UNIVERSITÉ DU QUÉBEC À MONTRÉAL

LANGAGES APÉRIODIQUES ET LANGAGES COMPLÈTEMENT RÉDUCTIBLES

MÉMOIRE

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN MATHÉMATIQUES

PAR

YEENA KOMI KPEGLO

AOÛT 2014

REMERCIEMENTS

J'exprime ma reconnaissance et gratitude à l'administration , au département de mathématiques et à l'ensemble du corps enseignant de l'Université du Québec À Montréal (UQÀM) pour leurs efforts à garantir l'aboutissement de ce programme de maîtrise.

Je tiens à remercier mon Directeur de mémoire, Monsieur Christophe REUTENAUER pour son orientation vers les bonnes thématiques, sa disponibilité et ses conseils avisés tout au long de la réalisation de ce mémoire et de ce programme.

Je remercie particulièrement mes parents, ma soeur et mon frère pour leur attention, leur soutien moral et pour tous les efforts qu'ils ont consentis pendant ces années d'étude.

Enfin, je remercie toutes les personnes de mon entourage, amis et proches, qui de diverses manières m'ont permis de mener ce travail dans de meilleures conditions.

TABLE DES MATIÈRES

RÉSUMÉ

Nous caractérisons dans ce travail les langages reconnaissables sans-étoile et les langages reconnaissables complètement réductibles. Les langages sans-étoile sont ceux construits à partir des lettres et en n'utilisant que les opérateurs booléens et produit, mais sans utiliser l'étoile de Kleene. Le principal outil de caractérisation de ces langages, qui utilise le monoïde syntaxique, est le théorème de Schützenberger dont la preuve complète sera exposée. Les langages complètement réductibles sont quant à eux, ceux dont la répresentation syntaxique de leur série caractéristique est complètement réductible. Cette famille contient des langages remarquables, tels que les langages birécurrents, en particulier les sous-monoïdes engendrés par un code bifixe.

INTRODUCTION

Ce mémoire est principalement subdivisé en deux (2) parties. La première partie s'intéresse aux langages reconnaissables sans-étoile et la démonstration du théorème de Schützenberger qui permet de les caractériser. Avant d'aborder les outils qui entrent directement dans la démonstration de ce théorème, nous définissons dans les premiers chapitres, les notions importantes de la théorie des langages et des automates, notamment le théorème de Kleene qui stipule que les langages obtenus par les opéarations rationnelles à partir de langages finis sont reconnaissables. Le théorème de Schützenberger énonce que les langages sans-étoile, c'est-à-dire ceux obtenus sans utiliser l'opérateur étoile sont reconnus par des automates finis dont le monoïde de transition est apériodique. Les documents utilisés dans cette première partie sont (AUTEBERT, 1994), (EILENBERG, 1974) et (PIN, 1984). La démonstration du théorème de Schützenberger est principalement tirée de (LAWSON, 2004) et de (SCHÜTZENBERGER, 1965).

La deuxième partie, qui concerne les langages complètement réductibles, commence par des rappels et définitions des termes utilisés dans cette partie. Un langage est complètement réductible si sa représentation linéaire syntaxique est complètement réductible. Le théorème de Perrin énonce que les langages birécurents, c'est-à-dire ceux dont l'automate minimal est fortement connexe, ainsi que automate minimal miroir, sont complètement réductibles. Les références de cette partie sont (PIN, 1984), (REUTENAUER, 1981) et (BERSTEL, J.; PERRIN, D.; REUTENAUER C., 2010) ; le schéma s'inspirant de l'article (PERRIN, 2013).

CHAPITRE I

LANGAGES FORMELS

Le but de ce chapitre est de définir les notions de mots et langage que nous utiliserons par la suite. Nous y aborderons également les différentes opérations de composition de langages, notamment l'étoile de Kleene.

1.1 Alphabet et Mots

Définition 1.1.1. Soit Σ un ensemble fini non vide de symboles qu'on appelle *lettres*. L'ensemble Σ est appelé *alphabet*.

Un *mot* sur l'alphabet Σ est une suite finie non vide de lettres de Σ ; il est donné par une fonction

$$w : \{0, 1, \ldots, n-1\} \to \Sigma.$$

Ainsi, un mot w est entièrement déterminé par ses valeurs

$$w(0), w(1) \ldots, w(n-1).$$

Par souci de clarté, nous l'écrivons $w = w_0 w_1 w_2 \ldots w_{n-1}$. L'entier n est la *longueur* du mot w et est notée $|w|$.

Le mot vide correspond à la suite vide et est noté ε. L'ensemble de tous les mots

sur l'alphabet Σ est noté Σ^* et l'ensemble de tous les mots privé de ε est noté Σ^+.

Définition 1.1.2. Etant donnés deux mots $x, y \in \Sigma^*$, nous pouvons former un mot $x \cdot y$ appelé la *concaténation* de x et y, en faisant suivre les lettres de y à celles de x. L'opération $\cdot$ est donc définie comme suit :

$$\cdot : \Sigma^* \times \Sigma^* \to \Sigma^*$$
$$(x, y) \mapsto x \cdot y \overset{noté}{=} xy$$

Cette opération est associative avec pour élement identité ε. L'ensemble Σ^* possède donc une structure de monoïde. Σ^* est le *monoïde libre* sur Σ.

Un mot $w \in \Sigma^*$ est un *facteur* d'un mot $x \in \Sigma^*$ s'il existe $u, v \in \Sigma^*$ tel que $x = uwv$. On vérifie aisément que la relation *est un facteur de* est une relation d'ordre partiel sur Σ^*. Un facteur w de x est *propre* si $w \neq x$.
Un mot $w \in \Sigma^*$ est un *préfixe* d'un mot $x \in \Sigma^*$ s'il existe un mot $u \in \Sigma^*$ tel que $x = wu$. La relation *est un préfixe de* est également une relation d'ordre partiel sur Σ^* appelée *ordre préfixe*. Nous écrivons $w \leq x$ quand w est un préfixe de x et $w < x$ quand nous avons $w \leq x$ et $w \neq x$.
De manière symétrique, nous définissons le *suffixe* w d'un mot x par $x = vw$ pour $v \in \Sigma^*$.

Définition 1.1.3. Étant donnés deux monoïdes M et N, un *morphisme* de monoïdes $\varphi : M \to N$ est une application de M dans N telle que :
- $\varphi(\varepsilon_M) = \varepsilon_N$
- $\varphi(xy) = \varphi(x)\varphi(y)$ pour tout $x, y \in M$

Le terme *morphisme* designera par la suite, selon le contexte, soit un morphisme de monoïdes, soit un morphisme de semi-groupes.

Exemple 1.1.1. Les ensembles

- $\Sigma_1 = \{0, 1\}$;
- $\Sigma_2 = \{a, b, c, \ldots, z\}$;
- $\Sigma_3 = \{\diamondsuit, \heartsuit, \clubsuit, \spadesuit\}$.

sont des alphabets.

Exemple 1.1.2. Soit $\Sigma = \{a, b\}$ un alphabet. $w = ab$ et $w' = bbaa$ sont des mots sur Σ. Les longueurs $|w| = 2$ et $|w'| = 4$.
La concatenation de w et w', $w \cdot w' = ww' = ab \cdot bbaa = abbbaa$.

1.2 Langages

Définition 1.2.1. Soit Σ un alphabet. Un *langage* L sur Σ est un sous-ensemble de Σ^*.

1.3 Opérations sur les langages

Soit L et M, deux langages sur Σ. Nous définissons les opérations suivantes :

1.3.1 Opérations booléennes

Les ensembles $L \cap M$, $L \cup M$ et $L \setminus M$ sont des langages sur Σ. Le langage $\overline{L} = \Sigma^* \setminus L$ est le complement de L dans Σ^*.
Les opérations d'intersection ($\cap$), d'union ($\cup$) et de différence ensembliste ($\setminus$) sont appelées des *opérations booléennes*.

Remarque 1.3.1. Nous préfererons parfois, selon le contexte, $L + M$ à $L \cup M$ pour l'union des langages.

1.3.2 Produit

Nous définissons le produit de L et M comme suit :

$$L \cdot M = \{xy : x \in L\ ,\ y \in M\}.$$

Remarque 1.3.2. Nous n'écrirons le $\cdot$ que lorsqu'il est (absolument) nécessaire.

1.3.3 Étoile de Kleene

Définition 1.3.1. Soit $L \subseteq \Sigma^*$ un langage. Nous pouvons définir $L^0 = \{\varepsilon\}$ et $L^n = L^{n-1} \cdot L$.

Le langage L^n avec $n > 0$ contient donc tous les mots w de la forme

$$w = w_1 w_2 \dots w_n;\ w_i \in L.$$

L'*étoile de Kleene* d'un langage L notée L^* est définie comme suit :

$$L^* = L^0 + L^1 + L^2 + \dots .$$

Nous pouvons également définir

$$L^+ = L^1 + L^2 + \dots .$$

Notation. Soit un mot w, nous notons $w^n, n \geq 1$, la concaténation de w avec lui-même n-fois.

Nous pouvons définir Σ^n récursivement par :

- $\Sigma^0 = \{\varepsilon\}$
- $\Sigma^n = \Sigma^{n-1} \cdot \Sigma$

Remarque 1.3.3. Un langage peut-être défini en utilisant les opérations booléennes, le produit et l'étoile de Kleene

Exemple 1.3.1. Soit $\Sigma = \{a, b\}$ un alphabet.

Ci-dessous quelques exemples de langages sur Σ :

- $\Sigma^* = \{a, b\}^* \overset{noté}{=} (a + b)^*$.
- $L_1 = ab(a + b)^*$ est l'ensemble des mots qui commencent par ab.
- $L_2 = (a + b)^5$ est l'ensemble des mots de longueur 5 sur Σ.

CHAPITRE II

LANGAGES RECONNAISSABLES ET THÉORÈME DE KLEENE

Dans ce chapitre nous définissons les notions d'automate fini, de langage reconnaissable et de langages rationnels. Nous y demontrons également le théorème de de Kleene qui établit le lien entre langages reconnaissables et langages rationnels. Tout au long du chapitre, Σ désigne toujours un alphabet fini.

2.1 Automates finis

Définition 2.1.1. Soit Σ un alphabet fini. Un *automate déterministe fini* ou, plus simplement, *automate fini* $\mathcal{A}$ est un quintuplet :

$$\mathcal{A} = (\Sigma, Q, I, \delta, F)$$

où :

- Q est un ensemble *fini* d'éléments appelés *états* ;
- I est un sous-ensemble de Q contenant un seul élément appelé *état initial* ;
- δ est une fonction $\delta : Q \times \Sigma \to Q$ appelée *fonction de transition* ;
- F est un sous-ensemble de Q appelé ensemble des *états finaux*.

Définition 2.1.2. Une *arête* de l'automate $\mathcal{A}$ est un triplet (p, σ, q) avec $p, q \in Q$

et $\sigma \in \Sigma$ et tels que $\delta(p, \sigma) = q$. Un *chemin* c dans $\mathcal{A}$ est une séquence finie

$$c = (q_0, \sigma_1, q_1)(q_1, \sigma_2, q_2)...(q_{k-1}, \sigma_k, q_k)$$

d'arêtes consécutives. $k > 0$ est appelé la *longueur* du chemin.

Notation. Une arête est notée

$$\sigma : p \to q$$

ou

$$p \xrightarrow{\sigma} q.$$

Un chemin c est noté

$$c = (q_0, \sigma_1, \cdots, \sigma_k, q_k)$$

ou

$$q_0 \xrightarrow{\sigma_1} q_1 \cdots \xrightarrow{\sigma_k} q_k$$

ou

$$q_0 \xrightarrow{c} q_k$$

ou encore

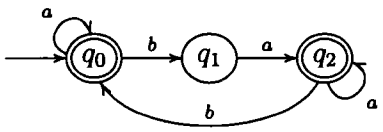
$$c : q_0 \to q_k.$$

L'élément $s = \sigma_0 \cdots \sigma_k \in \Sigma^*$ est appelé *l'étiquette* de c et est noté $|\, c \,|$.
Le *chemin nul* ou *chemin trivial* ε_q est celui de longueur 0, qui commence et se termine à q, avec $q \in Q$; nous avons alors $|\varepsilon_q| = \varepsilon$.
Un chemin $c : i \to f$ avec $i \in I$, $f \in F$, c'est-à-dire qui commence à un état initial et se termine à un état final, est dit *réussi*. Les étiquettes des chemins réussis dans $\mathcal{A}$ définissent un sous-ensemble $L(\mathcal{A})$ de Σ^* appelé le *langage accepté* ou *reconnu* par $\mathcal{A}$.

Exemple 2.1.1. Soit un automate fini $\mathcal{A} = (\Sigma, Q, I, \delta, F)$ défini comme suit :
- $\Sigma = \{a, b\}$;

- $Q = \{q_0, q_1, q_2\}$;
- $I = \{q_0\}$;
- $\delta = \{(q_0, a, q_0), (q_0, b, q_1), (q_1, a, q_2), (q_2, a, q_2), (q_2, b, q_0)\}$;
- $F = \{q_0, q_2\}$.

Il est représenté graphiquement par :



où les flèches entrantes désignent les états initiaux et les doubles cercles les états finaux.

Remarque 2.1.1. Nous pouvons étendre la fonction transition δ à une fonction $\delta^* : Q \times \Sigma^* \to Q$ telle que, pour $\sigma \in \Sigma$, $w \in \Sigma^*$ et $q \in Q$:

- $\delta^*(q, \varepsilon) = q$;
- $\delta^*(q, \sigma) = \delta(q, \sigma)$;
- $\delta^*(q, \sigma w) = \delta^*(\delta(q, \sigma), w)$.

Nous désignons $\delta^*(q, w)$ par $q \cdot w$ ou qw s'il n'y a pas d'ambiguïté.

2.2 Langages reconnaissables

Définition 2.2.1. (Reconnaissabilité par un automate) Un langage L est dit *reconnaissable* s'il existe un automate fini $\mathcal{A}$ tel que $L(\mathcal{A}) = L$.

Un langage L n'est donc reconnaissable que si tous les mots de L sont reconnus par un automate fini $\mathcal{A}$ et si $\mathcal{A}$ ne reconnaît que les mots de L.

Nous énonçons maintenant quelques propositions de composition de langages reconnaissables que nous utiliseront par la suite :

Proposition 2.2.1. *Soit L et M deux langages reconnaissables sur Σ. Alors $L+M$ est reconnaissable.*

Démonstration. Soit $L = L(\mathcal{A})$ et $M = L(\mathcal{B})$, avec $\mathcal{A} = (\Sigma, Q_A, I_A, \delta_A, F_A)$ et $\mathcal{B} = (\Sigma, Q_B, I_B, \delta_B, F_B)$. Sans perte de généralité, supposons $Q_A \cap Q_B = \emptyset$. Définissons

$$\mathcal{C} = \mathcal{A} \cup \mathcal{B} = (\Sigma, Q_A \cup Q_B, I_A \cup I_B, \delta_C, F_A \cup F_B).$$

Une arête est dans $\mathcal{C}$ ssi elle est dans $\mathcal{A}$ ou dans $\mathcal{B}$. Il en résulte immédiatement que chaque chemin dans $\mathcal{C}$ est soit un chemin dans $\mathcal{A}$ soit un chemin dans $\mathcal{B}$. D'où

$$L(\mathcal{C}) = L(\mathcal{A} \cup \mathcal{B}) = L(\mathcal{A}) \cup L(\mathcal{B}) = L + M. \qquad \square$$

Proposition 2.2.2. *Si L et M sont reconnaissables, alors LM est reconnaissable.*

Démonstration. Soit $L = L(\mathcal{A})$ et $M = L(\mathcal{B})$, avec $\mathcal{A} = (\Sigma, Q_A, I_A, \delta_A, F_A)$ et $\mathcal{B} = (\Sigma, Q_B, I_B, \delta_B, F_B)$. Sans perte de généralité, supposons $Q_A \cap Q_B = \emptyset$. Nous supposerons également $\varepsilon \notin M$ car si $\varepsilon \in M$ alors $LM = L + LM'$ avec $M' = M \setminus \varepsilon$. Il suffit, d'après la proposition 2.2.1, de démontrer que LM' est reconnaissable. Définissons :

$$\mathcal{C} = (\Sigma, Q_A \cup Q_B, I_A, \delta_C, F_B).$$

La fonction de transition δ_C est définie comme suit : on reporte dans $\mathcal{C}$ toutes les transitions de $\mathcal{A}$ et de $\mathcal{B}$ auxquelles on ajoute, pour tout $f_A \in F_A$ et pour toute transition $i_B \xrightarrow{a} q_B$ dans $\mathcal{B}$, $i_B \in I_B$, de nouvelles transitions $f_A \xrightarrow{a} q_B$; c'est-à-dire pour chaque état final de $\mathcal{A}$ on copie toutes les transitions sortantes des états initiaux de $\mathcal{B}$.

Vérifions maintenant que $L(\mathcal{C}) = LM$. Nous avons $x \in LM$ ssi $x = uw$ où $u \in L, w \in M$, avec $w \neq \varepsilon$. On a $w = av$, $a \in \Sigma$ et $v \in \Sigma^*$. Ainsi $x = uav$ où $u : i_A \to f_A$, $f_A \xrightarrow{a} q_B$ et $v : q_B \to f_B$ avec $i_A \in I_A, f_A \in F_A, q_B \in Q_B, f_B \in F_B$. Ceci équivaut, par construction, à $x \in L(\mathcal{C})$. D'où $L(\mathcal{C}) = LM$. $\square$

Proposition 2.2.3. *Si L est reconnaissable, alors il en est de même pour L^*.*

Démonstration. Soit $L = L(\mathcal{A})$ avec $\mathcal{A} = (\Sigma, Q, I, \delta, F)$. Construisons l'automate

$$\mathcal{B} = (\Sigma, Q \cup \{q_\varepsilon\}, I \cup \{q_\varepsilon\}, \gamma, F \cup \{q_\varepsilon\}).$$

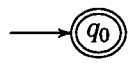
Les transitions de $\mathcal{B}$ sont celles de $\mathcal{A}$ plus de nouvelles transitions obtenues comme suit : on crée pour tout $f \in F$ et pour toute transition $i \xrightarrow{a} q$ dans $\mathcal{A}$, $i \in I$, des transitions $f \xrightarrow{a} q$; c'est-à-dire pour chaque état final on copie toutes les transitions sortantes des états initiaux dans $\mathcal{A}$.

Vérifions que cet automate reconnaît bien L^*. Le mot vide est reconnu par le nouvel état q_ε.

Considérons donc $x \in L^*$, avec x non-vide. On a $x = v_1 \dots v_n$, $v_i \in L, v_i \neq \varepsilon$. Chaque v_i appartient à $L(\mathcal{A})$ et $v_i = a_i u_i$, $a_i \in \Sigma$. Donc $x = a_1 u_1 a_2 u_2 \dots a_n u_n$, ce qui équivaut à l'existence dans $\mathcal{B}$ d'un chemin réussi étiqueté x, les $a_1, a_2 \dots$ étant les étiquettes des nouvelles transitions. D'où $L^* = L(\mathcal{B})$. □

Exemple 2.2.1. L'automate vide $\mathcal{A}$ sans aucun état reconnait le langage $L(\mathcal{A}) = \emptyset$.

