**UNIVERSITE MOHAMED BOUDIAFDE M'SILA**

**Faculté des Mathématiques et de l'Informatique**

**Département de Mathématiques**

# MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du Diplôme de **MASTER**

**Domaine :** Mathématiques et Informatique

**Filière:** Mathématiques

**Option :** Algèbre et mathématique discrète

**Par**

**Souhaila Ben naoui**

**Sujet**

# Congruence dans un monoïde libre et leurs applications

Date de soutenance : 20 / 06 / 2018

## Devant le jury :

| | | |
|---|---|---|
| Mr. Douadi Mihoubi | Pr. Univ de M'sila | Président |
| Mr. Lakhdar Heboub | MAA. Univ de M'sila | Examinateur |
| Mr. Nacer Ghadbane | MCB. Univ de M'sila | Encadreur |

**Promotion : 2017 / 2018**

# *Dédicace*

*Je dédie ce modeste travail à ceux qui m'ont encouragé et soutenu moralement et matériellement pendant les moments les plus difficiles et durant toute ma vie, et qui me sont les plus chères sur cette planète : mon père et ma mère.*

*A tous mes amies.*

*A tous ceux que j'aime.*

*A tous les étudiants de ma promotion.*

*Avec l'expression de tous mes sentiments de respect.*

*Je dédie ce mémoire.*

# *Remerciements*

*Nous remercions avant tous ALLAH pour son aide, ses innombrables dons, ALLAH qui nos a donné la force, la volonté et le moral pour accomplir nos études en master en mathématique.*

*Ainsi, nous tenons également á exprimer nos vifs remerciements á notre encadreur Dr. N. Ghadbane pour avoir d'abord proposer ce thème, pour son suivi continuel tout le long de la réalisation de ce mémoire et quelle n'a pas cessée de vous donner ses conseils.*

*Notre remerciements vont au président du jury et aux membres du jury qui nos ont fait l'honneur de participer au jury.*

*Nous remercions évidemment nos parents, nos fréres et soeurs, qui depuis de si longues années, nos ont encourage et soutenu dans la poursuite de nos études.*

*Enfin, Nous tenons á exprimer notre reconnaissance á tous nos amis et collègues pour le soutien moral · · ·*

# Table des matières

# Notations

$\Sigma$ **:** alphabet fini

$\Sigma^*$ : monoïde libre sur $\Sigma$

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

$|w|$ : la longueur du mot $w$

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

$S = \langle \Sigma, \mathcal{R} \rangle$ : un semi-système de réécriture de mots

$IRR(w)$ : le mot irréductible de $w$

$L$ : langage sur l'alphabet $\Sigma$

$\mathcal{R}^0$ : 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 $\mathcal{R}$

$\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$ : la congruence engendrée par $\mathcal{R}$

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

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

$\cong$ : isomorphe

$C(a)$ : la classe d'équivalence de $a$

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

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

# Introduction générale

L'objectif visé dans ce travail est l'étude de la congruence dans un monoïde et quelques ses applications. Soit $(M, \cdot, 1_M)$ un monoïde, une congruence sur $(M, \cdot, 1_M)$ est une relation d'équivalence $\equiv$ stable par la multiplication à droite et à gauche, c'est-a-dire :

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

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 congruence joue un rôle fondamental dans la construction des structures algébriques quotients.

Ce travail est composé de trois chapitres.

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

Dans le deuxième chapitre, on fait une étude sur la présentation de quelques monoïdes par générateurs et relations ainsi que certaines de leurs propriétés.

Enfin, dans le troisième chapitre, on étude un système de cryptage qui basé sur le problème du mot dans un monoïde libre : Le protocole ATS-monoïde, sécurité de ATS monoïde et quelques attaques contre ATS monoïde.

# Chapitre 1

# Préliminaires

## Introduction

Ce premier chapitre contient les définitions et les propriétés des outils que nous utiliserons par la suite : les relations binaires et leurs propriétés, monoïde, mots et langages, et généralités sur la cryptographie à clé publique.

Contenu

1.1. Les relations binaires et leurs propriétés.
1.2. Monoïde.
1.3. Mots et langages.
1.4. Généralités sur la cryptographie à clé publique.

## 1.1 Les relations binaires et leurs propriétés

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

**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 $x\mathcal{R}y$.

**Définition 1.1.2**

Les relations étant 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,

$$x\mathcal{R}_1 y \Longrightarrow x\mathcal{R}_2 y.$$

**Définition 1.1.3**

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

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

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

**Exemple 1.1.4**

Soient $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$, $C = \{x, y, z\}$, on pose, $\mathcal{R}_1 = \{(b, x), (b, z), (c, y), (d, z)\}$, $\mathcal{R}_2 = \{(1, a), (2, d), (3, a), (3, b), (3, d)\}$.
Donc on a $\mathcal{R}_1 \circ \mathcal{R}_2 = \{(2, z), (3, x), (3, z)\}$.

**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 $\mathcal{R} \cap \mathcal{R}^0 = \emptyset$, c'est-à-dire il n'existe pas un élément $x \in E$ que vérifie $x\mathcal{R}x$.
- Symétrique si on a $\mathcal{R}^{-1} \subseteq \mathcal{R}$, c'est-à-dire $y\mathcal{R}x$ dés que $x\mathcal{R}y$, tel que :

$$\mathcal{R}^{-1} = \{(y, x)/\ (x, y) \in R\}.$$

- 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 $xRy$ et $y\mathcal{R}z$ alors $x\mathcal{R}z$.

**Définition 1.1.6**

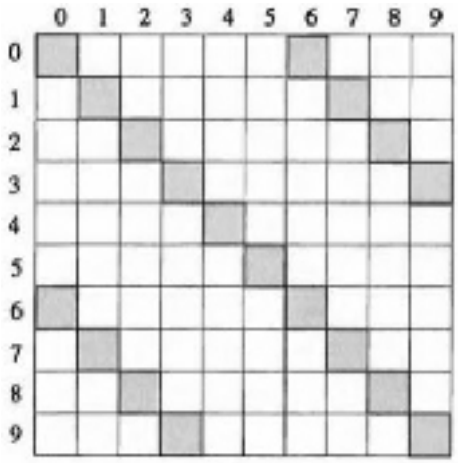
Une relation d'équivalence $\mathcal{R}$ sur un ensemble $E$ est une relation binaire qui est à la fois réflexive, symétrique et transitive.

**-** On peut associer à chaque é1ément $a$ de $E$ l'ensemble des é1éments qui lui sont équivalents, c'est une partie de $E$ qu'on appelle la classe équivalence de $a$ et qu'on note $\overline{a}$ ou $C(a)$, tel que $C(a) = \{x \in E\ /\ x\mathcal{R}a\}$.

L'ensemble des classes d'équivalence s'appelle l'ensemble quotient de $E$ par la relation $\mathcal{R}$, on le note $E/\mathcal{R}$.

**Exemple 1.1.7**

Sur $E = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ on définit une relation $\mathcal{R}$ on déclarant $\ll x\mathcal{R}y$ quand $x-y$ est un multiple de 6 $\gg$, donnée par la table ci-dessous. C'est une relation d'équivalence, en effet, $x - x = 0 \times 6$ donc $x$ est en relation avec lui même et la relation est réflexive, si $x$ est en relation avec $y$, il existe un entier $p$ tel que $x-y = p\times 6$, mais alors : $y-x = (-p)\times 6$ donc $y - x$ est un multiple de 6 et la relation est symétrique, enfin si $x$ est en relation avec $y$ et $y$ en relation avec $z$, il existe $p$ et $q$ tels que : $x - y = p \times 6$ et $y - z = q \times 6$, ce qui donne $x - z = (p + q) \times 6$, donc $x - z$ est aussi un multiple de 6 et la relation est transitive.




