, on s'assure de toujours commencer par lire le tuple $(\#, \#, \#, \#)$.
3. On remplace chaque transition de \mathcal{A}' par un sous-automate qui accepte les relations correspondantes en binaire. Nous allons détailler certaines des transitions et les autres peuvent être obtenues par des raisonnements similaires. Nous pouvons repartir des étiquettes des transitions de l'automate \mathcal{A} représenté dans la figure 4.1 puisque les transitions de \mathcal{A}' sont obtenues à partir de celles de \mathcal{A} . Nous rappelons que si une transition va d'un état p à un état q dans \mathcal{A}' , la transition correspondante dans \mathcal{A} va de q à p .

- (a) Considérons une transition étiquetée $(d, 1)$ dans \mathcal{A} dont la transition correspondante dans \mathcal{A}' va d'un état p à un état q . Alors, nous voulons que l'automate acceptant la relation correspondante en binaire accepte une entrée de longueur l $(v_1 \cdots v_l, s_{1,1} \cdots s_{1,l}, s_{2,1} \cdots s_{2,l}, s_{3,1} \cdots s_{3,l})$ si

$$[s_{3,1} \cdots s_{3,l}]_2 - [s_{1,1} \cdots s_{1,l}]_2 - [s_{2,1} \cdots s_{2,l}]_2 = 1.$$

Cet automate est représenté dans la figure 4.2. En effet, si nous notons p_i le poids $s_{3,i} - s_{1,i} - s_{2,i}$ pour tout $i \in \{1, \dots, l\}$ et si nous posons

$$\nu := [s_{3,1} \cdots s_{3,l}]_2 - [s_{1,1} \cdots s_{1,l}]_2 - [s_{2,1} \cdots s_{2,l}]_2,$$

alors,

$$\nu = \sum_{i=1}^l w_i 2^{i-1}.$$

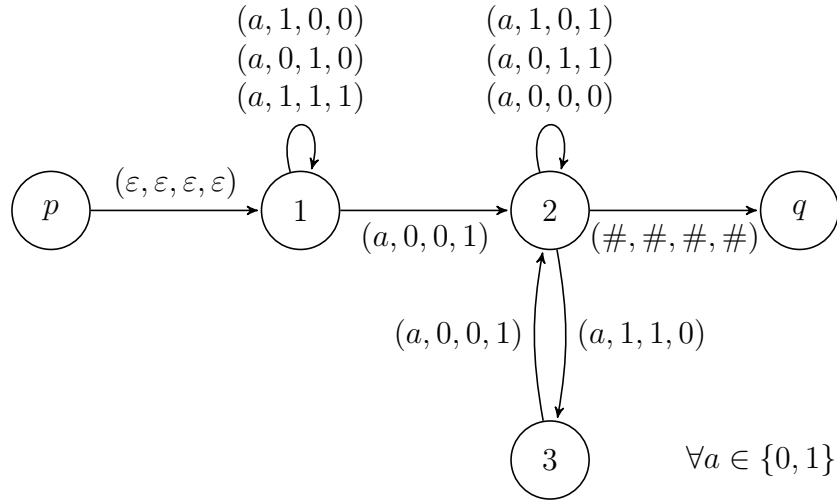
On peut boucler sur l'état 1 si le poids vaut -1 , puis on passe de l'état 1 à l'état 2 si le poids est égal à 1, cela apporte une contribution de 1 à ν . Ensuite, on peut boucler sur l'état 2 si le poids vaut 0 et cela ne modifie pas la valeur de ν . Finalement, on peut passer de l'état 2 à l'état 3 si le poids suivant vaut -2 , puis directement retourner dans l'état 2 si le poids vaut 1 et cela ne modifie pas la valeur de ν .

- (b) Considérons une transition étiquetée $(d, 2)$ dans \mathcal{A} dont la transition correspondante dans \mathcal{A}' va d'un état p à un état q . Alors, nous voulons que l'automate acceptant la relation correspondante en binaire accepte une entrée de longueur l $(v_1 \cdots v_l, s_{1,1} \cdots s_{1,l}, s_{2,1} \cdots s_{2,l}, s_{3,1} \cdots s_{3,l})$ si

$$[s_{3,1} \cdots s_{3,l}]_2 - [s_{1,1} \cdots s_{1,l}]_2 - [s_{2,1} \cdots s_{2,l}]_2 = 2.$$

Cet automate est représenté dans la figure 4.3. En effet, si nous notons p_i le poids $s_{3,i} - s_{1,i} - s_{2,i}$ pour tout $i \in \{1, \dots, l\}$ et si nous posons

$$\nu := [s_{3,1} \cdots s_{3,l}]_2 - [s_{1,1} \cdots s_{1,l}]_2 - [s_{2,1} \cdots s_{2,l}]_2,$$


 FIGURE 4.2 – Automate traduisant en binaire la transition de \mathcal{A} étiquetée $(d, 1)$

alors,

$$\nu = \sum_{i=1}^l w_i 2^{i-1}.$$

On passe de l'état p à l'état 1 si $p_1 = 0$, ce qui apporte une contribution de 0 à ν . Ensuite, on peut boucler sur l'état 1 tant que le poids est égal à -1 et on passe à l'état 2 si le poids vaut 1, cela apporte une contribution de 2 à ν . On peut boucler sur l'état 2 si le poids vaut 0 et cela ne modifie pas la valeur de ν . Finalement, on peut passer de l'état 2 à l'état 3 si le poids vaut -2 , puis directement retourner dans l'état 2 si le poids suivant vaut 1, et cela ne modifie pas la valeur de ν .

- (c) Considérons une transition étiquetée $(d, -d)$ dans \mathcal{A} dont la transition correspondante dans \mathcal{A}' va d'un état p à un état q . Alors, nous voulons que l'automate acceptant la relation correspondante en binaire accepte une entrée de longueur l $(v_1 \cdots v_l, s_{1,1} \cdots s_{1,l}, s_{2,1} \cdots s_{2,l}, s_{3,1} \cdots s_{3,l})$ si

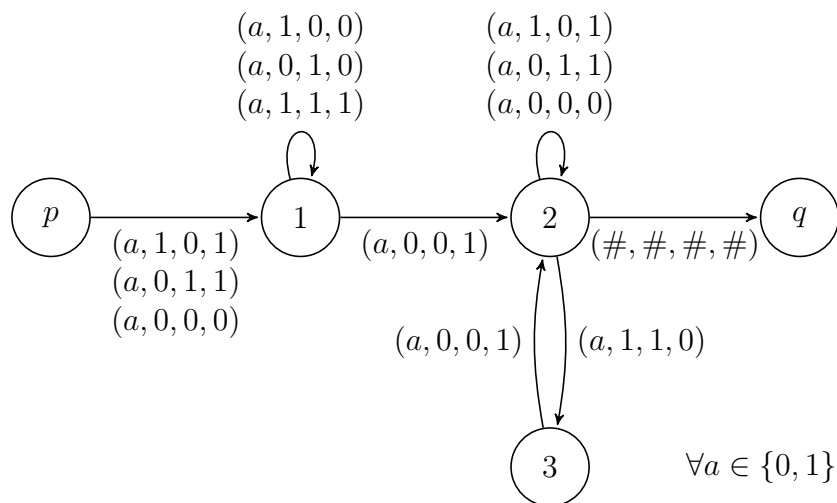
$$[v_1 \cdots v_l]_2 + [s_{3,1} \cdots s_{3,l}]_2 - [s_{1,1} \cdots s_{1,l}]_2 - [s_{2,1} \cdots s_{2,l}]_2 = 0.$$

Cet automate est représenté dans la figure 4.4. En effet, si nous notons p_i le poids $v_i + s_{3,i} - s_{1,i} - s_{2,i}$ pour tout $i \in \{1, \dots, l\}$ et si nous posons

$$\nu := [v_1 \cdots v_l]_2 + [s_{3,1} \cdots s_{3,l}]_2 - [s_{1,1} \cdots s_{1,l}]_2 - [s_{2,1} \cdots s_{2,l}]_2,$$

alors,

$$\nu = \sum_{i=1}^l w_i 2^{i-1}.$$


 FIGURE 4.3 – Automate traduisant en binaire la transition de \mathcal{A} étiquetée $(d, 2)$

Nous pouvons boucler sur l'état 1 si le poids vaut zéro et cela apporte une contribution de 0 à ν . Nous pouvons également passer de l'état 1 à l'état 2 si le poids vaut -2 , puis directement retourner dans l'état 1 si le poids suivant vaut 1 et cela apporte une contribution de 0 à ν .

4. L'état final de \mathcal{B} est exactement le même que dans l'automate \mathcal{A}' .
5. Puisque R et A^{fin} sont ω -réguliers, nous pouvons construire un automate de Büchi qui accepte $\{(v, s_1, s_2, s_3) : v \in R, s_1, s_2, s_3 \in A_v^{\text{fin}}\}$. Nous prenons alors l'intersection de cet automate avec l'automate \mathcal{B} , ce qui préserve l' ω -régularité au vu de la proposition 2.1.2.

Ainsi, l'automate construit accepte les tuples $(v, s_1, s_2, s_3) \in R \times (A_v^{\text{fin}})^3$ tels que

$$Z_v(s_1) + Z_v(s_2) = Z_v(s_3).$$

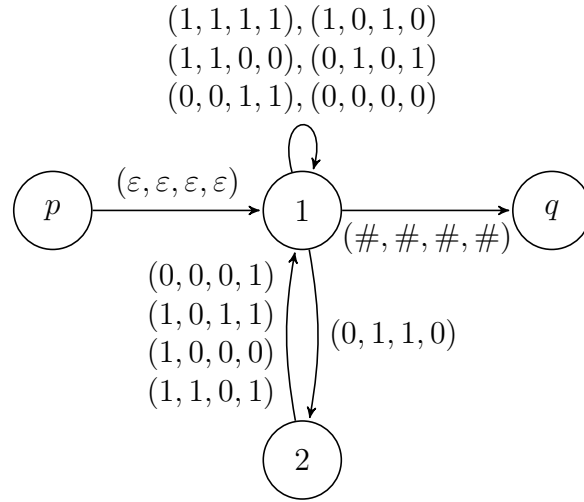
Or, l'ensemble de ces tuples est \oplus^{fin} , ce qui prouve son ω -régularité. \square

Maintenant, nous allons étendre l'automate construit dans la preuve du théorème 4.2.2 pour obtenir un automate de Büchi qui accepte l'addition modulo 1 sur I_α pour tout irrationnel $\alpha \in]0, 1[$.

Définition 4.2.3. Soit $v \in R$. Nous définissons les ensembles suivants :

$$\begin{aligned} \oplus &= \{(v, s_1, s_2, s_3) : v \in R, s_1, s_2, s_3 \in A_v, O_v(s_1) + O_v(s_2) \equiv O_v(s_3) \pmod{1}\}, \\ \oplus_v &= \{(s_1, s_2, s_3) : s_1, s_2, s_3 \in A_v, O_v(s_1) + O_v(s_2) \equiv O_v(s_3) \pmod{1}\}. \end{aligned}$$

Proposition 4.2.4. Soit \mathcal{B} un automate de Büchi sur un alphabet Σ tel que tous ses états sont finaux. Soit $w \in \Sigma^\omega$. Soit $(u_n)_{n \in \mathbb{N}}$ une suite de mots de Σ^ω telle que les n premières lettres de u_n sont les mêmes que celles de w pour tout naturel n . Si u_n est accepté par \mathcal{B} pour tout naturel n , alors w est aussi accepté par \mathcal{B} .


 FIGURE 4.4 – Automate traduisant en binaire la transition de \mathcal{A} étiquetée $(d, -d)$

Cette proposition est une conséquence du lemme de König (preuve analogue dans [10, Lemma 4.3]).

Si $w = w_1 w_2 \cdots \in \Sigma^\omega$, alors nous notons $w[i \cdots j]$ le facteur $w_i w_{i+1} \cdots w_{j-1} w_j$.

Lemme 4.2.5. L'ensemble \oplus est ω -régulier. De plus, $\oplus^{\text{fin}} \subset \oplus$.

Démonstration. Démontrons d'abord l'inclusion. Soit $(v, s_1, s_2, s_3) \in \oplus^{\text{fin}}$. Par le lemme 3.3.15, pour tout $s \in A_v^{\text{fin}}$, nous savons que

$$\alpha(v)Z_v(s) - O_v(s) \equiv 0 \pmod{1}.$$

Ainsi,

$$\begin{aligned} O_v(s_3) &\equiv \alpha(v)Z_v(s_3) \pmod{1} \\ &\equiv \alpha(v)Z_v(s_1) + \alpha(v)Z_v(s_2) \pmod{1} \\ &\equiv O_v(s_1) + O_v(s_2) \pmod{1}. \end{aligned}$$

D'où $(v, s_1, s_2, s_3) \in \oplus$.

Démontrons maintenant que \oplus est ω -régulier. Soit \mathcal{B}^{fin} un automate de Büchi acceptant l'ensemble \oplus^{fin} . Supposons que \mathcal{B}^{fin} est émondé (i.e. les états inaccessibles depuis les états initiaux et les états ne permettant pas d'atteindre un état final ont été retirés). Nous notons \mathcal{B}' l'automate \mathcal{B}^{fin} où tous les états sont finaux, et $S = L(\mathcal{B}')$.

Soit $v \in R$. Rappelons que si X, Y sont deux ensembles et Z un sous-ensemble de $X \times Y$, alors, pour tout $x \in X$, nous notons Z_x l'ensemble $\{y \in Y : (x, y) \in Z\}$.

Si nous montrons que $S_v = \oplus_v$, alors nous aurons prouvé que \oplus est ω -régulier par ω -régularité de S . Soient $s_1, s_2, s_3 \in A_v$. Démontrons que

$$(s_1, s_2, s_3) \in \oplus_v \Leftrightarrow (s_1, s_2, s_3) \in S_v.$$

Supposons d'abord que $(s_1, s_2, s_3) \in \oplus_v$. Par définition, nous avons

$$O_v(s_1) + O_v(s_2) \equiv O_v(s_3) \pmod{1}.$$

Par propriétés des représentations d'Ostrowski, nous allons construire $(s_{m,1}, s_{m,2}, s_{m,3})_{m \in \mathbb{N}}$ une suite de $(A_v^{\text{fin}})^3$ telle que

1. les m premières lettres de $s_{m,i}$ sont les mêmes que celles de s_i pour tout $i \in \{1, 2, 3\}$,
2. $O_v(s_{m,1}) + O_v(s_{m,2}) \equiv O_v(s_{m,3}) \pmod{1}$.

Rappelons que v est de la forme

$$v = \#v_1\#v_2\#\dots$$

Comme $s_1, s_2, s_3 \in A_v$, alors pour tout $i \in \{1, 2, 3\}$, on a

$$s_i = \#s_{i,1}\#s_{i,2}\#s_{i,3}\#\dots \quad (4.3)$$

tel que

1. $[s_{i,1}]_2 < [v_1]_2$;
2. $[s_{i,k}]_2 \leq [v_k]_2$ pour tout $k > 1$;
3. Si $[s_{i,k}]_2 = [v_k]_2$, alors $[w_{k-1}]_2 = 0$, pour tout $k > 1$;
4. $[s_{i,k}]_2 \neq [v_k]_2$ pour une infinité de k impairs.

Or, pour appartenir à A_v^{fin} , il faut non seulement respecter les 3 premières conditions ci-dessus, mais également contenir un nombre fini de 1. Ainsi, pour tout $i \in \{1, 2, 3\}$, pour tout $m \in \mathbb{N}$, nous posons

$$s_{m,i} := s_i[1 \dots m]x_i$$

où $x_i \in \{0, 1, \#\}^\omega$ tel que x_i respecte les 3 premières conditions ci-dessus, contient un nombre fini de 1 et un nombre infini de $\#$ (i.e. $s_{m,i} = \#s_{m,i,1}\#s_{m,i,2}\#\dots$) et tel que

$$\sum_{n \geq 0} \beta_n([s_{m,1,n}]_2 + [s_{m,2,n}]_2 - [s_{m,3,n}]_2) \in \mathbb{Z}$$

où β_n est la n -ème différence de $\alpha(v)$.