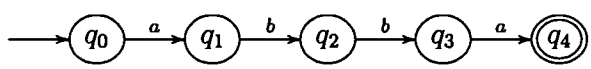
Exemple 2.2.2. Le mot vide ε est reconnu par un automate $\mathcal{A}$ dont un état initial est aussi état final :



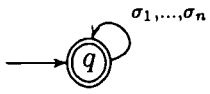
Exemple 2.2.3. Soit $w = \sigma_1 \dots \sigma_n \in \Sigma^*$ un mot. Le singleton $\{w\}$ est reconnu par l'automate $\mathcal{A}$ dont les transitions sont :

$$i \xrightarrow{\sigma_1} q_1 \xrightarrow{\sigma_2} \cdots \xrightarrow{\sigma_n} f$$

Soit $\Sigma = \{a, b\}$ et $w = abba$, nous avons l'automate $\mathcal{A}$ suivant :



Exemple 2.2.4. Soit un automate $\mathcal{A} = (\Sigma, \{q\}, \{q\}, \delta, \{q\})$ qui a un seul état à la fois initial et final et qui a une transition $q \xrightarrow{\sigma} q$ pour chaque $\sigma \in \Sigma$. Tous les chemins sont réussis, d'où $L(\mathcal{A}) = \Sigma^*$.



Proposition 2.2.4. *Tout langage fini est reconnaissable.*

Démonstration. Soit $L = \{a_1, a_2, \ldots, a_n\}$, un langage fini.
On a $L = \{a_1\} + \{a_2\} + \cdots + \{a_n\}$. D'après l'exemple 2.2.3 et la proposition 2.2.1, L est reconnaissable. □

2.3 Langages rationnels

Définition 2.3.1. Soit $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$ un alphabet. On appelle *expression rationnelle sur* Σ, une séquence de symboles formée en appliquant un nombre fini de fois les règles suivantes :

1. $\emptyset$, ε, $\sigma_1, \ldots, \sigma_n$ sont, chacune, des expressions rationnelles.
2. Si s et t sont des expressions rationnelles, alors $(s + t)$, (st) et s^* sont également des expressions rationnelles.

Les opérateurs $+$, $\cdot$ et $*$ sont appelés *opérateurs rationnels.*

Notation. Toute expression rationnelle s "décrit" un langage, noté $L(s)$, obtenu par les règles suivantes :

(i) $L(\emptyset) = \emptyset$.

(ii) $L(\varepsilon) = \varepsilon$.

(iii) $L(\sigma_i) = \sigma_i$.

(iv) $L(s + t) = L(s) + L(t)$.

(v) $L(s \cdot t) = L(s) \cdot L(t)$.

(vi) $L(s^*) = L(s)^*$.

Un langage L est *rationnel* s'il existe une expression rationnelle s telle que $L = L(s)$.

2.4 Théorème de Kleene

Nous pouvons maintenant énoncer le premier résultat (LAWSON, 2004).

Théorème 2.4.1. *(Kleene) Un langage est reconnaissable si et seulement s'il est rationnel.*

Démonstration. Montrons que $Rat(\Sigma^*) \subseteq Rec(\Sigma^*)$. Nous procédons par récurrence sur le nombre d'opérateurs rationnels dans l'expression rationnelle.
D'abord, les expressions rationnelles ne contenant aucun opérateur rationnel décrivent les langages $\emptyset$, ε et $\sigma, \sigma \in \Sigma$. Ces langages sont reconnaissables.
Hypothèse de récurrence : Soit r une expression rationnelle. Si r contient au plus $n-1$ opérateurs rationnels, alors $L(r)$ est reconnaissable.
Soit maintenant r une expression rationnelle contenant n opérateurs rationnels. On a $r = s + t$ ou $r = st$ ou bien $r = s^*$ avec s, t des expressions rationnelles contenant au plus $n-1$ opérateurs rationnels. Par hypothèse de récurrence, $L(s)$ et $L(t)$ sont reconnaissables et d'après les propositions 2.2.1, 2.2.2 et 2.2.3, il en résulte que $L(r)$ est reconnaissable, d'où $Rat(\Sigma^*) \subseteq Rec(\Sigma^*)$.
Réciproquement, montrons que $Rec(\Sigma^*) \subseteq Rat(\Sigma^*)$. Nous procéderons par récurrence sur le *nombre de transitions* de $\mathcal{A}$; c'est-à-dire le nombre d'arêtes dans l'automate $\mathcal{A}$.
Dans un premier temps, si le nombre de transitions de $\mathcal{A}$ est nul, alors $L(\mathcal{A}) = \emptyset$ ou $L(\mathcal{A}) = \varepsilon$.

Hypothèse de récurrence : Si le nombre de transitions de $\mathcal{A}$ est au plus égal à $n-1$, alors $L(\mathcal{A})$ est rationnel.

Soit maintenant $\mathcal{A} = (\Sigma, Q, I, \delta, F)$ un automate avec un nombre de transitions n. En considérant que $\mathcal{A}$ contient au moins une transition, nous construisons quatre autres automates en supprimant de $\mathcal{A}$ une transition, que nous notons $p \xrightarrow{a} q$, mais en gardant toutes les autres, tels que :

- $\mathcal{A}_1 = (\Sigma, Q, I, \delta \setminus p \xrightarrow{a} q, F)$;
- $\mathcal{A}_2 = (\Sigma, Q, I, \delta \setminus p \xrightarrow{a} q, \{p\})$;
- $\mathcal{A}_3 = (\Sigma, Q, \{q\}, \delta \setminus p \xrightarrow{a} q, \{p\})$;
- $\mathcal{A}_4 = (\Sigma, Q, \{p\}, \delta \setminus p \xrightarrow{a} q, F)$.

Le nombre de transitions de chacun de ces automates est $n-1$ (par construction), donc $L(\mathcal{A}_1)$, $L(\mathcal{A}_2)$, $L(\mathcal{A}_3)$ et $L(\mathcal{A}_4)$ sont rationnels d'après l'hypothèse de récurrence. Soit $L = L(\mathcal{A})$. Alors $x \in L$ si et seulement s'il existe un chemin réussi dans $\mathcal{A}$, ce qui équivaut à :

- soit ce chemin ne passe pas par la transition $p \xrightarrow{a} q$, dans ce cas $x \in L(\mathcal{A}_1)$,
- soit ce chemin passe par $p \xrightarrow{a} q$ et admet donc une factorisation

$$i \xrightarrow{u} p \xrightarrow{a} q \xrightarrow{v_1} p \xrightarrow{a} q \cdots q \xrightarrow{v_n} p \xrightarrow{a} q \xrightarrow{w} f$$

$i \in I$ et $f \in F$. On a ainsi $x \in (L(\mathcal{A}_2)a)(L(\mathcal{A}_3)a)^*(L(\mathcal{A}_4))$.

D'où L $= L(\mathcal{A}_1) + (L(\mathcal{A}_2)a)(L(\mathcal{A}_3)a)^*(L(\mathcal{A}_4))$ est rationnel. □

CHAPITRE III

MONOÏDE SYNTAXIQUE

Le but de ce chapitre est de définir le monoïde syntaxique d'un langage ainsi que la reconnaissabilité d'un langage par un monoïde. Pour ce faire, nous introduisons d'abord la notion d'automate minimal et de monoïde de transition. Les propositions et théorèmes énoncés dans ce chapitre interviennent directement dans la preuve du théorème de Schützenberger.

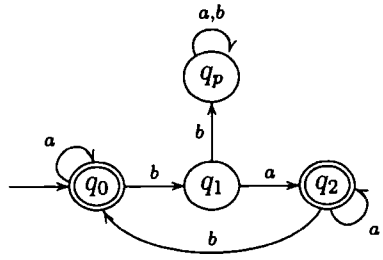
3.1 Automate minimal

3.1.1 Automate complet

Définition 3.1.1. Un automate $\mathcal{A} = (\Sigma, Q, I, \delta, F)$ est dit *complet* si pour tout $q \in Q$ et $\sigma \in \Sigma$ il y a exactement une arête $q \xrightarrow{\sigma} p$ dans $\mathcal{A}$; c'est-à-dire qu'une transition est toujours possible.

Exemple 3.1.1. Considérons l'automate de l'exemple 2.1.1 que nous rendons

"complet" sans modifier le langage qu'il reconnait :



3.1.2 Automate accessible et réduit

Définition 3.1.2. Un automate $\mathcal{A} = (\Sigma, Q, I, \delta, F)$ est dit *accessible* si pour tout état $q \in Q$ il existe un chemin $c : i \to q$ avec $i \in I$. Un état qui satisfait une telle condition est dit *accessible* et *inaccessible* sinon.

L'automate $\mathcal{A}^a = (\Sigma, Q^a, I, \delta^a, F^a)$ constitué de la *partie accessible* de $\mathcal{A}$ est définie comme suit :

1. Q^a est l'ensemble des états accessibles, obtenu en retirant de Q les états inaccessibles.
2. δ^a est obtenu en retirant les transitions qui commencent par, ou qui se terminent à des états inaccessibles.
3. $F^a = F \cap Q^a$.

Proposition 3.1.1. *Soit $\mathcal{A} = (\Sigma, Q, I, \delta, F)$ un automate fini, alors $L(\mathcal{A}^a) = L(\mathcal{A})$.*

Démonstration. Il est évident que $L(\mathcal{A}^a) \subseteq L(\mathcal{A})$.
Soit $x \in L(\mathcal{A})$, alors il existe une chemin $c : i \to f$, $i \in I, f \in F$ tel que $|c| = x$. Puisque tous les états de ce chemin sont accessibles, alors ce chemin appartient également à $\mathcal{A}^a$, d'où $L(\mathcal{A}) \subseteq L(\mathcal{A}^a)$. □

Définition 3.1.3. Soit $\mathcal{A} = (\Sigma, Q, i, \delta, F)$ un automate complet. On définit la relation d'équivalence (équivalence de Nérode), notée $\sim_{\mathcal{A}}$ (ou simplement $\sim$ lorsqu'il n'y a pas d'ambiguïté) par :

$$s \sim t \Leftrightarrow \{u \mid su \in F\} = \{u \mid tu \in F\}$$

avec $s, t \in Q$ et $u \in \Sigma^*$.

Si cette relation d'équivalence est l'égalité, on dit que l'automate $\mathcal{A}$ est *réduit.* Alors $\mathcal{A}$ est réduit si :

$$\forall s, t \in Q, \{u \mid su \in F\} = \{u \mid tu \in F\} \Leftrightarrow s = t.$$

Proposition 3.1.2. *Soit $\mathcal{A} = (\Sigma, Q, i, \delta, F)$ un automate complet. On définit un automate quotient $\mathcal{A}/\sim$ qui est réduit et tel que $L(\mathcal{A}^r) = L(\mathcal{A})$. L'automate $\mathcal{A}/\sim$ est noté A^r et appelé* automate réduit *de $\mathcal{A}$.*

Démonstration. Soit $q \in Q$ un état de l'automate $\mathcal{A}$. Notons $[q]$ la classe d'équivalence de q et $[F] = \{[f] : f \in F\}$.
Définissons un automate $\mathcal{A}^r = (\Sigma, [Q], [i], \delta_\sim, [F])$ avec $\delta_\sim$ définie par $[q]\cdot\sigma = [q\cdot\sigma]$, pour tout $q \in Q, \sigma \in \Sigma$. La fonction de transition $\delta_\sim$ est bien définie ; c'est-à-dire si $[q] = [q']$ et $\sigma \in \Sigma$, alors $[q \cdot \sigma] = [q' \cdot \sigma]$. En effet, soit $w \in \Sigma^*$, alors on a $(q \cdot \sigma) \cdot w \in F$ quand $q \cdot (\sigma \cdot w) \in F$. Puisque $q \sim q'$,

$$q \cdot (\sigma w) \in F \Leftrightarrow q' \cdot (\sigma w) \in F.$$

Donc on a $(q \cdot \sigma) \cdot w \in F$ quand $(q' \cdot \sigma) \cdot w \in F$ ce qui implique $q \cdot \sigma \sim q' \cdot \sigma$. D'où $[q \cdot \sigma] = [q' \cdot \sigma]$ et ainsi $\delta_\sim$ est bien définie.
Soit maintenant $[q] \sim [q']$ dans $\mathcal{A}^r$, $[q], [q'] \in [Q]$. On a $[q] \cdot w \in [F] \Leftrightarrow [q'] \cdot w \in [F]$ pour chaque $w \in \Sigma^*$, donc $[q \cdot w] \in [F] \Leftrightarrow [q' \cdot w] \in [F]$. Or, un état $[q]$ est final dans $\mathcal{A}^r$ si q est final dans $\mathcal{A}$. Il s'ensuit que

$$q \cdot w \in F \Leftrightarrow q' \cdot w \in F.$$

D'où $[q] = [q']$ et $\mathcal{A}^r$ est réduit.

Soit $x \in L(\mathcal{A})$, alors $i \cdot x \in F$. Ce qui équivaut, par définition, à $[i \cdot x] \in [F]$, puis $[i] \cdot x \in [F]$. D'où $L(\mathcal{A}) = L(\mathcal{A}^r)$. □

3.1.3 Isomorphisme d'automates

Définition 3.1.4. Soit $\mathcal{A}_1 = (\Sigma, Q_1, i_1, \delta_1, F_1)$ et $\mathcal{A}_2 = (\Sigma, Q_2, i_2, \delta_2, F_2)$ deux automates. Un *isomorphisme d'automates*

$$\varphi : \mathcal{A}_1 \to \mathcal{A}_2$$

est une fonction $\varphi : Q_1 \to Q_2$ vérifiant :

(i) φ est bijective.

(ii) $\varphi(i_1) = i_2$

(iii) $f_1 \in F_1 \Leftrightarrow \varphi(f_1) \in F_2$

(iv) $\varphi(q_1 \cdot \sigma) = \varphi(q_1) \cdot \sigma$ pour tout $q_1 \in Q_1$ et $\sigma \in \Sigma$

Proposition 3.1.3. *Soit $\mathcal{A}_1 = (\Sigma, Q_1, i_1, \delta_1, F_1)$ et $\mathcal{A}_2 = (\Sigma, Q_2, i_2, \delta_2, F_2)$ deux automates accessibles réduits reconnaissant L, alors A_1 et A_2 sont isomorphes.*

Démonstration. Soit $q_1 \in Q_1$, puisque $\mathcal{A}_1$ est accessible alors il existe $x \in \Sigma^*$ tel que $q_1 = i_1 \cdot x$. Définissons

$$\varphi(q_1) = i_2 \cdot x$$

– Démontrons que φ est bien définie et injective ; c'est-à-dire

$$q_1 = q_1' \Leftrightarrow \varphi(q_1) = \varphi(q_1')$$

avec $q_1 = i_1 \cdot x$ et $q_1' = i_1 \cdot y$.

On a :

$$q_1 \sim q_1' \Leftrightarrow \{u \mid (i_1 \cdot x)u \in F_1\} = \{u \mid (i_1 \cdot y)u \in F_1\}$$

qui équivaut à

$$\{u \mid i_1 \cdot (xu) \in F_1\} = \{u \mid i_1 \cdot (yu) \in F_1\}$$

puis à

$$\{u \mid i_2 \cdot (xu) \in F_2\} = \{u \mid i_2 \cdot (yu) \in F_2\}$$

car $\mathcal{A}_1$ et $\mathcal{A}_2$ reconnaissent le même langage. D'où $i_2 \cdot x \sim i_2 \cdot y$.

Puisque $\mathcal{A}_1$ et $\mathcal{A}_2$ sont réduits, il s'ensuit que :

$$\varphi(q_1) = \varphi(q_1') \Leftrightarrow q_1 = q_1'$$

donc φ est bien définie et injective.

De plus, soit $q_2 \in Q_2$, alors il existe $x \in \Sigma^*$ tel que $q_2 = i_2 \cdot x$ car $\mathcal{A}_2$ est accessible. Par définition de φ, on a toujours $\varphi(q_1) = q_2$ avec $q_1 = i_1 \cdot x$. D'où φ est surjective.

Nous venons ainsi de montrer la bijectivité de φ.

- $i_1 = i_1 \cdot \varepsilon$ donc $\varphi(i_1) = i_2 \cdot \varepsilon = i_2$
- Soit $f_1 \in F_1$. Vu que $\mathcal{A}_1$ est accessible, il existe $x \in \Sigma^*$ tel que $f_1 = i_1 \cdot x$. Or puisque $L(\mathcal{A}_1) = L(\mathcal{A}_2)$,

$$i_1 \cdot x \in F_1 \Leftrightarrow i_2 \cdot x \in F_2$$

ce qui équivaut à $\varphi(f_1) \in F_2$. Donc

$$f_1 \in F_1 \Leftrightarrow \varphi(f_1) \in F_2$$

- Pour tout $q_1 \in Q_1$ et $\sigma \in \Sigma$, on a

$$\varphi(q_1) \cdot \sigma = (i_2 \cdot x) \cdot \sigma = i_2 \cdot (x \cdot \sigma)$$

avec $q_1 = i_1 \cdot x$ pour un certain $x \in \Sigma^*$.

Par ailleurs

$$\varphi(q_1 \cdot \sigma) = \varphi((i_1 \cdot x) \cdot \sigma) = \varphi(i_1 \cdot (x \cdot \sigma)) = i_2 \cdot (x \cdot \sigma)$$

d'où $\varphi(q_1) \cdot \sigma = \varphi(q_1 \cdot \sigma)$. □

Revenons à la notion de minimalité d'un automate.
Un automate complet $\mathcal{A}$ est dit *minimal* (pour un langage L) si $L(\mathcal{A}) = L$ et si $\mathcal{A}'$ est un automate complet reconnaissant L, alors le nombre d'états de $\mathcal{A}$ est inférieur ou égal au nombre d'états de $\mathcal{A}'$.

Théorème 3.1.4. *Un automate complet $\mathcal{A} = (\Sigma, Q, i, \delta, F)$ reconnaissant L est minimal si et seulement s'il est accessible et réduit.*

Démonstration. Soit $\mathcal{A}$ un automate minimal pour L. Supposons $\mathcal{A}$ non accessible (resp. non réduit), alors $\mathcal{A}^a$ (resp. $\mathcal{A}^r$) a moins d'états que $\mathcal{A}$ et $L(\mathcal{A}^a) = L$ (resp. $L(\mathcal{A}^r) = L$). Ceci contredit la minimalité de $\mathcal{A}$ et donc $\mathcal{A}$ est accessible (resp. réduit).
Soit $\mathcal{A}$ un automate accessible et réduit tel que $L(\mathcal{A}) = L$. Soit $\mathcal{A}' = (\Sigma, Q', i', \delta', F')$ un automate quelconque reconnaissant L. On a $L(\mathcal{A}'^{ar}) = L$ et $\mid Q'^{ar} \mid \leq \mid Q' \mid$. D'après la proposition 3.1.3, $\mathcal{A}$ et $\mathcal{A}'^{ar}$ sont isomorphes donc $\mid Q \mid \leq \mid Q' \mid$; d'où $\mathcal{A}$ est minimal. □

Corollaire 3.1.5. *Il existe un* unique *automate minimal à isomorphisme près reconnaissant L.*

3.1.4 Automate minimal : méthode des quotients

Définition 3.1.5. Soit L un langage sur Σ et $u \in \Sigma^*$. On appelle *quotient à gauche (ou* résiduel à gauche*) de L par u*, le langage

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

De manière analogue, on définit le *quotient à droite de L par u* comme étant

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

Notation. Par défaut, nous désignons par quotient, le quotient à gauche.

