PEOPLE'S DEMOCRATIC REPUBLIC ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
Mohamed Boudiaf University of Msila
Faculty of Mathematics and Informatics
Department of Mathematics

Master of Mathematics

Mathematics and Informatics
Specialty: Mathematics
Option: Algebra and Discrete Mathematics

Theme

Syntactic relations on monoids and its applications

Presented by:

BENYOUNES Malika

Publicly presented on: 2022-2023

In front of the jury: .....

Mr. Douadi Mihoubi	Prof.	University of Msila	**President**.
Mr. Nacer Ghadbane	M. C. A.	University of Msila	**Supervisor**.
Mr. Lakhdar Heboub	M. A. A.	University of Msila	**Examiner**.

University year: 2022/2023

Acknowledgements

I can't begin and finish my work without thanking my praise and gratitude the greatest Allah the almighty who granted me strength and patience to complete this work.

First and foremost, I am indebted to my supervisor **Mr. Nacer Ghadbane** for here patience, valuable advice and guidance and consistent encouragement that she provided throughout this research, and for the excellent example he has provided as a successful male mathematician and Doctor, I am honored to have here throughout my thesis studies.

I am also deeply grateful to **Benchouikh Cheyma** for his help during the realization of this work and his remarks and suggestions which allowed me to finalize this thesis.

Finally, I would you like to extend my thanks and gratitude to my family for their help, support and patience, to all my loved ones my friends and to everyone who contributed to the completion of this work from near or from far.

Dedication

To the one woven my happiness with threads woven from her heart

"My Mother"

To the one who keeps the thorns away from my path of knowledge for me

"My Father"

To those who shared my childhood with them and loved me with sincerity and my support in life

"My Brothers"

To those who walked with me together as we paved the road to success together, here we are picking

the flower of our effort to

"My Friends and Colleagues"

To those who from their knowledge and success for me

"My Honorable Professors

Contents

Notations

Σ: Finite alphabet.

Σ^*: Free monoid on Σ.

$|w|_\sigma$: Number of occurrences of the letter σ in the word w.

$|w|$: Length of the word w.

$card$: Cardinal of a set.

$P(\Sigma^*)$: Set of languages over Σ.

$\mathcal{S}$: Semi-group.

$\mathcal{R}$: Binary relation.

$\mathcal{R}^0$: Identity relation.

$\mathcal{R}^n$: n_th composition of $\mathcal{R}$.

$\mathcal{R}^r$: Reflexive closure of $\mathcal{R}$.

$\mathcal{R}^s$: Symmetric closure of $\mathcal{R}$.

$\mathcal{R}^t$: Transitive closure of $\mathcal{R}$.

$\mathcal{S} = (\Sigma; \mathcal{R})$: A word rewriting semi system.

L: Language over alphabet Σ.

L^*: Iterative of a language L (or Kleen closure).

$\equiv$: Congruence.

$\cong$: Isomorphic.

$(Q^Q, \circ)$: Monoid of all functions from Q to Q.

$\Sigma^*/\sim_L$: Monoid quotient.

$Hom(\Sigma^*, \Delta^*)$: The set of monoid morphism between Σ^* and Δ^*.

$Iso(\Sigma^*, \Delta^*)$: The set of monoid isomorphism between Σ^* and Δ^*.

Introduction

Computational semi-group theory is an area of research that is subject to growing interest.

Congruence is an important part of semi-group theory.

A semi-group's congruence determine its homomorphic images in a manner analogous to a group's normal sub-group's.

The syntactic relation is widely used in computation theory due its applications in automate theory and regular languages.

This thesis is organized as four chapters:

In chapter 1: we begin with some elementary material concerning of binary relations and its properties, congruence semi-groups and public key cryptography.

In chapter 2: we present free monoid and we will give some results of languages and compatible relations on monoids.

In chapter 3: we will be studying presentation of monoid by generators and relations.

In chapter 4: we interested in the ATS-monoid (proposed by **P.J. Abish, D.G. Thomas** and **K.G. Subramanian**).

Chapter 1

Preliminaries

1.1 Introduction

This first chapter contains the definitions and properties of the tools that we will use later: Semi-group, Monoid, and finally The public Key cryptography.

Content:

1.2 Semi-group

Definition 1.1

A semi-group is a set $\mathcal{S}$ equipped with an internal law, i.e, with an application "." : $\mathcal{S} \times \mathcal{S} \to \mathcal{S}$, that satisfies the following one condition:

1. Associativity:

$$\forall x, y, z \in \mathcal{S} : (x \cdot y) \cdot z = x \cdot (y \cdot z).$$

Example 1.2

1. $(\mathbb{N}, +), (\mathbb{Z}, +)$ *are semi-groups.*

2. Let A and B be two nonempty sets. We define on $A \times B$ the law "$*$" as follows:

$$\forall (a, x) \in A \times B, \forall (b, y) \in A \times B, (a, x) * (b, y) = (a, y).$$

We show that $(A \times B, *)$ is a semi-group.

- *The law "$*$" is associative on $A \times B$.*

We have $((a, x) * (b, y)) * (c, z) = (a, y) * (c, z) = (a, z)$

and, $(a, x) * ((b, y) * (c, z)) = (a, x) * (b, z) = (a, z)$

Then, "$*$" is associative.

Definition 1.3

Let $(\mathcal{S}, \cdot)$ be a semi-group. A nonempty part $\mathcal{B}$ of $\mathcal{S}$ is called sub

semi-groups of $\mathcal{S}$ if it's "stable" for the operation " $\cdot$ ", i.e

$$\forall a, b \in \mathcal{B} : a \cdot b \in \mathcal{B}.$$

1.2.1 Congruence on a semi-group

Definition 1.4

Let $\mathcal{S}$ be a semi-group, a congruence on $\mathcal{S}$ is a stable equivalence relation $\mathcal{R}$ under right and left, i.e

$$\forall x, y, z \in \mathcal{S} : x\mathcal{R}y \ \Rightarrow \begin{cases} xz\mathcal{R}yz \\ zx\mathcal{R}zy \end{cases}$$

1.2.2 Homomorphism of semi-group

Definition 1.5

Let $(S, .)$ and $(T, *)$ be two semi-groups and $f : S \longrightarrow T$ a map. We call f a semi-group homomorphism if:

$$\forall a, b \in S : f(ab) = f(a) * f(b).$$

1.3 Monoid

Definition 1.6

A monoid $(\mathcal{M}, \cdot)$ consists a set $\mathcal{M}$ together with a binary operation " $\cdot$ " on $\mathcal{M}$ such that:

• $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $\forall (a, b, c) \in \mathcal{M}^3$ *(associativity).*

• *There exist an identity* $1_{\mathcal{M}} \in \mathcal{M}$ *such that* $a \cdot 1_{\mathcal{M}} = 1_{\mathcal{M}} \cdot a$, $\forall a \in \mathcal{M}$.

An element $m' \in \mathcal{M}$ *is said symmetric of the element* $m \in \mathcal{M}$ *if*

$$m.m' = m'.m = 1_{\mathcal{M}}.$$

Example 1.7

1. Let

$$\mathcal{K} = \left\{ \begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix}, s \in \mathbb{N}, m \in \mathbb{N} \right\}$$

1. We show that $(\mathcal{K}, \times)$ *is a monoid.*

• *The law " × " is internal on* $\mathcal{K}$.

Let

$$\begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix} \in \mathcal{K} \text{ and } \begin{pmatrix} 1 & 0 \\ s' & m' \end{pmatrix} \in \mathcal{K}$$

We have:

$$\begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ s' & m' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ s + ms' & mm' \end{pmatrix} \in \mathcal{K}$$

• *The law " × " (matrix product) is associative.*

• *The neutral element:*

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{K}$$

and $\forall A \in \mathcal{K}, A \times I_2 = I_2 \times A = A$.

Then, $(\mathcal{K}, \times)$ *is a monoid.*

Remark 1.8

1. A monoid $(\mathcal{M}, .)$ which is such that every element of $\mathcal{M}$ has a symmetric is a group.

2. Any group is a monoid but inverse is not always true.

1.3.1 Submonoid

Definition 1.9

Let $\mathcal{M}$ be a monoid and $\mathcal{N} \subseteq \mathcal{M}$. we say that $\mathcal{N}$ is a sub-monoid of $\mathcal{M}$ if:

1. $\mathcal{N} \subseteq \mathcal{M}$.

2. $1_{\mathcal{M}} = 1_{\mathcal{N}}$.

3. $\forall m, m' \in \mathcal{N} : m.m' \in \mathcal{N}$.

1.3.2 Congruence on a monoid

Let $(\mathcal{M}, ., 1_{\mathcal{M}})$ be a monoid, a congruence on $(\mathcal{M}, ., 1_{\mathcal{M}})$ is an equivalence relation denoted $\equiv$ stable by right and left multiplication, i.e:

$$\forall x, y, z \in \mathcal{M} : x \equiv y \Rightarrow (x.z \equiv y.z \text{ and } z.x \equiv z.y).$$

Definition 1.10

Let $\mathcal{M}$ be a monoid, and $\equiv$ a congruence defined on $\mathcal{M}$. The quotient $\mathcal{M}/\equiv$ is the monoid of the congruence classes of $\mathcal{M}$ for the equivalence relation $\equiv$, the composition law of $\mathcal{M}/\equiv$ is defined as

follows

$$\bar{u} *_{\mathcal{M}/\equiv} \bar{v} = \overline{(u *_{\mathcal{M}} v)}.$$

Example 1.11

We define on the monoid $(\mathbb{Z}, +)$ *the congruence relation modulo* n *by:*

$$x \equiv y[n] \Leftrightarrow \exists k \in \mathbb{Z}, x - y = k.n \qquad .$$

- *The relation* $\equiv$ *is reflexive: for all* $x \in \mathbb{Z}$*, we have*

$x - x = 0 = 0.n$*, then* $x \equiv x[n]$*.*

- *The relation* $\equiv$ *is symmetric: Let* $x, y \in \mathbb{Z}$*, suppose that* $x \equiv y[n]$*,*

i.e $\exists k \in \mathbb{Z}, x - y = k.n$*.*

Then, $\exists k \in \mathbb{Z}, y - x = (-k).n$*. So,* $y \equiv x[n]$*.*

- *The relation* $\equiv$ *is transitive: Let* $x, y, z \in \mathbb{Z}$*, suppose that*

$$\begin{cases} x \equiv y[n]. \\ y \equiv z[n]. \end{cases} \quad i.e \begin{cases} \exists k \in \mathbb{Z} \ : \ x - y = k.n \\ \exists l \in \mathbb{Z} \ : \ y - z = l.n \end{cases}$$

Then, $(x - z) = (k + l).n$*. So,* $x \equiv z[n]$*.*

- *The relation* $\equiv$ *is compatible with the monoid law.*

$x \equiv x'[n], \exists k \in \mathbb{Z}, x - x' = k.n$*.*

and

$y \equiv y'[n], \in l \in \mathbb{Z}, y - y' = l.n$*.*

So by addition: $x + y - (x' + y') = (k + l).n$*.*

Then, $x + y \equiv (x' + y')[n]$*.*

1.3.3 Homomorphism of monoid

Definition 1.12

Let $(\mathcal{M}, \cdot, 1_{\mathcal{M}})$ and $(N, *, 1_N)$ a two monoids, a homomorphism of monoid $h : \mathcal{M} \to N$ is a map that satisfies:

- $\forall x, y \in \mathcal{M} : h(x \cdot y) = h(x) * h(y)$.
- $h(1_{\mathcal{M}}) = 1_N$.

Definition 1.13

An isomorphism of monoids is simply a bijective monoid morphism.

Example 1.14

We consider the monoide $(\mathbb{N} \times \mathbb{N}, *)$ where the law " $*$ " is defined by $\forall (s, m), (s', m') \in \mathbb{N} \times \mathbb{N}, (s, m) * (s', m') = (s + sm', mm')$

Let the application:

$$h : (\mathbb{N} \times \mathbb{N}, *) \to (\mathcal{K}, \times)$$
$$(s, m) \to \begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix}$$

We show that h is isomorphism of monoid.