Nous avons $(A_v^{\text{fin}})^3 \cap \oplus_v = \oplus_v^{\text{fin}}$. En effet, nous avons montré précédemment que $\oplus^{\text{fin}} \subset \oplus$. De plus, si $(s_1, s_2, s_3) \in (A_v^{\text{fin}})^3 \cap \oplus_v$, alors il existe des entiers u_1, u_2, u_3, u_4 tels que

$$\begin{aligned} O_v(s_1) + O_v(s_2) &= O_v(s_3) + u_4 \\ \Leftrightarrow \alpha(v)Z_v(s_1) + u_1 + \alpha(v)Z_v(s_2) + u_2 &= \alpha(v)Z_v(s_3) + u_3 + u_4 \\ \Leftrightarrow \alpha(v)(Z_v(s_1) + Z_v(s_2) - Z_v(s_3)) &= u_3 + u_4 - u_1 - u_2. \end{aligned}$$

Le premier membre est soit un nombre irrationnel, soit vaut zéro. Or, puisque le deuxième membre est un entier, alors le premier membre doit valoir zéro, ce qui est le cas si et seulement si

$$Z_v(s_1) + Z_v(s_2) - Z_v(s_3) = 0.$$

Donc, on obtient que $(s_1, s_2, s_3) \in \oplus_v^{\text{fin}}$.

Ainsi, pour tout naturel m , on a $(v, s_{m,1}, s_{m,2}, s_{m,3}) \in \oplus_v^{\text{fin}}$ et est donc accepté par l'automate \mathcal{B}^{fin} et par conséquent aussi par l'automate \mathcal{B}' . Par la proposition 4.2.4, nous savons que (v, s_1, s_2, s_3) est accepté par \mathcal{B}' et donc que $(s_1, s_2, s_3) \in S_v$.

Supposons maintenant que $(s_1, s_2, s_3) \in S_v$. Alors, (v, s_1, s_2, s_3) est accepté par l'automate \mathcal{B}' . Pour tout $i \in \{1, 2, 3\}$, pour tout m naturel, posons $w_{m,i} \in \Sigma_{\#}^*$ tel que $w_{m,i}$ est le préfixe de s_i s'arrêtant au $(m+1)$ -ème $\#$. Puisque \mathcal{B}^{fin} est émondé, alors il existe $s_{m,1}, s_{m,2}, s_{m,3} \in A_v^{\text{fin}}$ des extensions de $w_{m,1}, w_{m,2}, w_{m,3}$ telles que $(v, s_{m,1}, s_{m,2}, s_{m,3})$ est accepté par \mathcal{B}^{fin} . Ainsi, on a $(s_{m,1}, s_{m,2}, s_{m,3}) \in \oplus_v^{\text{fin}}$. Posons

$$x = O_v(s_1), \quad y = O_v(s_2), \quad z = O_v(s_3),$$

et, pour tout m naturel, posons

$$x_m = O_v(s_{m,1}), \quad y_m = O_v(s_{m,2}), \quad z_m = O_v(s_{m,3}).$$

Par la proposition 2.3.21, on a

$$\lim_{m \rightarrow +\infty} (x_m, y_m, z_m) = (x, y, z).$$

Comme $(s_{m,1}, s_{m,2}, s_{m,3}) \in \oplus_v^{\text{fin}}$ et que $\oplus_v^{\text{fin}} \subset \oplus_v$, alors

$$x_m + y_m \equiv z_m \pmod{1},$$

d'où

$$x + y \equiv z \pmod{1}.$$

Ainsi, nous obtenons que $(s_1, s_2, s_3) \in \oplus_v$. □

Notations 4.2.6. Soit $v \in R$.

- Si $(s_1, s_2, s_3) \in \oplus_v^{\text{fin}}$, alors nous notons $s_1 \oplus_v^{\text{fin}} s_2 = s_3$.
- Si $(t_1, t_2, t_3) \in \oplus_v$, alors nous notons $t_1 \oplus_v t_2 = t_3$.

Chapitre 5

Structures et décidabilité

Dans ce chapitre, nous allons établir différents résultats de décidabilité afin de prouver que la théorie du premier ordre de la collection d'extensions de l'arithmétique de Presburger par un mot sturmien interprété comme une fonction unaire est décidable. Pour cela, nous allons introduire le concept de structures et nous intéresser à une structure en particulier : \mathcal{R}_α (où α est un réel strictement positif).

5.1 Structures ω -régulières

Dans cette section, nous introduisons quelques définitions et présentons certains résultats qui nous seront utiles dans la suite du chapitre.

Définitions 5.1.1. Une **structure logique** \mathcal{M} est un tuple $(M; R_1, \dots, R_m)$ où

- M est un ensemble non vide (appelé le **domaine** de \mathcal{M}),
- R_1, \dots, R_m sont des relations sur M . (La liste des relations de \mathcal{M} est appelée la **signature** de \mathcal{M} .)

Si on note \mathcal{L} la signature de \mathcal{M} , alors on dit que \mathcal{M} est une **\mathcal{L} -structure**.

Soient deux structures $(M; R_1, \dots, R_m)$ et $(N; S_1, \dots, S_m)$ telles que R_i et S_i aient la même arité (notée $ar(i)$) pour tout $i \in \{1, \dots, m\}$. Ces **structures** sont dites **isomorphes** s'il existe f une fonction bijective de M dans N telle que, pour tout $i \in \{1, \dots, m\}$, on a $x \in R_i$ si et seulement si $f(x) \in S_i$ pour tout $x \in M^{ar(i)}$.

Une **structure** $\mathcal{M} = (M; R_1, \dots, R_m)$ est **ω -régulière** si son domaine M et ses relations R_1, \dots, R_m sont ω -réguliers.

Soient \mathcal{L} une signature et \mathcal{M} une \mathcal{L} -structure. La **théorie du premier ordre de \mathcal{M}** est l'ensemble des \mathcal{L} -formules closes (i.e. ne contenant pas de variables libres) vraies dans \mathcal{M} et est notée $\text{FO}(\mathcal{M})$. La signature de $\text{FO}(\mathcal{M})$ est la signature de \mathcal{M} .

Une **théorie** est dite **décidable**, si on peut décider si une formule close est vraie ou fausse.

Proposition 5.1.2. Si \mathcal{U} est une structure ω -régulière, alors la théorie $\text{FO}(\mathcal{U})$ est décidable.

Cette proposition est démontrée dans [5].

Définition 5.1.3. Fixons $m \in \mathbb{N}$ et une fonction $\text{ar} : \{1, \dots, m\} \rightarrow \mathbb{N}$. Soit un ensemble Z . Pour tout $z \in Z$, soit une structure $\mathcal{U}_z = (U_z; R_{1,z}, \dots, R_{m,z})$ telle que $R_{i,z} \subseteq U_z^{\text{ar}(i)}$. On dit que $(\mathcal{U}_z)_{z \in Z}$ est une **famille uniforme de structures ω -régulières** si

- l'ensemble $\{(z, y) : z \in Z, y \in U_z\}$ est ω -régulier, et
- l'ensemble $\{(z, y_1, \dots, y_{\text{ar}(i)}) : z \in Z, (y_1, \dots, y_{\text{ar}(i)}) \in R_{i,z}\}$ est ω -régulier pour tout $i \in \{1, \dots, m\}$.

On note $\text{FO}(\{\mathcal{U}_z : z \in Z\})$ l'ensemble des formules closes vraies sur \mathcal{U}_z pour tout $z \in Z$.

Proposition 5.1.4. Soient $(\mathcal{U}_z)_{z \in Z}$ une famille uniforme de structures ω -régulières et φ une formule écrite avec la signature de ces structures. Alors l'ensemble

$$\{(z, y) : z \in Z, y \in U_z, \mathcal{U}_z \models \varphi(y)\}$$

est ω -régulier, et l'automate acceptant cet ensemble peut être construit effectivement. De plus, la théorie $\text{FO}(\{\mathcal{U}_z : z \in Z\})$ est décidable.

Démonstration. Si φ est une formule atomique, alors la proposition découle directement de la définition de famille uniforme de structures ω -régulières. De plus, par la proposition 2.1.2, la propriété reste vraie pour toute formule φ . On peut conclure par le théorème de Büchi sur la décidabilité de la théorie monadique du second ordre [5]. \square

5.2 La structure \mathcal{R}_α

Dans cette section, nous allons nous intéresser de près à la structure \mathcal{R}_α et à des résultats de décidabilité qui la concernent. Ces résultats seront essentiels pour discuter de la décidabilité de propriétés sur les mots sturmiens.

Nous notons \mathcal{L}_m la signature¹ de la théorie $\text{FO}(\mathbb{R}, <, +, \mathbb{Z})$ et $\mathcal{L}_{m,a}$ la signature obtenue en ajoutant un symbole de fonction unaire a à \mathcal{L}_m .

Soit $\alpha \in \mathbb{R}_0^+$. Nous notons \mathcal{R}_α la $\mathcal{L}_{m,a}$ -structure $(\mathbb{R}, <, +, \mathbb{Z}, \alpha \mathbb{Z})$.

Dans cette section, nous allons nous intéresser à la décidabilité de la théorie du premier ordre de la structure \mathcal{R}_α .

Théorème 5.2.1. Si $\alpha \in \mathbb{Q}$, alors $\text{FO}(\mathcal{R}_\alpha)$ est décidable.

1. En logique, on parle en général du langage de la théorie.

Lorsque α est un rationnel, alors la structure \mathcal{R}_α peut se réécrire $(\mathbb{R}, <, +, \mathbb{Z})$. Or, Weispfenning [26] a prouvé que la théorie du premier ordre de de cette structure est décidable.

Théorème 5.2.2. Si α est un irrationnel quadratique, alors $\text{FO}(\mathcal{R}_\alpha)$ est décidable.

Ce théorème a été prouvé dans [12]. Cependant, ces deux théorèmes ne sont pas suffisants pour nous permettre de discuter de la décidabilité de propriétés sur les mots sturmiens. C'est pourquoi, nous allons nous intéresser à \mathcal{R}_α quand α est irrationnel.

Dans les chapitres précédents, nous avons prouvé que $A^{\text{fin}}, \prec^{\text{fin}}, \oplus^{\text{fin}}, A, \prec$ et \oplus sont ω -réguliers. Nous souhaitons établir un lien entre ces ensembles et la structure \mathcal{R}_α quand α est un irrationnel. Autrement dit, le but sera de passer d'une addition et d'un ordre sur les naturels (dans les systèmes de numérations d'Ostrowski) à une addition et un ordre sur les réels (dans \mathcal{R}_α). Pour cela, nous allons passer par la structure

$$([- \alpha(v), +\infty[, <, +, \mathbb{N}, \alpha(v)\mathbb{N})$$

où $v \in R$, et établir des isomorphismes entre certaines structures afin d'établir un résultat de décidabilité pour la collection de \mathcal{R}_α tels que α est un irrationnel.

Remarque 5.2.3. Par le lemme 3.3.10, nous savons que la fonction $Z_v : A_v^{\text{fin}} \rightarrow \mathbb{N}$ est bijective. Nous savons également que, pour tout $v \in R$, pour tout $s_1, s_2, s_3 \in A_v^{\text{fin}}$, on a $s_1 \prec_v^{\text{fin}} s_2$ si et seulement si $Z_v(s_1) < Z_v(s_2)$ et on a $s_1 \oplus_v^{\text{fin}} s_2 = s_3$ si et seulement si $Z_v(s_1) + Z_v(s_2) = Z_v(s_3)$. Il en découle que

$$Z_v : (A_v^{\text{fin}}, \prec_v^{\text{fin}}, \oplus_v^{\text{fin}}) \rightarrow (\mathbb{N}, <, +)$$

est un isomorphisme pour tout $v \in R$. Or, nous pouvons établir une bijection entre \mathbb{N} et $\alpha(v)\mathbb{N}$ pour tout $v \in R$. De plus, pour tout $v \in R$, pour tout $s_1, s_2, s_3 \in A_v^{\text{fin}}$, on a $s_1 \prec_v^{\text{fin}} s_2$ si et seulement si $\alpha(v)Z_v(s_1) < \alpha(v)Z_v(s_2)$ et on a $s_1 \oplus_v^{\text{fin}} s_2 = s_3$ si et seulement si $\alpha(v)Z_v(s_1) + \alpha(v)Z_v(s_2) = \alpha(v)Z_v(s_3)$. Ainsi, il en découle que

$$\alpha(v)Z_v : (A_v^{\text{fin}}, \prec_v^{\text{fin}}, \oplus_v^{\text{fin}}) \rightarrow (\alpha(v)\mathbb{N}, <, +)$$

est un isomorphisme pour tout $v \in R$.

Lemme 5.2.4. Soit $v \in R$. Soient $t_1, t_2, t_3 \in A_v$ tels que $t_1 \oplus_v t_2 = t_3$. Alors, nous avons

$$O_v(t_1) + O_v(t_2) = \begin{cases} O_v(t_3) + 1 & \text{si } 0_v \prec_v t_1 \text{ et } t_3 \prec_v t_2, \\ O_v(t_3) - 1 & \text{si } t_1 \prec_v 0_v \text{ et } t_2 \prec_v t_3, \\ O_v(t_3) & \text{sinon.} \end{cases}$$

Démonstration. Soit $v \in R$. Soient $t_1, t_2, t_3 \in A_v$ tels que $t_1 \oplus_v t_2 = t_3$. Par souci de lisibilité, nous noterons $\alpha = \alpha(v)$ et $x_i = O_v(t_i)$ pour tout $i \in \{1, 2, 3\}$. Par définition de la fonction O_v , nous avons $x_1, x_2, x_3 \in I_\alpha$. Et par définition de l'ensemble \oplus_v , on a

$x_1 + x_2 \equiv x_3 \pmod{1}$. De plus, par définition de \prec_v , on a $t_i \prec_v t_j$ si et seulement $x_i < x_j$ pour tout $i, j \in \{1, 2, 3\}$. Nous soulignons également que $O_v(0_v) = 0$.

Si $0 < x_1$ et $x_3 < x_2$: comme $x_3 \in I_\alpha = [-\alpha, 1 - \alpha[$, nous avons $1 - \alpha < x_1 + x_2$. Il en découle

$$\begin{aligned} -\alpha &= 1 - \alpha - 1 \\ &< x_1 + x_2 - 1 \\ &< (1 - \alpha) + (1 - \alpha) - 1 && (\text{car } x_1, x_2 \in I_\alpha) \\ &= 1 - 2\alpha \\ &< 1 - \alpha. \end{aligned}$$

Ainsi, nous avons $x_1 + x_2 - 1 \in [-\alpha, 1 - \alpha[= I_\alpha$. Or, comme $x_1 + x_2 \equiv x_3 \pmod{1}$ et $x_3 \in I_\alpha$, alors $x_3 = x_1 + x_2 - 1$.

Si $x_1 < 0$ et $x_2 < x_3$: comme $x_3 \in I_\alpha = [-\alpha, 1 - \alpha[$, nous avons $x_1 + x_2 < -\alpha$. Il en découle

$$\begin{aligned} 1 - \alpha &> 1 + x_1 + x_2 \\ &\geq 1 - \alpha - \alpha && (\text{car } x_1, x_2 \in I_\alpha) \\ &> -\alpha && (\text{car } 1 - \alpha > 0). \end{aligned}$$

Ainsi, nous avons $x_1 + x_2 + 1 \in [-\alpha, 1 - \alpha[= I_\alpha$. Or, comme $x_1 + x_2 \equiv x_3 \pmod{1}$ et $x_3 \in I_\alpha$, alors $x_3 = x_1 + x_2 + 1$.

Sinon : alors 0 et x_1 sont ordonnés de la même manière que x_2 et x_3 . Or, comme $x_1 + x_2 \equiv x_3 \pmod{1}$, nous avons

$$||x_1 - 0| - |x_3 - x_2|| = k$$

où k est un naturel. Si $k > 0$, cela implique que, soit $|x_1 - 0| \geq 1$, soit $|x_3 - x_2| \geq 1$. Or, cela est impossible puisque $x_1, x_2, x_3 \in I_\alpha$. Donc, nous avons $k = 0$ et $x_1 - 0 = x_3 - x_2$. \square

Notation 5.2.5. Soit $v \in R$. Soit un naturel n . Nous notons

$$n_v = \underbrace{(((1_v \oplus_v^{\text{fin}} 1_v) \oplus_v^{\text{fin}} 1_v) \cdots \oplus_v^{\text{fin}} 1_v)}_{n \text{ fois}}.$$

Remarquons que, pour tout $v \in R$, pour tout naturel n , nous avons $Z_v(n_v) = n$.