Donc les classe d'équivalences des é1éments de $E$ sont :
$\overline{0} = \{0,6\}, \overline{1} = \{1,7\}, \overline{2} = \{2,8\}, \overline{3} = \{3,9\}, \overline{4} = \{4\}, \overline{5} = \{5\}, \overline{6} = \{0,6\}, \overline{7} = \{1,7\}, \overline{8} = \{2,8\}, \overline{9} = \{3,9\}$.

**Proposition 1.1.8**

Une relation d'équivalence $\mathcal{R}$ sur un ensemble $E$ peut être aussi définie des plusieurs manières :

1. Par la donnée d'un partition $P$ de $E$ :

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

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

$$x\mathcal{R}y \Longleftrightarrow f(x) = f(y).$$

**Notation 1.1.9**

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 1.1.10**

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.

**Proposition 1.1.11** [10]

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

$$\mathcal{R} \subseteq \widetilde{\mathcal{R}} \subseteq \mathcal{S}.$$

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

• 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 $\mathcal{R}$ sur $E$. D'autre part, pour toute famille de relations $\mathcal{S}$ de $E \times E$ vérifiant la propriété $P$, on a bien la relation $\bigcap \mathcal{S}$ vérifie aussi cette propriété. Il en résulte que :

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

est la plus petite relation binaire contenant $\mathcal{R}$ est possédant la propriété $P$. On a les formules suivantes :

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

**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 $\mathcal{R}$ 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 $\mathcal{S}$ une autre relation transitive qui contient $\mathcal{R}$. Montrons que $\bigcup_{n=1}^{+\infty} \mathcal{R}^n \subset \mathcal{S}$.

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 $\mathcal{R} \subset \mathcal{S}$ alors $x\mathcal{S}x_1, x_1\mathcal{S}x_2, ..., x_{q_1-1}\mathcal{S}y$, comme $\mathcal{S}$ est transitive, alors $x\mathcal{S}y$.

**Exemple 1.1.12**

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

- $\mathcal{R}^s = \mathcal{R} \cup \mathcal{R}^{-1} = \{(1, 2), (1, 3), (2, 1), (2, 3), (3, 4), (3, 1), (3, 2), (4, 3)\}$.
- $\mathcal{R}^r = \mathcal{R} \cup \mathcal{R}^0 = \{(1, 2), (1, 3), (2, 1), (2, 3), (3, 4), (1, 1), (2, 2), (3, 3), (4, 4)\}$.
- $\mathcal{R}^+ = \{(1, 2), (1, 3), (2, 1), (2, 3), (3, 4)(1, 1), (1, 4)(2, 2)(2, 4)\}$.
- $\mathcal{R}^* = \mathcal{R}^+ \cup \mathcal{R}^r = \{(1, 2), (1, 3), (2, 1), (2, 3), (3, 4)(1, 1), (1, 4)(2, 2)(2, 4), (1, 1), (3, 3), (4, 4)\}$.
- $\widetilde{\mathcal{R}} = \mathcal{R}^* \cup \mathcal{R}^s = \left\{ \begin{array}{c} (1, 2), (1, 3), (2, 1), (2, 3), (3, 4), (1, 1), (2, 2)(2, 4), (1, 4), (3, 3), \\ (4, 4), (3, 1), (3, 2), (4, 3), (4, 2) \end{array} \right\}$.

## 1.2 Monoïde

**Définition 1.2.1**

Un monoïde est un ensemble muni d'une loi interne, i.e, d'une application "$\cdot$" : $M \times M \to M$, qui satisfait aux conditions suivantes :

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

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

**Exemple 1.2.2**

$(\mathbb{N}, +, 0)$ , $(\mathbb{N} \cup \{+\infty\}, \min, +\infty)$ sont des monoïdes.

**Remarque 1.2.3**

Un monoïde $(M, \cdot)$ qui est tel que tout élément de $M$ possède un inverse est un groupe.

**Remarque 1.2.4**

Tout groupe est un monoïde, mais l'inverse n'est pas toujours vrai. Par exemple $(\mathbb{N}, +)$ est un monoïde qui n'est pas un groupe.

**Définition 1.2.5**

Soient $(M\ , \cdot, 1_M)$ un monoïde et $N \subseteq M$. On dit que $(N, \cdot, 1_N)$ est un sous monoïde de $(M\ , \cdot, 1_M)$ si :

**1-** $1_M \in N$, $1_M$ étant l'élément neutre de $M$,

**2-** $\forall x, y \in N$, $x \cdot y \in N$ sous semi groupe de $M$.

**Définition 1.2.6**

Un morphisme (ou encore homomorphisme) d'un monoïde $M$ dans un monoïde $N$ est une application $h$ telle que :

**1-** $\forall u, v \in M : h(uv) = h(u)h(v)$,

**2-** $h(1_M) = 1_N$ : l'image de l'élément neutre de $M$ est l'élément neutre de $N$.

Un isomorphisme de monoïdes est un homomorphisme bijectif de monoïdes.

**Exemple 1.2.7**

La fonction exponentielle représente un isomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+ - \{0\}, \times)$. Elle est bijective et vérifie : $\exp(x + y) = \exp(x) \times \exp(y)$ et $\exp(0) = 1$.

**Définition 1.2.8**

Soit $(M, \cdot, 1_M)$ un monoïde, une congruence sur $(M, \cdot, 1_M)$ est une relation d'équivalence $\equiv$ stable par la 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 1.2.9**

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 1.2.10**

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.

## 1.3 Mots et langages

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

**Définitions 1.3.1**

- Un alphabet est un ensemble fini $\Sigma$, les éléments de $\Sigma$ sont appelés lettres ou symboles. Ainsi $\Gamma = \{a, b, d, e\}, \Omega = \{0, 1\}$ sont des alphabets.

- Un mot $w$ sur l'alphabet $\Sigma$ est une suite finie $\sigma_1\sigma_2...\sigma_n$ de lettres de $\Sigma$. L'entier $n$ est appelé la longueur de $w$ notée $|w|$. On note $|w|_\alpha$ le nombre de d'occurrence de la lettre $\sigma$ dans le mot $w$. Si l'on note $w = \sigma_1\sigma_2...\sigma_n$ :

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

- 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 $\varepsilon$.

- La concaténation de deux mots $u = u_1\ u_2...u_m$ et $v = v_1v_2...v_n$ est le mot noté $u.v$ ou $uv$ et égal à $u_1\ u_2...u_mv_1v_2...v_n$ obtenu simplement par juxtaposition.

**Proposition 1.3.2**

Soit $\Sigma$ un alphabet quelconque. Le monoïde $\Sigma^*$ possède les deux propriétés suivantes :

**1-** Tout élément de $\Sigma^*$ est une suite finie d'éléments de $\Sigma$.

**2-** Deux suites distinctes d'éléments de $\Sigma$ définissent deux éléments distincts de $\Sigma^*$.

**Remarque 1.3.3**

Notons que si $P$ et $P^{'}$ deux partitions de monoïde libre $\Sigma^*$, 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 $P$.

**Définition 1.3.4**

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

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

**Remarque 1.3.5**

1. Notons que cet morphisme $h$ est complètement déterminé ayant les images des lettres de $\Sigma$ dans $\Delta^*$, i.e, $h(\sigma)$ pour tout $\sigma$ appartenant à $\Sigma$.

2. Nous noterons $Hom\,(\Sigma^*, \Delta^*)$ l'ensembles des morphismes de monoïdes entre $\Sigma^*$ et $\Delta^*$. Nous dirons que $h \in Hom\,(\Sigma^*, \Delta^*)$ est non trivial s'il existe au moins une lettre $\sigma \in \Sigma$ pour laquelle $h(\sigma) \neq \varepsilon$.

3. Un morphisme de monoïdes bijectif est appelé isomorphisme de monoïdes; $Iso\,(\Sigma^*, \Delta^*)$ désignera alors l'ensemble des isomorphismes de monoïdes entre $\Sigma^*$ et $\Delta^*$.

**Exemple 1.3.6**

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 $\Sigma^*$ soit appelé monoïde libre.

Cette propriété caractérise le monoïde libre engendré par $\Sigma$.

