الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique Et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère De L'enseignement Supérieur et de la Recherche Scientifique

Université Mohamed Boudiaf M'sila
Faculté des mathématiques et de L'informatiques
- Département de mathématiques *-*

جامعة محمد بوضياف بالمسيلة
كلية الرياضيات والإعلام الآلي
-*قسم الرياضيات*-

N° d'ordre :

THESE

Présentée pour l'obtention du diplôme de

Doctorat en sciences

Spécialité : Mathématiques

Par

Nacer GHADBANE

Thème

Systèmes de réécriture et le problème du mot dans un monoïde

Soutenu publiquement, le **23/01/2017** devant le jury composé de :

Mr. Hocine BELOUADAH	Prof.	Université de M'sila	Président
Mr. Douadi MIHOUBI	Prof.	Université de M'sila	Rapporteur
Mr. Abdelaziz AMROUNE	Prof.	Université de M'sila	Examinateur
Mr. Abdelouaheb MOUSSAOUI	Prof.	Université de Sétif	Examinateur
Mr. Lemnaour NOUI	Prof.	Université de Batna	Examinateur
Mr. Mokhtar HAFAYED	M.C.A.	Université de Biskra	Examinateur
Mr. Abdelmadjid BOUDAOUD	Prof.	Université de M'sila	Invité

2016/2017

ملخص الأطروحة باللغة العربية

في هذه الأطروحة نهتم بدراسة نصف أنظمة إعادة كتابة الكلمات (Σ,R) تسمى أيضا نصف أنظمة Thue و مسألة الكلمة في نصف زمرة حرة حيث Σ مجموعة منتهية كيفية و R علاقة ثنائية معرفة على نصف الزمرة الحرة Σ* من بين خصائص أنظمة إعادة الكتابة خاصية الانتهاء التى تعني عدم وجود سلسلة لانهائية في حساب ما وخاصية الإغلاق التى تبرر وحدانية النتيجة رغم تعدد طرق الحساب. في هذا العمل قمنا بإعطاء عدة معايير للحصول على أنظمة إعادة كتابة منتهية كما تناولنا عدة تطبيقات حول أنظمة إعادة الكتابة و مسألة الكلمة في نصف زمرة حرة وهي كمايلى:

1) تشكيل بعض الشفرات الزمرية.

2) تمثيل بعض نصف الزمر والزمر بواسطة مولدات وعلاقات.

3) بعض الملاحظات حول نظام تشفير اساسه مسألة الكلمة في نصف الزمرة الحرة.

4) اللغات المولدة بنصف أنظمة Thue .

5) استعمال أساسيات Gröbner في نصف أنظمة Thue .

الكلمات الافتتاحية: نصف الزمرة الحرة, تماثل نصف الزمرة الحرة, نصف أنظمة Thue, أساسيات Gröbner, أنظمة التشفير ذات المفاتيح المعلنة.

RESUME

Notre recherche dans cette thèse se situe dans le cadre de semi-systèmes de réécriture dit aussi semi-système de Thue et le problème du mot dans un monoïde. Un semi-système de réécriture est un couple $(\Sigma, \mathcal{R})$ où Σ est un alphabet et $\mathcal{R}$ est un ensemble fini de couples de mots sur Σ, i.e, $\mathcal{R} \subseteq \Sigma^* \times \Sigma^*$ où Σ^* est le monoïde libre engendré par Σ muni de l'opération la concaténation des mots.

L'étude des propriétés des semi-systèmes de réécriture forme un domaine très important depuis de nombreuses années. Parmi les propriétés les plus étudiées et les plus importantes des semi-systèmes de réécriture se trouvent la terminaison qui assure l'existence d'un résultat à un calcul et la confluence qui nous permet de garantir l'unicité de ce résultat.

Dans ce travail on donne des critères pour assurer la propriété de terminaison dans les deux cas suivants:
Dans le premier cas, on utilise un morphisme non contractant entre le semi-système $(\Sigma, \mathcal{R})$ en question et un autre semi-système possédant déjà cette propriété. Dans le second cas, on utilise une fonction poids entre le semi-système $(\Sigma, \mathcal{R})$ et un ensemble muni d'un ordre bien fondé.

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture. La congruence $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ engendrée par $\mathcal{R}$ est définie par:

- $w \underset{\mathcal{R}}{\Longleftrightarrow} w'$, s'il existe x, y de Σ^* et $(r, s) \in (\mathcal{R} \cup \mathcal{R}^{-1})$ tels que $w = xry$ et $w' = xsy$,
- $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w'$, s'il existe une suite finie de mots $u_0, u_1, ..., u_n$ de Σ^* avec,

$$u_0 = w, u_i \underset{\mathcal{R}}{\Longleftrightarrow} u_{i+1}, \forall 0 \leq i \leq n-1 \text{ et } u_n = w'.$$

Une présentation (par générateurs et relations) d'un monoïde M est la donnée d'un alphabet Σ et d'une relation binaire $\mathcal{R}$ sur Σ^* tels que M soit isomorphe au quotient de Σ^* par la congruence notée $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ engendré par $\mathcal{R}$, i.e, $M \cong \Sigma^* / \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$.

Etants données deux semi-systèmes de réecriture $(\Sigma_1, \mathcal{R}_1)$ et $(\Sigma_2, \mathcal{R}_2)$. Nous avons déterminé quelques conditions sur les relations $\mathcal{R}_1$ et $\mathcal{R}_2$ qui permettent d'assurer l'existence d'un morphisme entre les monoïdes $\Sigma_1^* / \overset{*}{\underset{\mathcal{R}_1}{\Longleftrightarrow}}$ et $\Sigma_2^* / \overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}}$ pour assurer le passage entre les deux

monoïdes quotients. D'autre part, on donne une relation spécifique $\mathcal{R}$ sur Σ^* qui fait du monoïde quotient $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ un groupe.

Le problème du mot dans un monoïde libre qu'on peut formuler comme suit : Etant donnés le semi-système de réécriture $(\Sigma, \mathcal{R})$ et les deux mots w, w' de Σ^* , déterminer si on peut dériver w' à partir de w en utilisant la congruence engendré par $\mathcal{R}$, c'est-à-dire $w\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}w'$. Ce problème est connu qu'il est en général indécidable.

Enfin, on s'intéresse au protocole ATS-monoïde , l'idée de ce protocole est de transformer un semi-système de Thue $(\Sigma, \mathcal{R})$ pour lequel le problème du mot est indécidable en un semi-système de Thue $(\Delta, \mathcal{R}_\theta)$ où $\theta \subseteq \Delta \times \Delta$ pour lequel le problème du mot est décidable en temps linéaire. Plus précisément, on donne des attaques contre ATS-monoïde dans des cas spécifiques et quelques exemples sur ces cas.

MOTS CLES : Monoïde libre, semi-systèmes de réécriture de mots (semi-système de Thue), morphisme de monoïdes, la fermeture d'une relation binaire, ordre bien fondé, problème du mot dans un monoïde, cryptographie à clé publique, les bases de Grôbner.

ABSTRACT

Our research in this thesis is in the rewriting system framework and the word problem in a monoid. A rewriting system is a pair $(\Sigma, \mathcal{R})$ where Σ is an alphabet and $\mathcal{R}$ is a finite set of pairs of words over Σ.

The study of the properties of rewriting systems form a very important area for many years. Among the most studied and most important properties of rewriting systems are termination that ensures the existence of a result to a calculation and the confluence that allows us to guarantee the uniqueness of this result.

In this work we give criteria to ensure the termination property in the following two cases:
In the first case, we use a non-contracting morphism between the system $(\Sigma, \mathcal{R})$ in question and another system already has this property. In the second case, we use a weight function between the system $(\Sigma, \mathcal{R})$ and a set with an well-founded ordering.

Let Σ^* be the free monoid over a finite alphabet Σ and $\mathcal{R}$ a binary relation on Σ^*. The congruence generated by $\mathcal{R}$ is defined as follows :

- $xry \underset{\mathcal{R}}{\Longleftrightarrow} xsy$, whenever $x, y \in \Sigma^*$ and $r\mathcal{R}s$ or $s\mathcal{R}r$,
- $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w'$, whenever $u_0, u_1, ..., u_n \in \Sigma^*$ with,$u_0 = w, u_i \underset{\mathcal{R}}{\Longleftrightarrow} u_{i+1}, \forall 0 \leq i \leq n-1, u_n = w'$.

A presentation (by generators and relations) of a monoid M is a pair $S = (\Sigma, \mathcal{R})$ such that M is isomorphic to the quotient of Σ^* by the congruence noted $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ generated by R, i.e, $M \cong \Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$. We consider two systems of rewriting $S_1 = (\Sigma_1, \mathcal{R}_1)$ and $S_2 = (\Sigma_2, \mathcal{R}_2)$. The purpose of this study is to determine some conditions on the relations $\mathcal{R}_1$ and $\mathcal{R}_2$ that ensure the existence of a morphism between the quotient monoids $\Sigma_1^*/\overset{*}{\underset{\mathcal{R}_1}{\Longleftrightarrow}}$ and $\Sigma_2^*/\overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}}$. We give also a specific relation $\mathcal{R}$ on Σ^* making the quotient monoid $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ a group.

The word problem in the system $(\Sigma, \mathcal{R})$ is to determine for all words u, v of Σ^* if we have $u \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} v$.

Finally, we are interested in ATS-monoid protocol (proposed by P. J. Abisha, D. G. Thomas and K. G. Subramanian) the idea of this protocol is to transform a system of Thue

$S_1 = (\Sigma, \mathcal{R})$ for which the word problem is undecidable a system of Thue $S_2 = (\Delta, \mathcal{R}_\theta)$ or $\theta \subseteq \Delta \times \Delta$ for which the word problem is decidable in linear time. Specifically, it gives attacks against ATS monoid in spésifiques case and thenme examples of these cases.

KEY WORDS : Free monoid, word rewriting systems (Thue System), morphism of monoids,the closure of a binary relation, well-founded, the word problem in a monoid, public key cryptography, Grôbner bases.

UNIVERSITE DE MOHAMED BOUDIAF DE M'SILA

THESE

Présentée pour obtenir le grade de docteur

Spécialité : Mathématiques

Nacer Ghadbane

Systèmes de réécriture et le problème du mot dans un monoïde

Devant le Jury:

Mr. Hocine BELOUADAH	Prof.	Université de M'sila	Président
Mr. Douadi MIHOUBI	Prof.	Université de M'sila	Rapporteur
Mr. Abdelaziz AMROUNE	Prof.	Université de M'sila	Examinateur
Mr. Abdelouaheb MOUSSAOUI	Prof.	Université de Sétif	Examinateur
Mr. Lemnaour NOUI	Prof.	Université de Batna	Examinateur
Mr. Mokhtar HAFAYED	M.C.A.	Université de Biskra	Examinateur
Mr. Abdelmadjid BOUDAOUD	Prof.	Université de M'sila	Invité

Remerciements

Je tiens à exprimer ma reconnaissance et gratitude à M^{er}. Douadi MIHOUBI, pour avoir accepté de diriger ce travail de thèse ainsi que pour ses conseils et son dynamisme.

Je remercie les membres du jury qui ont accepté de juger mon travail.
M^{er}. Hocine BELOUADAH, que me fait l'honneur de présider ce jury,
M^{ers}. Abdelaziz AMROUNE, Abdelouaheb MOUSSAOUI, Lemnaour NOUI, Mokhtar HAFAYED, Abdelmadjid BOUDAOUD pour avoir accepté d'être examinateurs de cette thèse et pour l'intérêt qu'ils lui ont porté.

Je ne peux oublier de remercier le professeur Yves LAFONT du l'institut de mathématique de Luminy, Marseille, France, pour son soutien, sa gentillesse durant mon stage.

Je voudrais exprimer ici, ma reconnaissance à tous ceux qui se sont impliqués dans ce travail, directe ou indirectement. Les responsables de l'université de M'sila pour la chance qu'ils m'ont donné de faire des stages à l'étranger.

Enfin, il me reste à remercier ma famille et mes amis pour leur soutien pendant ces six années.

Notations

Σ : alphabet fini

Σ^* : monoïde libre sur Σ

$\mathcal{R}$: relation binaire sur Σ^*

$|w|$: la longueur du mot w

$|w|_\sigma$: le nombre d'occurence de la lettre σ dans le mot w

$(\Sigma, \mathcal{R})$: un semi-système de réécriture de mots

$IRR(w)$: le mot irréductible de w

L : langage sur l'alphabet Σ

$\mathcal{R}^0$: la relation d'identité

$\rceil(\mathcal{R})$: le complémentaire de la relation $\mathcal{R}$

$\mathcal{R}^n$: la $n-ième$ composition de $\mathcal{R}$

$\mathcal{R}^r$: la fermeture réflexive de $\mathcal{R}$

$\mathcal{R}^s$: la fermeture symétrique de $\mathcal{R}$

$\mathcal{R}^+$: la fermeture transitive de $\mathcal{R}$

$\mathcal{R}^*$: la fermeture réflexive et transitive de $\mathcal{R}$

$\mathcal{R}^{rst}$: la fermeture d'équivalence de $\mathcal{R}$

$\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$: la congruence engendré par $\mathcal{R}$

$[w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$: la classe d'équivalence de w modulo $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$

$\Sigma^* \diagup \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$: le monoïde quotient

$\cong$: isomorphe

$\geq$: ordre bien fondé

$>$: ordre strict

$\preceq$: ordre lexicographique

$L(\Gamma, \mathcal{R})$: langage engendré par un semi-système de réécriture

$\varphi(n)$: indicateur d'Euler

$C(n)$: complexité d'un algorithme

$Hom(\Sigma^*, \Delta^*)$: l'ensemble des morphismes de Σ^* vers Δ^*

$Iso(\Sigma^*, \Delta^*)$: l'ensemble des isomorphismes de Σ^* vers Δ^*

Introduction

La réécriture est utilisée depuis l'antiquité, bien que nos ancêtres en aient fait sans le savoir, mais son étude formelle ne date que du vingtième siècle. Elle comprend des aspects pratiques et théoriques.

Nous illustrons ici l'aspect pratique de la réécriture à l'aide de quelques exemples élémentaires. L'utilisation la plus courante de la réécriture est la fonction recherher/remplacer présente dans tout éditeur de texte. Cette fonction permet de décrire un semi-système de réécriture très simple qui remplace (réécrit) le mot à rechercher par celui donné comme remplaçant. Un deuxième exemple est celui de la classe des logiciels dits compilateurs qui réécrivent les programmes d'un formalisme dans un autre.

Remarquons que toute personne pratique quotidiennement la réécriture lorsqu' elle effectue des calculs. Si nous désirons connaître la valeur de $8 \times 5 + 6 \times 10$, nous commençons par évaluer les expressions 8×5 et 6×10 puis nous remplaçons ces expressions par leurs valeurs respectives, obtenant ainsi $40 + 60$, avant d'évaluer cette dernière expression et de trouver 100. L'opération consistant à remplacer l'expression 8×5 par sa valeur 40 est l'application de la règle de réécriture $8 \times 5 \longrightarrow 40$ à l'expression $8 \times 5 + 6 \times 10$.
Mais la réécriture n'est pas seulement un outil pratique, c'est aussi un outil théorique dans le domaine de l'informatique (modélisation de programmes ou de langages de programmation) que dans celui de la logique formelle.

L'étude des propriétés des semi-systèmes de réécriture forme un domaine très important depuis de nombreuses années. Parmi les propriétés les plus étudiées et les plus importantes des semi-systèmes de réécriture se trouvent la terminaison qui assure l'existence d'un résultat à un calcul et la confluence qui nous permet de garantir l'unicité de ce résultat. Ainsi, dans le cas du semi- système de réécriture:

$$(\mathcal{R}) \begin{cases} 8 \times 5 \longrightarrow 40 \\ 6 \times 10 \longrightarrow 60 \\ 40 + 60 \longrightarrow 100 \end{cases}$$

La terminaison de ce semi-système garantit que, pour toute expression arithmétique, on ne peut effectuer qu'un nombre fini d'opérations. Il existe cependant deux manières de conduire les calculs pour obtenir 100 à partir de l'expression $8 \times 5 + 6 \times 10$ à l'aide du semi-système

($\mathcal{R}$). Nous pouvons obtenir la séquence de réduction $8 \times 5 + 6 \times 10 \longrightarrow 40 + 6 \times 10 \longrightarrow 40 + 60 \longrightarrow 100$ ou bien la séquence $8 \times 5 + 6 \times 10 \longrightarrow 8 \times 5 + 60 \longrightarrow 40 + 60 \longrightarrow 100$. La confluence garantit que, quelle que soit la manière de conduire les calculs, nous obtiendrons bien le même résultat.

Toutefois ces deux propriétés sont dites indécidables : il n'est pas possible de trouver un algorithme prenant en entrée un semi-système de réécriture et rendant vrai si et seulement si ce semi-système termine sur toute expression, ou conflue sur toute expression dans le second cas.

L'un des enjeux de l'étude des semi-systèmes de réécriture devient alors la recherche de critères simples à vérifier, dans notre cas syntaxiques, permettant de garantir ces propriétés.

L'idée centrale de la réécriture est d'imposer une direction dans l'utilisation des axiomes, qui sont alors orientés en règles de réécriture.
Par exemple le système ci-dessous modélise les groupes non commutatifs suivant la définition mathématique usuelle :

$$\begin{cases} (x.y).z =_A x.(y.z) \ldots\ldots (A) \text{ (l'associativité)}, \\ x.e =_N x \ldots\ldots\ldots (N) \text{ (e l'élément neutre)}, \\ x.x^{-1} =_S e \ldots\ldots\ldots (S) \text{ (x^{-1} l'inverse de x)}. \end{cases}$$

Où $=_i, i \in \{A, N, S\}$ désigne l'utilisation de la règle (i). Avec les égalités précédentes, il est possible de monter que $e^{-1} = e$ grâce aux étapes suivantes :

$$\begin{aligned} e^{-1} =_N e^{-1}.e =_I e^{-1}(e^{-1}(e^{-1})^{-1}) =_A (e^{-1}.e^{-1})(e^{-1})^{-1} =_{N,I} (e^{-1}.e^{-1})(e^{-1}.(e.e^{-1}))^{-1} \\ =_A (e^{-1}.e^{-1})((e^{-1}.e).e^{-1})^{-1} =_N (e^{-1}.e^{-1})(e^{-1}.e^{-1})^{-1} =_I e \end{aligned}$$

La transformation de l'ensemble d'égalités en semi-système de réécriture soulève plusieurs problèmes,

$$\begin{cases} (x.y).z \longrightarrow x.(y.z) \ldots\ldots\ldots (A) \\ x.e \longrightarrow x \ldots\ldots\ldots (N) \\ x.x^{-1} \longrightarrow e \ldots\ldots\ldots (I) \end{cases}$$

Tout d'abord, il n'est plus possible de montrer que $e^{-1} = e$.

La réécriture peut apporter une réponse partielle au problème de mots dans un monoïde : on utilise ici le fait que la réécriture est un calcul de formes normales. En effet, supposons que $(\Sigma, \mathcal{R})$ soit une présentation convergente. Alors, pour tout $u \in \Sigma^*$, u possède une unique forme normale $IRR(u)$, comme tout enchainement de réductions partant de u et arrivant à une forme normale aboutit forcément à $IRR(u)$ en un nombre fini d'étapes, on a un algorithme de calcul de $IRR(u)$ pour tout u.

Ce travail est composé de quatre chapitres.

Le premier chapitre consiste en un rappel des notions et notations utilisées par la suite : relations binaires et leurs propriétés, monoïdes, mots et langages, homomorphismes des monoïdes, complexité d'un algorithme et enfin généralités sur la cryptographie à clé publique.

Dans le second chapitre, on fait une étude sur les semi-systèmes de réécriture ainsi que certaines de leurs propriétés telles que : la terminaison et la confluence.

Dans le troisième chapitre, on s'intérèsse au problème du mot dans un monoïde, on pu exhiber des cas spécifiques où le problème est résoluble.

Enfin, on donne dans le quatrième chapitre quelques applications de semi-systèmes de réécriture et le problème du mot dans un monoïde telles que : la construction de certains codes à groupes, présentation de quelques monoïdes par générateurs et relations, présentation de quelques groupes par générateurs et relations, étude d'un système de cryptage basé sur le problème du mot dans un monoïde libre, langage engendré par un système de réécriture, les bases de Gröbner et leurs utilsations sur les semi-systèmes de rééctiture de mots.

Table des matières

Chapitre 1

Préliminaires

Introduction

Ce premier chapitre contient les définitions et les propriétés des outils que nous utiliserons par la suite : relations binaires et leurs propriétés, monoïde, homomorphisme de monoïdes, mots et langages, complexité d'un algorithme, généralités sur la cryptographie à clé publique.

Contenu du chapitre 1

1.1 Relations binaires et leurs propriétés

Dans ce qui suit, on donne quelques définitions et notations concernant les relations binaires.

Définition 1.1.1

Une relation binaire sur un ensemble E est une partie $\mathcal{R}$ de $E \times E$. Si un couple (x, y) est dans $\mathcal{R}$, on note souvent $x\mathcal{R}y$. En réécriture, on note $\longrightarrow$ les relations binaires pour insister sur leurs caractère de dérivation ou bien substitution dans les étapes dans un calcul.

Définition 1.1.2

Les relations étants des parties de $E \times E$, on définit de manière usuelle le complémentaire $\rceil(\mathcal{R})$, la réunion $\mathcal{R}_1 \cup \mathcal{R}_2$ et l'intersection $\mathcal{R}_1 \cap \mathcal{R}_2$ de relations $\mathcal{R}_1$ et $\mathcal{R}_2$. On a :

• $(x, y) \in \mathcal{R}_1 \cup \mathcal{R}_2$ si, et seulement si $x\mathcal{R}_1 y$ ou $x\mathcal{R}_2 y$.

• $(x, y) \in \mathcal{R}_1 \cap \mathcal{R}_2$ si, et seulement si $x\mathcal{R}_1 y$ et $x\mathcal{R}_2 y$.

• $x\rceil(\mathcal{R})y$ si, et seulement si $(x, y) \notin \mathcal{R}$.

• On dit que $\mathcal{R}_1$ implique $\mathcal{R}_2$ (ce qui revient au même de dire que $\mathcal{R}_2$ contient $\mathcal{R}_1$) si, et seulement si $\mathcal{R}_1 \subseteq \mathcal{R}_2$, c'est-à-dire si, et seulement si pour tout x et y de E, $x\mathcal{R}_1 y \Rightarrow x\mathcal{R}_2 y$.

Définition 1.1.3

La composition des relations sur E est l'opération sur $\mathcal{P}(E \times E)$ définie par :

$$\forall \mathcal{R}_1, \mathcal{R}_2 \in \mathcal{P}(E \times E), \mathcal{R}_1 \circ \mathcal{R}_2 = \{(x, z) \in E \times E : \exists y \in E, (x, y) \in \mathcal{R}_2, (y, z) \in \mathcal{R}_1\}.$$

La composition des relations est associative et admet comme élément neutre la relation identité $\mathcal{R}^0 = \{(x, x) / x \in E\}$. Autrement dit, $(\mathcal{P}(E \times E), \circ, \mathcal{R}^0)$ est un monoïde.

Exemple 1.1.4

Soit E l'ensemble des droites d'un plan affine euclidien et $\mathcal{R}_1 = \mathcal{R}_2 = \perp$ où $\perp$ désigne la relation d'orthogonalité. Alors $\mathcal{R}_1 \circ \mathcal{R}_2 = //$ avec $//$ désigne la relation de parallélisme. En effet, pour toutes droites D et D' du plan E, on a :

$$\left(D//D'\right) \Longleftrightarrow \left(\exists D'', D \perp D'' \text{ et } D'' \perp D'\right).$$

On peut donc écrire ici : $\perp \circ \perp = //$.

Définition 1.1.5

Une relation binaire $\mathcal{R}$ sur E est dite :

• Réflexive si $\mathcal{R}^0 \subseteq \mathcal{R}$, c'est-à-dire $x\mathcal{R}x$ pour tout $x \in E$.

• Antiréflexive si on a $\mathcal{R}^0 \cap \mathcal{R} = \emptyset$, c-à-d il n'existe pas un élément $x \in E$ qui vérifie $x\mathcal{R}x$.

• Symétrique si on a $\mathcal{R}^{-1} \subseteq \mathcal{R}$, c'est-à-dire $y\mathcal{R}x$ dès que $x\mathcal{R}y$.

• Antisymétrique si $\mathcal{R} \cap \mathcal{R}^{-1} = \mathcal{R}^0$, c'est-à-dire si $x\mathcal{R}y$ et $y\mathcal{R}x$, alors $x = y$.

• Transitive si on a $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$, c'est-à-dire si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $x\mathcal{R}z$.

Un ordre sur un ensemble E est une relation binaire réflexive, antisymétrique et transitive. Un ordre strict est une relation binaire antiréflexive et transitive. Un préordre est une relation binaire réflexive et transitive. Une équivalence est une relation binaire sur E qui est réflexive, symétrique et transitive.

Un ordre $\leq$ sur un ensemble E est total s'il vérifie la propriété suivante : $\forall x, y \in E : x \leq y$ ou $y \leq x$. A une relation d'ordre $\leq$, on associe la relation d'ordre stricte $<$ définie par : $x < y \Longleftrightarrow x \leq y$ et $x \neq y$.

Notations 1.1.6

Soit $\mathcal{R}$ une relation binaire définie sur un ensemble E. On dénote par :

• $E \times E$ la relation pleine.

• $\mathcal{R}^0$ l'identité sur E.

• $\mathcal{R}^n$ la n-ième composition de $\mathcal{R}, \mathcal{R}^n = \mathcal{R} \circ \mathcal{R}^{n-1} = \mathcal{R}^{n-1} \circ \mathcal{R}$, pour $n > 0$.

• $\mathcal{R}^r$ la fermeture réflexive de $\mathcal{R}$.

• $\mathcal{R}^{-1}$ l'inverse de $\mathcal{R}$.

• $\mathcal{R}^s$ la fermeture symétrique de $\mathcal{R}$.

• $\mathcal{R}^+$ ou $\mathcal{R}^t$ la fermeture transitive de $\mathcal{R}$.

• $\mathcal{R}^*$ ou $\mathcal{R}^{rt}$ la fermeture réflexive et transitive de $\mathcal{R}$.

• $\mathcal{R}^{rts}$ la fermeture réflexive, transitive et symétrique de $\mathcal{R}$.

Définition 1.1.7

Soient $E_1, ..., E_k$ des ensembles partiellement ordonnés par les relations $\leq_i$, $i = 1, ..., k$, respectivement. L'ordre lexicographique $\preceq$ sur $E_1 \times ... \times E_k = \prod_{i=1}^{i=k} E_i$ est défini par : $(x_1, ..., x_k) \preceq (y_1, ..., y_k)$ si soit $(x_1, ..., x_k) = (y_1, ..., y_k)$, soit il existe un d, $1 \leq d \leq k$ tel que $x_d \leq_d y_d$ avec $x_d \neq y_d$ et pour tout $i = 1, ..., d-1$, on a $x_i = y_i$.

Exemple 1.1.8

Soit $E_1 = E_2 = \mathbb{N}$ muni de l'ordre usuel. Alors, avec l'ordre lexicographique $\preceq$ sur $\mathbb{N}^2$, on a les couples $(0, i)$ précèdent les couples $(1, i)$, de même $(1, i)$ précèdent $(2, i)$ et ainsi de suite, pour tout $i \in \mathbb{N}$.

Définition 1.1.9

Soient E un ensemble non vide et P une propriété des relations vérifiée par $E \times E$. Si l'intersection de toute famille de relations vérifiant P est une relation qui vérifie P, alors il existe pour toute relation $\mathcal{R}$ une plus petite relation vérifiant P et contenant $\mathcal{R}$. On l'appelle la P-fermeture de $\mathcal{R}$. C'est le cas pour les propriétés de réflexivité, de symétrie, de transitivité et toutes les combinaisons de ces propriétés.

Définition 1.1.10 [25]

Soit P une propriété des relations vérifiéé par $E \times E$.

Soit R une relation binaire sur un ensemble E et soit P une propriété qui peut être vérifiée par R ou non. On cherche s'il existe une relation $\widetilde{\mathcal{R}}$ possédant la propriété P avec $\widetilde{\mathcal{R}}$ contenant R. On demande de plus que $\widetilde{\mathcal{R}}$ soit minimale, c'est-à-dire, s'il existe une autre relation $\overset{\wedge}{\mathcal{R}}$ possèdant la propriété P on doit avoir :

$$R \subseteq \widetilde{\mathcal{R}} \subseteq \overset{\wedge}{\mathcal{R}},$$

En d'autres mots, la relation $\widetilde{\mathcal{R}}$ est la plus petite relation, au sens de l'inclusion, contenant R et possédant la propriété P.

Proposition 1.1.11

Etant donnée une propriété P des relations vérifiéé par $E \times E$. Par exemple, si la propriété P est la réflexivité, la symétrie ou la transitivité, La relation pleine $E \times E$ possède la propriété P et contenant toute relation R sur E. D'autre part, pour toute famille de relations $\overset{\wedge}{\mathcal{R}}$ de $E \times E$ vérifiant la propriété P, on a bien la relation $\cap\overset{\wedge}{\mathcal{R}}$ vérifie aussi cette propriété. Il en résulte que :

$$\widetilde{\mathcal{R}} = \bigcap_{\substack{\mathcal{R} \subseteq \overset{\wedge}{\mathcal{R}} \\ \overset{\wedge}{\mathcal{R}} \text{ vérifie } P}} \overset{\wedge}{\mathcal{R}}$$

est la plus petite relation binaire contenat R est possédant la propriété P. On a les formules suivantes :

- *Si P est la réflexivité, alors* $\widetilde{\mathcal{R}} = R^r = R \cup R^0$
- *Si P est la symétrie, alors* $\widetilde{\mathcal{R}} = R^s = R \cup R^{-1}$
- *Si P est la transitivité, alors* $\widetilde{\mathcal{R}} = R^+ = \bigcup_{n=1}^{+\infty} R^n$

Démonstration

Faisons par exemple une démonstration de la dernière formule.

1. La relation $\bigcup_{n=1}^{+\infty} \mathcal{R}^n$ contient $\mathcal{R}$. En effet on a $\bigcup_{n=1}^{+\infty} \mathcal{R}^n = \mathcal{R} \cup \bigcup_{n=2}^{+\infty} \mathcal{R}^n$.

2. Montrons que $\bigcup_{n=1}^{+\infty} \mathcal{R}^n$ est transitive :

Soient x, y et $z \in E$, supposons que $x \bigcup_{n=1}^{+\infty} \mathcal{R}^n y$ et $y \bigcup_{n=1}^{+\infty} \mathcal{R}^n z$,

On a $x \bigcup_{n=1}^{+\infty} \mathcal{R}^n y$ est équivalente a $\exists q_1 \in \mathbb{N}^* : x \mathcal{R}^{q_1} y$, donc $\exists (x_1, x_2, ..., x_{q_1-1}) \in E^{q_1-1}$ tels que :

$$x \mathcal{R} x_1, x_1 \mathcal{R} x_2, ..., x_{q_1-1} \mathcal{R} y.$$

De même on a $y \bigcup_{n=1}^{+\infty} \mathcal{R}^n z$ ce qui équivaut à dire $\exists q_2 \in \mathbb{N}^* : y \mathcal{R}^{q_2} z$, donc $\exists (y_1, y_2, ..., y_{q_2-1})$ $\in E^{q_2-1}$ tels que :

$$y \mathcal{R} y_1, y_1 \mathcal{R} y_2, ..., y_{q_2-1} \mathcal{R} z.$$

On a $x \mathcal{R} x_1, x_1 \mathcal{R} x_2, ..., x_{q_1-1} \mathcal{R} y$ et $y \mathcal{R} y_1, y_1 \mathcal{R} y_2, ..., y_{q_2-1} \mathcal{R} z$ c'est-à-dire $x \mathcal{R}^{q_1+q_2} z$, ce qui montre que $x \bigcup_{n=1}^{+\infty} \mathcal{R}^n z$, est par conséquent la relation $\bigcup_{n=1}^{+\infty} \mathcal{R}^n$ est transitive.

3. Soit $\overset{\wedge}{\mathcal{R}}$ une autre relation transitive qui contient $\mathcal{R}$. Montrons que $\bigcup_{n=1}^{+\infty} \mathcal{R}^n \subset \overset{\wedge}{\mathcal{R}}$,

On a $x \bigcup_{n=1}^{+\infty} \mathcal{R}^n y$ c'est-à-dire $\exists q_1 \in \mathbb{N}^* : x \mathcal{R}^{q_1} y$, donc $\exists (x_1, x_2, ..., x_{q_1-1}) \in E^{q_1-1}$ tels que :

$x \mathcal{R} x_1, x_1 \mathcal{R} x_2, ..., x_{q_1-1} \mathcal{R} y$. Comme $\mathcal{R} \subset \overset{\wedge}{\mathcal{R}}$, alors $x \overset{\wedge}{\mathcal{R}} x_1, x_1 \overset{\wedge}{\mathcal{R}} x_2, ..., x_{q_1-1} \overset{\wedge}{\mathcal{R}} y$,

comme $\overset{\wedge}{\mathcal{R}}$ est transitive, alors $x \overset{\wedge}{\mathcal{R}} y$. $\square$

Remarque 1.1.12

Dans le cas où l'ensemble E est fini, de cardinal k, l'identité $\mathcal{R}^+ = \bigcup_{n=1}^{+\infty} \mathcal{R}^n$ s'écrit sous la formule plus sympathique suivante : $\mathcal{R}^+ = \bigcup_{n=1}^{n=k} \mathcal{R}^n$.