Nous pouvons également souligner que n_v est ω -régulier pour un $v \in R$ fixé. En effet, puisque n_v est un mot infini, il suffit de construire un automate qui transite vers un nouvel état en lisant chaque nouveau caractère de n_v et tant qu'il y a des 1. De plus, n_v appartient à A_v^{fin} , donc à partir d'un certain caractère, le mot ne contient plus que des 0 et des #.

Donc, il suffit de terminer par un état final qui boucle sur 0 et # pour avoir un nombre fini d'états dans l'automate. (Il faut également s'assurer que l'élément est aligné avec v , mais nous avons vu précédemment que la relation d'alignement est ω -régulière).

Définition 5.2.6. Nous définissons l'ensemble suivant :

$$F = \{(v, s) \in A^{\text{fin}} : \alpha(v)Z_v(s) < 1\}.$$

Lemme 5.2.7. L'ensemble F est ω -régulier et pour tout $(v, s) \in F$, on a

$$O_v(s) = \begin{cases} \alpha(v)Z_v(s) & \text{si } \alpha(v)(Z_v(s) + 1) < 1, \\ \alpha(v)Z_v(s) - 1 & \text{sinon.} \end{cases}$$

Démonstration. Rappelons que si X, Y sont deux ensembles et si $Z \subseteq X \times Y$, alors pour tout $x \in X$, nous notons Z_x l'ensemble $\{y \in Y : (x, y) \in Z\}$.

Démontrons d'abord que F est ω -régulier. Nous pouvons écrire F de la manière suivante :

$$F = \{(v, s) \in A_v^{\text{fin}} : \alpha(v) < \frac{1}{2}, \alpha(v)Z_v(s) < 1\} \cup \{(v, s) \in A_v^{\text{fin}} : \alpha(v) > \frac{1}{2}, \alpha(v)Z_v(s) < 1\}.$$

Or, par le lemme 3.2.11, nous savons que l'ensemble

$$\{w \in R : \alpha(w) < \frac{1}{2}\}$$

est ω -régulier. Son complémentaire l'est aussi par la proposition 2.1.2.

Soit $v \in R$. Considérons d'abord le cas où $\alpha(v) > \frac{1}{2}$. Dans ce cas, pour tout $s \in A_v^{\text{fin}}$, on a

$$\alpha(v)Z_v(s) < 1 \Leftrightarrow Z_v(s) < 2 \Leftrightarrow Z_v(s) \in \{0, 1\} \Leftrightarrow s \in \{0_v, 1_v\}.$$

Il en découle que $F_v = \{0_v, 1_v\}$ qui est un ensemble ω -régulier au vu du lemme 3.3.14.

Soit $v \in R$. Considérons maintenant le cas où $\alpha(v) < \frac{1}{2}$. Soit $n \in \mathbb{N}$ maximal tel que $n\alpha(v) < 1$. Nous avons

$$\begin{aligned} n\alpha(v) < 1 &\Leftrightarrow n\alpha(v) - \alpha(v) < 1 - \alpha(v) \\ &\Leftrightarrow (n-1)\alpha(v) < 1 - \alpha(v). \end{aligned}$$

Or, puisque $\alpha(v) \in]0, 1[$, nous avons les inégalités suivantes :

$$-\alpha(v) < 0 = 0\alpha(v) < 1\alpha(v) < 2\alpha(v) < \dots < (n-1)\alpha(v) < 1 - \alpha(v).$$

D'où $0\alpha(v), 1\alpha(v), \dots, (n-1)\alpha(v) \in [0, 1 - \alpha(v)[\subset I_{\alpha(v)}$. Donc, par le lemme 3.3.15, pour tout $i \in \{0, 1, \dots, n-1\}$, il existe un entier u_i tel que

$$O_v(i_v) = \alpha(v)Z_v(i_v) + u_i = i\alpha(v) + u_i \in I_{\alpha(v)}.$$

Pour tout $i \in \{0, 1, \dots, n-1\}$, comme $i\alpha(v) \in I_{\alpha(v)}$, alors $u_i = 0$. De plus,

$$O_v(i_v) = i\alpha(v) \geq 0 = O_v(0_v)$$

pour tout $i \in \{0, 1, \dots, n-1\}$. D'où $0_v \preceq_v i_v$ pour tout $i \in \{0, 1, \dots, n-1\}$.

Par définition de n , nous avons $(n+1)\alpha(v) \geq 1$ et

$$\begin{aligned} (n+1)\alpha(v) \geq 1 &\Leftrightarrow n\alpha(v) + \alpha(v) \geq 1 \\ &\Leftrightarrow n\alpha(v) \geq 1 - \alpha(v). \end{aligned}$$

D'où $n\alpha(v) \in [1 - \alpha(v), 1[$. Il en découle que $n\alpha(v) - 1 \in [-\alpha(v), 0[\subset I_{\alpha(v)}$. Par le lemme 3.3.15, il existe un entier u_2 tel que

$$O_v(n_v) = Z_v(n_v)\alpha(v) + u_2 = n\alpha(v) + u_2 \in I_{\alpha(v)}.$$

Comme $n\alpha(v) - 1 \in I_{\alpha(v)}$, alors $u_2 = -1$. De plus,

$$O_v(n_v) = n\alpha(v) - 1 < 0 = O_v(0_v).$$

D'où $n_v \prec_v 0_v$. Ainsi n_v est l'élément minimal de A_v^{fin} au sens de \prec_v^{fin} tel que $n_v \prec_v 0_v$. Ainsi, pour tout $s \in F_v$, on a

$$Z_v(s)\alpha(v) \leq Z_v(n_v)\alpha(v) < 1.$$

Or, cette condition est vraie si et seulement si

$$Z_v(s) \leq Z_v(n_v).$$

Ainsi, nous avons prouvé que

$$F_v = \{s \in A_v^{\text{fin}} : s \preceq_v^{\text{fin}} n_v\}$$

qui est un ensemble ω -régulier par ω -régularité de n_v , de A^{fin} et de \preceq^{fin} . Il s'ensuit l' ω -régularité de F .

Démontrons maintenant la deuxième partie de l'énoncé. Soit $(v, s) \in F$. Par le lemme 3.3.15, il existe un entier u tel que

$$O_v(s) = Z_v(s)\alpha(v) + u.$$

Si $\alpha(v)(Z_v(s) + 1) < 1$: alors $\alpha(v)Z_v(s) < 1 - \alpha(v)$. Et comme $\alpha(v)Z_v(s) \geq 0$, nous avons

$$\alpha(v)Z_v(s) \in I_{\alpha(v)}.$$

D'où $O_v(s) = Z_v(s)\alpha(v)$ dans ce cas.

Si $\alpha(v)(Z_v(s) + 1) \geq 1$: alors $\alpha(v)Z_v(s) \geq 1 - \alpha(v)$. Et comme $\alpha(v)Z_v(s) < 1$, nous avons

$$\alpha(v)Z_v(s) \in [1 - \alpha(v), 1[.$$

Ainsi

$$\alpha(v)Z_v(s) - 1 \in [-\alpha(v), 0[\subset I_{\alpha(v)}.$$

D'où $O_v(s) = Z_v(s)\alpha(v) - 1$ dans ce cas. \square

Lemme 5.2.8. Soient $v \in R$ et $t \in A_v^{\text{fin}}$. Alors il existe $u \in F_v$ et $s \in A_v^{\text{fin}}$ tels que $s \preceq_v 0_v$ et $t = s \oplus_v^{\text{fin}} u$. En particulier, nous avons

$$A_v^{\text{fin}} = \{s \oplus_v^{\text{fin}} u : s \in A_v^{\text{fin}}, s \preceq_v 0_v, u \in F_v\}.$$

Démonstration. Rappelons que si X, Y sont deux ensembles et si $Z \subseteq X \times Y$, alors pour tout $x \in X$, nous notons Z_x l'ensemble $\{y \in Y : (x, y) \in Z\}$.

Soit $v \in R$. La deuxième partie de l'énoncé découle directement de la première partie. Démontrons donc la première partie. Soient $t \in A_v^{\text{fin}}$ et $n \in \mathbb{N}$ maximal tel que $n\alpha(v) < 1$. On veut trouver $u \in F_v$ et $s \in A_v^{\text{fin}}$ tels que $s \preceq_v 0_v$ et $t = s \oplus_v^{\text{fin}} u$.

Rappelons, vu la preuve du lemme 5.2.7, que

$$F_v = \{0_v, 1_v\} \cup \{s \in A_v^{\text{fin}} : s \preceq_v^{\text{fin}} n_v\}.$$

Si $Z_v(t) \leq n$: alors $t \preceq_v^{\text{fin}} n_v$, d'où $t \in F_v$. Ainsi, il est suffisant de prendre $s = 0_v \in A_v^{\text{fin}}$ et $u = t \in F_v$ puisque $t = 0_v \oplus_v^{\text{fin}} t$ et $0_v \preceq_v 0_v$.

Si $t \preceq_v 0_v$: alors il est suffisant de prendre $s = t \in A_v^{\text{fin}}$ et $u = 0_v \in F_v$ puisque $t = t \oplus_v^{\text{fin}} 0_v$.

Si $Z_v(t) > n$ et $0_v \prec_v t$: Soit $i \in \{1, \dots, n\}$ tel que $O_v(t) - i\alpha(v) \in] - \alpha(v), 0]$. Nous pouvons affirmer qu'un tel i existe. En effet, nous avons

$$\begin{aligned} 0_v \prec_v t &\Leftrightarrow 0 < O_v(t) \\ &\Leftrightarrow O_v(t) \in]0, 1 - \alpha(v)[. \end{aligned}$$

Ainsi, en soustrayant $\alpha(v)$ un certain nombre i de fois à $O_v(t)$, on finit par arriver dans l'intervalle $] - \alpha(v), 0]$ puisqu'il est de taille $\alpha(v)$. De plus, nous avons

$$O_v(t) - n\alpha(v) < 1 - \underbrace{(n+1)\alpha(v)}_{\geq 1} < 0.$$

Nous en déduisons que i doit appartenir à l'ensemble $\{1, \dots, n\}$.

Soit $s \in A_v^{\text{fin}}$ tel que $Z_v(s) = Z_v(t) - i$. Un tel s existe si $Z_v(t) - i \geq 0$. Cela est bien le cas puisque $Z_v(t) - n > 0$ et que $i \in \{1, \dots, n\}$. Ainsi, nous avons

$$\begin{aligned} Z_v(s) = Z_v(t) - i &\Leftrightarrow Z_v(s) + i = Z_v(t) \\ &\Leftrightarrow Z_v(s) + Z_v(i_v) = Z_v(t) \\ &\Leftrightarrow s \oplus_v^{\text{fin}} i_v = t. \end{aligned}$$

Ainsi, comme $i_v \in F_v$, il suffit de montrer que $s \preceq_v 0_v$. Par le lemme 5.2.7, nous savons que

$$O_v(i_v) \equiv i\alpha(v) \pmod{1}.$$

Ainsi,

$$\begin{aligned} O_v(s) + i\alpha(v) &\equiv O_v(s) + O_v(i_v) \pmod{1} \\ &\equiv O_v(t) \pmod{1} \end{aligned} \quad (\text{par définition de } \oplus_v).$$

Donc, il existe un entier k tel que

$$O_v(s) = O_v(t) - i\alpha(v) + k \in I_{\alpha(v)}.$$

Or, comme $O_v(t) - i\alpha(v) \in]-\alpha(v), 0] \subset I_{\alpha(v)}$, nous avons

$$O_v(s) = O_v(t) - i\alpha(v) \leq 0 = O_v(0_v).$$

D'où $s \preceq_v 0_v$. □

Le lemme qui suit est vraiment un résultat clef de ce mémoire. Il va nous permettre de discuter de la décidabilité de la collection de \mathcal{R}_α tels que α est irrationnel.

Lemme 5.2.9. Il existe une famille uniforme de structures ω -régulières $(\mathcal{C}_v)_{v \in R}$ telle que, pour tout $v \in R$, nous avons

$$\mathcal{C}_v \simeq ([-\alpha(v), +\infty[, <, +, \mathbb{N}, \alpha(v)\mathbb{N}).$$

Démonstration. Rappelons que si X, Y sont deux ensembles et si $Z \subseteq X \times Y$, alors pour tout $x \in X$, nous notons Z_x l'ensemble $\{y \in Y : (x, y) \in Z\}$.

Définissons l'ensemble suivant :

$$B = \{(v, s) \in A^{\text{fin}} : s \preceq_v 0_v\}.$$

Cet ensemble est ω -régulier par ω -régularité de A^{fin} , de \preceq et de 0_* . Pour tout $v \in R$, nous définissons la fonction

$$g_v : B_v \rightarrow \mathbb{N} : s \mapsto \alpha(v)Z_v(s) - O_v(s).$$

Notation	Définition
B	$\{(v, s) \in A^{\text{fin}} : s \preceq_v 0_v\}$
\prec^B	$\{(v, s_1, s_2) : v \in R, s_1, s_2 \in B_v, s_1 \prec_v^{\text{fin}} s_2\}$
\oplus^B	$\left\{ (v, s_1, s_2, s_3) : v \in R, s_1, s_2 \in B_v, \right.$ $\left. s_3 = \begin{cases} s_1 \oplus_v^{\text{fin}} s_2 & \text{si } s_1 \oplus_v^{\text{fin}} s_2 \preceq_v s_2 \\ (s_1 \oplus_v^{\text{fin}} s_2) \oplus_v^{\text{fin}} 1_v & \text{sinon} \end{cases} \right\}$
\ominus^B	$\{(v, s_1, s_2, s_3) : v \in R, s_1, s_2, s_3 \in B_v, s_2 \oplus_v^B s_3 = s_1\}$
0_v^B	$g_v^{-1}(0)$
1_v^B	$g_v^{-1}(1)$
C	$\{(v, s, t) \in (H_\infty)^3 : (v, s) \in B, (v, t) \in A\}$
\prec^C	$\left\{ (v, s_1, t_1, s_2, t_2) : v \in R, \right.$ $\left. (s_1, t_1), (s_2, t_2) \in C_v, (s_1 \prec_v^B s_2) \vee ((s_1 = s_2) \wedge (t_1 \prec_v t_2)) \right\}$
\oplus^C	$\left\{ (v, s_1, t_1, s_2, t_2, s_3, t_3) : v \in R, (s_1, t_1), (s_2, t_2) \in C_v, \right.$ $\left. (s_3, t_3) = \begin{cases} ((s_1 \oplus_v^B s_2) \ominus_v^B 1_v^B, t_1 \oplus_v t_2) & \text{si } t_1 \prec_v 0_v \text{ et } t_2 \prec t_1 \oplus_v t_2 \\ ((s_1 \oplus_v^B s_2) \oplus_v^B 1_v^B, t_1 \oplus_v t_2) & \text{si } 0_v \prec_v t_1 \text{ et } t_1 \oplus_v t_2 \prec t_2 \\ (s_1 \oplus_v^B s_2, t_1 \oplus_v t_2) & \text{sinon} \end{cases} \right\}$
1_v^C	$T_v^{-1}(1)$
g_v	$B_v \rightarrow \mathbb{N} : s \mapsto \alpha(v)Z_v(s) - O_v(s)$
T_v	$C_v \rightarrow [-\alpha(v), +\infty[: (s, t) \mapsto g_v(s) + O_v(t)$

TABLE 5.1 – Liste de notations utilisées dans la preuve du lemme 5.2.9

Si $s \in B_v$, alors $g_v(s)$ est bien un naturel. En effet, par le lemme 3.3.15, on sait que c'est un entier, et comme $\alpha(v) \in]0, 1[$, $Z_v(s) \in \mathbb{N}$ et $O_v(s) \leq 0$, alors $\alpha(v)Z_v(s) - O_v(s)$ est positif.