**Proposition 1.3.7**

Soit $M$ un monoïde quelconque et $f$ est une application d'un alphabet $\Sigma$ dans $M$. Alors il existe un homomorphisme unique $\widetilde{f}$ de $\Sigma^*$ dans $M$ qui prolonge $f$ c'est-à-dire :

$$\forall \alpha \in \Sigma,\ \widetilde{f}(\alpha) = f(\alpha).$$

**Démonstration**

- L'existence : Posons

$\widetilde{f}(\varepsilon) = 1_M$ et $\widetilde{f}(\alpha_1\alpha_2...\alpha_n) = f(\alpha_1)f(\alpha_2)...f(\alpha_n),\ n \in \mathbb{N},\ \alpha_i \in \Sigma,\ 1 \leq i \leq n.$

Et facile de voir que $\widetilde{f}$ est bien un homomorphisme.

- Unicité : Soient $\widetilde{f}$ et $\widetilde{g}$ deux homomorphismes de $\Sigma^*$ dans $M$ tels que :

$\forall \alpha \in \Sigma,\ \widetilde{f}(\alpha) = \widetilde{g}(\alpha)$.

Alors $\widetilde{f}(\varepsilon) = \widetilde{g}(\varepsilon) = 1_M$ et pour tout mot $w = \alpha_1\alpha_2...\alpha_n \in \Sigma^*$, on a :

$\widetilde{f}(w) = \widetilde{f}(\alpha_1\alpha_2...\alpha_n) = f(\alpha_1)f(\alpha_2)...f(\alpha_n) = \widetilde{g}(\alpha_1\alpha_2...\alpha_n) = \widetilde{g}(w)$.

**Définition 1.3.8**

On appelle langage sur un alphabet $\Sigma$ tout sous-ensemble de $\Sigma^*$. Un langage est dit fini ou infini selon qu'il comprend un nombre fini ou infini de mots.

**Exemple 1.3.9**

**i)** $\emptyset, \Sigma^1, \Sigma^2, ..., \Sigma^n, \Sigma^*$ sont des langages sur $\Sigma$. On appelle $\emptyset$ le langage vide.

**ii)** L'ensemble des identificateurs est un langage sur $\{A, B, ..., Z, a, b, ..., z, 0, 1, ..., 9\}$.

**Définition 1.3.10**

Soit $L \subseteq \Sigma^*$ un langage. On définit sur $\Sigma^*$ la relation suivante. Soient $u, v \in \Sigma^*$. on a :

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

- Il est facile de vérifier qu'il s'agit d'une relation d'équivalence sur $\Sigma^*$ et même d'une congruence (à droite et à gauche), i.e,

$$\forall \sigma \in \Sigma \ , u \equiv_L v \Longrightarrow (u\sigma \equiv_L v\sigma \text{ et } \sigma u \equiv_L \sigma v).$$

- On parle souvent de la congruence syntaxique $\equiv_L$ et on dit que $u$ et $v$ sont syntaxiquement équivalents.

**Exemple 1.3.11**

Soit $\Sigma = \{0, 1\}$ et soit les deux langages $L = \{w \in \{0,1\}^* : |w|_1 \equiv 0[2]\}$ et $L' = \{w \in \{0,1\}^* : |w|_1 \equiv 1[2]\}$. On calcul le monoïde syntaxique de $L$.

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

$\Longleftrightarrow (\forall x, y \in \Sigma^* : |xuy|_1 \equiv 0[2] \Longleftrightarrow |xvy|_1 \equiv 0[2])$

$\Longleftrightarrow (\forall x, y \in \Sigma^* : |x|_1 + |u|_1 + |y|_1 \equiv 0[2] \Longleftrightarrow |x|_1 + |v|_1 + |y|_1 \equiv 0[2])$.

Alors $\Sigma^*/\equiv_L = \{[w] \ / \ w \in \Sigma^*\}$, tel que $[w] = \{u \in \Sigma^*/ \ u \equiv_L w\}$.

- Soit $w \in L$, donc :

$[w] = \{u \in \Sigma^*/ \ \forall x, y \in \Sigma^* : |x|_1 + |u|_1 + |y|_1 \equiv 0[2] \Longleftrightarrow |x|_1 + |v|_1 + |y|_1 \equiv 0[2]\}$

$= L$.

- Soit $w \in L'$,

$[w] = \{u \in \Sigma^*/ \ \forall x, y \in \Sigma^* : |x|_1 + |u|_1 + |y|_1 \equiv 1[2] \Longleftrightarrow |x|_1 + |v|_1 + |y|_1 \equiv 1[2]\}$

$= L'$.

Donc $\Sigma^*/\equiv_L = \{L, L'\}$.

## 1.4 Généralité sur la cryptographie à clé publique

La cryptographie à clé publique est récente, elle provient de l'article fondateur de Diffie et Hellman[12]. 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.

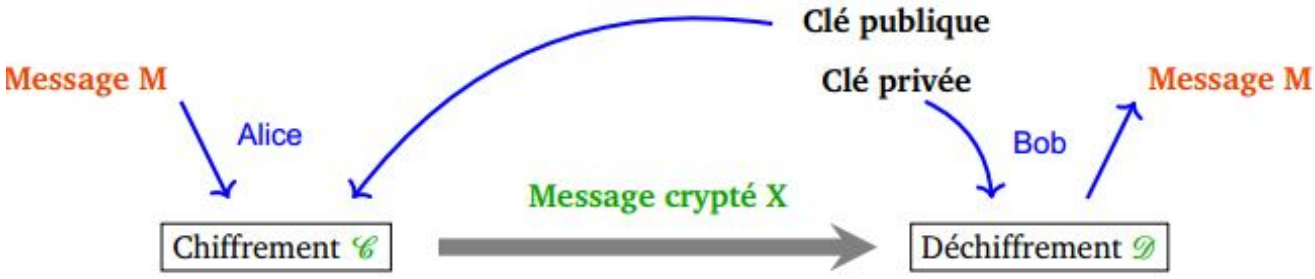
**L'algorithme asymétriques (ou schéma à clé publique)**

Ils ont été introduits par Diffie et Hellman en 1976 : deux clés différentes sont nécessaires, une clé secrète s et une clé publique p de telle sorte que la connaissance de p ne permette pas de retrouver facilement s. Plus précisément, il ne doit pas exister d'algorithme efficace permettant de calculer s à partir de p .

Un algorithme asymétrique est généralement basé sur un problème complexe, c'est-à-dire difficile à résoudre, de sorte qu'il n'existe pas d'algorithme efficace permettant de trouver la solution .

L'efficacité d'un algorithme est susceptible d'évoluer en fonction des progrès des ordinateurs (gain en puissance et en rapidité), mais aussi en fonction des découvertes et des améliorations d'algorithmes permettant de résoudre les problèmes difficiles sous-jacents plus efficacement.

Dans le but d'envoyer un message confidentiel à B (le receveur B appelé Bob), A (l'envoyeur A appelé Alice par convention) utilise la clé publique de B pour chiffrer ce message, A étant le seul possesseur de la clé secrète (seule clé autorisant le déchiffrement), il est le seul à même de déchiffrer le message envoyé par A.




**Fonction à sens unique**

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 $\phi$ telle que $\phi \circ \psi = id_M$ où $id_M$ est l'application identique de $M$. La construction du couple $(\psi, \phi)$ réalise le mécanisme de chiffrement et de déchiffrement et la publication de $\psi$ ne doit rien révéler sur $\phi$.

**Définition 1.4.1**

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 1.4.2**

Soit $G$ un groupe cyclique d'ordre $n$ et $g$ un générateur de $G$. Soit la fonction $f : [0, n-1] \longrightarrow G, k \longrightarrow f(k) = g^k$, $f$ 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 exponentiels ou quasi exponentielles en la taille $n$ de $G$.

# Chapitre 2

# Présentation de quelques monoïdes par générateurs et relations

## Introduction

Ce chapitre constitue une présentation générale de quelques monoïdes ainsi que certaines propriétés essentielles qui les concernent.