Théorème 1.1.13

Soit R une relation binaire définie sur un ensemble E. Il existe une unique relation d'équivalence $\widetilde{\mathcal{R}}$ telle que :

1. $R \subseteq \widetilde{\mathcal{R}}$.
2. *Si $\widehat{\mathcal{R}}$ est une relation d'équivalence vérifiant $R \subseteq \widehat{\mathcal{R}} \subseteq \widetilde{\mathcal{R}}$, alors $\widehat{\mathcal{R}} = \widetilde{\mathcal{R}}$.*
3. *La fermeture d'équivalence de R est définie par :*

$$\widetilde{\mathcal{R}} = \mathcal{R}^{rst} = \bigcap_{\substack{\mathcal{R} \subseteq \widehat{\mathcal{R}} \\ \widehat{\mathcal{R}} \text{ relation d'équivalence}}} \qquad \widehat{\mathcal{R}} = R^0 \bigcup \left(\bigcup_{n=1}^{+\infty} (R \cup R^{-1})^n\right) = \bigcup_{n=1}^{+\infty} (R \cup R^{-1} \cup R^0)^n.$$

Exemple 1.1.14

Soit $E = \{1, 2, 3, 4\}$ et $\mathcal{R} = \{(1,2), (1,3), (2,1), (2,3), (3,4)\}$, on a donc

- $\mathcal{R}^s = \mathcal{R} \cup \mathcal{R}^{-1} = \{(1,2), (1,3), (2,1), (2,3), (3,4), (3,1), (3,2), (4,3)\}$.
- $\mathcal{R}^r = \mathcal{R} \cup \mathcal{R}^0 = \{(1,2), (1,3), (2,1), (2,3), (3,4), (1,1), (2,2), (3,3), (4,4)\}$.
- $\mathcal{R}^+ = \{(1,2), (1,3), (2,1), (2,3), (3,4)(1,1), (1,4)(2,2)(2,4)\}$.
- $\mathcal{R}^* = \mathcal{R}^+ \cup \mathcal{R}^r = \{(1,2), (1,3), (2,1), (2,3), (3,4)(1,1), (1,3)(2,2)(2,4), (1,4), (3,3), (4,4)\}$.

Proposition 1.1.15

Soit R une relation binaire définie sur un ensemble E. On a :

1. $(R^r)^s = (R^s)^r$.
2. $(R^r)^+ = (R^+)^r$.
3. $(R^+)^s \subseteq (R^s)^+$.

Démonstration

On fait remarquer que, pour deux relations binaires $\mathcal{R}_1$ et $\mathcal{R}_2$ quelconques sur un même ensemble E, on a :

$$(\mathcal{R}_1 \cup \mathcal{R}_2)^{-1} = \mathcal{R}_1^{-1} \cup \mathcal{R}_2^{-1}.$$

Ainsi que, pour toute relation binaire $\mathcal{R}$ sur un ensemble E, on a $(\mathcal{R}^0)^{-1} = \mathcal{R}^0$. Par suite, Pour l'identité (1) on a : $(\mathcal{R}^r)^s = (\mathcal{R} \cup \mathcal{R}^0)^s = (\mathcal{R} \cup \mathcal{R}^0) \cup (\mathcal{R} \cup \mathcal{R}^0)^{-1} = \mathcal{R} \cup \mathcal{R}^0 \cup \mathcal{R}^{-1} \cup (\mathcal{R}^0)^{-1}$ $= \mathcal{R} \cup \mathcal{R}^{-1} \cup \mathcal{R}^0 = \mathcal{R}^s \cup \mathcal{R}^0 = (\mathcal{R}^s)^r$.

Notons que pour toute relation binaire $\mathcal{R}$ sur un ensemble E et pour tout entier n, on a $(\mathcal{R} \cup \mathcal{R}^0)^n = \bigcup_{k=0}^{n} \mathcal{R}^k$. Par conséquent, l'identité (2) s'écrit

$$(\mathcal{R}^r)^+ = (\mathcal{R} \cup \mathcal{R}^0)^+ = \bigcup_{n=1}^{+\infty} (\mathcal{R} \cup \mathcal{R}^0)^n = \bigcup_{n=1}^{+\infty} \bigcup_{k=0}^{n} \mathcal{R}^k = \bigcup_{n=1}^{+\infty} \mathcal{R}^n = (\bigcup_{n=1}^{+\infty} \mathcal{R}^n) \cup \mathcal{R}^0 = (\mathcal{R}^+)^r.$$

Enfin pour (3), on a,

$(\mathcal{R}^+)^s = (\bigcup_{n=1}^{+\infty} \mathcal{R}^n) \cup (\bigcup_{n=1}^{+\infty} \mathcal{R}^n)^{-1} = (\bigcup_{n=1}^{+\infty} \mathcal{R}^n) \cup (\bigcup_{n=1}^{+\infty} \mathcal{R}^{-n})$, du faite que $\mathcal{R}^{-n}$ est la relation $(\mathcal{R}^{-1})^n$. Toujours par définition on a :

$$(\mathcal{R}^s)^+ = \bigcup_{n=1}^{+\infty} (\mathcal{R} \cup \mathcal{R}^{-1})^n.$$

Or, pour tout entier n non nul, $\mathcal{R}^n$ et $\mathcal{R}^{-n}$ sont contenues dans $(\mathcal{R} \cup \mathcal{R}^{-1})^n$, donc dans $(\mathcal{R}^s)^+$. Donc $\mathcal{R}^+$ et $(\mathcal{R}^{-1})^+$ sont aussi contenues dans $(\mathcal{R}^s)^+$.

Ce qui donne bien $(\mathcal{R}^+)^s \subseteq (\mathcal{R}^s)^+$. $\square$

Proposition 1.1.16

Une relation d'équivalence R sur un ensemble E peut être aussi définie des manières suivantes :

1. *Par la donnée d'une partition P de E :*

$$xRy \Longleftrightarrow \exists X \in P \text{ tel que: } x \in X \text{ et } y \in X.$$

2. *Par la donnée d'une application f de E dans un ensemble quelconque F :*

$$xRy \Longleftrightarrow f(x) = f(y).$$

3. *Par la donnée d'une application h de $E \times E$ dans l'ensemble $U = \{z \in \mathbb{C} : |z| = 1\}$ vérifiant la condition : $\forall (x, y, z) \in E^3, h(x, y)h(y, z) = h(x, z)$.*

En posant, $xRy \Longleftrightarrow h(x, y) = 1$.

Démonstration

On donne une démonstration pour le dernier cas.

• On montre que $\mathcal{R}$ est réflexive c'est-à-dire $\forall x \in E, h(x,x) = 1$.

On a $\forall (x,y,z) \in E^3, h(x,y)h(y,z) = h(x,z)$, en pariculier,

si $x = y = z$, alors $h(x,x)h(x,x) = h(x,x)$, donc $(h(x,x))^2 - h(x,x) = 0$ c'est-à-dire $h(x,x)(h(x,x)-1) = 0$. On a $h(x,x) \neq 0$, car $h(x,x) \in U$, par conséquent $h(x,x) = 1$.

• On montre que $\mathcal{R}$ est symétrique.

Premièrement montrons que $\forall (x,y) \in E^2$, si $h(x,y) = 1$, alors $h(x,y) = \overline{h(y,x)}$, où $\overline{h(y,x)}$ désigne le conjugué de nombre complexe $h(y,x)$.

On a $\forall (x,y,z) \in E^3, h(x,y)h(y,z) = h(x,z)$, en particulier, si $x = z$,

alors $h(x,y)h(y,x) = h(x,x) = 1$, ce qui montre que $h(x,y)h(y,x) = 1$....(1).

D'autre part $h(x,y)\overline{h(x,y)} = |h(x,y)|^2 = 1^2 = 1$.....(2), où $|h(x,y)|$ désigne le module de $h(x,y)$. D'après (1) et (2) on a $h(x,y) = \overline{h(y,x)}$. On montre que $x\mathcal{R}y \Rightarrow y\mathcal{R}x$.

On a $x\mathcal{R}y \Longleftrightarrow h(x,y) = 1$, comme $h(y,x) = \overline{h(x,y)}$, alors $h(y,x) = 1$, ce qui équivaut à dire $y\mathcal{R}x$. Donc $\mathcal{R}$ est symétrique.

• Finalement on montre que $\mathcal{R}$ est transitive :

On a $(x\mathcal{R}y)$ et $(y\mathcal{R}z) \Leftrightarrow (h(x,y) = 1\ h(y,z) = 1)$, et comme $h(x,y)h(y,z) = h(x,z)$,

alors $h(x,z) = 1$, ce qui montre que $x\mathcal{R}z$. $\square$

1.2 Monoïde

Définition 1.2.1

Un monoïde est un ensemble muni d'une loi interne, i.e, d'une application

$\cdot : M \times M \longrightarrow M$, qui satisfait les conditions suivantes :

▶ L'opération " $\cdot$ " est associative : $\forall x, y, z \in M : (x \cdot y) \cdot z = x \cdot (y \cdot z)$.

▶ Il existe un neutre (unique) $1_M \in M$ tel que $\forall x \in M : x \cdot 1_M = 1_M \cdot x = x$.

Un élément $m' \in M$ est dit le symétrique de l'élément $m \in M$ si $m \cdot m' = m' \cdot m = 1_M$.

Remarque 1.2.2

Un Monoïde $(M, \cdot, 1_M)$ qui est tel que tout élément de M possède un symétrique est un groupe.

Exemple 1.2.3

Tout groupe est un monoïde, $(\mathbb{N}, +, 0)$ est un monoïde qui n'est pas un groupe.

Proposition 1.2.4

Soit G un groupe et H un sous ensemble non vide de G.

1. *H est un sous groupe de G si, et seulement si $\forall x, y \in H : x \cdot y^{-1} \in H$.*

2. *Le sous groupe H est normal ou distingué si, $\forall x \in G, \forall h \in H : x \cdot h \cdot x^{-1} \in H$.*

Définitions 1.2.5

• Soit un monoïde $(M, \cdot, 1_M)$. Un sous monoïde de $(M, \cdot, 1_M)$ est un triplet $\left(M^{'}, \cdot, 1_{M'}\right)$ tel que :

► $M^{'} \subseteq M$,

► $1_M = 1_{M'}$,

► $\forall m, m^{'} \in M^{'} : m \cdot m^{'} \in M^{'}$.

• Soit I un ensemble d'indices et si $\forall i \in I, (M_i, \cdot, 1_M)$ est un sous monoïde de $(M, \cdot, 1_M)$, alors $(\cap_{i \in I} M_i, \cdot, 1_M)$ est un sous monoïde de $(M, \cdot, 1_M)$.

• Soit X une partie d'un monoïde M. On appelle sous monoïde engendré par X, le plus petit sous monoïde de $(M, \cdot, 1_M)$ contenant X, on le note X^*. D'après ce qui précède X^* est l'intersection de tous les sous monoïdes de $(M, \cdot, 1_M)$ qui contiennent X.

Exemple 1.2.5

Soit A l'ensemble des nombres pairs et B l'ensemble des nombres impairs. $(A, +, 0)$ est un sous monoïde de $(\mathbb{N}, +, 0)$ engendré par $\{2\}$ tandis que $(B, +, 0)$ n'est pas un sous monoïde de $(\mathbb{N}, +, 0)$.

Définitions 1.2.6

Soit $(M, \cdot, 1_M)$ un monoïde , une congruence sur $(M, \cdot, 1_M)$ est une relation d'équivalence $\equiv$ stable par multiplication à droite et à gauche, c'est-a-dire :

$$\forall x, y, z \in M : x \equiv y \Rightarrow x \cdot z \equiv y \cdot z \text{ et } z \cdot x \equiv z \cdot y$$

Définition 1.2.7

Soit M un monoïde et $\equiv$ une congruence définie sur M. Le quotient $M/\equiv$ est le monoïde des classes de congruence de M pour la relation $\equiv$. La loi de composition de $M/\equiv$ est définie de la manière suivante : $\overline{u} *_{M/\equiv} \overline{v} = \overline{u *_M v}$.

La projection naturelle (la surjection canonique) de M dans $M/\equiv$ est noté P.

Exemple 1.2.8

Soit le monoïde $(\mathbb{N}, +)$ et soit la relation $\equiv$ définie par $x \equiv y$ si, et seulement si, x et y ont même parité. la relation $\equiv$ est une congruence. Le quotient de $\mathbb{N}$ par cette relation donne un monoïde comprenant deux éléments, notés $\overline{0}$ et $\overline{1}$ correspondant respectivement aux entiers pairs et impairs.

Définition 1.2.9

Soit $\equiv$ une congruence sur un monoïde M.

1. Une partie X de M est dite saturée par $\equiv$ si $\forall x \in X : \overline{x} \subseteq X$.

2. On appelle partie saturée engendrée par une partie A de M et on note $Sat(A)$, la plus petite partie saturée par $\equiv$ de M contenant A.

Proposition 1.2.10

Soit $\equiv$ une congruence sur un monoïde M.

1. *La réunion et l'intersection de parties saturées par $\equiv$ sont saturées.*

2. *Pour toute partie A de M , on a $Sat(A) = \bigcup_{x \in A} \overline{x}$.*

3. *Si $f : M \longrightarrow M'$ est un morphisme de monoïdes et si $\equiv$ la congruence sur M définie par: $x \equiv y \Longleftrightarrow f(x) = f(y)$, alors $S \subseteq M$ est saturée par $\equiv$ si, et seulement si $f^{-1}(f(S)) = S$.*

1.3 Mots et langages

On introduit dans ce paragraphe quelques définitions, propriétés et notations concernant les mots et les langages.

Définition 1.3.1

On appelle vocabulaire (ou alphabet) un ensemble fini quelconque Σ. Les éléments d'un vocabulaire sont appelés lettres, caractères ou symboles.

Exemple 1.3.2

Le biologiste intéressé par l'étude de l'ADN utilisera un alphabet à quatre lettres $\{A, C, G, T\}$ pour les quatre constituants des gènes: Adénine, Cytosine, Guanine et Thymine.

Définition 1.3.3

• Soit Σ un alphabet, un mot sur Σ est une suite finie de symbole. Par exemple, 00110 et 110 sont deux mots sur l'alphabet $\{0, 1\}$. La longueur d'un mot w est le nombre de symboles constituant ce mot, on le note $|w|$. Ainsi, $|00110| = 5$ et $|110| = 3$.

L'unique mot de longueur 0 est le mot correspondant à la suite vide. Ce mot s'appelle le mot vide et on le note 1, ou bien ϵ.

L'ensemble des mots sur Σ est noté Σ^*. Par exemple

$\{0, 1, 2\}^* = \{\epsilon, 0, 1, 2, 00, 01, 02, 11, 12, 20, 21, 22, 000, 001, ...\}$ (ϵ est le mot vide).

• Si σ est une lettre de l'alphabet Σ, pour tout mot $w = \sigma_1\sigma_2...\sigma_k$ de Σ^*, on note par :

$$|w|_\sigma = card\{i \in \{1, 2, ..., k\} : \sigma_i = \sigma\}.$$

le nombre d'occurrences de la lettre σ dans le mot w et $w(i)$ sa i-ème lettre.

Par exemple $|00110|_0 = 3$ et $|00110|_1 = 2$, $00110\,(1) = 0$, $00110\,(4) = 1$.

Proposition 1.3.4

Soit Σ un alphabet,

1. l'ensemble Σ^* est infini.

2. l'ensemble Σ^* est dénombrable.

Démonstration

1. l'ensemble Σ^* est infini, en effet on a $\Sigma^* = \bigcup_{n=0}^{+\infty} \Sigma^n = \Sigma^0 \cup \Sigma...\Sigma^n \cup ....$

2. On montre que Σ^* est dénombrable (la méthode de Gödel). Comme Σ est fini, on peut donc numéroter ses éléments, par exemple, si $\Sigma = \{\alpha, \beta, \gamma\}$, alors $n\,(\alpha) = 1, n\,(\beta) =$

$2, n(\gamma) = 3$. Ensuite, soit u un mot de Σ^*, on considère les longueurs $|u|$ premiers nombres premiers, par exemple si $|u| = 5$, on a les 5 premiers nombres premiers sont $p(1) = 2, p(2) = 3, p(3) = 5, p(4) = 7, p(5) = 11$.

On forme le nombre $f(u) = \prod_{i=1}^{i=|u|} p(i)^{n(u(i))}$, où $u(i)$ désigne la i-ème lettre de u. Par exemple si $u = \alpha\gamma\beta\alpha\alpha$, alors, $f(u) = \prod_{i=1}^{i=|u|} p(i)^{n(u(i))} = \prod_{i=1}^{i=5} p(i)^{n(u(i))} = 2^1 \times 3^3 \times 5^2 \times 7^1 \times 11^1$. Donc on peut définir une application $f : \Sigma^* \longrightarrow \mathbb{N}, u \longmapsto f(u) = \prod_{i=1}^{i=|u|} p(i)^{n(u(i))}$. Par l'unicité de la décomposition d'un entier en facteurs premiers, l'application f est injective. Enfin, comme f est injective et l'ensemble $\mathbb{N}$ est dénombrable, alors Σ^* est dénombrable.

Définition 1.3.5

La concaténation est l'opération qui associe à deux mots u et v le mot noté $u.v$ ou uv défini par : si $u = \alpha_1\alpha_2...\alpha_n$ et $v = \beta_1\beta_2...\beta_p$, alors $uv = \gamma_1\gamma_2...\gamma_{n+p}$ avec $\gamma_i = \alpha_i$ pour $i = 1, ...n$ et $\gamma_{n+i} = \beta_i$ pour $i = 1, ...p$. Par exemple, la concaténation des mots 00011 et 011 donne le mot 00011011. On vérifie facilement que la concaténation est une opération associative admettant le mot vide comme élément neutre :

$$\forall x, y, z \in \Sigma^* : (xy)z = x(yz).$$
$$\forall x \in \Sigma^* : x\epsilon = \epsilon x = x.$$

Propriété 1.3.6

Soit Σ un alphabet quelconque le monoïde Σ^* possède les deux propriétés suivantes :

1. *Tout élément de Σ^* est une suite finie d'éléments de Σ.*
2. *Deux suites distinctes d'éléments de Σ définissent deux éléments distincts de Σ^*.*

La propriété (1) distingue le monoïde Σ^* par exemple du monoïde $(\Sigma \cup \{\sigma\})^*$, avec $\sigma \notin \Sigma$. La propriété (2) distingue le monoïde $\{\alpha, \beta\}^*$ par exemple du monoïde commutatif M obtenu en postulant que l'opération de concaténation est commutative : les deux mots $\alpha\beta$ et $\beta\alpha$ définissent alors le même élément de M. Σ^* est le seul monoïde satisfaisant les propriétés (1) et (2), on dit que Σ^* est le monoïde libre sur Σ. On dit que Σ est une base de Σ^*.

Propriété (de Levi) 1.3.7

Soient t, u, v, w quatre mots de monoïde libre Σ^*.

1. *Si $tu = vw$ et $|t| \leq |v|$ alors il existe un unique mot z de Σ^* tel que $v = tz$ et $u = zw$.*

2. *Si $uv = wt$ et $|u| = |w|$ alors $u = w$ et $v = t$.*

3. *Pour tout $i \in \mathbb{N} - \{0\}$, $(u^i = v^i \Longleftrightarrow u = v)$.*

4. *Le monoïde libre Σ^* est simplifiable, c'est à dire,*

$$4.1\ uv = uw \Rightarrow v = w;$$
$$4.2\ uv = wv \Rightarrow u = w;$$
$$4.3\ uvw = utw \Rightarrow v = t.$$

5. *Les propositions suivantes sont équivalentes :*

5.1 $uv = vu$,

5.2 *Il existe deux entiers n et m non tous deux nuls tels que $u^n = v^m$,*

5.3 *Il existe un mot z et deux entiers p et q tels que $u = z^p$ et $v = z^q$.*

Définition 1.3.8

Un langage sur un alphabet Σ est simplement un ensemble (fini ou infini) de mots sur Σ. En d'autres termes, un langage est une partie de Σ^*. On distingue en particulier le langage vide $\emptyset$ qui ne contient aucun mot.

Définition 1.3.9

Soient $L, M \subseteq \Sigma^*$, deux langages. La concaténation des langages L et M est le langage,

$$LM = \{uv, u \in L, v \in M\}$$

En particulier, on peut définir la puissance $n - ième$ d'un langage L, $n > 0$, par :

$$L^n = \{w_1 w_2 ... w_n, \forall i \in \{1, 2...n\}\, w_i \in L\}.$$

Et on pose $L^0 = \{\epsilon\}$.

Exemple 1.3.10

Soient les deux langages $L = \{u \in \Sigma^* : |u| \text{ est paire}\}$ *et* $K = \{u \in \Sigma^* : |u| \text{ est impaire}\}$. On a alors les égalités suivantes :

$LK = KL = K$; $LL = L$; $KK = L - \{\epsilon\}$.

Définition 1.3.11

On dit qu'un mot $u \in \Sigma^*$ est facteur de $w \in \Sigma^*$ s'il existe deux mots $f, g \in \Sigma^*$ tel que $w = fug$.

Exemple 1.3.12

Soit l'alphabet $\Sigma = \{a, b, c\}$, et le mot $w = aabc$, alors ab est un facteur de w, mais ac ne l'est pas.

Définition 1.3.14

Soit L est un langage sur un alphabet Σ. La congruence syntaxique de L notée $\equiv_L$ est définie par, pour tous $u, v \in \Sigma^*, (u \equiv_L v) \Longleftrightarrow (\forall x, y \in \Sigma^*, xuy \in L \Longleftrightarrow xvy \in L)$.

1.4 Homomorphisme de monoïdes

Dans ce paragraphe, nous donnerons quelques propriétés sur la notion d'un homomorphisme de monoïdes.

Définition 1.4.1

Soient $(M, \cdot, 1_M)$, $(M', \cdot', 1_{M'})$ deux monoïdes. Une application $\varphi : M \longrightarrow M'$ est un morphisme (ou encore homomorphisme) de monoïdes si :

- $\forall x, y \in M : \varphi(x \cdot y) = \varphi(x) \cdot' \varphi(y)$,
- $\varphi(1_M) = 1_{M'}$.

Un isomorphisme de monoïdes est un homomorphisme bijectif de monoïdes.

Exemple 1.4.2

L'application longueur $|.| : \Sigma^* \longrightarrow \mathbb{N}$ est un morphisme de monoïdes entre $(\Sigma^*, .)$ et $(\mathbb{N}, +)$. En effet, $\forall u, v \in \Sigma^* : |uv| = |u| + |v|$ et $|\epsilon| = 0$.

Exemple 1.4.3 [35]

Soit $\Sigma = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ un alphabet, $n \in \mathbb{N} \setminus \{0, 1\}$.

La fonction de Parikh $\Psi : \Sigma^* \longrightarrow \mathbb{N}^n,\ \Psi(w) = (|w|_{\alpha_1}, ..., |w|_{\alpha_n})$,

est un morphisme de monoïdes entre $(\Sigma^*, .)$ et $(\mathbb{N}^n, +)$.

Exemple 1.4.4

Soit $\Sigma = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ un alphabet, $n \in \mathbb{N} \setminus \{0, 1\}$.

Et soit $\lambda : \Sigma \longrightarrow \mathbb{N},\ \alpha_i \longmapsto \lambda(\alpha_i)$. On définit $\widetilde{\lambda} : \Sigma^* \longrightarrow \mathbb{N}$ comme suit :

$$\widetilde{\lambda}(w) = \sum_{i=1}^{i=n} \lambda(\alpha_i)\, |w|_{\alpha_i}\,.$$

$\widetilde{\lambda}$ est un homomorphisme de monoïdes.
Et si $\forall 1 \leq i \leq n,\ \lambda(\alpha_i) = 1$, alors $\widetilde{\lambda} = |.|$ (le morphisme de longueur).

La proposition suivante justifie le fait que le monoïde Σ^* soit appelé monoïde libre. Cette propriété caractérise le monoide libre engendré par Σ.

Proposition 1.4.5 [4]

Toute fonction $\mu : \Sigma \longrightarrow M$ de Σ dans un monoïde M se prolonge de façon unique en un morphisme de Σ^* dans M.

Démonstration

L'existence : posons
$\widetilde{\mu}(\epsilon) = 1_M$ et $\widetilde{\mu}(\alpha_1\alpha_2...\alpha_n) = \mu(\alpha_1)\mu(\alpha_2)...\mu(\alpha_n),\ n \in \mathbb{N} - \{0\}\,,\ \alpha_i \in \Sigma,\ 1 \leq i \leq n.$
Il est facile de voir que $\widetilde{\mu}$ est bien un homomorphisme
L'unicité : Si $\widetilde{\mu}$ et $\widetilde{\lambda}$ sont deux homomorphismes de Σ^* dans M tels que :
$\forall \alpha \in \Sigma, \widetilde{\mu}(\alpha) = \widetilde{\lambda}(\alpha)$, alors $\widetilde{\mu}(1) = \widetilde{\lambda}(1) = 1_M$ et pour tout mot $w = \alpha_1\alpha_2...\alpha_n$,
on a $\widetilde{\mu}(w) = \widetilde{\mu}(\alpha_1\alpha_2...\alpha_n) = \mu(\alpha_1)\mu(\alpha_2)...\mu(\alpha_n) = \widetilde{\lambda}(\alpha_1\alpha_2...\alpha_n) = \widetilde{\lambda}(w)$. $\square$

Définition 1.4.6

Un morphisme entre deux monoïdes libres Σ^* et Δ^* est une application $\psi : \Sigma^* \longrightarrow \Delta^*$ qui satisfait :

$$\psi(xy) = \psi(x)\psi(y) \qquad \forall x, y \in \Sigma^*.$$

Notons que cet morphisme ψ est complètement déterminé ayant les images des lettres de Σ dans Δ^*, i.e, $\psi(\sigma)$ pour tout σ appartenant à Σ. Nous dirons que le morphisme ψ est non trivial s'il existe au moins une lettre $\sigma \in \Sigma$ pour laquelle $\psi(\sigma) \neq \epsilon$.
En fait remarquer que la propriété $\psi(xy) = \psi(x)\psi(y)$ implique $\psi(\epsilon) = \epsilon$.

Définition 1.4.7

1. Une relation binaire $\mathcal{R}$ sur un ensemble E est noethérienne s'il n'existe pas une chaine infinie d'éléments de E en relation par $\mathcal{R}$, en d'autres mots il n'existe pas une suite infinie $(e_n)_{n\in\mathbb{N}}$ d'éléments de E tel que, pour tout entier naturel n, on a $e_n\mathcal{R}e_{n+1}$.

2. Un ordre sur un ensemble E est bien fondé s'il ne contient pas de suite infini d'éléments de E strictement décroissante.

3. La partie strict d'une relation d'ordre bien fondé $\geq$ noté $>$ et définie par: $x > y$ si $x \geq y$ et $x \neq y$.

Exemples 1.4.8

1. La relation $\mathcal{R}$ définie sur $\mathbb{N}$ par $x\mathcal{R}y \Longleftrightarrow x$ divise y et $x \neq y$ est bien fondé.

2. La relation usielle $\geq$ est un ordre bien fondé sur l'ensemble des entiers $\mathbb{N}$.

Définition 1.4.9

Soient P et $P^{'}$ deux partitions de monoïde libre Σ^*, on dit que P est plus fine que $P^{'}$ si : $\forall p \in P, \exists p' \in P'$ tel que $p \subseteq p'$. Dans ce cas on dit que P est plus fine que P' ou bien P' est plus grossière que P.

Exemple 1.4.10

Soit le *monoïde* $(\mathbb{Z}, +)$. On définit sur $(\mathbb{Z}, +)$ les deux congruences $\equiv_1$ et $\equiv_2$ suivantes :

$$\begin{cases} x \equiv_1 y \iff x \equiv y\,[2]\,, \text{ i.e, } \exists k \in \mathbb{Z} : x - y = 2k, \\ x \equiv_2 y \iff x \equiv y\,[4]\,, \text{ i.e, } \exists k \in \mathbb{Z} : x - y = 4k. \end{cases}$$

Il est clair que $\equiv_2 \subset \equiv_1$. En effet, si $x \equiv_2 y$, i.e, $x \equiv y\,[4]$, alors $\exists k \in \mathbb{Z} : x - y = 4k$,
et par concéquent $\exists k \in \mathbb{Z} : x - y = 2\,(2k)$, i.e, $x \equiv_1 y$.
On a $P = \left\{[o]_{\equiv_2}, [1]_{\equiv_2}, [2]_{\equiv_2}, [3]_{\equiv_2}\right\}$ et $P' = \left\{[o]_{\equiv_1}, [1]_{\equiv_1}\right\}$ sont deux partitions de $\mathbb{Z}$.
De plus, on a $[o]_{\equiv_2} \cup [2]_{\equiv_2} \subset [o]_{\equiv_1}$ et $[1]_{\equiv_2} \cup [3]_{\equiv_2} \subset [1]_{\equiv_1}$. Donc P est plus fine que P'.

1.5 Complexité d'un algorithme

L'objet de la théorie de la complexité est :

• Pour les algorithmes d'évaluer le nombre d'opérations élémentaires (complexité temporelle) et l'espace mémoire nécessaire (complexité saptiale) pour leur résolution.

• Pour les problèmes (de décision), de les calssifier suivants leur niveau de difficulté.

Définition 1.5.1

Soient f et g deux fonctions à variable entière et à valeurs positives.
$f(n) = O(g(n))$ s'il existe une constante $c > 0$ et un entier n_0 tels que
$\forall n \geq n_0, 0 \leq f(n) \leq cg(n)$. On dit que g domine f ou que f ne croit pas plus vite que g multiplié par une constante.

Définition 1.5.2

Soit n un entier, on note D les données de taille inférieur ou égale n, $C(D)$ le coût associé à l'exécution de la donnée D par un algorithme et $C(n)$ la complexité de l'algorithme. Alors on peut définir $C(n)$ de trois façons différentes :

1. Complexité dans le pire des cas **:**
$C(n) = Max\{C(D), D \text{ donnée de taille inférieur ou égale } n\}$.
2. Complexité en moyenne **:** $C(n) = \sum_{D \text{ donnée de taille inférieur ou égale } n} P(D)\,C(D)$.
où $P(D)$ est la probabilité d'obtenir la donnée D.
3. Complexité dans le meilleur des cas **:**
$C(n) = Min\{C(D), D \text{ donnée de taille inférieur ou égale } n\}$.

Définition 1.5.3

Un algorithme est de complexité polynômiale si sa complexité dans le pire des cas est de la forme $O\left(n^k\right)$ où k est une constante. Si sa complexité ne peut être majorée par aucun polynôme, on dit que l'algorithme est de complexité exponentielle**.** Un algorithme est quasi exponentielle si sa complexité est une fonction de la forme $\exp^{O(n)}$.

1.6 Généralités sur la cryptographie à clé publique

L'idée de la cryptographie à clé publique est récente, elle provient de l'article fondateur de Diffie et Hellman [13]. Son principe est basé sur le faite que le mécanisme de chiffrement

est différent de celui de déchiffrement, le chiffrement est fait au moyen d'une clé Publique et le déchiffrement est effectué au moyen d'une clé Secrète.

Une fonction $\psi : M \longrightarrow C$ est dite à sens unique si pour tout x de M, il est facile de calculer $\psi(x)$ mais il est difficile de trouver pour $y \in \psi(M)$ un $x \in M$ tel que $\psi(x) = y$. Le calcul dans le sens inverse (déchiffrement) doit être aussi efficace pour vu qu'on dispose d'une information secrète (la trappe), i.e, une fonction ϕ telle que $\phi \circ \psi = id_M$ où id_M est l'application identique de M. La construction du couple (ψ, ϕ) réalise le mécanisme de chifferement et de déchiffrement et la publication de ψ ne doit rien révéler sur ϕ.

Définition 1.6.1

Une fonction $f : E \longrightarrow F$ est dite à sens unique s'il est facile de calculer $f(x)$, $\forall x \in E$ (complexité au plus polynômiale) et il est difficile (complexité exponentielle) étant donné y de trouver x tel que $y = f(x)$. Une fonction est à sens unique est avec trappe si l'on connaît un secret permettant de l'inverser.

Exemple 1.6.2

Soit G un groupe cyclique d'ordre n et g un générateur de G. Soit la fonction $f : [0, n-1] \longrightarrow G, k \longmapsto f(k) = g^k$, f est à sens unique si G est un groupe cyclique d'ordre assez grand de sorte que connaissant y, la résolution de $y = g^k$ est difficile pour k secret (c'est le problème du logarithme discret). Il existe plusieurs algorithmes pour résoudre le logarithme discret mais ils sont tous exsponentiells ou quasi exponentiels en la taille n de G.

Exemple 1.6.3

On considère l'application $f : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*, x \longmapsto f(x) = x^e$, où $(\mathbb{Z}/n\mathbb{Z})^*$ désigne le groupe d'unité de l'anneau $((\mathbb{Z}/n\mathbb{Z}), +, \times)$, f est à sens unique avec trappe si $n = pq$ produit de deux nombres premiers très grands de même taille de sorte que la factorisation soit difficile et $e \wedge \varphi(n) = 1$ où $\varphi(n) = (p-1)(q-1)$ avec p, q et $\varphi(n)$ sont secretes. Ici la trappe correspond à la connaissance de $\varphi(n)$ car on peut calculer d tel que $ed = 1 \pmod{\varphi(n)}$ avec l'algorithme étendu d'Euclide. Dans ce cas $y = x^e \pmod{n}$ si et seulement si $x = y^d \pmod{n}$.