Définissons maintenant \prec^B comme étant la restriction de \prec^{fin} à B . Autrement dit, on a

$$\prec^B = \{(v, s_1, s_2) : v \in R, s_1, s_2 \in B_v, s_1 \prec_v^{\text{fin}} s_2\}.$$

Nous noterons $s_1 \prec_v^B s_2$ si $(v, s_1, s_2) \in \prec^B$. L'ensemble \prec^B est ω -régulier par ω -régularité de R , de B et de \prec^{fin} .

Nous définissons également l'ensemble \oplus^B de la manière suivante :

$$\oplus^B = \left\{ (v, s_1, s_2, s_3) : v \in R, s_1, s_2 \in B_v, s_3 = \begin{cases} s_1 \oplus_v^{\text{fin}} s_2 & \text{si } s_1 \oplus_v^{\text{fin}} s_2 \preceq_v s_2 \\ (s_1 \oplus_v^{\text{fin}} s_2) \oplus_v^{\text{fin}} 1_v & \text{sinon} \end{cases} \right\}.$$

On note $s_1 \oplus_v^B s_2 = s_3$ si $(v, s_1, s_2, s_3) \in \oplus^B$. Cet ensemble est ω -régulier par ω -régularité de R , de B , de \oplus^{fin} , de 1_* et de \preceq .

Démontrons que, pour tout $v \in R$ et pour tout $s_1, s_2 \in B_v$, on a $s_1 \oplus_v^B s_2 \in B_v$ et

$$g_v(s_1 \oplus_v^B s_2) = g_v(s_1) + g_v(s_2). \quad (5.1)$$

Soient $v \in R$ et $s_1, s_2 \in B_v$. Considérons d'abord le cas où $s_1 \oplus_v^{\text{fin}} s_2 \preceq_v s_2$. Ainsi, $O_v(s_1 \oplus_v^{\text{fin}} s_2) \leq O_v(s_2) \leq 0$, d'où $s_1 \oplus_v^B s_2 \in B_v$. De plus, comme $s_1 \in B_v$, alors $s_1 \preceq_v 0_v$. Ainsi, comme $s_1 \oplus_v^{\text{fin}} s_2 = s_1 \oplus_v s_2$ (par le lemme 4.2.5 car $s_1, s_2 \in A_v^{\text{fin}}$), alors, par le lemme 5.2.4, nous avons

$$O_v(s_1) + O_v(s_2) = O_v(s_1 \oplus_v^{\text{fin}} s_2).$$

Ainsi,

$$\begin{aligned} g_v(s_1 \oplus_v^B s_2) &= g_v(s_1 \oplus_v^{\text{fin}} s_2) && \text{(Par définition de } \oplus^B) \\ &= \alpha(v)Z_v(s_1 \oplus_v^{\text{fin}} s_2) - O_v(s_1 \oplus_v^{\text{fin}} s_2) && \text{(Par définition de } g_v) \\ &= \alpha(v)(Z_v(s_1) + Z_v(s_2)) - O_v(s_1) - O_v(s_2) \\ &= g_v(s_1) + g_v(s_2). \end{aligned}$$

Considérons maintenant le cas où $s_2 \prec_v s_1 \oplus_v^{\text{fin}} s_2$. Nous savons que $-\alpha(v)$ est plus petit ou égal à $O_v(s_1)$ et $O_v(s_2)$. Cela implique que $-2\alpha(v) \leq O_v(s_1) + O_v(s_2)$ et donc $-\alpha(v) \leq O_v(s_1) + O_v(s_2) + \alpha(v)$. De plus, comme $s_1, s_2, 1_v \in A_v^{\text{fin}}$, alors $(s_1 \oplus_v^{\text{fin}} s_2) \oplus_v^{\text{fin}} 1_v = (s_1 \oplus_v s_2) \oplus_v 1_v$ au vu du lemme 4.2.5.

$$\begin{aligned} O_v((s_1 \oplus_v^{\text{fin}} s_2) \oplus_v^{\text{fin}} 1_v) &= O_v(s_1) + O_v(s_2) + O_v(1_v) \pmod{1} && \text{(Par définition de } \oplus) \\ &= O_v(s_1) + O_v(s_2) + \alpha(v) \pmod{1} && \text{(Par le lemme de 3.3.15).} \end{aligned}$$

De plus, $s_1 \prec_v 0_v$. En effet, $s_1 \preceq_v 0_v$ et s_1 doit être différent de 0_v , sinon $s_1 \oplus_v^{\text{fin}} s_2$ serait égal à s_2 , ce qui est en contradiction avec l'hypothèse $s_2 \prec_v s_1 \oplus_v^{\text{fin}} s_2$.

Donc, comme $s_2 \prec_v s_1 \oplus_v^{\text{fin}} s_2$ et $s_1 \prec_v 0_v$, par le lemme 5.2.4, nous savons que

$$O_v(s_1 \oplus_v^{\text{fin}} s_2) = O_v(s_1) + O_v(s_2) + 1 < 1 - \alpha(v).$$

Ainsi, $O_v(s_1) + O_v(s_2) + \alpha(v) < 0$. D'où $O_v(s_1) + O_v(s_2) + \alpha(v) \in I_{\alpha(v)}$ et

$$O_v((s_1 \oplus_v^{\text{fin}} s_2) \oplus_v^{\text{fin}} 1_v) = O_v(s_1) + O_v(s_2) + \alpha(v).$$

Et comme $O_v(s_1) + O_v(s_2) < -\alpha(v)$, alors

$$\begin{aligned} O_v(s_1 \oplus_v^B s_2) &= O_v((s_1 \oplus_v^{\text{fin}} s_2) \oplus_v^{\text{fin}} 1_v) \\ &= O_v(s_1) + O_v(s_2) + \alpha(v) \\ &< -\alpha(v) + \alpha(v) \\ &= 0. \end{aligned}$$

D'où $s_1 \oplus_v^B s_2 \in B_v$. De plus, on a

$$\begin{aligned} g_v(s_1 \oplus_v^B s_2) &= g_v((s_1 \oplus_v^{\text{fin}} s_2) \oplus_v^{\text{fin}} 1_v) && \text{(Par déf. de } \oplus^B) \\ &= \alpha(v)Z_v((s_1 \oplus_v^{\text{fin}} s_2) \oplus_v^{\text{fin}} 1_v) - O_v((s_1 \oplus_v^{\text{fin}} s_2) \oplus_v^{\text{fin}} 1_v) && \text{(Par déf. de } g_v) \\ &= \alpha(v)(Z_v(s_1) + Z_v(s_2) + 1) - O_v(s_1) - O_v(s_2) - \alpha(v) \\ &= g_v(s_1) + g_v(s_2). \end{aligned}$$

Comme annoncé en (5.1), nous avons démontré que, pour tout $v \in R$, $s_1 \oplus_v^B s_2 \in B_v$ et

$$g_v(s_1) + g_v(s_2) = g_v(s_1 \oplus_v^B s_2).$$

Démontrons que, pour tout $v \in R$, $s_1, s_2 \in B_v$, nous avons

$$s_1 \prec_v^B s_2 \Leftrightarrow g_v(s_1) < g_v(s_2).$$

Soient $v \in R$, $s_1, s_2 \in B_v$, alors

$$\begin{aligned} s_1 \prec_v^B s_2 &\Leftrightarrow s_1 \prec_v^{\text{fin}} s_2 \\ &\Leftrightarrow Z_v(s_1) < Z_v(s_2). \end{aligned}$$

De plus, comme $s_1, s_2 \in B_v$, alors $O_v(s_1), O_v(s_2) \in [-\alpha(v), 0]$.

D'une part, supposons que $Z_v(s_1) < Z_v(s_2)$. Alors s_2 doit être différent de 0_v . Sinon, $Z_v(s_1) < Z_v(s_2) = 0$, mais $Z_v(s_1) \in \mathbb{N}$ et ne peut donc pas être strictement négatif. D'où $O_v(s_2) \in [-\alpha(v), 0[$. Ainsi,

$$Z_v(s_1) - \underbrace{\frac{O_v(s_1)}{\alpha(v)}}_{\in[-1,0]} \leq Z_v(s_2) < Z_v(s_2) - \underbrace{\frac{O_v(s_2)}{\alpha(v)}}_{\in[-1,0]}.$$

Cela implique que $\alpha(v)Z_v(s_1) - O_v(s_1) < \alpha(v)Z_v(s_2) - O_v(s_2)$, d'où $g_v(s_1) < g_v(s_2)$.

D'une autre part, supposons que $g_v(s_1) < g_v(s_2)$. Par définition, c'est équivalent à $\alpha(v)Z_v(s_1) - O_v(s_1) < \alpha(v)Z_v(s_2) - O_v(s_2)$. Cela implique que

$$Z_v(s_1) - \underbrace{\frac{O_v(s_1)}{\alpha(v)}}_{\in[-1,0]} < Z_v(s_2) - \underbrace{\frac{O_v(s_2)}{\alpha(v)}}_{\in[-1,0]}.$$

D'où

$$Z_v(s_1) < Z_v(s_2) - \underbrace{\frac{O_v(s_2)}{\alpha(v)}}_{\in[-1,0]}.$$

Or, comme $Z_v(s_1), Z_v(s_2) \in \mathbb{N}$, alors $Z_v(s_1) \leq Z_v(s_2)$. Cependant, $Z_v(s_1) \neq Z_v(s_2)$, sinon $s_1 = s_2$, ce qui impliquerait $g_v(s_1) = g_v(s_2)$, et cela entrerait en contradiction avec notre hypothèse $g_v(s_1) < g_v(s_2)$. Ainsi, on a $Z_v(s_1) < Z_v(s_2)$.

Démontrons que la fonction g_v est bijective pour tout $v \in R$. Soit $v \in R$. Nous commençons par prouver son injectivité. Pour tout $s_1, s_2 \in B_v$, nous avons

$$g_v(s_1) = g_v(s_2) \Leftrightarrow Z_v(s_1) = Z_v(s_2).$$

Sinon $Z_v(s_1) > Z_v(s_2)$ (resp. $Z_v(s_1) < Z_v(s_2)$). Or, vu ce qui a été démontré précédemment, cela impliquerait que $g_v(s_1) > g_v(s_2)$ (resp. $g_v(s_1) < g_v(s_2)$). Donc, par injectivité de Z_v , on a $s_1 = s_2$.

Démontrons maintenant que g_v est surjective pour tout $v \in R$. Soit $v \in R$. Rappelons que $\alpha(v) \in]0, 1[$. Pour tout $m \in \mathbb{N}$, montrons qu'il existe $s \in B_v$ tel que $g_v(s) = m$. Or, si on prend $s = n_v$ où n est le plus grand naturel tel que $n\alpha(v) < m$. Ainsi, $Z_v(s)\alpha(v) \in]m - \alpha(v), m[$. Ainsi, nous avons $-\alpha(v) < O_v(s) \leq 0$. D'où s appartient bien à l'ensemble B_v (par la remarque 5.2.3).

Ainsi, pour tout $v \in R$,

$$g_v : (B_v, \prec_v^B, \oplus_v^B) \rightarrow (\mathbb{N}, <, +)$$

est un isomorphisme.

Nous définissons l'ensemble suivant :

$$C = \{(v, s, t) \in (H_\infty)^3 : (v, s) \in B, (v, t) \in A\}.$$

Cet ensemble est ω -régulier par ω -régularité de H_∞ , de B et de A .

Pour tout $v \in R$, nous définissons la fonction

$$T_v : C_v \rightarrow [-\alpha(v), +\infty[: (s, t) \mapsto g_v(s) + O_v(t).$$

Pour tout $v \in R$, la fonction T_v est bijective. En effet, tout réel appartenant à $[-\alpha(v), +\infty[$ peut se décomposer de manière unique en la somme $n + y$ où $n \in \mathbb{N}$ et $y \in I_{\alpha(v)}$.

Nous définissons l'ensemble suivant :

$$\prec^C = \{(v, s_1, t_1, s_2, t_2) : v \in R, (s_1, t_1), (s_2, t_2) \in C_v, (s_1 \prec_v^B s_2) \vee ((s_1 = s_2) \wedge (t_1 \prec_v t_2))\}.$$

Nous notons $(s_1, t_1) \prec_v^C (s_2, t_2)$ si $(v, s_1, t_1, s_2, t_2) \in \prec^C$. Cet ensemble est ω -régulier par ω -régularité de R , de C , de \prec^B et de \prec .

Démontrons, pour tout $v \in R$ que

$$T_v(s_1, t_1) < T_v(s_2, t_2) \Leftrightarrow (s_1, t_1) \prec_v^C (s_2, t_2).$$

Soit $v \in R$. Soient $(s_1, t_1), (s_2, t_2) \in C_v$. Comme $O_v(t_1), O_v(t_2) \in [-\alpha(v), 1 - \alpha(v)[$, alors $|O_v(t_1) - O_v(t_2)| < 1$. Par définition de T_v , nous avons que $T_v(s_1, t_1) < T_v(s_2, t_2)$ si et seulement si $g_v(s_1) + O_v(t_1) < g_v(s_2) + O_v(t_2)$. Par définition de \prec^C , nous avons

$$\begin{aligned} (s_1, t_1) \prec_v^C (s_2, t_2) &\Leftrightarrow s_1 \prec_v^B s_2 \quad \text{ou} \quad (s_1 = s_2 \quad \text{et} \quad t_1 \prec_v t_2) \\ &\Leftrightarrow g_v(s_1) < g_v(s_2) \quad \text{ou} \quad (s_1 = s_2 \quad \text{et} \quad O_v(t_1) < O_v(t_2)). \end{aligned}$$

Supposons d'abord que $g_v(s_1) \geq g_v(s_2)$, alors $g_v(s_1) - g_v(s_2) \in \mathbb{N}$ et

$$\begin{aligned} (s_1, t_1) \prec_v^C (s_2, t_2) &\Leftrightarrow s_1 = s_2 \quad \text{et} \quad O_v(t_1) < O_v(t_2) \\ &\Leftrightarrow g_v(s_1) = g_v(s_2) \quad \text{et} \quad O_v(t_1) < O_v(t_2) \quad (\text{Par bijectivité de } g_v) \\ &\Leftrightarrow \underbrace{g_v(s_1) - g_v(s_2)}_{\in \mathbb{N}} < \underbrace{O_v(t_2) - O_v(t_1)}_{\in]-1, 1[} \\ &\Leftrightarrow g_v(s_1) + O_v(t_1) < g_v(s_2) + O_v(t_2). \end{aligned}$$

Supposons maintenant que $((s_1 \neq s_2) \vee (O_v(t_1) > O_v(t_2)))$, alors

$$\begin{aligned} (s_1, t_1) \prec_v^C (s_2, t_2) &\Leftrightarrow g_v(s_1) < g_v(s_2) \\ &\Leftrightarrow g_v(s_2) - g_v(s_1) \geq 1 \\ &\Rightarrow \underbrace{g_v(s_2) - g_v(s_1)}_{\in \mathbb{Z}} > \underbrace{O_v(t_1) - O_v(t_2)}_{\in]-1, 1[}. \end{aligned}$$

De plus, si $g_v(s_2) - g_v(s_1) > O_v(t_1) - O_v(t_2)$, puisque $O_v(t_1) - O_v(t_2) > -1$ et comme $((s_1 \neq s_2) \vee (O_v(t_1) > O_v(t_2)))$, alors $g_v(s_2) - g_v(s_1) \in \mathbb{N}_0$ et donc $g_v(s_2) - g_v(s_1) \geq 1$. Ainsi, on obtient que

$$(s_1, t_1) \prec_v^C (s_2, t_2) \Leftrightarrow g_v(s_1) + O_v(t_1) < g_v(s_2) + O_v(t_2).$$

Nous définissons les éléments $0_v^B = g_v^{-1}(0)$ et $1_v^B = g_v^{-1}(1)$ pour tout $v \in R$. Remarquons que, pour tout $v \in R$, on a

$$\begin{aligned} g_v^{-1}(0) &= 0_v, \\ g_v^{-1}(1) &= \{n_v : n = \max\{m \in \mathbb{N} : m\alpha(v) < 1\}\}. \end{aligned}$$

En effet, pour tout $v \in R$, si $g_v(s) = m$, alors $s = n_v$ convient (où n est le plus grand naturel tel que $n\alpha(v) < m$), car $Z_v(n_v)\alpha(v) \in]m - \alpha(v), m[$ et donc $-\alpha(v) < O_v(n_v) \leq 0$, d'où $n_v \in B_v$. Or, puisque g_v est bijective pour tout $v \in R$, alors cet élément est unique.