Contenu

2.1. Quelques définitions.
2.2. Présentation de quelques monoïdes.
2.3. Quelques propriétés sur la présentation d'un monoïde.

## 2.1 Quelques définitions

**Définition 2.1.1**

Un semi-système de réécriture de mot, dit aussi semi-système de Thue, est un couple $S = \langle \Sigma, \mathcal{R} \rangle$ où $\Sigma$ un alphabet fini et $\mathcal{R}$ une relation binaire sur le monoïde libre $\Sigma^*$. Un élément $(r, s)$ de $\mathcal{R}$ est dit une règle de réécriture ou substitution. Appliquer une règle quelconque de la forme $r\mathcal{R}s$ de $S = \langle \Sigma, \mathcal{R} \rangle$ à un mot $f$ contenant le facteur $r$ consiste à remplacer $r$ par $s$ dans $f$. S'il n'y a aucune règle de $S = \langle \Sigma, \mathcal{R} \rangle$ applicable à $f$, alors $f$ est dit irréductible ou sous la forme normale.

**Exemple 2.1.2**

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

**Définition 2.1.3**

Etant données deux mots $u, v \in \Sigma^*$, on dit que $v$ dérive directement de $u$, et on note $u \underset{\mathcal{R}}{\rightarrow} v$ si, et seulement si, il existe une règle $(r, s)$ de $\mathcal{R}$ et $x, y \in \Sigma^*$ tels que :

$$u = xry \text{ et } v = xsy.$$

On dit que $v$ dérive de $u$, et on note $u \overset{*}{\underset{\mathcal{R}}{\rightarrow}} v$, s'il existe une suite finie de mots $u_0, u_1, ..., u_n$ de $\Sigma^*$ avec,

$$\begin{aligned} u_0 &= u, \\ u_i &\underset{\mathcal{R}}{\rightarrow} u_{i+1}, \forall 0 \leq i \leq n-1, \\ \text{et } u_n &= v. \end{aligned}$$

Notons que la relation $\overset{*}{\underset{\mathcal{R}}{\rightarrow}}$ est la fermeture réflexive et transitive de $\underset{\mathcal{R}}{\rightarrow}$ et $\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$ est la fermeture d'équivalence de $\underset{\mathcal{R}}{\rightarrow}$.

**Remarque 2.1.4**

1. Un branchement de $\langle \Sigma, \mathcal{R} \rangle$ est un triplet $(x, y, z)$ d'éléments de $\Sigma^*$ 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.

2. On dit qu'un système de réécriture $S = \langle \Sigma, \mathcal{R} \rangle$ termine ou qu'il est noethérien, s'il n'existe pas de chaine de réécriture infini de la forme $w_0 \underset{\mathcal{R}}{\rightarrow} w_1 ... \underset{\mathcal{R}}{\rightarrow} w_n \underset{\mathcal{R}}{\rightarrow} ...$ c'est-à-dire il n'existe pas une dérivation infini dans $S = \langle \Sigma, \mathcal{R} \rangle$.

**3.** 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.

**Définition 2.1.5**

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

**Proposition 2.1.6**

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

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

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

## 2.2 Présentation de quelques monoïdes

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

**Définition 2.2.1**

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

$$M \cong \Sigma^* / \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}.$$

Si les deux ensembles $\Sigma$ et $\mathcal{R}$ sont finis, on dit que le monoïde $M$ est finement présenté.

**Exemple 2.2.2**

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

**ii)** La présentation du monoïde $(\mathbb{N}^2, +)$ : Soient $\Sigma = \{\alpha, \beta\}$, et la relation $\mathcal{R} = \{(\alpha\beta, \beta\alpha)\}$. On a pour tout $w \in \{\alpha, \beta\}^*$, il existe un unique $(m, n) \in \mathbb{N}^2$ tel que $w \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} \beta^m\alpha^n$ avec $m = |w|_\beta$ et $n = |w|_\alpha$.

On définit l'application $\psi : \mathbb{N}^2 \longrightarrow \Sigma^*/\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$ , $\psi(m, n) = [\beta^m\alpha^n]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$, l'application $\psi$ est morphisme car pour tout $(m, n) \in \mathbb{N}^2$, $(p, q) \in \mathbb{N}^2$.

On a :

$$\begin{aligned}
\psi((m, n) + (p, q)) &= \psi(m + p, n + q) \\
&= [\beta^{m+p}\alpha^{n+q}]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} \\
&= [\beta^m\beta^p\alpha^n\alpha^q]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} \\
&= [\beta^m\alpha^n\beta^p\alpha^q]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} \\
&= [\beta^m\alpha^n]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} \cdot [\beta^p\alpha^q]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} \\
&= \psi(m, n) \cdot \psi(p, q).
\end{aligned}$$

D'autre part on a pour tout $(m, n) \in \mathbb{N}^2$, $(p, q) \in \mathbb{N}^2$:

$$\begin{aligned}
\psi(m, n) = \psi(p, q) &\iff [\beta^m\alpha^n]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} = [\beta^p\alpha^q]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} \\
&\iff (m = p \text{ et } n = q).
\end{aligned}$$

Donc $\psi$ est injective, et il est clair que $\psi$ est surjective.

Finalement on a : $(\mathbb{N}^2, +) \cong \Sigma^*/\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$.

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

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

Donc $\mathbb{Z} \cong \Sigma^*/\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} = \{[\varepsilon]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}, [\alpha^n]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}, [\beta^m]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}, (n, m) \in \mathbb{N}^2\}$, où l'isomorphisme $\phi$ est défini par: $\phi(0) = [\varepsilon]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$, si $n > 0$, alors $\phi(n) = \left[\beta^{-n}\right]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$.

**Proposition 2.2.3**

**1-** Soit $h : \Sigma^* \longrightarrow \Gamma^*$ est un homomorphisme, alors la congruence associée à $h$, notée $\equiv_h$, est définie par :

$$\forall u, v \in \Sigma^*, u \equiv_h v \Longleftrightarrow h(u) = h(v).$$

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

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

**Proposition 2.2.4**

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 $\varepsilon$.

Soient $\Sigma = \{\alpha_{x_i}, x_i \in M, 1 \leq i \leq n\}$ et la relation $\mathcal{R} = \left\{(\alpha_{x_i}\alpha_{x_j}, \alpha_{x_i x_j}), (\alpha_e, \varepsilon), x_i, x_j \in M\right\}$, où $\varepsilon$ 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 $w \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} \alpha_{x_k}$, où $x_k = x_i...x_j$.

Finalement on a $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} = \left\{[w_{x_k}]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}, x_k \in M, 1 \leq k \leq n\right\}$, et par suite on définit l'isomorphisme $\Psi$ comme suit: $\Psi : M \longrightarrow \Sigma^*/\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$, $\Psi(x_k) = [w_{x_k}]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$, où $x_k = x_i...x_j$, $w = \alpha_{x_i}...\alpha_{x_j}$, $\{x_i, ..., x_j\} \subseteq M$.

Montrons que $\Psi$ est un homomorphisme de monoïdes.

Pour $(x_k, x_l) \in M^2$, on a $\Psi(x_k x_l) = \Psi(x_m) = [w_{x_m}]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$, où $x_m = x_k x_l$ et $w = \alpha_{x_k}\alpha_{x_l}$, donc $[w_{x_m}]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} = [\alpha_{x_k}\alpha_{x_l}]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} = [\alpha_{x_k}]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}[\alpha_{x_l}]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} = \Psi(x_k)\Psi(x_l)$.

La surjectivité de $\Psi$ est triviale étant donnée que $\Psi([w_{x_k}]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}) = x_k$.