Chapitre 2

Les systèmes de réécriture de mots

Introduction

Ce chapitre constitue une présentation générale des semi-systèmes de réécriture sur le monoïde libre Σ^* ainsi que certaines propriétés essentielles qui les concernent. La réécriture est un moyen de calcul utilisé en informatique, en algèbre, en logique mathématique et en linguistique. Il s'agit de transformer des objets syntaxiques (mots, termes, programmes, preuves, graphes,...) en appliquant des règles bien précises. Voici quelques exemples classiques d'utilisation de la réécriture:

• Simplifier une expression algébrique (calcul formel).

• Etudier la structure d'un groupe ou d'un monoïde (algèbre combinatoire).

Un semi-système de réécriture est formé d'un ensemble de règles de réécriture, c'est-à-dire de règles de la forme $\exp_g \to \exp_d$ qui veut dire on peut remplacer l'expression gauche ($\exp_g$) par l'expression droite ($\exp_d$) dans une dérivation. Par exemple, soit le semi-système de réécriture :

(1) $x + 0 \to x$

(2) $x + s(y) \to s(x + y)$

où $s(y)$ désigne le successeur de y. Le terme $s(0 + s(0))$ sera réécrit de la façon suivante : $s(0 + s(0))$ devient $s(s(0 + 0))$ par application de la règle (2), puis $s(s(0))$ par application de la règle (1), et plus aucune règle ne s'applique encore. Une règle $\exp_g \to \exp_d$ s'applique à un terme t si ce terme contient une instance de $\exp_g$, c'est à dire $t = u \exp_g v \Rightarrow u \exp_d v$

où la relation $\Rightarrow$ désigne la dérivation associée à la règle $\exp_g \rightarrow \exp_d$. Dans l'exemple ci-dessus, les substitutions qui permettent de passer du terme $x + s(y)$ au terme $0 + s(0)$ sont : $x \mapsto 0, y \mapsto 0$ obtenus à partir des règles (1) et (2) en prenant $x = 0$ et $y = 0$.

On fait remarquer que l'obtention d'une unique forme normale (mot irréductible) est garantie si le semi-système de réécriture est convergent (c'est à dire s'il possède les propriétés de terminaison et de confluence). L'existence d'une forme normale d'un terme n'est pas systématiquement garantie en générale, toutefois la procédure de Knuth-Bendix [20] présenté dans le paragraphe 2.2 ci-dessous peut être, par exemple, appliquée pour tenter de rendre confluent un semi-système qui ne l'est pas déja.

Un système de Thue est une version symétrique d'un semi-système de Thue dans laquelle on peut tout aussi bien remplacer le membre droit d'une règle par son membre gauche.

Contenu du chapitre 2

2.1. Définitions et propriétés.
2.2. Problème de terminaison et confluence d'un semi-système de réécriture de mots.
2.3. Etude des cas où le semi-système de réécriture de mots termine.

2.1 Définitions et propriétés

Définition 2.1.1

Un semi-système de réécriture de mots, dit aussi semi-système de Thue, est un couple $(\Sigma, \mathcal{R})$ où Σ un alphabet fini et $\mathcal{R}$ une relation binaire sur le monoïde libre Σ^*. Tout élément (α, β) de $\mathcal{R}$ est appelé règle de réécriture qu'on note $\alpha \longrightarrow \beta$, avec α est sa partie gauche et β sa partie droite. Des règles $\alpha \longrightarrow \beta_1, \alpha \longrightarrow \beta_2, ..., \alpha \longrightarrow \beta_k$ ayant mème partie gauche sont souvent notées $\alpha \longrightarrow \beta_1 \setminus \beta_2 \setminus ... \setminus \beta_k$.

Exemple 2.1.2

Soient $\Sigma = \{\alpha, \beta, \gamma\}$ et $\mathcal{R} = \{\alpha\beta \longrightarrow \beta\alpha, \beta\alpha \longrightarrow \alpha\beta, \gamma \longrightarrow \epsilon, \epsilon \longrightarrow \gamma\}$, $(\Sigma, \mathcal{R})$ est un système de réécriture.

Définition 2.1.3

Appliquer une règle quelconque $u \longrightarrow v$ de $\mathcal{R}$ à un mot w contenant le facteur u consiste à remplacer u par v dans w. S'il n'y a aucune règle de $(\Sigma, \mathcal{R})$ applicable à w, alors w est dit irréductible ou sous la forme normale. Etant données deux mots $w_1, w_2 \in \Sigma^*$, on dit que w_2 dérive directement de w_1, et on note $w_1 \underset{\mathcal{R}}{\Rightarrow} w_2$, si et seulement si, il existe une règle $u \longrightarrow v$ de $\mathcal{R}$ et $x, y \in \Sigma^*$ tels que : $w_1 = xuy$ et $w_2 = xvy$. On dit que w_2 dérive de w_1, et on note $w_1 \overset{*}{\underset{\mathcal{R}}{\Rightarrow}} w_2$, s'il existe une suite finie de mots $u_0, u_1, ..., u_n$ de Σ^* avec, $u_0 = w_1, u_i \underset{\mathcal{R}}{\Rightarrow} u_{i+1}, \forall 0 \leq i \leq n-1$ et $u_n = w_2$. Notons que la relation $\overset{*}{\underset{\mathcal{R}}{\Rightarrow}}$ est la fermeture réflexive et transitive de $\underset{\mathcal{R}}{\Rightarrow}$.

Exemples 2.1.4

1. Soient $\Sigma_1 = \{0, 1\}$ et $\mathcal{R}_1 = \{10 \longrightarrow 01\}$. Soient $w_1, w_2 \in \Sigma_1^*$, si $w_1 \overset{*}{\underset{\mathcal{R}_1}{\Rightarrow}} w_2$, alors w_2 est la permutation des lettres de w_1 où tous les 0 seront avant les 1. Ce semi-système de réécriture trie les mots constitués de même chiffres binaires.

2. Soient $\Sigma_2 = \{0, 1, +\}$ et $\mathcal{R}_2 = \{0 + 0 \longrightarrow 0, 0 + 1 \longrightarrow 1, 1 + 0 \longrightarrow 1, 1 + 1 \longrightarrow 0\}$.

Ce semi-système de réécriture calcul la somme (modulo 2) d'une suite d'entiers binaires.

3. Soient $\Sigma_3 = \{0, 1, +, E\}$ et $\mathcal{R}_3 = \{E \longrightarrow 0, E \longrightarrow 1, E \longrightarrow E + E\}$.

Pour tout $w \in \{0, 1, +\}^*$, on a $E \overset{*}{\underset{\mathcal{R}_3}{\Rightarrow}} w$ si, et seulement si w est une expression construite avec les 0 et 1 et l'opérateur $+$.

4. Considérons le semi-système de réécriture sur la dérivation symbolique par rapport à x défini par:

$$\mathcal{R}_4 = \left\{ \begin{array}{c} D_x x \longrightarrow 1, D_x a \longrightarrow 0, D_x(y+z) \longrightarrow D_x y + D_x z, D_x(y*z) \longrightarrow z * D_x y + y * D_x z, \\ D_x(y-z) \longrightarrow D_x y - D_x z, D_x(-y) \longrightarrow -D_x y, D_x(y/z) \longrightarrow z * D_x y - y * D_x z)/z^2 \end{array} \right\}.$$

où a étant un symbole de constante.

5. Considérons le système de Thue donné par l'alphabet $\Sigma_5 = \{\alpha, \beta, E\}$ et la relation $\mathcal{R}_5 = \{E \longrightarrow \epsilon, \epsilon \longrightarrow E, E \longrightarrow \alpha\beta E, \alpha\beta E \longrightarrow E, \alpha\beta \longrightarrow \beta\alpha, \beta\alpha \longrightarrow \alpha\beta\}$. Par exemple on a la dérivation infinie suivante : $....\underset{\mathcal{R}_5}{\Longleftrightarrow} E \underset{\mathcal{R}_5}{\Longleftrightarrow} \alpha\beta E \underset{\mathcal{R}_5}{\Longleftrightarrow} \beta\alpha E \underset{\mathcal{R}_5}{\Longleftrightarrow} ...$

Définition 2.1.5

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture . Si un mot $u \in \Sigma^*$ peut se réécrire de manière non triviale, on dit qu'il est réductible. Dans le cas contraire, il est dit irréductible. On note alors $IRR(\mathcal{R})$ l'ensemble des éléments irréductibles de Σ^*.

Exemples 2.1.6

Soient $\Sigma = \{\alpha, \beta\}$ et $\mathcal{R} = \{\alpha\beta \longrightarrow \beta\alpha\}$. L'ensemble des mots irréductibles est

$IRR(\mathcal{R}) = \{\beta^n \alpha^m : n, m \in \mathbb{N}\}$.

Les mots irréductibles sont en effet les éléments de Σ^* qui ne contiennent pas $\alpha\beta$.

Notation 2.1.7

Pour un semi-système de réécriture $(\Sigma, \mathcal{R})$, on note $D(\mathcal{R}) = \{u \in \Sigma^*, \exists v \in \Sigma^* : u\mathcal{R}v\}$.

Proposition 2.1.8

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture. On a :

$IRR(\mathcal{R}) = \Sigma^* - \Sigma^* D(R)\Sigma^*$.

Démonstration

On montrer que $\Sigma^* - IRR(\mathcal{R}) = \Sigma^* D(\mathcal{R})\Sigma^*$:

Soit $w \in \Sigma^*$. On a

$w \in \Sigma^* - IRR(\mathcal{R}) \Leftrightarrow$ il existe $(u, v) \in \mathcal{R}$ tel que u soit un sous-mot de w

$\Leftrightarrow$ il existe $u \in D(\mathcal{R})$ tel que $w \in \Sigma^* u \Sigma^* \Leftrightarrow w \in \Sigma^* D(\mathcal{R})\Sigma^*$. $\square$

Définition 2.1.9

Soient $S_1 = (\Sigma_1, \mathcal{R}_1)$ et $S_2 = (\Sigma_2, \mathcal{R}_2)$ deux semi-systèmes de réécriture. Un morphisme de semi-systèmes de réécriture de S_1 vers S_2 est une application $\psi : \Sigma_1^* \longrightarrow \Sigma_2^*$ qui est faiblement compatible avec les relations de réductions, c'est-à-dire telle que $\psi(\underset{\mathcal{R}_1}{\Rightarrow}) \subseteq \overset{*}{\underset{\mathcal{R}_2}{\Rightarrow}}$, ou encore telle que, pour tous $x, y \in \Sigma_1^*$ vérifiant $x \underset{\mathcal{R}_1}{\Rightarrow} y$, on a $\psi(x) \overset{*}{\underset{\mathcal{R}_2}{\Rightarrow}} \psi(y)$.

Un tel morphisme est dit :

• Non contractant si $\psi(\underset{\mathcal{R}_1}{\Rightarrow}) \subseteq \overset{+}{\underset{\mathcal{R}_2}{\Rightarrow}}$, ce qui équivaut à dire si $x\underset{\mathcal{R}_1}{\Rightarrow}y$, alors $\psi(x)\overset{+}{\underset{\mathcal{R}_2}{\Rightarrow}}\psi(y)$.
• Strict si $\psi(\underset{\mathcal{R}_1}{\Rightarrow}) \subseteq \underset{\mathcal{R}_2}{\Rightarrow}$, ce qui équivaut à dire si $x\underset{\mathcal{R}_1}{\Rightarrow}y$, alors $\psi(x)\underset{\mathcal{R}_2}{\Rightarrow}\psi(y)$.

2.2 Problème de terminaison et confluence d'un semi-système de réécriture de mots

Nous allons présenter ici deux propriétés de semi-système de réécriture telles que : la terminaison et la confluence, si un semi-système de réécriture termine, cela signifie qu'il est impossible, partant d'un certain élément, d'effectuer une infinité d'opérations de dérivation quel que soit le point de départ, on arrivera, après un nombre fini d'opérations, à un élément sur lequel on ne peut plus agir, c'est-à-dire un élément x tel qu'il n'existe pas de y vérifiant $x\underset{\mathcal{R}}{\Rightarrow}y$. Et dans un semi-système de réécriture confluent, les choix effectués n'ont pas d'importance.

Définition 2.2.1

On dit qu'un semi-système de réécriture $(\Sigma, \mathcal{R})$ termine ou qu'il est noethérien s'il n'existe pas de chaine de réécriture infinie $w_0\underset{\mathcal{R}}{\Rightarrow}w_1...\underset{\mathcal{R}}{\Rightarrow}w_n\underset{\mathcal{R}}{\Rightarrow}...$

Exemples 2.2.2

Le semi-système de réécriture $(\Sigma_1, \mathcal{R}_1)$ avec $\Sigma_1 = \{\alpha, \beta\}$ et la relation $\mathcal{R}_1 = \{\alpha \longrightarrow \alpha\beta\}$, est non noethérien car la dérivation $\alpha\underset{\mathcal{R}_1}{\Rightarrow}\alpha\beta\underset{\mathcal{R}_1}{\Rightarrow}\alpha\beta\beta\underset{\mathcal{R}_1}{\Rightarrow}\alpha\beta\beta\beta\underset{\mathcal{R}_1}{\Rightarrow}...$ est bien infinie dans $(\Sigma_1, \mathcal{R}_1)$. De même le semi-système de réécriture $(\Sigma_2, \mathcal{R}_2)$ avec $\Sigma_2 = \{\alpha, \beta\}$ et la relation $\mathcal{R}_2 = \{\alpha \longrightarrow \beta, \beta \longrightarrow \alpha\}$, est non noethérien car la dérivation $\alpha\underset{\mathcal{R}_2}{\Rightarrow}\beta\underset{\mathcal{R}_2}{\Rightarrow}\alpha\underset{\mathcal{R}_2}{\Rightarrow}\beta\underset{\mathcal{R}_2}{\Rightarrow}...$ est bien infinie dans $(\Sigma_2, \mathcal{R}_2)$. Par contre le semi-système de réécriture $(\Sigma_3, \mathcal{R}_3)$, avec $\Sigma_3 = \{\alpha, \beta\}$ et la relation $\mathcal{R}_3 = \{\alpha\beta \longrightarrow \alpha\}$, est noethérien, car la seule règle $(\alpha\beta, \alpha)$ est applicable à un mot w de Σ_3^* si, et seulement si, $|w|_{\alpha\beta} \neq 0$, et si $|w|_\beta = k$, alors pas plus de k dérivations le processus de substitution termine.

Remarques 2.2.3

1. On remarque que si $(\Sigma, \mathcal{R})$ est un semi-système de réécriture tel qu'il existe un $u \in \Sigma^*$ avec $u\mathcal{R}u$, alors il ne termine pas. En particulier, tout semi-système de réécriture dont la relation est réflexive ne termine pas, c'est le cas de $(\mathbb{N}, \geq)$. En revanche, le système de réécriture $(\mathbb{N}, >)$ termine.

2. La terminaison implique que tout élément possède au moins une forme normale, on dit que $(\Sigma, \mathcal{R})$ est normalisant. La normalisation est une propriété plus faible que la terminaison, même dans le cas où la forme normale de chaque élément est unique, par exemple considérons un ensemble réduit à deux éléments, notés u et v, que l'on munit de la relation $\mathcal{R} = \{u \longrightarrow u, u \longrightarrow v\}$. alors v est l'unique forme normale de u et de v, cependant, comme nous l'avons déjà remarqué, le fait que u vérifie $u\mathcal{R}u$ empêche $\mathcal{R}$ de terminer.

Définition 2.2.4

Soient $(\Sigma, \mathcal{R})$ un semi-système de réécriture et deux mots $u, v \in \Sigma^*$. S'il existe $w \in \Sigma^*$ tel que $u \underset{\mathcal{R}}{\Rightarrow} w$ et $v \underset{\mathcal{R}}{\Rightarrow} w$, alors on dit que u et v sont joignables. On désignera par $u{\downarrow}v$ l'ensemble de tous les éléments $w \in \Sigma^*$ tels que $u \underset{\mathcal{R}}{\Rightarrow} w$ et $v \underset{\mathcal{R}}{\Rightarrow} w$. (Ainsi, u et v sont joignables si, et seulement si $u{\downarrow}v \neq \emptyset$.

Exemple 2.2.5

Soient $\Sigma = \{\alpha, \beta\}$ et $\mathcal{R} = \{\alpha\beta \longrightarrow \beta\alpha\}$, $u = \alpha\beta\beta\alpha$ et $v = \beta\alpha\alpha\beta$, on a $\alpha\beta\beta\alpha \underset{\mathcal{R}}{\Rightarrow} \beta\alpha\beta\alpha$ et $\beta\alpha\alpha\beta \underset{\mathcal{R}}{\Rightarrow} \beta\alpha\beta\alpha$, donc $\beta\alpha\beta\alpha \in u{\downarrow}v$ et par conséquent u et v sont joignables.

Théorème 2.2.6

Soit (Σ_1, R_1) un semi-système de réécriture. Les assertions suivantes sont équivalentes :

1. *(Σ_1, R_1) est noethèrien.*
2. *Il existe un ordre strict $>$ sur Σ_1^* tel que $(\Sigma_1^*, >)$ termine et tel que si $x \underset{\mathcal{R}_1}{\Rightarrow} y$ alors $x > y$.*
3. *Il existe un autre semi-système de réécriture (Σ_2, R_2) qui termine ainsi qu'un morphisme de semi-systèmes de réécriture non contractant $\psi : (\Sigma_1, R_1) \longrightarrow (\Sigma_2, R_2)$.*

Démonstration

$1 \implies 2$. On montrer que $\overset{+}{\underset{\mathcal{R}_1}{\Rightarrow}}$ est un ordre strict qui termine sur Σ_1^*.

Pour l'anti réflexivité, on suppose qu'il existe $x \in \Sigma_1^*$ tel que $x \overset{+}{\underset{\mathcal{R}_1}{\Rightarrow}} x$, par définition, il existe un chemin de longueur l non nulle de x à x dans $(\Sigma_1, \mathcal{R}_1)$, ce qui équivaut à dire, il existe $l \in \mathbb{N} - \{0\}$ tel que $(x, x) \in \left(\underset{\mathcal{R}_1}{\Rightarrow}\right)^l$ en mettant bout à bout une infinité de copies de ce chemin, on obtient un chemin infini (une dérivation infinie) dans $(\Sigma_1, \mathcal{R}_1)$, ce qui contredit l'hypothèse.

Pour la transitivité, on suppose que x, y, et z sont trois éléments de Σ_1^* tels que $x \overset{+}{\underset{\mathcal{R}_1}{\Rightarrow}} y$ et $y \overset{+}{\underset{\mathcal{R}_1}{\Rightarrow}} z$: Il existe donc un chemin de longueur non nulle dans $(\Sigma_1, \mathcal{R}_1)$ de x à y et un autre de

y à z, en les recollant, on obtient un chemin de longueur non nulle de x à z dans $(\Sigma_1, \mathcal{R}_1)$, ce qui donne $x \overset{+}{\underset{\mathcal{R}_1}{\Rightarrow}} z$.
Enfin, pour la terminaison, on suppose qu'il existe une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de Σ_1^* tels que $x_n \overset{+}{\underset{\mathcal{R}_1}{\Rightarrow}} x_{n+1}$ pour tout n, il existe donc, pour tout n, un chemin de longueur non nulle de x_n à x_{n+1} dans $(\Sigma_1, \mathcal{R}_1)$, mis bout à bout, tous ces chemins donnent un chemin infini partant de x_0 dans $(\Sigma_1, \mathcal{R}_1)$, ce qui contredit encore l'hypothèse.
Il ne reste plus qu' à montrer que si $x \underset{\mathcal{R}_1}{\Rightarrow} y$ alors $x \overset{+}{\underset{\mathcal{R}_1}{\Rightarrow}} y$. Ce qui est, par définition de la fermeture transitive $\overset{+}{\underset{\mathcal{R}_1}{\Rightarrow}}$ de $\underset{\mathcal{R}_1}{\Rightarrow}$.

2 $\Longrightarrow$ 3. On prend $\Sigma_2 = \Sigma_1$ et la relation $\mathcal{R}_2$ est l'ordre strict $>$ et ψ est l'application identique de Σ_1^* et on le note $id_{\Sigma_1^*}$. Par hypothèse, $(\Sigma_1, >)$ termine et ψ est un morphisme strict, donc non contractant, de $(\Sigma_1, \mathcal{R}_1)$ vers $(\Sigma_1, >)$.

2 $\Longrightarrow$ 3. Supposons qu'il existe une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de Σ_1^* tels que $x_n \underset{\mathcal{R}_1}{\Rightarrow} x_{n+1}$ pour tout n. Alors, le morphisme ψ nous donne une suite $(\psi(x_n))_{n\in\mathbb{N}}$ d'éléments de Σ_2^* tels que $\psi(x_n) \overset{+}{\underset{\mathcal{R}_2}{\Rightarrow}} \psi(x_{n+1})$ pour tout n. Or, comme $(\Sigma_2, \mathcal{R}_2)$ termine, en appliquant $1 \Rightarrow 2$, on a la terminaison de $(\Sigma_2, \overset{+}{\underset{\mathcal{R}_2}{\Rightarrow}})$, ce qui contredit l'existence d'une telle suite. □

Définition 2.2.7

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture. On dit que le principe de récurrence est vrai dans $(\Sigma, \mathcal{R})$ si, pour toute propriété P définie sur Σ^*, on a,
si pour tout $x \in \Sigma^*$, le fait que $P(y)$ soit vraie pour tous les $y \in \Sigma^*$ tels que $x \overset{+}{\underset{\mathcal{R}}{\Rightarrow}} y$ implique que $P(x)$ est vraie, alors $P(x)$ est vraie pour tout $x \in \Sigma^*$, en symboles,

$$(\forall x \in \Sigma^*, (\forall y \in \Sigma^* : \left(P(y) \text{ et } x \overset{+}{\underset{\mathcal{R}}{\Rightarrow}} y\right) \Rightarrow P(x))) \Rightarrow (\forall x P(x)).$$

Exemple 2.2.8

Dans le cas de $(\mathbb{N}, >)$, il s'agit du principe de récurrence usuelle :

si $P(0)$ est vraie et $(\forall n \in \mathbb{N}, P(m)$ est vraie tels que $n > m) \Rightarrow P(n)$ est vraie, alors $P(n)$ est vraie pour tout n, en symboles,

$$(P(0) \text{ et } (\forall n \in \mathbb{N}, \forall m \in \mathbb{N} : (P(m) \text{ et } n > m) \Rightarrow P(n))) \Rightarrow (\forall n P(n)).$$

Dans cet exemple en fait remarquer que la relation $>$ est transitive, alors sa fermeture transitive est égale à lui-même.

Théorème 2.2.9

Un semi-système de réécriture $(\Sigma, \mathcal{R})$ *est noethèrien si, et seulement si le principe de récurrence est vrai dans* $(\Sigma, \mathcal{R})$.

Démonstration

En fait la démonstration de l'implication : si le semi-système de réécriture $(\Sigma, \mathcal{R})$ est noethérien alors, le principe de récurrence est vrai dans $(\Sigma, \mathcal{R})$, par l'absurde. Supposons que $(\Sigma, \mathcal{R})$ est noethérien mais que le principe de récurrence n'est pas vrai dans $(\Sigma, \mathcal{R})$. Alors il existe une propriété P telle que :

• pour tout $x \in \Sigma^*$, le fait que $P(y)$ soit vraie pour tous les $y \in \Sigma^*$ tels que $x \overset{+}{\underset{\mathcal{R}}{\Rightarrow}} y$ implique que $P(x)$ est vraie,

• il existe x_0 dans Σ^* tel que $P(x_0)$ est fausse.

Alors, il existe x_1 dans Σ^* tel que $x_0 \overset{+}{\underset{\mathcal{R}}{\Rightarrow}} x_1$ et $P(x_1)$ est fausse, sinon, on aurait $P(x_0)$. On recommence à partir de x_1, il existe forcément un x_2 dans Σ^* tel que $x_1 \overset{+}{\underset{\mathcal{R}}{\Rightarrow}} x_2$ et $P(x_2)$ est fausse. On peut donc construire un chemin de réduction infini dans $(\Sigma, \mathcal{R})$ qui ne termine pas, ce qui contredit le fait que $(\Sigma, \mathcal{R})$ est noethérien.

Réciproquement **:** supposons que le principe de récurrence est vrai dans $(\Sigma, \mathcal{R})$. On note $P(x)$ la formule propositionnelle :

$P(x)$:(Il n'existe pas de chemin de réduction infini partant de x dans $(\Sigma, \mathcal{R})$).

Soit $x \in \Sigma^*$ et supposons que $P(y)$ est vraie pour tous les $y \in \Sigma^*$ tels que $x \overset{+}{\underset{\mathcal{R}}{\Rightarrow}} y$, en particulier, il n'existe aucun chemin infini partant d'un y tel que $x \overset{+}{\underset{\mathcal{R}}{\Rightarrow}} y$, ce qui exclut la possibilité d'avoir un chemin infini partant de x. Donc $(\Sigma, \mathcal{R})$ est noethérien. □

Définition 2.2.10

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture. Un branchement de $(\Sigma, \mathcal{R})$ est un triplet (x, y, z) d'éléments de Σ^* tels que $x \overset{*}{\underset{\mathcal{R}}{\Rightarrow}} y$ et $x \overset{*}{\underset{\mathcal{R}}{\Rightarrow}} z$, x est appelé la source d'un tel branchement. On dit qu'un branchement (x, y, z) est local si $x \underset{\mathcal{R}}{\Rightarrow} y$ et $x \underset{\mathcal{R}}{\Rightarrow} z$. Un branchement (x, y, z) est dit confluent s'il existe un $w \in \Sigma^*$ tel que $y \overset{*}{\underset{\mathcal{R}}{\Rightarrow}} w$ et $z \overset{*}{\underset{\mathcal{R}}{\Rightarrow}} w$. On dit d'un tel w qu'il ferme le branchement (x, y, z).

Définition 2.2.11

On dit qu' un semi-système de réécriture est confluent (resp. localement confluent) si tous ses branchement (resp. branchements locaux) sont confluents. On dit aussi que la relation binaire $\mathcal{R}$ est (localement) confluente.

Exemple 2.2.12

On considère le semi-système de réécriture $(\Sigma, \mathcal{R})$ où $\Sigma = \{\alpha, \beta\}$, $\mathcal{R} = \{\alpha\beta \longrightarrow \alpha, \beta\alpha \longrightarrow \beta\}$. Ce semi-système n'est pas confluent, car on a :

$\alpha\beta\alpha \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \alpha\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \alpha$ et $\alpha\beta\alpha \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \alpha\alpha$, mais les mots $\alpha\alpha, \alpha$ sont en formes normaux.

Proposition 2.2.13

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture.

1. *Pour tout (x, y) de R, le branchement (x, y, y) est confluent*

2. *Si (x, y, z) est un branchement confluent, alors*

- *Pour tout mot u de Σ^*, les deux branchement $(ux, u\,\mathrm{y}, uz)$ et (xu, yu, zu) sont confluents.*
- *Pour tous mots u, v de Σ^*, le branchement $(uxv, u\,\mathrm{y}v, uzv)$ est confluent.*

3. *Pour tous $(x, y), (z, t)$ de R, le branchement (xz, yz, xt) est confluent. Dans ce cas on dit que les réductions (xz, yz) et (xz, xt) sont disjointes.*

Définition 2.2.14

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture. Un branchement est critique s'il n'est pas de la forme $(ux, u\,\mathrm{y}, uz)$ ou (xu, yu, zu) où (x, y, z) un branchement, u est un mot non vide et ses réductions ne sont ni égales ni disjointes.

Proposition 2.2.15

Un branchement critique dans un semi-système de réécriture $(\Sigma, \mathcal{R})$ est nécessairement d'une de ces deux formes :

- *Un chevauchement (uxv, yv, uz) où $(ux, y), (xv, z) \in R$ et $u, x, v \neq \epsilon$.*
- *Une inclusion (uxv, uyv, z) où $(x, y), (uxv, z) \in R$ et $ux, xv \neq \epsilon$.*

Proposition 2.2.16

Si tous les branchements critiques d'un semi-système de réécriture $(\Sigma, \mathcal{R})$ sont confluents, alors tous les branchements le sont.

Démonstration

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture dont tous les branchements critiques sont confluents. Un branchement (x, y, z) est forcément dans un des cas suivants :

• Si (x, y, z) est critique, alors, par hypothèse, il est confluent.

• Si $y = z$, on a vu que le branchement (x, y, y) est confluent.

• Si les réductions $x \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} y$ et $x \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} z$ sont disjointes, on a vu que le branchement (x, y, z) est confluent.

• Si $(x, y, z) = (ux', uy', uz')$ ou $(x, y, z) = (x'u, y'u, z'u)$, où (x', y', z') est un branchement et u un mot différent de ϵ, on peut supposer que $(x', y', z') \neq (vx", vy", vz")$ et $(x', y', z') \neq (x"v, y"v, z"v)$ où $(x", y", z")$ est un branchement et v un mot différent de ϵ. Donc le branchement (x', y', z') entre forcément dans un des cas précédents. Ainsi, (x', y', z') est confluent. Alors, on a vu que les branchements (ux', uy', uz') et $(x'u, y'u, z'u)$ sont confluents aussi. Donc (x, y, z) est confluent. □

Exemple 2.2.17

Soient $\Sigma = \{\alpha, \beta\}$ et $\mathcal{R} = \{\alpha\beta \longrightarrow \epsilon, \beta\alpha \longrightarrow \epsilon\}$, on a donc deux branchements critiques confluents $(\alpha\beta\alpha, \alpha, \alpha)$, $(\beta\alpha\beta, \beta, \beta)$. Donc $(\Sigma, \mathcal{R})$ est confluent.

Définition 2.2.18

Un semi-système de réécriture $S = (\Sigma, \mathcal{R})$ est dit convergent ou complet s'il termine et s'il est confluent. On dit aussi que la relation binaire $\mathcal{R}$ est convergente.

Exemples 2.2.19

1. Soient $\Sigma = \{0, 1\}$ et $\mathcal{R}_1 = \{01 \longrightarrow 1, 11 \longrightarrow 1\}$, le semi-système $(\Sigma, \mathcal{R})$ est convergent, mais si on remplace la règle $11 \longrightarrow 1$ par la règle $11 \longrightarrow 11$, le semi-système $(\Sigma, \mathcal{R})$ non convergent.

2. Soient $\Sigma_2 = \{\alpha, \beta\}$ et $\mathcal{R}_2 = \{\alpha\beta \longrightarrow \epsilon\}$, le système $(\Sigma, \mathcal{R})$ est convergent, car on a, $\forall u, v \in \Sigma^* : u\alpha\beta v \underset{\mathcal{R}_2}{\Rightarrow} uv$, et par suite on distingue deux cas:

· Si $u \neq \alpha$ ou $v \neq \beta$ alors le mot uv est irréductible.

·Si $u = \alpha$ et $v = \beta$, on $\alpha\alpha\beta\beta \underset{\mathcal{R}_2}{\Rightarrow} \alpha\beta \underset{\mathcal{R}_2}{\Rightarrow} \epsilon$.

3. Soient $\Sigma_3 = \{\alpha, \beta, \gamma\}$ et $\mathcal{R}_3 = \{\alpha\beta \longrightarrow \epsilon, \beta\gamma \longrightarrow \epsilon\}$, le système n'est pas confluent, car on a $\alpha\beta\gamma \underset{\mathcal{R}_3}{\Rightarrow} \alpha$ et $\alpha\beta\gamma \underset{\mathcal{R}_3}{\Rightarrow} \gamma$, mais les mots α et γ sont sous formes irréductibles.

Théorème 2.2.20

Un semi-système de réécriture $(\Sigma, \mathcal{R})$ est convergent si et seulement si il termine et s'il est localement confluent.

Démonstration

Pour l'implication directe, supposons que $(\Sigma, \mathcal{R})$ est un semi-système de réécriture convergent. Par définition, il termine et est confluent. Or, il est évident que la confluence implique la confluence locale puisque les branchements locaux sont aussi des branchements.

Réciproquement: Supposons que $(\Sigma, \mathcal{R})$ termine et qu'il est localement confluent. Comme $(\Sigma, \mathcal{R})$ termine, on peut utiliser le principe de récurrence pour monter que tout branchement est confluent. Plus précisément, on pose $P(x)$ la formule propositionnelle
$P(x)$: (Tout branchement de source x est confluent).
Si x est une forme normale, alors le seul branchement de source x est (x, x, x) qui est toujours confluent: on a $x \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} x$ pour tout x. A présent, considérons un x dans Σ^* et supposons que $P(y)$ est vraie pour tous les $y \in \Sigma^*$ tels que $x \underset{\mathcal{R}}{\overset{+}{\Rightarrow}} y$.
Soit (x, y, z) un branchement, distinguons deux cas:
1. Si $x = y$ (ou $x = z$), le branchement est confluent car $y = x \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} z$ et $z \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} z$.
2. Sinon, il existe y' et x' dans Σ^* tels que $x \underset{\mathcal{R}}{\Rightarrow} y' \underset{\mathcal{R}}{\overset{+}{\Rightarrow}} y$ et $x \underset{\mathcal{R}}{\Rightarrow} z' \underset{\mathcal{R}}{\overset{+}{\Rightarrow}} z$: on a un branchement local (x, y', z') donc, comme $(\Sigma, \mathcal{R})$ est localement confluent, il existe $w \in \Sigma^*$ tel que $y' \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} w$ et $z' \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} w$. On obtient donc un branchement (y, y', w). Comme $x \underset{\mathcal{R}}{\Rightarrow} y'$, on peut appliquer l'hypothèse de récurrence à y' et en déduire qu'il existe $u \in \Sigma^*$ tel que $y \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} u$ et $w \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} u$. Puisque $x \underset{\mathcal{R}}{\Rightarrow} z'$, on applique de nouveau l'hypothèse de récurrence à z' pour conclure que le branchement (z', u, z) est confluent, c'est-à-dire qu'il existe $v \in \Sigma^*$ tel que $u \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} v$ et $z \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} v$. Le branchement (x, y, z) est donc confluent et $P(x)$ est vérifiée. $\square$

Corollaire 2.2.21

Si un semi-système de réécriture est noethérien et si tous les branchements critiques sont confluents, alors il est convergent.