- *h is a morphism:*

Let $(s, m), (s', m') \in (\mathbb{N} \times \mathbb{N})$

We have:

$h((s, m) * (s', m')) = h((s + ms', mm'))$

$h((s,m)*(s',m')) =$

$$\begin{pmatrix} 1 & 0 \\ s+ms' & mm' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ s' & m' \end{pmatrix}$$

$h((s,m)*(s',m')) = h(s,m) \times h(s',m')$

• *h is bijective.*

1. h is injective.

Let $(s,m),(s',m') \in (\mathbb{N} \times \mathbb{N})$

we have: $h(s,m) = h(s',m')$

$\Leftrightarrow$

$$\begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ s' & m' \end{pmatrix}$$

$\Leftrightarrow$

$$\begin{cases} s = s' \\ m = m' \end{cases} \Leftrightarrow (s,m) = (s',m')$$

2. h is surjective.

Let $A \in \mathcal{K}$, *then*

$$A = \begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix}$$

we have: $h(s,m) = A$, *then h is surjective.*

Finally, h is isomorphism.

1.3.4 Action of a monoid on a set

Definition 1.15

An action of a monoid $\mathcal{M}$ on a set X is a function:

$$\mathcal{M} \times X \longrightarrow (g.x) \in X.$$

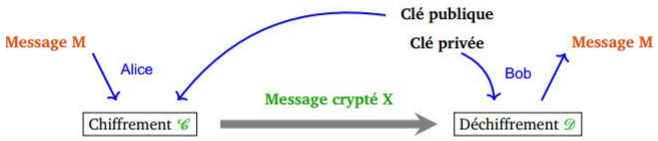
that takes a pair (g, x) of an element $x \in X$ and a monoid element $g \in \mathcal{M}$ to $(g, x) \in X$ such that:

- $(g_1.g_2).x = g_1.(g_2.x)$ *for all* $x \in X, g_1, g_2 \in \mathcal{M}$.
- $1_{\mathcal{M}}.x = x$ *for all* $x \in X$.

1.4 The Public key cryptography

The creation of public key cryptography by **Diffie** and **Hellman** in 1976 and the subsequent invention of the RSA public key cryptosystem by **Rivest**, **Shamir** and **Adleman** in 1978 are comma events in the long history of secret communications. Public key cryptography draws on many areas of mathematics, including number theory, abstract algebra, and information theory.

In public-key cryptography, a user U has a pair of related keys (pK,sK): the key pK is public and should be available to everyone, while the key sK must be kept secret by U. The fact that sK is kept secret by a single entity creates any asymmetry,hence the name asymmetric cryptography.



The essential steps are the following:

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.

2. Each system publishes its encryption key (public key) keeping its companion key private.

3. If **Alice** wishes to send a private message to **Bob**, **Alice** encrypts the message using **Bob's** public key.

4. When **Bob** receives the message, she decrypts it using her private key. No one else decrypt the message becauce only **Bob** knows its private key.

One-way function

Definition 1.16

• *A **one-way function** f is a function that maps a domain into range such that every function value has a unique inverse, with the condition that the calculation of the function is easy where the calculation of the inverse is infeasible:*

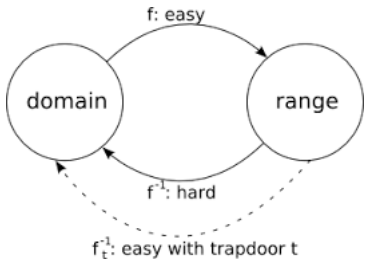
$$\begin{aligned} y &= f(x) \qquad easy \\ x &= f^{-1}(y) \qquad infeasible \end{aligned}$$

1. "Easy" is defined to mean a problem that can solved in polynomial as a function of input length (n). For example, the time to compute is proportional to n^a where a is a fixed constant.
2. "Infeasible" is not well defined however. Generally we can say that if the effort to solve is greater than polynomial time the problem is infeasible, if time to compute is proportional 2^n.

• *Trapdoor **one-way function** are a family of invertible functions f_t such that $y = f_t(x)$ is easy if t and x known, and $x = f_t^{-1}(y)$ is infeasible if y is known but t is not known.*

Remark 1.17

The development of a partical public-key scheme depends on the discovery of a suitable trapdoor one-way function.



Example 1.18

1. ***Discrete logarithm***

Let $(G, *)$ *be a cyclic group of order* n *and* g *a generator of* G *such that:*

$G =< g >, \exists g \in G$ *with* $|G| = n$

$G = \{ g, g^2, g^3, ..., g^k, ..., g^{k-1}, g^k = 1_G\}$

Let the function $f : [0, n-1] \longrightarrow G, k \longrightarrow f(k) = g^k$, f *is one-way if* G *is a cyclic group*

$y \in G \Rightarrow \exists n \in \mathbb{N} : y = g^k$.

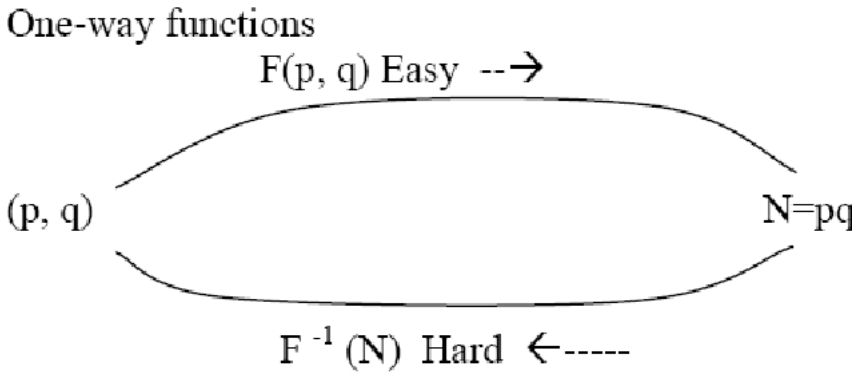
We have: $Log_g y = Log_g g^k = k$ *(Discrete logarithm)*

Solving $y = g^k$ *is difficult for secret* k *(this is the discrete logarithm problem) there are several algorithms to solve the discrete logarithm but they are all exponential in size* n *of* G.

2. ***The factorization of an integer***

Let (p, q) *be two very large prime numbers.*

It easy to calculate $N = p \times q$, *but it is very hard to find* (p, q) *primes.*


One-way functions
F(p, q) Easy --→
(p, q)
N=pq
F -1 (N) Hard ←-----

Chapter 2

Free monoid

2.1 Introduction

In this chapter, we will give some notes of words, languages and syntactic monoids.

Content:

2.2 Free monoid

Definition 2.1

An alphabet is a finite non empty set. The elements of an alphabet Σ *are called letters or symbols. A word over an alphabet* Σ *is a finite sequence of symbols of* Σ*. The set of all words on the alphabet* Σ *is denoted by* Σ^* *and is equipped with associative operation defined by the concatenation of two sequences* $\alpha_1\alpha_2...\alpha_n$ *and* $\beta_1\beta_2...\beta_m$ *is the sequence* $\alpha_1\alpha_2...\alpha_n\beta_1\beta_2...\beta_m$*.*

The string consisting of zero letters is called the empty word, written ϵ*. Thus* $\{\ \epsilon, \alpha, \beta, \alpha\alpha\beta\alpha, \alpha\alpha\alpha\beta\alpha\}$ *are words over alphabet* $\{\ \alpha, \beta\}$*. Thus the set* Σ^* *of words is equipped with the structure of a monoid. it's called the free monoid on* Σ*. The length of a word* w*, denoted* $|w|$*, is the number of letters in* w *when each letter is counted as many times as it occurs. Again by definition,* $|\epsilon| = 0$*.*

Example 2.2

1. $|\alpha\alpha\beta\alpha| = 4$ *and* $|\alpha\alpha\alpha\beta\alpha| = 5$*.*

2. Let w *be a word over an alphabet* Σ*. For* $\sigma \in \Sigma$*. The number of occurrences of* σ *in* w *shall be denoted by* $|w|_\sigma$*, for example,* $|\alpha\alpha\beta\alpha|_\beta = 1$ *and* $|\alpha\alpha\alpha\beta\alpha|_\sigma = 4$*.*

Proposition 2.3

Let Σ be any alphabet. The monoid Σ^* has the following two properties:

1. Any element of Σ^* is a finite sequence of elements of Σ.

2. Two distinct sequences of element of Σ define two distinct elements of Σ^*.

Proposition 2.4

Let Σ be an alphabet. Then,

1. The set Σ^* is infinite.

2. The set Σ^* is countable.

Proof 2.5

1. The set Σ^* is infinite indeed we have:

$$\Sigma^* = \cup_{n=0}^{\infty} \Sigma^n \ = \ \Sigma^0 \cup \Sigma \cup ...\Sigma^n \cup ...$$

2. We show that Σ^* is countable.

• *As Σ is finite, we can therefore number its elements, for example, if $\Sigma = \{ \alpha, \beta, \gamma\}$, then $n(\alpha) = 1, n(\beta) = 2, n(\gamma) = 3$.*

• *Then, let u be a word of Σ^*, we consider the lengths $|u|$ prime numbers, for example if $|u| = 5$, we have 5 the first prime numbers are $p(1) = 2, p(2) = 3, p(3) = 5, p(4) = 7, p(5) = 11$.*

• *We form the number $f(u) = \prod_{i=1}^{i=|u|} P(i)^{n(u(i))}$, where $u(i)$ designates the letter of u, for example if $u = \alpha\beta\alpha\alpha\alpha$, then*
$f(u) = \prod_{i=1}^{i=|u|} P(i)^{n(u(i))} = \prod_{i=1}^{i=5} P(i)^{n(u(i))} = 2^1 \times 3^3 \times 5^2 \times 7^2 \times 11^1$.

• *So we can define an application:*

$$\begin{aligned} f \ : \ \Sigma^* &\longrightarrow \mathbb{N} \\ u &\longrightarrow f(u) = \prod_{i=1}^{i=|u|} P(i)^{n(u(i))} \end{aligned}$$

by the uniqueness of the decomposition of an integer into prime factors, the map f is injective.
Finally, as f is injective and the set $\mathbb{N}$ is countable, then Σ^* is countable.

Definition 2.6

A morphism between two free monoids Σ^* and Δ^* is a map
$h : \Sigma^* \longrightarrow \Delta^*$ which satisfies:

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

Remark 2.7

1. Define a morphism h, it suffices to list all the words $h(\sigma)$, where a ranges over all the (finitely many) letters of Σ.
2. If $\mathcal{M}$ is a monoid, the any mapping $f : \Sigma \longrightarrow \mathcal{M}$ extends to a unique morphism $f : \Sigma^* \longrightarrow \mathcal{M}$. For instance, if $\mathcal{M}$ is the additive monoid $\mathbb{N}$, and f is defined by $f(\sigma) = 1$ for each $\sigma \in \Sigma$, then $f(u)$ is the length $|u|$ of the word u.
3. Let $h : \Sigma^* \longrightarrow \Delta^*$ be a morphism of monoids, if h is one-to-one and onto, then h is an isomorphism and the monoids Σ^* and Δ^* are isomorphism.

Example 2.8

1. Let $\Sigma = \{ \alpha_1, \alpha_2, ..., \alpha_n\}$ *be an alphabet,* $n \in \mathbb{N} \setminus \{ 0, 1\}$

Let:

$$\lambda : \Sigma \longrightarrow \mathbb{N}$$
$$\alpha_i \longrightarrow \lambda(\alpha_i)$$

We define:

$$\varphi : \Sigma^* \longrightarrow \mathbb{N}$$
$$\varphi(\omega) = \sum_{i=1}^{n} \lambda(\alpha_i)|\omega|_{\alpha_i}$$

We show that φ *is a morphism of monoids.*

• *Let* $u, v \in \Sigma^*$, *we have:*

$\varphi(uv) = \sum_{i=1}^{n} = \lambda(\alpha_i)(|u|_{\alpha_i} + |v|_{\alpha_i})$.

$\varphi(uv) = \sum_{i=1}^{n} \lambda(\alpha_i).|u|_{\alpha_i} + \sum_{i=1}^{n} \lambda(\alpha_i).|v_{\alpha_i}|$.

$\varphi(uv) = \varphi(u) + \varphi(v)$.

• *Also, we have:*

$\varphi(\epsilon) = \sum_{i=1}^{n} \lambda(\alpha_i).|\epsilon|_{\alpha_i}$ $(|\epsilon| = 0)$.

