Global and Stochastic Analysis
Vol. 3 No. 2, December (2016), 61-73

MUK PUBLICATIONS
Open Access Publisher

PRESENTATION OF MONOIDS BY GENERATORS AND RELATIONS

NACER GHADBANE* AND DOUADI MIHOUB

Abstract. Let A^* be the free monoid over a finite alphabet A and R a binary relation on A^*. The congruence generated by R is defined as follows:

- $xuy \underset{R}{\leftrightarrow} xvy$, whenever $x, y \in A^*$ and uRv or vRu
- $w \overset{*}{\underset{R}{\leftrightarrow}} w'$, whenever $u_0, u_1, ..., u_n \in A^*$ with,$u_0 = w, u_i \underset{R}{\leftrightarrow} u_{i+1}, \forall 0 \leq i \leq n-1, u_n = w'$.

A presentation (by generators and relations) of a monoid M is a pair $S = (A, R)$ such that M is isomorphic to the quotient of A^* by the congruence noted $\overset{*}{\underset{R}{\leftrightarrow}}$ generated by R, i.e, $M \cong A^*/\overset{*}{\underset{R}{\leftrightarrow}}$. We consider two systems of rewriting $S_1 = (A_1, R_1)$ and $S_2 = (A_2, R_2)$. The purpose of this study is to determine some conditions on the relations R_1 and R_2 that ensure the existence of a morphism between the quotient monoids $A_1^*/\overset{*}{\underset{R_1}{\leftrightarrow}}$ and $A_2^*/\overset{*}{\underset{R_2}{\leftrightarrow}}$. We give also a specific relation R on A^* making the quotient monoid $A^*/\overset{*}{\underset{R}{\leftrightarrow}}$ a group.

1. Intoduction

Let A be a set, called an alphabet in the following. Elements of A will be called symbols. A finite word over A is just a sequence of alphabet symbols. The set of all finite words over A is denoted with A^*. The concatenation of words is an associative operation with identity element ϵ. Hence, A^* has the structure of a monoid, called the free monoid generated by A. A semi-Thue system (or word rewriting system) over the alphabet A is just a set $R \subseteq A^* \times A^*$. We associate with R a binary relation $\rightarrow_R$ on A^*, alsocalled the, as follows: For all $u, v \in A^*, u \rightarrow_R v$ if and only if there exist $x, y \in A^*$ and $(l, r) \in R$ suth that $u = xly$ and $v = xry$. Elements (l, r) are called rules and usually written as $l \rightarrow r$. Note that $\overset{*}{\underset{R}{\leftrightarrow}}$ is a congruence generated by R and $[w]_{\overset{*}{\underset{R}{\leftrightarrow}}} = \left\{x \in A^* : x \overset{*}{\underset{R}{\leftrightarrow}} w\right\}$ be the equivalence class with respect to $\overset{*}{\underset{R}{\leftrightarrow}}$. Hence, we can defin the quotient monoid $A^*/\overset{*}{\underset{R}{\leftrightarrow}}$.

A presentation of a monoid M is a pair (A, R) where A is an alphabet, $R \subseteq A^* \times A^*$, and $M \cong A^*/\overset{*}{\underset{R}{\leftrightarrow}}$.

The remainder of this paper is organized as follows. In Section 2, some mathematical preliminaries. In Section 3, we consider two systems of rewriting $S_1 =$

2000 *Mathematics Subject Classification.* Primary 68Q42; Secondary 20M05.

Key words and phrases. Free monoid, morphism of monoids, closure of a binary relation, rewriting systems of words, Presentation of a monoid.

(A_1, R_1) and $S_2 = (A_2, R_2)$. The purpose of this study is to determine some conditions on the relations R_1 and R_2 that ensure the existence of a morphism between the quotient monoids $A_1^*/ \underset{R_1}{\overset{*}{\leftrightarrow}}$ and $A_2^*/ \underset{R_2}{\overset{*}{\leftrightarrow}}$. We give also a specific relation R on A^* making the quotient monoid $A^*/ \underset{R}{\overset{*}{\leftrightarrow}}$ a group. The Section 4 is devoted to the application on the notion of word problem in public key cryptography. Finally, we draw our conclusions in Section 5.