Exemple 2.2.22

Soient $\Sigma = \{\alpha, \beta\}$ et $\mathcal{R} = \{\alpha\beta \longrightarrow \epsilon, \beta\alpha \longrightarrow \epsilon\}$, on a deux branchements critiques $(\alpha\beta\alpha, \alpha, \alpha), (\beta\alpha\beta, \beta, \beta)$ qui sont confluents, le semi-système $(\Sigma, \mathcal{R})$ est convergent.

L'algorithme de Knuth-Bendix: [21]

L'algorithme de Knuth-Bendix consiste à transformer un semi-système de réécriture noethérien en un semi-système de réécriture convergent. Il s'agit d'une procédure de complétion, qui pour chaque branchement critique, regarde si il est conflue, et dans le cas où il n'est pas confluent, donc on rajoute une règle permettant d'obtenir la confluence.

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture noethérien. On notera $BC(\mathcal{R})$ l'ensemble des branchements critiques formées à partir des règles de $\mathcal{R}$.

Entrées**:** Un système de réécriture noethérien $(\Sigma, \mathcal{R})$ et un ordre de terminaison $<$.

Sorties**:** Un système de réécriture convergent $(\Sigma, \mathcal{R}')$, si la procédure termine avec succès, "Echec" si la procédure échoue.

Initialisation:

S'il existe un couple $(u, v) \in \mathcal{R}$ tel que $u \neq v, u \not< v$ et $v \not< u$ alors l'algorithme termine et on fait retourner "Echec",

Sinon $i := 0$ et $\mathcal{R}_0 := \{u \longrightarrow v \setminus (u, v) \in \mathcal{R} \text{ et } u < v\}$;

Répéter

$\mathcal{R}_{i+1} := \mathcal{R}_i$;

Pour chaque paire $\{x \longrightarrow y, x \longrightarrow z\} \in BC(\mathcal{R})$ faire

Réduire y et z à des formes normales $IRR(y)$ et $IRR(z)$;

Si $IRR(y) \neq IRR(z), IRR(y) \not< IRR(z)$ et $IRR(z) \not< IRR(y)$ alors terminer et retourner "Echec";

Si $IRR(z) < IRR(y)$ alors $\mathcal{R}_{i+1} := \mathcal{R}_{i+1} \cup \{IRR(y) \longrightarrow IRR(z)\}$;

Si $IRR(y) < RR(z)$ alors $\mathcal{R}_{i+1} := \mathcal{R}_{i+1} \cup \{IRR(z) \longrightarrow IRR(y)\}$;

$i := i + 1$;

Fin

Jusqu'à $\mathcal{R}_i := \mathcal{R}_{i-1}$;

Retourner $\mathcal{R}_i$;

Exemple 2.2.23 [21]

Soient $\Sigma = \{\alpha, \beta, \gamma\}$ et $\mathcal{R} = \{\alpha\beta\alpha \longrightarrow \beta\alpha\beta, \alpha\beta \longrightarrow \gamma\}$. Ce semi-système est noethérien mais il n'est pas confluent. Nous allons tenter grâce à l'algorithme de Knuth-Bendix de trouver un semi-système $(\Sigma, \mathcal{R}')$ convergent. Nous avons un premier branchement critique :

$(\alpha\beta\alpha, \beta\gamma, \gamma\alpha)\,; \alpha\beta\alpha \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\alpha, \alpha\beta\alpha \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \beta\alpha\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \beta\gamma.$

On rajoute donc la règle $\gamma\alpha \longrightarrow \beta\gamma$ au semi-système $(\Sigma, \mathcal{R})$. Nous avons un autre branchement critique :

$(\alpha\beta\alpha\beta, \beta\gamma\beta, \gamma\gamma)\,; \alpha\beta\alpha\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \beta\alpha\beta\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \beta\gamma\beta; \alpha\beta\alpha\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \alpha\beta\gamma \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\gamma.$

On rajoute donc la règle $\beta\gamma\beta \longrightarrow \gamma\gamma$ au semi-système $(\Sigma, \mathcal{R})$. Cette nouvelle règle forme un nouvel branchement critique non confluent: $(\alpha\beta\gamma\beta, \gamma\gamma\beta, \alpha\gamma\gamma)\,; \alpha\beta\gamma\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\gamma\beta, \alpha\beta\gamma\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \alpha\gamma\gamma.$

Il faut rajouter la règle $\gamma\gamma\beta \longrightarrow \alpha\gamma\gamma$ au semi-système $(\Sigma, \mathcal{R})$. Vérifions à présent si les branchements critiques restants sont confluents :

1. $(\gamma\alpha\beta, \beta\gamma\beta, \gamma\gamma) : \gamma\alpha\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \beta\gamma\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\gamma; \gamma\alpha\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\gamma.$
2. $(\alpha\beta\alpha\beta\alpha, \gamma\beta\gamma, \gamma\beta\gamma) : \alpha\beta\alpha\beta\alpha \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \alpha\beta\beta\alpha\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\beta\alpha\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\beta\gamma; \alpha\beta\alpha\beta\alpha \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \beta\alpha\beta\beta\alpha \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \beta\gamma\beta\alpha \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\gamma\alpha \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\beta\gamma.$
3. $(\gamma\alpha\beta\alpha, \gamma\beta\gamma, \gamma\beta\gamma) : \gamma\alpha\beta\alpha \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\beta\alpha\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\beta\gamma; \gamma\alpha\beta\alpha \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \beta\gamma\beta\alpha \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\gamma\alpha \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\beta\gamma.$
4. $(\gamma\gamma\beta\gamma\beta, \gamma\gamma\gamma\gamma, \gamma\gamma\gamma\gamma) : \gamma\gamma\beta\gamma\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\gamma\gamma\gamma; \gamma\gamma\beta\gamma\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \alpha\gamma\gamma\gamma\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \alpha\gamma\alpha\gamma\gamma \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \alpha\beta\gamma\gamma\gamma \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\gamma\gamma\gamma.$
5. $(\beta\gamma\beta\gamma\beta, \beta\gamma\gamma\gamma, \beta\gamma\gamma\gamma) : \beta\gamma\beta\gamma\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \beta\gamma\gamma\gamma; \beta\gamma\beta\gamma\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\gamma\gamma\beta \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \gamma\alpha\gamma\gamma \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} \beta\gamma\gamma\gamma.$

On obtient un nouvel semi-système convergent $(\Sigma, \mathcal{R}')$ où

$\mathcal{R}' = \{\alpha\beta\alpha \longrightarrow \beta\alpha\beta, \alpha\beta \longrightarrow \gamma, \gamma\alpha \longrightarrow \beta\gamma, \beta\gamma\beta \longrightarrow \gamma\gamma, \gamma\gamma\beta \longrightarrow \alpha\gamma\gamma\}.$

2.3 Etude des cas où le semi-système de réécriture de mots termine

Les corollaires qui suivent sont des conséquences de l'implication 3 $\Longrightarrow$ 1 du théorème 2.2.6

Corollaire 2.3.1 [15]

Soit (Σ_1, R_1) *un semi-système de réécriture tel que* $R_1 = \{\alpha_i \longrightarrow \beta_i, 1 \leq i \leq n, n \in \mathbb{N}^*\}$. *Si* $\forall 1 \leq i \leq n, |\alpha_i| > |\beta_i|$, *alors le semi-système* (Σ_1, R_1) *est noethérien.*

Démonstration

On prend $(\Sigma_2, \mathcal{R}_2) = (\mathbb{N}, >)$, on a $(\mathbb{N}, >)$ termine et soit l'application de longueur
$\psi : (\Sigma_1, \mathcal{R}_1) \longrightarrow (\mathbb{N}, >)$, définie par $w \longmapsto |w|$.
L'application ψ est un morphisme de monoïdes et $\forall w_1, w_1 \in \Sigma_1^*$,
on a $w_1 \underset{\mathcal{R}_1}{\Rightarrow} w_2 \Longleftrightarrow \exists \alpha_i \longrightarrow \beta_i \in \mathcal{R}_1, \exists (x, y) \in \Sigma_1^* \times \Sigma_1^* : w_1 = x\alpha_i y$ et $w_2 = x\beta_i y)$.
On a $\psi(w_1) = \psi(x\alpha_i y) = |x| + |\alpha_i| + |y|$ et $\psi(w_2) = \psi(x\beta_i y) = |x| + |\beta_i| + |y|$,
comme $\forall 1 \leq i \leq n, |\alpha_i| > |\beta_i|$, alors $\psi(w_1) > \psi(w_2)$ donc $\psi(w_1) >^+ \psi(w_2)$. $\square$
Par conséquent $(\Sigma_1, \mathcal{R}_1)$ est noethérien.

Exemple 2 3.2

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture avec $\Sigma = \{\alpha, \beta\}$ et la relation $\mathcal{R} = \{\alpha\alpha \longrightarrow \beta\}$.
On $|\alpha\alpha| = 2, |\beta| = 1$, donc $|\alpha\alpha| > |\beta|$, et par consèquent le semi-système $(\Sigma, \mathcal{R})$ termine.

Remarque 2.3.3

L'inverse du corollaire 2.3.1 n'est pas vraie, par exemple le semi-système de réécriture $(\Sigma, \mathcal{R})$, avec $\Sigma = \{\alpha, \beta, \gamma\}$ et la relation $\mathcal{R} = \{\alpha\beta \longrightarrow \gamma\alpha\alpha\}$ est noethérien.

Corollaire 2.3.4 [15]

Soit $\Sigma = \{\sigma_1, \sigma_2, ..., \sigma_n\}$ *un alphabet,* $n \in \mathbb{N} - \{0, 1\}$. *Etant donnée l'application* $\lambda : \Sigma \longrightarrow \mathbb{N}$, $\sigma_i \longmapsto \lambda(\sigma_i)$. *On définit l'application* $\widetilde{\lambda} : \Sigma^* \longrightarrow \mathbb{N}$ *comme suit :* $\widetilde{\lambda}(w) = \sum_{i=1}^{i=n} \lambda(\sigma_i) |w|_{\sigma_i}$. *L'application* $\widetilde{\lambda}$ *est bien un morphisme de monoïdes.*
Soit (Σ_1, R_1) *un semi-système de réécriture avec* $R_1 = \{\alpha_j \longrightarrow \beta_j, 1 \leq j \leq m; m \in \mathbb{N}^*\}$.
Si pour tout $1 \leq j \leq m : \widetilde{\lambda}(\alpha_j) > \widetilde{\lambda}(\beta_j)$, *alors* (Σ_1, R_1) *est noethérien.*

Démonstration

On prend $(\Sigma_2, \mathcal{R}_2) = (\mathbb{N}, >)$, on a $(\mathbb{N}, >)$ termine. Et soit $\psi : (\Sigma_1, \mathcal{R}_1) \longrightarrow (\Sigma_2, \mathcal{R}_2)$, définie par $\psi(w) = \widetilde{\lambda}(w)$. L'application ψ est bien un morphisme de monoïdes.

On a : $\forall w_1, w_2 \in \Sigma_1^*, w_1 \underset{\mathcal{R}_1}{\Rightarrow} w_2 \iff \exists \alpha_j \longrightarrow \beta_j \in \mathcal{R}_1, \exists (x, y) \in \Sigma_1^* \times \Sigma_1^* : w_1 = x\alpha_j y$ et $w_2 = x\beta_j y$. Donc $\psi(w_1) = \psi(x\alpha_j y) = \widetilde{\lambda}(x) + \widetilde{\lambda}(\alpha_j) + \widetilde{\lambda}(y)$ et $\psi(w_2) = \psi(x\beta_j y) = \widetilde{\lambda}(x) + \widetilde{\lambda}(\beta_j) + \widetilde{\lambda}(y)$, comme $1 \leq j \leq m : \widetilde{\lambda}(\alpha_j) > \widetilde{\lambda}(\beta_j)$, alors $\psi(w_1) > \psi(w_2)$ donc $\psi(w_1) >^+ \psi(w_2)$.

Enfin $(\Sigma_1, \mathcal{R}_1)$ est noethérien. □

Exemple 2.3.5

Soit $\Sigma = \{\alpha, \beta, \gamma\}$ un alphabet, et soit $\lambda : \Sigma \longrightarrow \mathbb{N}$, avec $\lambda(\alpha) = 1, \lambda(\beta) = 2, \lambda(\gamma) = 3$.

Et Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture tel que $\Sigma = \{\alpha, \beta, \gamma\}$ et la relation $\mathcal{R}$ définie par $\{\beta\beta \longrightarrow \alpha\alpha, \gamma\beta \longrightarrow \alpha\beta\}$.

Comme $|\beta\beta| = |\alpha\alpha|$ et $|\gamma\beta| = |\alpha\beta|$ on utilise le Corollaire 2.3.4 au lieu du Corollaire 2.3.1 car les conditions dans ce dernier ne sont pas verifiées.

Vérifions qu'on a : $\widetilde{\lambda}(\beta\beta) > \widetilde{\lambda}(\alpha\alpha)$ et $\widetilde{\lambda}(\gamma\beta) > \widetilde{\lambda}(\alpha\beta)$.

On a $\widetilde{\lambda}(\beta\beta) = \lambda(\alpha)\,|\beta\beta|_\alpha + \lambda(\beta)\,|\beta\beta|_\beta + \lambda(\gamma)\,|\beta\beta|_\gamma = 1 \times 0 + 2 \times 2 + 3 \times 0 = 4$.

De même $\widetilde{\lambda}(\alpha\alpha) = \lambda(\alpha)\,|\alpha\alpha|_\alpha + \lambda(\beta)\,|\alpha\alpha|_\beta + \lambda(\gamma)\,|\alpha\alpha|_\gamma = 1 \times 2 + 2 \times 0 + 3 \times 0 = 2$.

Dautre part on $\widetilde{\lambda}(\gamma\beta) = \lambda(\alpha)\,|\gamma\beta|_\alpha + \lambda(\beta)\,|\gamma\beta|_\beta + \lambda(\gamma)\,|\gamma\beta|_\gamma = 1 \times 0 + 2 \times 1 + 3 \times 1 = 5$.

Et $\widetilde{\lambda}(\alpha\beta) = \lambda(\alpha)\,|\alpha\beta|_\alpha + \lambda(\beta)\,|\alpha\beta|_\beta + \lambda(\gamma)\,|\alpha\beta|_\gamma = 1 \times 1 + 2 \times 1 + 3 \times 0 = 3$.

Finalement $(\Sigma, \mathcal{R})$ est noethérien.

Une autre méthode pour montrer la terminaison d'un semi-système de réécriture de mots $(\Sigma, \mathcal{R})$ utilise une fonction de poids $P : \Sigma^* \longrightarrow T$ où l'ensemble T est muni d'un ordre $\geq$ bien fondé, on démontre alors que cette fonction vérifie la condition suivante :

Si $w_1 \underset{\mathcal{R}}{\Rightarrow} w_2$, alors $P(w_1) > P(w_2)$. L'existence d'une telle fonction implique la terminaison d'un semi-système de réécriture et réciproquement. Puisque l'ordre sur les entiers naturels est bien fondé, une condition suffisante de terminaison est donnée par l'existence d'une fonction $P : \Sigma^* \longrightarrow \mathbb{N}$, on fait remarquer que la condition : "si $w_1 \underset{\mathcal{R}}{\Rightarrow} w_2$ alors $P(w_1) > P(w_2)$" est décidable si P est un morphisme de *monoïde*s de $(\Sigma^*, \cdot)$ vers $(\mathbb{N}, +)$ et l'application P vérifie pour tout $u \longrightarrow v$ de $\mathcal{R}$: $P(u) > P(v)$.

Proposition 2.3.6 [15]

Soit (Σ, R) *un semi-système de réécriture de mots,* $\psi : (\Sigma^*, \cdot) \longrightarrow (\mathbb{N}, +)$ *un morphisme de monoïdes non trivial et la fonction* $P : \Sigma^* \longrightarrow \mathbb{N}$ *définie par* $P(w) = \sum_{i=1}^{i=|w|} n^i \times \psi(w(i))$, $n \in \mathbb{N} - \{0\}$ *où* $w(i)$ *désigne la i-éme lettre de* w.

Si $\forall u \longrightarrow v \in R$, $\begin{cases} |u| = |v| & (C_1) \\ \text{et} & \\ P(u) > P(v) & (C_2) \end{cases}$ *alors* (Σ, R) *est noethérien.*

Démonstration

Tout d'abord on montre qu'on a: $\forall x, y \in \Sigma^* : P(xy) = P(x) + n^{|x|} \times P(y)$.

On a $P(xy) = \sum_{i=1}^{i=|xy|} n^i \times \psi((xy)(i)) = \sum_{i=1}^{i=|x|} n^i \times \psi((xy)(i)) + \sum_{i=|x|+1}^{i=|x|+|y|} n^i \times \psi((xy)(i))$

$= \sum_{i=1}^{i=|x|} n^i \times \psi((x)(i)) + \sum_{i=1}^{i=|y|} n^{|x|+i} \times \psi((xy)(|x|+i))$

$= \sum_{i=1}^{i=|x|} n^i \times \psi((x)(i)) + \sum_{i=1}^{i=|y|} n^{|x|+i} \times \psi((y)(i)) = P(x) + n^{|x|} \times P(y)$.

Soient $u \longrightarrow v \in \mathcal{R}$ et $x, y \in \Sigma^*$, on montre que $P(xuy) > P(xuy)$.

On a $P(xuy) = P(x(uy)) = P(x) + n^{|x|} \times P(u\,y) = P(x) + n^{|x|}\big(P(u) + n^{|u|} \times P(y)\big)$

$= P(x) + n^{|x|} \times P(u) + n^{|x|+|u|} \times P(y)$. D'autre part, $P(xvy) = P(x(vy)) = P(x) + n^{|x|} \times P(v\,y) = P(x) + n^{|x|}\big(P(v) + n^{|v|} \times P(y)\big) = P(x) + n^{|x|} \times P(v) + n^{|x|+|v|} \times P(y)$. D'après les conditions (C_1), (C_2), décrites ci-dessus on a $P(xuy) > P(xvy)$ et par conséquent $(\Sigma, \mathcal{R})$ est noethérien. □

Exemple 2.3.7 [15]

Soit $\Sigma = \{\alpha, \beta, \gamma\}$ un alphabet et la relation $\mathcal{R}$ définie par $\{\beta\alpha \longrightarrow \alpha\beta, \gamma\beta \longrightarrow \beta\gamma\}$.

On considère le morphisme, $\psi : \Sigma^* \longrightarrow \mathbb{N}$, avec $\psi(\alpha) = 3, \psi(\beta) = 2, \psi(\gamma) = 1$ et la fonction de poids $P : \Sigma^* \longrightarrow \mathbb{N}$, où $P(w) = \sum_{i=1}^{i=|w|} 2^i \times \psi(w(i))$.

Pour la condition (C_1), on a $|\beta\alpha| = |\alpha\beta| = 2$ et $|\gamma\beta| = |\beta\gamma| = 2$.

Pour la condition (C_2), on montre que $P(\beta\alpha) > P(\alpha\beta)$ et $P(\gamma\beta) > P(\beta\gamma)$.

On a, $P(\beta\alpha) = \sum_{i=1}^{i=2} 2^i \times \psi(\beta\alpha(i)) = 2 \times \psi(\beta) + 2^2 \times \psi(\alpha) = 16$.

De même $P(\alpha\beta) = \sum_{i=1}^{i=2} 2^i \times \psi(\alpha\beta(i)) = 2 \times \psi(\alpha) + 2^2 \times \psi(\beta) = 14$, donc $P(\beta\alpha) > P(\alpha\beta)$.

Pour $P(\gamma\beta)$, on a, $P(\gamma\beta) = \sum_{i=1}^{i=2} 2^i \times \psi(\gamma\beta(i)) = 2 \times \psi(\gamma) + 2^2 \times \psi(\beta) = 10$.

De même $P(\beta\gamma) = \sum_{i=1}^{i=2} 2^i \times \psi(\beta\gamma(i)) = 2 \times \psi(\beta) + 2^2 \times \psi(\gamma) = 8$, donc $P(\gamma\beta) > P(\beta\gamma)$.
Par conséquent $(\Sigma, \mathcal{R})$ est noethérien.

Proposition 2.3.8 [15]

Soit (Σ, R) *un semi-système de réécriture de mots,* $\psi : (\Sigma^*, \cdot) \longrightarrow (\mathbb{N}, +)$ *un morphisme de monoïdes non trivial et la fonction* $P : \Sigma^* \longrightarrow \mathbb{N}$ *définie par* $P(w) = \sum_{i=1}^{i=|w|} i \times \psi(w(i))$, *où* $w(i)$ *désigne la i-éme lettre de* w.

Si $\forall u \longrightarrow v \in R$, $\begin{cases} |u| = |v| & (C_1) \\ \text{et} & \\ P(u) > P(v) & (C_2) \\ \text{et} & \\ \psi(u) > \psi(u) & (C_3) \end{cases}$ *alors* $(\Sigma, \mathcal{R})$ est noethérien.

Démonstration

Tout d'abord on montre qu'on a: $\forall x, y \in \Sigma^* : P(xy) = P(x) + P(y) + |x| \times \psi(y)$.

On a $P(xy) = \sum_{i=1}^{i=|xy|} i \times \psi(xy(i)) = \sum_{i=1}^{i=|x|} i \times \psi(xy(i)) + \sum_{i=|x|+1}^{i=|x|+|y|} i \times \psi(xy(i))$

$= \sum_{i=1}^{i=|x|} i \times \psi(x(i)) + \sum_{i=1}^{i=|y|} (|x| + i) \times \psi((xy)(|x| + i))$

$= \sum_{i=1}^{i=|x|} i \times \psi((x)(i)) + \sum_{i=1}^{i=|y|} (|x| + i) \times \psi((y)(i)) = P(x) + P(y) + |x| \times \psi(y)$. $\left(\sum_{i=1}^{i=|y|} \psi((y)(i)) = \psi((y) \right)$.

Soient $u \longrightarrow v \in \mathcal{R}$ et $x, y \in \Sigma^*$, on montre que $P(xuy) > P(xuy)$.

On a $P(xuy) = P(x(uy)) = P(x) + P(u\,\mathrm{y}) + |x| \times \psi(u\,\mathrm{y}) = P(x) + P(u) + P(y) + |u| \times \psi(\mathrm{y}) + |x| \times (\psi(u) + \psi(\mathrm{y})) = [P(x) + P(y) + |x| \times \psi(y)] + [P(u) + |u| \times \psi(\mathrm{y}) + |x| \times \psi(u)]$. D'autre part, $P(xvy) = [P(x) + P(y) + |x| \times \psi(y)] + [P(v) + |v| \times \psi(\mathrm{y}) + |x| \times \psi(v)]$. D'après les conditions (C_1), (C_2), (C_1) décrites ci-dessus on a $P(xuy) > P(xvy)$ et par conséquent $(\Sigma, \mathcal{R})$ est noethérien. □

Exemple 2.3.9

Soit $\Sigma = \{\alpha, \beta, \gamma\}$ un alphabet et la relation $\mathcal{R}$ définie par $\{\beta\alpha \longrightarrow \beta\gamma, \alpha\beta \longrightarrow \alpha\gamma\}$.

On considère le morphisme, $\psi : \Sigma^* \longrightarrow \mathbb{N}$, avec $\psi(\alpha) = 2, \psi(\beta) = 1, \psi(\gamma) = 0$ et la fonction de poids $P : \Sigma^* \longrightarrow \mathbb{N}$, où $P(w) = \sum_{i=1}^{i=|w|} i \times \psi(w(i))$.

Pour la condition (C_1), on a $|\beta\alpha| = |\beta\gamma| = 2$ et $|\alpha\beta| = |\alpha\gamma| = 2$.

Pour la condition (C_2), on montre que $P(\beta\alpha) > P(\beta\gamma)$ et $P(\alpha\beta) > P(\alpha\gamma)$.

On a, $P(\beta\alpha) = \sum_{i=1}^{i=2} i \times \psi(\beta\alpha(i)) = 1 \times \psi(\beta) + 2 \times \psi(\alpha) = 5$.

De même, $P(\beta\gamma) = \sum_{i=1}^{i=2} i \times \psi(\beta\gamma(i)) = 1 \times \psi(\beta) + 2 \times \psi(\gamma) = 1$, donc $P(\beta\alpha) > P(\beta\gamma)$.

Pour $P(\alpha\beta)$, on a $P(\alpha\beta) = \sum_{i=1}^{i=2} i \times \psi(\alpha\beta(i)) = 1 \times \psi(\alpha) + 2 \times \psi(\beta) = 4$.

Pour $P(\alpha\gamma)$, on a, $P(\alpha\gamma) = \sum_{i=1}^{i=2} i \times \psi(\alpha\gamma(i)) = 1 \times \psi(\alpha) + 2 \times \psi(\gamma) = 2$.

Donc, on a bien $P(\alpha\beta) > P(\alpha\gamma)$.

Pour la condition (C_3), on montre que $\psi(\beta\alpha) > \psi(\beta\gamma)$ et $\psi(\alpha\beta) > \psi(\alpha\gamma)$.

On a $\psi(\beta\alpha) = 3, \psi(\beta\gamma) = 1, \psi(\alpha\beta) = 3, \psi(\alpha\gamma) = 2$.

Finalement les conditions $(C_1), (C_2)$ et (C_3) étants vérifiées, alors $(\Sigma, \mathcal{R})$ est noethérien.

Chapitre 3

Problème du mot dans un monoïde

Introduction

Soit E un ensemble et $p(x)$ une propriété qui dépend de la variable x de E (l'univers). Le problème P : " Est-ce que $P(x)$ est vrai?" est dit décidable s'il existe un algorithme qui pour chaque x dit "oui" ou "non" à la question précedente. Ce problème avait été posé la première fois par David Hilbert, au Congrès International des Mathématiciens qui a eu lieu à Paris en 1900. L'indécidabilité est la négation de la décidabilité. Parmi les problèmes connus indécidables, on cite par exemple le le problème de Post qui on peut le formuler comme suit : On donne deux suites finis X et Y de mots sur un alphabet Σ, $X = u_1, u_2, ..., u_n$ et $Y = v_1, v_2, ..., v_k$. Existe-t-il une suite $i_1, i_2, ..., i_m$ telle que $u_{i_1}u_{i_2}...u_{i_m} = v_{i_1}v_{i_2}...v_{i_m}$?. Par exemple, sur l'alphabet $\Sigma = \{0, 1\}$, le problème avec $X = 1, 10111, 10$,
$Y = 111, 11, 011$ est décidable : on a $u_2u_1u_1u_3 = v_2v_1v_1v_3$. Mais le problème avec $X = 10, 011, 101, Y = 101, 11, 011$ n'a pas de solution.

On introduit dans ce paragraphe quelques définitions, propriétés et notations concernant la notion d'indécidabilité d'un problème du mot dans un monoïde libre. Le problème du mot on peut le formuler comme suit : etants donnés un monoïde Σ^* librement et finiment engendré par un ensemble Σ, et une congruence de ce monoïde engendrée elle-même par une relation finie $\mathcal{R}$, le problème du mot consiste à reconnaitre si deux éléments du quotient, définis par deux représentants dans Σ^*, sont distincts ou non. Il est bien connu que ce problème est en général indécidable [21, 30]. Cependant, on peut chercher des cas spécifiques

pour que ce problème devienne décidable, c'est le cas si dans toute classe d'équivalence on sait trouver un représentant canonique. Une idée simple est de prendre comme représentant un mot de plus courte longueur dans sa classe. Certains auteurs (Adjan, Book, Huet, Knuth et Bendix et Nivat), ont donné des conditions suffisantes sur $\mathcal{R}$ qui permettent l'existence d'un algorithme de décision pour le problème du mot. Une des méthodes de décision consiste à associer à $\mathcal{R}$ un semi-système $(\Sigma, \mathcal{R})$ de règles de réécriture, tel que deux mots $w_1$et w_2 sont équivalents modulos $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ si, et seulement si il existe au moins une suite de dérivations de source w_1 et une suite dérivations de source w_2 qui aboutissent au même mot. Dans le cas où on peut trouver un tel semi-système complet (c-à-d termine et confluent) et fini, il est alors claire que le problème du mot est résoluble.

Contenu du chapitre 3

3.1 Notations et définitions

Définition 3.1.1

Etant donnés un alphabet Σ et une relation $\mathcal{R}$ sur le monoïde libre Σ^*, on définit la congruence engendrée par $\mathcal{R}$, notée $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$, comme la plus petite relation d'équivalence contenant $\mathcal{R}$ et compatible avec la concaténation des mots, le quotient de Σ^* par $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est alors le monoïde défini par les générateurs Σ et la relation $\mathcal{R}$.

Proposition 3.1.2

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture. La congruence $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ engendrée par R est définie comme suit :

- $w \underset{\mathcal{R}}{\Longleftrightarrow} w'$, *s'il existe u, v de Σ^* et $r \longrightarrow s \in (\mathcal{R} \cup \mathcal{R}^{-1})$ tels que $w = urv, w' = usv$.*
- $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w'$, *s'il existe une suite finie de mots $u_0, u_1, ..., u_n$ de Σ^* avec,*

$$u_0 = w, u_i \underset{\mathcal{R}}{\Longleftrightarrow} u_{i+1}, \forall 0 \leq i \leq n-1 \text{ et } u_n = w'.$$

Proposition 3.1.3

1. *Soit $h : \Sigma^* \longrightarrow \Gamma^*$ un morphisme, la congruence associée à h, notée $\equiv_h$, est définie par : pour tous $u, v \in \Sigma^*, u \equiv_h v \iff h(u) = h(v)$.*

2. *Soit R une relation sur Σ^* qui vérifie $h(r) = h(s)$ pour tout $(r, s) \in R$, alors il existe un unique morphisme $\psi : \Sigma^* / \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \longrightarrow \Gamma^*$ tel que $\psi \circ p = h$ où $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est la congruence engendré par R et p est la surjection canonique.*

Définition 3.1.4

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture.

Si $(\Sigma, \mathcal{R})$ est complet, alors pour tout $w \in \Sigma^*$, l'unique $m \in IRR(\mathcal{R})$ tel que $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} m$ est appelée forme normale de w.

Exemple 3.1.5

Soient $\Sigma = \{\alpha, \beta\}$ et $\mathcal{R} = \{\alpha\beta \longrightarrow \beta\alpha\}$. Pour tout mot $w \in \Sigma^*$, l'unique $m \in IRR(\mathcal{R})$ tel que $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} m$ est $m = \beta^p \alpha^q$ où $p = |w|_\beta$ et $q = |w|_\alpha$.

Définition 3.1.6

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture. Décider l'équivalence de deux mots modulo $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est un classique problème dit le problème du mot dans un monoïde il s'agit donc étants

données deux mots quelconques w et w' appartenant à Σ^* décider s'ils appartiennent à la même classe d'équivalence modulo la congruence $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$.

Exemples 3.1.7

1. Soit $\Sigma = \{\alpha\}$, et $\mathcal{R} = \{\alpha^2 \longrightarrow \epsilon\}$, ϵ est le mot vide. $\forall w \in \Sigma^*$, on distingue deux cas :

• si $|w|$ est paire alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \epsilon$.

• si $|w|$ est impaire alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha$.

Finalement $\Sigma^* / \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} = \left\{ [\alpha]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \right\}$ et le problème du mot dans cet exemple est résoluble.

Théorème 3.1.8

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture. Si $(\Sigma, \mathcal{R})$ est complet, alors

$$P : IRR(\mathcal{R}) \longrightarrow (\Sigma^* / \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}),\ w \longmapsto [w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$$

où $[w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ désigne la classe d'équivalence du mot w modulo la congruence $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$, est une bijection.

Démonstration

L'application $P : \Sigma^* \longrightarrow (\Sigma^* / \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}})$ étant surjective, montrer ce théorème revient à montrer que pour tout mot m de Σ^*, il existe un unique w irréductible tel que $P(m) = P(w)$, autrement dit, qu'on a $m \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w$.

• L'existence **:** Comme $(\Sigma, \mathcal{R})$ est noethérien, toute chaine $m = m_0 \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} m_1 ... \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} m_k ...$ s'arrête en un nombre fini d'étapes q. Alors m_q sera irréductible et $m \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} m_q$.