Proposition 3.1.6. *(Opérations sur les quotients) Soit $u, v \in \Sigma^*$ et $\sigma \in \Sigma$.*

(i) *Si $L = \emptyset$ ou $L = \varepsilon$ alors $u^{-1}(LM) = L(u^{-1}M)$;*

(ii) $u^{-1}(L + M) = u^{-1}L + u^{-1}M$;

(iii) $\sigma^{-1}(LM) = \begin{cases} (\sigma^{-1}L)M & Si\ \varepsilon \notin L; \\ (\sigma^{-1}L)M + (\sigma^{-1}M) & Si\ \varepsilon \in L; \end{cases}$

(iv) $\sigma^{-1}L^* = (\sigma^{-1}L)L^*$;

(v) $(uv)^{-1}L = v^{-1}(u^{-1}L)$.

Démonstration. (i) Évident.

(ii) $v \in u^{-1}(L+M) \Leftrightarrow uv \in (L+M) \Leftrightarrow (uv \in L)$ ou $(uv \in M) \Leftrightarrow v \in u^{-1}L$ ou $v \in u^{-1}M$ d'où $v \in u^{-1}L + u^{-1}M$.

(iii) D'une part $\varepsilon \notin L \Leftrightarrow l = \sigma l'$, pour $l \in L$, un certain $\sigma \in \Sigma$ et un certain $l' \in \Sigma^*$.

Or $\sigma l' \in L \Leftrightarrow l' \in \sigma^{-1}L$.

De plus $x \in \sigma^{-1}(LM) \Leftrightarrow \sigma x \in (LM)$ équivaut à $\sigma x = lm$ avec $l \in L$ et $m \in M$. puis à $\sigma x = \sigma l' m$ où $x = l'm \Leftrightarrow x \in (\sigma^{-1}L)M$.

D'autre part si $\varepsilon \in L$ alors $L = \varepsilon + L'$ avec $L' = L \setminus \varepsilon$ alors

$$\sigma^{-1}(LM) = \sigma^{-1}(M + L'M) = (\sigma^{-1}M) + (\sigma^{-1}L')M.$$

(iv) $x \in \sigma^{-1}L^* \Leftrightarrow \sigma x \in L^*$ ssi $\sigma x = u_1 u_2 \dots u_n$ avec $u_i \in L$ et u_i non vide.

En posant $u_1 = \sigma u$ pour un certain u, on a $u \in \sigma^{-1}L$.

$$\sigma x = u_1 u_2 \dots u_n \Leftrightarrow x = u(u_2 \dots u_n)$$

D'où $x \in (\sigma^{-1}L)L^*$.

(v) $x \in (uv)^{-1}L \Leftrightarrow (uv)x \in L$

Si et seulement si $u(vx) \in L \Leftrightarrow vx \in u^{-1}L$

Si et seulement si $x \in v^{-1}(u^{-1}L)$. □

Soit L un langage qui admet un nombre fini de quotients. Construisons l'automate $\mathcal{A}_L = (\Sigma, Q, i, \delta, F)$ avec :

- $Q = \{u^{-1}L \mid u \in L^*\}$ qui est fini.
- $i = \varepsilon^{-1}L = L$
- $F = \{u^{-1}L \mid \varepsilon \in u^{-1}\}$, l'ensemble des quotients contenant ε
- $\delta(u^{-1}L, \sigma) = \sigma^{-1}(u^{-1}L) = (u\sigma)^{-1}L$

Théorème 3.1.7. *Un langage est reconnaissable si et seulement s'il admet un nombre fini de quotients distincts.*

Démonstration. Soit L un langage reconnaissable par un automate $\mathcal{A} = (\Sigma, Q, i, \delta, F)$. L'ensemble des quotients de L est $\{L(\mathcal{A}_q), q \in Q)\}$ avec $\mathcal{A}_q = (\Sigma, Q, q, \delta, F)$ et il faut se restreindre aux q accessibles : il y en a un nombre fini.
Réciproquement, soit $w = w_1 w_2 \dots w_n$ un mot. Alors $w \in L(\mathcal{A}_L)$ si et seulement s'il existe un chemin dans $\mathcal{A}_L$ tel que

$$L \xrightarrow{w_1} w_1^{-1}L \xrightarrow{w_2} (w_1 w_2)^{-1}L \xrightarrow{w_3} \cdots \xrightarrow{w_n} (w_1 w_2 \dots w_n)^{-1}L = w^{-1}L.$$

Par définition de F celà équivaut à $\varepsilon \in w^{-1}L \Leftrightarrow w \in L$. D'où $L = L(\mathcal{A}_L)$. □

Nous venons de construire, dans la preuve du théorème 3.1.7, un automate $\mathcal{A}_L = (\Sigma, Q, i, \delta, F)$ tel que :

- $Q = \{u^{-1}L \mid u \in L^*\}$;
- $i = \varepsilon^{-1}L = L$;
- $F = \{u^{-1}L \mid \varepsilon \in u^{-1}\}$;
- $\delta(u^{-1}L, \sigma) = \sigma^{-1}(u^{-1}L) = (u\sigma)^{-1}L$.

Ce qui nous permet d'énoncer

Théorème 3.1.8. *Soit L un langage reconnaissable, alors $\mathcal{A}_L$ est l'automate minimal de L.*

Démonstration. $\mathcal{A}_L$ est complet par construction.

Soit $u^{-1}L$ un état de $\mathcal{A}_L$. Il existe toujours un chemin

$$L \xrightarrow{u_1} u_1^{-1}L \xrightarrow{u_2} (u_1u_2)^{-1}L \xrightarrow{u_3} \cdots \xrightarrow{u_n} (u_1u_2\ldots u_n)^{-1}L$$

avec $u = u_1u_2\ldots u_n$. Donc $\mathcal{A}_L$ est accessible.

Montrons que $\delta(u^{-1}L, x) = (ux)^{-1}L$, $u, x \in \Sigma^*$.

Soit $x = x_1x_2\ldots x_n$, on a

$$u^{-1}L \xrightarrow{x_1} (ux_1)^{-1}L \xrightarrow{x_2} (ux_1x_2)^{-1}L \xrightarrow{x_3} \cdots \xrightarrow{x_n} (ux_1x_2\ldots x_n)^{-1}L$$

donc $\delta(u^{-1}L, x) = (ux)^{-1}L$.

Soit maintenant $u^{-1}L \sim v^{-1}L \Leftrightarrow \{x \mid (u^{-1}L)\cdot x \in F\} = \{x \mid (v^{-1}L)\cdot x \in F\}$ pour $x \in \Sigma^*$

Celà équivaut à

$$\{x \mid \varepsilon \in (ux)^{-1}L)\} = \{x \mid \varepsilon \in (vx)^{-1}L)\} \Leftrightarrow \{x \mid x \in u^{-1}L)\} = \{x \mid x \in v^{-1}L)\}$$

D'où $u^{-1}L = v^{-1}L$ $\mathcal{A}_L$; $\mathcal{A}_L$ est réduit.

D'après le théorème 3.1.4, $\mathcal{A}_L$ est minimal. □

3.2 Monoïde syntaxique

Définition 3.2.1. Soit $\mathcal{A} = (\Sigma, Q, i, \delta, F)$ un automate fini.

À tout mot $w \in \Sigma^*$, on associe une application :

$$f_w : Q \to Q$$
$$q \mapsto \delta(q, w)$$

Le monoïde engendré par toutes les applications $f_w, w \in \Sigma^*$ est appelé : le *monoïde de transition*, noté $M(\mathcal{A})$, de l'automate $\mathcal{A}$.

En effet, prouvons que $f_u f_v = f_{uv}$ en utilisant la notation à gauche ; c'est-à-dire nous écrivons qf_u au lieu de $f_u(q)$. La démonstration se fait par récurrence sur la longueur de u.
L'assertion est vérifiée si $u = \varepsilon$. Supposons qu'elle est vraie si u est de longueur infieure ou égale à n. Soit u de longueur $n+1$. Alors $u = \sigma u'$ avec $\sigma \in \Sigma$ et u' de longueur n. On a

$$f_u f_v = f_{\sigma u'} f_v = f_\sigma f_{u'} f_v = f_\sigma f_{u'v} = f_{\sigma u'v} = f_{uv}$$

car d'après l'hypothèse de récurrence, on a successivement $f_\sigma f_{u'} = f_{\sigma u'}$, puis $f_{u'} f_v = f_{u'v}$ et enfin $f_\sigma f_{u'v} = f_{\sigma u'v}$.

Le monoïde $M(\mathcal{A})$ est engendré par les applications $q \to \delta(q, \sigma)$ des lettres $\sigma \in \Sigma$ et on a un morphisme canonique $\alpha : \Sigma^* \to M(\mathcal{A})$.

Définition 3.2.2. Soit $L \subseteq \Sigma^*$ un langage. On appelle *congruence syntaxique* de L, la congruence $\equiv_L$ définie sur Σ^* par

$$u \equiv_L v \Leftrightarrow (\forall x, y \in \Sigma^*, xuy \in L \Leftrightarrow xvy \in L).$$

Le *monoïde syntaxique* de L est le monoïde quotient $M(L) = \Sigma^* / \equiv_L$

Théorème 3.2.1. *Soit L un langage reconnaissable, alors le monoïde syntaxique de L est égal au monoïde de transition de l'automate minimal de L.*

Démonstration. Soit $s, t \in \Sigma^*$. On a

$$(us)^{-1}L = (ut)^{-1}L, \forall u \in \Sigma^*;$$

ce qui équivaut, par définition de $(us)^{-1}L$, à

$$usv \in L \Leftrightarrow utv \in L, \forall u, v \in \Sigma^*;$$

c'est-à-dire deux mots sont syntaxiquement équivalents si et seulement s'ils ont la même action sur les états $q, q \in Q$, de l'automate minimal $\mathcal{A}_L$ de L. □

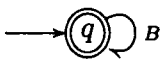
Théorème 3.2.2. *Un langage L est reconnaissable si et seulement si son monoïde syntaxique est fini.*

Démonstration. Soit $\mathcal{A}_L = (\Sigma, Q, i, \delta, F)$ l'automate minimal de L avec Q fini. Donc, le nombre d'applications de Q dans Q est aussi fini (au plus $n^n, |Q| = n$), d'où $M(L)$ est fini.
Inversement, supposons $M(L)$ fini. Définissons l'automate

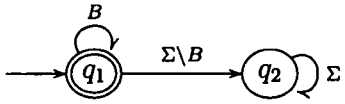
$$\mathcal{A} = (\Sigma, M(L), [\varepsilon], \delta, \{[x] \mid x \in L\})$$

tel que $\delta([x], \sigma) = [x\sigma]$. On a $w \in L(\mathcal{A})$ ssi $[\varepsilon] \cdot w \in L \Leftrightarrow [w] \in L$. Puisque $[w] \in L \Leftrightarrow w \in L$ alors $L(\mathcal{A}) = L$. □

Exemple 3.2.1. Soit $L = B^*$ un langage avec $B \subseteq \Sigma$. Si $B = \Sigma$ alors l'automate suivant est complet et minimal :

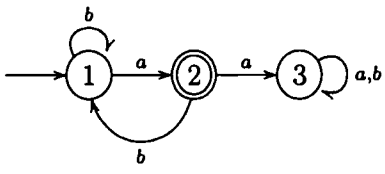


Nous avons $M(L) = \varepsilon$. Si $B \neq \Sigma$ alors nous aurions :

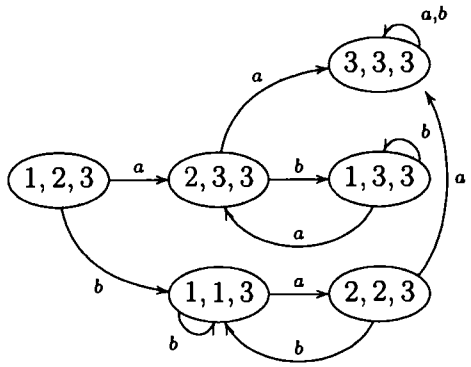


Nous avons dans ce cas tous les éléments de B en relation avec l'identité ε et ceux de $\Sigma \setminus B$ en relation avec la transformation vide (nous la noterons 0) avec $00 = 0$. $M(L)$ contient donc deux (2) éléments : $M(L) = \{\varepsilon, 0\}$.

Exemple 3.2.2. Soit $\Sigma = \{a, b\}$ un alphabet et $L = \Sigma^* \setminus \Sigma^* aa\Sigma^*$ (les mots ne contenant pas aa). Nous avons $\mathcal{A}_L$, l'automate minimal de L ci-dessous :



Les applications du monoïde de transition $M(\mathcal{A}_L)$ sont données par le graphe suivant :



Chaque entrée du graphe représente la liste des états de l'automate ($\mathcal{A}_L$ dans notre exemple). Pour chaque entrée nous appliquons toutes les lettres de l'alphabet. Une lettre $\sigma \in \Sigma$ fait passer l'entrée $(q_1, \ldots, q_n)$ à l'entrée $(\delta(q_1, \sigma), \ldots, \delta(q_n, \sigma))$. Autrement dit i, j, k représente la fonction $\begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix}$.

Les applications de $M(\mathcal{A}_L)$ sont données par les combinaisons distinctes de mots qui permettent d'atteindre toutes les entrées du graphe. Dans le cas présent toutes les entrées sont atteintes par les mots : a, b, a^2, ab, ba. Nous avons donc $M(\mathcal{A}_L) = \{f_\varepsilon, f_a, f_b, f_{a^2}, f_{ab}, f_{ba}\}$. Puisque le monoïde de transitions $M(\mathcal{A}_L)$ est isomorphe au monoïde syntaxique $M(L)$, on en déduit que $M(L) = \{\varepsilon, a, b, a^2, ab, ba\}$.

3.3 Reconnaissabilité par un monoïde

Définition 3.3.1. Soit $L \subseteq \Sigma^*$ un langage, M un monoïde et $\varphi : \Sigma^* \to M$ un morphisme de monoïdes. On dit que φ *reconnaît* L s'il existe $P \subseteq M$ telle que $L = \varphi^{-1}(P)$. On dira généralement que le monoïde M *reconnaît* L.

Définition 3.3.2. Un langage est dit *reconnaissable* (par un monoïde) s'il est reconnu par un monoïde fini.

Proposition 3.3.1. *Un langage $L \subseteq \Sigma^*$ est reconnaissable par un automate si et seulement s'il est reconnaissable par un monoïde.*

Démonstration. Soit un automate $\mathcal{A} = (\Sigma, Q, i, \delta, F)$ tel que $L(\mathcal{A}) = L$. Notons $\varphi : \Sigma^* \to M(\mathcal{A})$ le morphisme canonique et posons $P = \varphi(L)$. D'une part, nous avons clairement $L \subseteq \varphi^{-1}(P)$. D'autre part, soit $u \in \varphi^{-1}(P)$, alors par définition, $\varphi(u) \in P = \varphi(L)$. Donc il existe un certain $v \in L$ tel que $\varphi(u) = \varphi(v)$; autrement dit u et v définissent la même application de Q dans Q. Or $v \in L = L(\mathcal{A})$ donc $u \in L(\mathcal{A}) = L$ car u et v ont un même effet sur les états de $\mathcal{A}$.
Réciproquement, soit L reconnaissable par un monoïde fini M. Alors il existe un morphisme $\varphi : \Sigma^* \to M$ et $P \subseteq M$ telle que $L = \varphi^{-1}P$. Définissons l'automate $\mathcal{A} = (\Sigma, M, \varepsilon, \delta, P)$, avec δ défini de manière à ce que pour $m \in M$ et $w \in \Sigma^*$, on ait $m \cdot w = m(\varphi(w))$. Alors

$$L(\mathcal{A}) = \{w \mid \varepsilon \cdot w \in P\} = \{w \mid \varepsilon(\varphi(w)) \in P\} = \{w \mid \varphi(w) \in P\} = \varphi^{-1}P = L.$$

□

Définition 3.3.3. Soit S et T deux monoïdes. On dit que S *divise* T (notation $S < T$) si S est *quotient* d'un sous-monoïde de T.
On dit que S est un *quotient* de T' s'il existe un morphisme surjectif $\varphi : T' \to S$.

Proposition 3.3.2. *Soit $\alpha : \Sigma^* \to S$ un morphisme de monoïdes et $\beta : T \to S$ un morphisme surjectif. Alors il existe un morphisme $\gamma : \Sigma^* \to S$ tel que $\alpha = \beta \circ \gamma$.*

Démonstration. Puisque β est surjective, alors pour $s \in S$, $\beta^{-1}(s)$ est non-vide. Associons pour chaque lettre $\sigma \in \Sigma$ un élément de $\beta^{-1}(\alpha(\sigma))$. L'application, notons $\gamma\prime : \Sigma \to T$, ainsi définie se prolonge en un morphisme $\gamma : \Sigma^+ \to S$ avec pour $w = w_1 w_2 \dots w_n \in \Sigma^+$

$$\gamma(w) = \gamma\prime(w_1)\gamma\prime(w_2)\dots\gamma\prime(w_n).$$

□

Proposition 3.3.3. *Soit $L \subseteq \Sigma^*$ un langage. Un monoïde M reconnaît L si et seulement si $M(L)$ divise M.*

Démonstration. Supposons que M reconnaît L. Alors il existe un morphisme $\varphi : \Sigma^* \to M$ et $P \subseteq M$ telle que $L = \varphi^{-1}(P)$. Montrons que $M(L)$ reconnaît L. Soit le morphisme canonique $\eta : \Sigma^* \to M(L)$. On a $L \subseteq \eta^{-1}(\eta(L))$. Soit $w \in \eta^{-1}(\eta(L))$, alors $\eta(w) \in \eta(L)$; c'est-à-dire il existe $v \in L$ tel que $\eta(w) = \eta(v)$; autrement dit $w \equiv_L v$. D'où $w \in L$ et $L = \eta^{-1}(\eta(L))$; ce qui entraine $L = \eta^{-1}(\eta(\varphi^{-1}(P)))$. Dans ces conditions, l'application $\eta \circ \varphi^{-1}$ définie de P dans $M(L)$ est surjective donc $M(L)$ divise M.
Supposons que $M(L)$ divise M, alors il existe un monoïde $M' \subseteq M$ et des morphismes $\alpha : M' \to M$ injectif et $\beta : M' \to M(L)$ surjectif. Notons $\eta : \Sigma^* \to M(L)$ le morphisme canonique. D'après la proposition 3.3.2, il existe un morphisme $\gamma : \Sigma^* \to M'$ tel que $\eta = \beta\gamma$. Posons $P = \alpha\beta^{-1}\eta(L) \subseteq M$. On a

$$(\alpha\gamma)^{-1}(P) = \gamma^{-1}\alpha^{-1}\alpha\beta^{-1}\eta(L) = \gamma^{-1}\beta^{-1}\eta(L) = \eta^{-1}\eta(L) = L;$$

donc M reconnaît L. □

Proposition 3.3.4. *Soit $L \subseteq \Sigma^*$ un langage. Si M reconnaît L, alors M reconnaît $\overline{L} = \Sigma^* \setminus L$.*

Démonstration. Soit $\varphi : \Sigma^* \to M$ et $P \subseteq M$ tels que $L = \varphi^{-1}(P)$. Alors $\overline{L} = \varphi^{-1}(M \setminus P)$. □

Proposition 3.3.5. *Soit $L_1, L_2 \subseteq \Sigma^*$ deux langages. Si M_1 et M_2 sont des monoïdes qui reconnaissent respectivement L_1 et L_2, alors $M_1 \times M_2$ reconnaît $L_1 \cap L_2$ et $L_1 \cup L_2$.*

Démonstration. Soit $\varphi_1 : \Sigma^* \to M_1$, $P_1 \subseteq M_1$ et $\varphi_2 : \Sigma^* \to M_2$, $P_2 \subseteq M_2$ tels que $L_1 = \varphi_1^{-1}(P_1)$ et $L_2 = \varphi_2^{-1}(P_2)$.
Soit le morphisme $\varphi : \Sigma^* \to M_1 \times M_2$ défini par $\varphi(x) = (\varphi_1(x), \varphi_2(x))$. On a alors

$$L_1 \cap L_2 = \varphi^{-1}(P_1 \times P_2)$$

et

$$L_1 \cup L_2 = \varphi^{-1}((P_1 \times M_2) \cup (M_1 \times P_2)).$$

□

3.3.1 Produit de Schützenberger

Soit M et N deux monoïdes et $X \subseteq M \times N$. Pour $m \in M$ et $n \in N$, on définit $mX = \{(mx, y) \mid (x, y) \in X\}$ et $Xn = \{(x, yn) \mid (x, y) \in X\}$. Soit R la famille de tous les ensembles de couples $(m, n) \in M \times N$. Notons $M \diamond N$ le produit des ensembles $M \times R \times N$ et définissons un produit sur $M \diamond N$ par : pour tout $(m_1, X_1, n_1), (m_2, X_2, n_2) \in M \diamond N$:

$$(m_1, X_1, n_1)(m_2, X_2, n_2) = (m_1 m_2, m_1 X_2 \cup X_1 n_2, n_1 n_2).$$

Représentons les éléments (m, X, n) de $M \diamond N$ par des matrices 2×2 et leur produit de la manière suivante :

$$\begin{pmatrix} m_1 & X_1 \\ \emptyset & n_1 \end{pmatrix} \begin{pmatrix} m_2 & X_2 \\ \emptyset & n_2 \end{pmatrix} = \begin{pmatrix} m_1 m_2 & m_1 X_2 \cup X_1 n_2 \\ \emptyset & n_1 n_2 \end{pmatrix}$$

On vérifie aisément que le produit sur $M \diamond N$ ainsi défini est *associatif*. De plus, on a :

$$\begin{pmatrix} e_m & \emptyset \\ \emptyset & e_n \end{pmatrix} \begin{pmatrix} m & X \\ \emptyset & n \end{pmatrix} = \begin{pmatrix} e_m m & e_m X \\ \emptyset & e_n n \end{pmatrix} = \begin{pmatrix} m & X \\ \emptyset & n \end{pmatrix}$$

et

$$\begin{pmatrix} m & X \\ \emptyset & n \end{pmatrix} \begin{pmatrix} e_m & \emptyset \\ \emptyset & e_n \end{pmatrix} = \begin{pmatrix} m e_m & X e_n \\ \emptyset & n e_n \end{pmatrix} = \begin{pmatrix} m & X \\ \emptyset & n \end{pmatrix}$$

Nous venons de montrer que le produit ainsi défini sur $M \diamond N$ est associatif avec pour élément neutre $(e_m, \emptyset, e_n)$.