Pour l'injectivité de $\Psi$, 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 :

$$\begin{aligned}\Psi(x_i...x_j) = \Psi(x_s...x_t) &\Longrightarrow \left[\alpha_{x_i}...\alpha_{x_j}\right]_{\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}} = \left[\alpha_{x_s}...\alpha_{x_t}\right]_{\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}} \\ &\Longrightarrow \left[\alpha_{x_i...x_j}\right]_{\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}} = \left[\alpha_{x_s...x_t}\right]_{\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}} \\ &\Longrightarrow x_i...x_j = x_s...x_t \\ &\Longrightarrow x_k = x_l.\end{aligned}$$

**Exemple 2.2.5**

Considérons 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 Cayly de $M$ est définit par :

| $\cdot$ | $x_0$ | $x_1$ | $x_2$ |
|---|---|---|---|
| $x_0$ | $x_0$ | $x_1$ | $x_2$ |
| $x_1$ | $x_1$ | $x_1$ | $x_2$ |
| $x_2$ | $x_2$ | $x_1$ | $x_2$ |

.

Le monoïde $M$ satisfait les deux propriétés suivantes :

pour tout $x_i \in M$, $x_i \cdot x_1 = x_1$ et $x_i \cdot x_2 = x_2$.

Soit $\Sigma = \{\alpha_{x_i}, x_i \in M, 0 \leq i \leq 2\}$ et $\mathcal{R} = \{(\alpha_{x_0}, \varepsilon), (\alpha_{x_i}\alpha_{x_j}, \alpha_{x_i x_j}),\ x_i, x_j \in M\}$, donc pour tout $w \in \Sigma^*$, il existe $\{x_i, ..., x_j\} \subseteq M$, tels que :

$w = \alpha_{x_i}...\alpha_{x_j}$, et $w \underset{\mathcal{R}}{\overset{*}{\leftrightarrow}} \alpha_{x_k}$, où $x_k = x_i...x_j$. On distingue les trois cas suivants :

- si $w = u\alpha_{x_1}$, $u \in \Sigma^*$, dans ce cas on a $w \underset{\mathcal{R}}{\overset{*}{\leftrightarrow}} \alpha_{x_1}$.
- si $w = u\alpha_{x_2}$, $u \in \Sigma^*$, dans ce cas on a $w \underset{\mathcal{R}}{\overset{*}{\leftrightarrow}} \alpha_{x_2}$.
- si $w = \alpha_{x_0}...\alpha_{x_0}$, dans ce cas on a $w \underset{\mathcal{R}}{\overset{*}{\leftrightarrow}} \varepsilon$.

Donc $\Sigma^*/\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}} = \left\{ [\varepsilon]_{\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}}, [\alpha_{x_1}]_{\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}}, [\alpha_{x_2}]_{\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}} \right\}$, par conséquent on peut définir l'isomorphisme $\lambda$ comme suit : $\lambda : M \longrightarrow \Sigma^*/\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}$ .

$\lambda(x_0) = [\varepsilon]_{\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}}$ , $\lambda(x_1) = [\alpha_{x_1}]_{\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}}$ , $\lambda(x_2) = [\alpha_{x_2}]_{\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}}$.

Finalement $M \cong \Sigma^*/\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}$.

## 2.3 Quelques propriétés sur la présentation d'un monoïde

Les propositions qui suivants permettent de donner des conditions sur les relations qui assurent l'existence d'homomorphisme entre deux monoïdes quotient.

**Proposition 2.3.1**

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

**Démonstration**

Comme on a $[h(r)]_{\underset{\mathcal{R}_2}{\overset{*}{\leftrightarrow}}} = [h(s)]_{\underset{\mathcal{R}_2}{\overset{*}{\leftrightarrow}}}$ pour tout $(r, s) \in \mathcal{R}_1$, donc l'homomorphisme $p_2 \circ h$, vérifie la propriété suivante : pour tout $(r, s) \in \mathcal{R}_1$, $(p_2 \circ h)(r) = (p_2 \circ h)(s)$.

Donc, il existe un unique morphisme $\varphi$ de $\Sigma_1^*/ \underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}$ vers $\Sigma_2^*/ \underset{\mathcal{R}_2}{\overset{*}{\leftrightarrow}}$, avec $\varphi \circ p_1 = p_2 \circ h$.

**Exemple 2.3.2**

Considérons les deux monoïdes $\Sigma_1^*$ et $\Sigma_2^*$ ainsi que les deux relations $\mathcal{R}_1$ et $\mathcal{R}_2$,

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

Et soit $h$ le morphisme de $\Sigma_1^*$ dans $\Sigma_2^*$ défini par : $\begin{cases} h(\alpha) = \gamma\lambda. \\ h(\beta) = \mu. \end{cases}$

On a $p_2 : \Sigma_2^* \longrightarrow \Sigma_2^*/ \underset{\mathcal{R}_2}{\overset{*}{\leftrightarrow}}$ vérifie les égalités suivante : $p_2(\mu\gamma) = p_2(\gamma), p_2(\lambda\mu) = p_2(\lambda)$.

Maintenant 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 $\varphi$ de $\Sigma_1^*/ \underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}$ dans $\Sigma_2^*/ \underset{\mathcal{R}_2}{\overset{*}{\leftrightarrow}}$, avec $\varphi \circ p_1 = p_2 \circ h$.

**Proposition 2.3.3**

Soient $\langle \Sigma_1, \mathcal{R}_1 \rangle$ et $\langle \Sigma_2, \mathcal{R}_2 \rangle$ deux systèmes de réécriture convergents et $h : \Sigma_1^* \longrightarrow \Sigma_2^*$ un isomorphisme de monoïdes tels que $[h(r)]_{\underset{\mathcal{R}_2}{\overset{*}{\leftrightarrow}}} = [h(s)]_{\underset{\mathcal{R}_2}{\overset{*}{\leftrightarrow}}}$ et $h(Irr(\mathcal{R}_1)) \subseteq Irr(\mathcal{R}_2)$, on obtient dans ce cas :

$$\Sigma_1^*/ \underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}} \cong \Sigma_2^*/ \underset{\mathcal{R}_2}{\overset{*}{\leftrightarrow}}.$$

**Démonstration**

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

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

Plus précisément l'homomorphisme $\varphi$ est défini par : $\varphi([x]_{\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}}) = [h(x)]_{\underset{\mathcal{R}_2}{\overset{*}{\leftrightarrow}}}$.

Montrons que $\varphi$ est injectif.

Soient $[x]_{\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}}, [y]_{\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}} \in \Sigma_1^*/\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}$, comme $\langle \Sigma_1, \mathcal{R}_1 \rangle$ est convergent, alors il existe $(u,v) \in Irr(\mathcal{R}_1)$ tels que : $([x]_{\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}} = [u]_{\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}}$ et $[y]_{\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}} = [v]_{\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}})$.

Donc $\varphi([x]_{\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}}) = \varphi([y]_{\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}}) \Longleftrightarrow \varphi([u]_{\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}}) = \varphi([v]_{\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}})$

$\Longleftrightarrow [h(u)]_{\underset{\mathcal{R}_2}{\overset{*}{\leftrightarrow}}} = [h(v)]_{\underset{\mathcal{R}_2}{\overset{*}{\leftrightarrow}}}$.

Comme $h(Irr(\mathcal{R}_1)) \subseteq Irr(\mathcal{R}_2)$ et $\langle \Sigma_2, \mathcal{R}_2 \rangle$ est convergent on a $h(u) = h(v)$ et par suite $u = v$ car $h$ est injectif ce qui montre qu'on a bien $[x]_{\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}} = [y]_{\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}}$.

Enfin, d'après la surjectivité de $h$, l'homomorphisme $\varphi$ est surjectif car pour tout $y \in \Sigma_2^*, \exists x \in \Sigma_1^*$, avec $y = h(x)$ ce qui permet à écrire $[y]_{\underset{\mathcal{R}_2}{\overset{*}{\leftrightarrow}}} = [h(x)]_{\underset{\mathcal{R}_2}{\overset{*}{\leftrightarrow}}} = \varphi([x]_{\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}}})$.

Finalement on a bien $\Sigma_1^*/\underset{\mathcal{R}_1}{\overset{*}{\leftrightarrow}} \cong \Sigma_2^*/\underset{\mathcal{R}_2}{\overset{*}{\leftrightarrow}}$.