$\varphi(\epsilon) = \sum_{i=1}^{n} \lambda(\alpha_i).0 = 0$.

Definition 2.9

If $f : A^* \longrightarrow B^*$ *is a morphism of monoids, Then* $Kerf$ *is a congruence defined by:*

$$\forall u, v \in \Sigma^* : uKerfv \Leftrightarrow f(u) = f(v).$$

Proposition 2.10

Let $\mathcal{M}$ be any monoid and f is a mapping from an alphabet Σ into $\mathcal{M}$. There exists a unique homomorphism $\tilde{f}$ from Σ^* into $\mathcal{M}$ which extends f, i.e

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

Proof 2.11

• *Existence: let's put*

$\tilde{f}(\epsilon) \ = \ 1_{\mathcal{M}}$ *and* $\tilde{f}(\alpha_1\alpha_2, ..., \alpha_n) \ = \ f(\alpha_1)f(\alpha_2)...f(\alpha_n), n \in \mathbb{N}, \alpha_i \in \Sigma, 1 \leqslant i \leqslant n$

And easy to see that $\tilde{f}$ is indeed a homomorphism.

• *Uniqueness: Let $\tilde{f}$ and $\tilde{g}$ be two homomorphism from Σ^* to $\mathcal{M}$ such that:*

$\forall \alpha \in \Sigma, \tilde{f}(\alpha) = \tilde{g}(\alpha)$ *and* $\tilde{f}(\epsilon) = \tilde{g}(\epsilon) = 1_{\mathcal{M}}$ *and for any word* $w = \{\ \alpha_1\alpha_2, ..., \alpha_n\} \in \Sigma^*$.

We have:

$\tilde{f}(w) = \tilde{f}(\alpha_1\alpha_2, ..., \alpha_n)$.

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

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

$\tilde{f}(w) = \tilde{g}(w)$.

2.3 Words and languages

Definition 2.12

Let Σ be an alphabet. We call formal language any subset $L \subseteq \Sigma^*$.

Remark 2.13

Σ^* is the largest language over Σ in the sense of inclusion.

Example 2.14

1. $L^0 = \{\ \epsilon\}$ is the language containing the single word ϵ.

2. $L = \varnothing$ is the empty language.

3. Consider the alphabet $\Sigma = \{\ a, b, c\}$. The set $L = \{\ \epsilon, a, aa, bbc, ccca, aba, bab\}$ is a finite language.

Definition 2.15

Language being sets, we can apply the operations defined by:

• *The union of two language L_1 and L_2 is the languages, denoted $L_1 \cup L_2$*

$$L_1 \cup L_2 = \{\ x : x \in L_1 \text{ or } x \in L_2\}.$$

• *The intersection of two languages L_1 and L_2 is the languages, denoted $L_1 \cap L_2$*

$$L_1 \cap L_2 = \{\ x : x \in L_1 \text{ and } x \in L_2\}.$$

• *The difference of two languages L_1 and L_2 is the languages, denoted $L_1 - L_2$*

$$L_1 - L_2 = \{\ x : x \in L_1 \text{ and } X \notin L_2\}.$$

- *The complement of L is the language, denoted L^c*

$$L^c = \{\ x : x \notin L\}.$$

Definition 2.16

For $L \subseteq \Sigma^*$, L^+ denotes the language

$$L^+ \ = \ L \cup L^2 \cup \ ... \cup L^n \cup ...$$

We definite the star (Known as of Kleene) of L by:

$$L^* \ = \ L^+ \ \cup \{\ \epsilon\}$$

Example 2.17

With $\Sigma = \{\ a, b\}$, let us set $L_1 = \{\ a, b\}$ and $L_2 = \{\ ab\}$ when then have $L_1 L_2 = \{\ aab, bab\}$ and $L_2^* = \{\ \epsilon, ab, abab, ...\}$.

Definition 2.18

Let Σ be an alphabet. The family of rational language denoted $Rat(\Sigma^*)$ is the smallest language family of Σ^* satisfying the following conditions:

- $\varnothing \in Rat(\Sigma^*)$.
- $\forall \sigma \in \Sigma : \{\ \sigma\} \in Rat(\Sigma^*)$.
- *$Rat(\Sigma^*)$ is closed (stable) by union and finite products, i.e: $\forall L_1, L_2 \in Rat(\Sigma^*) : L_1 \cup L_2$ and $L_1 L_2$ are also in $Rat(\Sigma^*)$.*
- $\forall L \in Rat(\Sigma^*), L^* \in Rat(\Sigma^*)$. *(The star closure).*

2.4 Syntactic monoids

Definition 2.19

Let Σ be an alphabet. For any subset L of Σ^*, we call context of $w \in \Sigma^*$ the set

$$c(w) \ = \ \{(u,v) \in (\Sigma^*)^2 \ : \ uwv \in L\}.$$

The relation $\equiv_L$ defined on Σ^* by:

$$w \equiv_L w' \ \Leftrightarrow c(w) \ = \ c(w') \Leftrightarrow \forall u, v \in \Sigma^* \ : \ (uwv \in L \Leftrightarrow uw'v \in L).$$

is called the syntactic congruence of L.

Definition 2.20

If $L \subseteq \Sigma^*$ is a language over Σ, The quotient monoid $\Sigma^*/\equiv_L$ is called the syntactic monoid of L and denoted by $syn(L)$.

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

$\Sigma^*/\equiv_L = \{ \ \bar{u}, u \in \Sigma^*\}$.

$(\Sigma^*/\equiv_L, \odot)$ *is the syntactic monoid of L where " $\odot$ " is defines by*

$$\odot : \Sigma^*/\equiv_L \times \Sigma^*/\equiv_L \rightarrow \Sigma^*/\equiv_L$$
$$(\bar{u}, \bar{v}) \rightarrow \bar{u} \odot \bar{v} = \overline{(u,v)}$$

Example 2.21

Let $\Sigma = \{ 0, 1\}$ *and let's two languages.*

$L = \{ w \in \{ 0, 1\}^* : |w|_1 \equiv 0[2]\}$ *and* $L' = \{ w \in \{ 0, 1\}^* : |w|_1 \equiv 1[2]\}$.

We calculate the syntactic monoid of L.

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

$u \equiv_L v \Leftrightarrow (\forall x, y \in \Sigma^* : |xuy|_1 \equiv 0[2] \Leftrightarrow |xvy|_1 \equiv 0[2])$.

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

Then, $\Sigma^*/ \equiv_L = \{ [w]/w \in \Sigma^*\}$, *such that:* $[w] = \{ u \in \Sigma^*/u \equiv_L v\}$.

• *Let* $w \in L$, *then:*

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

$[w] = L$.

• *Let* $w \in L'$, *then:*

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

$[w] = L'$.

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

Chapter 3

Presentation of monoid by generators and relations

3.1 Introduction

In this chapter, we will study the closure of relation, the congruence generated by a relation and some properties of presentation by generators and relations.

Content:

3.2 Closure of relation.

3.3 The congruence generated by a relation.

3.4 Some properties of presentation by generators and relations.

3.2 Closure of relation

Definition 3.1

A binary relation on Σ^* *is a subset* $\mathcal{R} \subseteq \Sigma^* \times \Sigma^*$. *If* $(x, y) \in \mathcal{R}$, *we say that* x *is related to* y *by* $\mathcal{R}$, *denoted* $x\mathcal{R}y$. *The inverse relation of* $\mathcal{R}$ *is the binary relations* $\mathcal{R}^{-1} \subseteq \Sigma^* \times \Sigma^*$ *defined by* $\{\ y\mathcal{R}^{-1}x \Leftrightarrow (x, y) \in \mathcal{R}\}$. *The relation* $I_{\Sigma^*} = \{\ (x, x) : x \in \Sigma^*\}$ *is called the identity relation. The relation* $(\Sigma^*)^2$ *is called the complete relation.*

Definition 3.2

Let $\mathcal{R} \subseteq \Sigma^* \times \Sigma^*$ *and* $\mathcal{S} \subseteq \Sigma^* \times \Sigma^*$ *two a binary relations. The composition of* $\mathcal{R}$ *and* $\mathcal{S}$ *is a binary relation* $\mathcal{S} \circ \mathcal{R} \subseteq \Sigma^* \times \Sigma^*$ *defined by:*

$$x(\mathcal{S} \circ \mathcal{R})z \Leftrightarrow \exists y \in \Sigma^* \text{ such that } x\mathcal{R}y \text{ and } y\mathcal{S}z.$$

Definition 3.3

The relation $\mathcal{R}$ *is called an equivalence relation if, it's reflexive, symmetric, and transitive. and in this case, if* $x\mathcal{R}y$, *we say that* x *and* y *are equivalent.*

Proposition 3.4

Let $\mathcal{R}$ *be a relation on a set* Σ^*. *The Reflexive closure of* $\mathcal{R}$ *is the smallest reflexive relation* $\mathcal{R}^r$ *on* Σ^* *that contains* $\mathcal{R}$, *that is*

1. $\mathcal{R} \subseteq \mathcal{R}^r$.
2. *If* $\mathcal{R}'$ *is a reflexive relation on* Σ^* *and* $\mathcal{R} \subseteq \mathcal{R}'$, *then* $\mathcal{R}^r \subseteq \mathcal{R}'$.
3. $\mathcal{R}^r = \mathcal{R} \cup I_{\Sigma^*}$ *or* $I_{\Sigma^*} = \{\ (x, x), x \in \Sigma^*\}$.

• *The Symmetric closure of* $\mathcal{R}$ *is the smallest symmetric relation* $\mathcal{R}^s$ *on* Σ^* *that contains* $\mathcal{R}$*,that is*

1. $\mathcal{R} \subseteq \mathcal{R}^s$.

2. If $\mathcal{R}'$ *is a symmetric relation on* Σ^* *and* $\mathcal{R} \subseteq \mathcal{R}'$*, then* $\mathcal{R}^s \subseteq \mathcal{R}'$.

3. $\mathcal{R}^s = \mathcal{R} \cup \mathcal{R}^{-1}$*, or* $\mathcal{R}^{-1}$ *is the inverse relation of* $\mathcal{R}$.

• *The Transitive closure of* $\mathcal{R}$ *is the smallest transitive relation* $\mathcal{R}^t$ *on* Σ^* *that contains* $\mathcal{R}$*, that is*

1. $\mathcal{R} \subseteq \mathcal{R}^t$.

2. If $\mathcal{R}'$ *is a transitive relation on* Σ^* *and* $\mathcal{R} \subseteq \mathcal{R}'$*, then* $\mathcal{R}^t \subseteq \mathcal{R}'$.

3. $\mathcal{R}^t = \cup_{k=1}^{\infty} \mathcal{R}^k, \mathcal{R}^0 = 1_{\Sigma^*}, \mathcal{R}^{k+1} = \mathcal{R} \circ \mathcal{R}^k = \mathcal{R}^k \circ \mathcal{R}$

Proof 3.5

1. $\mathcal{R}^r = \mathcal{R} \cup I_{\Sigma^*}$ *is the smallest relation containing* $\mathcal{R}$*:*

• *It's clear that* $\mathcal{R} \subseteq \mathcal{R}^r$.

• *the relation* $\mathcal{R}^r = \mathcal{R} \cup I_{\Sigma^*}$ *is reflexive :*

we have $(\forall x \in \Sigma^* : x(\mathcal{R} \cup I_{\Sigma^*})x)$.

If $\mathcal{R}'$ *is a reflexive relation on* Σ^* *and* $\mathcal{R} \subseteq \mathcal{R}'$*, then* $\mathcal{R}^r \subseteq \mathcal{R}'$.

We show that $\mathcal{R} \cup I_{\Sigma^*} \subseteq \mathcal{R}'$.

Let $(x, y) \in \mathcal{R} \cup I_{\Sigma^*}$.

if $(x, y) \in \mathcal{R}$*, we have* $(x, y) \in \mathcal{R}'$ *(because:* $\mathcal{R} \subseteq \mathcal{R}'$*).*

if $(x, y) \in I_{\Sigma^*}$*, we have* $(x, y) \in \mathcal{R}'$ *(because :* $\mathcal{R}'$ *is reflexive relation).*

2. $\mathcal{R}^s = \mathcal{R} \cup \mathcal{R}^{-1}$ *is the smallest relation containing* $\mathcal{R}$*:*

• *It's clear that* $\mathcal{R} \subseteq \mathcal{R}^s$.