Définition 3.3.4. Le monoïde $M \diamond N$ est appelé le *produit de Schützenberger de* M *et* N.

Proposition 3.3.6. *Soit* $L_1, L_2 \subseteq \Sigma^*$ *deux langages. Si* M_1 *et* M_2 *sont des monoïdes qui reconnaissent respectivement* L_1 *et* L_2, *alors* $L_1 L_2$ *est reconnu par* $M_1 \diamond M_2$.

Démonstration. Soit $\varphi_1 : \Sigma^* \to M_1$, $P_1 \subseteq M_1$ et $\varphi_2 : \Sigma^* \to M_2$, $P_2 \subseteq M_2$ tels que $L_1 = \varphi_1^{-1}(P_1)$ et $L_2 = \varphi_2^{-1}(P_2)$. Définissons un homomorphisme de monoïdes $\varphi : \Sigma^* \to M \subseteq M_1 \diamond M_2$ tel que pour tout $x \in \Sigma^*$

$$\varphi(x) = (\varphi_1(x), X(x), \varphi_2(x))$$

avec

$$X(x) = \{(\varphi_1(x'), \varphi_2(x'')) \mid x', x'' \in \Sigma^*; x'x'' = x\}.$$

Montrons d'abord que φ est un homomorphisme. Il suffira de montrer que : pour tout $x, y \in \Sigma^*$

$$X(xy) = \varphi_1(x)X(y) + X(x)\varphi_2(y).$$

On a

$$X(xy) = \{(\varphi_1(x'), \varphi_2(x'')) \mid x', x'' \in \Sigma^*; x'x'' = xy\}$$

qui est égal à

$$\{(\varphi_1(x'), \varphi_2(x''y)) \mid x', x'' \in \Sigma^*; x'x'' = x\} + \{(\varphi_1(xy'), \varphi_2(y'')) \mid y', y'' \in \Sigma^*; y'y'' = y\}$$

soit

$$\{(\varphi_1(x'), \varphi_2(x'')\varphi_2(y)) \mid x', x'' \in \Sigma^*; x'x'' = x\} + \{(\varphi_1(x)\varphi_1(y'), \varphi_2(y'')) \mid y', y'' \in \Sigma^*; y'y'' = y\}$$

et donc

$$X(xy) = X(x)\varphi_2(y) + \varphi_1(x)X(y) = \varphi_1(x)X(y) + X(x)\varphi_2(y)$$

ce qui prouve que φ est un homomorphisme.

Montrons maintenant qu'il existe $P \subseteq M$ tel que $L_1L_2 = \varphi^{-1}(P)$. Soit $P = \varphi(L_1L_2)$, alors $L_1L_2 \subseteq \varphi^{-1}(P)$.
Soit $x \in \varphi^{-1}(P)$ alors $\varphi(x) \in P = \varphi(L_1L_2)$, c'est-à-dire il existe $l_1 \in L_1$ et $l_2 \in L_2$ tels que

$$\varphi(x) = \varphi(l_1l_2) = (\varphi_1(l_1l_2), X(l_1l_2), \varphi_2(l_1l_2)).$$

Or $(\varphi(l_1), \varphi(l_2)) \in X(l_1l_2)$ et $X(l_1l_2) = X(x)$ donc $x = x'x''$ avec $\varphi(x') = \varphi_1(l_1) \in P_1$ et $\varphi(x'') = \varphi_2(l_2) \in P_2$. D'où $x' \in L_1$ et $x'' \in L_2$ et alors $x \in L_1L_2$.
Puisque M est un sous-monoïde de $M_1 \diamond M_2$ et que M reconnaît L_1L_2, $M_1 \diamond M_2$ reconnaît L_1L_2. □

CHAPITRE IV

LANGAGES SANS-ÉTOILE ET THÉORÈME DE SCHÜTZENBERGER

Le but de ce chapitre est d'exposer la preuve du théorème de Schützenberger qui caractérise les langages apériodiques. Dans ce chapitre Σ désigne toujours un alphabet fini.

4.1 Monoïdes apériodiques

Proposition 4.1.1. *Soit M un monoïde engendré par un élément a. Si M est fini, alors il existe des entiers $n \geq 0$ et $p > 0$ tels que $a^n = a^{n+p}$ et $M = \{a, a^2, \ldots, a^{n+p-1}\}$. De plus M contient un unique idempotent qui est l'élément neutre du groupe cyclique $G = \{a^n, a^{n+1}, \ldots, a^{n+p-1}\}$ d'ordre p dans M .*

Démonstration. Puisque M est fini, il existe une puissance de a qui se répète. Soit n, le plus petit entier positif tel qu'il existe k vérifiant $a^n = a^{n+k}$ et notons p le plus petit tel k. Par construction les éléments $a, a^2, \ldots, a^{n+p-1}$ sont distincts. Par ailleurs, si $m > p$, on a $m = qp + r$ où $q \geq 0$ et $0 \leq r < p$ alors

$$a^{n+m} = a^{n+qp+r} = a^{n+r}$$

Il s'ensuit que $S = \{a, a^2, \ldots, a^{n+p-1}\}$. Soit $G = \{a^n, a^{n+1}, \ldots, a^{n+p-1}\}$ et $\gamma : G \to \mathbb{Z}/p\mathbb{Z}$ définie par $\gamma(a^{n+i} = n+i(\mod p))$. L'application γ est un isomorphisme de

G sur $\mathbb{Z}/p\mathbb{Z}$ et donc G contient un seul idempotent. Puisque que tout élément de M a une puissance dans G, alors M contient également un unique idempotent. □

Le nombre n est appelé *index* de a et p est appelé *période* de a.

Définition 4.1.1. Un monoïde M est dit *apériodique* si pour tout $x \in M$, il existe un entier n tel que $x^n = x^{n+1}$.

Nous rappelons qu'un *groupe trivial* est un groupe contenant uniquement l'élement identité.

Proposition 4.1.2. *Soit M un monoïde fini. Alors les conditions suivantes sont équivalentes*

(i) *M est apériodique*

(ii) *Il existe $m > 0$ tel que pour tout $x \in M$, $x^m = x^{m+1}$*

(iii) *Les groupes dans M sont triviaux.*

Démonstration. (i) $\Rightarrow$ (ii) Si M est apériodique alors pour tout $x \in M$, il existe n tel que $x^n = x^{n+1}$. Pour chaque x, notons n_x le plus petit entier tel que $x^{n_x} = x^{n_x+1}$. Soit $m = \max_{x \in M} n_x$, alors on a $x^m = x^{m+1}$ pour tout $x \in M$.
(ii) $\Rightarrow$ (iii) Soit G un groupe, $G \subset M$. Si $x \in G$ alors il existe k tel que $x(x^k) = x$. Il s'ensuit que $x = x(x^{km}) = x(x^{km+1}) = x^2x^{km} = x^2$. Donc x est idempotent et G est trivial.
(iii) $\Rightarrow$ (i) Soit $x \in M$ et T le monoïde engendré par x. D'après la proposition 4.1.1, $T = \{x, x^2, \ldots, x^{n+p-1}\}$ avec $x^n = x^{n+p}$ et $G = \{x^n, x^{n+1}, \ldots, x^{n+p-1}\}$ est un groupe dans T. G est trivial et donc x a une période 1. □

Théorème 4.1.3. *(Premier théorème d'isomorphisme) Soient G et H des groupes. Soit $\alpha : G \to H$, un morphisme de monoïdes. Alors $\alpha(G)$ est isomorphe à $G/\ker(\alpha)$.*

Démonstration. Soit $K = \ker(\alpha)$: c'est un sous-groupe distingué dans G et soit $\theta : G/\ker(\alpha) \to \alpha(G)$ le morphisme défini par $\theta(Kg) = \alpha(g)$.
Le morphisme θ est bien défini et bijectif car : soit $g, g' \in G$, on a

$$\theta(Kg) = \theta(Kg') \Leftrightarrow \alpha(g) = \alpha(g') \Leftrightarrow \alpha(g)(\alpha(g'))^{-1} = e_H \Leftrightarrow \alpha(gg'^{-1}) = e_H$$

$$\alpha(gg'^{-1}) = e_H \Leftrightarrow gg'^{-1} \in K = \ker(\alpha) \Leftrightarrow Kg = Kg'$$

De plus, on a pour $y \in \alpha(G)$, il existe $x \in G$ tel que $\alpha(x) = y$ donc Kx tel que $\theta(Kx) = \alpha(x) = y$. □

Proposition 4.1.4. *Soit M un monoïde. Si M est apériodique et M' est un sous-monoïde de M, alors M' est apériodique.*

Démonstration. Puisque M ne contient que des groupes triviaux, alors M' ne contient également que des groupes triviaux. □

Proposition 4.1.5. *Soient M et N deux monoïdes. Si M est apériodique et N divise M alors N est apériodique.*

Démonstration. N divise M donc il existe un monoïde $M' \subseteq M$ et un morphisme surjectif $\varphi : M' \to N$. Soit $n \in N$, alors il existe $m' \in M'$ tel que $\varphi(m') = n$. D'après la proposition 4.1.4 M' est apériodique donc il existe $k > 0$ tel que $m'^k = m'^{k+1}$. Mais puisqu'on a $\varphi(m'^k) = n^k$ et $\varphi(m'^{k+1}) = n^{k+1}$ alors $n^k = n^{k+1}$. D'où N est apériodique. □

Proposition 4.1.6. *Soient M_1 et M_2 deux monoïdes. Si M_1 et M_2 sont apériodiques alors $M_1 \times M_2$ est apériodique.*

Démonstration. Les monoïdes M_1 et M_2 sont apériodiques donc, d'après la proposition 4.1.4, il existe $k_1, k_2 > 0$ tels que pour tout $m_1 \in M_1$, $m_1^{k_1} = m_1^{k_1+1}$ et pour

tout $m_2 \in M_2$, $m_2^{k_2} = m_2^{k_2+1}$. Soit maintenant $(m_1, m_2) \in M_1 \times M_2$ et supposons $k_1 \leq k_2$ (la démonstration est similaire pour le cas $k_1 > k_2$). On a :

$$(m_1, m_2)^{k_2} = (m_1^{k_2}, m_2^{k_2}) = (m_1^{k_1+(k_2-k_1)}, m_2^{k_2}).$$

Or $m_1^{k_1+(k_2-k_1)} = m_1^{k_1+(k_2-k_1)+1} = m_1^{k_2+1}$ et $m_2^{k_2} = m_2^{k_2+1}$ donc

$$(m_1, m_2)^{k_2} = (m_1, m_2)^{k_2+1},$$

D'où $M_1 \times M_2$ est apériodique. □

Proposition 4.1.7. *Soient M et N deux monoïdes. Alors tout sous-groupe G de $M \diamond N$ est isomorphe à un sous-groupe de $M \times N$.*

Démonstration. Soit $G = \{(m_i, X_i, n_i) \mid i \in I_G\}$, alors le sous-groupe $M' \times N' = \{(m_i, n_i) \mid i \in I_G\}$ est, par construction, une image par un morphisme de G.
Soit $K = G \cap \{(e_M, X, e_N) \mid X \in R\}$ avec e_M, e_N les éléments neutres respectifs de M et N. On vérifie aisément que K est un sous-groupe de G.
Soit $e = (e_M, X, e_N)$ l'élément neutre de G et soient $p = (e_M, Y, e_N) \in K$ et $q = (e_M, Z, e_N) \in K$ tels que $pq = e$. On a

$$e = e^2 \Rightarrow (e_M, X, e_N) = (e_M, e_M X \cup X e_N, e_N) \Rightarrow X = e_M X \cup X e_N.$$

Puis

$$e = pq \Rightarrow (e_M, X, e_N) = (e_M, e_M Z \cup Y e_N, e_N) \Rightarrow X = e_M Z \cup Y e_N.$$

Il en résulte que $e_M Z \cup e_M Y e_N = e_M X \subset X$ (car $X = e_M X \cup X e_N$). Par ailleurs

(en faisant nos calculs sous la représentation matricielle)

$$\begin{aligned} epe &= \begin{pmatrix} e_M & X \\ \emptyset & e_N \end{pmatrix} \begin{pmatrix} e_M & Y \\ \emptyset & e_N \end{pmatrix} \begin{pmatrix} e_M & X \\ \emptyset & e_N \end{pmatrix} \\ &= \begin{pmatrix} e_M & X \\ \emptyset & e_N \end{pmatrix} \begin{pmatrix} e_M & e_M X \cup Y e_N \\ \emptyset & e_N \end{pmatrix} \\ &= \begin{pmatrix} e_M & e_M X \cup Y e_N \cup X e_N \\ \emptyset & e_N \end{pmatrix}, \end{aligned}$$

or $Ye_N = e_M Ye_N$ donc

$$epe = \begin{pmatrix} e_M & e_M X \cup e_M Y e_N \cup X e_N \\ \emptyset & e_N \end{pmatrix}.$$

On a alors

$$p = epe \Rightarrow (e_M, Y, e_N) = (e_M, e_M X \cup e_M Y e_N \cup X e_N, e_N) \Rightarrow Y = e_M X \cup e_M Y e_N \cup X e_N,$$

puis

$$Y = e_M X \cup X e_N \cup e_M Y e_N = X \cup e_M Y e_N,$$

or $e_M Y e_N \subset X$ donc $Y = X$ d'où $e = p = q$.

Nous venons de montrer que $K = \{e\}$.

D'après le théorème 4.1.3, G/K est isomorphe à $M' \times N'$ et comme $K = \{e\}$ alors G est isomorphe à $M' \times N'$. □

Proposition 4.1.8. *Soient M_1 et M_2 deux monoïdes. Si M_1 et M_2 sont apériodiques alors $M_1 \diamond M_2$ est apériodique.*

Démonstration. Cette proposition vient du fait que tout sous-groupe de $M_1 \diamond M_2$ est isomorphe à $M_1' \times M_2'$ où M_1' et M_2' sont des sous-groupes appropriés de M_1 et M_2. □

Lemme 4.1.9. *(Propriété de simplification) Soit M un monoïde apériodique. Soient $m, a, a' \in M$ tels que $m = ama'$, alors $m = am = ma'$.*

Démonstration. M est un monoïde apériodique donc il existe un entier $n > 0$ tel que $a^n = a^{n+1}$ pour tout $a \in M$. On a $m = ama' = a(ama')a' = \ldots = a^n ma'^n$. Alors

$$m = a^{n+1}ma'^n = a(a^n ma'^n) = am,$$

respectivement

$$m = a^n ma'^{n+1} = (a^n ma'^n)a' = ma'.$$

□

Proposition 4.1.10. *Soit M un monoïde apériodique. Alors pour tout $m \in M$,*

$$\{m\} = (mM \cap Mm) \setminus W_m$$

avec $W_m = \{m' \in M \mid m \notin Mm'M\}$.

Démonstration. Soit $m' \notin W_m$ et $m' \in (mM \cap Mm)$, celà équivaut à dire qu'il existe a, a', a_1, a_2 tels que $m = am'a'$ et $m' = ma_1 = a_2 m$. Alors $m = a(a_2 m)a' = (aa_2)ma'$ et par la propriété de simplification (lemme 4.1.9), on a $m = aa_2 m = ma'$. Ainsi $m = am' = ama_1$ et en appliquant encore la propriété de simplification, $m = am = ma_1$, d'où $m = m'$. □

4.2 Langages sans-étoile

Définition 4.2.1. Une *expression sans-étoile* est définie par :

(i) $\emptyset, \varepsilon$ et a, $a \in \Sigma$, sont des expressions sans-étoile.

(ii) Si s et t sont des expressions sans-étoile alors $s + t$, $s \cap t$, $\overline{s}$ et $s \cdot t$ le sont où $^-$est la complémentation dans Σ^*.

(iii) Toute expression sans-étoile est obtenue en appliquant un nombre fini de fois les règles (i) et (ii).

Chaque expression sans-étoile définit un langage noté $L(s)$. Un langage $L \subseteq \Sigma^*$ est *sans-étoile* s'il peut être obtenu à partir d'une expression sans-étoile s ; c'est-à-dire $L = L(s)$. Un langage est donc sans-étoile s'il est construit en utilisant seulement les opérations booléennes et le produit mais pas l'étoile de Kleene.

Exemple 4.2.1. Le langage Σ^* est sans étoile car $\Sigma^* = \overline{\emptyset}$.

Exemple 4.2.2. Soit le langage $L = (ab)^*$. Le langage L peut-être également décrit comme :

- ne contenant ni les chaines aa, ni bb ;
- ne commençant pas par b ;
- et ne se terminant pas par a.

Donc

$$L = (ab)^* = \overline{(\overline{\emptyset}aa\overline{\emptyset} + \overline{\emptyset}bb\overline{\emptyset} + b\overline{\emptyset} + \overline{\emptyset}a)}$$

d' où $L = (ab)^*$ est sans-étoile.

Nous remarquons qu'il peut-être assez difficile de déterminer si un langage est sans-étoile ou pas. Ainsi, le théorème de Schützenberger, que nous allons énoncer, nous fournit l'outil nécessaire pour caractériser ces derniers.