**Exemple 2.3.4**

Considérons les deux monoïdes $\Sigma_1^*$ et $\Sigma_2^*$ ainsi que les deux relations $\mathcal{R}_1$ et $\mathcal{R}_2$,

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

Et soit $h$ le morphisme de longueur de $\Sigma_1^*$ dans $\Sigma_2^*$ défini par : $w \longmapsto |w|$, il est clair que $h$ est bijectif .

Maintenant on montre que $(p_2 \circ h)(\alpha\alpha) = (p_2 \circ h)(\varepsilon)$.

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

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

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

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

**Proposition 2.3.5**

Soit $h : \Sigma^* \longrightarrow M$ un morphisme de monoïdes et $\mathcal{R}$ une relation binaire sur $\Sigma^*$ tel que $h(r) = h(s)$ pour tout $(r, s) \in \mathcal{R}$, alors pour tout $u \in \Sigma^*$, la congruence engendrée par $\mathcal{R}$ est inclus dans la congruence de la classe d'équivalence de $u$ modulo $\equiv_h$.

Autrement dit : $\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} \subseteq \equiv_{\overline{u}_{\equiv_h}}$ avec $\equiv_{\overline{u}_{\equiv_h}}$ 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 à l'homomorphisme $h$.

**Démonstration**

Comme $h(r) = h(s)$ pour tout $(r, s) \in \mathcal{R}$, on a $\mathcal{R} \subseteq \equiv_h$ et donc $\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} \subseteq \equiv_h$, i.e, $\Sigma^*/ \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$ est plus fine que $\Sigma^*/ \equiv_h$ et par conséquent pour tout $[u]_{\equiv_h} \in \Sigma^*/ \equiv_h$ il existe une famille de mots $\{v_i\}_{i \in I}$ de $\Sigma^*$ tel que $[u]_{\equiv_h} = \bigcup_{\in I} [v_i]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$.

Montrons maintenant que $\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} \subseteq \equiv_{[u]_{\equiv_h}}$. Soit $\left(w, w'\right) \in \Sigma^*$ tel que $w \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} w'$, on vérifie que pour tout $(x, y) \in \Sigma^*$, $\left(xwy \in [u]_{\equiv_h} \Longleftrightarrow xw'y \in [u]_{\equiv_h}\right)$.

On a $xwy \in [u]_{\equiv_h} = \bigcup_{\in I} [v_i]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} \Longleftrightarrow \exists i_0 \in I$ tel que : $xwy \in [v_{i_0}]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$, donc $xwy \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} v_{i_0}$.

De plus on a $w \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} w'$ implique que $xwy \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} xw'y$ car $\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$ est une congruence et par conséquent $xw'y \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} v_{i_0}$ ce qui montre $xw'y \in [v_{i_0}]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$ et donc $xw'y \in [u]_{\equiv_h} = \bigcup_{\in I} [v_i]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$.

De même manière on peut vérifier l'inverse.

Finalement $\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} \subseteq \equiv_{[u]_{\equiv_h}}$.

**Exemple 2.3.6**

Soient $\Sigma = \{\alpha, \beta\}$, et la relation $\mathcal{R} = \{(\alpha\beta, \beta\alpha)\}$ et $h : \Sigma^* \longrightarrow \mathbb{N}$ l'homomorphisme de longueur, on a pour tout $u \in \Sigma^*$, $[u]_{\equiv_h} = \{x \in \Sigma^* : |x| = |u|\}$, et le monoïde quotient $\Sigma^*/ \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} = \left\{ [\beta^n \alpha^m]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}, (n, m) \in \mathbb{N}^2 \right\}$.

Montrons que $\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} \subseteq \equiv_{[u]_{\equiv_h}}$.

Soit $(w, w') \in \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$, i.e, il existe $(p, q) \in \mathbb{N}^2$ tel que :

$w \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} \beta^p \alpha^q, w' \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} \beta^p \alpha^q$, 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 :

$$\begin{aligned} xwy \in [u]_{\equiv_h} &\Longleftrightarrow |xwy| = |u| \\ &\Longleftrightarrow |x| + |w| + |y| = |u|. \end{aligned}$$

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 même manière on peut vérifier l'inverse.

Enfin $\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} \subseteq \equiv_{[u]_{\equiv_h}}$.

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

**Proposition 2.3.7**

Soient $\Sigma = \{\sigma_1, \sigma_2, ..., \sigma_n\}$ un alphabet fini et la relation définie sur $\Sigma^*$ par $\mathcal{R} = \{(\sigma_i\sigma_i, \varepsilon), 1 \leq i \leq n\}$ où $\varepsilon$ est le mot vide. On obtient donc, le monoïde quotient $\Sigma^*/\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$ a une structure de groupe.

**Démonstration**

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

Soient $w = \sigma_{i_1}\sigma_{i_2}...\sigma_{i_k} \in \Sigma^*$ et $[w]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$ sa classe d'équivalence modulo $\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$, autrement dit $[w]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} \in \Sigma^*/\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$, 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 miroir de $w$). On a :

$$\begin{aligned}
[w]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}[\widetilde{w}]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} &= [(\sigma_{i_1}\sigma_{i_2}...\sigma_{i_k})]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}[(\sigma_{i_k}...\sigma_{i_2}\sigma_{i_1})]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} \\
&= [(\sigma_{i_1}\sigma_{i_2}...\sigma_{i_k}\sigma_{i_k}...\sigma_{i_2}\sigma_{i_1})]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} \\
&= \left[\left(\sigma_{i_1}\sigma_{i_2}...\sigma_{i_{k-1}}\right)\right]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}[(\sigma_{i_k}\sigma_{i_k})]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}\left[\left(\sigma_{i_{k-1}}...\sigma_{i_2}\sigma_{i_1}\right)\right]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} \\
&= \left[\left(\sigma_{i_1}\sigma_{i_2}...\sigma_{i_{k-1}}\right)\right]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}[\varepsilon]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}\left[\left(\sigma_{i_{k-1}}...\sigma_{i_2}\sigma_{i_1}\right)\right]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} \\
&= ...\,[(\sigma_{i_1}\sigma_{i_1})]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}} = [\varepsilon]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}.
\end{aligned}$$

**Exemple 2.3.8**

Soient $\Sigma = \{\sigma_1\}$ et la relation $\mathcal{R} = \{(\sigma_1\sigma_1, \varepsilon)\}$ où $\varepsilon$ est le mot vide.

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

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

| $\cdot$ | $[\varepsilon]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$ | $[\sigma_1]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$ |
|---|---|---|
| $[\varepsilon]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$ | $[\varepsilon]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$ | $[\sigma_1]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$ |
| $[\sigma_1]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$ | $[\sigma_1]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$ | $[\varepsilon]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$ |

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

# Chapitre 3

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

## Introduction

Dans ce chapitre, 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 système de Thue $S_1 = \langle \Sigma, \mathcal{R} \rangle$ pour lequel le problème du mot est indécidable en un système de Thue $S_2 = \langle \Delta, \mathcal{R}_\theta \rangle$ où $\theta \subseteq \Delta \times \Delta$ pour lequel le problème du mot est décidable en temps linéaire.

Contenu

## 3.1 Le protoccole ATS-monoïde

Le problème du mot dans le système $S = \langle \Sigma, \mathcal{R} \rangle$ est de pouvoir déterminer pour tous mots $u, v$ de $\Sigma^*$ s'il on a $u \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} v$. Il est bien connu que ce problème est indécidable en général c'est-à-dire il n'est pas possible de trouver un algorithme pour le résoudre ( problème a été soulevé en premier lieu par A. Thue (1914) et montrait qu'il indécidable par E. Post et A.A. Markov en (1974)) [12] .