• *We show that* $\mathcal{R}^s = \mathcal{R} \cup \mathcal{R}^{-1}$ *is symmetric relation:*

Let $(x, y) \in \Sigma^* \times \Sigma^*$, *xe show that*

$x(\mathcal{R} \cup \mathcal{R}^{-1})y \Rightarrow y(\mathcal{R} \cup \mathcal{R}^{-1})x.$

We have

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

$x(\mathcal{R} \cup \mathcal{R}^{-1})y \Rightarrow (x, y) \in \mathcal{R} \vee (x, y) \in \mathcal{R}^{-1}.$

$x(\mathcal{R} \cup \mathcal{R}^{-1})y \Rightarrow (y, x) \in \mathcal{R} \vee (y, x) \in \mathcal{R}^{-1}.$

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

$x(\mathcal{R} \cup \mathcal{R}^{-1})y \Rightarrow y(\mathcal{R} \cup \mathcal{R}^{-1})x.$

• *if* $\mathcal{R}'$ *is a symmetric relation on* Σ^* *and* $\mathcal{R} \subseteq \mathcal{R}'$, *then* $\mathcal{R}^s \subseteq \mathcal{R}'$.

We show that $\mathcal{R} \cup \mathcal{R}^{-1} \subseteq \mathcal{R}'$.

We have $\mathcal{R} \subseteq \mathcal{R}'$ *and* $\mathcal{R}^{-1} \subseteq \mathcal{R}'$, *then* $\mathcal{R} \cup \mathcal{R}^{-1} \subseteq \mathcal{R}'$, *then* $\mathcal{R}^s = \mathcal{R} \cup \mathcal{R}^{-1}$.

3. $\mathcal{R}^t = \cup_{n=1}^{\infty} \mathcal{R}^n$*is the smallest relation containing* $\mathcal{R}$*:*

• *It's clear* $\mathcal{R} \subseteq \mathcal{R}^t$.

• *We show that* $\mathcal{R}^t = \cup_{n=1}^{\infty} \mathcal{R}^n$ *is transitive relation.*

Let $x, y, z \in \Sigma^*$, *we suppose that*

$$\begin{cases} x(\cup_{n=1}^{\infty} \mathcal{R}^n)y \\ y(\cup_{n=1}^{\infty} \mathcal{R}^n)z \end{cases}$$

$\Rightarrow$ *i.e:*

$$\begin{cases} (x, y) \in \mathcal{R}^n \\ (y, z) \in \mathcal{R}^n \end{cases}$$

$\Leftrightarrow$

$$\begin{cases} \exists i \in \mathbb{N}^* such\ as : (x,y) \in \mathcal{R}^i = \mathcal{R} \circ \mathcal{R} \circ ... \circ \mathcal{R}(i\ -times) \\ \exists k \in \mathbb{N}^* such\ as : (y,z) \in \mathcal{R}^k = \mathcal{R} \circ \mathcal{R} \circ ... \circ \mathcal{R}(k\ -times) \end{cases}$$

There is a dialing chain

We have $(x,z) \in \mathcal{R}^{i+k} \Rightarrow (x,z) \in \cup_{n=1}^{\infty} \mathcal{R}^n$

• *Let* $\mathcal{R}'$ *is a transitive relation on* Σ^* *and* $\mathcal{R} \subseteq \mathcal{R}'$*, show that* $\cup_{n=1}^{\infty} \mathcal{R}^n \subseteq \mathcal{R}'$

Let $\mathcal{R}'$ *be another transitive relation such as :* $\mathcal{R} \subseteq \mathcal{R}'$*, show that:* $\mathcal{R}^t = \cup_{n=1}^{\infty} \mathcal{R}^n \subseteq \mathcal{R}'$

let $(x,y) \in \cup_{n=1}^{\infty} \mathcal{R}^n$*, then*$\exists k \in \mathbb{N}^* such\ that : (x,y) \in \mathcal{R}^k$*, i.e*

$\exists (x_1, x_2, ..., x_{k-1}) \in \Sigma such\ that : (x\mathcal{R}x_1, x\mathcal{R}x_2, ...x_{k-2}\mathcal{R}x_{k-1})$

$\Rightarrow (x\mathcal{R}'x_1, x\mathcal{R}'x_2, ...x_{k-2}\mathcal{R}'x_{k-1})\ \mathcal{R} \subseteq \mathcal{R}'$

then: $\cup_{n=1}^{\infty} \mathcal{R}^n \subseteq \mathcal{R}' \Rightarrow \mathcal{R}^t = \cup_{n=1}^{\infty} \mathcal{R}^n$

Proposition 3.6

Let $\mathcal{R}$ *be a binary relation on a set* E *we have:*

• $(\mathcal{R}^r)^s = (\mathcal{R}^s)^r$.

• $(\mathcal{R}^r)^t = (\mathcal{R}^t)^r$.

• $(\mathcal{R}^t)^s \subseteq (\mathcal{R}^s)^t$.

Proof 3.7

Note that for any two binary relations $\mathcal{R}_1$ and $\mathcal{R}_2$ on the same set E, we have:

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

• *For any binary relation $\mathcal{R}$ on a set E, we have:* $(\mathcal{R}^0)^{-1} = \mathcal{R}^0$.

We have: $(\mathcal{R}^r)^s) = (\mathcal{R} \cup \mathcal{R}^0)^s) = (\mathcal{R} \cup \mathcal{R}^0) \cup (\mathcal{R} \cup \mathcal{R}^0) = \mathcal{R} \cup \mathcal{R}^0 \cup \mathcal{R}^{-1} \cup (\mathcal{R}^0)^{-1} = \mathcal{R} \cup \mathcal{R}^{-1} \cup \mathcal{R}^0 = \mathcal{R}^s \cup \mathcal{R}^0 = (\mathcal{R}^s)^r$

Then, $(\mathcal{R}^r)^s = (\mathcal{R}^s)^r$.

• *For any binary relation $\mathcal{R}$ on a set E, and for any integer n, we have:* $(\mathcal{R} \cup \mathcal{R}^0)^n = \cup_{k=0}^{n} \mathcal{R}^k$, *is written* $(\mathcal{R}^r)^t = (\mathcal{R} \cup \mathcal{R}^0)^t = \cup_{n=1}^{\infty} (\mathcal{R} \cup \mathcal{R}^0)^n = \cup_{n=1}^{\infty} \cup_{k=0}^{\infty} \mathcal{R}^k = (\cup_{n=1}^{\infty} \mathcal{R}^n) = (\cup_{n=1}^{\infty} \mathcal{R}^n) \cup \mathcal{R}^0 = (\mathcal{R}^t)^r$

Then, $(\mathcal{R}^r)^t = (\mathcal{R}^t)^r$.

• *We have:* $(\mathcal{R}^t)^s = (\cup_{n=1}^{\infty} \mathcal{R}^n) \cup (\cup_{n=1}^{\infty} \mathcal{R}^n)^{-1} = (\cup_{n=1}^{\infty} \mathcal{R}^n) \cup (\cup_{n=1}^{\infty} \mathcal{R}^{-n})$

from the fact that $\mathcal{R}^{-n}$ is the relation $(\mathcal{R}^{-1})^n$

by definition $(\mathcal{R}^s)^t = \cup_{n=1}^{\infty} (\mathcal{R} \cup \mathcal{R}^{-1})^n$

For any non-null integern, $\mathcal{R}^n$ and $\mathcal{R}^{-n}$ are contained in $(\mathcal{R} \cup \mathcal{R}^{-1})$, therefore in $(\mathcal{R}^s)^t$, therefore $\mathcal{R}^t$ and $(\mathcal{R}^{-1})$ are also contained in $(\mathcal{R}^s)^t$. Which indeed gives $(\mathcal{R}^t)^s \subseteq (\mathcal{R}^s)^t$.

3.3 Congruence generated by a relation

Definition 3.8

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:

• $xuy \leftrightarrow_{\mathcal{R}} xvy$, *whenever* $x, y \in \Sigma^*$ *and* $u\mathcal{R}v$ *or* $v\mathcal{R}u$.

• $w \leftrightarrow^*_{\mathcal{R}} w'$, *whenever* $u_0, u_1, ..., u_n \in \Sigma^*$ *with,* $u_0 = w, u_i \leftrightarrow_{\mathcal{R}} u_{i+1}, \forall 0 \leqslant i \leqslant n-1, u_n = w'$.

Definition 3.9

We consider the congruence generated by a relation denoted by $\leftrightarrow^*_{\mathcal{R}}$ *and*

$[w]_{\leftrightarrow^*_{\mathcal{R}}} = \{\ x \in \Sigma^* : x \leftrightarrow^*_{\mathcal{R}} w\}$ *be the equivalence class with respect to* $\leftrightarrow^*_{\mathcal{R}}$. *Hence, we can define the quotient monoid* $\Sigma^*/\leftrightarrow^*_{\mathcal{R}}$.

Definition 3.10

A presentation of a monoid $\mathcal{M}$ *is a pair* $S = (\Sigma, \mathcal{R})$ *such that* $\mathcal{M}$ *is isomorphic to the quotient of* Σ^* *by the congruence noted* $\leftrightarrow^*_{\mathcal{R}}$ *generated by* $\mathcal{R}$, *i.e:*

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

The element of Σ *are called generators, and those of* $\mathcal{R}$ *are called relations. If there are finitely many generators and relation, i.e:*
$\Sigma = \{\ a_1, a_2, ..., a_n\}$ *and* $\mathcal{R} = \{\ (r_1, r'_1), ..., (r_q, r'_q)\}$, *we say that the monoid* $\mathcal{M}$ *is finitely presentable, and we write*

$$\mathcal{M} \cong < a_1, ..., a_n / r_1 = r'_1, ..., r_q = r'_q > .$$

Example 3.11

1. Let $A = \{\ a, b\}$ *and* $\mathcal{R} = \{\ (ab, \epsilon), (ba, \epsilon)\}$, *for all* $w \in \{\ a, b\}^*$, *there is only three cases to be considered*

• *If* $|w|_a = |w|_b$, *in this case we have* $w \leftrightarrow^*_{\mathcal{R}} \epsilon$.

• *If* $|w|_a > |w|_b$, *i.e,* $|w|_a = |w|_b + k, k \in \mathbb{N} - \{ 0\}$, *in this case we have* $w \leftrightarrow^*_{\mathcal{R}} a^k$.

• *If* $|w|_b > |w|_a$, *i.e,* $|w|_b = |w|_a + l, l \in \mathbb{N} - \{ 0\}$, *in this case we have* $w \leftrightarrow^*_{\mathcal{R}} b^l$.

Then $\mathbb{Z} \cong \{ a, b\}^* / \leftrightarrow^*_{\mathcal{R}} = \{ [\epsilon]_{\leftrightarrow^*_{\mathcal{R}}}, [a^k]_{\leftrightarrow^*_{\mathcal{R}}}, (k, l) \in (\mathbb{N} - \{ 0\})^2\}$, *with the isomorphism* $\varnothing : \mathbb{Z} \to \{ a, b\}^* / \leftrightarrow^*_{\mathcal{R}}$ *defined by:* $0 \longmapsto [\epsilon]_{\leftrightarrow^*_{\mathcal{R}}}$, *if* $n > 0$, *then* $n \longmapsto [a^n]_{\leftrightarrow^*_{\mathcal{R}}}$, *if* $n < 0$, *then* $n \longmapsto [b^{-n}]_{\leftrightarrow^*_{\mathcal{R}}}$.

Therefore the monoid presented by $< a, b / ab = \epsilon, ba = \epsilon >$, *is isomorphism to the additive monoid* $(\mathbb{Z}, +)$.

3.4 Some properties of presentation by generators and relations

Proposition 3.12

Every finite monoid has a finite presentation.

Proof 3.13

Let $\mathcal{M} = \{ x_1, ..., x_n\}$ *be a finite monoid of cardinality* $n, n \in \mathbb{N}^*$ *and neutral element* $1_{\mathcal{M}}$.