• L'unicité**:** Supposons qu'il existe $w, w' \in IRR(\mathcal{R})$ tels que $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w'$. Alors il existe une suite $w = w_0, w_1, ..., w_q = w' \in \Sigma^*$ telle que $w_i \underset{\mathcal{R}}{\Longleftrightarrow} w_{i+1}$, pour $i = 0, ..., q-1$. Montrons par récurrence sur k dans $[0, q]$ que w_0 et w_k sont joignables. Si $k = 0$, $w = w_0 = w'$. C'est donc évident. Supposons que w_0 et w_k sont joignables et montrons que w_0 et w_{k+1} sont joignables pour $k \leqslant q-1$. Soit $v \in w_0 \downarrow w_k$. Si $w_k \underset{\mathcal{R}}{\Longleftarrow} w_{k+1}$, alors par transitivité, $w_{k+1} \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} v$ et donc $v \in w_0 \downarrow w_{k+1}$, sinon $w_k \underset{\mathcal{R}}{\Longrightarrow} w_{k+1}$. Par hypothèse de confluence, on obtient l'éxistance de $v' \in v \downarrow w_{k+1}$. Par suite, $v' \in w_0 \downarrow w_{k+1}$. Finalement, $w = w_0$ et $w' = w_q$ sont donc joignables. Soit $u \in w \downarrow w'$, comme w et w' sont irréductibles, alors on a $w = u = w'$, d'où l'unicité. □

Remarque 3.1.9

La même congruence peut être engendré par plusieurs relations.

Exemple 3.1.10

Considérons, sur l'alphabet $\Sigma = \{\alpha, \beta\}$, les relations $\mathcal{R}_1 = \left\{\alpha\beta\alpha\beta \longrightarrow \epsilon, \beta\alpha\beta\alpha \longrightarrow \epsilon, \beta^2 \longrightarrow \epsilon\right\}$, $\mathcal{R}_2 = \left\{\beta\alpha\beta\alpha \longrightarrow \epsilon, \beta^2 \longrightarrow \epsilon\right\}$. On a $\overset{*}{\underset{\mathcal{R}_1}{\Longleftrightarrow}} = \overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}}$, car $\alpha\beta\alpha\beta \overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}} \beta\beta\alpha\beta\alpha\beta \overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}} \beta\beta \overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}} \epsilon$.

Notation 3.1.11

Les notations qui suivent ont étés données par Maurice Nivat dans [28].

Pour tous $w_1, w_2 \in \Sigma^*$,

1. $w_1 \underset{\mathcal{R}}{\Longleftrightarrow} w_2 \Longleftrightarrow \exists x, y \in \Sigma^*, \exists u \longrightarrow v \in \mathcal{R} \cup \mathcal{R}^{-1} : w_1 = xu\,\text{y et } w_2 = xvy.$
2. $w_1 \overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}} w_2 \Longleftrightarrow w_1 \underset{\mathcal{R}}{\Longleftrightarrow} w_2$ et $|w_1| > |w_2|$.
3. $w_1 \overset{=}{\underset{\mathcal{R}}{\Longleftrightarrow}} w_2 \Longleftrightarrow w_1 \underset{\mathcal{R}}{\Longleftrightarrow} w_2$ et $|w_1| = |w_2|$.

On notera par $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$(resp. $\left(\overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}}\right)^*, \left(\overset{=}{\underset{\mathcal{R}}{\Longleftrightarrow}}\right)^*$) les fermetures transitives et réflexives de $\underset{\mathcal{R}}{\Longleftrightarrow}, \overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}}, \overset{=}{\underset{\mathcal{R}}{\Longleftrightarrow}}$.

Définition 3.1.12

La définition suivante a été formuler par Jean Berstel dans [7].

1. La relation $\mathcal{R}$ est dite quasi-parfaite si, et seulement si, la condition suivante est satisfaite :

$$\forall h, h' \in IRR(\mathcal{R}) : h \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} h' \Rightarrow h \left(\overset{=}{\underset{\mathcal{R}}{\Longleftrightarrow}}\right)^* h'.$$

2. La relation $\mathcal{R}$ est dite parfaite si, et seulement si, la condition suivante est satisfaite :

$$\forall h, h' \in IRR(\mathcal{R}) : h \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} h' \Rightarrow h = h'.$$

Ramarque 3.1.13

Il est immédiat que $\mathcal{R}$ est quasi-parfaite si elle est parfaite.

Définition 3.1.14 [7]

Une congruence Θ sur le monoïde libre Σ^* est quasi-parfaite (resp. parfaite) si, et seuelement si, il existe une relation quasi-parfaite (resp. parfaite) $\mathcal{R}$ tel que $\Theta = \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$.

Définition 3.1.15 [29]

Soit $(\Sigma, \mathcal{R})$ un semi-système de réécriture de mots, nous appelons chaîne allant de w_1 en w_2, toute suite de mots $x_1, ..., x_{k+1}$ de Σ^* satisfaisant :

1. $x_1 = w_1$,

2. $x_{k+1} = w_2$,

3. pour tout $i = 1, ..., k,\ x_i \underset{\mathcal{R}}{\Longleftrightarrow} x_{i+1}$

La longueur de la chaîne $x_1, ..., x_{k+1}$ est égale à k.

Il est claire que, pour tout couple de mots, w_1, w_2 de Σ^*, on a

$w_1 \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w_2$ ce qui équivant à dire, il existe une chaîne allant de w_1 en w_2.

Définition 3.1.16 [29]

Une chaîne $x_1, ..., x_{k+1}$ est dite décomposable si, et seuelement si, s'il existe deux indices $1 \leq i \leq j \leq k+1$ tels que:

1. $x_1 \overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}} x_2 \overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}} ... \overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}} x_i$,
2. $x_i \overset{=}{\underset{\mathcal{R}}{\Longleftrightarrow}} x_{i+1} \overset{=}{\underset{\mathcal{R}}{\Longleftrightarrow}} ... \overset{=}{\underset{\mathcal{R}}{\Longleftrightarrow}} x_j$,
3. $x_j \left(\overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}}\right)^{-1} x_{j+1} \left(\overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}}\right)^{-1} ... \left(\overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}}\right)^{-1} x_{k+1}$.

Proposition 3.1.17 [29]

Soit $(\Sigma, \mathcal{R})$ un système de réécriture de mots, la relation R est quasi-parfaite si, et seulement si, pour toute chaîne $x_1, ..., x_{k+1}$ de Σ^*, il existe une chaîne décomposable allant de x_1 à x_{k+1}.

Démonstration

Pour l'implication directe, on suppose que pour toute chaîne $x_1, ..., x_{k+1}$ de Σ^*, il existe une chaîne décomposable allant de x_1 à x_{k+1} et montrons que la relation $\mathcal{R}$ est quasi-parfaite. Soient $(h, h') \in IRR(\mathcal{R})$ tels que $h \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} h'$, alors il existe une chaîne $x_1, ..., x_{k+1}$ de Σ^*allant de h en h'. D'après l'hypothèse, il existe une chaîne décomposable $y_1, ..., y_{m+1}$ allant de h en h', donc il existe deux indices $1 \leq i \leq j \leq m+1$ tels que :

1. $y_1 \overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}} y_2 \overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}} ... \overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}} y_i$,
2. $y_i \overset{=}{\underset{\mathcal{R}}{\Longleftrightarrow}} y_{i+1} \overset{=}{\underset{\mathcal{R}}{\Longleftrightarrow}} ... \overset{=}{\underset{\mathcal{R}}{\Longleftrightarrow}} y_j$,
3. $y_j \left(\overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}}\right)^{-1} y_{j+1} \left(\overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}}\right)^{-1} ... \left(\overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}}\right)^{-1} y_{m+1}$.

Comme $(h, h') \in IRR(\mathcal{R})$, alors $\forall 1 \leq i \leq m : y_i \overset{=}{\underset{\mathcal{R}}{\Longleftrightarrow}} y_{i+1}$, donc $h \left(\overset{=}{\underset{\mathcal{R}}{\Longleftrightarrow}}\right)^* h'$.

Pour la réciproque, soient $w_1, w_2 \in \Sigma^*$ tels que $w_1 \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w_2$. Construisons, tant que cela est possible, la suite $x_1 = w_1, x_1, ..., x_{k+1}$ en prenant, pour tout $i = 1, ..., k$, $x_{i+1} = \left\{h : x_i \overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}} h\right\}$. cette construction s'arrête quand on arrive a un mot x_{k+1} tel que $\left\{h : x_{k+1} \overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}} h\right\} = \emptyset$, autrement dit, x_{k+1} est irréductible. De la même façons, on construit la suite

$y_1 = w_2, y_2, ..., y_{l+1}$ telle que $y_1 \overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}} y_2 \overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}} ... \overset{>}{\underset{\mathcal{R}}{\Longleftrightarrow}} y_{l+1}$, avec y_{l+1} est irréductible. Il est immédiat que x_{k+1} et y_{l+1} sont congrus modulo $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ i.e, $x_{k+1} \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} y_{l+1}$ et comme la relation $\mathcal{R}$ est quasi-parfaite on a $x_{k+1} \left(\overset{=}{\underset{\mathcal{R}}{\Longleftrightarrow}}\right)^* y_{l+1}$ et par suite il existe une suite $h_1 = x_{k+1}, h_2, ..., h_{m+1} = y_{l+1}$ telle que, pour tout $i = 1, ..., m, h_i \overset{=}{\underset{\mathcal{R}}{\Longleftrightarrow}} h_{i+1}$. La suite $x_1 = w_1, x_1, ..., x_{k+1} = h_1, h_2, ..., h_{m+1}, y_l, ..., y_1 = w_2$ est bien une chaîne décomposable allant de w_1 en w_2. $\square$

Définition 3.1.18 [9]

Soit Θ une congruence sur le monoïde libre Σ^*, et soit A un ensemble fini de mots de Σ^* dont nous supposerons que

$$\Sigma^* = \bigcup_{w \in A} [w]_\Theta ,$$

où $[w]_\Theta$ désigne la classe de w modulo Θ. On définit l'application λ comme suit:

$\lambda : \Sigma^* \longrightarrow \mathbb{N}$

$w \longmapsto \lambda(w) = \inf \left\{ k \in \mathbb{N} : A^K \cap [w]_\Theta \neq \emptyset \right\}$.

L'application λ est dite la longueur sur Σ^* associée à Θ par A.

Nous dirons que cette longueur est archimédienne si, et seulement si,

$$\forall w \in \Sigma^*, \lambda(ww) \leq \lambda(w) \Rightarrow \lambda(w) = 0.$$

Exemples 3.1.19

1. Soit $\Sigma = \{\alpha\}$, et $\mathcal{R} = \{\alpha^2 \longrightarrow \epsilon\}$, ϵ est le mot vide, $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est la congruence engendré par $\mathcal{R}$.

Pour tout $w \in \Sigma^*$, on distingue deux cas :

• Si $|w|$ est paire alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \epsilon$.

• Si $|w|$ est impaire alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha$.

Finalement $\Sigma^* / \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} = \left\{ [\alpha]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \right\}$. On pose $A = \{\alpha, \epsilon\}$, on a $\Sigma^* = \bigcup_{w \in A} [w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$.

Si $|w|$ est paire alors $[w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ et $\lambda(w) = 0$.

Si $|w|$ est impaire alors $[w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\alpha]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ et $\lambda(w) = 1$.

2. On pose $\Sigma = \{\alpha\}$, et $\mathcal{R} = \{\alpha^n \longrightarrow \epsilon\}$, ϵ est le mot vide, $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est la congruence engendré par $\mathcal{R}$. Soit $w \in \Sigma^*$, on distingue les cas suivants:

• Si $|w| \equiv 0(\text{mod } n)$, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \epsilon$.

• Si $|w| \equiv 1(\text{mod } n)$, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha$.

• Si $|w| \equiv n-1(\text{mod } n)$, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha^{n-1}$.

Alors $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} = \left\{ [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, [\alpha]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, ..., [\alpha^{n-1}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \right\}$. On pose $A = \{\epsilon, \alpha, \alpha^2, ..., \alpha^{n-1}\}$.

On a $\Sigma^* = \bigcup_{w \in A} [w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$. Par conséquent :

• Si $|w| \equiv 0(\text{mod } n)$, alors $[w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ et $\lambda(w) = 0$.

• Si $|w| \equiv 1(\text{mod } n)$, alors $[w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\alpha]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ et $\lambda(w) = 1$.

.

.

.

• Si $|w| \equiv n-1(\text{mod } n)$, alors $[w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\alpha^{n-1}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ et $\lambda(w) = n-1$.

Corollaire 3.1.20

Si la congruence $\Theta = \{(u, v) \in \Sigma^* \times \Sigma^* : |u| = |v|\}$ *et* $A = \Sigma$, *alors* $[w]_\Theta = \{u \in \Sigma^* : |u| = |w|\}$ *et pour tout* w *de* Σ^* *on a* $\lambda(w) = |w|$ *i.e,* λ *est la fonction longueur.*

Propriété 3.1.21 [28]

Soit λ *la longueur sur* Σ^* *associée à* $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ *par* A.

L'application λ *vérifiée les propriétés suivantes :*

• $\forall w \in \Sigma^* : \lambda(w) = 0 \Longleftrightarrow w \in [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$.

• $\forall w, w' \in \Sigma^* : \lambda(ww') \preceq \lambda(w) + \lambda(w')$.

Démonstration

Pour l'implication directe, si $\lambda(w) = 0$, alors $A^0 \cap [w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \neq \emptyset$, on a $A^0 = \{\epsilon\}$, donc $\epsilon \in [w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, c'est-à-dire $[w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$.

Pour la réciproque, si $w \in [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \epsilon$, donc $\epsilon \in [w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, mais $A^0 = \{\epsilon\}$,

par conséquent $A^0 \cap [w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \neq \emptyset$ et $\lambda(w) = 0$. $\square$

Lemme 3.1.22 [28]

Soit λ une application longueur archimédienne associée à la congruence $\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$ par A.

On a, $\forall w, w' \in \Sigma^* : \left[ww'\right]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \Rightarrow \left[w'w\right]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$.

Démonstration

Soient $w, w^{'} \in \Sigma^*$, on suppose que $\left[ww^{'}\right]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, c'est-à-dire , $ww\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}\epsilon$. On a bien $w^{'}ww^{'}w\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}w^{'}w$, car $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est une congruence. Donc $\lambda(w^{'}ww^{'}w) = \lambda(w^{'}w)$, comme λ est archimédienne, alors $\lambda(w^{'}w)$, et par conséquent $\left[w^{'}w\right]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$. $\square$

Propriété 3.1.23

Soient Σ un alphabet fini, $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ une congruence sur Σ^* et λ la longueur archimédienne. On a les propriétés suivantes :

1. L'ensemble $M = \left\{ w \in \Sigma^* : \Sigma^* w \Sigma^* \cap [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \neq \emptyset \right\}$ est un sous monoïde de Σ^*.

2. Le monoïde quotient $M/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est un groupe.

Démonstration

M est un sous monoïde de Σ^*, en effet,

1. $\epsilon \in M$, car $\Sigma^*\epsilon\Sigma^* \cap [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \neq \emptyset, (\Sigma^*\epsilon\Sigma^* = \Sigma^*\Sigma^* = (\Sigma^*)^2 = \Sigma^*)$.

2. Soient $w, w^{'} \in M$, alors ils existent $u, v, u^{'}, v^{'} \in \Sigma^*$ tels que :

$$(uwv \in [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \text{ et } u^{'}w^{'}v^{'} \in [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}).$$

On a d'après le lemme précédent:

$(uwv \in [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \text{ et } u^{'}w^{'}v^{'} \in [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}) \Rightarrow (vuw \in [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \text{ et } w^{'}v^{'}u^{'} \in [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}})$

$\Rightarrow (vuw\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}\epsilon \text{ et } w^{'}v^{'}u\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}\epsilon)$. Comme $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est congruence, alors $(vuw\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}\epsilon \text{ et } vuww^{'}v^{'}u\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}vuw)$

On a $vuww^{'}v^{'}u\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}\epsilon \Rightarrow \Sigma^*ww^{'}\Sigma^* \cap [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \neq \emptyset \Rightarrow ww^{'} \in M$.

• Montrons que $M/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est un groupe:

Notons P le morphisme canonique de Σ^* sur $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$.

Si $w \in M$, alors il existe $u, v \in \Sigma^*$ tels que $uwv \in [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, d'où encore $vuw \in [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, qui s'écrit $[vuw]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$.

On a les égalités suivantes :

$[vuw]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \Longleftrightarrow P(vuw) = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \Longleftrightarrow P(vu)P(w) = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$,

Alors l'inverse à gauche de $P(w)$ est $P(vu)$.

D'autre part, $uwv \in [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \Rightarrow wvu \in [\epsilon] \Rightarrow P(wvu) = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \Rightarrow P(w)P(vu) = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$.

Alors l'inverse à droite de $P(w)$ est $P(vu)$. Finalement l'inverse de $P(w)$ est $P(vu)$ et par conséquent $M/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est un groupe. $\square$

3.2 Quelques exemples où le problème du mot est résoluble

La réécriture peut apporter une réponse partielle au problème du mot dans un monoïde : on utilise ici le fait que la réécriture est un calcul de formes normales. En effet, supposons que $(\Sigma, \mathcal{R})$ soit une présentation convergente. Alors, pour tout $u \in \Sigma^*$, u possède une unique forme normale $IRR(u)$, comme tout enchainement de réductions partant de u et arrivant à une forme normale aboutit forcément à $IRR(u)$ en un nombre fini d'étapes, on a un algorithme de calcul de $IRR(u)$ pour tout u.

Proposition 3.2.1

Soient u et v deux éléments d'un semi-système convergent (Σ, R).

On a, $u \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} v$ si et seulement si $IRR(u) = IRR(v)$.

Démonstration

Pour l'implication directe, comme $(\Sigma, \mathcal{R})$ est convergent. Si on a $u\mathcal{R}v$, alors $IRR(u) = IRR(v)$, on en déduit que, si $u \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} v$, alors $IRR(u) = IRR(v)$.

Réciproquement **:** si, $IRR(u) = IRR(v)$, alors $u \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} IRR(u) = IRR(v) \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} v$, et donc $u \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} v$.

Exemples 3.2.2

1. Soient $\Sigma = \{\alpha, \beta\}$, et $\mathcal{R} = \{\alpha\beta \longrightarrow \beta\alpha\}$,

On a, pour tout $w \in \Sigma^*$, il existe un unique $(n, m) \in \mathbb{N}^2$ tels que $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \beta^n \alpha^m$,

où $m = |w|_\alpha$ et $n = |w|_\beta$.

On a le problème du mot est résoluble car,

$\forall w, w' \in \Sigma^*$, si $(|w|_\alpha = |w'|_\alpha$ et $|w|_\beta = |w'|_\beta)$, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w'$.

2. On pose $\Sigma = \{\alpha\}$, et $\mathcal{R} = \{\alpha^n \longrightarrow \epsilon, n \in \mathbb{N} - \{0, 1\}\}$, ϵ est le mot vide.

Soit $w \in \Sigma^*$, on distingue les cas suivants:

- Si $|w| \equiv 0 (\text{mod } n)$, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \epsilon$.
- Si $|w| \equiv 1 (\text{mod } n)$, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha$.

  .

  .

  .

- Si $|w| \equiv n - 1 (\text{mod n})$, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha^{n-1}$.

Alors $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} = \left\{ [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, [\alpha]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, ..., [\alpha^{n-1}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \right\}$, dans ce cas le problème est résoluble car, $\forall w, w' \in \Sigma^*$, on a, si $|w| \equiv |w'| \pmod n$, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w'$.

3. Soient $\Sigma = \{\alpha, \beta\}$, et $\mathcal{R} = \{\alpha\beta \longrightarrow \epsilon, \beta\alpha \longrightarrow \epsilon\}$, ϵ est le mot vide.

Soit $w \in \Sigma^*$, on distingue les cas suivants:

- Si $|w|_\alpha = |w|_\beta$, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \epsilon$.
- Si $|w|_\alpha > |w|_\beta$, c'est-à-dire $|w|_\alpha = |w|_\beta + n, n \in \mathbb{N}^*$, dans ce cas $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha^n$.
- Si $|w|_\beta > |w|_\alpha$, c'est-à-dire $|w|_\beta = |w|_\alpha + m, m \in \mathbb{N}^*$, dans ce cas $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \beta^m$.

Donc $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} = \left\{ [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, [\alpha^n]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, [\beta^m]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, (n, m) \in \mathbb{N}^* \times \mathbb{N}^* \right\}$. Le problème du mot dans ce monoïde est résoluble puisque :

$\forall w, w' \in \Sigma^*$, on a, si $|w|_\alpha - |w|_\beta = |w'|_\alpha - |w'|_\beta$ ou $|w|_\beta - |w|_\alpha = |w'|_\beta - |w'|_\alpha$,

alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w'$.

Définition 3.2.3

Dans [9], on a la définition suivante :

Soient Σ un alphabet et $\Delta \subseteq \Sigma$ un sous alphabet, notons $P_\Delta : \Sigma^* \longrightarrow \Delta^*$ la projection définie par : $\begin{cases} P_\Gamma(\sigma) = \sigma & \text{si } \sigma \in \Delta, \text{ et} \\ P_\Gamma(\sigma) = \epsilon & \text{si } \sigma \notin \Delta. \end{cases}$

Théorème 3.2.4 [9]

Soient $u, v \in \Sigma^*, \theta \subseteq \Sigma \times \Sigma$ une relation sur Σ et soit Δ un sous alphabet de Σ, i.e, $\Delta \subseteq \Sigma$. *On considère la projection sur Δ $P_\Delta : \Sigma^* \longrightarrow \Delta^*$. On a*

$$u \overset{*}{\underset{T_\theta}{\Longleftrightarrow}} v \Longleftrightarrow \begin{cases} i) P_{\{\sigma\}}(u) = P_{\{\sigma\}}(v), \text{ pour tout } \sigma \text{ de } \Sigma \text{ et} \\ ii) P_{\{\alpha,\beta\}}(u) = P_{\{\alpha,\beta\}}(v), \text{ pour tout } (\alpha, \beta) \notin \theta \end{cases}$$

où $T_\theta = \{\alpha\beta \longrightarrow \beta\alpha : (\alpha, \beta) \in \theta\}$.

Démonstration

Pour l'implication directe, on suppose que $u \overset{*}{\underset{T_\theta}{\Longleftrightarrow}} v$ et on montre que

$$\begin{cases} P_{\{\sigma\}}(u) = P_{\{\sigma\}}(v), \text{ pour tout } \sigma \text{ de } \Sigma \text{ et} \\ P_{\{\alpha,\beta\}}(u) = P_{\{\alpha,\beta\}}(v), \text{ pour tout } (\alpha, \beta) \notin \theta \end{cases}$$

On a $u \overset{*}{\underset{T_\theta}{\Longleftrightarrow}} v$ ssi $(u, v) \in id_{\Sigma^*} \cup \left(\bigcup_{n=1}^{n=+\infty} \left(\underset{T_\theta}{\Longrightarrow} \cup \underset{T_\theta}{\Longrightarrow}^{-1} \right)^n \right)$, on distingue les deux cas :

1. Si $(u, v) \in id_{\Sigma^*}$, donc on a les deux conditions $i)$ et $ii)$.

2. Si $(u,v) \in \left(\bigcup_{n=1}^{n=+\infty} \left(\underset{T_\theta}{\Longrightarrow} \cup \underset{T_\theta}{\Longrightarrow}^{-1} \right)^n \right)$, i.e, $\exists m \in \mathbb{N} - \{0\} : (u,v) \in \left(\underset{T_\theta}{\Longrightarrow} \cup \underset{T_\theta}{\Longrightarrow}^{-1} \right)^m$,

Si $m = 1$, i.e, $u \left(\underset{T_\theta}{\Longrightarrow} \cup \underset{T_\theta}{\Longrightarrow}^{-1} \right) v$, alors $\exists\, (\lambda,\mu) \in \theta, \exists x, y \in \Sigma^*$ tels que:
$(u = x\lambda\mu y$ et $v = x\mu\lambda y)$ ou $(u = x\mu\lambda y$ et $v = x\lambda\mu y)$. Dans le cas où, $(u = x\lambda\mu y$ et $v = x\mu\lambda y)$ on vérifit que $\forall \sigma \in \Sigma : P_{\{\sigma\}}(u) = P_{\{\sigma\}}(v)$. On a les cas suivants:

• Si $\sigma \neq \lambda$ et $\sigma \neq \mu$, alors $P_{\{\sigma\}}(x\lambda\mu y) = P_{\{\sigma\}}(x\mu\lambda y) = P_{\{\sigma\}}(xy)$.

• Si $\sigma = \lambda$, alors $P_{\{\lambda\}}(x\lambda\mu y) = P_{\{\lambda\}}(x\mu\lambda y) = P_{\{\lambda\}}(x)\, \lambda P_{\{\lambda\}}(y)$.

• Si $\sigma = \mu$, alors $P_{\{\mu\}}(x\lambda\mu y) = P_{\{\mu\}}(x\mu\lambda y) = P_{\{\mu\}}(x)\, \lambda P_{\{\mu\}}(y)$.

De la même manière on vérifit que

• Si $(u = x\mu\lambda y$ et $v = x\lambda\mu y)$, alors, $\forall \sigma \in \Sigma : P_{\{\sigma\}}(u) = P_{\{\sigma\}}(v)$.

Montrons que $\forall\, (\alpha,\beta) \notin \theta : P_{\{\alpha,\beta\}}(u) = P_{\{\alpha,\beta\}}(v)$.

• Si $(u = x\lambda\mu y$ et $v = x\mu\lambda y)$, on a $P_{\{\alpha,\beta\}}(u) = P_{\{\alpha,\beta\}}(x)P_{\{\alpha,\beta\}}(\lambda\mu)P_{\{\alpha,\beta\}}(y)$. Et $P_{\{\alpha,\beta\}}(v) = P_{\{\alpha,\beta\}}(x)P_{\{\alpha,\beta\}}(\mu\lambda)P_{\{\alpha,\beta\}}(y)$, donc pour montrer que, $\forall\, (\alpha,\beta) \notin \theta : P_{\{\alpha,\beta\}}(u) = P_{\{\alpha,\beta\}}(v)$, il suffit de vérifier que $\forall\, (\alpha,\beta) \notin \theta : P_{\{\alpha,\beta\}}(\lambda\mu) = P_{\{\alpha,\beta\}}(\mu\lambda)$. On suppose que $\exists\, (\alpha,\beta) \notin \theta : P_{\{\alpha,\beta\}}(\lambda\mu) \neq P_{\{\alpha,\beta\}}(\mu\lambda)$. On a les deux cas suivants :

• Si $P_{\{\alpha,\beta\}}(\lambda\mu) = \lambda\mu$ et $P_{\{\alpha,\beta\}}(\mu\lambda) = \mu\lambda$ avec $\lambda \neq \mu$, alors $(\lambda = \alpha$ et $\mu = \beta)$ ou $(\lambda = \beta$ et $\mu = \alpha)$. Dans les dex cas on a, $\{\alpha,\beta\} = \{\lambda,\mu\}$, donc $(\alpha,\beta) \in \theta$, contradiction.

• Si $\big(P_{\{\alpha,\beta\}}(\lambda\mu) = \lambda$ et $P_{\{\alpha,\beta\}}(\mu\lambda) = \mu avec \lambda \neq \mu\big)$ ou $\big(P_{\{\alpha,\beta\}}(\lambda\mu) = \mu$ et $P_{\{\alpha,\beta\}}(\mu\lambda) = \lambda,\ \lambda \neq \mu\big)$, alors $\{\alpha,\beta\} = \{\lambda,\mu\}$, donc $(\alpha,\beta) \in \theta$, contradiction.

• Si $m \geq 2$, on a $(u,v) \in \left(\underset{T_\theta}{\Longrightarrow} \cup \underset{T_\theta}{\Longrightarrow}^{-1} \right)^m$ i.e, il existe une suite d'éléments $u_1, ..., u_{m-1}$ de Σ^* tels que :
$u_1 \left(\underset{T_\theta}{\Longrightarrow} \cup \underset{T_\theta}{\Longrightarrow}^{-1} \right) u_2$ et $u_2 \left(\underset{T_\theta}{\Longrightarrow} \cup \underset{T_\theta}{\Longrightarrow}^{-1} \right) u_3, ..., u_{m-1} \left(\underset{T_\theta}{\Longrightarrow} \cup \underset{T_\theta}{\Longrightarrow}^{-1} \right) v$. Dans ce cas il est claire qu'on a les deux conditions vérifieés.

Pour la réciproque, raisonnons par récurrence sur la longueur commune de u et v. Pour $|u| = |v|$, comme $P_{\{\sigma\}}(u) = P_{\{\sigma\}}(v)$, pour tout σ de Σ, on a $u = v$, donc $(u,v) \in id_{\Sigma^*}$, alors $u \underset{T_\theta}{\overset{*}{\Longleftrightarrow}} v$. On suppose que $|u| = |v| \geq 2$ et posons $u = \sigma_0 u'$ avec $\sigma_0 \in \Sigma, u' \in \Sigma^*$. Comme $P_{\{\sigma_0\}}(u) = P_{\{\sigma_0\}}(v)$, on a $P_{\{\sigma_0\}}(v) \neq \epsilon$. Posons $v = v'\sigma_0 v$" avec $P_{\{\sigma_0\}}(v') = \epsilon$ (si on commence par σ_0, on prend $v' = \epsilon$, sinon $v' \neq \epsilon$). Montrons d'abord que $\sigma_0 v' \underset{T_\theta}{\overset{*}{\Longleftrightarrow}} v'\sigma_0$, cela est vrai si $v' = \epsilon$, sinon soit $\eta_1 \in Alph\,(v')$. Alors $P_{\{\sigma_0,\eta_1\}}(v)$ commence par η_1 tandis que $P_{\{\sigma_0,\eta_1\}}(u)$ commence par σ_0, cela implique que $(\sigma_0,\eta_1) \in \theta$, donc $\sigma_0\eta_1 \underset{T_\theta}{\overset{*}{\Longleftrightarrow}} \eta_1\sigma_0$. On

note $v' = \eta_1 ... \eta_n$, on a $\forall 1 \leq i \leq n : (\sigma_i, \eta_1) \in \theta$, donc $\sigma_0 \eta_i \overset{*}{\underset{T_\theta}{\Longleftrightarrow}} \eta_i \sigma_0$, et par conséquent $\sigma_0 v' \overset{*}{\underset{T_\theta}{\Longleftrightarrow}} v' \sigma_0$. Ainsi on a $\sigma_0 v' v" \overset{*}{\underset{T_\theta}{\Longleftrightarrow}} v' \sigma_0 v"$ i.e, $\sigma_0 v' v" \overset{*}{\underset{T_\theta}{\Longleftrightarrow}} v$. On montre que $v' v" \overset{*}{\underset{T_\theta}{\Longleftrightarrow}} u'$, soient $\alpha, \beta \in \Sigma$ tels que $(\alpha, \beta) \notin \theta$, on distingue les deux cas suivants:

• Si $\sigma_0 \notin \{\alpha, \beta\}$, alors,

$$P_{\{\alpha,\beta\}}(v'v") = P_{\{\alpha,\beta\}}(v'\sigma_0 v") = P_{\{\alpha,\beta\}}(v) = P_{\{\alpha,\beta\}}(u) = P_{\{\alpha,\beta\}}(\sigma_0 u') = P_{\{\alpha,\beta\}}(u').$$

• Si par contre $\sigma_0 \in \{\alpha, \beta\}$, supposons par exemple $\alpha = \sigma_0$, on a

$P_{\{\sigma_0,\beta\}}(v) = P_{\{\sigma_0,\beta\}}(v'\sigma_0 v") = \sigma_0 P_{\{\sigma_0,\beta\}}(v") = \sigma_0 P_{\{\sigma_0,\beta\}}(v'v") = P_{\{\sigma_0,\beta\}}(u) = \sigma_0 P_{\{\sigma_0,\beta\}}(u')$,

d'où $P_{\{\sigma_0,\beta\}}(v'v") = P_{\{\sigma_0,\beta\}}(u')$, maintenant montrons que,

$\forall \sigma \in \Sigma : P_{\{\sigma\}}(v'v") = P_{\{\sigma\}}(u')$, on distingue les deux cas:

• Si $\sigma \neq \sigma_0$, on a, $P_{\{\sigma\}}(u) = P_{\{\sigma\}}(v) \Rightarrow P_{\{\sigma\}}(\sigma_0 u') = P_{\{\sigma\}}(v'\sigma_0 v") \Rightarrow P_{\{\sigma\}}(u') = P_{\{\sigma\}}(v'v")$.

• Si $\sigma = \sigma_0$, on a, $P_{\{\sigma_0\}}(u) = P_{\{\sigma_0\}}(\sigma_0 u') = \sigma_0 P_{\{\sigma_0\}}(u')$

et $P_{\{\sigma_0\}}(v) = P_{\{\sigma_0\}}(v'\sigma_0 v") = \sigma_0 P_{\{\sigma_0\}}(v'v")$.

Et par l'hypothèse de récurence, on a donc $v'v" \overset{*}{\underset{T_\theta}{\Longleftrightarrow}} u'$, on a $v'v" \overset{*}{\underset{T_\theta}{\Longleftrightarrow}} u' \Rightarrow \sigma_0 v'v" \overset{*}{\underset{T_\theta}{\Longleftrightarrow}} \sigma_0 u'$.

Finalement on a $\left(\sigma_0 v'v" \overset{*}{\underset{T_\theta}{\Longleftrightarrow}} \sigma_0 u' \text{ et } \sigma_0 v'v" \overset{*}{\underset{T_\theta}{\Longleftrightarrow}} v\right)$, donc $u \overset{*}{\underset{T_\theta}{\Longleftrightarrow}} v$.

Chapitre 4

Quelques applications de semi-systèmes de réécriture et le problème du mot dans un monoïde

Introduction

Dans ce chapitre on donne quelques applications de semi-systèmes de réécriture et le problème du mot dans monoïde.