4.3 Théorème de Schützenberger

Théorème 4.3.1. *Un langage reconnaissable est sans étoile si et seulement si son monoïde syntaxique est apériodique.*

Démonstration. Prouvons d'abord le théorème suivant :

Théorème 4.3.2. *Le monoïde syntaxique d'un langage sans-étoile est apériodique.*

Démonstration. Nous procédons par récurrence sur le nombre n d'opérateurs dans l'expression sans-étoile du langage. Vérifions d'abord que les langages $\{\emptyset\}$, $\{\varepsilon\}$ et $\{\sigma\}$, $\sigma \in \Sigma$ ont un monoïde syntaxique apériodique. Le calcul montre en effet que $M(\{\sigma\})$ est apériodique (d'après l'exemple 3.2.1).
Supposons par hypothèse de récurrence que $M(L(r))$ est apériodique pour toutes les expressions sans étoile r ayant au plus n opérateurs. Soit r une expression ayant $n+1$ opérateurs. Alors $r = \overline{s}$ ou $r = s \cup t$ ou $r = s \cap t$ ou bien $r = s \cdot t$, avec s et t des expressions sans-étoile contenant au plus n opérateurs, donc $M(L(s))$ et $M(L(t))$ sont apériodiques.
Si $r = \overline{s}$ alors d'après la proposition 3.3.4, $M(L(s))$ reconnaît $L(\overline{s})$ et $M(L(s)) = M(L(\overline{s}))$. Donc $M(L(r))$ est apériodique.
Si $r = s \cup t$ ou $r = s \cap t$, alors $L(r)$ est reconnu par $M(L(s)) \times M(L(t))$ (d'après la proposition 3.3.5) ; $M(L(s)) \times M(L(t))$ étant apériodique par la proposition 4.1.6. De plus $M(L(r))$ divise $M(L(s)) \times M(L(t))$ d'après la proposition 3.3.3 et par conséquent $M(L(r))$ est apériodique (proposition 4.1.5).
Si $r = s \cdot t$, alors d'après la proposition 3.3.6 $L(r)$ est reconnu par un sous-monoïde G de $M(L(s)) \diamond M(L(t))$. D'après les propositions 4.1.8 puis 4.1.4 respectivement, $M(L(s)) \diamond M(L(t))$ est apériodique donc G l'est également. D'après la proposition 3.3.3 $M(L(r))$ divise $M(L(s)) \diamond M(L(t))$, il en résulte, par la proposition 4.1.5, que $M(L(r))$ est apériodique. □

Réciproquement :

Théorème 4.3.3. *Soit $L \subseteq \Sigma^*$ un langage reconnaissable de monoïde syntaxique $M(L)$ apériodique. Alors L est sans-étoile.*

Démonstration. Soit le morphisme canonique de monoïdes $\varphi : \Sigma^* \to M(L)$ et

$P \subseteq M(L)$ tels que $L = \varphi^{-1}(P)$. On a

$$L = \varphi^{-1}(P) = \bigcup_{m \in P} \varphi^{-1}(m)$$

et il suffit ainsi que chaque $\varphi^{-1}(m)$ soit sans-étoile pour démontrer que L l'est. Nous procédons par récurrence sur $|MmM|$.

Pour $m = \varepsilon$ on a

Lemme 4.3.4. *Soit $\varphi : \Sigma^* \to M$ un morphisme de monoïdes avec M apériodique. Alors $\varphi^{-1}(\varepsilon)$ est un langage sans-étoile de Σ^*.*

Démonstration. Posons $W = \{\sigma \in \Sigma \mid \varphi(\sigma) \neq \varepsilon\}$. Soit $\sigma \in W$ et $w, w' \in \Sigma^*$ tels que $\varphi(w\sigma w') = \varepsilon$. Alors $\varepsilon = \varphi(w)\varphi(\sigma)\varepsilon\varphi(w')$. D'après la propriété de simplification (lemme 4.1.9) on a $\varepsilon = \varphi(w)\varphi(\sigma) = \varphi(w')$. Une nouvelle application de la propriété de simplification (lemme 4.1.9) à $\varepsilon = \varphi(w)\varepsilon\varphi(\sigma)$ donne $\varepsilon = \varphi(w) = \varphi(\sigma)$, ce qui est contradictoire avec la définition de W. Donc pour tout $w'' \in \Sigma^* W \Sigma^*$, $\varphi(w'') \neq \varepsilon$.

Par ailleurs, soit $w \in \Sigma^* \setminus \Sigma^* W \Sigma^*$, w non vide et supposons $\varphi(w) \neq \varepsilon$. On a $w = \sigma_1\sigma_2 \ldots \sigma_n$ avec $\sigma_i \in \Sigma$. Il existe alors au moins un σ_i tel que $\varphi(\sigma_i) \neq \varepsilon$ c'est-à-dire $\sigma_i \in W$ (par définition) et donc $w \in \Sigma^* W \Sigma^*$, ce qui contredit notre hypothèse. D'où on a $\varphi^{-1}(\varepsilon) = \Sigma^* \setminus \Sigma^* W \Sigma^*$ qui est sans-étoile. □

Lemme 4.3.5. *Soit M un monoïde apériodique. On a $m = \varepsilon$ si et seulement si $|MmM| = |M|$.*

Démonstration. Si $m = \varepsilon$ alors $M\varepsilon M = M^2 = M$.

Si $|MmM| = |M|$ on a $M = MmM$ car $MmM \subseteq M$ et M est fini. Alors il existe u', u'' tels que $\varepsilon = u'mu'' = (u'm)\varepsilon u''$. De là, en appliquant une première fois la propriété de simplification (lemme 4.1.9) on a $\varepsilon = (u'm) = u''$; puis une seconde application à $\varepsilon = u'\varepsilon m$ nous donne $\varepsilon = u' = m$. □

Nous venons de prouver que $\varphi^{-1}(\varepsilon)$ est sans-étoile et que pour tout $m \in M \setminus \varepsilon$, M étant un monoïde apériodique, $|MmM| < |M\varepsilon M| = |M|$; autrement dit

$$|M\varepsilon M| = \max_{m \in M} |MmM|.$$

Supposons, comme hypothèse de récurrence, que pour tout $n \in M$ tel que $|MnM| > |MmM|$, $\varphi^{-1}(n)$ est sans-étoile. Nous démontrons que $\varphi^{-1}(m)$ peut s'écrire comme une combinaison sans-étoile d'ensembles $\varphi^{-1}(n)$ comme suit :

Proposition 4.3.6. *Soit un morphisme de monoïdes $\varphi : \Sigma^* \to M$, avec M apériodique et soit $m \in M \setminus \varepsilon$, alors*

$$\varphi^{-1}(m) = (X\Sigma^* \cap \Sigma^* X') \setminus \Sigma^* W \Sigma^*$$

avec X, X', W des sous-ensembles de Σ^* définis comme suit :

- $X = \{\varphi^{-1}(n)\sigma \mid n\varphi(\sigma)M = mM$ *mais* $n \notin mM, \sigma \in \Sigma, n \in M\}$.
- $X' = \{\sigma\varphi^{-1}(n) \mid M\varphi(\sigma)n = Mm$ *mais* $n \notin Mm, \sigma \in \Sigma, n \in M\}$.
- $W = \{\sigma \in \Sigma \mid m \notin M\varphi(\sigma)M\} \cup \{\sigma\varphi^{-1}(n)\sigma' \mid m \in (M\varphi(\sigma)nM \cap Mn\varphi(\sigma')M)$ *mais* $m \notin M\varphi(\sigma)n\varphi(\sigma')M\}$ *avec* $\sigma, \sigma' \in \Sigma, n \in M\}$.

De plus, les éléments $n \in M$ apparaissant dans chacune de ces trois définitions satisfont $|MnM| > |MmM|$.

Démonstration. Montrons d'abord que $\varphi^{-1}(m) \subseteq (X\Sigma^* \cap \Sigma^* X') \setminus \Sigma^* W \Sigma^*$.
Soit $w \in \varphi^{-1}(m)$, alors $\varphi(w) = m$. Soit $u \in \Sigma^*$ le plus petit préfixe de w tel que $\varphi(u)M = mM$ (resp. plus petit suffixe de w tel que $M\varphi(u) = Mm$).
D'une part, supposons $u = \varepsilon$, alors on aurait $M = mM$ et il existerait $m' \in M$ tel que $\varepsilon = mm' = m\varepsilon m'$ (resp. $M = Mm$ et $\varepsilon = m'm$). D'après la propriété de simplification (lemme 4.1.9), celà reviendrait à $m = \varepsilon$ ce qui est contradictoire avec le fait que $m \in M \setminus \varepsilon$. On a donc $u \neq \varepsilon$, ce qui permet d'écrire $u = v\sigma$ (resp. $u = \sigma v$), avec $\sigma \in \Sigma$ et $v \in \Sigma^*$. En prenant $n = \varphi(v)$ on a

$$mM = \varphi(u)M = \varphi(v)\varphi(\sigma)M = n\varphi(\sigma)M,$$

et respectivement

$$Mm = M\varphi(u) = M\varphi(\sigma)\varphi(v) = M\varphi(\sigma)n.$$

D'autre part, supposons $n \in mM$, alors $n = mm'$ (resp. $n = m'm$) pour un certain $m' \in M$. Alors on aurait

$$\varphi(v)M = mm'M \subseteq mM \quad (resp.\, M\varphi(v) = Mm'm \subseteq Mm)$$

et

$$mM = \varphi(u)M = \varphi(v)\varphi(\sigma)M \subseteq \varphi(v)M$$

$$(resp.\, Mm = M\varphi(u) = M\varphi(\sigma)\varphi(v) \subseteq M\varphi(v))$$

Ce qui nous donne $\varphi(v)M = mM$ (resp. $M\varphi(v) = Mm$) qui contredit la minimalité du préfixe u. Donc $w \in X\Sigma^*$ (resp. $w \in \Sigma^*X'$), d'où $w \in X\Sigma^* \cap \Sigma^*X'$.
De plus, supposons $y \in W$, alors on a soit $y = \sigma$ et $m \notin M\varphi(\sigma)M$, soit $\varphi(y) = \varphi(\sigma)n\varphi(\sigma')$ et $m \notin M\varphi(\sigma)n\varphi(\sigma')M$. Donc $m \notin M\varphi(y)M$. Si $w \in \Sigma^*W\Sigma^*$ alors $w = uyv$ pour un certain $y \in W$ et $u, v \in \Sigma^*$. Alors $m = \varphi(w) = \varphi(u)\varphi(y)\varphi(v) \in M\varphi(y)M$, ce qui est contradictoire. Donc $w \notin \Sigma^*W\Sigma^*$.
Montrons maintenant que $(X\Sigma^* \cap \Sigma^*X') \setminus \Sigma^*W\Sigma^* \subseteq \varphi^{-1}(m)$.
Soit $w \in (X\Sigma^* \cap \Sigma^*X') \setminus \Sigma^*W\Sigma^*$ et prenons $n = \varphi(w)$. Nous allons montrer que $\{n\} = \{m\}$. Nous savons déjà que $\{m\} = (mM \cap Mm) \setminus W_m$ d'après la proposition 4.1.10. On a $w \in X\Sigma^*$ (resp. $w \in \Sigma^*X'$) ce qui implique $w = xv$ où $x \in X$ c'est-à-dire $\varphi(x) = n\varphi(\sigma)$ avec $n\varphi(\sigma)M = mM$. Alors $n = \varphi(w) = \varphi(x)\varphi(v) = n\varphi(\sigma)\varphi(v) \in mM$. De manière analogue en partant de $w \in \Sigma^*X'$ on a $n \in Mm$, d'où $n \in mM \cap Mm$.
Supposons maintenant que $m \notin MnM$ c'est-à-dire $m \notin M\varphi(w)M$. Soit un facteur f de w, i.e. $w = ufv$, de longueur minimum tel que $m \notin M\varphi(f)M$.

- Supposons $f = \varepsilon$; alors m n'appartiendrait pas à $M^2 = M$, ce qui est contradictoire. Donc $f \neq \varepsilon$.

- Si $f \in \Sigma$ alors par hypothèse $m \notin M\varphi(f)M$ et donc $f \in W$ ce qui implique $w \in \Sigma^* W \Sigma^*$, ce qui est contradictoire.
- Donc $|f| \geq 2$ alors $f = \sigma f' \sigma'$ où $\sigma, \sigma' \in \Sigma$ et $f' \in \Sigma^*$. Il s'ensuit que $m \in M\varphi(\sigma)\varphi(f')M$ et $m \in M\varphi(f')\varphi(\sigma')M$ par minimalité de f. Donc $f \in W$, ce qui est contradictoire.

D'où $m \in MnM$ et donc $n \in W_m$.

Prouvons l'assertion finale de la proposition i.e. on a $|MnM| > |MmM|$.
Cas de X : On a $MmM = Mn\varphi(\sigma)M \subseteq MnM$ (resp. $MmM = M\varphi(\sigma)nM \subseteq MnM$) donc $|MnM| \geq |MmM|$. Supposons que $|MnM| = |MmM|$ alors $MnM = MmM$ par finitude. On a ainsi $n = m'mm''$ pour un certain $m', m'' \in M$. De plus, puisque $m \in n\varphi(\sigma)M$ (resp. $m \in M\varphi(\sigma)n$), on a $m = np$ (resp. $m = pn$) pour un $p \in M$. Alors $n = m'mm'' = m'(np)m'' = m'n(pm'')$ (resp. $n = m'mm'' = m'(pn)m'' = (m'p)nm''$) et d'après la propriété de simplification (lemme 4.1.9), on a $n = m'n = npm''$ donc $n = mm''$ (resp. $n = m'pn = nm''$ donc $n = m'm$) c'est-à-dire $n \in mM$ (resp. $n \in Mm$), ce qui est contradictoire. Alors $|MnM| \neq |MmM|$ et $|MnM| > |MmM|$.

Cas de X' : Symétrique du cas de X.

Cas de W : Soit maintenant $m \in M\varphi(\sigma)nM \cap Mn\varphi(\sigma')M$ et $m \notin M\varphi(\sigma)n\varphi(\sigma')M$. On a $|MnM| \geq |MmM|$. Supposons que $|MnM| = |MmM|$ alors $MnM = MmM$ par finitude. On a ainsi $n = m'mm''$ pour un certain $m', m'' \in M$. On a également $m = m_1\varphi(\sigma)nm_1' = m_2n\varphi(\sigma')m_2'$ avec $m_1, m_1', m_2, m_2' \in M$. Alors $n = m'mm'' = m'(m_1\varphi(\sigma)nm_1')m'' = (m'm_1\varphi(\sigma))n(m_1'm'')$ et par la propriété de simplification (lemme 4.1.9), on a $n = m'm_1\varphi(\sigma)n$. Ainsi $m = m_2n\varphi(\sigma')m_2' = m_2(m'm_1\varphi(\sigma)n)\varphi(\sigma')m_2' = (m_2m'm_1)\varphi(\sigma)n\varphi(\sigma')m_2' \in M\varphi(\sigma)n\varphi(\sigma')M$, ce qui est contradictoire. Donc $|MnM| \neq |MmM|$ et $|MnM| > |MmM|$. □

Revenons à la preuve du théorème 4.3.3.

Nous venons de montrer que pour tout $m \in M$, $\varphi^{-1}(m)$ peut se décomposer en combinaison sans-étoile d'ensembles $\varphi^{-1}(n)$ tel que $|MnM| > |MmM|$ qui, selon notre hypothèse de récurrence, est sans-étoile donc $\varphi^{-1}(m)$ l'est également, ce qui conclut notre démonstration. □

En combinant les théorèmes 4.3.2 et 4.3.3 nous avons prouvé le théorème de Schützenberger. □

CHAPITRE V

RELATIONS DE GREEN

Ce chapitre s'intéresse aux relations de Green. Nous y démontrons le lemme de Green et le théorème de Clifford-Miller. Ces résultats sont utiles pour traiter les langages réductibles.

5.1 Relations et Lemme de Green

Soit M un monoïde dans lequel on définit les relations d'équivalence $\mathcal{R}, \mathcal{L}, \mathcal{J}, \mathcal{H}$ suivantes : pour $m, n \in M$, nous avons

- $m\mathcal{R}n \Leftrightarrow mM = nM$.
- $m\mathcal{L}n \Leftrightarrow Mm = Mn$.
- $m\mathcal{J}n \Leftrightarrow MmM = MnM$.
- $m\mathcal{H}n \Leftrightarrow m\mathcal{R}n$ et $m\mathcal{L}n$.

Nous pouvons également définir les relations de *préordre* (c'est-à-dire *reflexive* et *transitive*) suivantes :

- $m \leq_{\mathcal{R}} n \Leftrightarrow mM \subseteq nM$.
- $m \leq_{\mathcal{L}} n \Leftrightarrow Mm \subseteq Mn$.
- $m \leq_{\mathcal{J}} n \Leftrightarrow MmM \subseteq MnM$.
- $m \leq_{\mathcal{H}} n \Leftrightarrow m \leq_{\mathcal{R}} n$ et $m \leq_{\mathcal{L}} n$.

En particulier, nous avons $m\mathcal{R}n$ si et seulement s'il existe $m', n' \in M$ tels que $mm' = n$ et $nn' = m$ et nous avons $m\mathcal{L}n$ si et seulement s'il existe $m', n' \in M$ tels que $m'm = n$ et $n'n = m$.

Proposition 5.1.1. *Les relations $\leq_{\mathcal{R}}$ et $\mathcal{R}$ sont compatibles à gauche avec la multiplication. Les relations $\leq_{\mathcal{L}}$ et $\mathcal{L}$ sont compatibles à droite avec la multiplication. Aussi, la multiplication est le produit du monoide.*

Démonstration. Supposons $m \leq_{\mathcal{R}} n$, alors $mM \subseteq nM$, donc $m'mM \subseteq m'nM$ pour tout $m' \in M$. D'où $m'mM \leq_{\mathcal{R}} m'nM$. De manière analogue, nous démontrons les autres assertions. □

Nous définissons maintenant une nouvelle relation $\mathcal{D}$, de la manière suivante :

Proposition 5.1.2. *Les relations $\mathcal{R}$ et $\mathcal{L}$ commutent et la relation $\mathcal{D} = \mathcal{R}\mathcal{L} = \mathcal{L}\mathcal{R}$ est la plus petite relation d'équivalence contenant $\mathcal{R}$ et $\mathcal{L}$.*

Démonstration. Supposons $m\mathcal{L}\mathcal{R}n$; c'est-à-dire qu'il existe $m' \in M$ tel que $m\mathcal{L}m'$ et $m'\mathcal{R}n$. Donc, il existe $m_1, n_1 \in M$ tels que $m = m_1m'$ et $n = m'n_1$. Nous avons ainsi $mn_1 = m_1m'n_1 = m_1n = n'$. De plus, d'après la proposition 5.1.1 :
- $m\mathcal{L}m'$ implique $n' = mn_1\mathcal{L}m'n_1 = n$ et
- $m'\mathcal{R}n$ implique $m = m_1m'\mathcal{R}m_1n = n'$.