Let $\Sigma = \{ \alpha_{x_i}, x_i \in \mathcal{M}, 1 \leqslant i \leqslant n\}$ *be the relation* $\mathcal{R} = \{ (\alpha_{x_i}, \alpha_{x_j}, \alpha_{x_i x_j})$, *where* ϵ *is the empty word, then for all* $w \in \Sigma^*, (\alpha_\epsilon, \epsilon), x_i, x_j \in \mathcal{M}$ *there exists* $\{ x_i, ..., x_j\} \subseteq \mathcal{M}$, *such that:*

$w = \{ \alpha_{x_i}, ..., \alpha_{x_j}\}$, *and* $w \leftrightarrow^*_{\mathcal{R}} \alpha_{x_k}$, *where* $x_k = \{ x_i, ..., x_j\}$.

Finally, we have $\Sigma^*/\leftrightarrow^*_{\mathcal{R}} = \{ [w_{x_k}]_{\leftrightarrow^*_{\mathcal{R}}}, x_k \in \mathcal{M}, 1 \leqslant k \leqslant n\}$, *and hence we defined isomorphism* ψ *as follows:*

$\psi : \mathcal{M} \longrightarrow \Sigma^*/\leftrightarrow^*_{\mathcal{R}}, \psi(x_k) = [w_{x_k}]_{\leftrightarrow^*_{\mathcal{R}}}$, *where*

$x_k = \{ x_i, ..., x_j\}, w = \alpha_{x_i}, ..., \alpha_{x_j}, \{ x_i, ..., x_j\} \subseteq \mathcal{M}$.

Let us show that ψ *is a homomorphism of monoids for* $(x_k, x_l) \in \mathcal{M}^2$, *we have* $\psi(x_k x_l) = \psi(x_m) = [w_{x_m}]_{\leftrightarrow^*_{\mathcal{R}}}$, *where* $x_m = x_k x_l$ *and* $w = \alpha_{x_k}\alpha_{x_l}$, *then* $[w_{x_m}]_{\leftrightarrow^*_{\mathcal{R}}} = [\alpha_{x_k}]_{\leftrightarrow^*_{\mathcal{R}}} \cdot [\alpha_{x_l}]_{\leftrightarrow^*_{\mathcal{R}}} = \psi(x_k)\psi(x_l)$.

The surjectivity of ψ *is trivial given that* $\psi([w_{x_k}]_{\leftrightarrow^*_{\mathcal{R}}}) = x_k$.

For the injectivity of ψ, *we have* $\forall (x_k, x_l) \in \mathcal{M}^2$, *there exists* $\{ x_i, ..., x_j\}, \{ x_s, ..., x_t\} \subseteq \mathcal{M} : x_k = \{ x_i, ..., x_j\}$ *and* $x_l = \{ x_s, ..., x_t\}$, *if* $\psi(x_k) = \psi(x_l)$, *then:*

$$\psi(x_i, ..., x_j) = \psi(x_s, ..., x_t) \Rightarrow [\alpha_{x_i}, ..., \alpha_{x_j}]_{\leftrightarrow^*_{\mathcal{R}}} = [\alpha_{x_s}, ..., \alpha_{x_t}]$$
$$\psi(x_i, ..., x_j) = \psi(x_s, ..., x_t) \Rightarrow x_i, ..., x_j = x_s, ..., x_t$$
$$\psi(x_i, ..., x_j) = \psi(x_s, ..., x_t) \Rightarrow x_k = x_l$$

Example 3.14

Consider the monoid

$$\mathcal{M} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, x_1 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, x_2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

provided with matrix multiplication. The Cayley table of $\mathcal{M}$ *is defined*

as follows (see Table 1):

$\cdot$	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

The monoid $\mathcal{M}$ satisfies the following two properties:

for all $x_i \in \mathcal{M}, x_i.x_1 = x_1$ and $x_i.x_2 = x_2$.

Let $A = \{\ a_{x_i}, x_i \in \mathcal{M}, 0 \leqslant i \leqslant 2\}$ and

$\mathcal{R} = \{\ (a_{x_0}, \epsilon), (a_{x_i}a_{x_j}, a_{x_ix_j}), x_i, x_j \in \mathcal{M}\}$.

Then for all $w \in \Sigma^*$, there exist $\{\ x_i, ..., x_j\} \subseteq \mathcal{M}$ such that

$w = \{\ a_{x_i}, ..., a_{x_j}\}$ and $w \leftrightarrow^*_{\mathcal{R}}$, with $x_k = \{\ x_i, ..., x_j\}$. There is only three cases to be considered:

- *If $w = ua_{x_1}, u \in \Sigma^*$, in this case we have $w \leftrightarrow^*_{\mathcal{R}} a_{x_1}$.*
- *If $w = ua_{x_2}, u \in \Sigma^*$, in this cases we have $w \leftrightarrow^*_{\mathcal{R}} a_{x_2}$.*
- *If $w = a_{x_0}, ..., a_{x_0}$, in this cases we have $w \leftrightarrow^*_{\mathcal{R}} \epsilon$.*

Then $\Sigma^*/\leftrightarrow^*_{\mathcal{R}} = \{\ [\epsilon]_{\leftrightarrow^*_{\mathcal{R}}}, [a_{x_1}]_{\leftrightarrow^*_{\mathcal{R}}}, [a_{x_2}]_{\leftrightarrow^*_{\mathcal{R}}}\}$ and we define the isomorphism $\lambda : \mathcal{M} \longrightarrow \Sigma^*/\leftrightarrow^*_{\mathcal{R}}$ by:

$\lambda(x_0) = [\epsilon]_{\leftrightarrow^*_{\mathcal{R}}}, \lambda(x_1) = [a_{x_1}]_{\leftrightarrow^*_{\mathcal{R}}}, \lambda(x_2) = [a_{x_2}]_{\leftrightarrow^*_{\mathcal{R}}}$.

Finally $\mathcal{M} \cong \Sigma^*/\leftrightarrow^*_{\mathcal{R}}$.

The following propositions, make it possible to give conditions on relations that ensure the existence of morphism between two monoids quotient.

Proposition 3.15

We consider two systems of rewriting $S_1 = (\Sigma_1, \mathcal{R}_1), S_2 = (\Sigma_2, \mathcal{R}_2)$

and $f : \Sigma_1^* \longrightarrow \Sigma_2^*$ *is a morphism of monoids such that for all* $(r, s) \in \mathcal{R}_1 : [f(r)]_{\leftrightarrow^*_{\mathcal{R}_2}} = [f(s)]_{\leftrightarrow^*_{\mathcal{R}_2}}$, *then there exists a unique morphism*
$\psi : \Sigma_1^*/\leftrightarrow^*_{\mathcal{R}_1} \longrightarrow \Sigma_2^*/\leftrightarrow^*_{\mathcal{R}_2}$ *with* $\psi \circ \pi_{\mathcal{R}_1} = \pi_{\mathcal{R}_2} \circ f$.

Proof 3.16

We have for all $(r, s) \in \mathcal{R}_1 : [f(r)]_{\leftrightarrow^*_{\mathcal{R}_2}} = [f(s)]_{\leftrightarrow^*_{\mathcal{R}_2}}$, *then the morphism* $\pi_{\mathcal{R}_2} \circ f$ *satisfies the following property:*
for all $(r, s) \in \mathcal{R}_1, (\pi_{\mathcal{R}_2} \circ f)(r) = (\pi_{\mathcal{R}_2} \circ f)(s)$, *then there exists a unique morphism*
$\psi : \Sigma_1^*/\leftrightarrow^*_{\mathcal{R}_1} \longrightarrow \Sigma_2^*/\leftrightarrow^*_{\mathcal{R}_2}$ *with* $\psi \circ \pi_{\mathcal{R}_1} = \pi_{\mathcal{R}_2} \circ f$.

Example 3.17

Let $S_1 = (\Sigma_1, \mathcal{R}_1)$ *and* $S_2 = (\Sigma_2, \mathcal{R}_2)$ *be two systems of rewriting, where,*

$$\begin{cases} \Sigma_1 = \{\ a, b\} \\ \mathcal{R}_1 = \{\ (ab, a), (ba, a) \end{cases} \quad and \quad \begin{cases} \Sigma_2 = \{\ c, d, e\} \\ \mathcal{R}_2 = \{\ (ec, c), (de, d)\} \end{cases}$$

We consider the morphism $f : \Sigma_1^* \longrightarrow \Sigma_2^*$, *with:*

$$\begin{cases} f(a) = cd \\ f(b) = e \end{cases}$$

We have $\pi_{\mathcal{R}_2} : \Sigma_2^*/\leftrightarrow^*_{\mathcal{R}_2}$ *satisfies following equalities:*
$\pi_{\mathcal{R}_2}(ec) = \pi_{\mathcal{R}_2}(c)$ *and* $\pi_{\mathcal{R}_2}(de) = \pi_{\mathcal{R}_2}(d)$.

Now we show that for all $(r,s) \in \mathcal{R}_1, (\pi_{\mathcal{R}_2} \circ f)(r) = (\pi_{\mathcal{R}_2} \circ f)(s)$, *we have*

$(\pi_{\mathcal{R}_2} \circ f)(ab) = \pi_{\mathcal{R}_2}(cde) = \pi_{\mathcal{R}_2}(c)\pi_{\mathcal{R}_2}(de) = \pi_{\mathcal{R}_2}(c)\pi_{\mathcal{R}_2}(d) = \pi_{\mathcal{R}_2}(cd)(\pi_{\mathcal{R}_2} \circ f)(a)$.

$(\pi_{\mathcal{R}_2} \circ f)(ba) = \pi_{\mathcal{R}_2}(ecd) = \pi_{\mathcal{R}_2}(ec)\pi_{\mathcal{R}_2}(d) = \pi_{\mathcal{R}_2}(c)\pi_{\mathcal{R}_2}(d) = \pi_{\mathcal{R}_2}(cd)(\pi_{\mathcal{R}_2} \circ f)(a)$.

Consequently there exists a unique morphism $\psi : \Sigma_1^*/\leftrightarrow_{\mathcal{R}_1}^* \longrightarrow \Sigma_2^*/\leftrightarrow_{\mathcal{R}_2}^*$ *with* $\psi \circ \pi_{\mathcal{R}_1} = \pi_{\mathcal{R}_2} \circ f$.

Proposition 3.18

Let $S_1 = (\Sigma_1, \mathcal{R}_1), S_2 = (\Sigma_2, \mathcal{R}_2)$ *be two systems canonical and* $f : \Sigma_1^* \longrightarrow \Sigma_2^*$ *is a isomorphism of monoids where for all* $(r,s) \in \mathcal{R}_1$: $[f(r)]_{\leftrightarrow_{\mathcal{R}_2}^*} = [f(s)]_{\leftrightarrow_{\mathcal{R}_2}^*}$ *and* $f(Irr(\mathcal{R}_1)) \subseteq Irr(\mathcal{R}_2)$, *we have,*

$$\Sigma_1^*/\leftrightarrow_{\mathcal{R}_1}^* \cong \Sigma_2^*/\leftrightarrow_{\mathcal{R}_2}^*$$

Proof 3.19

We have for all $(r,s) \in \mathcal{R}_1 : [f(r)]_{\leftrightarrow_{\mathcal{R}_2}^*} = [f(s)]_{\leftrightarrow_{\mathcal{R}_2}^*}$, *then for all* $(r,s) \in \mathcal{R}_1 : (\pi_{\mathcal{R}_2} \circ f)(r) = (\pi_{\mathcal{R}_2} \circ f)(s)$, *then there exists a unique morphism* $\psi : \Sigma_1^*/\leftrightarrow_{\mathcal{R}_1}^* \longrightarrow \Sigma_2^*/\leftrightarrow_{\mathcal{R}_2}^*$ *with* $\psi \circ \pi_{\mathcal{R}_1} = \pi_{\mathcal{R}_2} \circ f$.

Specifically the morphism ψ *is defined by:* $\psi([x]_{\leftrightarrow_{\mathcal{R}_1}^*}) = [f(x)]_{\leftrightarrow_{\mathcal{R}_2}^*}$.

We show that ψ *is one-to-one: Let* $[x]_{\leftrightarrow_{\mathcal{R}_1}^*}, [y]_{\leftrightarrow_{\mathcal{R}_1}^*} \in \Sigma_1^*/\leftrightarrow_{\mathcal{R}_1}^*$, *since* $S_1 = (\Sigma_1, \mathcal{R}_1)$ *is canonical, then there exists* $u, v \in Irr(\mathcal{R}_1)$ *such that* $[x]_{\leftrightarrow_{\mathcal{R}_1}^*} = [u]_{\leftrightarrow_{\mathcal{R}_1}^*}$ *and* $[y]_{\leftrightarrow_{\mathcal{R}_1}^*} = [v]_{\leftrightarrow_{\mathcal{R}_1}^*}$.