Ainsi, nous en concluons que 0_v^B et 1_v^B sont ω -réguliers par ω -régularité de 0_* et de n_v pour tout $v \in R$.

Nous définissons \ominus^B de la manière suivante :

$$\ominus^B = \{(v, s_1, s_2, s_3) : v \in R, s_1, s_2, s_3 \in B_v, s_2 \oplus_v^B s_3 = s_1\}.$$

Nous notons $s_1 \ominus_v^B s_2 = s_3$ si $(v, s_1, s_2, s_3) \in \ominus^B$. Remarquons que \ominus^B est l'inverse (partiel) de \oplus^B . De plus, l'ensemble \ominus^B est ω -régulier par ω -régularité de R , de B et de \oplus^B .

Soient $v \in R, s_1, s_2, s_3 \in B_v$. Si $s_1 \ominus_v^B s_2 = s_3$, alors $s_2 \oplus_v^B s_3 = s_1$ et donc

$$\begin{aligned} g_v(s_1) &= g_v(s_2 \oplus_v^B s_3) \\ &= g_v(s_2) + g_v(s_3) \\ &= g_v(s_2) + g_v(s_1 \ominus_v^B s_2). \end{aligned}$$

Ainsi, nous avons

$$g_v(s_1 \ominus_v^B s_2) = g_v(s_1) - g_v(s_2).$$

Nous définissons l'ensemble suivant :

$$\oplus^C = \left\{ \begin{array}{l} (v, s_1, t_1, s_2, t_2, s_3, t_3) : v \in R, (s_1, t_1), (s_2, t_2) \in C_v, \\ (s_3, t_3) = \begin{cases} ((s_1 \oplus_v^B s_2) \ominus_v^B 1_v^B, t_1 \oplus_v t_2) & \text{si } t_1 \prec_v 0_v \text{ et } t_2 \prec t_1 \oplus_v t_2 \\ ((s_1 \oplus_v^B s_2) \oplus_v^B 1_v^B, t_1 \oplus_v t_2) & \text{si } 0_v \prec_v t_1 \text{ et } t_1 \oplus_v t_2 \prec t_2 \\ (s_1 \oplus_v^B s_2, t_1 \oplus_v t_2) & \text{sinon} \end{cases} \end{array} \right\}.$$

Si $(v, s_1, t_1, s_2, t_2, s_3, t_3) \in \oplus^C$, nous notons

$$(s_1, t_1) \oplus_v^C (s_2, t_2) = (s_3, t_3).$$

Remarquons que \oplus^C est partiellement défini. En effet, pour $v \in R$, et pour $(s_1, t_1), (s_2, t_2) \in C_v$, si $t_1 \prec_v 0_v$, $t_2 \prec t_1 \oplus_v t_2$ et $s_1 = s_2 = 0_v^B$, alors

$$(s_1, t_1) \oplus_v^C (s_2, t_2) = ((0_v^B \oplus_v^B 0_v^B) \ominus_v^B 1_v^B,$$

ce qui n'est pas défini dans le domaine de \ominus^B .

De plus, l'ensemble \oplus^C est ω -régulier par ω -régularité de \oplus^B , de R , de C , de \oplus , de \prec , de 0_* , de \ominus^B et de 1_v^B .

Démontrons que, pour tout $v \in R$, $(s_1, t_1), (s_2, t_2) \in C_v$, on a

$$T_v((s_1, t_1) \oplus_v^C (s_2, t_2)) = T_v(s_1, t_1) + T_v(s_2, t_2).$$

Soient $v \in R$, $(s_1, t_1), (s_2, t_2) \in C_v$. Par définitions de \oplus^C et de T_v , nous avons

$$\begin{aligned} & T_v((s_1, t_1) \oplus_v^C (s_2, t_2)) \\ &= \begin{cases} g_v((s_1 \oplus_v^B s_2) \ominus_v^B 1_v^B) + O_v(t_1 \oplus_v t_2) & \text{si } t_1 \prec_v 0_v \text{ et } t_2 \prec t_1 \oplus_v t_2, \\ g_v((s_1 \oplus_v^B s_2) \oplus_v^B 1_v^B) + O_v(t_1 \oplus_v t_2) & \text{si } 0_v \prec_v t_1 \text{ et } t_1 \oplus_v t_2 \prec t_2, \\ g_v(s_1 \oplus_v^B s_2) + O_v(t_1 \oplus_v t_2) & \text{sinon.} \end{cases} \end{aligned}$$

En utilisant le lemme 5.2.4, on obtient

$$\begin{aligned} & T_v((s_1, t_1) \oplus_v^C (s_2, t_2)) \\ &= \begin{cases} g_v((s_1 \oplus_v^B s_2) \ominus_v^B 1_v^B) + O_v(t_1) + O_v(t_2) + 1 & \text{si } t_1 \prec_v 0_v \text{ et } t_2 \prec t_1 \oplus_v t_2, \\ g_v((s_1 \oplus_v^B s_2) \oplus_v^B 1_v^B) + O_v(t_1) + O_v(t_2) - 1 & \text{si } 0_v \prec_v t_1 \text{ et } t_1 \oplus_v t_2 \prec t_2, \\ g_v(s_1 \oplus_v^B s_2) + O_v(t_1) + O_v(t_2) & \text{sinon.} \end{cases} \end{aligned}$$

De plus, nous avons démontré précédemment que $g_v(s_1 \oplus_v^B s_2) = g_v(s_1) + g_v(s_2)$, ainsi

$$\begin{aligned} & T_v((s_1, t_1) \oplus_v^C (s_2, t_2)) \\ &= \begin{cases} g_v(s_1) + g_v(s_2) - g_v(1_v^B) + O_v(t_1) + O_v(t_2) + 1 & \text{si } t_1 \prec_v 0_v \text{ et } t_2 \prec t_1 \oplus_v t_2, \\ g_v(s_1) + g_v(s_2) + g_v(1_v^B) + O_v(t_1) + O_v(t_2) - 1 & \text{si } 0_v \prec_v t_1 \text{ et } t_1 \oplus_v t_2 \prec t_2, \\ g_v(s_1) + g_v(s_2) + O_v(t_1) + O_v(t_2) & \text{sinon.} \end{cases} \end{aligned}$$

Comme $g_v(1_v^B) = 1$, nous obtenons finalement que

$$T_v((s_1, t_1) \oplus_v^C (s_2, t_2)) = g_v(s_1) + g_v(s_2) + O_v(t_1) + O_v(t_2) = T_v(s_1, t_1) + T_v(s_2, t_2).$$

Ainsi, pour tout $v \in R$,

$$T_v : (C_v, \prec_v^C, \oplus_v^C) \rightarrow ([-\alpha(v), +\infty[, <, +)$$

est un isomorphisme.

Nous voulons que

$$(\mathcal{C}_v)_{v \in R} = (C_v, \prec_v^C, \oplus_v^C, T_v^{-1}(\mathbb{N}), T_v^{-1}(\alpha(v)\mathbb{N}))_{v \in R}$$

soit une famille uniforme de structures ω -régulières. Nous avons déjà démontré que

- l'ensemble $C = \{(v, s, t) : v \in R, (s, t) \in C_v\}$ est ω -régulier,
- l'ensemble $\prec^C = \{(v, s_1, t_1, s_2, t_2) : v \in R, (s_1, t_1, s_2, t_2) \in \prec_v^C\}$ est ω -régulier,
- l'ensemble $\oplus^C = \{(v, s_1, t_1, s_2, t_2, s_3, t_3) : v \in R, (s_1, t_1, s_2, t_2, s_3, t_3) \in \oplus_v^C\}$ est ω -régulier.

Il ne reste plus qu'à prouver que les ensembles suivants sont ω -réguliers :

1. $\{(v, s, t) \in C : (s, t) \in T_v^{-1}(\mathbb{N})\}$,
2. $\{(v, s, t) \in C : (s, t) \in T_v^{-1}(\alpha(v)\mathbb{N})\}$.

Ainsi, on aura bien une famille uniforme de structures ω -régulières $(\mathcal{C}_v)_{v \in R}$ telle que, pour tout $v \in R$,

$$T_v : (C_v, \prec_v^C, \oplus_v^C, T_v^{-1}(\mathbb{N}), T_v^{-1}(\alpha(v)\mathbb{N})) \rightarrow ([-\alpha(v), +\infty[, <, +, \mathbb{N}, \alpha(v)\mathbb{N})$$

soit un isomorphisme.

Pour démontrer que le premier ensemble est ω -régulier, il suffit d'observer que

$$T_v^{-1}(\mathbb{N}) = \{(s, t) \in C_v : O_v(t) = 0\} = \{(s, t) \in C_v : t = 0_v\}$$

et on peut donc conclure par ω -régularité de R , de C et de 0_* .

Démontrons maintenant que le deuxième ensemble est ω -régulier. Notons

$$\begin{aligned} U_1 &= \{(v, s, t) \in C : s = t\} \text{ et} \\ U_2 &= \{(v, s, t) \in C : t \in F_v\}. \end{aligned}$$

Ces ensembles sont ω -réguliers par ω -régularité de C et de F (par le lemme 5.2.7). Nous définissons également

$$1_v^C = T_v^{-1}(1) = \{(s, t) \in C_v : s = 1_v^B\}$$

pour tout $v \in R$. Cet élément est ω -régulier par ω -régularité de C et de 1_v^B . Nous définissons également l'ensemble

$$U = \{(v, (s_1, t_1) \oplus_v^C (0_v, t_2)) : (v, s_1, t_1) \in U_1, (0_v, t_2) \in U_2, 0_v \preceq_v t_2\} \\ \cup \{(v, ((s_1, t_1) \oplus_v^C (0_v, t_2)) \oplus_v^C 1_v^C) : (v, s_1, t_1) \in U_1, (0_v, t_2) \in U_2, t_2 \prec_v 0_v\}.$$

Cet ensemble est ω -régulier par ω -régularité de \oplus^C , de 0_* , de U_1 , de U_2 , de 1_v^C , de \prec et de \preceq .

Nous allons montrer que $T_v^{-1}(\alpha(v)\mathbb{N}) = U_v$. Soient $(v, s, s) \in U_1$ et $(v, 0_v, t) \in U_2$. Autrement dit, nous avons $v \in R$, $s \in A_v^{\text{fin}}$, $s \preceq_v 0_v$ et $t \in F_v$.

Considérons d'abord le cas où $0_v \preceq_v t$. Alors, nous avons

$$T_v((s, s) \oplus_v^C (0_v, t)) = T_v(s, s) + T_v(0_v, t) \\ = \alpha(v)Z_v(s) - O_v(s) + O_v(s) + \alpha(v)Z_v(0_v) - O_v(0_v) + O_v(t) \\ = \alpha(v)Z_v(s) + O_v(t).$$

Puisque $t \in F_v$ et $0_v \preceq_v t$, alors le lemme 5.2.7 nous dit que $O_v(t) = \alpha(v)Z_v(t)$. Ainsi,

$$T_v((s, s) \oplus_v^C (0_v, t)) = \alpha(v)Z_v(s) + \alpha(v)Z_v(t) \\ = \alpha(v)(Z_v(s) + Z_v(t)) \\ = \alpha(v)(Z_v(s \oplus_v^{\text{fin}} t)) \in \alpha(v)\mathbb{N}.$$

Considérons maintenant le cas où $t \prec_v 0_v$. Alors, nous avons

$$T_v(((s, s) \oplus_v^C (0_v, t)) \oplus_v^C 1_v^C) \\ = T_v(s, s) + T_v(0_v, t) + 1 \\ = \alpha(v)Z_v(s) - O_v(s) + O_v(s) + \alpha(v)Z_v(0_v) - O_v(0_v) + O_v(t) + 1 \\ = \alpha(v)Z_v(s) + O_v(t) + 1.$$

Puisque $t \in F_v$ et $t \prec_v 0_v$, alors le lemme 5.2.7 nous dit que $O_v(t) = \alpha(v)Z_v(t) - 1$. Ainsi,

$$T_v((s, s) \oplus_v^C (0_v, t)) = \alpha(v)Z_v(s) + \alpha(v)Z_v(t) - 1 + 1 \\ = \alpha(v)(Z_v(s) + Z_v(t)) \\ = \alpha(v)(Z_v(s \oplus_v^{\text{fin}} t)) \in \alpha(v)\mathbb{N}.$$

Nous avons donc montré que $T_v(U_v) \subseteq \alpha(v)\mathbb{N}$. Or, par le lemme 5.2.8, nous savons que

$$A_v^{\text{fin}} = \{t \oplus_v^{\text{fin}} s : t \in A_v^{\text{fin}}, t \preceq_v 0_v, s \in F_v\}$$

pour tout $v \in R$. Nous pouvons en déduire que $T_v(U_v) = \alpha(v)Z_v(A_v^{\text{fin}}) = \alpha(v)\mathbb{N}$ pour tout $v \in R$. \square

Armés du lemme précédent, nous allons enfin pouvoir aborder les résultats de décidabilité concernant \mathcal{R}_α . La preuve suivante a été rédigée grâce aux éclaircissements de Christian Schulz [25].

Théorème 5.2.10. Il existe une famille uniforme de structures ω -régulières $(\mathcal{D}_v)_{v \in \mathbb{R}}$ telle que \mathcal{D}_v est isomorphe à $\mathcal{R}_{\alpha(v)}$ pour tout $v \in \mathbb{R}$.

Démonstration. Soit $v \in \mathbb{R}$. Dans la structure $([-\alpha(v), +\infty[, <, +, \mathbb{N}, \alpha(v)\mathbb{N})$, nous définissons l'ensemble suivant :

$$E = \{(x, y) : x \geq 0, y \geq 0, (x = 0 \vee y = 0)\} \subset [-\alpha(v); +\infty[^2.$$

Nous définissons l'ordre \prec^E sur E : pour tout $(x, y), (u, v) \in E$, on a

$$(x, y) \prec^E (u, v) \Leftrightarrow (x < u \vee y > v).$$

Nous définissons également la relation \oplus^E sur E : pour tout $(x, y), (u, v) \in E$, on a

$$(x, y) \oplus^E (u, v) = \begin{cases} (0, y + v) & \text{si } x = 0 \text{ et } u = 0, \\ (x + u, 0) & \text{si } y = 0 \text{ et } v = 0, \\ (x - v, 0) & \text{si } y = 0, u = 0 \text{ et } x \geq v, \\ (0, v - x) & \text{si } y = 0, u = 0 \text{ et } x < v, \\ (u - y, 0) & \text{si } x = 0, v = 0 \text{ et } u \geq y, \\ (0, y - u) & \text{si } x = 0, v = 0 \text{ et } u < y. \end{cases}$$

Nous posons la fonction suivante :

$$f : E \rightarrow \mathbb{R} : (x, y) \mapsto \begin{cases} x & \text{si } y = 0, \\ -y & \text{si } x = 0. \end{cases}$$

Ainsi, il est clair que la fonction f est une bijection entre E et \mathbb{R} , puisqu'à chaque réel positif on peut associer un unique élément $(x, 0)$ de E (où $x \geq 0$) et à chaque réel strictement négatif on peut associer un unique élément $(0, y)$ de E (où $y > 0$).

Démontrons que

$$f((x, y) \oplus^E (u, v)) = f(x, y) + f(u, v)$$

pour tout $(x, y), (u, v) \in E$. Soient $x, y, u, v \in \mathbb{R}^+$. Nous avons

$$\begin{aligned} f((0, y) \oplus^E (0, v)) &= f(0, y + v) = y + v = f(0, y) + f(0, v), \\ f((x, 0) \oplus^E (u, 0)) &= f(x + u, 0) = x + u = f(x, 0) + f(u, 0), \\ f((x, 0) \oplus^E (0, v)) &= \begin{cases} f(x - v, 0) = x - v = f(x, 0) + f(0, v) & \text{si } x \geq v, \\ f(0, v - x) = x - v = f(x, 0) + f(0, v) & \text{si } x < v, \end{cases} \\ f((0, y) \oplus^E (u, 0)) &= \begin{cases} f(u - y, 0) = u - y = f(0, y) + f(u, 0) & \text{si } u \geq y, \\ f(0, y - u) = u - y = f(0, y) + f(u, 0) & \text{si } u < y. \end{cases} \end{aligned}$$

Démontrons que

$$f(x, y) < f(u, v) \Leftrightarrow (x, y) \prec^E (u, v)$$

pour tout $(x, y), (u, v) \in E$. Soient $x, y, u, v \in \mathbb{R}^+$. Nous avons

$$f(x, 0) < f(u, 0) \Leftrightarrow x < u \Leftrightarrow (x, 0) \prec^E (u, 0),$$

$$f(0, y) < f(0, v) \Leftrightarrow -y < -v \Leftrightarrow v < y \Leftrightarrow (0, y) \prec^E (0, v).$$

De plus, si $x = 0$ et $v = 0$ alors on a $f(x, y) < f(u, v)$ si et seulement si $-y < u$, ce qui est toujours vrai si y et u sont différents de zéro. Et si $y = 0$ et $u = 0$, alors $f(x, y)$ n'est jamais inférieur à $f(u, v)$.