2. Preliminaries

A monoid is a set M equipped with an associative product $x, y \longmapsto xy$, together with a (left and right) unit 1. In the commutative case, it is common to use the additive notation: $x + y$ instead of xy, and 0 instead of 1.

If $X \subset M$, we write X^* for the submonoid of M generated by X, that is the set of finite products $x_1 x_2 ... x_n$ with $x_1, x_2, ..., x_n \in X$, including the empty product 1. It is the smallest submonoid of M containing X.

Let A be a set, which we call an alphabet. A word w on the alphabet A is a finite sequence of elements of A

$$w = (a_1, a_2, ..., a_n) \qquad a_i \in A.$$

The set of all words on the alphabet A is denoted by $A^*$and is equipped with the associative operation defined by the concatenation of two sequences

$$(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_m) = (a_1, a_2, ..., a_n, b_1, b_2, ..., b_m)$$

This operation is associative. This allows us to write $w = a_1\ a_2, ...\ a_n$. The string consisting of zero letters is called the empty word, written ϵ. Thus, $\epsilon, 0, 1, 011, 1111|$ are words over the alphabet $\{0, 1\}$. Thus the set A^* of words is equipped with the structure of a monoid. the monoid A^* is called the free monoid on A. The reverse of a word $w = a_1\ a_2, ...\ a_n$, is $\widetilde{w} = a_n\ a_{n-1}, ...\ a_1$. Note that for all $u, v \in A^*, \widetilde{uv} = \widetilde{v}\widetilde{u}$.

The length of a word u, in symbols $|u|$, is the number of letters in u when each letter is counted as many times as it occurs. Again by definition, $|\epsilon| = 0$. The length function possesses some of the formal properties of logarithm:

$$|uv| = |u| + |v|, \left|u^i\right| = i\,|u|,$$

for any words u and v and integers $i \geq 0$. For example $|011| = 3$ and $|1111| = 4$. For a subset B of A, we let $|w|_B$ denote the number of letters of w which are in B. Thus $|w| = \sum_{a \in A} |w|_a$. A language L over A^* is any subset of A^* [1].

Let $f : S \longrightarrow U$ be a mapping of sets.

• We say that f is **one-to-one** if for every $a, b \in S$ where $f(a) = f(b)$, we have $a = b$.

• We say that f is **onto** if for every $y \in U$, there exists $a \in S$ such that $f(a) = y$.

A mapping $h : A^* \longrightarrow \Delta^*$, where A and Δ are alphabets, satisfying the condition

$$h(uv) = h(u)h(v), \text{ for all words } u \text{ and } v,$$

is called a morphism, define a morphism h, it suffices to list all the words $h(\sigma)$, where a ranges over all the (finitely many) letters of A. If M is a monoid, then any mapping $f : A \longrightarrow M$ extends to a unique morphism $\widetilde{f} : A^* \longrightarrow M$. For instance, if M is the additive monoid $\mathbb{N}$, and f is defined by $f(\sigma) = 1$ for each $\sigma \in A$, then $\widetilde{f}(u)$ is the length $|u|$ of the word u.

Let $h : A^* \longrightarrow \Delta^*$ be a morphism of monoids. if h is one-to-one and onto, then h is an isomorphism and the monoids A^* and Δ^* are isomorphic. we denote $Hom(A^*, \Delta^*)$ the set of morphisms from A^* to Δ^* and $Isom(A^*, \Delta^*)$ the set of isomorphisms from A^* to Δ^*.

A binary reation on A^* is a subset $R \subseteq A^* \times A^*$. If $(x, y) \in R$, we say that x is related to y by R, denoted xRy. The inverse relation of R is the binary reation $R^{-1} \subseteq A^* \times A^*$ defined by $yR^{-1}x \Longleftrightarrow (x, y) \in R$.

The relation $I_{A^*} = \{(x, x), x \in A^*\}$ is called the identity relation. The relation $(A^*)^2$ is called the complete relation.