We have $\psi([x]_{\leftrightarrow_{\mathcal{R}_1}^*}) = \psi([y]_{\leftrightarrow_{\mathcal{R}_1}^*}) \Leftrightarrow \psi([u]_{\leftrightarrow_{\mathcal{R}_1}^*}) = \psi([v]_{\leftrightarrow_{\mathcal{R}_1}^*}) \Leftrightarrow [f(u)]_{\leftrightarrow_{\mathcal{R}_2}^*} =$

$[f(v)]_{\leftrightarrow^*_{\mathcal{R}_2}}$, *since* $f(Irr(\mathcal{R}_1)) \subseteq Irr(\mathcal{R}_2)$ *and* $S_2 = (\Sigma_2, \mathcal{R}_2)$ *is canonical, we have* $f(u) = f(v)$, *then* $u = v$ *because* f *is one-to-one, which shows that* $[x]_{\leftrightarrow^*_{\mathcal{R}_1}} = [y]_{\leftrightarrow^*_{\mathcal{R}_1}}$.

Now we show that ψ *is onto: since* f *is onto, then for all* $y \in \Sigma_2^*$, *there exists* $x \in \Sigma_1^*$ *such that* $y = f(x)$, *which to write* $[y]_{\leftrightarrow^*_{\mathcal{R}_2}} = [f(x)]_{\leftrightarrow^*_{\mathcal{R}_2}} = \psi([x]_{\leftrightarrow^*_{\mathcal{R}_1}})$.

Finally:

$$\Sigma_1^*/ \leftrightarrow^*_{\mathcal{R}_1} \cong \Sigma_2^*/ \leftrightarrow^*_{\mathcal{R}_2}$$

Example 3.20

Let $S_1 = (\Sigma_1, \mathcal{R}_1)$ *and* $S_2 = (\Sigma_2, \mathcal{R}_2)$ *be two systems of rewriting, where,*

$$\begin{cases} \Sigma_1 = \{\ a\} \\ \mathcal{R}_1 = \{\ (aa, \epsilon)\} \end{cases} \quad and \quad \begin{cases} \Sigma_2^* \ = \ \mathbb{N} \ = < 1 > \\ \mathcal{R}_2 \ = \ \{\ (0+0,0), (0+1,1), (1+0,1), (1+1,0)\} \end{cases}$$

We consider the isomorphism of length

$$\begin{aligned} f \ : \ \Sigma_1^* &\longrightarrow \mathbb{N} \\ w &\longrightarrow \ |w| \end{aligned}$$

We have $(\pi_{\mathcal{R}_2} \circ f)(aa) = \pi_{\mathcal{R}_2}(2) = \pi_{\mathcal{R}_2}(0) = (\pi_{\mathcal{R}_2} \circ f)(\epsilon)$, *and* $Irr(\mathcal{R}_1) = \{\ \epsilon, a\}, f(Irr(\mathcal{R}_1)) = \{\ 0, 1\} = Irr(\mathcal{R}_2)$.

Finally

$$\Sigma_1^*/ \leftrightarrow^*_{\mathcal{R}_1} \cong \mathbb{N}/ \leftrightarrow^*_{\mathcal{R}_2}$$

In the following proposition we give a condition on the relation of a

rewrite system to show that the congruence generated by this relation is included in the syntactic congruence class of any word modulo congruence associated morphism of monoids

Proposition 3.21

Let $f : \Sigma^* \longrightarrow \mathcal{M}$ *be a monoids morphism and* $\mathcal{R}$ *is a binary relation on a set* Σ^* *such that for all* $(r, s) \in \mathcal{R}, f(r) = f(s)$.
Then for all $w \in \Sigma^*$, *the congruence generated by* $\mathcal{R}$ *is included in the syntactic congruence of the equivalence class of* w *modulo* $Kerf$, *i.e*

$$\leftrightarrow^*_{\mathcal{R}} \subseteq \equiv_{[w]_{ker\ f}}$$

Proof 3.22

Since for all $(r, s) \in \mathcal{R}, f(r) = f(s)$, *we have* $\mathcal{R} \subseteq Kerf$, *then* $\leftrightarrow^*_{\mathcal{R}} \subseteq Kerf$.
Now we show that $\leftrightarrow^*_{\mathcal{R}} \subseteq \equiv_{[w]_{ker\ f}}$, *let* $(u, v) \in \Sigma^* \times \Sigma^*$ *such that* $u \leftrightarrow^*_{\mathcal{R}} v$, *we check that* $u \equiv_{[w]_{ker\ f}}$, *i.e,*
for all $(x, y) \in \Sigma^* \times \Sigma* : xuy \in [w]_{Kerf} \Leftrightarrow xvy \in [w]_{Kerf}$.
We have $xuy \in [w]_{Kerf} \Leftrightarrow xuy \in \cup_{i \in I} [c_i]_{\leftrightarrow^*_{\mathcal{R}}}$, *because* $\leftrightarrow^*_{\mathcal{R}} \subseteq Kerf \Leftrightarrow \exists i_0 \in I$ *such that* $xuy \in [c_{i_0}]_{\leftrightarrow^*_{\mathcal{R}}}$, *then* $xuy \leftrightarrow^*_{\mathcal{R}} c_{i_0}$.
Furthermore $u \leftrightarrow^*_{\mathcal{R}} v$ *implies that* $xuy \leftrightarrow^*_{\mathcal{R}} xvy$.
We have:

$$\begin{cases} xuy \leftrightarrow^*_{\mathcal{R}} c_{i_0} \\ xuy \leftrightarrow^*_{\mathcal{R}} xvy \end{cases} \Rightarrow xvy \leftrightarrow^*_{\mathcal{R}} c_{i_0} \text{ then } xvy \in [w]_{Kerf}$$

A similar argument shows that if $xvy \in [w]_{Kerf}$ *then* $xuy \in [w]_{Kerf}$. *Finally*

$$\leftrightarrow_{\mathcal{R}}^{*} \subseteq \equiv_{[w]_{ker\ f}}$$

Example 3.23

Let $\Sigma = \{\ a, b\}, \mathcal{R} = \{\ (ab, ba)\}$ *and*

$$\begin{aligned} f\ &:\ \Sigma^{*} \longrightarrow \mathbb{N} \\ &\quad f(u)\ =\ |u| \end{aligned}$$

We have $\Sigma^{*}/\ \leftrightarrow_{\mathcal{R}}^{*} = \{\ [b^{m}a^{n}]_{\leftrightarrow_{\mathcal{R}}^{*}}, (m,n) \in \mathbb{N} \times \mathbb{N}\}$ *and for all* $w \in \Sigma^{*}, [w]_{Kerf} = \{\ x \in \Sigma^{*} : |x| = |w|\}$.

Now we show that exists $(p,q) \in \mathbb{N} \times \mathbb{N} : u \leftrightarrow_{\mathcal{R}}^{*} b^{p}a^{q}$ *and* $v \leftrightarrow_{\mathcal{R}}^{*} b^{a}a^{q}$, *there* $(|u|_a = |v|_a = q)$ *and* $(|u|_b = |v|_b = p)$, *we check that* $u \equiv_{[w]_{Kerf}} v$, *i.e, for all* $(x,y) \in \Sigma^{*} \times \Sigma^{*} : xuy \in [w]_{Kerf} \Leftrightarrow xvy \in [w]_{Kerf}$.

Let $(x,y) \in \Sigma^{*} \times \Sigma^{*}$, *we have:*

$xuy \in [w]_{Kerf} \Leftrightarrow |xuy| = |w| \Leftrightarrow |xvy| = |w| \Leftrightarrow xvy \in [w]_{Kerf}$, *because* $(|u|_a = |v|_a = q)$ *and* $(|u|_b = |v|_b = q)$.

Finally

$$\leftrightarrow_{\mathcal{R}}^{*} \subseteq \equiv_{[w]_{ker\ f}}$$

In the following proposition we give also a specific relation $\mathcal{R}$ *on* Σ^{*} *making the quotient monoid* $\Sigma^{*}/\ \leftrightarrow_{\mathcal{R}}^{*}$ *a group.*

Proposition 3.24

Let $\Sigma = \{ a_1, ..., a_n\}$ *and* $\mathcal{R} = \{ (a_i a_i, \epsilon), 1 \leqslant i \leqslant n\}$.

We have the quotient monoid $\Sigma^* / \leftrightarrow^*_{\mathcal{R}}$ *is a group.*

Proof 3.25

It suffices to show that every element of $\Sigma^* / \leftrightarrow^*_{\mathcal{R}}$ *is invertible, let* $w = \{ a_{i_1,...,a_{i_k}}\} \in \Sigma^* / \leftrightarrow^*_{\mathcal{R}}$.

We take $([w]_{\leftrightarrow^*_{\mathcal{R}}})^{-1} = [\tilde{w}]_{\leftrightarrow^*_{\mathcal{R}}}$, *there* w *is the reverse of a word* w, *we have* $[w]_{\leftrightarrow^*_{\mathcal{R}}} \cdot [\tilde{w}]_{\leftrightarrow^*_{\mathcal{R}}} = [\tilde{w}]_{\leftrightarrow^*_{\mathcal{R}}} \cdot [w]_{\leftrightarrow^*_{\mathcal{R}}} = [\epsilon]_{\leftrightarrow^*_{\mathcal{R}}}$.

Example 3.26

Let $\Sigma = \{ a\}$ *and* $\mathcal{R} = \{ (aa, \epsilon)\}$, *we have* $\Sigma^* / \leftrightarrow^*_{\mathcal{R}} = \{ [\epsilon]_{\leftrightarrow^*_{\mathcal{R}}}, [a]_{\leftrightarrow^*_{\mathcal{R}}}\}$, *there*

$[\epsilon]_{\leftrightarrow^*_{\mathcal{R}}} = \{ w \in \Sigma^* : |w| \equiv 0[2]\}$ *and* $[a]_{\leftrightarrow^*_{\mathcal{R}}} = \{ w \in \Sigma^* : |w| \equiv 1[2]\}$.

The Cayley table of $\Sigma^* / \leftrightarrow^*_{\mathcal{R}}$ *is defined as follows (see Table* 1*)*

	$[\epsilon]_{\leftrightarrow^*_{\mathcal{R}}}$	$[a]_{\leftrightarrow^*_{\mathcal{R}}}$
$[\epsilon]_{\leftrightarrow^*_{\mathcal{R}}}$	$[\epsilon]_{\leftrightarrow^*_{\mathcal{R}}}$	$[a]_{\leftrightarrow^*_{\mathcal{R}}}$
$[a]_{\leftrightarrow^*_{\mathcal{R}}}$	$[a]_{\leftrightarrow^*_{\mathcal{R}}}$	$[\epsilon]_{\leftrightarrow^*_{\mathcal{R}}}$

We have the group $\Sigma^* / \leftrightarrow^*_{\mathcal{R}}$ *and* $(\mathbb{Z}/2\mathbb{Z}, \oplus)$ *are isomorphic.*

Chapter 4

The Public-key cryptosystems based on Thue Monoid Morphism Interpretation(TMMI)

4.1 Introduction

In this chapter, we are interested in the ATS-monoid protocol (proposed by **P.J. Abisha**, **D.G.Thomas** and **K.G Subramanian**). To build the ATS-monoid protocol, the idea is transform a system of Thue $\mathcal{S}_1 = (\Sigma, \mathcal{R})$ for which the word problem is undecidable in a Thue system $\mathcal{S}_2 = (\Delta, \mathcal{R}_\theta)$ with $\theta \subseteq \Delta \times \Delta$ and $\mathcal{R}_\theta = \{ (ab, ba) : (a, b) \in \theta\}$ for which the word problem is decidable in linear time.