Contenu du chapitre 4

4.1. La construction de certains codes à groupes.
4.2. Présentation de quelques monoïdes par générateurs et relations.
4.3. Présentation de quelques groupes par générateurs et relations.
4.4. Etude d'un système de cryptage basé sur le problème du mot dans un monoïde libre.
4.5. Langage engendré par un semi-système de réécriture.
4.6. Les bases de Gröbner et semi-systèmes de rèèctiture de mots.

4.1 La construction de certains codes à groupes

Dans la théorie de code, on distingue deux grandes familles de codes : les codes de longueurs constantes, les codes de longueurs variables.

Les codes de longueurs variables constituent une classe d'objets très importante, comme témoignent les différents domaines dans lesquels ils furent introduits : en théorie de l'information par SHANNON (1950), dans la théorie des langages formels par SCHUTZENBERGER (1956).

Dans ce travail, on s'intéresse à ce dernier type de code plus précisément les codes de longueurs variables dits codes à groupes.

Définition 4.1.1

Une partie X de Σ^* est un code si, et seulement, si tout mot de X^+ admet une unique factorisation en mots de X. Autrement dit, pour tous $m, n \geq 1$ et $x_1, ..., x_n, y_1, ..., y_m \in X$, la condition $x_1x_2...x_n = y_1y_2...y_m$ implique $n = m$ et $x_i = y_i$ pour tout $i = 1, ..., n$.

On dit qu'un code X sur Σ est maximal dans Σ^* (au sens de l'inclusion) si pour tout code $X' \subseteq \Sigma^*$, si $X \subseteq X'$, alors $X = X'$.

Exemple 4.1.2

1. Soit l'alphabet $\Sigma = \{a, b\}$, l'ensemble $X = \{a^n b^n : n \geq 1\}$ est un code.

2. Soit l'alphabet $\Sigma = \{a, b\}$, l'ensemble $X = \{a, ab, ba\}$ n'est pas un code puisque $aba \in X^+$ et $aba = a(ba) = (ab)a$ (aba admet donc deux factorisations différents en mots de X).

Définition 4.1.3

Une partie X de Σ^* est préfixe (resp. suffixe) si aucun facteur gauche (resp. droit) propre d'un mot de X n'est dans X, en symboles: $X \cap X\Sigma^+ = \emptyset$ (resp. $X \cap X\Sigma^+ = \emptyset$). La partie X de Σ^* est bi-préfixe s'il est à la fois préfixe et suffixe.

Proposition 4.1.4

Soient G un groupe et H un sous groupe de G, $\psi : \Sigma^* \longrightarrow G$ un morphisme. Posons $X^* = \psi^{-1}(H)$ avec X l'ensemble minimal générateur de X^*. Alors:

1. *X est un code bi-préfixe.*

2. *Si ψ est surjectif, alors X est un code maximal bi-préfixe.*

Remarque 4.1.5

1. Dans le cas où le morphisme ψ est surjectif, la base X de X^* (qui est donc toujours un code bi-préfixe maximal) est nommée code à groupe. Nous dirons que c'est le code à groupe défini à partir de G, H et ψ, nous le noterons $X\,(G,H)_{\psi}$.

2. Soit $X\,(G,H)_{\psi}$ un code à groupe. Nous dirons que X est de degré d si $[G:H]=d$.

Nous dirons que X est régulier si $H=\{1_G\}$.

Exemples 4.1.6 [16]

1. Considérons le morphisme de monoïdes $\psi:\{a,b\}^*\longrightarrow(\mathbb{Z},+)$ defini par :

$\psi(a)=1,\psi(b)=-1,\psi(\epsilon)=0$. Donc, $\forall w\in\{a,b\}^*:\psi(w)=|w|_a-|w|_b$.

l' application ψ est surjective car $\forall m\in\mathbb{Z},\exists w\in\{a,b\}^*$ tel que $\psi(w)=m$.

On distingue les cas suivants :

1. Si $m=0$, alors $\psi(\epsilon)=0$.

2. Si $m>0$, alors $\psi(a^m)=m\cdot\psi(a)=m\cdot 1=m$.

3. Si $m<0$, alors $\psi(b^{-m})=-m\cdot\psi(b)=-m\cdot(-1)=m$.

Soit $H=\{0\}$ le sous groupe trivial de $(\mathbb{Z},+)$. Alors

$X^*=\psi^{-1}(\{0\})=\{w\in\{a,b\}^*:\psi(w)=|w|_a-|w|_b=0\}$

$=\{w\in\{a,b\}^*:|w|_a=|w|_b\}$. Donc X est infini car X contient les mots de la forme $a^nb^n,n>0$, finalement, d'après la proposition 4.1.4**,** X est un code maximal bipréfixe.

2. Soit $\psi:\Sigma^*\longrightarrow(\mathbb{Z}/n\mathbb{Z},\oplus)$ le morphisme de monoïdes défini par :

$\psi(\sigma)=\overline{1}$ pour tout $\sigma\in\Sigma$ et $\psi(\epsilon)=\overline{0}$.

Donc pour tout $w\in\Sigma^*:\psi(w)=|w|\ mod\,(n)$. L'application ψ est surjective car pour tout $\overline{m}\in\mathbb{Z}/n\mathbb{Z}$, il existe $w=\sigma^m\in\Sigma^*$, $\sigma\in\Sigma$, tel que $\psi(\sigma^m)=\overline{m}$.

$X^*=\psi^{-1}(\{\overline{0}\})=\{w\in\Sigma^*:|w|\equiv 0\ (\mathrm{mod}\ n)\}$.

Alors $X=\Sigma^n$. D'après la proposition 4.1.4**,** X est un code maximal bi-préfixe.

Proposition 4.1.7

Soit $X\subseteq\Sigma^*$. Alors X est un code à groupe si, et seulement si le monoïde syntaxique $M(X^*)$ est un groupe.

Exemple 4.1.8

Considérons le morphisme $\psi:\{a,b\}^*\longrightarrow(\mathbb{Z}/2\mathbb{Z},\oplus)$ défini par :

$\psi(a)=\overline{0},\psi(b)=\overline{1},\psi(\epsilon)=0$.

On pose $X^* = \psi^{-1}(\{\overline{0}\}) = \{w \in \{a,b\}^* : |w|_b \equiv 0\,[2]\}$. Donc $X = ba^*b \cup \{a\}$.

le monoïde syntaxique $M(X^*)$ est un groupe d'ordre 2.

Proposition 4.1.9

Soit $X \subseteq \Sigma^*$ un code fini. $M(X^*)$ est un groupe si, et seulement si $X = \Sigma^n$. Et dans ce cas $M(X^*)$ est cyclique d'ordre n.

Exemple 4.1.10 [16]

Considérons le morphisme $\psi : \{a,b\}^* \longrightarrow \mathbb{Z}/3\mathbb{Z}$ défini par :

$\psi(a) = \psi(b) = \overline{1}, \psi(\epsilon) = \overline{0}$.

On pose $X^* = \psi^{-1}(\{\overline{0}\}) = \{w \in \{a,b\}^* : |w| \equiv 0\,[3]\}$.

Alors $X = \{a,b\}^3 = \{aaa, abb, aab, aba, baa, bbb, bab, bba\}$. $M(X^*)$ est un groupe cyclique d'ordre 3.

Proposition 4.1.11 [16]

Soient G un groupe et H un sous groupe de G. Soit $\psi : \Sigma^* \longrightarrow G$ un morphisme surjectif. Le Sous monoïde $X^* = \psi^{-1}(H)$ est complet.

Démonstration

Le Sous monoïde $X^* = \psi^{-1}(H)$ est complet si, et seulement si pour tout $w \in \Sigma^*$, il existe $u, v \in \Sigma^*$ tels que $uwv \in X^*$. Comme $X^* = \psi^{-1}(H)$, On a

$$uwv \in X^* \Longleftrightarrow \psi(uwv) \in H \Longleftrightarrow \psi(u)\psi(w)\psi(v) \in H.$$

On pose $\psi(u) = (\psi(w))^{-1}$ où $((\psi(w))^{-1}$ désigne l'inverse de $\psi(w)$ dans le groupe G), i.e., $u \in \psi^{-1}\left(\left\{(\psi(w))^{-1}\right\}\right)$ avec $\psi^{-1}\left(\left\{(\psi(w))^{-1}\right\}\right)$ est l'image réciproque de $\left\{(\psi(w))^{-1}\right\}$ et $v = \epsilon$. Donc $\psi(u)\psi(w)\psi(v) = (\psi(w))^{-1}.\psi(w).\psi(\epsilon) = 1_G.1_G = 1_G \in H$.

Exemple 4.1.12 [16]

Considérons le morphisme de monoïdes $\psi : \{a,b\}^* \longrightarrow (\mathbb{Z}, +)$ defini par:

$\psi(a) = 1, \psi(b) = -1, \psi(\epsilon) = 0$. Donc, $\forall w \in \{a,b\}^* : \psi(w) = |w|_a - |w|_b$.

On pose $X^* = \psi^{-1}(\{0\}) = \{w \in \{a,b\}^* : |w|_a = |w|_b\}$. On montre que X^* est un sous monoïde complet de $\{a,b\}^*$. Soit $w \in \{a,b\}^*$, on distingue les cas suivants :

Cas 1 :

Si $w \in X^*$, alors $|w|_a = |w|_b$, dans ce cas on pose $u = v = \epsilon$, on a $\epsilon w \epsilon = w \in X^*$.

Cas 2 :

Si $|w|_a < |w|_b$, alors il suffit de prendre $u = a^{|w|_b - |w|_a}$ et $v = \epsilon$. On a

$|uwv|_a = |u|_a + |w|_a + |v|_a = |w|_b - |w|_a + |w|_a + 0 = |w|_b$.

De même on a $|uwv|_b = |u|_b + |w|_b + |v|_b = 0 + |w|_b + 0 = |w|_b$.

Alors , on a $|uwv|_a = |uwv|_b$ et par conséquent $uwv \in X^*$.

Cas 3 :

Si $|w|_a > |w|_b$, alors il suffit de prendre $u = b^{|w|_a - |w|_b}$ et $v = \epsilon$.

On a $|uwv|_a = |u|_a + |w|_a + |v|_a = 0 + |w|_a + 0 = |w|_a$.

De même on a $|uwv|_b = |u|_b + |w|_b + |v|_b = |w|_a - |w|_b + |w|_b + 0 = |w|_a$.

Par suite on a $|uwv|_a = |uwv|_b$ donc $uwv \in X^*$.

4.2 Présentation de quelques monoïdes par générateurs et relations

Une présentation d'un monoïde M est la donnée d'un ensemble Σ, appelé alphabet, et d'un ensemble $\mathcal{R}$ de relations sur Σ^*, de telle manière que le monoïde M soit isomorphe à l'ensemble de mots engendré par l'alphabet, quotienté par la relation de congruence $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ engendré par $\mathcal{R}$, i.e, $M \cong \Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$.

Définition 4.2.1

Une présentation (par générateurs et relations) d'un monoïde M est la donnée d'un alphabet Σ et d'une relation binaire R sur Σ^* tels que M soit isomorphe au quotient de Σ^* par la congruence $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ engendrée par R, i.e, $M \cong \Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$.
Si les deux ensembles Σ et R sont finis, on dit que le monoïde M est finiment présenté.

Exemples 4.2.2

1. Soient $\Sigma = \{\sigma\}$, et la relation $\mathcal{R} = \varnothing$ (la relation vide), On a $(\{\sigma\}^*, \cdot) \cong (\mathbb{N}, +)$ où l'isomorphisme est défini par : $\epsilon \mapsto 0, \sigma \mapsto 1$.

2. La présentation du monoïde $(\mathbb{N}^2, +)$: Soient $\Sigma = \{\alpha, \beta\}$ et la relation $\mathcal{R} = \{\alpha\beta \longrightarrow \beta\alpha\}$. On a, pour tout $w \in \Sigma^*$, il existe un unique $(n, m) \in \mathbb{N}^2$ tels que $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \beta^n\alpha^m$, où $m = |w|_\alpha$ et $n = |w|_\beta$. On définit l'isomorphisme $\psi : \mathbb{N}^2 \longrightarrow \Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$, $\psi(n, m) = [\beta^n\alpha^m]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ où $[\beta^n\alpha^m]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ désigne la classe d'équivalence du mot $\beta^n\alpha^m$. L'application ψ est un morphisme. En effet, pour $(n, m) \in \mathbb{N}^2, (p, q) \in \mathbb{N}^2$, on a $\psi((n, m) + (p, q)) = \psi(n + p, m + q)$
$= \left[\beta^{n+p}\alpha^{m+q}\right]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\beta^n\beta^p\alpha^m\alpha^q]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\beta^n\alpha^m\beta^p\alpha^q]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\beta^n\alpha^m]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \cdot [\beta^p\alpha^q]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = \psi(n, m)\, \psi(p, q)$.
Il est clair que ψ est surjectif. Montrons maintenant que ψ est injectif.
On a $\forall (n, m) \in \mathbb{N}^2, \forall (p, q) \in \mathbb{N}^2, \psi(n, m) = \psi(p, q) \Longleftrightarrow [\beta^n\alpha^m]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\beta^p\alpha^q]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$
$\Longleftrightarrow (n = p \text{ et } m = q)$.

3. La présentation du monoïde $(\mathbb{Z}, +)$: Soient $\Sigma = \{\alpha, \beta\}$, et la relation $\mathcal{R} = \{\alpha\beta \longrightarrow \epsilon, \beta\alpha \longrightarrow \epsilon\}$. Soit $w \in \Sigma^*$, on distingue les trois cas suivants :

- Si $|w|_\alpha = |w|_\beta$, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \epsilon$.
- Si $|w|_\alpha > |w|_\beta$, c'est-à-dire $|w|_\alpha = |w|_\beta + n, n \in \mathbb{N}^*$, dans ce cas $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha^n$.
- Si $|w|_\beta > |w|_\alpha$, c'est-à-dire $|w|_\beta = |w|_\alpha + m, m \in \mathbb{N}^*$, dans ce cas $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \beta^m$.

Donc $\mathbb{Z} \cong \Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} = \left\{ [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, [\alpha^n]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, [\beta^m]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, (n,m) \in \mathbb{N}^* \times \mathbb{N}^* \right\}$, Où l'isomorphisme ϕ est défini par : $\phi(0) = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, si $n > 0$, alors $\phi(n) = [\alpha^n]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, si $n < 0$, alors $\phi(n) = \left[\beta^{-n}\right]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$.

La proposition suivante est spécifique à la présentation d'un monoïde fini.

Proposition 4.2.3

Tout monoïde fini a une présentation finie.

Démonstration

Soit $M = \{x_1, ..., x_n\}$ un monoïde fini de cardinal n, $n \in \mathbb{N}^*$ et d'élément neutre e.

Soient $\Sigma = \{\alpha_{x_i}, x_i \in M, 1 \leq i \leq n\}$ et la relation $\mathcal{R} = \left\{\alpha_{x_i}\alpha_{x_j} \longrightarrow \alpha_{x_i x_j}, \alpha_e \longrightarrow \epsilon, x_i, x_j \in M\right\}$.

Où ϵ est le mot vide, alors pour tout $w \in \Sigma^*$, il existe $\{x_i, ..., x_j\} \subseteq M$, tels que

$w = \alpha_{x_i}...\alpha_{x_j}$, et $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha_{x_k}$, où $x_k = x_i...x_j$. Finalement on a

$\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} = \left\{ [w_{x_k}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, x_k \in M, 1 \leq k \leq n \right\}$, et par suite on définit l'isomorphisme ψ comme suit :

$\psi : M \longrightarrow \Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$, $\psi(x_k) = [w_{x_k}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, où $x_k = x_i...x_j$, $w = \alpha_{x_i}...\alpha_{x_j}, \{x_i, ..., x_j\} \subseteq M$.

Montrons que ψ est un morphisme de monoïdes. Pour $(x_k, x_l) \in M^2$,

on a $\psi(x_k x_l) = \psi(x_m) = [w_{x_m}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, où $x_m = x_k x_l$ et $w = \alpha_{x_k}\alpha_{x_l}$.

Donc $[w_{x_m}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\alpha_{x_k}\alpha_{x_l}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\alpha_{x_k}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \cdot [\alpha_{x_l}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = \psi(x_k)\psi(x_l)$. La surjectivité de ψ est triviale étant donnée que $\psi([w_{x_k}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}) = x_k$. Pour l'injectivité de ψ, on a $\forall (x_k, x_l) \in M^2$, il existe $\{x_i, ...x_j\}, \{x_s, ..., x_t\} \subseteq M : x_k = x_i...x_j$ et $x_l = x_s...x_t$, si $\psi(x_k) = \psi(x_l)$ alors

$\psi(x_i...x_j) = \psi(x_s...x_t) \Rightarrow \left[\alpha_{x_i}...\alpha_{x_j}\right]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\alpha_{x_s}...\alpha_{x_t}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \Rightarrow \left[\alpha_{x_i...x_j}\right]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\alpha_{x_s...x_t}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$

$\Rightarrow x_i...x_j = x_s...x_t \Rightarrow x_k = x_l$. □

Exemple 4.2.4

Soit le monoïde $M = \left\{ x_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, x_1 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, x_2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$ muni de la multiplication des matrices. La table de Cayley de M est définie comme suit:

$\cdot$	x_0	x_1	x_2
x_0	x_0	x_1	x_2
x_1	x_1	x_1	x_2
x_2	x_2	x_1	x_2

Le monoïde M vérifie les deux propriétés suivantes:$\forall x_i \in M, x_i x_1 = x_1$ et $x_i x_2 = x_2$.

Considérons $\Sigma = \{\alpha_{x_i}, x_i \in M, 0 \leq i \leq 2\}$ et $\mathcal{R} = \left\{\alpha_{x_i}\alpha_{x_j} \longrightarrow \alpha_{x_i x_j}, \alpha_{x_0} \longrightarrow \epsilon, x_i, x_j \in M\right\}$.

Où ϵ est le mot vide, donc pour tout $w \in \Sigma^*$, il existe $\{x_i, ..., x_j\} \subseteq M$ tels que
$w = \alpha_{x_i}...\alpha_{x_j}$ et $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha_{x_k}$, avec $x_k = x_i...x_j$. On distingue les trois cas suivants :

• Si $w = u\alpha_{x_1}$, $u \in \Sigma^*$, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha_{x_1}$.

• Si $w = u\alpha_{x_2}$, $u \in \Sigma^*$, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha_{x_2}$.

• Si $w = \alpha_{x_0}...\alpha_{x_0}$, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \epsilon$.

Donc $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} = \left\{ [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, [\alpha_{x_1}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, [\alpha_{x_2}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \right\}$. Par conséquent on peut définir l'isomorphisme ψ comme suit: $\psi : M \longrightarrow \Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}, \psi(x_0) = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, \psi(x_1) = [\alpha_{x_1}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, \psi(x_2) = [\alpha_{x_2}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$.

Les propositions qui suivent permettent de donner des conditions sur les relations qui assurent l'existence d'un morphisme entre les deux monoïdes quotients.

Proposition 4.2.5 [18]

Soient $(\Sigma_1, \mathcal{R}_1)$ et $(\Sigma_2, \mathcal{R}_2)$ deux semi-systèmes de réécriture et $h : \Sigma_1^* \longrightarrow \Sigma_2^*$ un morphisme de monoïdes tel que $[h(r)]_{\overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}}} = [h(s)]_{\overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}}}$ pour tout $r \longrightarrow s \in R_1$, où $[h(x)]_{\overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}}}$ désigne la classe d'équivalence de l'élément $h(x)$ modulo la congruence engendrée par R_2, alors il existe un unique morphisme ψ de $\Sigma_1^*/\overset{*}{\underset{\mathcal{R}_1}{\Longleftrightarrow}}$ dans $\Sigma_2^*/\overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}}$, avec $\psi \circ p_1 = p_2 \circ h$.

Démonstration

Comme on a $[h(r)]_{\overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}}} = [h(s)]_{\overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}}}$ pour tout $r \longrightarrow s \in \mathcal{R}_1$, donc le morphisme $p_2 \circ h$,
vérifie la propriété suivante : pour tout $r \longrightarrow s \in \mathcal{R}_1$, $(p_2 \circ h)(r) = (p_2 \circ h)(s)$.
Donc, il existe un unique morphisme ψ de $\Sigma_1^*/\overset{*}{\underset{\mathcal{R}_1}{\Longleftrightarrow}}$ vers $\Sigma_2^*/\overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}}$, avec $\psi \circ p_1 = p_2 \circ h$.

Exemple 4.2.6

Considérons les deux monoïdes Σ_1^* et Σ_2^* ainsi que les deux relations $\mathcal{R}_1$ et $\mathcal{R}_2$,

où, $\begin{cases} \Sigma_1 = \{\alpha, \beta\}. \\ \mathcal{R}_1 = \{\alpha\beta \longrightarrow \alpha, \beta\alpha \longrightarrow \alpha\}. \end{cases}$ et $\begin{cases} \Sigma_2 = \{\gamma, \lambda, \mu\}. \\ \mathcal{R}_2 = \{\mu\gamma \longrightarrow \gamma, \lambda\mu \longrightarrow \lambda\}. \end{cases}$

Et soit h le morphisme de Σ_1^* dans Σ_2^* defini par: $\begin{cases} h(\alpha) = \gamma\lambda \\ h(\beta) = \mu \end{cases}$.

On a $p_2 : \Sigma_2^* \longrightarrow \Sigma_2^*/\overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}}$ vérifie les égalités suivante: $p_2(\mu\gamma), p_2(\lambda\mu) = p_2(\lambda)$.
On montre que pour tout (r, s) de $\mathcal{R}_1$, on a $(p_2 \circ h)(r) = (p_2 \circ h)(s)$.
On a $(p_2 \circ h)(\alpha\beta) = p_2(\gamma\lambda\mu) = p_2(\gamma)p_2(\lambda\mu) = p_2(\gamma)p_2(\lambda) = p_2(\gamma\lambda) = (p_2 \circ h)(\alpha)$.
De même $(p_2 \circ h)(\beta\alpha) = p_2(\mu\gamma\lambda) = p_2(\mu\gamma)p_2(\lambda) = p_2(\gamma)p_2(\lambda) = p_2(\gamma\lambda) = (p_2 \circ h)(\alpha)$.
Et par conséquent il existe un unique morphisme ψ de $\Sigma_1^*/\overset{*}{\underset{\mathcal{R}_1}{\Longleftrightarrow}}$ dans $\Sigma_2^*/\overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}}$,
avec $\psi \circ p_1 = p_2 \circ h$.

Proposition 4.2.7 [18]

Soient $(\Sigma_1, \mathcal{R}_1)$ *et* $(\Sigma_2, \mathcal{R}_2)$ *deux semi-systèmes de réécriture convergents et* $h : \Sigma_1^* \longrightarrow \Sigma_2^*$ *un isomorphisme de monoïdes tels que* $[h(r)]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_2}} = [h(s)]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_2}}$ *et* $h(IRR(R_1)) \subseteq IRR(R_2)$*, on obtient dans ce cas :* $\Sigma_1^*/\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1} \cong \Sigma_2^*/\overset{*}{\Longleftrightarrow}_{\mathcal{R}_2}$.

Démonstration

Comme $[h(r)]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_2}} = [h(s)]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_2}}$, alors pour tout $r \longrightarrow s \in \mathcal{R}_1$, $(p_2 \circ h)(r) = (p_2 \circ h)(s)$.

Donc il existe un unique morphisme ψ de $\Sigma_1^*/\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}$ dans $\Sigma_2^*/\overset{*}{\Longleftrightarrow}_{\mathcal{R}_2}$, avec $\psi \circ p_1 = p_2 \circ h$.

Plus précisément le morphisme ψ est défini par : $\psi([x]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}}) = [h(x)]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_2}}$.

Montrons que ψ est injectif. Soient $[x]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}}, [y]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}} \in \Sigma_1^*/\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}$, comme $(\Sigma_1, \mathcal{R}_1)$ est convergent, alors il existe $(u, v) \in IRR(\mathcal{R}_1)$ tels que $([x]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}} = [u]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}}$ et $[y]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}} = [v]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}})$, donc $\psi([x]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}}) = \psi([y]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}}) \Leftrightarrow \psi([u]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}}) = \psi([v]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}}) \Leftrightarrow [h(u)]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_2}} = [h(v)]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_2}}$, comme $h(IRR(\mathcal{R}_1)) \subseteq IRR(\mathcal{R}_2))$ et $(\Sigma_2, \mathcal{R}_2)$ est convergent on a $h(u) = h(v)$ et par suite $u = v$ car h est injectif ce qui montre qu'on a bien $[x]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}} = [y]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}}$. Enfin, d'après la surjectivité de h, le morphisme ψ est surjectif car pour tout $y \in \Sigma_2^*, \exists x \in \Sigma_1^*$, avec $y = h(x)$ ce qui permet à écrire $[y]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_2}} = [h(x)]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_2}} = \psi([x]_{\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1}})$. Finalement on a bien $\Sigma_1^*/\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1} \cong \Sigma_2^*/\overset{*}{\Longleftrightarrow}_{\mathcal{R}_2}$. □

Exemple 4.2.8

Considérons les deux monoïdes Σ_1^* et Σ_2^* ainsi que les deux relations $\mathcal{R}_1$ et $\mathcal{R}_2$,

où, $\begin{cases} \Sigma_1 = \{\alpha\}. \\ \mathcal{R}_1 = \{\alpha\alpha \longrightarrow \epsilon\}. \end{cases}$ et $\begin{cases} \Sigma_2^* = \mathbb{N} = \langle 1 \rangle. \\ \mathcal{R}_2 = \{0+0 \longrightarrow 0, 0+1 \longrightarrow 1, 1+0 \longrightarrow 1, 1+1 \longrightarrow 0\}. \end{cases}$

Et soit h le morphisme de longueur de Σ_1^* dans Σ_2^* défini par: $w \longmapsto |w|$, il est clair que h est bijectif.

On montre que $(p_2 \circ h)(\alpha\alpha) = (p_2 \circ h)(\epsilon)$.

On a $(p_2 \circ h)(\alpha\alpha) = p_2(2) = p_2(0) = (p_2 \circ h)(\epsilon)$.

De plus on a $IRR(\mathcal{R}_1) = \{\epsilon, \alpha\}$ et $h(IRR(\mathcal{R}_1)) = \{0, 1\} = IRR(\mathcal{R}_2)$.

Finalement on a $\Sigma_1^*/\overset{*}{\Longleftrightarrow}_{\mathcal{R}_1} \cong \Sigma_2^*/\overset{*}{\Longleftrightarrow}_{\mathcal{R}_2}$.

Dans la proposition suivante, on donne une condition sur la relation d'un semi-système de réécriture pour montrer que la congruence engendrée par cette relation est incluse dans la congruence syntaxique de la classe d'un mot quelconque modulo de la congruence associée un morphisme de *monoïde*s.

Proposition 4.2.9 [18]

Soit $h : \Sigma^* \longrightarrow M$ un morphisme de monoïdes et R une relation binaire sur Σ^* tel que $h(r) = h(s)$ pour tout $r \longrightarrow s \in R$, alors pour tout $u \in \Sigma^*$, la congruence engendrée par R est incluse dans la congruence syntaxique de la classe d'équivalence de u modulo $\equiv_h$. Auterment dit: $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \subseteq \equiv_{[u]_{\equiv_h}}$ avec $\equiv_{[u]_{\equiv_h}}$ désigne la congruence syntaxique du langage $[u]_{\equiv_h}$ où $[u]_{\equiv_h}$ est le langage de la classe d'équivalence du mot u modulo la congruence associée au morphisme h.

Démonstration

Comme $h(r) = h(s)$ pour tout $r \longrightarrow s \in \mathcal{R}$, on a $\mathcal{R} \subseteq \equiv_h$ et donc $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \subseteq \equiv_h$, i.e $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est plus fine que $\Sigma^*/\equiv_h$. Par conséquent, pour tout $[u]_{\equiv_h} \in \Sigma^*/\equiv_h$, il existe une famille de mots $\{v_i\}_{i\in I}$ de Σ^* tel que $[u]_{\equiv_h} = \bigcup [v_i]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$. Montrons qu'on a $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \subseteq \equiv_{[u]_{\equiv_h}}$. Soit $\left(w, w'\right) \in \Sigma^*$ tel que $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w'$, *on doit vérifier que pour tout* $(x, y) \in \Sigma^*$, on a : $\left(xwy \in [u]_{\equiv_h} \Leftrightarrow xw'y \in [u]_{\equiv_h}\right)$.

On a $xwy \in [u]_{\equiv_h} = \bigcup [v_i]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \Leftrightarrow \exists i_0 \in I$ tel que $xwy \in [v_{i_0}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, et par suite $xwy \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} v_{i_0}$.

De plus on a $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w'$ ceci implique que $xwy \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} xw'y$ car $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est une congruence et par conséquent $xw'y \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} v_{i_0}$, ce qui montre que $xw'y \in [v_{i_0}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ et par conséquent $xw'y \in [u]_{\equiv_h} = \bigcup [v_i]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$. De la même manière on peut vérifier la réciproque. Finalement, on obtient $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \subseteq \equiv_{[u]_{\equiv_h}}$. $\square$

Exemple 4.2.10

Soit $\Sigma = \{\alpha, \beta\}$ et soit la relation $\mathcal{R} = \{\alpha\beta \longrightarrow \beta\alpha\}$. On considère le morphisme de longueur $h : \Sigma^* \longrightarrow \mathbb{N}$. On a pour tout $u \in \Sigma^*$, $[u]_{\equiv_h} = \{x \in \Sigma^* : |x| = |u|\}$. D'autre part, le *monoïde* quotient $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} = \left\{[\beta^n\alpha^m]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} : (n, m) \in \mathbb{N}^2\right\}$. Montrons que $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \subseteq \equiv_{[u]_{\equiv_h}}$, soit $(w, w') \in \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$, i.e il existe $(p, q) \in \mathbb{N}^2$ tel que $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \beta^p\alpha^q, w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \beta^p\alpha^q$, où $\left(|w|_\beta = |w'|_\beta = p, |w|_\alpha = |w'|_\alpha = q\right)$. On vérifie que $w \equiv_{[u]_{\equiv_h}} w'$, soit $(x, y) \in \Sigma^*$ tel que $xwy \in [u]_{\equiv_h}$, on a $xwy \in [u]_{\equiv_h} \Longleftrightarrow |xwy| = |u| \Longleftrightarrow |x| + |w| + |y| = |u|$, comme $\left(|w|_\beta = |w'|_\beta = p, |w|_\alpha = |w'|_\alpha = q\right)$ donc $|w| = |w'|$ ce qu'implique que $|xw'y| = |u|$, alors $xw'y \in [u]_{\equiv_h}$. De la même manière on peut vérifier l'inverse. Finalement $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \subseteq \equiv_{[u]_{\equiv_h}}$.

Finalement, on donne une relation $\mathcal{R}$ sur le *monoïde* libre Σ^* dont le *monoïde* quotient $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est un groupe.

Proposition 4.2.11 [18]

Soient $\Sigma = \{\sigma_1, \sigma_2, ..., \sigma_n\}$ *un alphabet fini et la relation définie sur* Σ^* *par* $R = \{\sigma_i\sigma_i \longrightarrow \epsilon, 1 \leq i \leq n\}$ *où* ϵ *est le mot vide.*

On obtient donc, le monoïde quotient $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ *a une structure de groupe.*

Démonstration

Il suffit de montrer que chaque classe de $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est symétrisable.

Soient $w = \sigma_{i_1}\sigma_{i_2}...\sigma_{i_k} \in \Sigma^*$ et $[w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ sa classe d'équivalence modulo $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$, autrement dit $[w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \in \Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$, avec $[w]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} = [(\sigma_{i_1}\sigma_{i_2}...\sigma_{i_k})]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$. On pose $\widetilde{w} = \sigma_{i_k}...\sigma_{i_2}\sigma_{i_1}$ ($\widetilde{w}$ est l'image miroire de w).

On a $[w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}\,[\widetilde{w}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [(\sigma_{i_1}\sigma_{i_2}...\sigma_{i_k})]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}\,[(\sigma_{i_k}...\sigma_{i_2}\sigma_{i_1})]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [(\sigma_{i_1}\sigma_{i_2}...\sigma_{i_k}\sigma_{i_k}...\sigma_{i_2}\sigma_{i_1})]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$
$= [(\sigma_{i_1}\sigma_{i_2}...\sigma_{i_k}\sigma_{i_k}...\sigma_{i_2}\sigma_{i_1})]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = \left[\left(\sigma_{i_1}\sigma_{i_2}...\sigma_{i_{k-1}}\right)\right]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}\,[(\sigma_k\sigma_k)]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}\,\left[\left(\sigma_{i_{k-1}}...\sigma_{i_2}\sigma_{i_1}\right)\right]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$
$= \left[\left(\sigma_{i_1}\sigma_{i_2}...\sigma_{i_{k-1}}\right)\right]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}\,[\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}\,\left[\left(\sigma_{i_{k-1}}...\sigma_{i_2}\sigma_{i_1}\right)\right]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = ...\,[(\sigma_1\sigma_1)]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$. □

Exemple 4.2.12

Soient $\Sigma = \{\sigma_1\}$ et la relation $\mathcal{R} = \{\sigma_1\sigma_1 \longrightarrow \epsilon\}$ où ϵ est le mot vide.

On a $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} = \left\{[\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, [\sigma_1]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}\right\}$ où $[\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = \{\sigma_1^n,\ n \text{ est pair}\}, [\sigma_1]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} = \{\sigma_1^n,\ n \text{ est impair}\}$.