Donc $m\mathcal{R}n'$ et $n'\mathcal{L}n$ d'où $m\mathcal{R}\mathcal{L}n$. Réciproquement si nous avons $m\mathcal{R}\mathcal{L}n$ alors $m\mathcal{L}\mathcal{R}n$, donc $\mathcal{L}\mathcal{R} = \mathcal{R}\mathcal{L}$. □

Définition 5.1.1. Soit M un monoïde, les relations d'équivalence $\mathcal{R}, \mathcal{L}, \mathcal{J}, \mathcal{H}$ et $\mathcal{D}$ sont appelées les *relations de Green.*

Proposition 5.1.3. *Dans un monoïde fini M, $\mathcal{J} = \mathcal{D}$.*

Démonstration. Soient $m, n \in M$. Si $m\mathcal{D}n$ alors il existe $m' \in M$ tel que $m\mathcal{R}m'$ et $m'\mathcal{L}n$. Ceci nous donne (car $m\mathcal{R}m' \Rightarrow m\mathcal{J}m'$ et $m'\mathcal{L}n \Rightarrow m'\mathcal{J}n$) $m\mathcal{J}m'$, puis $m'\mathcal{J}n$, d'où $m\mathcal{J}n$.

Réciproquement, supposons $m\mathcal{J}n$. Alors par définition il existe $u, v, x, y \in M$ tels que $umv = n$ et $xny = m$. Remarquons que $(xu)m(vy) = xny = m$ donc $(xu)^k m(vy)^k$ pour tout $k > 0$. Puisque M est fini, il existe $k > 0$ et $l > 0$ tels que $(xu)^k = e$ et $(vy)^l = f$ soient des idempotents. Donc $(xu)^{kl}m(vy)^{kl} = m = emf$. Nous en déduisons

$$(xu)^k m = em = e(emf) = emf = m = emf = (emf)f = mf = m(vy)^l$$

Donc $um\mathcal{L}m$ et $mv\mathcal{R}m$.

Mais nous avons, d'après la proposition 5.1.1, $n = umv\mathcal{L}mv$ d'où $m\mathcal{D}n$. □

Proposition 5.1.4. *Soit e un idempotent de M. Alors $m \leq_{\mathcal{R}} e$ si et seulement si $m = em$ et $m \leq_{\mathcal{L}} e$ si et seulement si $m = me$.*

Démonstration. Si $m \leq_{\mathcal{R}} e$, alors il existe $n \in M$ tel que $m = en$. Il s'ensuit

$$em = een = en = m$$

Réciproquement $m = em \Rightarrow m \leq_{\mathcal{R}} e$ de manière immédiate.

La preuve pour le cas $m \leq_{\mathcal{L}} e$ est analogue. □

Soit $\mathcal{K}$ une relation de Green, nous notons $\mathcal{K}$-classe la classe d'équivalence selon la relation $\mathcal{K}$.

Remarque 5.1.1. Soit $m \in M$. Nous noterons $R(m)$ (respectivement $L(m)$, $H(m)$ et $D(m)$) la $\mathcal{R}$-classe (respectivement $\mathcal{L}$-classe, $\mathcal{H}$-classe et $\mathcal{D}$-classe) contenant m.

Définition 5.1.2. Un élément $m \in M$ est *régulier* s'il existe $s \in M$ tel que $msm = m$, et une $\mathcal{D}$-classe est *régulière* si tous ses éléments sont réguliers.

Proposition 5.1.5. *Soit D une $\mathcal{D}$-classe. Les conditions suivantes sont équivalentes :*

(i) *D est régulière.*

(ii) *D contient un élément régulier.*

(iii) *Chaque $\mathcal{R}$-classe de D contient au moins un idempotent.*

(iv) *Chaque $\mathcal{L}$-classe de D contient au moins un idempotent.*

(v) *D contient au moins un idempotent.*

Démonstration. Si $m = msm$, alors $m\mathcal{R}e$ avec $e = e^2 = ms$. Réciproquement, si $m\mathcal{R}e$ où e est un idempotent, alors il existe $m' \in M$ tel que $mm' = e$ et donc d'après la proposition 5.1.4 (car $m\mathcal{R}e \Rightarrow m \leq_{\mathcal{R}} e$)

$$m = em = e^2m = mm'em.$$

Nous avons donc montré que m est régulier si et seulement si $R(m)$ contient un idempotent. Similairement, nous avons $m = msm$ si et seulement si $L(m)$ contient un idempotent.

Soit m un élément régulier et $d \in D$. Alors il existe c tel que $m\mathcal{R}c\mathcal{L}d$. Puisque m est régulier, $R(m) = R(c)$ contient un idempotent et c est un élément régulier. Il en résulte que $L(c) = L(d)$ contient un idempotent et d est régulier.

Nous venons de démontrer (i) $\Leftrightarrow$(ii)$\Leftrightarrow$ (iii) $\Leftrightarrow$ (iv).

De plus (v) $\Rightarrow$ (ii) et (iii) $\Rightarrow$ (v) sont évidents. □

Proposition 5.1.6. *(Lemme de Green) Soient $s, t \in M$ tels que $s\mathcal{R}t$. Il existe alors $u, v \in M$ tels que $su = t$ et $tv = s$. Alors les applications $\rho_u : x \mapsto xu$ et $\rho_v : x \mapsto xv$ induisent des bijections réciproques de $L(s)$ sur $L(t)$ et de $L(t)$ sur $L(s)$, qui préservent les $\mathcal{H}$-classes, c'est-à-dire pour tout $x, y \in L(s)$ (resp. $L(t)$), $x\mathcal{H}y$ si et seulement si $\rho_u(x)\mathcal{H}\rho_u(y)$ (resp. $\rho_v(x)\mathcal{H}\rho_v(y)$).*

Démonstration. Puisque $x\mathcal{L}s \Rightarrow xu\mathcal{L}su = t$ (d'après la proposition 5.1.1), ρ_u est une application de $L(s)$ dans $L(t)$ et il existe $m \in M$ tel que $x = ms$. Donc

$$\rho_v(\rho_u(x)) = xuv = msuv = mtv = ms = x$$

ce qui prouve que $\rho_v \circ \rho_u$ est l'identité sur $L(s)$.
De manière analogue nous montrons que ρ_v est une application de $L(t)$ sur $L(s)$ et que $\rho_u \circ \rho_v$ est l'identité sur $L(t)$. Par ailleurs, si $x \in L(s)$, nous avons $xuv = x$ donc $x\mathcal{R}xu$. Il en résulte que $x\mathcal{H}y$ implique $xu\mathcal{H}yu$ car $x\mathcal{H}y \Leftrightarrow x\mathcal{R}y$ et $x\mathcal{L}y$ et la relation $\mathcal{L}$ est compatible à droite. De même

$$xu\mathcal{H}yu \Rightarrow x = xuv\mathcal{H}yuv = y.$$

□

Remarque 5.1.2. Nous avons une version duale du Lemme de Green (proposition 5.1.6) pour les éléments $\mathcal{L}$-équivalents.

5.2 Théorème de Clifford-Miller

Théorème 5.2.1. *(Clifford-Miller) Soit D une $\mathcal{D}$-classe d'un monoïde fini M et soient $s, t \in D$. Alors les conditions suivantes sont équivalentes :*

(i) $st \in R(s) \cap L(t)$.

(ii) $R(t) \cap L(s)$ *contient un idempotent.*

(iii) $st \in D$.

Démonstration. (i) $\Leftrightarrow$ (ii) Supposons $st \in R(s) \cap L(t)$. D'après la proposition 5.1.6, l'application ρ_t induit une bijection de $L(s)$ sur $L(t)$ préservant les $\mathcal{H}$-classes. En particulier, il existe un élément $e \in R(t) \cap L(s)$ tel que $\rho_t(e) = et = t$. Puisque $e\mathcal{R}t$, il existe $u \in M$ tel que $e = tu$ et donc

$$ee = etu = tu = e.$$

Réciproquement, si $e = e^2 \in R(t) \cap L(s)$, alors $et = t$ et $se = s$ (d'après la proposition 5.1.4). Puisque $e\mathcal{R}t$, nous avons $s = se\mathcal{R}st$ et comme $e\mathcal{L}s$, nous avons $t = et\mathcal{L}st$ d'où $st \in R(s) \cap L(t)$.
Finalement, (i) $\Leftrightarrow$ (iii) par la proposition 5.1.3. En effet, $st \in R(s) \cap L(t)$ équivaut à st appartient à une $\mathcal{J}$-classe et puisque $\mathcal{J} = \mathcal{D}$, celà équivaut à $st \in D$ □

Corollaire 5.2.2. *Soit H une $\mathcal{H}$-classe de M. Les conditions suivantes sont equivalentes :*

(i) *H contient un idempotent.*

(ii) *Il existe $s, t \in H$ tels que $st \in H$.*

(iii) *H est un groupe maximal dans M.*

Démonstration. Les implications (i) $\Rightarrow$ (ii) et (iii) $\Rightarrow$ (i) sont claires. Vérifions (ii) $\Rightarrow$ (iii). Supposons (ii) vérifié, nous avons $H = R(s) \cap L(t) = R(t) \cap L(s)$ et donc H contient un idempotent d'après le théorème 5.2.1. Si $u, v \in H$, nous avons $e \in R(v) \cap L(u)$ et $uv \in H$ toujours d'après le théorème 5.2.1. De plus pour tout $x \in H$ nous avons $ex = x = xe$ d'après la proposition 5.1.4. Donc H est un monoïde. Par ailleurs, si $h \in H$, d'après le lemme de Green (proposition 5.1.6), l'application ρ_h est une bijection de H sur H. En particulier, il existe $h' \in H$ tel que $\rho_h(h') = h'h = e$. Par le dual du lemme de Green, on démontre également que h a un inverse à droite.
Donc H est un groupe avec e pour identité. Finalement, tout élément g d'un groupe contenant e, avec g' comme inverse, vérifie :

$$gg' = g'g = e = eg = ge = g.$$

Ce qui pouve que $g\mathcal{H}e$. □

Nous avons comme corollaire

Corollaire 5.2.3. *Pour tout $m, m' \in H$ avec H une $\mathcal{H}$-classe, soit $mm' \notin H$ soit H est un groupe.*

Démonstration. Découle immédiatement du corollaire précédent (5.2.2). □

CHAPITRE VI

ENSEMBLES COMPLÈTEMENT RÉDUCTIBLES

Dans ce chapitre sur les langages complètement réductibles, nous établissons les conditions nécessaires et suffisantes de réductiblité complète. Nous y voyons aussi que les langages birécurrents sont complètement réductibles.

6.1 Complément sur les automates

Soit $\mathcal{A} = (\Sigma, Q, i, \delta, F)$ un automate fini. Nous rappelons qu'un état $q \in Q$ est dit *accessible* s'il existe un chemin de l'état initial i à q ; c'est-à-dire il existe un mot w tel que $i \cdot w = q$. De manière analogue, un état $q \in Q$ est dit *coaccessible* s'il existe un chemin de q à un état final ; c'est-à-dire il existe un mot $w \in \Sigma^*$ tel que $q \cdot w \in F$. Un automate est dit *émondé* si chaque état est à la fois accessible et coaccessible.

Remarque 6.1.1. L'automate minimal d'un langage L est émondé.

Définition 6.1.1. Soit $\mathcal{A} = (\Sigma, Q, I, \delta, F)$ un automate. L'automate $\mathcal{A}$ est *fortement connexe* si pour tous $p, q \in Q$, il existe un mot $w \in \Sigma^*$ tel que $p \cdot w = q$.

Le *rang* d'un mot $w \in \Sigma^*$ dans $\mathcal{A}$, noté par $rang_{\mathcal{A}}(w)$, est défini par :

$$rang_{\mathcal{A}}(w) = \mathrm{Card}(Q \cdot w)$$

C'est un entier.

Un idéal I d'un monoïde M est dit *minimal* s'il ne contient aucun autre idéal de M, autrement dit pour tout idéal non vide J de M, $J \subseteq I \Rightarrow J = I$. Il existe un idéal minimal si M est fini ou si M possède un zéro. Quand M possède un zéro alors $\{0\}$ est l'idéal minimal. Un idéal $I \neq 0$ est appelé *idéal 0-minimal* si les seuls idéaux contenus dans I sont I lui-même et 0, c'est-à-dire pour tout idéal J de M, $J \subseteq I$ implique $J = I$ ou $J = \{0\}$.

Proposition 6.1.1. *Soit $\mathcal{A} = (\Sigma, Q, i, \delta, F)$ un automate fortement connexe. Le monoïde de transition M de $\mathcal{A}$ a, selon que M contient un zéro ou pas, soit un unique idéal 0-minimal, soit un unique idéal minimal D, formé des éléments de rang minimal non-nul. C'est une $\mathcal{D}$-classe régulière et pour tout $m \in D$, soit $m^2 = 0$, soit la $\mathcal{H}$-classe de m est un groupe.*

Démonstration. Supposons, dans un premier temps, que M contienne un zéro. Soit r le rang minimal non-nul des éléments de M et soit D l'ensemble des éléments de rang r. Nous remarquons clairement que $D \cup 0$ est un idéal. De plus, soient $m, m' \in D$, $p, q, p', q' \in Q$ tels que $pm = q$ et $p'm' = q'$. Puisque $\mathcal{A}$ est fortement connexe, il existe $u \in M$ tel que $qu = p'$ donc $pmum' = q'$ et par suite $mum' \neq 0$. Nous venons de prouver que pour tout $m, m' \in D$, il existe $u \in M$ tel que $mum' \neq 0$. Prenons $u \in M$ tel que $mu \neq 0$, alors il existe $v \in M$ tel que $mu(vm) \neq 0$. Soit $I = Q \cdot m$ l'image de m et $z = uvm$; nous avons $z \in Mm$ donc $Iz \subseteq I$. Puisque $z \neq 0$, $Iz \subseteq I \Rightarrow Iz = I$ par minimalité de rang de m. Il existe alors un entier strictement positif k tel que $z^k = e_I$, avec e_I l'identité sur I donc

$me_I = m$. Prenons ensuite $w = vmz^{k-1}$; alors nous avons

$$\begin{aligned} m &= me_I \\ &= mz^k = mzz^{k-1} \\ &= m(uvm)z^{k-1} = mu(vmz^{k-1}), \\ m &= muw, \end{aligned}$$

d'où $mu \in R(m)$, autrement dit $muM = mM$. Nous venons donc de prouver que l'idéal à droite mM est 0-minimal. Il existe ainsi $v \in M$ tel que $mum'v = m$ donc $mum' \in R(m)$.

Symétriquement nous avons $mum' \in L(m')$, donc D est une $\mathcal{D}$-classe et D est un idéal 0-minimal. Prenons maintenant $m'' = um'$, alors nous avons $mm'' \in R(m) \cap L(m'')$ et d'après le théorème 5.2.1, $R(m'') \cap L(m)$ contient un idempotent, d'où D est une $\mathcal{D}$-classe régulière. De plus, d'après le corollaire 5.2.3, pour $m \in D$:

- soit $m^2 \in H(m)$ et $H(m)$ est un groupe.
- soit $m^2 \notin H(m)$. Mais dans ce cas, d'abord $m^2M \neq mM$ (car $m^2 \notin H(m) \Rightarrow m^2 \notin R(m) \Rightarrow m^2M \neq mM$), puis mM étant un idéal à droite 0-minimal, il est impossible d'avoir $m^2 \neq 0$; car si $m^2 \neq 0$ alors m^2M serait un idéal à droite inclus dans mM, ce qui contredirait la 0-minimalité de ce dernier ; d'où $m = 0$.

La démonstration est analogue pour le cas où M ne contient pas de zéro. □

6.2 Représentation syntaxique

Définition 6.2.1. Soit K un corps commutatif. Une *série formelle* S sur un alphabet Σ à coefficients dans K est une application $S : \Sigma^* \to K$. La valeur de S sur w est notée (S, w) et (S, ε) est appelé le *terme constant* de S ; ε étant le mot vide.

L'ensemble des séries formelles possède une structure d'espace vectoriel :

- Soient S et T des séries formelles, $(S+T,w) = (S,w) + (T,w)$.
- Pour $\alpha \in K$, la série αS est définie par $(\alpha S, w) = \alpha(S,w)$.

Définition 6.2.2. Soit n un entier strictement positif. Soient $\lambda \in K^{1\times n}$ - un vecteur ligne, $\mu : \Sigma^* \to K^{n\times n}$ - un morphisme de monoïdes, $\gamma \in K^{n\times 1}$ - un vecteur colonne. Le triplet (λ, μ, γ) est appelé une *représentation linéaire* d'une série S si pour tout mot w :

$$(S,w) = \lambda\mu(w)\gamma.$$

Nous disons également que (λ, μ, γ) *reconnaît* S.

Le vecteur λ est appelé le *vecteur initial* et γ le *vecteur terminal.* Une série S est *reconnaissable* si elle a une représentation linéaire.

Définition 6.2.3. Soit Σ un alphabet et K un corps commutatif. Un polynôme non-commutatif est une combinaison linéaire sur K de mots sur Σ^*. On appelle *algèbre associative libre*, notée $K\langle\Sigma\rangle$, l'ensemble des polynômes non-commutatifs.

Soit $\mathfrak{A}$ une algèbre. Un morphisme $\psi : K\langle\Sigma\rangle \to \mathfrak{A}$ *reconnaît* une série S s'il existe une application linéaire $\pi : \mathfrak{A} \to K$ telle que $(S,w) = \pi(\psi(w))$ pour tout $w \in \Sigma^*$.

Proposition 6.2.1. *Une série est reconnaissable si et seulement si elle est peut être reconnue par un morphisme dans une algèbre de dimension finie.*

Démonstration. Dans un premier temps, soit S une série reconnaissable et soit (λ, μ, γ) une représentation linéaire de S. Avec μ un morphisme de $K\langle\Sigma\rangle \to K^{n\times n}$; ce qui est possible car tout morphisme de monoïdes de Σ^* dans $K^{n\times n}$ se prolonge de manière unique en un morphisme d'algèbres de $K\langle\Sigma\rangle$ dans $K^{n\times n}$. Le morphisme μ reconnaît S car l'application linéaire :

$$\pi : K^{n\times n} \to K$$
$$\pi(m) \mapsto \lambda m \gamma$$

satisfait $(S, w) = \pi(\mu(w))$ pour tout mot $w \in \Sigma^*$.

Réciproquement, soit ψ un morphisme dans une algèbre de dimension finie $\mathfrak{A}$, reconnaissant une série S. Choisissons une base de $\mathfrak{A}$, alors prenons les éléments du triplet (λ, μ, γ) de la manière suivante :

- Soit λ le vecteur de taille n représentant $\psi(1)$.
- L'application :

$$\rho : \mathfrak{A} \to \mathfrak{A}$$
$$x \mapsto x\psi(w)$$

  est linéaire et représentée par une matrice carrée $\mu(w)$ de taille n.
- Soit γ le vecteur colonne de taille n pris tel que $\pi(x) = x\gamma^t$ pour tout $x \in \mathfrak{A}$.

Nous avons alors $\lambda\mu(w)\gamma = (S, w)$ pour tout $w \in \Sigma^*$. □

Soit S une série formelle. Pour $u \in \Sigma^*$, nous notons $S \cdot u$, la série définie par $(S \cdot u, v) = (S, uv)$. Les formules ci-dessous sont satisfaites :

- $S \cdot 1 = S$,
- $(S \cdot u) \cdot v = S \cdot uv$.

Définition 6.2.4. On appelle *espace syntaxique* de S, noté V_S, l'espace vectoriel engendré par les séries $S \cdot u$, pour $u \in \Sigma^*$. La *représentation syntaxique* de S est le morphisme $\psi_S : K\langle\Sigma\rangle \to \mathrm{End}(V_S)$ défini, pour tout $X \in V_S$ et $w \in \Sigma^*$, par :

$$X\psi_S(w) = X \cdot w.$$

Définition 6.2.5. L'*algèbre syntaxique* de S, notée $\mathfrak{A}_S$, est l'image de l'algèbre libre associative $K\langle\Sigma\rangle$ par la représentation syntaxique.