Content:

3.2 Word rewriting semi system.

3.3 The ATS-monoid protocol.

3.4 Security of ATS-monoid protocol.

3.5 Some attacks against ATS-monoid.

4.2 Word rewriting semi system

Definition 4.1

A word rewriting semi system, also called a Thue semi system, is a couple $S = (\Sigma^*, \mathcal{R})$ *where* Σ *a finite alphabet and* $\mathcal{R}$ *a binary relation on the free monoid* Σ^**. An element* (r, s) *of* $\mathcal{R}$ *is called a rewriting or substitution rule. Applying any rule of the form* $r\mathcal{R}s$ *of* $S = (\Sigma, \mathcal{R})$ *to a word* f *containing the factor* r *consists in replacing* r *by* s *in* f*. If there is no rule of* $S = (\Sigma, \mathcal{R})$ *applicable to* f*, then* f *is said to be irreducible or in normal form, we denote by* $Irr(\mathcal{R})$ *the set of irreducible elements of* Σ^**.*

Definition 4.2

Given two words $u, v \in \Sigma^*$*, we say that* v *derives directly from* u*, and we write* $u \longrightarrow_{\mathcal{R}} v$ *if, and only if, there exists a rule* (r, s) *of* $\mathcal{R}$ *i.e,* $r\mathcal{R}s$ *and* $x, y \in \Sigma^*$ *such that:*

$$u = xry \text{ and } v = xsy$$

We say that v *derives from* u*, and we denote by* $u \longrightarrow^*_{\mathcal{R}} v$*, if there exists a finite sequence of a words* $u_0, u_1, ..., u_n$ *of* Σ^* *such that,*

$$\begin{gathered} u_0 \;=\; u, \\ u_i \rightarrow_{\mathcal{R}} u_{i+1},\ \forall 0 \leqslant i \leqslant n-1 \\ \text{and } u_n \;=\; v. \end{gathered}$$

Definition 4.3

Let $(\Sigma, \mathcal{R})$ be a rewrite semi-system. Deciding the equivalence of two modulo $\leftrightarrow^*_{\mathcal{R}}$ is a classic problem called the word problem in a monoid it's therefore a matter of being given any two words w and w' belonging to Σ^*, deciding if there belong to the same equivalence class modulo the congruence $\leftrightarrow^*_{\mathcal{R}}$.

Theorem 4.4

Let $u, v \in \Sigma^*, \theta \subseteq \Sigma \times \Sigma$ and a sub alphabet $\Delta \subseteq \Sigma$. We define, $P_\Delta : \Sigma^* \longrightarrow \Delta^*$ by:

$$\begin{cases} P_\Delta(\sigma) = \sigma, \ if \ \sigma \in \Delta \ and \\ P_\Delta(\sigma) = \epsilon, \ if \ \sigma \notin \Delta \end{cases}$$

Then :

$$u \leftrightarrow^*_{\mathcal{R}_\theta} v \Leftrightarrow \begin{cases} P_{\{\sigma\}}(u) = P_{\{\sigma\}}(v) \ for \ all \ \sigma \in \Sigma \ and \\ P_{\{\sigma,\mu\}}(u) = P_{\{b\}}(v) \ for \ all \ (\sigma, \mu) \notin \theta \end{cases}$$

4.3 The ATS-monoid protocol

The ATS-monoid protocol. **P.J. Abisha**, **D.G. Thomas** and **K.G.Subramanian**, used the theorem of **R, Cori** and **D. Perrin**, to build the ATS-monoid protocol.

Definition 4.5

The idea of ATS-monoid protocol is transform a system of Thue $\mathcal{S}_1 =$

$(\Sigma, \mathcal{R})$ *for which the word problem is undecidable in a Thue system* $\mathcal{S}_2 = (\Delta, \mathcal{R}_\theta)$ *with* $\theta \subseteq \Delta \times \Delta$ *and* $\mathcal{R}_\theta = \{\ (ab, ba) : (a, b) \in \theta\}$ *for which the word problem is decidable in linear time.*

• *Public-Key (pK): A Thue system* $\mathcal{S}_1 = (\Sigma, \mathcal{R})$ *and two words* w_0, w_1 *of* Σ^*. $(\Sigma, \mathcal{R}, w_0, w_1)$ *constitute a public-key.*

• *Secret-Key (sK): A Thue system* $\mathcal{S}_2 = (\Delta, \mathcal{R}_\theta)$ *where* Δ *an alphabet of size smaller than* Σ*, a morphism* h *from* Σ^* *to* Δ^**, such that for all* $(r, s) \in \mathcal{R}$*:*

$$\begin{cases} (h(r), h(s)) \in \{\ (ab, ba), (ba, ab)\}; for\ a\ pair\ (a, b) \in \theta, or \\ h(r) = h(s) \end{cases}$$

Therefore,

$$for\ all\ u, v \in \Sigma^*, u \leftrightarrow^*_{\mathcal{R}} v \Rightarrow h(u) \leftrightarrow^*_{\mathcal{R}_\theta} h(v)$$

Thus if $h(u)$ *and* $h(v)$ *are not equivalent with respect to* $\leftrightarrow^*_{\mathcal{R}_\theta}$*, then* u *and* v *are not equivalent with respect to* $\leftrightarrow^*_{\mathcal{R}}$.

And, we also we have two words x_0, x_1 *of* Δ^* *such that* $x_0 \leftrightarrow^*_{\mathcal{R}_\theta} h(w_0), x_1 \leftrightarrow^*_{\mathcal{R}_\theta} h(w_1)$ *with* $h(w_0)$ *and* $h(w_1)$ *are not equivalent with respect to*

$\leftrightarrow^*_{\mathcal{R}_\theta}$ *.*$(\Delta, \mathcal{R}_\theta, h \in Hom(\Sigma^*, \Delta^*))$ *constitute a secret-key.*

• *Encryption : for encrypt a bit* $b \in \{\ 0, 1\}$, ***Alice*** *chooses a word* c *of* Σ^* *in the equivalent class of* w_b *with respect to* $\leftrightarrow^*_{\mathcal{R}}$*, i.e,* $c \in [w_b]_{\leftrightarrow^*_{\mathcal{R}}}$ *where* $[w_b]_{\leftrightarrow^*_{\mathcal{R}}}$ *denotes the equivalence class of* w_b *with respect to* $\leftrightarrow^*_{\mathcal{R}}$

and then sent to Alice.

• *Decryption : Upon receipt of a word c of* Σ^*, ***Bob*** *calculated* $h(c) \in \Delta^*$, *since* $c \leftrightarrow^*_{\mathcal{R}} w_b$ *and according to the result for all* $u, v \in \Sigma^*, u \leftrightarrow^*_{\mathcal{R}} v \Rightarrow h(u) \leftrightarrow^*_{\mathcal{R}_\theta} h(v)$ *we have* $h(c) \leftrightarrow^*_{\mathcal{R}_\theta} h(w_b)$, *for example if* $h(c) \leftrightarrow^*_{\mathcal{R}_\theta} x_0$ *the message is decrypted* 0.

Example 4.6

• *Public-Key (pK):*

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

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

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

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

• *Secret-Key (sK):*

$\Delta = \{\ a, b, c\}, \theta = \{\ (a, b), (a, c)\}$ *and* $h : \Sigma^* \longrightarrow \Delta^*$ *is defined by:*

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

We have $\mathcal{R}_\theta = \{\ (a, b), (a, c)\}, h(w_0) = x_0 = acbabc$ *and* $h(w_1) = x_1 = acbca$.

Now we verify the following conditions:

1. $h(w_0)$ *and* $h(w_1)$ *are not equivalent with respect to* $\leftrightarrow^*_{\mathcal{R}_\theta}$.

2. for all $(r, s) \in \mathcal{R}$:

$$\begin{cases} (h(r), h(s)) \in \{\ (ab, ba), (ba, ab)\}; for\ a\ pair\ (a, b) \in \theta, or \\ h(r) = h(s) \end{cases}$$

For condition 1. Just use the theorem of ***R. Cori*** *and* ***D. Perrin****, we have* $P_{\{b\}}(h(w_0)) = P_{\{b\}}(acbabc) = bb$ *and* $P_{\{b\}}(h(w_1)) = P_{\{b\}}(acbca) = b$*, then* $h(w_0)$ *and* $h(w_1)$ *are not equivalent with respect to* $\leftrightarrow^*_{\mathcal{R}_\theta}$.

For condition 2. we have $\mathcal{R} = \{\ (\sigma_2\sigma_3, \sigma_3\sigma_2), (\sigma_2\sigma_4, \sigma_4\sigma_2), (\sigma_1\sigma_3, \sigma_3\sigma_1)\}$ *then,*

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

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

$(h(\sigma_1\sigma_3), h(\sigma_3\sigma_1)) = (b, b)$ *(we have* $h(\sigma_1\sigma_3) = h(\sigma_3\sigma_1)$*).*

Therefore:

$$for\ all\ u, v \in \Sigma^*,\ u \leftrightarrow^*_{\mathcal{R}} v \Rightarrow\ h(u) \leftrightarrow^*_{\mathcal{R}_\theta} h(v)$$

- *Encryption:*

For example, for encrypt the 0, ***Alice*** *chooses a word* c *of* $\{\ \sigma_1, \sigma_2, \sigma_3, \sigma_4\}^*$ *in the equivalence class of* w_0 *with respect to* $\leftrightarrow^*_{\mathcal{R}}$*, i.e,* $c \in [w_0]_{\leftrightarrow^*_{\mathcal{R}}}$ *where* $[w_0]_{\leftrightarrow^*_{\mathcal{R}}}$ *denotes the equivalence class of* w_0 *with respect to* $\leftrightarrow^*_{\mathcal{R}}$*, and then sent to* ***Bob****.*

We have:

$w_0 = \sigma_1\sigma_2\sigma_4\sigma_3\sigma_1\sigma_2\sigma_3\sigma_4 \leftrightarrow^*_{\mathcal{R}} \sigma_1\sigma_4\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3\sigma_4 \leftrightarrow^*_{\mathcal{R}} \sigma_1\sigma_4\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3\sigma_4$.

We choose $c = \sigma_1\sigma_4\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3\sigma_4$

- *Decryption:*

Upon receipt of a word c *of* $\{\ \sigma_1, \sigma_2, \sigma_3, \sigma_4\}^*$, ***Alice*** *calculated* $h(c) = h(\sigma_1\sigma_4\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3\sigma_4) = cbaabc \in \{\ a, b, c\}^*$, *Now using the theorem of* ***R. Cori*** *and* ***D. Perrin****, such that* $h(c) \leftrightarrow^*_{\mathcal{R}_\theta} h(w_0)$.

We have:

$P_{\{a\}}(h(c)) = P_{\{a\}}(h(w_0)) = aa$

$P_{\{b\}}(h(c)) = P_{\{b\}}(h(w_0)) = bb$

$P_{\{c\}}(h(c)) = P_{\{c\}}(h(w_0)) = cc.$

then for all σ *of* $\{\ a, b, c\}, P_{\{\sigma\}}(h(c)) = P_{\{\sigma\}}(h(w_0))$. *In addition it is verified that* $P_{\{\sigma,\mu\}}(h(c)) = P_{\{\sigma,\mu\}}(h(w_0))$, *for all* $(\sigma, \mu) \notin \theta$, *we have complementary of* θ *is* $C_{\Delta\times\Delta}\theta = \{\ (a,a), (b,a), (b,b), (b,c), (c,a), (c,b), (c,c)\}$, *then* $P_{\{b,c\}}(h(c)) = P_{\{b,c\}}(h(w_0)) = cbbc.$

Finally $h(c) \leftrightarrow^*_{\mathcal{R}_\theta} h(w_0) = x_0$ *and the word is decrypted* 0.

4.4 Security of ATS-monoid protocol

An attack against ATS-monoid does not allow to find exactly the Secret-Key. We will get rather a key that is equivalent to it in the following direction:

We say that $(\Delta', \mathcal{R}_\theta, h' \in Hom(\Sigma^*, \Delta'^*))$ is an equivalent key to the Secret-Key$(\Delta, \mathcal{R}_\theta, h \in Hom(\Sigma^*, \Delta^*))$ if any message encrypted with the Public-Key $(\Sigma, \mathcal{R}, w_0, w_1)$ can be decrypted with $(\Delta', \mathcal{R}_\theta, h' \in Hom(\Sigma^*, \Delta'^*))$.

This is the case for example if $(\Delta', \mathcal{R}_\theta, h' \in Hom(\Sigma^*, \Delta'^*))$ checks the following three conditions :

1. h' is non trivial and $|\Delta'| \leqslant |\Sigma|$.