Let $R \subseteq A^* \times A^*$ and $S \subseteq A^* \times A^*$ binary relations. The composition of R and S is a binary relation $S \circ R \subseteq A^* \times A^*$ defined by

$$x(S \circ R)z \Longleftrightarrow \exists y \in A^* \text{ such that } xRy \text{ and } ySz.$$

A binary relation R on a set A^* is said to be

- reflexive if xRx for all x in A^*;
- symmetric if xRy implies yRx;
- transitive if xRy and yRz imply xRz.

The relation R is called an equivalence relation if it is reflexive, symmetric, and transitive. And in this case, if xRy, we say that x and y are equivalent. The set of all equivalence classes is denoted by A^*/R and is called the quotient of A^* mod R.

Let R be a relation on a set A^*. The reflexive closure of R is the smallest reflexive relation $r(R)$ on A^* that contains R; that is,

- $R \subseteq r(R)$
- if R' is a reflexive relation on A^* and $R \subseteq R'$, then $r(R) \subseteq R'$.

The symmetric closure of R is the smallest symmetric relation $s(R)$ on A^* that contains R; that is,

- $R \subseteq s(R)$
- if R' is a symmetric relation on A^* and $R \subseteq R'$, then $s(R) \subseteq R'$.

The transitive closure of R is the smallest transitive relation $t(R)$ on A^* that contains R; that is,

- $R \subseteq t(R)$
- if R' is a transitive relation on A^* and $R \subseteq R'$, then $t(R) \subseteq R'$.

Let R be a relation on a set A^*. Then

- $r(R) = R \cup I_{A^*}$,
- $s(R) = R \cup R^{-1}$
- $t(R) = \bigcup_{k=1}^{k=+\infty} R^k$.

A congruence on a monoid M is an equivalence relation $\equiv$ on M compatible with the operation of M, i.e, for all $m, m' \in M, u, v \in M$

$$m \equiv m' \Longrightarrow umv \equiv um'v$$

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

$$\forall u, v \in A^* : uKer\ f\ v \Longleftrightarrow f(u) = f(v).$$

Let L be a language over A, the syntactic congruence of L denoted by $\equiv_L$ is defined by:

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

The quotient of A^* by $\equiv_L$ is, by definition, the syntactic monoid of L denoted $M(L)$, i.e., $M(L) = A^*/\equiv_L$.

A semi-Thue system is a pair (A, R) where A is an alphabet and R is a non-empty finite binary on A^*, we write $urv \rightarrow_R ur'v$ whenever $u, v \in A^*$ and $(r, r') \in R$. We write $u \rightarrow_R^* v$ if there words $u_0, u_1, ..., u_n \in A^*$ such that,

$$\begin{aligned} &u_0 = u, \\ &u_i \longrightarrow_R u_{i+1}, \forall 0 \leq i \leq n-1 \\ &\text{and } u_n = v. \end{aligned}$$

If $n = o$, we get $u = v$, and if $n = 1$, we get $u \rightarrow_R v$. $\rightarrow_R^*$ is the reflexive transitive closure of $\rightarrow_R$.

The congruence generated by R is defined as follows:

- $urv \longleftrightarrow_R ur'v$ whenever $u, v \in A^*$, and rRr' or $r'Rr$;
- $u \underset{R}{\overset{*}{\leftrightarrow}} v$ whenever $u = u_0 \longleftrightarrow_R u_1 \longleftrightarrow_R ... \longleftrightarrow_R u_n = v$.

$\longleftrightarrow_R^*$ is the reflexive symmetric transitive closure of $\rightarrow_R$. Let $\pi_R : A^* \longrightarrow A^*/ \underset{R}{\overset{*}{\leftrightarrow}}$ be the canonical surjective monoid morphism that maps a word $w \in A^*$ to its equivalence class with respect to $\underset{R}{\overset{*}{\leftrightarrow}}$. A monoid M is finitely generated if it is ithenmorphic to a monoid of the form $A^*/ \underset{R}{\overset{*}{\leftrightarrow}}$. In this case, we also say that M is finitely generated by A. If in addition to A also R is finite, then M is a finitely presented monoid. The word problem of $M \simeq A^*/ \underset{R}{\overset{*}{\leftrightarrow}}$ with respect to R is the set $\{(u, v) \in A^* \times A^* : \pi_R(u) = \pi_R(v)\}$ it is undecidable in general [6, 7, 10].