Posons les ensembles suivants :

$$Z = \{(x, y) \in E : x, y \in \mathbb{N}\},$$

$$\alpha(v)Z = \{(x, y) \in E : x, y \in \alpha(v)\mathbb{N}\}.$$

Par définition de ces ensembles, nous pouvons facilement observer que

$$f(x, y) \in \mathbb{Z} \Leftrightarrow (x, y) \in Z,$$

$$f(x, y) \in \alpha(v)\mathbb{Z} \Leftrightarrow (x, y) \in \alpha(v)Z.$$

Ainsi, nous avons démontré que

$$f : (E, \prec^E, \oplus^E, Z, \alpha(v)Z) \rightarrow (\mathbb{R}, <, +, \mathbb{Z}, \alpha(v)\mathbb{Z})$$

est un isomorphisme uniforme (on parle d'une forme d'uniformité ici, car les définitions de E, \prec^E, \oplus^E et Z ne dépendent pas de $\alpha(v)$).

Autrement dit, la structure $([-\alpha(v), +\infty[, <, +, \mathbb{N}, \alpha(v)\mathbb{N})$ définit uniformément une copie de $\mathcal{R}_{\alpha(v)} = (\mathbb{R}, <, +, \mathbb{Z}, \alpha(v)\mathbb{Z})$.

Or, par le lemme 5.2.9, nous savons qu'il existe une famille uniforme de structures ω -régulières $(\mathcal{C}_v)_{v \in R}$ telle que, pour tout $v \in R$, nous avons

$$\mathcal{C}_v \simeq ([-\alpha(v), +\infty[, <, +, \mathbb{N}, \alpha(v)\mathbb{N}).$$

Ainsi, pour définir \mathcal{D}_v pour tout $v \in R$, nous pouvons utiliser, dans la structure \mathcal{C}_v cette fois, les mêmes formules que celles qui ont été employées pour définir la structure $(\mathbb{R}, <, +, \mathbb{Z}, \alpha(v)\mathbb{Z})$. Nous obtenons alors que \mathcal{D}_v est bien isomorphe à $\mathcal{R}_{\alpha(v)}$. De plus, vu les définitions de ces formules, l' ω -régularité est préservée. \square

Notons l'ensemble $\text{Irr} =]0, 1[\setminus \mathbb{Q}$. Nous notons également

$$\mathcal{K} = \{\mathcal{R}_\alpha : \alpha \in \text{Irr}\}.$$

Corollaire 5.2.11. La théorie $\text{FO}(\mathcal{K})$ est décidable.

Démonstration. Par le théorème 5.2.10, nous savons qu'il existe une famille de structures ω -régulières $(\mathcal{D}_v)_{v \in R}$ telle que \mathcal{D}_v est isomorphe à $\mathcal{R}_{\alpha(v)}$ pour tout $v \in R$. Ainsi, on peut conclure par la proposition 5.1.4 \square

5.3 Décidabilité de propriétés des mots sturmiens

Dans cette section, nous arrivons au but théorique de ce travail : prouver la décidabilité de la théorie du premier ordre de la collection d'extensions de l'arithmétique de Presburger par un mot Sturmien interprété comme une fonction unaire. Pour cela, nous allons introduire une définition des mots sturmiens, puis utiliser le résultat de décidabilité de $\text{FO}(\mathcal{K})$ qui a été démontré dans la section précédente.

Définition 5.3.1. Soient α un irrationnel et ρ un réel. Le **mot Sturmien de pente α et d'intercept ρ** est le mot $c_{\alpha,\rho} = c_{\alpha,\rho}(1)c_{\alpha,\rho}(2)\cdots \in \{0,1\}^\omega$ tel que

$$c_{\alpha,\rho}(n) = \lfloor (n+1)\alpha + \rho \rfloor - \lfloor n\alpha + \rho \rfloor - \lfloor \alpha \rfloor$$

pour tout $n \in \mathbb{N}$. Si $\rho = 0$, alors on dit que $c_{\alpha,0}$ est le **mot caractéristique de pente α** .

Exemple 5.3.2. Soient $\alpha = \sqrt{2}$ et $\rho = 1$. Alors, nous obtenons

$$\begin{aligned} c_{\alpha,\rho}(1) &= \lfloor 2\alpha + 1 \rfloor - \lfloor \alpha + 1 \rfloor - \lfloor \alpha \rfloor = 3 - 2 - 1 = 0, \\ c_{\alpha,\rho}(2) &= \lfloor 3\alpha + 1 \rfloor - \lfloor 2\alpha + 1 \rfloor - \lfloor \alpha \rfloor = 5 - 3 - 1 = 1, \\ c_{\alpha,\rho}(3) &= \lfloor 4\alpha + 1 \rfloor - \lfloor 3\alpha + 1 \rfloor - \lfloor \alpha \rfloor = 6 - 5 - 1 = 0, \\ c_{\alpha,\rho}(4) &= \lfloor 5\alpha + 1 \rfloor - \lfloor 4\alpha + 1 \rfloor - \lfloor \alpha \rfloor = 8 - 6 - 1 = 1, \\ c_{\alpha,\rho}(5) &= \lfloor 6\alpha + 1 \rfloor - \lfloor 5\alpha + 1 \rfloor - \lfloor \alpha \rfloor = 9 - 8 - 1 = 0, \\ c_{\alpha,\rho}(6) &= \lfloor 7\alpha + 1 \rfloor - \lfloor 6\alpha + 1 \rfloor - \lfloor \alpha \rfloor = 10 - 9 - 1 = 0, \\ c_{\alpha,\rho}(7) &= \lfloor 8\alpha + 1 \rfloor - \lfloor 7\alpha + 1 \rfloor - \lfloor \alpha \rfloor = 12 - 10 - 1 = 1. \end{aligned}$$

Il en découle que $c_{\alpha,\rho} = 0101001\dots$

Nous notons \mathcal{L} la signature de la théorie $\text{FO}(\mathbb{N}, <, +, 0, 1)$ et \mathcal{L}_c la signature obtenue en ajoutant un symbole fonctionnel unaire c à \mathcal{L} . Nous posons $\mathcal{N}_{\alpha,\rho}$ comme étant la \mathcal{L}_c -structure $(\mathbb{N}, <, +, 0, 1, n \rightarrow c_{\alpha,\rho}(n))$.

Notation 5.3.3. Nous notons

$$\begin{aligned} \mathcal{K}_{\text{sturm}} &= \{\mathcal{N}_{\alpha,\rho} : \alpha \in \text{Irr}, \rho \in \mathbb{R}\}, \\ \mathcal{K}_{\text{car}} &= \{\mathcal{N}_{\alpha,0} : \alpha \in \text{Irr}\}. \end{aligned}$$

Théorème 5.3.4. Les théories $\text{FO}(\mathcal{K}_{\text{sturm}})$ et $\text{FO}(\mathcal{K}_{\text{car}})$ sont décidables.

Démonstration. Rappelons que

$$\mathcal{R}_\alpha = (\mathbb{R}, <, +, \mathbb{Z}, \alpha \mathbb{Z}).$$

où $\alpha \in \mathbb{R}_0^+$.

Soit α irrationnel. La structure \mathcal{R}_α permet de définir le nombre 0, l'ensemble des naturels et l'ensemble $\alpha\mathbb{N}$. En effet, on peut écrire zéro de comme étant

$$\exists x \in \mathbb{Z}, \forall n \in \mathbb{Z} : n + x = n,$$

l'ensemble \mathbb{N} comme étant

$$\{x \in \mathbb{Z} : x \geq 0\},$$

et l'ensemble de $\alpha\mathbb{N}$ comme étant

$$\{x \in \alpha\mathbb{Z} : x \geq 0\} \subset \mathbb{R}.$$

La structure \mathcal{R}_α permet également de définir la fonction successeur et la fonction $\lfloor \cdot \rfloor : \mathbb{R} \rightarrow \mathbb{Z}$. En effet, nous pouvons écrire la fonction successeur sur \mathbb{N} de la manière suivante :

$$\forall x \in \mathbb{N}, \exists n \in \mathbb{N} : (x < n) \wedge (\forall c \in \mathbb{N} : (c > x) \Rightarrow (n \leq c)),$$

et la fonction plancher de la manière suivante :

$$\forall x \in \mathbb{R}, \exists n \in \mathbb{Z} : (n \leq x < n + 1).$$

Ici, $n + 1$ peut être défini à partir de n puisque nous avons défini la fonction successeur. Notons que nous pouvons également définir de manière similaire la fonction successeur sur $\alpha\mathbb{N}$.

De plus, il est évident que nous pouvons également définir le singleton $\{\alpha\}$ à partir de $\alpha\mathbb{Z}$, de zéro et de la fonction successeur.

Nous pouvons également définir à partir de \mathcal{R}_α l'ensemble

$$E = \{(\rho, \alpha n, c_{\alpha, \rho}(n)) : \rho \in \mathbb{R}, n \in \mathbb{N}, c_{\alpha, \rho}(n) = \lfloor (n + 1)\alpha + \rho \rfloor - \lfloor n\alpha + \rho \rfloor - \lfloor \alpha \rfloor\}.$$

en utilisant la fonction plancher et la fonction successeur sur $\alpha\mathbb{N}$. À partir de cet ensemble et grâce à la définissabilité de $\{\alpha\}$, nous pouvons définir la fonction qui à l'élément $\alpha n \in \alpha\mathbb{N}$ associe l'élément $\alpha c_{\alpha, \rho}(n) \in \{0, \alpha\}$ de la manière suivante :

$$\alpha n \mapsto \begin{cases} 0 & \text{si } (\rho, \alpha n, 0) \in E, \\ \alpha & \text{sinon,} \end{cases}$$

où ρ est une variable libre.

Ainsi, la \mathcal{L}_c -structure $(\alpha\mathbb{N}, <, +, 0, \alpha n \mapsto \alpha, \alpha c_{\alpha, \rho}(n))$ peut être définie dans \mathcal{R}_α uniformément par rapport à α (uniforme dans le sens où les propriétés de α n'interviennent pas dans la définition de la structure, α peut être considéré comme un simple symbole).

Or, la fonction

$$f : \mathbb{N} \rightarrow \alpha\mathbb{N} : x \mapsto \alpha x$$

forme un isomorphisme entre les structures $\mathcal{N}_{\alpha, \rho}$ et $(\alpha\mathbb{N}, <, +, 0, \alpha, \alpha n \mapsto \alpha c_{\alpha, \rho}(n))$. Ainsi, pour toute \mathcal{L}_c -formule φ , il existe une $\mathcal{L}_{m, a}$ -formule $\psi(\rho)$ telle que

- $\varphi \in \text{FO}(\mathcal{K}_{\text{sturm}})$ si et seulement si $\forall x \psi(x) \in \text{FO}(\mathcal{K})$,
- $\varphi \in \text{FO}(\mathcal{K}_{\text{car}})$ si et seulement si $\psi(0) \in \text{FO}(\mathcal{K})$.

Nous pouvons conclure par le corollaire 5.2.11. □

Ce théorème nous permet de décider si une propriété sur les mots sturmiens exprimée dans $\mathcal{K}_{\text{sturm}}$ ou \mathcal{K}_{car} est vraie ou fausse.

Chapitre 6

Le logiciel Pecan

Pecan est un logiciel qui représente des prédicats logiques à l'aide d'automates de Büchi et qui permet de déterminer automatiquement si une propriété exprimée dans $\mathcal{K}_{\text{sturm}}$ ou \mathcal{K}_{car} est vraie ou fausse. Il est possible d'installer le logiciel sur votre ordinateur en se référant aux instructions données sur les pages GitHub de Reed Oei [20] et [21]. Nous allons montrer à travers ce chapitre quelques exemples d'utilisation du logiciel, et en particulier, pour démontrer des propriétés sur les mots sturmiens. Tous les tests réalisés dans le cadre de ce travail ont été effectués avec le système d'exploitation Ubuntu (version 20.04.6) sur une machine virtuelle (7 gigaoctets de mémoire et 4 processeurs). Nous tenons également à souligner que Pecan n'a pas été mis à jour depuis septembre 2021, cela s'explique probablement par le décès de Reed Oei en avril 2022. Ainsi, certaines optimisations et améliorations prévues n'ont pas été implémentées.

Pecan peut nous permettre, par exemple, de prouver des propriétés simples d'arithmétique comme la commutativité de l'addition de naturels. Pour cela, nous donnons en entrée le code suivant :

```
Restrict x, y are nat.
```

```
Theorem ("Commutativity of addition", {  
  forall x, y. x + y = y + x  
}).
```

Spécifier le type de variables est important pour permettre à Pecan d'utiliser les bonnes définitions des opérateurs arithmétiques utilisés. Ici, nous obtenons en sortie le message :

```
[INFO] Checking if Commutativity of addition is true.  
Commutativity of addition is true.
```

Ainsi, le logiciel confirme immédiatement que la propriété est vraie. Pecan nous permet aussi de définir des prédicats. Pour mieux comprendre son fonctionnement, nous allons montrer un autre exemple simple d'utilisation du logiciel. Nous pouvons prouver grâce à Pecan que tout naturel est soit un nombre pair, soit un nombre impair. Nous commençons

par définir les fonctions `is_even(x)` et `is_odd(x)` qui vérifient respectivement si x est un nombre pair ou impair (à condition que x soit naturel).

```
is_even(x is nat) := exists y is nat. x = 2*y
```

```
is_odd(x is nat) := exists y is nat. x = 2*y+1
```

Maintenant, nous pouvons demander à Pecan de vérifier si tout nombre naturel est soit pair, ou soit impair.

```
Theorem ("Every natural is even or odd", {
  forall x is nat. is_even(x) or is_odd(x)
}).
```

Nous obtenons en sortie le message :

```
[INFO] Checking if Every natural is even or odd is true.
Every natural is even or odd is true.
```

Ainsi, le logiciel confirme immédiatement que la propriété est vérifiée. Une autre fonctionnalité de Pecan est sa capacité à transformer un prédicat en un automate et à l'enregistrer en format HOA [8] afin de pouvoir s'en servir par la suite. Par exemple, si nous voulons créer et enregistrer les automates de Büchi correspondant aux prédicats `is_even` et `is_odd`, alors nous pouvons utiliser les instructions suivantes :

```
#save_aut("is_even.aut", is_even)
#save_aut("is_odd.aut", is_odd)
```

Maintenant, si nous voulons utiliser à nouveau les prédicats `is_even` et `is_odd`, nous ne devons plus définir ces fonctions à chaque fois, il nous suffit d'importer leurs automates à l'aide des commandes suivantes :

```
#load("is_even.aut", "hoa", is_even(x))
#load("is_odd.aut", "hoa", is_odd(x))
```

Nous pouvons même enregistrer le prédicat sous le format SVG afin d'avoir une représentation visuelle de l'automate correspondant. En effet, si nous entrons la commande suivante :

```
#save_aut_img("is_even.svg", is_even)
```

alors, nous avons enregistré au format SVG la représentation du prédicat `is_even`. L'automate de Büchi obtenu se trouve dans la Figure 6.1 et accepte un mot si et seulement s'il est de la forme $0(0|1)^*0^\omega$. Nous précisons que `__ap7` représente x sous forme binaire.