L'algèbre syntaxique est aussi définie comme le quotient de l'algèbre libre associative $K\langle\Sigma\rangle$ par la relation d'équivalence

$$p \equiv 0 \Leftrightarrow (S, upv) = 0, \forall u, v \in \Sigma^*.$$

Le morphisme ψ_S reconnaît S car l'application $\pi : \mathfrak{A}_S \to K$ définie par $\pi(\psi_S(w)) = (S, w)$ est bien définie et linéaire.

Proposition 6.2.2. *Si $\psi : K\langle\Sigma\rangle \to \mathfrak{A}$ est un morphisme surjectif reconnaissant S, alors il existe un morphisme $\rho : \mathfrak{A} \to \mathfrak{A}_S$ tel que $\psi_S = \rho \circ \psi$.*

Démonstration. Il suffit de montrer que si $p \in K\langle\Sigma\rangle$ est tel que $\psi(p) = 0$, alors $\psi_S(p) = 0$. Soit $\pi : \mathfrak{A} \to K$, l'application linéaire telle que $\pi(\psi(w)) = (S, w)$ pour tout $w \in \Sigma^*$. Si $\psi(p) = 0$, alors pour tout $u, v \in \Sigma^*$, nous avons

$$(S, upv) = \pi(\psi(upv)) = \pi(\psi(u)\psi(p)\psi(v)) = 0$$

or d'après la définition 6.2.5, $(S, upv) = 0 \Leftrightarrow p \equiv 0$ et donc $\psi_S(p) = 0$. □

Soit $L \subseteq \Sigma^*$, nous notons par χ_L, la série caractéristique de L qui est définie par :

$$(\chi_L, x) = \begin{cases} 1 & \text{Si } x \in L \\ 0 & \text{Sinon} \end{cases} \tag{6.1}$$

Proposition 6.2.3. *Soit $L \subseteq \Sigma^*$ et $S = \chi_L$. Soit $\varphi : \Sigma^* \to M(L)$ le morphisme canonique de Σ^* sur le monoïde syntaxique $M(L)$ de L. Alors pour tout $u, v \in \Sigma^*$,*

$$\varphi(u) = \varphi(v) \Leftrightarrow \psi_S(u) = \psi_S(v).$$

En particulier $\psi_S(\Sigma^*)$ est isomorphe au monoïde syntaxique $M(L)$ de L.

Démonstration. Supposons que $\varphi(u) = \varphi(v)$. Puisque V_S est un espace engendré par les séries $S \cdot r$, avec $r \in \Sigma^*$, il suffit de montrer que pour tout $r \in \Sigma^*$,

$$(S \cdot r)\psi_S(u) = (S \cdot r)\psi_S(v).$$

Nous avons, pour tout $s \in \Sigma^*$

$$((S \cdot r)\psi_S(u), s) = (S \cdot ru, s) = (S, rus) = (S, rvs) = ((S \cdot r)\psi_S(v), s),$$

l'égalité $(S, rus) = (S, rvs)$ étant due au fait que u et v sont syntaxiquement équivalents.

Réciproquement, supposons $\psi_S(u) = \psi_S(v)$. Alors, pour tout $r \in \Sigma^*$,

$$S \cdot ru = (S \cdot r)\psi_S(u) = (S \cdot r)\psi_S(v) = S \cdot rv.$$

Puis ensuite, pour tout $s \in \Sigma^*$,

$$(S, rus) = (S \cdot ru, s) = (S \cdot rv, s) = (S, rvs).$$

C'est-à-dire $rus \in L$ si et seulement si $rvs \in L$ i.e $\varphi(u) = \varphi(v)$. □

6.3 Réductibilité complète

Soit V un K-espace vectoriel et M un sous-monoïde du monoïde $\mathrm{End}(V)$ des applications linéaires de V vers V. Un sous-espace vectoriel V' de V est *stable* sous M si $V'm \subset V'$ pour tout $m \in M$.

Le monoïde M est *irréductible* si $V \neq 0$ et les seuls sous-espaces stables sont 0 et V.

Définition 6.3.1. Un monoïde est *complètement réductible* si chaque sous-espace stable de V admet un espace supplémentaire stable, c'est-à-dire pour chaque sous-espace stable V' de V, il existe un sous-espace stable V'' tel que $V = V' \oplus V''$.

Si V est de dimension finie, alors un sous-monoïde complètement réductible de $\mathrm{End}(V)$ a la forme suivante : il existe une décomposition de V en sous-espaces stables V_i

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$$

tel que les restictions des éléments de M à chaque V_i soit un sous-monoïde irréductible de $\mathrm{End}(V_i)$. Chaque sous-espace stable de V est la somme de au moins un V_i, à M-isomorphisme près. Cette dernière assertion est énoncée dans (PERRIN, 2013) ; on retrouve également une version pour les algèbres semisimples dans (A. H. CLIFFORD et G. B. PRESTON, 1961) et nous verrons par la suite qu'on parle indifféremment de semisimplicité ou de complète réductibilité.
En effet, soit V' un sous-espace stable de V, alors $V = V' \oplus V''$. Puisque les restictions des éléments de M à chaque V_i est un sous-monoïde irréductible de $\mathrm{End}(V_i)$, il est impossible d'avoir $V' \subset V_i$. Le sous-espace V' est donc la somme d'un certain nombre de V_i, prenons $V_1 \oplus \cdots \oplus V_j$ et d'un sous-espace, notons V_c. On a donc $V' = V_1 \oplus \cdots \oplus V_j \oplus V_c$. Or V_c est forcement stable donc il est soit nul, soit égal à un V_i.
Réciproquement, si V est de cette forme, alors M est complètement réductible.

Définition 6.3.2. Soit M un monoïde et V un K-espace vectoriel de dimension finie. Une *représentation linéaire* de M sur V est un morphisme φ de M dans $\mathrm{End}(V)$.

Un sous-espace vectoriel W de V est stable sous φ s'il est stable sous $\varphi(M)$. La représentation est complètement réductible si le monoïde $\varphi(M)$ est complètement réductible. Nous avons le résultat suivant (BERSTEL, J. ; PERRIN, D. ; REUTENAUER C., 2010) :

Théorème 6.3.1. *(Maschke) Une représentation linéaire d'un groupe fini est complètement réductible.*

Démonstration. Soit V un K-espace vectoriel. Il suffit de montrer que chaque sous-groupe fini du monoïde $\mathrm{End}(V)$ est complètement réductible. Soit G un sous-groupe fini de $\mathrm{End}(V)$ et soit W un sous-espace de V stable sous G. Soit W'' un

sous-espace supplémentaire quelconque de W dans V. Soit $\pi : V \to V$ l'application linéaire qui à $\rho \in V$ associe l'unique $\rho'' \in W''$ tel que $\rho = \rho'' + \rho'$, avec $\rho' \in W$. Alors $\pi(\rho) = 0$ pour tout $\rho \in W$ et $\pi(\rho) = \rho$ pour tout $\rho \in W''$. De plus $\rho - \pi(\rho) \in W$ pour tout $\rho \in V$. Soit une application linéaire $\theta : V \to V$ définie comme suit, en prenant $n = \text{Card}(G)$ et pour tout $\rho \in V$:

$$\theta(\rho) = \frac{1}{n} \sum_{g \in G} \pi(\rho g) g^{-1}.$$

Soit $W' = \theta(V)$. Nous allons prouver que W' est un sous-espace de V supplémentaire de W et qui est stable sous G. Dans un premier temps montrons que W' est un sous-espace supplémentaire de W. Soit $\rho \in W$, alors $\rho g \in W$ pour tout $g \in G$, puisque W est stable sous G. Donc $\pi(\rho g) = 0$ et par conséquent

$$\theta(\rho) = 0, \, \forall \rho \in W.$$

Ce qui implique que $W \subseteq \ker(\theta)$. Par ailleurs, nous avons pour tout $\rho \in V$

$$\rho - \theta(\rho) = \rho - \frac{1}{n} \sum_{g \in G} \pi(\rho g) g^{-1} = \frac{1}{n} \sum_{g \in G} \pi(\rho g - \pi(\rho g)) g^{-1}.$$

Or, par définition de π, chaque $\rho g - \pi(\rho g) \in W$ pour $g \in G$ et puisque W est stable sous G, $(\rho g - \pi(\rho g))g^{-1} \in W$ également. D'où

$$\rho - \theta(\rho) \in W, \, \forall \rho \in V.$$

Ce qui entraîne $\ker(\theta) \subseteq W$, car $\rho \in \ker(\theta)$ implique $\rho - \theta(\rho) = \rho$. D'où :

$$W = \ker(\theta).$$

De plus, nous avons $\theta(\rho) - \theta^2(\rho) = \theta(\rho - \theta(\rho))$. Puisque $\rho - \theta(\rho) \in W$, $\theta(\rho) - \theta^2(\rho) = 0$, donc $\theta^2 = \theta$. D'où les sous-espaces $W = \ker(\theta)$ et $W' = \text{im}(\theta)$ sont supplémentaires.

Montrons maintenant que W' est stable sous G. Soient $\rho \in V$ et $h \in G$. Alors nous avons :

$$\theta(\rho)h = \frac{1}{n} \sum_{g \in G} \pi(\rho g) g^{-1} h.$$

L'application de G dans G qui à g associe $k = h^{-1}g$ est bijective donc

$$\theta(\rho)h = \frac{1}{n}\sum_{g\in G}\pi(\rho hk)k^{-1} = \theta(\rho h).$$

D'où W' est stable dans G, ce qui achève notre preuve. □

Une représentation d'une algèbre $\mathfrak{A}$ dans un espace vectoriel V est un morphisme φ de $\mathfrak{A}$ dans l'algèbre $\mathrm{End}(V)$. Elle est *fidèle* si φ est injective. La représentation est réductible (resp. complètement réductible) si $\varphi(\mathfrak{A})$ réductible (resp. complètement réductible).

Soit $\mathfrak{A}$ une K-algèbre et φ une représentation de $\mathfrak{A}$ dans un espace vectoriel V. Alors on vérifie que $(v, x) \mapsto v\varphi(x)$ définit une structure de $\mathfrak{A}$-module sur V. Réciproquement, si V est un $\mathfrak{A}$-module, alors l'application $\varphi : \mathfrak{A} \mapsto \mathrm{End}(V)$ définie par $v\varphi(x) = vx$ est une représentation linéaire de $\mathfrak{A}$ dans V.

Soit $\mathfrak{A}$ une K-algèbre et $e \neq 0$ un idempotent de $\mathfrak{A}$. Nous vérifions que $e\mathfrak{A}e$ est une algèbre et que pour un $\mathfrak{A}$-module V, l'espace Ve est un $e\mathfrak{A}e$-module appelé le *module condensé* de V et e est appelé l'*idempotent de condensation.*

Nous avons ainsi la proposition suivante :

Proposition 6.3.2. *Si V est un $\mathfrak{A}$-module irréductible de dimension finie tel que $Ve \neq 0$, alors Ve est un $e\mathfrak{A}e$-module irréductible.*

Démonstration. Soit W un $e\mathfrak{A}e$-sous-module non-nul de Ve. Alors $W = We$ car e est un idempotent. Notons $W\mathfrak{A}$ le sous-espace généré par les éléments wa avec $w \in W$ et $a \in \mathfrak{A}$. Nous vérifions que $W\mathfrak{A}$ est un $\mathfrak{A}$-module non-nul, ce qui entraine $W\mathfrak{A} = V$ puisque V est irréductible. Donc

$$Ve = (W\mathfrak{A})e = (We\mathfrak{A})e = W(e\mathfrak{A}e) \subset W$$

D'où $W = Ve$. □

Théorème 6.3.3. *Soit $\mathfrak{A}$ une algèbre de dimension finie et $e \in \mathfrak{A}$ un idempotent. Soit V un $\mathfrak{A}$-module de dimension finie. Alors les conditions suivantes sont équivalentes :*

(i) $V = \bigoplus_{i=1}^{m} V_i$ *avec* V_i *des* $\mathfrak{A}$*-modules irréductibles et* $V_i e \neq 0$ *pour* $1 \leq i \leq m$.

(ii) Ve *est complètement réductible comme* $e\mathfrak{A}e$*-module,* $V = Ve\mathfrak{A}$ *et* $\{v \in V | v\mathfrak{A}e = 0\} = 0$

De plus, si la première condition est vérifiée, alors $Ve = \bigoplus_{i=1}^{m} V_i e$ *avec* $V_i e$ *des* $e\mathfrak{A}e$*-modules irréductibles.*

Démonstration. Supposons (i). Alors $Ve = \bigoplus_{i=1}^{m} V_i e$; V_i étant stable, alors $V_i e \subseteq V_i$, ce qui préserve le caractère direct de la somme. D'après la proposition 6.3.2, chaque $V_i e$ est un $e\mathfrak{A}e$-sous-module irréductible de V_i. Donc Ve est complètement réductible. Nous avons également $Ve\mathfrak{A} = \bigoplus_{i=1}^{m} V_i e\mathfrak{A} = V$ parce que $V_i e\mathfrak{A} = V_i$ (car V_i est irréductible). Soit maintenant $W = \{v \in V | v\mathfrak{A}e = 0\}$. Puisque W est stable, il est isomorphe à une somme directe de certains V_i ; mais $We = 0$. Alors $W = 0$ car si $W \neq 0$ celà contredirait le fait que $V_i e \neq 0$, $\forall i$.
Supposons maintenant (ii). Soit V' un sous-espace stable de V. Alors $W' = V'e$ est un sous-espace de Ve stable sous $e\mathfrak{A}e$, donc il a un complément W'' dans Ve stable sous $e\mathfrak{A}e$. Puisque nous avons $V = Ve\mathfrak{A}$ et $Ve = W' + W''$, nous avons

$$V = Ve\mathfrak{A} = W'\mathfrak{A} + W''\mathfrak{A}$$

mais vu que $W'\mathfrak{A} = V'e\mathfrak{A} \subset V'\mathfrak{A} \subset V'$, le premier terme est inclus dans V'. Donc $V'' = W''\mathfrak{A}$, on a $V = V' + V''$. Par ailleurs, si $v \in V' \cap V''$, alors $v\mathfrak{A}e \subset V'\mathfrak{A}e \cap V''\mathfrak{A}e \subset V'e \cap V''e = W' \cap W''$ et donc $v\mathfrak{A}e = 0$ ce qui entraine $v = 0$ (par la dernière assertion de (ii)). Donc $V' \cap V'' = 0$ et ainsi $V = V' \oplus V''$, d'où V est complètement réductible. Soit $V = \bigoplus_{i=1}^{m} V_i$ avec V_i des $\mathfrak{A}$-modules irréductibles. Si $V_i e = 0$, alors tout élément $v \in V_i$ est dans l'ensemble $\{v \in V | v\mathfrak{A}e = 0\}$, ce qui signifierait que $V_i = 0$, qui est contradictoire. □

Nous avons comme conséquence le corollaire :

Corollaire 6.3.4. *Soit $\mathfrak{A}$ une algèbre de dimension finie et $e \in \mathfrak{A}$ un idempotent. Soit V un $\mathfrak{A}$-module de dimension finie tel que Ve soit complètement réductible dans $e\mathfrak{A}e$, $V = Ve\mathfrak{A}$ et $\{v \in V | v\mathfrak{A}e = 0\} = 0$. Alors V est complètement réductible.*

6.4 Ensembles complètement réductibles

Une algèbre $\mathfrak{A}$ est dite *simple* si elle n'a pas d'autres idéaux en dehors de 0 et $\mathfrak{A}$ elle-même. Elle est dite *semisimple* si elle est la somme directe finie d'algèbres simples.

Définition 6.4.1. Une série est *complètement réductible* si sa représentation syntaxique est complètement réductible.

Remarque 6.4.1. La réductibilité complète d'une série équivaut à la semisimplicité de son algèbre syntaxique. De plus, d'après la proposition 6.2.2, si une série S est reconnue par un morphisme dans une algèbre semisimple, alors S est complètement réductible.

Lemme 6.4.1. *Soit $\varphi_1 : \Sigma^* \to \mathrm{End}(V_1)$ et $\varphi_2 : \Sigma^* \to \mathrm{End}(V_2)$ deux morphismes. Soit $V = V_1 \times V_2$. Si φ_1 et φ_2 sont complètement réductibles, alors le morphisme $\varphi : \Sigma \to \mathrm{End}(V)$ défini par $\varphi(w)(v_1, v_2) = (\varphi_1(w)(v_1), \varphi_2(w)(v_2))$ est complètement réductible.*

Démonstration. Puisque V_1 et V_2 sont des sommes directes de composantes irréductibles, il en est de même pour V donc φ est complètement réductible. □

Proposition 6.4.2. *Toute combinaison linéaire de séries complètement réductibles est complètement réductible.*

Démonstration. Si une série S est complètement réductible, alors il est clair que αS est complètement réductible, pour tout $\alpha \in K$. Soit S_1, S_2 des séries complètement réductibles. Pour $i = 1, 2$, soit $\pi_i : \mathfrak{A}_{S_i} \to K$, l'application linéaire définie par $\pi_i(\psi_{S_i}(w)) = (S_i, w)$. Considérons le morphisme $\psi : \Sigma^* \to \mathfrak{A}_{S_1} \times \mathfrak{A}_{S_2}$ défini par $\psi(w) = (\psi_1(w), \psi_2(w))$; ce morphisme reconnaît $S_1 + S_2$ car l'application $\pi : \mathfrak{A}_{S_1} \times \mathfrak{A}_{S_2} \to K$ définie par $\pi(x) = \pi_1(x) + \pi_2(x)$ est linéaire et telle que $\pi(\psi(w)) = (S_1, w) + (S_2, w)$. D'après le lemme 6.4.1, ψ est complètement réductible, d'où $\psi(K\langle\Sigma\rangle)$ est semisimple c'est-à-dire que $S_1 + S_2$ est complètement réductible. □

Nous rappelons que le *résiduel à gauche* de $L \subseteq \Sigma^*$ par $u \in \Sigma^*$ est le quotient $u^{-1}L = \{v \in \Sigma^* | uv \in L\}$. On définit également le résiduel à droite $Lu^{-1} = \{v \in \Sigma^* | vu \in L\}$.

Pour un mot $w = w_1 w_2 \dots w_n$, avec $w_i \in \Sigma$, on apelle *miroir* de w noté $\widetilde{w}$, le mot $\widetilde{w} = w_n \dots w_2 w_1$. Par convention, $\widetilde{\varepsilon} = \varepsilon$. Soit un langage $L \subseteq \Sigma^*$, alors le miroir de L est $\widetilde{L} = \{\widetilde{w} | w \in L\}$.

Définition 6.4.2. La représentation syntaxique (resp. algèbre) d'un ensemble $L \subseteq \Sigma^*$ est la représentation syntaxique (resp. algèbre) de sa série caractéristique. Un ensemble reconnaissable est *complètement réductible* si sa série caractéristique est complètement réductible.