The semi-Thue system (A, R) is terminating if there does not exist an infinite chain $w_1 \rightarrow_R w_2 \rightarrow_R w_3 \rightarrow_R ...$ in A^*. The set of irreducible words with respect to R is $Irr(R) = \{u \in A^*, \neg v \in A^* : u \rightarrow_R v\}$. (A, R) is confluent (resp. locally confluent) if for all $x, y, z \in A^*$ with $x \rightarrow_R^* y$ and $x \rightarrow_R^* z$ (resp. $x \rightarrow_R y$ and $x \rightarrow_R z$) there exists $w \in A^*$ with $y \rightarrow_R^* w$ and $z \rightarrow_R^* w$. If (A, R) is terminating, then by Newman's lemma (A, R) is confluent if and only if (A, R) is locally confluent. A semi-Thue system (A, R) is canonical if (A, R) is confluent and terminating. If (A, R) is canonical, then every word u has a unique normal form $NF_R(u) \in Irr(R)$ suth that $u \rightarrow_R^* NF_R(u)$ and moreover, the function $\pi_R \mid Irr(R)$ (i.e., π_R restricted to $Irr(R)$) is bijective. Thus, if R is in addition finite, then the word problem of $A^*/ \underset{R}{\overset{*}{\leftrightarrow}}$ is decidable: $\pi_R(u) = \pi_R(v)$ if and only if $NF_R(u) = NF_R(v)$ [8].

The congruence generated by R is defined as follows:

- $xuy \underset{R}{\leftrightarrow} xvy$, whenever $x, y \in A^*$ and uRv or vRu

- $w \overset{*}{\underset{R}{\leftrightarrow}} w'$, whenever $u_0, u_1, ..., u_n \in A^*$ with,$u_0 = w, u_i \underset{R}{\leftrightarrow} u_{i+1}, \forall 0 \leq i \leq n-1, u_n = w'$.

The equivalence class of w with respect to $\overset{*}{\underset{R}{\leftrightarrow}}$ denoted by $[w]_{\overset{*}{\underset{R}{\leftrightarrow}}}$

We get a quotient monoid $A^*/ \overset{*}{\underset{R}{\leftrightarrow}}$ and a canonical surjection $\pi_R : A^* \longrightarrow A^*/ \overset{*}{\underset{R}{\leftrightarrow}}$. Moreover, if $h : A^* \longrightarrow M$ is a mapping such that $h(x) = h(y)$ whenever xRy, we get a unique morphism $\psi : A^*/ \overset{*}{\underset{R}{\leftrightarrow}} \longrightarrow M$ such that $h \circ \pi_R = \psi$.

3. Presentations of some monoids

Definition 3.1. A presentation of a monoid M is a pair $S = (A, R)$ such that M is isomorphic to the quotient of A^* by the congruence noted $\overset{*}{\underset{R}{\leftrightarrow}}$ generated by R , i.e, $M \cong A^*/ \overset{*}{\underset{R}{\leftrightarrow}}$. The elements of A are called generators, and those of R are called relations. If there are finitely many generators and relations, i.e. $A = \{a_1, ..., a_p\}$ and $R = \left\{(r_1, r'_1), ..., \left(r_q, r'_q\right)\right\}$, we say that the monoid M is finitely presentable, and we write $M \cong \left\langle a_1, ..., a_n / r_1 = r'_1, ..., r_q = r'_q \right\rangle$.

Example 3.2. Let $A = \{a\}$ and $R = \emptyset$ (R is the empty relation), we have $\left(\{a\}^*, \cdot\right) \cong (\mathbb{N}, +)$ with the isomorphism is defined by $\epsilon \longmapsto 0, a \longmapsto 1$. Then the monoid presented by $\langle a/\emptyset \rangle$ is isomorphic to the additive monoid $(\mathbb{N}, +)$.