Finalement, une dernière fonctionnalité que nous allons présenter est le fait que le logiciel peut donner des exemples qui vérifient certaines conditions données. Par exemple, nous pouvons demander à Pecan de nous donner un exemple de nombre pair et celui-ci

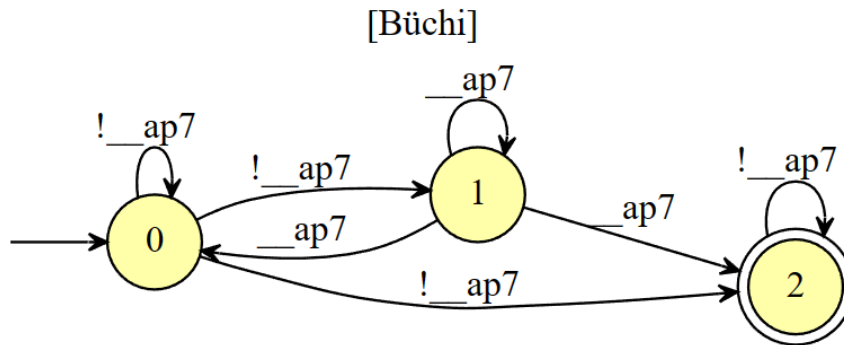


FIGURE 6.1 – Automate de Büchi produit par Pecan et acceptant l’ensemble des représentations binaires de nombres pairs

peut être donné sous différentes formes. Nous donnons en entrée :

```
Display example natFormat { x > 4 and is_even(x) }.
```

```
Display example stdFormat { x > 4 and is_even(x) }.
```

Alors en sortie, nous obtenons respectivement $[(x, 6)]$ et $[(x, [011(0)^\omega])]$.

6.1 Addition de codages binaires de représentations d’Ostrowski

Nous allons prouver grâce au logiciel Pecan que l’automate de Büchi décrit dans la preuve du théorème 4.2.2 accepte bien l’ensemble \oplus^{fin} .

Soit $a \in \mathbb{R}$. Soient x, y et z des a -représentations d’Ostrowski de naturels. Nous exprimons cela dans Pecan de la manière suivante :

```
Let a be bco_standard.
```

```
Let x, y, z be ostrowski(a).
```

Ici, `bco_standard` est un type de données pour les réels encodés en binaire et `ostrowski` est un type de données pour les a -représentations d’Ostrowski également encodées en binaire. Nous allons vérifier que notre automate satisfait la définition récursive de l’addition de nombres naturels : pour tout $x, y \in \mathbb{N}$, nous avons

$$\begin{aligned} 0 + y &= y \\ s(x) + y &= s(x + y) \end{aligned}$$

où $s : \mathbb{N} \rightarrow \mathbb{N}_0 : x \mapsto s(x)$ est la fonction successeur sur \mathbb{N} . Nous exprimons l’addition de

représentations d'Ostrowski dans Pecan de cette manière.

```
Theorem ("Addition base case (0 + y = y).", {
  forall a. forall x, y, z. if bco_zero(x)
  then (bco_adder(a, x, y, z) iff bco_eq(y, z))
}).
```

```
Theorem ("Addition inductive case (s(x) + y = s(x + y)).", {
  forall a. forall x, y, z, u, v. if (bco_succ(a, x, u) and bco_succ(a, z, v))
  then (bco_adder(a, x, y, z) iff bco_adder(a, u, y, v))
}).
```

où

- $\text{bco_zero}(x)$ vérifie si x appartient à l'ensemble 0_* ,
- $\text{bco_adder}(a, x, y, z)$ est l'automate de la preuve du théorème 4.2.2,
- $\text{bco_succ}(a, x, y)$ vérifie si (a, x, y) appartient à $\{(v, x, y) : v \in R, x, y \in A_v^{\text{fin}}, Z_v(x) + 1 = Z_v(y)\}$.

Puisque 0_* est accepté par un automate de Büchi, il est possible d'implémenter la fonction bco_zero dans Pecan via son automate. Il nous reste encore à implémenter la fonction bco_succ . Nous pouvons définir la fonction successeur sur \mathbb{N} peut être définie de la manière suivante :

$$s(x) = y \Leftrightarrow (x < y) \wedge (\forall z(z \leq x) \vee (z \geq y)).$$

Or, nous pouvons implémenter bco_succ de manière similaire.

```
bco_succ(a,x,y) := bco_valid(a,x) and bco_valid(a,y)
                  and bco_leq(x,y) and !(bco_eq(x,y))
                  and forall z. if bco_valid(a,z) then (bco_leq(z,x) or bco_leq(y,z))
```

où

- $\text{bco_eq}(x, y)$ vérifie si x et y sont égaux,
- $\text{bco_leq}(x, y)$ vérifie si $x \leq_{\text{colex}, 2} y$,
- $\text{bco_valid}(a, x)$ vérifie si x est une a -représentation d'Ostrowski.

Or, l'ensemble A^{fin} est ω -régulier et il est facile de construire un automate de Büchi qui accepte l'ensemble des couples de mots égaux. De plus, l'automate représenté dans la figure 3.4 accepte l'ensemble des couples de mots alignés (u, v) si $u \leq_{\text{colex}, 2} v$. Donc, ces trois fonctions peuvent être implémentées dans Pecan via leurs automates.

Ainsi, Pecan confirme immédiatement que les deux propriétés **Addition base case** et **Addition inductive case** sont vraies. En supposant que l'implémentation du logiciel et des automates de bco_standard , ostrowski , bco_zero , bco_adder , bco_eq , bco_leq et bco_valid est correcte, alors Pecan a prouvé que l'automate de Büchi décrit dans la preuve du théorème 4.2.2 accepte bien l'ensemble \oplus^{fin} .

6.2 Mots sturmiens

Dans cette section, nous allons montrer plusieurs exemples d'utilisation de Pecan pour prouver automatiquement des propriétés bien connues sur les mots sturmiens.

Proposition 6.2.1. Tous les mots sturmiens ayant la même pente possèdent le même ensemble de facteurs.

Cette proposition a été démontrée dans [1, Théorème 10.5.3]. Ainsi, si nous démontrons grâce à Pecan une propriété concernant l'ensemble des facteurs des mots caractéristiques, nous pourrions généraliser ce résultat à tous les mots sturmiens.

Définition 6.2.2. Un mot $w \in \{0, 1\}^\omega$ est **équilibré** si, pour tout $a \in \{0, 1\}$, pour tout n naturel, pour tout u, v facteurs de w de longueur n , on a

$$||u|_a - |v|_a| \leq 1.$$

Lemme 6.2.3. Un mot $w \in \{0, 1\}^\omega$ n'est pas équilibré si et seulement s'il existe un facteur u de w qui est un palindrome tel que $0u0$ et $1u1$ sont des facteurs de w .

Ce lemme a été prouvé dans [17, Proposition 2.1.3].

Rappelons que si $w = w_1w_2 \cdots \in \Sigma^\omega$, alors nous notons $w[i \cdots j]$ le facteur

$$w_iw_{i+1} \cdots w_{j-1}w_j.$$

Si $w \in \Sigma^*$, nous notons w^R le miroir de w .

Théorème 6.2.4. Les mots sturmiens sont équilibrés.

Ce théorème a été prouvé dans [15]. Nous pouvons également le prouver à l'aide de Pecan en nous servant du lemme 6.2.3. Soit $a \in \mathbb{R}$. Soient i, j, k et n des a -représentations d'Ostrowski de naturels. Nous exprimons cela dans Pecan de la manière suivante :

`Restrict a is bco_standard.`

`Restrict i, j, k, n are ostrowski(a).`

Ensuite, nous mettons en entrée le code suivant :

```
Theorem ("Characteristic words are balanced.", {
  forall a. forall i,n,j,k. !(palindrome(a, i, n)
  and factor_lt_len(a, i, n, j) and $C[j - 1] = 0 and $C[j + n] = 0
  and factor_lt_len(a, i, n, k) and $C[k - 1] = 1 and $C[k + n] = 1)
}).
```

où

- `palindrome(a, i, n)` vérifie si $c_{a,0}[i \cdots i + n] = c_{a,0}[i \cdots i + n]^R$,
- `factor_lt_len(a, i, n, j)` vérifie si $c_{a,0}[i \cdots i + n] = c_{a,0}[j \cdots j + n]$.

Ainsi, en supposant que l'implémentation des automates de `palindrome` et de `factor_lt_len` est correcte, selon l'article [13], le logiciel confirmerait bien que les mots caractéristiques sont équilibrés après un temps d'exécution de 321,73 secondes. Par la proposition 6.2.1, nous pouvons étendre notre conclusion à tous les mots sturmiens.

Cependant, dans le cadre de ce mémoire, en effectuant le test, nous avons laissé s'exécuter le code pendant plus de 4 heures sans obtenir de réponse. Pecan est très gourmand en terme de ressources, ainsi il n'est pas impossible que la mémoire allouée à la machine virtuelle utilisée soit insuffisante. Cela pourrait être une explication pour ce manque de résultat. En effet, par après, nous avons laissé s'exécuter le code durant 151 secondes sur un ordinateur disposant de plus de ressources (un MacBook), et le logiciel est parvenu à confirmer que le résultat est vrai.

Maintenant, nous allons nous intéresser à deux théorèmes liés aux puissances dans les mots sturmiens.

Définition 6.2.5. Soit x un mot non vide fini. On dit que x est une n -**ème puissance** s'il existe un mot fini y tel que x est le mot composé de $n - 1$ concaténations de y avec lui-même (i.e. $x = y^n$). Si x est une 2-ème puissance, on parle de **carré**, et s'il est une 3-ème puissance, on parle de **cube**.

Théorème 6.2.6. Tous les mots caractéristiques commencent par un carré arbitrairement long.

Ce théorème a été prouvé dans [7]. Nous allons également le démontrer grâce à Pecan. Soit $a \in \mathbb{R}$. Soient i, j, m et n des a -représentations d'Ostrowski de naturels.

```
Restrict a is bco_standard.
Restrict i, j, m, n are ostrowski(a).
```

Nous définissons la fonction `pow_2(a, i, n)` pour qu'elle vérifie si $c_{a,0}[i \cdots i + n - 1] = c_{a,0}[i + n \cdots i + 2n - 1]$.

```
pow_2(a, i, n) := n > 0 and i > 0 and
  forall j. i <= j and j < i + n and $C[j] = $C[j + n]
```

Nous avons voulu enregistrer son automate au format HOA afin de pouvoir réutiliser cette fonction. Cependant, nous avons laissé s'exécuter le code pendant plus de 2 heures sans obtenir de résultat. Nous avons également essayé d'exécuter le code sur un autre ordinateur plus performant (le MacBook mentionné précédemment), mais le programme s'est arrêté sur une erreur de segmentation. Nous nous sommes donc résolus à utiliser l'automate `pow_2` de la bibliothèque Pecan (possédant 155 états et qui aurait été construit comme décrit ci-dessus). Nous l'utilisons pour vérifier le théorème en entrant le code suivant :

```
Theorem ("Characteristic words start with arbitrarily long squares", {
  forall a. forall n. exists m, j. j = 1 and m > n and pow_2(a, j, m)
}).
```

Ainsi, Pecan confirme immédiatement que tous les mots caractéristiques commencent par un carré arbitrairement long. Nous pouvons demander au logiciel un exemple de mot caractéristique qui vérifie cette propriété.

```
start_with_square(a) := exists i, n. i = 1 and n > 0 and pow_2(a, i, n)
```

```
Example ( ostrowskiFormat , {
  bco_standard(a) and start_with_square(a)
}).
```

Ainsi, Pecan renvoie $[(a, [3][3]([2])^\omega)]$. Cela veut dire que pour l'irrationnel $a = [0; 3, 3, \bar{2}]$, alors $c_{a,0}$ commence par un carré. Nous pouvons aisément vérifier que cela est vrai. En effet, comme $a < \frac{1}{3}$, alors

$$\begin{aligned} c_{a,0}(1) &= \lfloor 2a \rfloor - \lfloor a \rfloor = 0, \\ c_{a,0}(2) &= \lfloor 3a \rfloor - \lfloor 2a \rfloor = 0. \end{aligned}$$

Donc $c_{a,0}$ commence par 00 qui est bien un carré.

Théorème 6.2.7. Tous les mots sturmiens contiennent un cube.

Ce théorème a été prouvé dans [7]. Nous allons également le démontrer grâce à Pecan. Soit $a \in \mathbb{R}$. Soient i et n des a -représentations d'Ostrowski de naturels.

```
Restrict a is bco_standard.
Restrict i, n are ostrowski(a).
```

Nous définissons la fonction $\text{pow}_3(a, i, n)$ pour qu'elle vérifie si $c_{a,0}[i \cdots i + n - 1] = c_{a,0}[i + n \cdots i + 2n - 1] = c_{a,0}[i + 2n \cdots i + 3n - 1]$.

```
cube (a, i, n) := pow_2(a, i, n) and pow_2(a, i + n, n)
```

Encore une fois, nous avons voulu enregistrer son automate au format HOA afin de pouvoir réutiliser cette fonction. Nous avons également essayé d'exécuter le code sur un autre ordinateur plus performant (le MacBook mentionné précédemment), mais le programme s'est arrêté sur une erreur de segmentation. Nous avons laissé s'exécuter le code pendant plus de 2 heures sans obtenir de résultat. Nous nous sommes donc résolus à utiliser l'automate pow_3 de la bibliothèque Pecan (possédant 126 états et qui aurait été construit comme décrit ci-dessus). Nous l'utilisons pour vérifier le théorème en entrant le code suivant :

```
Theorem ("Characteristic words contain cubes", {
  forall a. exists i, n. n > 0 & pow_3(a, i, n)
}).
```

Ainsi, Pecan confirme immédiatement que tous les mots caractéristiques contiennent un cube. Par la proposition 6.2.1, nous pouvons étendre notre conclusion à tous les mots sturmiens. Nous pouvons demander au logiciel un exemple de mot caractéristique qui vérifie cette propriété.

```
has_cube(a) := exists i, n. n > 0 and pow_3(a, i, n)
```

```
Example ( ostrowskiFormat , {
bco_standard(a) and has_cube(a)
}).
```

Ainsi, Pecan renvoie [(a, [4] [3] ([2])^ω)]. Cela veut dire que pour l'irrationnel $a = [0; 4, 3, \bar{2}]$, alors $c_{a,0}$ contient un cube. Nous pouvons aisément vérifier que cela est vrai. En effet, comme $a < \frac{1}{4}$, alors

$$\begin{aligned} c_{a,0}(1) &= \lfloor 2a \rfloor - \lfloor a \rfloor = 0, \\ c_{a,0}(2) &= \lfloor 3a \rfloor - \lfloor 2a \rfloor = 0, \\ c_{a,0}(3) &= \lfloor 4a \rfloor - \lfloor 3a \rfloor = 0. \end{aligned}$$

Donc $c_{a,0}$ commence par 000 qui est bien un cube.

Nous remarquons qu'il peut être difficile de travailler avec Pecan lorsque nous voulons créer de nouveaux automates à partir de prédicats : quand l'exécution ne s'arrête pas sur une erreur de segmentation, elle demande du temps et de la mémoire en suffisance. Des ressources importantes semblent être nécessaires pour permettre un bon fonctionnement du programme. Nous pouvons tout de même utiliser les automates de la bibliothèque de Pecan déjà construits pour prouver des théorèmes, mais cela peut être limitant en fonction des prédicats dont nous avons besoin. Pour être vraiment un outil de recherche efficace, Pecan nécessiterait encore d'être développé.

Chapitre 7

Pour aller plus loin

Dans ce mémoire, nous nous sommes fixés comme objectif de prouver la décidabilité des théories $\text{FO}(\mathcal{K}_{\text{sturm}})$ et $\text{FO}(\mathcal{K}_{\text{car}})$. Cependant, dans l'article [13, Section 6] qui a inspiré ce travail, certains résultats supplémentaires ont été abordés et permettraient d'approfondir le sujet.

Définition 7.1. Soit un ensemble $X \subseteq \text{Irr}^n$. Nous définissons l'ensemble suivant :

$$X_R = \{(v_1, \dots, v_n) \in R^n : v_1 \sim_{\#} v_2 \sim_{\#} \dots \sim_{\#} v_n, (\alpha(v_1), \dots, \alpha(v_n)) \in X\}.$$

On dit que X est **reconnaissable modulo $\sim_{\#}$** si X_R est ω -régulier.