Dans certains cas, le problème du mot peut être beaucoup plus facile. En effet, pour $\theta \subseteq \Sigma \times \Sigma$, nous dirons que :

$$u, v \in \Sigma^* \text{ sont congruents modulo } \theta, \text{ si, et seulement si, } u \overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}} v,$$

où $\overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}}$ est la fermeture d'équivalence de $\underset{\mathcal{R}_\theta}{\rightarrow}$ avec $\mathcal{R}_\theta = \{(ab, ba) : (a, b) \in \theta\}$.
Dans le système $S = \langle \Sigma, \mathcal{R}_\theta \rangle$, pour une taille fixée de $\Sigma$, R. V. Book et H. N. Liu ont montré [11] que le problème du mot est décidable en temps linéaire. Ce résultat est principalement basé sur le théorème suivant de R. Cori et D. Perrin[2].

**Définition 3.1.1**

Soit $\langle \Sigma, \mathcal{R} \rangle$ un semi-système de réécriture. Décider l'équivalence de deux mots modulo $\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$ 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 $\Sigma^*$, décider s'ils appartiennent à la même classe d'équivalence modulo la congruence $\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$.

**Exemple 3.1.2**

Soit $\Sigma = \{\alpha\}$, et la relation $\mathcal{R} = \{(\alpha^2, \varepsilon)\}$. $\forall w \in \Sigma^*$, on distingue deux cas :

- si $|w|$ est paire alors $w \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} \varepsilon$.
- si $|w|$ est impaire alors $w \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} \alpha$.

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

**Théorème 3.1.3**

Soient $u, v \in \Sigma^*, \theta \subseteq \Sigma \times \Sigma$ et un sous alphabet $\Delta \subseteq \Sigma$. Notons aussi $P_\Delta : \Sigma^* \longrightarrow \Delta^*$ la projection définie par :

$$\begin{cases} P_\Delta(\sigma) = \sigma, & \text{si } \sigma \in \Delta, \\ \qquad\qquad \text{et} \\ P_\Delta(\sigma) = \varepsilon, & \text{si } \sigma \notin \Delta. \end{cases}$$

Alors :

$$u \underset{\mathcal{R}_\theta}{\overset{*}{\leftrightarrow}} v \Longleftrightarrow \begin{cases} P_{\{\sigma\}}(u) = P_{\{\sigma\}}(v), \text{ pour tout } \sigma \text{ de } \Sigma, \\ \text{et} \\ P_{\{\sigma,\mu\}}(u) = P_{\{\sigma,\mu\}}(v), \text{ pour tout } (\sigma,\mu) \notin \theta. \end{cases}$$

**Démonstration** voir[6]

**Définition 3.1.4**

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

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

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

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

Par conséquent :

$$\forall\ u, v \in \Sigma^*, u \underset{\mathcal{R}}{\overset{*}{\leftrightarrow}} v \Longrightarrow h(u) \underset{\mathcal{R}_\theta}{\overset{*}{\leftrightarrow}} h(v).$$

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

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

Chiffrement **:** pour chiffrer un bit $b \in \{0, 1\}$, Alice choisit un mot $c$ de $\Sigma^*$ dans la classe d'équivalence de $w_b$ modulo $\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}$, i.e, $c \in [w_b]_{\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}}$ où $[w_b]_{\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}}$ désigne la classe de d'équivalence $w_b$ modulo $\underset{\mathcal{R}}{\overset{*}{\leftrightarrow}}$ est alors envoyé à Bob.

Déchiffrement **:** a la réception d'un mot $c$ de $\Sigma^*$, Bob calcule $h(c) \in \Delta^*$, comme $c \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} w_b$ et d'après la conséquence pour tout $u, v \in \Sigma^*, u \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} v \Longrightarrow h(u) \overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}} h(v)$ on a $h(c) \overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}} h(w_b)$, par exemple si $h(c) \overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}} x_0$ le message déchiffré est 0.

**Exemple 3.1.5**

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 :

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

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

Maintenant on vérifie les conditions suivantes :

1. $h(w_0)$ et $h(w_1)$ ne sont pas équivalent modulo $\overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}}$ ,
2. pour tout $(r, s) \in \mathcal{R}$ :

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

Pour la condition 1. Il suffit d'utilisé le théorème 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 $\overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}}$.

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 :

$(h(\sigma_2\sigma_3), h(\sigma_3\sigma_2)) = (ab, ba) \in \mathcal{R}_\theta$.

$(h(\sigma_2\sigma_4), h(\sigma_4\sigma_2)) = (ac, ca) \in \mathcal{R}_\theta$.

$(h(\sigma_1\sigma_3), h(\sigma_3\sigma_1)) = (b, b)$, (on a $h(\sigma_1\sigma_3) = h(\sigma_3\sigma_1)$).

Par conséquent :

$$\forall\ u, v \in \Sigma^*, u \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} v \Longrightarrow h(u) \overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}} h(v).$$

Chiffrement : par exemple pour chiffrer le 0, Alice choisit un mot $c$ de $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}^*$ dans la classe d'équivalence de $w_0$ modulo $\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$, i.e, $c \in [w_0]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$ où $[w_0]_{\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}}$ désigne la classe de $w_0$ modulo $\overset{*}{\underset{\mathcal{R}}{\leftrightarrow}}$ est alors envoyé à Bob.

On a $w_0 = \sigma_1\sigma_2\sigma_4\sigma_3\sigma_1\sigma_2\sigma_3\sigma_4 \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} \sigma_1\sigma_4\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3\sigma_4 \overset{*}{\underset{\mathcal{R}}{\leftrightarrow}} \sigma_1\sigma_4\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3\sigma_4$.

On choisit $c = \sigma_1\sigma_4\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3\sigma_4$.

Déchiffrement : a la réception d'un mot $c$ de $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}^*$, Bob calcule $h(c) = h(\sigma_1\sigma_4\sigma_3\sigma_2$ $\sigma_1\sigma_2\sigma_3\sigma_4) = cbaabc \in \{a, b, c\}^*$.

Maintenant en utilisant le théorème de R. Cori et D. Perrin, on vérifie que $h(c) \overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}} h(w_0)$.

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 $\sigma$ 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 $\theta$ 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 $h(c) \overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}} h(w_0) = x_0$ et le mot déchiffré est 0.

## 3.2 Sécurité de ATS monoïde

Une attaque contre ATS-monoïde ne permette pas de trouver exactement la clef secrète. Nous obtiendrons plutôt une clef qui lui est équivalente dans le sens suivant :

Nous dirons que $(\Delta', \mathcal{R}_{\theta'}, h' \in Hom(\Sigma^*, \Delta'^*))$ est une clef équivalente à la clef secrète $(\Delta, \mathcal{R}_\theta, h \in Hom(\Sigma^*, \Delta^*))$ 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:

- ▶ $h'$ est non trivial et $|\Delta'| \leq |\Sigma|$.
- ▶ $\forall (r,s) \in \mathcal{R}$, $\begin{cases} (h'(r), h'(s)) \in \{(ab, ba), (ba, ab)\}, \text{ pour une paire } (a,b) \in \theta', \\ \text{ou} \\ h'(r) = h'(s). \end{cases}$
- ▶ $h'(w_0)$ et $h'(w_1)$ ne sont pas équivalent modulo $\overset{*}{\underset{\mathcal{R}_{\theta'}}{\leftrightarrow}}$.

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

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

Donc 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 $(\Delta, \mathcal{R}_\theta, h \in Hom\,(\Sigma^*, \Delta^*))$ de complexité $|\mathcal{R}| \sum_{i=1}^{i=k} (i+1)^{|\Sigma|}$, avec $k = |\Delta|$.