La table de Cayley de groue $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est définie comme suit :

$\cdot$	$[\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$	$[\sigma_1]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$
$[\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$	$[\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$	$[\sigma_1]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$
$[\sigma_1]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$	$[\sigma_1]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$	$[\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$

qui est isomorphe au groupe $(\mathbb{Z}/2\mathbb{Z}, +)$.

4.3 Présentation de quelques groupes par générateurs et relations

Soient G un groupe et X une partie de G. On appelle sous groupe engendré par X, et on note $\langle X\rangle$, le plus petit (pour la relation d'inclusion) sous groupe de G contenant X. Notons que,

$$\langle X\rangle = \left\{x_1...x_n, n \in \mathbb{N}^*, x_i \in X \text{ ou } x_i^{-1} \in X, \forall 1 \leq i \leq n\right\}.$$

Si $\langle X\rangle = G$, on dit que X est une partie génératrice de G ou que X engendre G.
En fait remarquer que, si X est une partie génératrice d'un groupe G, tout élément g de G s'écrit $g = x_1...x_p$, avec $x_i \in X$ ou $x_i^{-1} \in X$. Mais cette écriture n'est pas unique. Dans cette section, on montre que pour tout ensemble X, il existe un groupe $L(X)$ dans lequel tout élément s'écrit de manière unique en fonction des générateurs $x_i \in X$. C'est le groupe libre de base X. Ce groupe est d'une grande importance, car on verra que tout groupe est isomorphe à un quotient d'un tel groupe. De plus, cela conduit à la notion de groupes présentés par générateurs et relations, qui sont des groupes dans lequels les écritures des éléments en fonction des générateurs peuvent être simplifiées à l'aide des relations entre ces générateurs.

Définition 4.3.1

Soient G un groupe et X une partie de G. Le groupe G est dit libre de base X si tout élément g de G s'écrit de maniére unique

$$g = x_{i_1}^{n_1} x_{i_2}^{n_2} ... x_{i_k}^{n_k}$$

avec $k, i_1, ..., i_k \in \mathbb{N}, n_1, ..., n_k \in \mathbb{Z}, x_{i_i}, ..., x_{i_k} \in X$, tels que $x_{i_j} \neq x_{i_{j+1}}$, pour
$j \in \{1, ..., k-1\}$. Si $k = 0$, on pose $g = 1_G$. On dit alors que X est une famille génératrice libre de G, ou encore que X est une base de G.

• Un groupe G est dit libre s'il possède une base.

• Si le groupe G possède une base finie, il est dit libre de type fini.

Exemple 4.3.2

Le groupe $(\mathbb{Z}, +)$ est un groupe libre de base $\{1\}$.

Théorème 4.3.3

Pour Tout ensemble X, il existe un groupe libre $L(X)$ de base X.

Définition 4.3.4

On appelle mot en $X \cup X^{-1}$ toute suite finie d'élements de $X \cup X^{-1}$

$$u = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} ... x_{i_n}^{\epsilon_n} \text{ où } \epsilon_i \in \{-1, 1\}, i \in \{1, ..., n\}.$$

• Dans l'écriture ci-dessus, l'entier n est la longueur du mot u, qu'on notera $|u|$.

• Par convention, il n'existe qu'un seul mot de longueur 0, qu'on notera ϵ. C'est le mot qui correspond à la suite vide de $X \cup X^{-1}$.

• Deux mots $x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} ... x_{i_n}^{\epsilon_n}$ et $x_{j_1}^{\tau_1} x_{j_2}^{\tau_2} ... x_{j_k}^{\tau_k}$ sont des mots égaux si $n = k$ et $\forall p, 1 \leq p \leq n, i_p = j_p$ et $\epsilon_p = \tau_p$.

• On note $\mathcal{M}(\mathcal{X})$ l'ensemble des mots en $X \cup X^{-1}$.

Remarque 4.3.5

Posons $X = \{x_i\}_{i \in I}$ et considérons X^{-1} un ensemble équipotent à X, dont on notera les éléments $x_i^{-1}, i \in I$. Il est important de noter qu'il s'agit là seulement d'une notation, qui sera commode dans la suite. Les éléments $x_i^{-1}, i \in I$ ne sont pas les inverses des x_i puisque, pour l'instant X et X^{-1} ne sont que des ensembles sans aucune structure algébrique. On aurait pu noter cet ensemble équipotent à X par Y et ses éléments par $y_i, i \in I$, mais, dans la suite, l'écriture des éléments en aurait été compliquée.

Exemple 4.3.6

Soit $X = \{\alpha, \beta, \gamma\}$, les suites $\alpha^{-1}\beta\alpha\beta^{-1}\gamma\alpha\gamma, \alpha\gamma^{-1}\beta\alpha^{-1}\beta\alpha^{-1}$ sont des mots de l'alphabet $X \cup X^{-1}$.

Définition 4.3.7

Soit $\mathcal{M}(\mathcal{X})$ l'ensemble des mots en $X \cup X^{-1}$, on définit sur $\mathcal{M}(\mathcal{X})$ un produit (loi de composition interne) par juxtaposition des mots. plus précisément, si $u = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} ... x_{i_n}^{\epsilon_n}$ et $v = x_{j_1}^{\tau_1} x_{j_2}^{\tau_2} ... x_{j_k}^{\tau_k}$ sont deux mots, alors $uv = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} ... x_{i_n}^{\epsilon_n} x_{j_1}^{\tau_1} x_{j_2}^{\tau_2} ... x_{j_k}^{\tau_k}$.

Remarque 4.3.8

On remarque que le produit qu'on défini sur $\mathcal{M}(\mathcal{X})$ est associative et admet le mot vide ϵ comme élément neutre ($\forall u \in \mathcal{M}(\mathcal{X}) : u\epsilon = \epsilon u = u$), mais que $\mathcal{M}(\mathcal{X})$ n'est pas un groupe car tout élément autre que ϵ ne peut avoir d'inverse. En effet, pour tous u et v dans $\mathcal{M}(\mathcal{X})$, on a $|uv| = |u| + |v|$, donc si u ou v est différent de ϵ, alors $|uv| > 0$ et $uv \neq \epsilon$. Pour cela, on peut définit sur $\mathcal{M}(\mathcal{X})$ une relation d'équivalence $\equiv$ telle que $\mathcal{M}(\mathcal{X})/\equiv$ soit un groupe pour le produit induit par celui de $\mathcal{M}(\mathcal{X})$.

Définition 4.3.9

Deux mots u et v de $\mathcal{M}(\mathcal{X})$ sont adjacents s'il existe $m_1, m_2 \in \mathcal{M}(\mathcal{X})$ et $a \in X \cup X^{-1}$ tels que : $u = m_1 m_2$ et $v = m_1 a a^{-1} m_2$ ou $u = m_1 a a^{-1} m_2$ et $v = m_1 m_2$,
avec la convention $(a^{-1})^{-1} = a$, pour tout $a \in X \cup X^{-1}$.
Si u et v sont deux mots adjacents, on écrira $u\mathcal{A}v$.

Définition 4.3.10

On définit la relation $\equiv$ sur $\mathcal{M}(\mathcal{X})$ par :

$$(u \equiv v) \Longleftrightarrow (\exists t_1, ..., t_n \in \mathcal{M}(\mathcal{X}) \text{ tels que } u = t_1, v = t_n \text{ et } t_i \mathcal{A} t_{i+1}, i = 1, ..., n-1).$$

Proposition 4.3.11

1. *La relation $\equiv$ est une relation d'équivalence.*
2. *La relation $\equiv$ est compatible avec la loi interne de $M(\mathcal{X})$.*
3. *L'ensemble $M(\mathcal{X})/\equiv$ est un groupe pour la loi induite par celle de $M(\mathcal{X})$.*

Notation 4.3.12

Pour tout u de $\mathcal{M}(\mathcal{X})$, on notera $[u]$ sa classe dans $\mathcal{M}(\mathcal{X})/\equiv$.

Démonstration

1. Pour tout u de $\mathcal{M}(\mathcal{X})$ on a $u \equiv u$, il suffit de prendre $n = 1, t_1 = u$, et on a la relation $\equiv$ est bien réflexive.

La relation d'adjacence étant symétrique, on en déduit qu'il est de même pour la relation $\equiv$. Soient $u, v, w \in \mathcal{M}(\mathcal{X})$ tels que$u \equiv v$ et $v \equiv w$, on a
$(u \equiv v) \Longleftrightarrow (\exists t_1, ..., t_n \in \mathcal{M}(\mathcal{X}) \text{ tels que } u = t_1, v = t_n \text{ et } t_i \mathcal{A} t_{i+1}, i = 1, ..., n-1)$ et
$(v \equiv w) \Longleftrightarrow (\exists t'_1, ..., t'_p \in \mathcal{M}(\mathcal{X}) \text{ tels que } v = t'_1, w = t'_p \text{ et } t'_j \mathcal{A} t'_{j+1}, j = 1, ..., p-1)$.
Donc $(u = t_1)\mathcal{A}...\mathcal{A}(t_n = v = t'_1 = t_{n+1})...\mathcal{A}t_{n+p} = w$. D'où $u \equiv w$ et la relation $\equiv$ est transitive.

2. Soient $u, v, w \in \mathcal{M}(\mathcal{X})$, remarquons que $u\mathcal{A}v$ implique que $uw\mathcal{A}vw$. En effet,

• Si $u = m_1 m_2$ et $v = m_1 a a^{-1} m_2$, alors $uw = m_1 (m_2 w)$ et $vw = m_1 a a^{-1} (m_2 w)$. Et par conséquent,

• Si $(u = t_1)\mathcal{A}...\mathcal{A}(t_n = v)$, alors $(uw = t_1 w)\mathcal{A}...\mathcal{A}(t_n w = vw)$, ce qui prouve que la relation $\equiv$ est compatible à droite avec la loi de $\mathcal{M}(\mathcal{X})$. Un raisonnement analogue montre la compatibilité à gauche.

3. Pour montrer que $\mathcal{M}(\mathcal{X})/\equiv$ est un groupe, il suffit donc de prouver que tout élément $[u]$ admet un élément symétrique. Considéroons d'abord le cas où $u \in X \cup X^{-1}$, il est clair que $uu^{-1} \equiv \epsilon$, car en prenant $t_1 = t_2 = \epsilon$,

on a $uu^{-1} = \epsilon u u^{-1} \epsilon$ et $\epsilon = \epsilon\epsilon$, d'où $uu^{-1}\mathcal{A}\epsilon$. De la même manière, $u^{-1}u \equiv \epsilon$. On en déduit donc que

$$\forall u \in X \cup X^{-1} : [uu^{-1}] = [u^{-1}u] = [\epsilon] \text{ ce qui équivaut à dire } \forall u \in X \cup X^{-1} : [u]^{-1} = [u^{-1}].$$

De plus la projection canonique $p : \mathcal{M}(\mathcal{X}) \longrightarrow \mathcal{M}(\mathcal{X})/\equiv, u \longmapsto [u]$ vérifie

$$\forall u, v \in \mathcal{M}(\mathcal{X}) : p(uv) = [uv] = [u][v] = p(u)\,p(v).$$

Donc pour tout $u = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} ... x_{i_n}^{\epsilon_n}$ où $\epsilon_i \in \{-1, 1\}, i \in \{1, ..., n\}$, $[u]$ est symétrisable et a pour symétrie

$[u]^{-1} = \left[x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} ... x_{i_n}^{\epsilon_n}\right]^{-1} = \left[x_{i_n}^{\epsilon_n}\right]^{-1} ... \left[x_{i_1}^{\epsilon_1}\right]^{-1} = \left[x_{i_n}^{-\epsilon_n}\right] ... \left[x_{i_1}^{-\epsilon_1}\right] = \left[x_{i_n}^{-\epsilon_n} ... x_{i_1}^{-\epsilon_1}\right]$. □

Remarque 4.3.13

On démontre que le groupe libre $L(X)$ cherché dans le théorème 4.3.3 est isomorphe à $\mathcal{M}(\mathcal{X})/\equiv$.

Définition 4.3.14

Un mot u de $\mathcal{M}(\mathcal{X})$ est réduit si $u = \epsilon$ ou $u = x_1 ... x_n$, avec $x_i \in X \cup X^{-1}$ tels que $x_{i+1} \neq x_i$, $i = 1, ..., n-1$.

Proposition 4.3.15

1. *Chaque classe d'équivalence de $M(\mathcal{X})$ pour la relation $\equiv$ contient un mot réduit et un seul.*

2. *Si deux mots sont adjacents, alors leurs formes réduites sont égales.*

3. *Deux mots équivalents et réduits sont égaux.*

Démonstration voir [19].

Théorème 4.3.16 (propriété universelle du groupe libre)

Soient G un groupe, X une partie génératrice de G et $i : X \longrightarrow G$ l'injection canonique. Le groupe G est libre de base X si, et seulement si, pour tout groupe G' et pour toute application $\mu : X \longrightarrow G'$, il existe un unique morphisme de groupes $f : G \longrightarrow G'$ tel que $f \circ i = \mu$.

Démonstration

Pour l'implication direct : supposons que $G = L(X)$, tout élément g de $L(X)$ s'écrit de manière unique

$g = x_{i_1}^{n_1} x_{i_2}^{n_2} ... x_{i_k}^{n_k}$, on pose, $f(g) = \mu(x_{i_1})^{n_1} ... \mu(x_{i_k})^{n_k}$ et $f(1_G) = 1_{G'}$.

Il est clair qu'on définit ainsi un morphisme de groupes $f : L(X) \longrightarrow G'$ vérifiant $foi = \mu$. De plus, si f' est un autre morphisme de groupes vérifiant $f'oi = \mu$, pour tout $g \in G = L(X)$, on a $f(g) = f'(g)$, d'où l'unicité.

Réciproquement : Supposons que toute application de X vers un groupe G' se prolonge en unique morphisme de G vers G'. On applique alors cet énoncé avec le couple $(L(X), j)$ où $j : X \longrightarrow L(X)$ est l'injection canonique. Il existe donc un unique morphisme

$\varphi : G \longrightarrow L(X)$ tel que $\varphi \circ i = j$. Comme, $L(X)$ étant libre sur X, on sait que l'injection canonique de X vers G se prolonge en un unique morphisme $\psi : L(X) \longrightarrow G$ tel que $\psi \circ j = i$. En notant $\varphi_{|X}$ et $\psi_{|X}$ les restrictions de φ et ψ à X, d'où $\psi \circ \varphi = Id_{L(X)}$, ce qui prouve que φ est injectif, puis $\varphi \circ \psi = Id_G$, ce qui prouve que φ est surjectif. Par conséquent les groupes G et $L(X)$ sont isomorphes. On en déduit que G est lui aussi libre sur X. □

Théorème 4.3.17

Tout groupe est isomorphe à un quotient d'un groupe libre.

Démonstration

Soient G un groupe, X une partie génératrice de G et $i : X \longrightarrow G$ l'injection canonique. D'après le théorème 4.3.16, il existe un morphisme de groupes $f : L(X) \longrightarrow G$ tel que $f_{|X} = id_X$. On a donc $G = \langle X \rangle = \langle f(X) \rangle$ et f est surjective. Le premier théorème d'isomorphisme permet alors d'affirmer que $G = \langle X \rangle = \langle f(X) \rangle$ est isomorphe à $L(X)/K\text{erf}$. □

Définition 4.3.18

Soit G un groupe engendré par un ensemble d'éléments $X = \{x_i\}_{i\in I}$, ces éléments vérifiant un ensemble de relations $\mathcal{R} = \{r_k = 1_G\}_{k\in K}$. On dit que $\langle X/R\rangle$ est une présentation de G par générateurs et relations si G est isomorphe au groupe quotient $L(X)/\langle R\rangle$, où $\langle R\rangle$ est le sous groupe normal du groupe libre $L(X)$, engendré par $\{r_k\}_{k\in K}$.

Remarque 4.3.19

Soit $G = \langle X/R\rangle$. Pour définir un morphisme surjectif de groupes $f : L(X) \longrightarrow G$, il suffit de définir $f(x)$ pour $x \in X$. De plus si $\langle R\rangle$ le sous groupe normal du groupe libre $L(X)$ engendré par R est égale à K erf, alors $G \simeq L(X)/\langle R\rangle$.

Exemples 4.3.20

1. On a $\langle \{x\}/\emptyset\rangle$ est une présentation de groupe monogène infini $(\mathbb{Z}, +)$.

2. Pour $n \in \mathbb{N} - \{0\}$, $\langle \{x\}/x^n\rangle$ est une présentation de groupe cyclique d'ordre n $(\mathbb{Z}/n\mathbb{Z}, \oplus)$.

3. $\langle \{x, y\}/x^n, y^2, xyxy\rangle$ avec $x \neq y$ et $n \geq 2$, est une présentation de groupe diédral D_n, où D_n est le groupe d'isométries du polygône réguliers à n côtés.

4.4 Etude d'un système de cryptage basé sur le problème du mot dans un monoïde libre

Dans cette section, on s'intéresse au protocole ATS-monoïde (proposé par P. J. Abisha, D. G. Thomas et K. G. Subramanian), l'idée de ce protocole est de transformer un semi-système de Thue $S_1 = (\Sigma, \mathcal{R})$ pour lequel le problème du mot est indécidable en un système de Thue $S_2 = (\Delta, \mathcal{R}_\theta)$ où $\theta \subseteq \Delta \times \Delta$ pour lequel le problème du mot est décidable en un temps linéaire. Plus précisément, on donne des attaques contre ATS-monoïde dans des cas spécifiques et quelques exemples sur ces cas

4.4.1 Définitions et notations

Définition 4.4.1.1

Dans [1], P. J. Abisha, D. G. Thomas et K. G. Subramanian, ont utilisé le thèorème de 3.2.4 R. Cori et D. Perrin pour construire le protocole ATS-monoïde. L'idée est de transformer un système de Thue $S_1 = (\Sigma, \mathcal{R})$ pour lequel le problème du mot est indécidable en un système de Thue $S_2 = (\Delta, \mathcal{R}_\theta)$ avec $\theta \subseteq \Delta \times \Delta$ et $\mathcal{R}_\theta = \{ab \longrightarrow ba : (a, b) \in \theta\}$ pour lequel le problème du mot est décidable en temps linéaire.

Clef Publique : Un système de Thue $S_1 = (\Sigma, \mathcal{R})$ et deux mots w_0, w_1 de Σ^*. Donc $(\Sigma, \mathcal{R}, w_0, w_1)$ constituent une clef publique.

Clef Secrète : Un système de Thue $S_2 = (\Delta, \mathcal{R}_\theta)$ où l'alphabet Δ de taille plus petite que Σ, un morphisme h de Σ^* vers Δ^*, vérifiant pour tout $r \longrightarrow s \in \mathcal{R}$:

$$\begin{cases} (h(r), h(s)) \in \{(ab, ba), (ba, ab)\}, \text{ pour une paire } (a, b) \in \theta, \\ \text{ou bien } h(r) = h(s). \end{cases}$$

Par conséquent, on a pour tout $u, v \in \Sigma^*, u \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} v \Rightarrow h(u) \overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}} h(v) \qquad (C)$.

ou par contraposition si $h(u)$ et $h(v)$ ne sont pas équivalents modulo $\overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}}$, alors u et v ne sont pas équivalents modulo $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$.

Et, nous avons aussi deux mots x_0, x_1 de Δ^* vérifiant $x_0 \overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}} h(w_0), x_1 \overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}} h(w_1)$ avec $h(w_0)$ et $h(w_1)$ ne sont pas équivalent modulo $\overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}}$. Le triplet $(\Delta, \mathcal{R}_\theta, h \in Hom(\Sigma^*, \Delta^*))$ constituent une clef secrète.

Chiffrement : Pour chiffrer un bit $b \in \{0,1\}$, Bob choisit un mot c de Σ^* dans la classe d'équivalence de w_b modulo $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$, i. e, $c \in [w_b]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ où $[w_b]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ désigne la classe d'équivalence w_b modulo $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ et l'envoi à Alice.

Déchiffrement : A la réception d'un mot c de Σ^*, Alice calcule $h(c) \in \Delta^*$. Comme $c \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w_b$ et d'après la conséquence (C) pour tous $u, v \in \Sigma^*, u \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} v \Rightarrow h(u) \overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}} h(v)$ on a $h(c) \overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}} h(w_b)$, par exemple si $h(c) \overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}} x_0$, alors le message déchiffré est 0.

Exemple 4.4.1.2:

Clef Publique :

$\Sigma = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$,

$\mathcal{R} = \{(\sigma_2\sigma_3, \sigma_3\sigma_2), (\sigma_2\sigma_4, \sigma_4\sigma_2), (\sigma_1\sigma_3, \sigma_3\sigma_1)\}$,

$w_0 = \sigma_1\sigma_2\sigma_4\sigma_3\sigma_1\sigma_2\sigma_3\sigma_4$,

$w_1 = \sigma_2\sigma_4\sigma_3\sigma_4\sigma_2\sigma_1$.

Clef Secrète :

$\Delta = \{a, b, c\}, \theta = \{(a, b), (a, c)\}$ et $h : \Sigma^* \longrightarrow \Delta^*$ est défini par :

$$h(\sigma_1) = \epsilon, h(\sigma_2) = a, h(\sigma_3) = b, h(\sigma_4) = c.$$

Nous avons bien $\mathcal{R}_\theta = \{ab \longrightarrow ba, ac \longrightarrow ca\}$, $h(w_0) = x_0 = acbabc$ et $h(w_1) = x_1 = acbca$.

Maintenant on vérifie les conditions suivantes :

1. $h(w_0)$ et $h(w_0)$ ne sont pas équivalent modulo $\overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}}$.
2. pour tout $r \longrightarrow s \in \mathcal{R}$:

$$\begin{cases} (h(r), h(s)) \in \{(ab, ba), (ba, ab)\}, \text{ pour une paire } (a, b) \in \theta, \\ \text{ou bien } h(r) = h(s). \end{cases}.$$

Pour la condition 1. Il suffit d'utilisé le thèorème de R. Cori et D. Perrin.

On a $P_{\{b\}}(h(w_0)) = P_{\{b\}}(acbabc) = bb$ et $P_{\{b\}}(h(w_1)) = P_{\{b\}}(acbca) = b$, donc $h(w_0)$ et $h(w_1)$ ne sont pas équivalent modulo $\overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}}$.

Pour la condition 2. On a $\mathcal{R} = \{(\sigma_2\sigma_3, \sigma_3\sigma_2), (\sigma_2\sigma_4, \sigma_4\sigma_2), (\sigma_1\sigma_3, \sigma_3\sigma_1)\}$ donc

$(h(\sigma_2\sigma_3), h(\sigma_3\sigma_2)) = (ab, ba) \in T_\theta, (h(\sigma_2\sigma_4), h(\sigma_4\sigma_2)) = (ac, ca) \in T_\theta,$

$(h(\sigma_1\sigma_3), h(\sigma_3\sigma_1)) = (b, b)$ (ona $h(\sigma_1\sigma_3) = h(\sigma_3\sigma_1)$.

Par conséquent, on a pour tout $u, v \in \Sigma^*, u \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} v \Rightarrow h(u) \overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}} h(v)$.

Chiffrement : Par exemple pour chiffrer le 0, Bob choisit un mot c de $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}^*$ dans la classe d'équivalence de w_0 modulo $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$, i. e, $c \in [w_0]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ où $[w_0]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ désigne la classe de w_0 modulo $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est alors envoyé à Alice.
On a $w_0 = \sigma_1\sigma_2\sigma_4\sigma_3\sigma_1\sigma_2\sigma_3\sigma_4 \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \sigma_1\sigma_4\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3\sigma_4 \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \sigma_1\sigma_4\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3\sigma_4$.
On choisit $c = \sigma_1\sigma_4\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3\sigma_4$.
Déchiffrement : A réception d'un mot c de $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}^*$,
Alice calcule $h(c) = h(\sigma_1\sigma_4\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3\sigma_4) = cbaabc \in \{a, b, c\}^*$. En utilisant alors le théorème de R. Cori et D. Perrin, on vérifie que $h(c) \overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}} h(w_0)$. On a
$P_{\{a\}}(h(c)) = P_{\{a\}}(h(w_0)) = aa, P_{\{b\}}(h(c)) = P_{\{b\}}(h(w_0)) = bb, P_{\{c\}}(h(c)) = P_{\{c\}}(h(w_0)) = cc$. Donc pour tout σ de $\{a, b, c\}$, $P_{\{\sigma\}}(h(c)) = P_{\{\sigma\}}(h(w_0))$. De plus on vérifie que $P_{\{\sigma,\mu\}}(h(c)) = P_{\{\sigma,\mu\}}(h(w_0))$, pour tout $(\sigma, \mu) \notin \theta$. Le complémentaire de θ par rapport $\Delta \times \Delta$ notée $C_{\Delta\times\Delta}\ \theta$ est $\{(a,a), (b,a), (b,b), (b,c), (c,a), (c,b), (c,c)\}$,
on $P_{\{b,c\}}(h(c)) = P_{\{b,c\}}(h(w_0)) = cbbc$. Finalement $h(c) \overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}} h(w_0) = x_0$ et le mot déchiffré est 0.

4.4.2 Sécurité de ATS-monoïde

Une attaque contre ATS-monoïde ne permette pas de trouver exactement la clef secréte. Nous obtiendrons plutôt une clef qui lui est équivalente dans le sens suivant :
Nous dirons que $(\Delta', \mathcal{R}_{\theta'}, h' \in H(\Sigma^*, \Delta'^*))$ est une clef équivalente à la clef secrète $(\Delta, \mathcal{R}_\theta, h \in Hom(\Sigma^*, \Delta^*))$ si tout message chiffré avec la clef publique $(\Sigma, \mathcal{R}, w_0, w_1)$ peut être décrypter avec $(\Delta', \mathcal{R}_{\theta'}, h' \in Hom(\Sigma^*, \Delta'^*))$. C'est le cas par exemple si $(\Delta', \mathcal{R}_{\theta'}, h' \in Hom(\Sigma^*, \Delta'^*))$ vérifie les trois conditions suivantes:
1. h' est non trivial et $|\Delta'| \leq |\Sigma|$.
2. $\forall r \longrightarrow s \in \mathcal{R}$, $\begin{cases} (h'(r), h'(s)) \in \{(ab, ba), (ba, ab)\}, \text{ pour une paire } (a, b) \in \theta', \\ \text{ou bien } h'(r) = h'(s). \end{cases}$
3. $h'(w_0)$ et $h'(w_0)$ ne sont pas équivalent modulo $\overset{*}{\underset{\mathcal{R}_{\theta'}}{\Longleftrightarrow}}$.
Nous donnons quelques clefs qui sont équivalentes à la clef secrète $(\Delta, \mathcal{R}_\theta, h \in Hom(\Sigma^*, \Delta^*))$.
1. Soient $h(\Sigma) = \{h(\sigma), \sigma \in \Sigma\}$ et $\theta' = \theta \cap h(\Sigma) \times h(\Sigma)$. Alors: $(h(\Sigma), \mathcal{R}_{\theta'}, h \in Hom(\Sigma^*, \Delta^*))$ est une clef équivalente à la clef secrète $(\Delta, \mathcal{R}_\theta, h \in Hom(\Sigma^*, \Delta^*))$.

2. Soient Δ' un alphabet de la même taille que Δ, $i \in Iso\left(\Delta^*, \Delta'^*\right)$ et $i(\theta) = \{(i(a), i(b)), (a,b) \in \theta\}$. Alors $\left(\Delta', \mathcal{R}_{i(\theta)}, i \circ h \in Hom\left(\Sigma^*, \Delta'^*\right)\right)$ est une clef équivalente à la clef secrète $(\Delta, \mathcal{R}_\theta, h \in Hom\left(\Sigma^*, \Delta^*\right))$.

Décrivons maintenant une attaque générale contre ATS-monoïde. Dans le premier temps nous remarquons qu'une clef $(\Delta', \mathcal{R}_{\theta'}, h' \in Hom\left(\Sigma^*, \Delta'^*\right))$ équivalente à la clef secrète $(\Delta, \mathcal{R}_\theta, h \in Hom\left(\Sigma^*, \Delta^*\right))$ est indépendente de l'alphabet Δ, la seule chose qui compte c'est la taille de Δ. D'autre part, nous observons que la relation $\mathcal{R}_{\theta'}$ est facilement déduite de la connaissance de $h' \in Hom\left(\Sigma^*, \Delta'^*\right)$.

Notons que, pour une Clef Publique $(\Sigma, \mathcal{R}, w_0, w_1)$ il existe un algorithme noté Algo-ATS-monoïde qui retourne une clef équivalente à la clé secrète $(\Delta, \mathcal{R}_\theta, h \in Hom\left(\Sigma^*, \Delta^*\right))$ de complexité $|\mathcal{R}| \sum_{i=1}^{i=k} (i+1)^{|\Sigma|}$, avec $k = |\Delta|$.

Algo-ATS-monoïde [30]

Entrée : $(\Sigma, \mathcal{R}, w_0, w_1)$, une clef publique de ATS-monoïde.

Sortie : $(\Delta_i, \mathcal{R}_{\theta_i}, h_i \in H(\Sigma^*, \Delta_i^*))$, une clef équivalente à la clef secrète.

Pour $i, 1 \leq i \leq |\Sigma|$ faire

Soit Δ_i un alphabet quelconque de i lettres

Pour $h_i \in H(\Sigma^*, \Delta_i^*)$ faire

$\theta_i \longleftarrow \emptyset$

Pour $(r, s) \in R$ faire

Calculer $h_i(r)$ et $h_i(s)$

Si $h_i(r) \neq h_i(s)$ alors

Si $h_i(r) = ab$ et $h_i(s) = ba$, pour $a, b \in \Delta_i$ alors

Si $(a, b) \notin \theta_i$ et $(b, a) \notin \theta_i$ alors $\theta_i \longleftarrow \theta_i \cup \{(a, b)\}$

Sinon Choisir un autre morphisme, i.e. retourner à la deuxième boucle Pour

FinSi

Finpour

Si $h_i(w_0)$ et $h_i(w_1)$ ne sont pas équivalents modulo $\overset{*}{\underset{\mathcal{R}_{\theta_i}}{\Longleftrightarrow}}$ alors Retourner $(\Delta_i, \mathcal{R}_{\theta_i}, h_i)$

Finpour

Finpour

4.3.3 Quelques attaques contre ATS-monoïde

Dans cette section on donne quelques attaques contre ATS-monoïde c'est-à-dire dans chaque cas nous retournons une clef équivalente à la clef secrète de ce protocole.

Corollaire 4.4.3.1 [17]

Soit $(\Sigma, \mathcal{R}, w_0, w_1)$ *une clef publique de protocole ATS-monoïde.*

Si $\forall r \longrightarrow s \in R, |r| = |s|$, *alors* $(\Delta_1 = \{a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ *où pour tout* $\sigma \in \Sigma, h_1(\sigma) = a$, *est une clef équivalente à la clef secréte.*

Démonstration

La clef $(\Delta_1 = \{a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ où pour tout $\sigma \in \Sigma, h_1(\sigma) = a$, vérifiée les trois conditions suivantes :

1. le morphisme h_1 est non trivial car pour tout $\sigma \in \Sigma, h_1(\sigma) = a \neq \epsilon$.

2. $\forall r \longrightarrow s \in \mathcal{R}, h_1(r) = h_1(s) = (a)^{|r|} = (a)^{|s|}$.

3. Comme $\mathcal{R}_\theta = \emptyset$, alors $\overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}} = id_{\Delta_1^*}$ et par conséquent $h_1(w_0)$ et $h_1(w_1)$ ne sont pas équivalent modulo $\overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}}$ puisque $h_1(w_0) \neq h_1(w_1)$. Donc $(\Delta_1 = \{a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ est une clef équivalente à la clef secréte.

Corollaire 4.4.3.2 [17]

Soit $(\Sigma, \mathcal{R}, w_0, w_1)$ une clef publique de protocole ATS-monoïde.

S'il existe $r \longrightarrow s \in R, |r| \neq |s|$, alors $(\Delta_1 = \{a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$

où $h_1(\Sigma) = \{a, \epsilon\}$, est une clef équivalente à la clef secréte.

Exemple 4.4.3.3

Clef Publique**:**

$\Sigma = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$,

$\mathcal{R} = \{(\sigma_1\sigma_3, \sigma_3\sigma_1), (\sigma_1\sigma_4, \sigma_4\sigma_1), (\sigma_2\sigma_3, \sigma_3\sigma_2), (\sigma_2\sigma_4, \sigma_4\sigma_2), (\sigma_5\sigma_3\sigma_1, \sigma_3\sigma_5)\}$,

$w_0 = \sigma_4\sigma_2\sigma_4\sigma_3\sigma_4\sigma_2\sigma_3\sigma_4, w_1 = \sigma_2\sigma_4\sigma_3\sigma_4\sigma_2\sigma_1$.

La clef $(\Delta_1 = \{a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ où $h_1(\sigma_1) = h_1(\sigma_3) = \epsilon$,

$h_1(\sigma_2) = h_1(\sigma_4) = h_1(\sigma_5) = a$ est vérifiée les conditions suivantes :

1. le morphisme h_1 est non trivial.

2. $\forall r \longrightarrow s \in \mathcal{R}, h_1(r) = h_1(s)$.

3. On a $h_1(w_0) = a^6$ et $h_1(w_1) = a^4$ et comme $\overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}} = id_{\Delta_1^*}$, alors $h_1(w_0)$ et $h_1(w_1)$ ne sont pas équivalent modulo $\overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}}$.