2. for all $(r, s) \in \mathcal{R}$

$$\begin{cases} (h'(r), h'(s)) \in \{\ (ab, ba), (ba, ab)\}; for\ a\ pair\ (a, b) \in \theta, or \\ h(r)' = h'(s) \end{cases}$$

3. $h'(w_0)$ et $h'(w_1)$ are not equivalent with respect to $\leftrightarrow^*_{\mathcal{R}'_\theta}$.

• Now we recall some keys that are equivalent to the Secret-Key $(\Delta, \mathcal{R}_\theta, h \in Hom(\Sigma^*, \Delta^*))$.

1. If $h(\Sigma) = \{\ h(\sigma), \sigma \in \Sigma\}$ and $\theta' = \theta \cap h(\Sigma) \times h(\Sigma)$. Then : $(h(\Sigma), \mathcal{R}_{\theta'}, h \in Hom(\Sigma^*, \Delta^*))$ is an equivalent key to the Secret-Key $(\Delta, \mathcal{R}_\theta, h \in Hom(\Sigma^*, \Delta^*))$.

2. If $|\Delta'| = |\Delta|, i \in Iso(\Delta^*, \Delta'^*)$ and $i(\theta) = \{\ (i(a), i(b)), (a, b) \in \theta\}$. Then, $(\Delta', \mathcal{R}_{i(\theta)}, i \circ h \in Hom(\Sigma^*, \Delta'^*))$ is an equivalent key to the Secret-Key $(\Delta, \mathcal{R}_\theta, h \in Hom(\Sigma^*, \Delta^*))$.

• Now describe a general attack against the ATS-monoid protocol. In the first time we notice that a key $(\Delta', \mathcal{R}_{\theta'}, h \in Hom(\Sigma^*, \Delta'^*))$ equivalent to the Secret-Key $(\Delta, \mathcal{R}_\theta, h \in Hom(\Sigma^*, \Delta'^*))$ is independent of alphabet Δ, the only thing that matters is the size of Δ.

On the other hand, we observe that the relation $\mathcal{R}_{\theta'}$ is easily deduced from the knowledge of $h' \in Hom(\Sigma^*, \Delta'^*)$.

Then for a Public-Key $(\Sigma, \mathcal{R}, w_0, w_1)$ there is a algorithm noted by

Algo-ATS-monoid which returns an equivalent key to the Secret-Key $(\Delta, \mathcal{R}_\theta, h \in Hom(\Sigma^*, \Delta^*))$ to complexity $|\mathcal{R}| \sum_{i=1}^{i=k} (i+1)^{|\Sigma|}$, with $k = |\Delta|$.

Algorithm-ATS-monoid

Data: $(\Sigma, \mathcal{R}, w_0, w_1)$, **Public-Key**(pK) of **ATS-monoid** protocol.

Result: $(\Delta_i, \mathcal{R}_{\theta_i}, h_i \in Hom(\Sigma^*, \Delta_i^*))$, equivalent key to the **Secret-Key**.

While i, $1 \leqslant i \leqslant |\Sigma|$ **Do**

Δ_i is any alphabet of i lettres

While $h_i \in Hom(\Sigma^*, \Delta_i^*)$ **Do**

$\theta_i \longleftarrow \emptyset$

While $(r, s) \in \mathcal{R}$ **Do**

Calculate $h_i(r)$ and $h_i(s)$

If $h_i(r) \neq h_i(s)$ **Then**

If $h_i(r) = ab$ and $h_i(s) = ba$, for $a, b \in \Delta_i$ **Then**

If $(a, b) \notin \theta_i$ then $\theta_i \longleftarrow \theta_i \cup \{ (a, b)\}$

If no choose another morphism, i.e. **Return** to the second loop **While**

End If

End While

If $h_i(w_0)$ and $h_i(w_1)$ are not equivalent modulo $\leftrightarrow^*_{\mathcal{R}_{\theta_i}}$ **Then**

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

End While

End While

4.5 Some attacks against ATS-monoid

In this section we give some attacks against ATS-monoid that is to say in each case we return equivalent key to the Secret-Key of this protocol.

Corollary 4.7

Let $(\Sigma, \mathcal{R}, w_0, w_1)$ *be a Public-Key of ATS-monoid protocol.*
If $\forall (r,s) \in \mathcal{R}, |r| = |s|$, *then* $(\Delta_1 = \{\ a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1))$ *where for all* $\sigma \in \Sigma, h_1(\sigma) = a$, *is an equivalent key to the Secret-Key*

Proof 4.8

The Key $(\Delta_1 = \{\ a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1))$ *where for all* $\sigma \in \Sigma, h_1(\sigma) = a$, *checked the following three condition:*
1. The morphism h_1 *is not trivial because for all* $\sigma \in \Sigma, h_1(\sigma) = a \neq \epsilon$.
2. $\forall (r,s) \in \mathcal{R}, h_1(r) = h_1(s) = (a)^{|r|} = (a)^{|s|}$.
3. If $\mathcal{R}_\theta = \emptyset$, *then* $\leftrightarrow^*_{\mathcal{R}_\theta} = I_{\Sigma^*}$ *consequently* $h_1(w_0)$ *and* $h_1(w_1)$ *are not equivalent modulo* $\leftrightarrow^*_{\mathcal{R}_\theta}$ *since* $h_1(w_0) \neq h_1(w_1)$. *then* $(\Delta_1 = a, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ *is an equivalently key to the Secret-Key.*

Corollary 4.9

Let $(\Sigma, \mathcal{R}, w_0, w_1)$ *be a Public-Key of ATS-monoid protocol. There exist* $(r,s) \in \mathcal{R}, |r| \neq |s|$, *then* $(\Delta_1 = a, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ *where* $h_1(\Sigma) = \{\ a, \epsilon\}$ *is an equivalent key to the Secret-Key.*

Example 4.10

Public-Key:

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

$\mathcal{R} = \{ (\sigma_1\sigma_3, \sigma_3\sigma_1), (\sigma_1\sigma_4, \sigma_4\sigma_1), (\sigma_2\sigma_3, \sigma_3\sigma_2), (\sigma_2\sigma_4, \sigma_4\sigma_2), (\sigma_5\sigma_3\sigma_1, \sigma_3\sigma_5\sigma_1)\}$.

$w_0 = \sigma_4\sigma_2\sigma_4\sigma_3\sigma_4\sigma_2\sigma_3\sigma_4, w_1 = \sigma_2\sigma_4\sigma_3\sigma_4\sigma_2\sigma_1$.

The key $(\Delta_1 = \{ a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ *or* $h_1(\sigma_1) = h_1(\sigma_3) = \epsilon, h_1(\sigma_2) = h_1(\sigma_4) = h_1(\sigma_5) = a$ *is verified the following conditions:*

1. The morphism h_1 *is non trivial.*

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

3. We have $h_1(w_0) = a^6$ *and* $h_1(w_1) = a^4$ *and like* $\leftrightarrow^*_{\mathcal{R}_\theta} = I^*_\Sigma$, *then* $h_1(w_0)$ *and* $h_1(w_1)$ *are not equivalent with respect to* $\leftrightarrow^*_{\mathcal{R}_\theta}$. *then* $(\Delta_1 = \{ a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ *is an equivalent key to the Secret-Key.*

Corollary 4.11

Let $(\Sigma, \mathcal{R}, w_0, w_1)$ *be a Public-Key of ATS-monoid protocol.*

If there exist σ_k *of the alphabet* Σ *such that for all* $(r, s) \in \mathcal{R}, |r|_{\sigma_k} = |s|_{\sigma_k} = 0$, *then* $(\Delta_1 = \{ a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ *or for all* $\sigma \in \Sigma$ *with* $\sigma \neq \sigma_k, h_1(\sigma) = \epsilon$ *and* $h_1(\sigma_k) = a$, *is an equivalent key to the Secret-Key.*

Proof 4.12

The key $(\Delta_1 = \{\ a\}, \mathcal{R}_\theta = \emptyset, h_1 \in Hom(\Sigma^*, \Delta_1^*))$ *is checked three conditions:*

1. The morphism h_1 *is non trivial. because* $h_1(\sigma_k) = a \neq \epsilon$.

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

3. If $\mathcal{R}_\theta = \emptyset$, *then* $\leftrightarrow^*_{\mathcal{R}_\theta} = I_{\Sigma^*}$, *so it must verify that* $h_1(w_0) \neq h_1(w_1)$.

Conclusion

After some preliminary notions and notations, we presented the free monoid and its properties. we also gived the closure of relation, the congruence generated by a relation and some properties of presentation by generators and relation.

Finally, we are interested in the word rewriting semi system and we studied the public key cryptosystems security of ATS-monoid protocol and some attacks against ATS-monoid.

Bibliography

[1] **Henk C.A. van Tilborg**."Fundamentals of Cryptology". Eindhoven University of Technology The Netherlands.

[2] **Johannes ARZ**."Syntactic congruence and syntactic Algerbras". R.A.I.R.O. Informatique théorique/Theoretical Informatics, vol 17, N 3, p. 231 à 238. (1983)

[3] **Josep Elgueta**."Normal submonoid and congruence on a monoid". arXiv :2210.08546v1 [math.GR] 16 Oct 2022.

[4] **Lila Kari** and**Gabriel Thierrin**, "Languages and compatible relations on monoids", University of Western Ontario London, Canada.

[5] **Marina Anagnostopoulou-Merkouri, James D. Mitchell**, and **Maria Tsalakou**". Computing the congruence of a finite semi-group or monoid".arXiv :2302.06295v1 [math.RA] 13 Feb 2023.

[6] **M. Torpey**."Semi group congruence computational Techniques and Theoretical applications", A Thesis submitted for the Degree

od PhD at the University of St Andrews. (2019).

[7] **N. Ghadbane**."On public key cryptosystems based and Thue Monoid Morphism Interpretation (TMMI)". Information Processing at the Digital Age, vol22. N.2, pp 31-38. (2018)

[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), pp 158-161. (2016).

[9] **N. Ghadbane**."Holomorphs of groups and their use in the Diffie-Hellman key-exchange protocol". Annals of Mathematics and Computer Science, vol 13, pp 53-59. (2023)

[10] **N. Ghadbane**."Semi groupes et automates fini", Université de M'sila.

[11] **N. Ghadbane**."On public key cryptosystem based on the word problem in a group". Journal of discrete mathematical science and cryptography, vol 25, No 6, pp. 1563-1568. (2022)

[12] **N. Ghadbane** and**D. Mihoubi**."Presentation of monoids by generators and relations". Global and Stochastic Analysis (GSA), vol 3(2), pp 61-73. (2016).

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

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

الملخص

هذه مذكرة ماستر جبر و رياضيات متقطعة موضوعها حول نظرية العلاقات على نصف الزمرة الحرة وتطبيقاتها على أنظمة التشفير ذات المفاتيح المعلنة في هذا العمل قمنا بدراسة مايلي :

- **مفاهيم أولية لنصف الزمرة الحرة .**
- **المجموعات الجزئية لنصف الزمرة الحرة .**
- **تمثيل بعض أنصاف الزمر بواسطة مولدات وعلاقات .**
- **نظام التشفير ذات المفاتيح المعلنة في نصف الزمرة الحرة .**

الكلمات المفتاحية :

نصف الزمرة الحرة – الكلمات واللغات – علاقة التكافؤ مولدة بعلاقة .

Résumé :

Ce mémoire de master Algèbre et Mathématique Discrète s'inscrit dans la théorie des relations sur le monoïde libre et ses applications à la cryptographie à clé public. Dans ce travail, nous avons étudié les points suivants :

- **Notions élémentaires sur le monoïde libre.**
- **Les langages du monoïde libre.**
- **Présentation de quelques monoïdes par générateurs et relations.**
- **Le crypto système à clé public basé sur le problème du mot dans un monoïde libre**

Mots clés :

Monoïde libre, mots et langage, La fermeture d'une relation binaire.

Abstract :

This memory of master degree Algebra and discrete mathematics lies within the theory of relation on free monoid and its applications in public key cryptography. In this work, we studied the following points :

- **Elementary notions on free monoid .**
- **The languages of free monoid .**
- **Presentation of monoid by generators and relations.**
- **The public key cryptosystems based on Thue Monoid Morphism Interpretation (TMMI).**

Key words :

Free monoid, words and languages, the closure of a binary relation