**Algo − ATS − monoïde**

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 $\Delta_i$ un alphabet quelconque de $i$ lettres

Pour $h_i \in Hom(\Sigma^*, \Delta_i^*)$ faire

$\theta_i \longleftarrow \emptyset$

Pour $(r, s) \in \mathcal{R}$ 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 $\theta_i \longleftarrow \theta_i \cup \{(a, b)\}$

Si non Choisir un autre morphisme, i.e, Retourner à la deuxième boucle Pour

Fin Si

Fin Pour

Si $h_i(w_0)$ et $h_i(w_1)$ ne sont pas équivalents modulo $\overset{*}{\underset{\mathcal{R}_{\theta_i}}{\leftrightarrow}}$ alors

Retourner $(\Delta_i, \mathcal{R}_{\theta_i}, h_i \in Hom(\Sigma^*, \Delta_i^*))$

Fin Pour

Fin Pour

## 3.3 Quelques attaques contre ATS monoïde

Dans cette section on s'intéresse à quelques attaque contre ATS-monoïde c'est-à-dire dans chaque cas nous retournons une clef équivalente à la clef secrète de ce protocole.

**Corollaire 3.3.1** [8]

Soit $(\Sigma, \mathcal{R}, w_0, w_1)$ une clef publique de protocole ATS-monoïde.

Si $\forall (r, s) \in \mathcal{R}, |r| = |s|$, 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 secrète.

**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 $\sigma \in \Sigma, h_1(\sigma) = a \neq \varepsilon$.

2. $\forall (r,s) \in \mathcal{R}$, $h_1(r) = h_1(s) = (a)^{|r|} = (a)^{|s|}$.

3. Comme $\mathcal{R}_\theta = \emptyset$, alors $\overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}} = id_{\Sigma^*}$ et par conséquent $h_1(w_0)$ et $h_1(w_1)$ ne sont pas équivalent modulo $\overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}}$ 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 secrète.

**Corollaire 3.3.2**

Soit $(\Sigma, \mathcal{R}, w_0, w_1)$ une clef publique de protocole ATS-monoïde.

S'il existe $(r,s) \in \mathcal{R}$, $|r| \neq |s|$, alors $(\Delta_1 = \{a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ où $h_1(\Sigma) = \{a, \varepsilon\}$, est une clef équivalente à la clef secrète.

**Exemple 3.3.3**

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 $h_1(\sigma_1) = h_1(\sigma_3) = \varepsilon, h_1(\sigma_2) = h_1(\sigma_4) = h_1(\sigma_5) = a$ est vérifiée les conditions suivantes:

1. le morphisme $h_1$ est non trivial.
2. $\forall (r,s) \in \mathcal{R}, h_1(r) = h_1(s)$.
3. On a $h_1(w_0) = a^6$ et $h_1(w_1) = a^4$ et comme $\overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}} = id_{\Sigma^*}$, alors $h_1(w_0)$ et $h_1(w_1)$ ne sont pas équivalent modulo $\overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}}$.

Donc $(\Delta_1 = \{a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ est une clef équivalente à la clef secrète.

**Remarque 3.3.4**

Dans le Corollaire 3.3.2 Il existe des cas où le morphisme $h_1$ est trivial.

**Corollaire 3.3.5**

Soit $(\Sigma, \mathcal{R}, w_0, w_1)$ une clef publique de protocole ATS-monoïde.

S'il existe une lettre $\sigma_k$ de l'alphabet $\Sigma$ telle que pour tout $(r,s) \in \mathcal{R}, |r|_{\sigma_k} = |s|_{\sigma_k} = 0$, alors $(\Delta_1 = \{a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ où pour tout $\sigma \in \Sigma$ avec $\sigma \neq \sigma_k, h_1(\sigma) = \varepsilon$ et $h_1(\sigma_k) = a$, est une clef équivalente à la clef secrète.

**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 $h_1(\sigma_k) = a \neq \varepsilon$.

2. $\forall (r,s) \in \mathcal{R}, h_1(r) = h_1(s) = \varepsilon$.

3. Comme $\mathcal{R}_\theta = \emptyset$, alors $\overset{*}{\underset{\mathcal{R}_\theta}{\leftrightarrow}} = id_{\Sigma^*}$, donc il doit vérifiée que $h_1(w_0) \neq h_1(w_1)$.

**Remarque 3.3.6**

Dans le Corollaire 3.3.5 Il existe des cas où le morphisme $h_1(w_0) = h_1(w_1)$.

# Conclusion

Nous avons présenté dans ce travail une étude sur la congruence dans un monoïde libre aussi que certaines de leur propriétés, en étudiant au même temps une présentation de quelques monoïdes par générateurs et relations. Enfin, on s'intéresse au protocole ATS-monoïde. Plus précisément, on étudier des attaques contre ATS-monoïde dans des cas spécifiques et quelques exemples sur ces cas.

# Bibliographie


[1] P. Berlioux, M. Echenim et M. Lévy. "Théorie des langages", 30 novembre 2009.

[2] R. Cori et D. Perrin. "Automates et Commutations Partielles," RAIRO-Informatique théorique, tome19, n$^o$ 1, p.21-32, (1985).

[3] A. Demaille et F. Yvon. "Théorie des langages Notes de cours", Juin 2008.

[4] W. Diffie and M. E. Hellman. "New Direction in Cryptography", IEEE Trans, on Inform Theory, 22(6), pp. 644-665, (1976).

[5] M. Eytan et G. TH. Guilbaud. "Présentation de quelques monoïdes finis", Mathématiques et sciences humaines, vol 7, pp. 3-10, (1964).

[6] N. Ghadbane. "Systèmes de réécriture et le problème du mot dans un monoïde", Thèse de doctorat, Université de M'sila, (2017).

[7] N. Ghadbane and D. Mihoubi. "Presentation of monoids by generators and relations", Global and Stochastic Analysis (GSA), vol 3(2), (2016).

[8] 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).

[9] S. Lipschutz et M. L. Lipson. "Discrete Mathematics", Temple University, University of Virginia.

[10] S. Marcel."Langage formels et monoïdes finis", Séminaire Dubreil. Algèbre et thèorie des nombres, vol. 23, no. 2, pp. 1-3, (1970).

[11] L. Perret. "Etude d'outils algébriques et combinatoires pour la cryptographie à clef publique", thèse de doctorat, Universit´e de Marne–la–Vallée, (2005).

[12] E. Post. "Recursive unthenlvability of a problem of Thue", Journal of Symbolic Logic, 12(1):1-11, (1947).

[13] M. Rigo. "Théorie des automates et langages formels", (2009–2010).

[14] H. Rosen. "Cryptography Theory and Practice", Third Edition, Chapman and Hall/CRC, (2006).

[15] J. Vélu. "Méthode mathématique pour l'informatique", Paris, (2013).

## الملخص

هذه مذكرة ماستر رياضيات متقطعة، هي جزء من موافقات نصف الزمر وتطبيقاتها على أنظمة التشفير ذات المفاتيح المعلنة. في هذا العمل نتبع الخطوات التالية :

- التمهيدات.

- تمثيل بعض نصف الزمر بواسطة مولدات وعلاقات.

- دراسة نظام التشفير أساسه مسالة الكلمة في نصف الزمرة الحرة.



**الكلمات المفتاحية**

نصف الزمرة الحرة، تماثل نصف الزمرة الحرة، علاقة تكافئ مولدة بعلاقة، نصف أنظمة Thue، أنظمة التشفير ذات المفاتيح المعلنة .



## Résumé :

Ce mémoire de master mathématique discrète s'inscrit dans le cadre de la congruence dans un monoïde libre et leurs applications sur la cryptographie à clé publique. Dans ce travail, nous suivrons les étapes suivantes :

- Préliminaires.
- Présentation de quelques monoïdes par générateurs et relations.
- Etude d'un système de cryptage basé sur le problème du mot dans un monoïde libre.



## Mots clés :

Monoïde libre, morphisme de monoïdes, La fermeture d'une relation binaire, Cryptographie à clé publique, Système de Thue.



## Abstract:

This memory of master degree mathematics discrete lies within the scope of congruence of monoid and their applications on the public key cryptography. In this work, we will follow the following stages:

• Preliminaries
• Presentation of monoids by generators and relations.
•Some attacks of an encryption system based on the word problem in a monoid



## Key words:

Free monoid, morphism of monoids, the closure of a binary relation, public key cryptography, Thue System.