. Donc $(\Delta_1 = \{a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ est une clef équivalente à la clef secréte.

Remarque 4.4.3.4

Dans le Corollaire 4.2.3.2 Il existe des cas où le morphisme h_1 est trivial.

Corollaire 4.4.3.5 [17]

Soit $(\Sigma, \mathcal{R}, w_0, w_1)$ une clef publique de protocole ATS-monoïde.

S'il existe une lettre σ_k de l'alphabet Σ telle que pour tout $r \longrightarrow s \in R, |r|_{\sigma_k} = |s|_{\sigma_k} = 0$, alors $(\Delta_1 = \{a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ où pour tout $\sigma \in \Sigma$ avec $\sigma \neq \sigma_k, h_1(\sigma) = \epsilon$ et $h_1(\sigma_k) = a$, est une clef équivalente à la clef secréte.

Démonstration

La clef $(\Delta_1 = \{a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ est vérifié les trois conditions suivantes:

1. le morphisme h_1 est non trivial car $h_1(\sigma_k) = a \neq \epsilon$.

2. $\forall r \longrightarrow s \in \mathcal{R}, h_1(R) = h_1(s) = \epsilon$.

3. Comme $\mathcal{R}_\theta = \emptyset$, alors $\overset{*}{\underset{\mathcal{R}_\theta}{\Longleftrightarrow}} = id_{\Delta_1^*}$, donc il doit vérifiée que $h_1(w_0) \neq h_1(w_1)$.

Remarque 4.4.3.6

Dans le Corollaire 4.2.3.5 Il existe des cas où le morphisme h_1 vérifie l'égalité $h_1(w_0) = h_1(w_1)$.

4.5 Langage engendré par un semi-système de réécriture

Le terme langage désigne d'une part les langues naturelles sous leur forme parlée et écrite, d'autre part les systèmes de notations, les formalismes, utilisés dans diverses sciences comme les mathématiques, la logique, la chimie, et en particulier en informatique (les langages de programmations par exemple). Tout langage comprend un ensemble d'objets élémentaires, que l'on peut composer pour constituer des unités qui ont un sens. La composition des objets élémentaires est le plus souvent un simple enchainement (une concaténation). La notion de langage formel est à distinguer de celle de langage de programmation, même s'il existe des liens entre les deux, les mots d'un langage formel sont étudiés indépendamment de toute sémantique. Les congruences constituent un procédé de langages formels au même titre que les automates. Nous allons présenter ici les langages engendrés par des semi-systèmes de réécriture.

Définition 4.5.1 [7, 28]

Soit (Σ, R) un semi-système de réécriture, un langage L sur Σ est congruentiel s'il existe un mot w sur Σ tel que $L = [w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$.

Exemple 4.5.2

Soient $\Sigma = \{\alpha, \beta\}$ et $R = \{(\alpha\beta, \epsilon), (\beta\alpha, \epsilon)\}$, le langage $L = \{w \in \{\alpha, \beta\}^* : |w| \text{ est paire}\}$ est congruentiel puisque $L = [\epsilon]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, par contre le langage $L' = \{w \in \{\alpha, \beta\}^* : w = \widetilde{w}\}$ où $\widetilde{w}$ est l'image miroire de w, n'est pas congruentiel.

Proposition 4.5.3 [7]

Soient $(\Sigma, \mathcal{R})$ *un semi-système de réécriture et* w un mot quelconque de Σ^*, on a pour tout u, v, f, f' de Σ^*,

$$\text{si } ufv, f, f' \in [w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}, \text{ alors } uf'v \in [w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}.$$

Démonstration

On a $f, f' \in [w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, i.e, $f \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} f'$, commme $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est une congruence, alors $ufv \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} uf'v$, donc $uf'v \in [w]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$. $\square$

Prpposition 4.5.4 [7]

Soient (Σ, R) *un semi-système de réécriture où* $\Sigma = \{\alpha_0, \alpha_1, ..., \alpha_n\}$ *et* $R = \{(\alpha_1\alpha_0...\alpha_n\alpha_0, \alpha_0)\}$. *On a,* $\alpha_0 + \alpha_1 [\alpha_0]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} ...\alpha_n [\alpha_0]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} \subseteq [\alpha_0]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$.

Démonstration

Soit $x \in \alpha_0 + \alpha_1 [\alpha_0]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} ...\alpha_n [\alpha_0]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, on distingue deux cas :

• Si $x = \alpha_0$, on $\alpha_0 \in [\alpha_0]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$.

• Si $x \in \alpha_1 [\alpha_0]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}} ...\alpha_n [\alpha_0]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, alors il existe $u_1, ..., u_n \in [\alpha_0]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ tels que $x = \alpha_1 u_1 ... \alpha_n u_n$.

On a $\forall 1 \leq i \leq n : u_i \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha_0$, donc $\alpha_1 u_1 ... \alpha_n u_n \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha_1\alpha_0 ... \alpha_n\alpha_0$,

et comme $\alpha_1\alpha_0 ... \alpha_n\alpha_0 \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \alpha_0$, alors $x \in [\alpha_0]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$. $\square$

Proposition 4.5.5

Soient (Σ, R) *un semi-système de réécriture et* L *un langage sur* Σ, *on a*

$$\textit{si } L \textit{ est saturé par } \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}, \textit{ alors } \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \subseteq \equiv_L.$$

Démonstration

Le langage L est saturé par $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ i.e, $L = \bigcup [c_i]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, où $c_i \in \Sigma^*$. La congruence syntaxique de L est définie par : $(w \equiv_L w') \Leftrightarrow (\forall x, y \in \Sigma^* : xwy \in L \Leftrightarrow xw'y \in L)$.

On montre que $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} \subseteq \equiv_L$. Soient $w, w' \in \Sigma^*$ tels que $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w'$, on vérifie que $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w'$. Soient $x, y \in \Sigma^*$ tels que $xwy \in L = \bigcup [c_i]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$, donc $\exists i_o \in I : xwy \in [c_{i_o}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ i.e, $xwy \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} c_{i_o}$. Comme $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ est une congruence, alors $w \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} w'$ implique $xwy \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} xw'y$. On a $\left(xwy \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} c_{i_o} \text{ et } xwy \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} xw'y\right)$, d'après la transitivité de $\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$, alors $xw'y \overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}} c_{i_o}$.

Donc $xw'y \in [c_{i_o}]_{\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}}$ i.e, $xw'y \in L$. $\square$

Définition 4.4.6 [14]

Soit $(\Sigma, \mathcal{R})$ *un semi-système de réécriture de mots.* A tout langage Γ sur Σ, on associe le langage : $L(\Gamma, \mathcal{R}) = \left\{ w \in \Sigma^*, \exists \gamma \in \Gamma : \gamma \underset{\mathcal{R}}{\overset{*}{\Rightarrow}} w \right\}$.

Autrement dit, le langage $L(\Gamma, \mathcal{R})$ est l'ensemble des mots w en lesquels se réécrivent les éléments de Γ selon $\underset{\mathcal{R}}{\overset{*}{\Rightarrow}}$.

Exemples 4.4.7

1. Soient $\Sigma_1 = \{\alpha, \beta\}, \mathcal{R}_1 = \{(\alpha\beta, \alpha\alpha\beta\beta), (\beta\alpha, \beta\beta\alpha)\}$ et $\Gamma_1 = \{\alpha\beta, \beta\alpha\}$.
Donc ona, $L(\Gamma_1, \mathcal{R}_1) = \left\{ w \in \Sigma_1^*, \exists \gamma \in \Gamma_1 : \gamma \underset{\mathcal{R}_1}{\overset{+}{\Rightarrow}} w \right\} = \{\alpha^n \beta^n, n > 0\} \cup \{\beta^n \alpha, n > 0\}$.
2. Soient $\Sigma_2 = \{A, B, C\}, \mathcal{R}_2 = \{(A, BA), (A, C)\}$ et $\Gamma_2 = \{A\}$,
Et par conséquent, $L(\Gamma_2, \mathcal{R}_2) = \left\{ w \in \Sigma_2^*, \exists \gamma \in \Gamma_2 : \gamma \underset{\mathcal{R}_2}{\overset{+}{\Rightarrow}} w \right\} = \{B^k C, k \geq 0\} \cup \{B^k A, k \geq 0\}$.

Remarque 4.5.8

Un semi-système de réécriture est un moyen très pratique pour produire des mots, en revanche, il n'est pas très facile à utiliser pour valider l'appartenance d'un mot à un langage. On appelle problème du mot la question de savoir si $w \in L(\Gamma, \mathcal{R})$, le problème du mot est indécidable.

4.6 Les bases de Gröbner et semi-systèmes de rèèctiture de mots

En algèbre appliquée, de nombreux problèmes de modélisation se formulent en terme d'équations polynomiales. L'étude des idéaux de polynômes à plusieurs indéterminées permet de résoudre des systèmes d'équations polynomiales à plusieurs inconnues, grâce à des méthodes algorithmiques. L'ensemble des polynômes à plusieurs indéterminées forme un anneau commutatif, noté $\Bbbk[x_1, ..., x_n]$. Un idéal de $\Bbbk[x_1, ..., x_n]$ est un sous-ensemble de cet anneau, stable pour l'addition et la multiplication. On peut définir des idéaux de $\Bbbk[x_1, ..., x_n]$ à partir d'une famille de polynômes, appelée base de l'idéal. L'idéal correspond alors à l'ensemble des combinaisons de polynômes de la base. cette définition invite au problème suivant : comment savoir si un polynôme donné appartient à l'idéal engendré par une base donnée? **(**Le problème de l'appartenance à un idéal**).** La division euclidienne peut répondre à cette question, par exemple, dans $\mathbb{R}[x]$, soient les trois polynômes $f = x^2 - x, g = x - 1, h = x^3 - 1$. On cherche à savoir si le polynôme h appartient à l'idéal $I = \langle f, g\rangle$. On procède alors à la division de h par f : $x^3 - 1 = f(x + 1) + x - 1$ puis on divise le reste $(x - 1)$ par le polynôme g : $x - 1 = g(x - 1) + 0$. Ainsi, le reste de la division euclidienne de h par f et g est nul. Donc $h \in I = \langle f, g\rangle$. Mais cette méthode n'est pas toujours opérationnelle. En effet, dans $\mathbb{R}[x]$, si $f = x^2 - 1, g = x^2 - x$ et $h = x - 1$, le reste de la division euclidienne de h par f et g est h qui n'est pas nul. Pourtant $h = f - g$ appartient à l'idéal engendré par f et g. Donc la division euclidienne ne permet pas toujours de résoudre le problème de l'appartenance à un idéal. Pour résoude ce probléme, une méthode consiste à trouver, pour un idéal donné, une base qui respecte cette équivalence entre la nullité du reste de la division d'un polynôme par cette base et l'appartenance de ce polynôme à l'idéal. On appellera cette base, base de Gröbner**.** Le mathématicien Buchberger à créé un algorithme qui, pour tout idéal, calcul une base de Gröbner**.** Cet algorithme termine avec succés en un nombre fini d'étape.

Définition 4.6.1

On appelle monôme en les indéterminées $x_1, ..., x_n$ tout produit de la forme $x_1^{\alpha_1}...x_n^{\alpha_n}$, où $\alpha_1, ..., \alpha_n$ sont des entiers de $\mathbb{N}$. On appelle degré total de ce monôme la somme $\alpha_1 + ... + \alpha_n$. On notant $\alpha = (\alpha_1, ..., \alpha_n)$, on pose $x^\alpha = x_1^{\alpha_1}...x_n^{\alpha_n}$. Par convontion, $x^{(0,...,0)} = 1$. On notera $M(x_1, ..., x_n) = \{x^\alpha : \alpha \in \mathbb{N}^n\}$ l'ensemble des monômes en les indéterminées $x_1, ..., x_n$.

Définition 4.6.2

On appelle polynôme en les indéterminées $x_1, ..., x_n$ toute combinaison linéaire (finie) à coefficient dans $\Bbbk$ de monôme en les indéterminées $x_1, ..., x_n$. Un polynôme f s'écrit $f = \sum_{\alpha} a_\alpha x^\alpha$, où la somme est indexée par un nombre fini de n-uplets α et les a_α sont des scalaires de $\Bbbk$.

Le scalaire a_α est appelé coefficient du monôme x^α.

Si $a_\alpha \neq 0$, alors on dit que $a_\alpha x^\alpha$ est un terme de f.

Proposition 4.6.3

L'ensemble des polynômes en les indéterminées $x_1, ..., x_n$ muni de l'addition et la multiplication forme un anneau commutatif noté $\Bbbk[x_1, ..., x_n]$.

Exemple 4.6.4

Soit $f = 5x^3y + yz + 1$ un polynôme de $\mathbb{R}[x, y, z]$, alors $5x^3y$ est un terme de f, x^3y est un monôme, de coefficient 5 et de degré total 4.

Définition 4.5.5

On dit qu'un sous ensemble I de $\Bbbk[x_1, ..., x_n]$ est un idéal si :

• 0 est élément de I,

• Pour tous polynômes f_1 et f_2 de I, $f_1 + f_2$ est un polynôme de I.

• Pour tout polynôme f de I, pour tout polynôme g de $\Bbbk[x_1, ..., x_n]$, fg est un polynôme de I.

Définition 4.6.6

Soient $f_1, ..., f_s$ des polynômes de $\Bbbk[x_1, ..., x_n]$, l'ensemble

$$\langle f_1, ..., f_s \rangle = \left\{ \sum_{i=1}^{i=s} h_i f_i : 1 \leq i \leq s \text{ et } h_i \in \Bbbk[x_1, ..., x_n] \right\}$$

est appelé idéal engendré par les polynômes $f_1, ..., f_s$.

Définition 4.6.7

On dit qu'un idéal I de $\Bbbk[x_1, ..., x_n]$ est finiment engendré ou de type fini, s'il existe un ensemble fini $\{f_1, ..., f_s\}$ de polynômes de $\Bbbk[x_1, ..., x_n]$ tels que $I = \langle f_1, ..., f_s \rangle$.

Définition 4.6.8

Un ordre monomial sur $M(x_1, ..., x_n)$ est une relation $\preceq$ sur $M(x_1, ..., x_n)$ telle que :

• $\preceq$ est un ordre total,

• Pour tous monômes $x^\alpha, x^\beta, x^\gamma$ de $M(x_1, ..., x_n)$, si $x^\alpha \preceq x^\beta$, alors $x^\alpha x^\gamma \preceq x^\beta x^\gamma$,

• Pour tout monôme x^α de $M(x_1, ..., x_n)$ distinct de 1, $1 \preceq x^\alpha$.

Exemple 4.6.9

On définit d'abord un ordre sur l'ensemble des indéterminées, généralement l'ordre alphabétique défini par $x_n \leq ... \leq x_1$. On définit l'ordre lexicographique en posant $x^\alpha \preceq_{Lex} x^\beta$, si le premier coefficient non nul du n-uplet $\beta - \alpha$ est positif. Par exemple, dans $M(x, y, z)$, $x^2yz^3 \preceq_{Lex} x^2y^5z$ puisque $(2, 5, 1) - (2, 1, 3) = (0, 4, -2)$ et $4 > 0$. L'ordre lexicographique est un ordre monomial.

Exemple 4.6.10

On définit sur $M(x_1, ..., x_n)$ l'ordre lexicographique par degré noté $\preceq_{Grlex}$ en posant $x^\alpha \preceq_{Grlex} x^\beta$ si

$$\left(\sum_{i=1}^{i=n} \alpha_i < \sum_{i=1}^{i=n} \beta_i\right) \text{ ou } \left(\sum_{i=1}^{i=n} \alpha_i = \sum_{i=1}^{i=n} \beta_i \text{ et } x^\alpha \preceq_{Lex} x^\beta\right).$$

Ainsi, dans $M(x, y, z)$, $x^2yz^3 \preceq_{Lex} x^2y^5z^3$ puisque $2 + 1 + 3 < 2 + 5 + 3$. L'ordre lexicographique par degré est aussi un ordre monomial.

Proposition 4.6.11

Soit $\preceq$ un ordre monomial sur $M(x_1, ..., x_n)$. Soient x^α, x^β deux monômes de $M(x_1, ..., x_n)$. On a, si x^α divise x^β, alors $x^\alpha \preceq x^\beta$.

Démonstration

En effet, si x^α divise x^β, alors il existe un monôme x^γ de $M(x_1, ..., x_n)$ tel que $x^\beta = x^\alpha x^\gamma$. Or, par définition, $1 \preceq x^\gamma$ d'où $x^\alpha \cdot 1 \preceq x^\alpha \cdot x^\gamma$. Donc $x^\alpha \preceq x^\beta$. □

Définition 4.6.12

Soit $\preceq$ un ordre monomial sur $M(x_1, ..., x_n)$. Soit f un polynôme de $\Bbbk[x_1, ..., x_n]$. Le polynôme f peut s'écrire sous la forme $f = a_1x^{\alpha_1} + ... + a_rx^{\alpha_r}$
où $a_1, ..., a_r$ sont des scalaires de $\Bbbk$ et $x^{\alpha_1}, ..., x^{\alpha_r}$ sont des monômes de $M(x_1, ..., x_n)$ tels que $x^{\alpha_1} \preceq ... \preceq x^{\alpha_r}$. On dit que :

• Le n-uplet α_r est le multidegré de f, que nous noterons mulitdeg(f),

• Le coefficient a_r est le cofficient dominant de f, que nous noterons $LC(f)$,

• Le monôme $x^{\alpha r}$ est le monôme dominant de f, que nous noterons $LM(f)$,

• Le terme $a_rx^{\alpha r}$ est le terme dominant de f, que nous noterons $LT(f) = LC(f) \cdot LM(f)$.

Exemple 4.6.13

On considère l'ordre lexicographique, avec l'ordre alphabétique $z < y < x$, le polynôme $f = x^2y^2z - x^2yz^3 + 2y^4z^4$ a pour multidegré $(2, 2, 1)$, pour coefficient dominant 1, pour monôme dominant x^2y^2z. Si on considère l'ordre lexicographique par degré, alors mulitdeg$(f) = (0, 4, 4)$, $LC(f) = 2$, $LT(f) = 2y^4z^4$.

Théorème 4.6.14

Soient $\preceq$ un ordre monomial sur $M(x_1, ..., x_n)$ et $F = (f_1, ..., f_s)$ un s-uplet de polynômes de $\Bbbk[x_1, ..., x_n]$. Alors tout polynôme f de $\Bbbk[x_1, ..., x_n]$ peut s'écrire sous la forme $f = a_1f_1 + ... + a_sf_s + r$ où a_i et r sont des polynômes de $\Bbbk[x_1, ..., x_n]$ et soit $r = 0$ soit aucun des monômes de r n'est divisible par $LT(f_1), ..., LT(f_s)$.

On dit alors que r est le reste de la division de f par F et on écrit $f \underset{F}{\Rightarrow} r$.

Définition 4.6.15

Soit I un idéal de $\Bbbk[x_1, ..., x_n]$, on note $LT(I) = \{LT(f) : f \in I\}$, $\langle LT(I)\rangle$ est l'idéal engendré par les éléments de $LT(I)$.

Proposition 4.6.16

Soit I un idéal de $\Bbbk[x_1, ..., x_n]$, si $I = \langle f_1, ..., f_s\rangle$, alors

$$\langle LT(f_1), ..., LT(f_s)\rangle \subset \langle LT(I)\rangle.$$

Définition 4.6.17

Etant donné un ordre monomial fixé, un sous ensemble $F = \{f_1, ..., f_s\}$ d'un idéal I de $\Bbbk[x_1, ..., x_n]$ est appelé base de Gröbner de I si $\langle LT(f_1), ..., LT(f_s)\rangle = \langle LT(I)\rangle$.
Dans ce cas tout polynôme f de I se décompose sous la forme

$$f = h_1f_1 + ... + h_sf_s,$$

où les h_i sont des polynômes de $\Bbbk[x_1, ..., x_n]$.

Exemple 4.6.18

Considérons l'idéal $I = \langle f_1, f_2\rangle$ de $\mathbb{R}[x, y]$ avec $f_1 = x^3 - 2xy$ et $f_2 = x^2y - 2y^2 + x$. Pour l'ordre lexicographique par degré les termrs dominants sont $LT(f_1) = x^3$ et $LT(f_2) = x^2y$, on a $yf_1 - xf_2 = -x^2 \in I$, mais le terme dominant $LT(yf_1 - xf_2) = LT(-x^2)$ n'est pas divisible par $LT(f_1)$ ou $LT(f_2)$, par suite, $LT(-x^2) \notin \langle LT(f_1), LT(f_2)\rangle$, donc l'ensemble $\{f_1, f_2\}$ n'est pas une base de Gröbner de I.

Définition 4.6.19

Soit $I = \langle f_1, ..., f_s \rangle$ un idéal de $\Bbbk[x_1, ..., x_n]$, on peut associer à I un semi-système de réécriture fini $(\Sigma, \mathcal{R})$ où

$$\Sigma = \{x_1, ..., x_n\} \text{ et } \mathcal{R} = \{LT(f_1) \longrightarrow LT(f_1) - f_1, ..., LT(f_s) \longrightarrow LT(f_s) - f_s\}.$$

Théorème 4.6.20

Une base $F = \{f_1, ..., f_s\}$ d'un idéal I est une base de Gröbner de I si, et seulement si, la relation de réduction $\underset{F}{\Rightarrow}$ est confluente.

Exemple 4.6.21

Considérons l'idéal $I = \langle f_1, f_2 \rangle$ de $\mathbb{R}[x, y, z]$ avec $f_1 = y - z^2$ et $f_2 = x - z^3$. Considérons l'ordre lexicographique induit par l'ordre alphabétique $x < y < z$. On obtient alors les deux règles de réécriture $z^2 \xrightarrow{f_1} y$ et $z^3 \xrightarrow{f_2} x$. On remarque que le monôme z^3 peut être réduit par les deux règles $z^3 \xrightarrow{f_1} yz, z^3 \xrightarrow{f_2} x$, on parle alors de paire critique. Les polynômes yz et x sont irréductibles. Donc le paire critique n'est pas confluente, d'où $\{f_1, f_2\}$ n'est pas une base de Gröbner de I pour cet ordre monomial.

Toutefois, si on concidère l'ordre lexicographique induit par l'ordre alphabétique $z < y < x$, on a les règles $y \xrightarrow{f_1} z^2, x \xrightarrow{f_2} z^3$.

On remarque que les deux polynômes f_1 et f_2 ne forment pas de paire critique, ainsi $\{f_1, f_2\}$ est une base de Gröbner de I .

Définition 4.6.22

Soient deux polynômes f et g de $\Bbbk[x_1, ..., x_n]$. On note

$$\alpha = (\alpha_1, ..., \alpha_n) = \text{multideg}(f) \text{ et } \beta = (\beta_1, ..., \beta_n) = \text{multideg}(g).$$

On pose $\gamma = (\gamma_1, ..., \gamma_n)$ où pour tout $i = 1, ..., n$ $\gamma_i = \max(\alpha_i, \beta_i)$.

• Le monôme x^γ est appelé le plus petit commun multiple de $LM(f)$ et $LM(g)$. Nous le noterons $PPCM(LM(f), LM(g))$.

• On appelle S-polynôme de f et g le polynôme $S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g$

Exemple 4.6.23

On considère l'anneau $\mathbb{R}[x, y]$ muni de l'ordre lexicographique, avec $y < x$. Soient $f = x^3y^2 - x^2y^3 + x$ et $g = 3x^4y + y^2$.

On a $S(f,g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g = S(f,g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g = -x^3y^3 - \frac{1}{3}y^3 + x^2$.

Théorème 4.6.24

Soit I un idéal de $\Bbbk[x_1, ..., x_n]$. Une base $F = \{f_1, ..., f_s\}$ de I est une base de Gröbner si, et seulement si, pour tous i et j de $\{1, ..., s\}$, on a $S(f_i, f_j) \xrightarrow{F} 0$.

Exemple 4.6.25

Considérons l'idéal $I = \langle f_1, f_2 \rangle$ de $\mathbb{R}[x, y, z]$ avec $f_1 = y - z^2$ et $f_2 = x - z^3$. Considérons l'ordre lexicographique induit par l'ordre alphabétique $z < y < x$. On a
$\alpha = \alpha =$multideg$(f_1) = (0, 1)$ et $\beta =$multideg$(f_2) = (1, 0)$, par suite $\gamma = (1, 1)$. Donc $S(f_1, f_2) = \frac{x^\gamma}{LT(f_1)} \cdot f_1 - \frac{x^\gamma}{LT(f_2)} \cdot f_2 = \frac{xy}{y} \cdot f_1 - \frac{xy}{x} \cdot f_2 = -x^3 + yz^3 = xf_1 - yf_2$, alors $S(f_1, f_2) \underset{F}{\Rightarrow} 0$. Finalement $F = \{f_1, f_2\}$ est une base de Gröbner de I.

Conclusion

1. Dans ce travail on a donné des certains conditions pour assurer la propriété de terminaison dans des cas particuliers. Notons que cette partie d'étude à fait l'objet d'une publication intitulée : $\ll$ On the termination problem forstring rewrite systems $\gg$ dans le journal $International\ Journal\ of\ Computer\ Applications, Vol, 146 - No.6, 2016.$

2. Etants données deux semi-systèmes de réecriture $(\Sigma_1, \mathcal{R}_1)$ et $(\Sigma_2, \mathcal{R}_2)$. Nous avons déterminé quelques conditions sur les relations $\mathcal{R}_1$ et $\mathcal{R}_2$ qui permettent d'assurer l'existence d'un morphisme entre les monoïdes $\Sigma_1^*/\overset{*}{\underset{\mathcal{R}_1}{\Longleftrightarrow}}$ et $\Sigma_2^*/\overset{*}{\underset{\mathcal{R}_2}{\Longleftrightarrow}}$ pour assurer le passage entre les deux monoïdes quotients. D'autre part, on donne une relation spécifique $\mathcal{R}$ sur Σ^* qui fait du monoïde quotient $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\Longleftrightarrow}}$ un groupe. Ce travail à fait l'objet d'une publication intitulée : $\ll$ Presentation of monoids by generators and relations $\gg$ dans le journal $Global\ and\ Stochastic\ Analysis\ (GSA) Vol.3 - No.2, 2016.$

3. La construction de certains codes à groupes dans un monoïde libre. Cette application a fait l'objet d'une publication intitulée : $\ll$ A Construction of Some Group Codes $\gg$ Parue dans le journal $International\ Journalof\ Electronics\ and\ Information\ Engineering, Vol.4, 2016.$

4. Enfin, on s'intéresse au protocole ATS-monoïde**.** Plus précisément, on donne des attaques contre ATS-monoïde dans des cas spécifiques et quelques exemples sur ces cas. Notons que ce résultat a fait l'objet aussi d'une publication intitulée :

$\ll$ Some attacks of an encryption system based on the word problem in a monoid $\gg$ dans le journal $International\ Journal\ of\ Applied\ Mathematical\ Research. Vol.5(4), 2016.$

Bibliographie

[1] P. J. Abisha, D. G. Thomas and K. G. Subramanian. "Public Key Cryptosystems Based on Free Partially Commutative Monoids and Groups, Lecture Notes in Computer Science, vol. 2904, Springer–Verlag, pp. 218–227, (2003).

[2] J. M. Autebert. "Théorie des langages et automates", Masson, (1994).

[3] M. Benois. "Application de l'étude de certaines congruences à un problème de décidabilité", Séminaire Dubreil , n^o 7, (1972).

[4] P. Berlioux , Mnacho. Echenim et Michel Lévy. "Théorie des langages", Ecole nationale supérieure d'informatique et de mathématiques appliquées de France, (2009).

[5] J. Berstel. "Automates et grammaires", Université de Marne-la-Vallée, (2005).

[6] J. Berstel. "Theory of codes", Academic Press, (1984).

[7] J. Berstel. "Congruences plus que parfaites et langages algébriques", Séminaire d'informatique théorique, (1977).

[8] R. V. Book and H. N. Liu. "Rewriting Systems and Word Problems in a Free Partially Commutative Monoid", Information Processing Letters n^o 26, pp. 29-32, (1987).

[9] R. Cori et D. Perrin. "Automates et Commutations Partielles", RAIRO-Informatique théorique, tome19, n^o 1, pp. 21-32, (1985).

[10] N. Dershowitz. "Termination of rewriting", Journal of Symbolic Computation, tome 3, pp. 69-116(1987).

[11] W. Diffie and M. E. Hellman. "New Direction in Cryptography", IEEE Trans, on Inform Theory, 22(6), pp. 644-665, (1976).

[12] H. Dubois. "Systèmes de règles de production et calcul de réécriture", Thèse de doctorat en informatique, Université Henri Poincaré-Nancy 1, (2001).

[13] M. Eytan et G. TH. Guilbaud. "Présentation de quelques monoïdes finis", Mathématiques et sciences humaines, vol 7, pp. 3-10, (1964).

[14] R. Floyd et R. Beigel, Traduction de D. Krob. "Le langage des machines", International Thomson France, paris, (1995).

[15] N. Ghadbane and D. Mihoubi."On the termination problem for string rewrite systems ", International Journal of Computer Applications, Vol. 146, n^o 6, (2016).

[16] N. Ghadbane and D. Mihoubi. "A Construction of Some Group Codes, International Journal of Electronics and Information Engineering, Vol. 4, (2016).

[17] N. Ghadbane and D. Mihoubi. "Some attacks of an encryption system based on the word problem in a monoid", International Journal of Applied Mathematical Research, vol 5(4), (2016).

[18] N. Ghadbane and D. Mihoubi. "Presentation of monoids by generators and relations", Global and Stochastic Analysis (GSA), vol 3(2), (2016).

[19] D. Guin et T. Hausberger. "Algèbre 1, Groupes, Corps et Théorie de Galois", EDP Sciences, (2008).

[20] Y. Guiraud. "Présentations d'opérades et systèmes de réécriture", Thèse de Doctorat, Institut de Mathématiques et de Modélisation de Montpellier, (2004).

[21] A. K. "Knuth-Bendix procedure and Buchberger Algorithm A Synthesis", Université Cadi Ayyad , Marrakech, Morocco, (1989).

[22] D. Kapur and P. Narendran. "A Finite Thue System With Decidable Word Problem and Without Equivalent Finite Canonical System", Theoretical Computer Science, vol 35, pp. 337-344, (1985).

[23] Y. Lafont. "Réécritue et problème du mot", Gazette des Mathématiciens 120. Laboratoire de Mathématiques Discrètes de Luminy, Marseille, France, (2009).

[24] Y. Lafont. "A new finiteness condition for monoids presented by complete rewrting systms", Laboratoire de Mathématiques Discrètes de Luminy, Marseille, France, (1995).

[25] S. Marcel."Langage formels et monoïdes finis", Séminaire Dubreil. Algèbre et théorie des nombres, vol. 23, no. 2, pp. 1-3, (1970).

[26] M. Marchand. "Outils mathématiques pour l'informaticien", De Boeck, (2005).

[27] Y. Metiver. "Calcul de longueurs de chaines de réécriture dans un monoïde libre", U.E.R, de Mathématiques et informatique, Université de Bordeaux 1, France (1983).

[28] M. Nivat. "Sur le noyau d'un homomorphisme du monoïde libre", Séminaire Schutzenberger, tom 1, exp. n^o 4, pp. 1-6, (1970).

[29] M. Nivat. "Congruence parfaites et quasi-parfaites", Séminaire Dubreil Algèbre, tom 1, exp, n^o 7, pp. 1-9, (1970).

[30] M. Nivat. "Eléments de la théorie général des codes, Université de Paris, (1965-1966).

[31] L. Perret. "Etude d'outils algébriques et combinatoires pour la cryptographie à clef publique", thèse de doctorat, Université de Marne–la–Vallée, (2005).

[32] H. Phan et Philippe Guillot. "Preuves de sécurité des schémas cryptographiques", université Paris 8, (2013).

[33] D. Perrin. "Le degré minimal du groupe d'un code bipréfixe fini", Journal of Combinatorial Theory, Series A, vol. 25, no. 2, pp. 749-759, (2003).

[34] L. Pierre. "Les systèmes de réécriture", Université de Nice Sophia-Antipolis,(2007).

[35] P. Rannou. "Réécriture de diagrammes et de Σ-diagrammes", Thèse de doctorat, Université d'Aix-Marseille, (2013).

[36] M. Rigo. "Théorie des automates et langages formels", Université de Liège, 2009.

[37] G. Rindone. "On syntactic groups", Bulletin Mathématique de Belgique, (2003-2004).

[38] B. Robin. "Correspondances entre les algorithmes de Knuth-Bendix et de Buchberger", Université de Claude Bernard Lyon.

[39] H. Rosen. "Cryptography Theory and Practice", Third Edition, Chapman and Hall/CRC, (2006).

[40] J. Rouyer. "Preuves de terminaison de systèmes de réécriture fondées sur les interprétations polynomiales", CRIN, Nancy, (1989).

[41] A. Salomma. "Jewels of formal language theory", University of Turku, (1977).

[42] H. J. Shyr. "Free monoids and languages", Department of Mathematicsn, Soochow University Taipei,Taiwan R.O.C,(1979).

[43] D. Sow. "Courbes elliptiques, Cryptographie à clés publiques et protocoles d'échange de clés", Thèse de doctorat, Unversité de Cheikh Diop de Dakar, (2013).

[44] G. Viennot. "Algèbre de Lie libres et monoïdes libres", Springer Berlin Heidelberg, New York, (1978).

[45] H. Zantema. "Termination of String Rewriting Proved Automatically, TU Eindhoven, (2004).