Théorème 7.2. Soient X_1, \dots, X_n des ensembles reconnaissables modulo $\sim_{\#}$ par des automates de Büchi $\mathcal{A}_1, \dots, \mathcal{A}_n$. Soit la structure

$$\mathcal{Q} = (\text{Irr}; X_1, \dots, X_n).$$

Alors $\text{FO}(\mathcal{Q})$ est décidable.

Ce résultat permet de démontrer le théorème ci-dessous.

Pour toute $\mathcal{L}_{m,a}$ -formule φ , nous posons

$$\mathcal{M}_{\varphi} = \{\alpha \in \text{Irr} : \mathcal{R}_{\alpha} \models \varphi\}.$$

Soit Irr_{quad} l'ensemble des irrationnels quadratiques dans $]0, 1[$. Nous définissons la structure

$$\mathcal{M} = (\text{Irr}, <, (\mathcal{M}_{\varphi})_{\varphi}, (q)_{q \in \text{Irr}_{\text{quad}}})$$

comme étant l'extension de l'ordre dense $(\text{Irr}, <)$ par des prédicats pour \mathcal{M}_{φ} pour toute $\mathcal{L}_{m,a}$ -formule φ , et par des symboles constants pour tout irrationnel quadratique dans $]0, 1[$.

Théorème 7.3. La théorie $\text{FO}(\mathcal{M})$ est décidable.

Ces deux résultats nous indiquent que, pour tout sous-ensemble de Irr^n qui est reconnaissable modulo $\sim_{\#}$, nous pouvons ajouter un prédicat à la structure \mathcal{M} et cela préservera la décidabilité de la structure. Ainsi, nous pouvons non seulement prouver des propriétés exprimées avec l'arithmétique de Presburger sur tous les mots sturmiens, mais également sur les mots sturmiens dont la pente appartient à un sous-ensemble de Irr qui est reconnaissable modulo $\sim_{\#}$.

Par exemple, les ensembles suivants sont reconnaissables modulo $\sim_{\#}$:

- l'ensemble des $\alpha \in \text{Irr}$ tels que les coefficients de leur développement en fraction continue sont des puissances de 2,
- l'ensemble des $\alpha \in \text{Irr}$ tels que les coefficients de leur développement en fraction continue appartiennent (ou non) à un ensemble fini donné,
- l'ensemble des $\alpha \in \text{Irr}$ tels que tous les coefficients pairs (ou impairs) de leur développement en fraction continue sont 1.

Cependant, cette méthode a ses limites. Nous ne pouvons pas, par exemple, ajouter un prédicat pour l'ensemble de tous les $\alpha \in \text{Irr}$ tels que les coefficients du développement en fraction continue de α sont strictement croissants, et nous assurer que la théorie de la structure obtenue soit toujours bien décidable.

Lexique

De nombreuses notations sont employées à travers ce mémoire. Pour faciliter sa lecture, nous vous proposons ci-dessous une liste des différentes notations qui sont utilisées.

- Z_x est, pour tout $x \in X$, l'ensemble $\{y \in Y : (x, y) \in Z\}$ si X, Y et Z sont des ensembles tels que $Z \subseteq X \times Y$.
- ε est le mot vide.
- $[w_0 \cdots w_n]_2$ est la valeur $\sum_{i=0}^n w_i 2^i$ où $w_i \in \{0, 1\}$ pour tout $i \geq 0$.
- $[b_1 b_2 \cdots b_{N+1}]_\alpha = X$ si $\alpha = [0; a_1, a_2, \dots]$, $X \in \mathbb{Z}$ et $X = \sum_{n=0}^N b_{n+1} q_n$ où $\frac{p_n}{q_n}$ est le n -ème convergent de α . On dit que X est la α -valeur de $b_1 b_2 \cdots b_{N+1}$.
De plus, si $X \in \mathbb{N}$, $0 \leq b_1 < a_1$, $0 \leq b_{n+1} \leq a_{n+1}$ pour tout $n \geq 1$, $b_n = 0$ quand $b_{n+1} = a_{n+1}$ pour tout $n \geq 1$, alors $b_1 b_2 \cdots b_{N+1}$ est une α -représentation d'Ostrowski de X (ou la α -représentation d'Ostrowski si on prend celle sans zéro de queue).
- $I_\alpha = [[\alpha] - \alpha, 1 + [\alpha] - \alpha[$.
- $[b_1 b_2 \cdots]_\alpha = x$ si $\alpha = [0; a_1, a_2, \dots]$, $x \in I_\alpha$ et $x = \sum_{n=0}^\infty b_{n+1} \beta_n$ où β_n est la n -ème différence de α . On dit que x est la α -valeur de $b_1 b_2 \cdots$.
De plus, si $b_n \in \mathbb{Z}$, $0 \leq b_n \leq a_n$ et $b_n = 0$ quand $b_{n+1} = a_{n+1}$ pour tout $n \geq 1$, $b_1 \neq a_1$ et $b_n \neq a_n$ pour une infinité de n impairs, alors $b_1 b_2 \cdots$ est la α -représentation d'Ostrowski de x .
- $f_\alpha : \mathbb{R} \rightarrow I_\alpha$ est la fonction qui à un réel x associe $x - u$ où u est l'unique entier tel que $x - u \in I_\alpha$.
- $\Sigma_\#$ est l'alphabet $\{0, 1, \#\}$.
- H_∞ est l'ensemble des mots infinis sur $\Sigma_\#$ qui commencent par $\#$ et dans lesquels $\#$ apparaît une infinité de fois.
- $\mathbb{N}_\#$ est l'alphabet $\mathbb{N} \cup \{\#\}$.
- \mathbb{N}_∞ est l'ensemble des mots infinis sur $\mathbb{N}_\#$ qui commencent par $\#$ et dans lesquels $\#$ apparaît une infinité de fois.
- R est l'ensemble des mots infinis sur $\Sigma_\#$ de la forme $(\#(0|1)^*1(0|1)^*)^\omega$.
- $\alpha(w)$ est, pour $w \in R$, l'unique irrationnel $\alpha \in]0, 1[$ tel que w est un $\#$ -codage binaire de la fraction continue de α .

- A_v^{fin} est, pour un $v \in R$ donné, l'ensemble des mots $w \in H_\infty$ tels que w est la $\#$ - v -représentation d'Ostrowski d'un nombre naturel.
- A_v est, pour un $v \in R$ donné, l'ensemble des mots $w \in H_\infty$ tels que w est la $\#$ - v -représentation d'Ostrowski d'un réel $c \in I_{\alpha(v)}$.
- $A^{\text{fin}} = \{(v, w) : v \in R, w \in A_v^{\text{fin}}\}$.
- $A = \{(v, w) : v \in R, w \in A_v\}$.
- $Z_v : A_v^{\text{fin}} \rightarrow \mathbb{N} : w \mapsto N$ tel que w est la $\#$ - v -représentation d'Ostrowski de N .
- $O_v : A_v \rightarrow I_{\alpha(v)} : w \mapsto c$ tel que w est la $\#$ - v -représentation d'Ostrowski de c .
- $0_v = Z_v^{-1}(0)$.
- $1_v = Z_v^{-1}(1)$.
- $0_* = \{(v, 0_v) : v \in R\}$.
- $1_* = \{(v, 1_v) : v \in R\}$.
- $\prec^{\text{fin}} = \{(v, s, t) \in R \times (A_v^{\text{fin}})^2 : Z_v(s) < Z_v(t)\}$.
- $\prec = \{(v, s, t) \in R \times (A_v)^2 : O_v(s) < O_v(t)\}$.
- $\mathcal{A} = (Q \cup \{\perp\}, \mathbb{Z}, (r_0, s_0), F, \delta)$ est l'automate fini déterministe à 2 bandes acceptant $(d_m \cdots d_1, w_m \cdots w_1) \in \mathbb{N}^m \times \mathbb{Z}^m$ si et seulement si pour tout irrationnel α tel que $\alpha = [0; d_1, \dots, d_m, \dots]$, on a $[w_1 \cdots w_m]_\alpha = 0$.
- $\oplus^{\text{fin}} = \{(v, s_1, s_2, s_3) : v \in R, s_1, s_2, s_3 \in A_v^{\text{fin}}, Z_v(s_1) + Z_v(s_2) = Z_v(s_3)\}$.
- $\oplus = \{(v, s_1, s_2, s_3) : v \in R, s_1, s_2, s_3 \in A_v, O_v(s_1) + O_v(s_2) \equiv O_v(s_3) \pmod{1}\}$.
- $w[i \cdots j]$ est le facteur $w_i w_{i+1} \cdots w_{j-1} w_j$ de $w = w_1 w_2 \cdots \in \Sigma^\omega$.
- \mathcal{L}_m est la signature de la théorie $\text{FO}(\mathbb{R}, <, +, \mathbb{Z})$.
- $\mathcal{L}_{m,a}$ est la signature obtenue en ajoutant un symbole de fonction unaire a à \mathcal{L}_m .
- \mathcal{R}_α est la $\mathcal{L}_{m,a}$ -structure $(\mathbb{R}, <, +, \mathbb{Z}, \alpha \mathbb{Z})$ où $\alpha \in \mathbb{R}_0^+$.
- $n_v = \underbrace{(((1_v \oplus_v^{\text{fin}} 1_v) \oplus_v^{\text{fin}} 1_v) \cdots \oplus_v^{\text{fin}} 1_v)}_{n \text{ fois}}$.
- $F = \{(v, s) \in A^{\text{fin}} : \alpha(v) Z_v(s) < 1\}$.
- $\text{Irr} =]0, 1[\setminus \mathbb{Q}$.
- $\mathcal{K} = \{\mathcal{R}_\alpha : \alpha \in \text{Irr}\}$.
- $c_{\alpha,\rho}(n) = \lfloor (n+1)\alpha + \rho \rfloor - \lfloor n\alpha + \rho \rfloor - \lfloor \alpha \rfloor$.
- \mathcal{L} est la signature de la théorie $\text{FO}(\mathbb{N}, <, +, 0, 1)$.
- \mathcal{L}_c est la signature obtenue en ajoutant un symbole fonctionnel unaire c à \mathcal{L} .
- $\mathcal{N}_{\alpha,\rho}$ est la \mathcal{L}_c -structure $(\mathbb{N}, <, +, 0, 1, n \rightarrow c_{\alpha,\rho}(n))$.
- $\mathcal{K}_{\text{sturm}} = \{\mathcal{N}_{\alpha,\rho} : \alpha \in \text{Irr}, \rho \in \mathbb{R}\}$.
- $\mathcal{K}_{\text{car}} = \{\mathcal{N}_{\alpha,0} : \alpha \in \text{Irr}\}$.

Bibliographie

- [1] Jean-Paul Allouche et Jeffrey Shallit, *Automatic sequences*, Cambridge University Press, Cambridge, 2003, Theory, applications, generalizations.
- [2] Christel Baier et Joost-Pieter Katoen, *Principles of model checking (representation and mind series)*, The MIT Press, 2008, disponible via l'URL <<https://dl.acm.org/doi/book/10.5555/1373322>>.
- [3] Aseem Baranwal, Luke Schaeffer et Jeffrey Shallit, *Ostrowski-automatic sequences : theory and applications*, Theoret. Comput. Sci. **858** (2021), p. 122-142, disponible via l'URL <<https://doi.org/10.1016/j.tcs.2021.01.018>>.
- [4] Jean Bernoulli, *Sur une nouvelle espece de calcul*, Recueil pour les astronomes, Desaint, Libraire rue du Foin, Paris, 1771, disponible via l'URL <<https://hal.science/hal-00482605>>, p. 33.
- [5] Julius Richard Büchi, *On a decision method in restricted second order arithmetic*, Logic, Methodology and Philosophy of Science (Proc. 1960 Internat. Congr.) Stanford Univ. Press, Stanford, Calif., 1962, p. 1-11.
- [6] Ethan M. Coven et Gustave A. Hedlund, *Sequences with minimal block growth*, Math. Systems Theory **7** (1973), p. 138-153, disponible via l'URL <<https://doi.org/10.1007/BF01762232>>.
- [7] Artūras Dubickas, *Squares and cubes in sturmian sequences*, RAIRO - Theoretical Informatics and Applications **43** (2009), n° 3, p. 615-624.
- [8] Alexandre Duret-Lutz, František Blahoudek, Jan Křetínský, Jan Strejček et Joachim Klein, *The Hanoi Omega-Automata Format*, disponible via l'URL <<http://adl.github.io/hoaf/>>.
- [9] Seth Fogarty et Moshe Y. Vardi, *Efficient büchi universality checking*, Tools and algorithms for the construction and analysis of systems (Javier Esparza et Rupak Majumdar, édés), Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, p. 205-220.
- [10] Alexi Block Gorman et Christian Schulz, *Fractal dimensions of k-automatic sets*, 2022, arXiv : 2205.02915 [math.LO].
- [11] Christoph Haase, *A survival guide to presburger arithmetic*, **5** (2018), n° 3, p. 67-82, disponible via l'URL <<https://www.cs.ox.ac.uk/people/christoph.haase/home/publication/haa-18/haa-18.pdf>>.

- [12] Philipp Hieronymi, *Expansions of the ordered additive group of real numbers by two discrete subgroups*, J. Symb. Log. **81** (2016), n° 3, p. 1007-1027, disponible via l'URL <<https://doi.org/10.1017/jsl.2015.34>>.
- [13] Philipp Hieronymi, Dun Ma, Reed Oei, Luke Schaeffer, Christian Schulz et Jeffrey Shallit, *Decidability for Sturmian words*, 2021, disponible via l'URL <<https://arxiv.org/abs/2102.08207>>.
- [14] Joseph Louis Lagrange, Joseph Alfred Serret et Gaston Darboux, *Œuvres de Lagrange*, Gauthier-Villars, Paris, 1867–1892, disponible via l'URL <<https://gallica.bnf.fr/ark:/12148/bpt6k215570z/f583.item>>.
- [15] Julien Leroy, *Cours de Combinatorics on Words*, Université de Liège, 2021.
- [16] Julien Leroy, *Cours de Logique et théorie des ensembles*, Université de Liège, 2022.
- [17] M. Lothaire, *Algebraic combinatorics on words*. Vol. 90, Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 2002, disponible via l'URL <<https://doi.org/10.1017/CB09781107326019>>.
- [18] Marston Morse et Gustav A. Hedlund, *Symbolic dynamics II. Sturmian trajectories*, Amer. J. Math. **62** (1940), p. 1-42, disponible via l'URL <<https://doi.org/10.2307/2371431>>.
- [19] Reed Oei, Dun Ma, Christian Schulz et Philipp Hieronymi, *Pecan : An Automated Theorem Prover for Automatic Sequences using Büchi Automata*, 2021, arXiv : 2102.01727 [cs.LO].
- [20] Reed Oei, Eric Ma, Christian Schulz et Philipp Hieronymi, *Pecan*, 2020, disponible via l'URL <<https://github.com/ReedOei/Pecan>>.
- [21] Reed Oei, Eric Ma, Christian Schulz et Philipp Hieronymi, *Pecan*, 2020, disponible via l'URL <<https://github.com/ReedOei/SturmianWords>>.
- [22] Dominique Perrin, *Infinite words automata, semigroups, logic and games*, Pure and applied mathematics; 141, Elsevier/Academic, San Diego, Calif. ; 2003.
- [23] Thomas Richez, *Les fractions continues*, mém. de mast., Université de Strasbourg, 2010–2011, disponible via l'URL <https://t-richez.pagesperso-orange.fr/ressources/recherche/memoire_fractions_continues.pdf>.
- [24] Andrew Mansfield Rockett et Peter Szűsz, *Continued fractions*, World Scientific Publishing Co., Inc., River Edge, NJ, 1992, disponible via l'URL <<https://doi.org/10.1142/1725>>.
- [25] Christian Carl Schulz, *A question on "Decidability for Sturmian words"*, Communication personnelle, Avril 2023.
- [26] Volker Weispfenning, *Mixed real-integer linear quantifier elimination*, Proceedings of the 1999 international symposium on symbolic and algebraic computation, ISSAC '99, Association for Computing Machinery, Vancouver, British Columbia, Canada, 1999, p. 129-136, disponible via l'URL <<https://doi.org/10.1145/309831.309888>>.