Proposition 6.4.3. *La famille des ensembles complètement réductibles est fermée par miroir.*

Démonstration. Soit L un ensemble complètement réductible et soit (λ, μ, γ) une représentation linéaire de χ_L. Soit $\nu : \Sigma^* \to K^{n \times n}$ le morphisme défini par $\nu(w) = \mu(\widetilde{w})^t$. Alors nous avons :

$$(\chi_{\widetilde{L}}, w) = (\chi_L, \widetilde{w}) = \lambda\mu(\widetilde{w})\gamma = (\lambda\mu(\widetilde{w})\gamma)^t = \gamma^t \nu(w) \lambda^t.$$

Donc $(\gamma^t, \nu, \lambda^t)$ est une représentation linéaire de $\chi_{\widetilde{L}}$. □

Théorème 6.4.4. *La famille des ensembles complètement réductibles est fermée par résiduel, complément et miroir.*

Démonstration. Soit Π la famille des ensembles complètement réductibles. Pour $X \in \Pi$ et $w \in \Sigma^*$, notons $Y = w^{-1}X$. Nous avons alors $\chi_Y = \chi_X \cdot w$ et notons V_{χ_Y} l'espace syntaxique engendré par les $\chi_Y \cdot u = \chi_X \cdot wu$. Puisque V_{χ_Y} est un sous-espace stable de V_{χ_X}, les sous-espaces stables de V_{χ_Y} sont également des sous-espaces stables de V_{χ_X}. Donc la représentation syntaxique de χ_Y est complètement réductible, d'où $Y \in \Pi$. Similairement et en utilisant le fait que la famille des ensembles complètement réductibles est fermée par miroir (proposition 6.4.3), nous demontrons que $Xw^{-1} \in \Pi$.
Soit maintenant $X \in \Pi$ et $Y = \Sigma^* \setminus X$. Puisque Σ^* est complètement réductible, alors, d'après la proposition 6.4.2, la série $\chi_Y = \chi_{\Sigma^*} - \chi_X$ est complètement réductible, donc $Y \in \Pi$. □

Proposition 6.4.5. *Pour tout ensemble reconnaissable L, les ensembles L et $L \cap \Sigma^+$ sont simultanément complètement réductibles.*

Démonstration. Considérons que $\varepsilon \in L$. Soit $Y = L \cap \Sigma^*$; puisque $\chi_Y = \chi_L - 1$ alors nous avons le résultat d'après la proposition 6.4.2. □

Proposition 6.4.6. *Si $L \subseteq \Sigma^*$ est complètement réductible, alors le monoïde syntaxique de L a une représentation fidèle complètement réductible.*

Démonstration. Résulte directement de la proposition 6.2.3. □

Nous rappelons que, d'après la remarque 6.4.1, la réductibilité complète de la représentation du monoïde syntaxique équivaut à la semisimplicité de son algèbre. On a alors une condition suffisante de complète réductibilité :

Proposition 6.4.7. *Si l'algèbre du monoïde syntaxique d'un ensemble $L \subseteq \Sigma^*$ est semisimple, alors L est complètement réductible.*

Démonstration. D'après la proposition 6.2.3 l'algèbre syntaxique de L est un quotient de l'algèbre $K\langle M(L)\rangle$, avec $M(L)$ le monoïde syntaxique de L. Ce qui, par conséquence prouve la proposition. □

6.4.1 Ensembles birécurrents

Définition 6.4.3. Un langage $X \subseteq \Sigma^*$ est un *code* si chaque mot dans X^* peut s'écrire *de manière unique* comme une concaténation de mots de X ; autrement dit si pour tout $n, m \geq 1$ et pour tous $x_1, \ldots, x_n, x'_1, \ldots, x'_m \in X$, la condition

$$x_1 \cdots x_n = x'_1 \cdots x'_m$$

entraîne $n = m$ et $x_i = x'_i$ pour $1 \leq i \leq n$.

Il est clair qu'un code ne contient pas le mot vide ε et que tout sous-ensemble d'un code est un code ; en particulier, l'ensemble vide est un code.

Exemple 6.4.1. L'ensemble $X = \{a, ab, ba\}$ sur $\Sigma = \{a, b\}$ n'est pas un code car le mot $w = aba$ a deux factorisations distinctes :

$$a = (ab)a = a(ba).$$

Exemple 6.4.2. Sur un alphabet à une seule lettre a, tout sous-ensemble de a^* est un code si et seulement s'il est un singleton différent de ε.

Définition 6.4.4. Un sous-ensemble $X \subseteq \Sigma^*$ est un *code préfixe* (resp. *suffixe*) si aucun mot de X n'est préfixe (resp. suffixe) propre d'un autre mot de X, autrement dit, si pour tout $u, v \in \Sigma^*$, $u \in X$ et $uv \in X$ (resp. $vu \in X$) entraîne $v = \varepsilon$. Un code qui est à la fois préfixe et suffixe est dit *bifixe*.

Il est clair qu'un code X est suffixe si et seulement si son miroir $\widetilde{X}$ est préfixe.

Soit M un monoïde et M' un sous-monoïde de M. Alors M' est *unitaire droit* dans M si pour tout $u, v \in M$,

$$u, uv \in M' \Rightarrow v \in M'.$$

Symétriquement, M' est *unitaire gauche* si pour tout $u, v \in M$,

$$u, vu \in M' \Rightarrow v \in M'.$$

Nous pourrions aussi dire que M' est unitaire droit si et seulement si $M'^{-1}M' = M'$, et M' est unitaire gauche si $M'M'^{-1} = M'$. Un sous-monoïde M' de M est *biunitaire* s'il est à la fois unitaire gauche et unitaire droit.

Nous avons alors

Proposition 6.4.8. *Un sous-monoïde M de Σ^* est engendré par un code préfixe (resp. suffixe, bifixe) si et seulement s'il est unitaire droit (resp. unitaire gauche, biunitaire). En particulier, un sous-monoïde de Σ^* unitaire droit (resp. unitaire gauche, biunitaire) est libre.*

Démonstration. Soit $M \subseteq \Sigma^*$ un sous-momoïde, $Q = M \setminus \varepsilon$ et $X = Q \setminus Q^2$ son ensemble génerateur minimal. Supposons M unitaire droit. Soit $x, xu \in X$ pour $u \in \Sigma^*$. Alors $x, xu \in M$ et donc $u \in M$. Si $u \neq \varepsilon$, alors $u \in Q$; mais alors $xu \in Q^2$ contredit notre hypothèse. D'où $u = \varepsilon$ et X est préfixe.
Réciproquement, supposons X préfixe. Soit $u, v \in \Sigma^*$ tel que $u, uv \in M = X^*$. Alors $u = x_1 \cdots x_n$, et $uv = y_1 \cdots y_m$ pour $x_1, \ldots, x_n, y_1, \ldots, y_m \in X$. Par conséquent

$$x_1 \cdots x_n v = y_1 \cdots y_m.$$

Puisque X est préfixe, ni x_1, ni y_1 n'est préfixe l'un de l'autre, donc $x_1 = y_1$ et ainsi de suite et nous avons $x_2 = y_2, \ldots x_n = y_n$. Nous avons alors $m \geq n$ et $v = y_{n+1} \cdots y_m \in M$ d'où M est unitaire droit. □

Définition 6.4.5. Un langage non vide X est dit *récurrent* si son automate minimal est fortement connexe et *birécurrent* si X et $\widetilde{X}$ sont récurrents.

Proposition 6.4.9. *Le sous-monoïde engendré par un code préfixe est récurrent.*

Démonstration. Soit X un code préfixe. D'après la proposition précédente (proposition 6.4.8), le sous-monoïde engendré par X est unitaire droit c'est-à-dire pour tout mots u, v si $u, uv \in X^*$, alors $v \in X^*$. Ceci implique que pour tout $x \in X^*$, nous avons $x^{-1}X^* = X^*$. Alors l'automate minimal de X^* est de la forme $\mathcal{A} = (\Sigma, Q, i, \delta, i)$ où l'ensemble des états finaux est réduit à l'état initial. Puisque $\mathcal{A}$ est émondé, alors $\mathcal{A}$ est fortement connexe. □

Corollaire 6.4.10. *Le sous-monoïde engendré par un code bifixe est birécurrent.*

Automate miroir accessible

Définition 6.4.6. Soit $\mathcal{A} = (\Sigma, Q, i, \delta, F)$ un automate. L'automate *miroir accessible* de $\mathcal{A}$, noté $\widetilde{\mathcal{A}}$, est l'automate obtenu en :

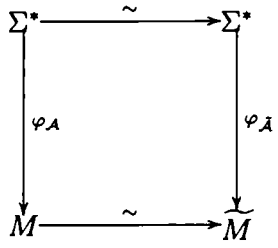
(i) inversant les arêtes de $\mathcal{A}$,

(ii) construisant un automate accessible en utilisant F comme état initial et les ensembles contenant i comme états finaux.

Nous avons alors $\widetilde{\mathcal{A}} = (\Sigma, \widetilde{Q}, F, \delta', J)$ où
- $\widetilde{Q}$ est la famille des ensembles non vides de la forme $w^{-1}F = \{q \in Q | q \cdot w \in F\}$
- $J = \{U \in \widetilde{Q} | i \in U\}$

Cet automate reconnaît $\widetilde{X}$. En effet, $y \in \widetilde{X} \Leftrightarrow i \cdot \widetilde{y} \in F$ et $i \cdot \widetilde{y} \in F \Leftrightarrow i \in F \cdot y$. Soit $M = \varphi_{\mathcal{A}}(\Sigma^*)$ et $\widetilde{M} = \varphi_{\widetilde{\mathcal{A}}}(\Sigma^*)$ les monoïdes de transitions respectifs de $\mathcal{A}$ et $\widetilde{\mathcal{A}}$. Il existe un anti-isomorphisme $m \mapsto \widetilde{m}$ tel que le diagramme ci-dessous est

commutatif :



En particulier, nous avons, pour tout mot w, $m = \varphi_{\mathcal{A}}(w)$ si et seulement si $\widetilde{m} = \varphi_{\widetilde{\mathcal{A}}}(\widetilde{w})$. L'action à gauche de M sur $\widetilde{Q}$, définie par $mU = V$ si $V = \{q \in Q | qm \in U\}$ est telle que :

$$mU = V \Leftrightarrow U\widetilde{m} = V \tag{6.2}$$

En effet,

$$(mm')U = V = \{q \in Q | q \cdot (mm') \in U\} = \{q \in Q | (q \cdot m) \cdot m' \in U\}$$

donc $(mm')U = m(m'U)$, ce qui prouve qu'on a une action à gauche.

Proposition 6.4.11. *Si $\mathcal{A}$ est un automate émondé reconnaissant X, alors $\widetilde{\mathcal{A}}$ est l'automate minimal de $\widetilde{X}$.*

Démonstration. Puisque $\mathcal{A}$ est émondé, pour tout mot w, nous avons

$$w^{-1}F \neq \emptyset \Leftrightarrow Xw^{-1} \neq \emptyset.$$

En effet, $w^{-1}F \neq \emptyset$ équivaut au fait qu'il existe des états dans $\mathcal{A}$ qui sont atteints par des mots v tels que $vw \in X$, autrement dit que Xw^{-1} est non-vide.
En outre, nous vérifions aisément que pour tout $w, w' \in \Sigma^*$,

$$w^{-1}F = w'^{-1}F \Leftrightarrow Xw^{-1} = Xw'^{-1}.$$

Puisque les ensembles non vides Xw^{-1} sont miroirs des états de l'automate minimal de $\widetilde{X}$, alors l'application $w^{-1}F \mapsto \widetilde{w}^{-1}\widetilde{X}$ est bijective et de ce fait, $\widetilde{\mathcal{A}}$ est l'automate minimal de $\widetilde{X}$. □

Réductibilité des ensembles birécurrents

Nous abordons cette section par les deux propositions suivantes :

Proposition 6.4.12. *Soit $\mathcal{A} = (\Sigma, Q, i, \delta, F)$ l'automate minimal d'un ensemble X. Soit $S = \chi_X$, $\tilde{S} = \chi_{\tilde{X}}$ et $\varphi = \varphi_{\mathcal{A}}$. Pour tout mot $w \in \Sigma^*$, on a*

(i) *$i\varphi(w) = i$ si et seulement si $S \cdot w = S$;*

(ii) *$\varphi(w)F = F$ si et seulement si $\tilde{S} \cdot \tilde{w} = \tilde{S}$.*

Démonstration. (i) Supposons $i \cdot w = i$. Alors, pour tout $u \in \Sigma^*$,

$$(S \cdot w, u) = 1 \Leftrightarrow wu \in X \Leftrightarrow i \cdot wu \in F \Leftrightarrow i \cdot u \in F \Leftrightarrow (S, u) = 1.$$

Donc $S \cdot w = S$. Réciproquement, si $S \cdot w = S$, alors pour tout $u \in \Sigma^*$,

$$i \cdot wu \in F \Leftrightarrow (S, wu) = 1 \Leftrightarrow (S \cdot w, u) = 1 \Leftrightarrow (S, u) = 1 \Leftrightarrow i \cdot u \in F$$

ce qui entraîne $w^{-1}X = X$, qui, d'après la définition de l'automate minimal, nous donne $i \cdot w = i$.

La démonstration du (ii) est analogue, en utilisant le fait que, d'après l'équation 6.2,

$$\varphi(w)F = F \Leftrightarrow F \cdot \tilde{w} = F$$

dans l'automate $\tilde{\mathcal{A}}$. □

Proposition 6.4.13. *Soit $\mathcal{A} = (\Sigma, Q, i, \delta, F)$ l'automate minimal d'un ensemble birécurrent X. Soit $\varphi = \varphi_{\mathcal{A}}$ et $M = \varphi(\Sigma^*)$. Le monoïde M contient un idempotent e tel que :*

(i) *$ie = i$ et $eF = F$*

(ii) *L'ensemble eMe est l'union d'un groupe fini G et d'un élément 0, si $0 \in M$.*

Démonstration. Supposons que M contienne un zéro. D'après la proposition 6.1.1, le monoïde M contient un unique idéal 0-minimal D qui est une $\mathcal{D}$-classe régulière. Soit w un mot tel que $\varphi(w) \in D$. Puisque $\mathcal{A}$ est fortement connexe, il existe un mot u tel que $i \in Q \cdot wu$. Posons $w' = wu$ et donc $\varphi(w') \in D$.
Ensuite, puisque $\widetilde{\mathcal{A}}$ est fortement connexe, il existe v tel que $F \cdot \widetilde{w'}v = F$ et donc $\varphi(\widetilde{v}w')F = F$ d'après l'équation 6.2. Alors $\varphi(\widetilde{v}w') \in D$ car D est un idéal et $\varphi(w') \in D$. Puisque $\varphi(\widetilde{v}w')F = F$, il est impossible d'avoir $\varphi(\widetilde{v}w')^2 = 0$ donc il existe une puissance de $\widetilde{v}w'$, notons x tel que $e = \varphi(x)$ soit un idempotent.
Puisque $i \in Q \cdot w'$, i est dans l'image de e ($Q \cdot w'$ étant dans $Q \cdot \varphi(\widetilde{v}w')^r = Q \cdot e$, avec $x = (\widetilde{v}w')^r$) et donc $ie = i$, vu que e est un idempotent. Nous avons aussi $eF = F$ car $\varphi(\widetilde{v}w')F = F \Rightarrow \varphi(\widetilde{v}w')^r F = eF = F$. En plus, les éléments non nuls du groupe eMe forment le groupe de la $\mathcal{D}$-classe. □

Nous avons maintenant tous les outils nécessaires pour énoncer et démontrer le résulat principal de cette section sur la réductibilité des ensembles birécurrents ; théorème dû à Dominique Perrin dans (PERRIN, 2013).

Théorème 6.4.14. *Les ensembles birécurrents sont complètement réductibles.*

Démonstration. Soit X un ensemble birécurrent, $S = \chi_X$ et $\mathcal{A} = (\Sigma, Q, i, \delta, F)$ l'automate minimal de X.
Soit $\varphi = \varphi_{\mathcal{A}}$ et $\psi = \psi_S$. D'après la proposition 6.4.13, il existe un mot $x \in \Sigma^*$ tel que $\varphi(x)$ soit un idempotent, $i\varphi(s) = i$ et $\varphi(x)F = F$ et tel que $\varphi(x\Sigma^* x)$ soit l'union d'un groupe fini et de 0 (si $0 \in \varphi(\Sigma^*)$).
Posons $M = \psi(\Sigma^*)$ et $e = \psi(\Sigma^*)$. D'après la proposition 6.2.3, e est un idempotent de M tel que eMe est l'union de 0 (si $0 \in M$) et d'un groupe fini. De plus, d'après la proposition 6.4.12, nous avons pour tout $u \in \Sigma^*$, $(S, u) = (S, ux) = (S, xu)$.
Posons également $V = V_S$ et prenons une base de V. Nous pouvons considérer M comme un monoïde de $n \times n$-matrices et V comme un espace vectoriel de

vecteurs-lignes de taille n. Soit λ le vecteur-ligne de taille n représentant S et soit γ le vecteur-colonne de taille n tel que, pour tout $w \in \Sigma^*$, $(S, w) = \lambda\psi(w)\gamma$.
Soit $\mathfrak{A}$ l'algèbre engendrée par M. Alors V est un $\mathfrak{A}$-module de dimension finie. Pour la démonstration du théorème, nous allons vérifier que les conditions du corollaire 6.3.4 sont satisfaites par $\mathfrak{A}$, V et e.
Dans un premier temps, puisque $e\mathfrak{A}e$ est l'algèbre engendrée par eMe, alors, d'après le théorème de Maschke (théorème 6.3.1), Ve est complètement réductible sur $e\mathfrak{A}e$. Ensuite, puisque $i\varphi(x) = i$, nous avons, $\lambda e = \lambda$ d'apres la proposition 6.4.12. Puisque V est engendré par les vecteurs λm, $m \in M$, il est donc engendré par l'ensemble λeM. D'où $V = Ve\mathfrak{A}$.
Soit maintenant W l'espace des vecteurs-colonnes de taille n. De manière symétrique au cas de V, W est engendré par les éléments $m\gamma$, $m \in M$. D'après le (ii) de la proposition 6.4.12, puisque $\varphi(x)F = F$, nous avons $e\gamma = \gamma$. Alors W est engendré par les éléments de l'ensemble $Me\gamma$, ce qui implique que $W = \mathfrak{A}eW$. De plus, nous avons $v\mathfrak{A}e = 0 \Leftrightarrow v\mathfrak{A}eW = 0$ et alors $\{v \in V | v\mathfrak{A}e = 0\}$ est l'espace orthogonal à l'espace engendré par $\mathfrak{A}eW$. D'où $\{v \in V | v\mathfrak{A}e = 0\} = 0$. La deuxième condition est ainsi satisfaite.
D'après le corollaire 6.3.4, nous concluons que le monoïde M est complètement réductible, ce qui achève notre démonstration. □

Ce théorème a pour conséquence le résultat suivant, dû à Chistophe Reutenauer dans (REUTENAUER, 1981).

Corollaire 6.4.15. *Le sous-monoïde engendré par un code bifixe reconnaissable est complétement réductible.*

RÉFÉRENCES

A. H. CLIFFORD et G. B. PRESTON. (1961). *The Algebraic Theory Of Semigroups.* American Mathematical Society.

AUTEBERT, J.-M. (1994). *Théorie des langages et des automates.* MASSON.

BERSTEL, J.; PERRIN, D.; REUTENAUER C. (2010). *Codes and automata.* Cambridge University Press.

EILENBERG, S. (1974). *Automata, Languages, and Machines.*, volume A. Academic Press.

LAWSON, M. V. (2004). *Finite Automata.* Chapman & Hall/CRC.

PERRIN, D. (2013). Completely reducible sets. *International Journal of Algebra and Computation, 23 (4)*, 915–942.

PIN, J.-E. (1984). *Variétés de langages formels.* MASSON.

REUTENAUER, C. (1981). Semisimplicity of the algebra associated to a biprefix code. *Semigroup Forum, 23*, 327–342.

SCHÜTZENBERGER, M. P. (1965). On finite monoids having only trivial subgroups. *Information And Control, 8*, 190–194.