Example 3.3. Let $A = \{a, b\}$ and $R = \{(ab, ba)\}$. We have, for all $w \in \{a, b\}^*$, there exists a unique $(m, n) \in \mathbb{N}^2$ suth that $w \overset{*}{\underset{R}{\leftrightarrow}} b^m a^n$ with $m = |w|_b$ and $n = |w|_a$. We define the mapping $\psi : \mathbb{N}^2 \longrightarrow A^*/ \overset{*}{\underset{R}{\leftrightarrow}}, \psi(m, n) = [b^m a^n]_{\overset{*}{\underset{R}{\leftrightarrow}}}$ where $[b^m a^n]_{\overset{*}{\underset{R}{\leftrightarrow}}}$ denotes the equivalence class of $b^m a^n$ with respect to $\overset{*}{\underset{R}{\leftrightarrow}}$. The mapping ψ is morphism because for all $(m, n) \in \mathbb{N}^2, (p, q) \in \mathbb{N}^2$, we have $\psi((m, n) + (p, q)) = \psi((m + p, n + q)) = [b^{m+p} a^{n+q}]_{\overset{*}{\underset{R}{\leftrightarrow}}} = [b^m b^p a^n a^q]_{\overset{*}{\underset{R}{\leftrightarrow}}}$
$= [b^m a^n b^p a^q]_{\overset{*}{\underset{R}{\leftrightarrow}}} = [b^m a^n]_{\overset{*}{\underset{R}{\leftrightarrow}}} \cdot [b^p a^q]_{\overset{*}{\underset{R}{\leftrightarrow}}} = \psi((m, n)) \cdot \psi((p, q))$

It is clear that ψ is onto. The mapping ψ is one-to-one because, we have for all $(m, n) \in \mathbb{N}^2, (p, q) \in \mathbb{N}^2$,
$\psi((m, n)) = \psi((p, q)) \Longleftrightarrow [b^m a^n]_{\overset{*}{\underset{R}{\leftrightarrow}}} = [b^p a^q]_{\overset{*}{\underset{R}{\leftrightarrow}}} \Longleftrightarrow (m = p \text{ and } n = q)$.

Therefore the monoid presented by $\langle a, b/ab = ba \rangle$ is isomorphic to the additive monoid $\left(\mathbb{N}^2, +\right)$.

Example 3.4. Let $A = \{a, b\}$ and $R = \{(ab, \epsilon), (ba, \epsilon)\}$, for all $w \in \{a, b\}^*$, there is only three cases to be considered.

- If $|w|_a = |w|_b$, in this case we have $w \overset{*}{\underset{R}{\leftrightarrow}} \epsilon$.
- If $|w|_a > |w|_b$, i.e, $|w|_a = |w|_b + k, k \in \mathbb{N} - \{0\}$, in this case we have $w \overset{*}{\underset{R}{\leftrightarrow}} a^k$.
- If $|w|_b > |w|_a$, i.e, $|w|_b = |w|_a + l, l \in \mathbb{N} - \{0\}$, in this case we have $w \overset{*}{\underset{R}{\leftrightarrow}} b^l$.

Then $\mathbb{Z} \cong \{a,b\}^* / \overset{*}{\underset{R}{\leftrightarrow}} = \left\{ [\epsilon]_{\overset{*}{\underset{R}{\leftrightarrow}}}, \left[a^k\right]_{\overset{*}{\underset{R}{\leftrightarrow}}}, \left[b^l\right]_{\overset{*}{\underset{R}{\leftrightarrow}}}, (k,l) \in (\mathbb{N} - \{0\})^2 \right\}$. with the isomorphism $\phi : \mathbb{Z} \longrightarrow \{a,b\}^* / \overset{*}{\underset{R}{\leftrightarrow}}$ is defined by:

$0 \longmapsto [\epsilon]_{\overset{*}{\underset{R}{\leftrightarrow}}}$, if $n > 0$, then $n \longmapsto [a^n]_{\overset{*}{\underset{R}{\leftrightarrow}}}$,if $n < 0$, then $n \longmapsto [b^{-n}]_{\overset{*}{\underset{R}{\leftrightarrow}}}$.

Therefore the monoid presented by $\langle a, b / ab = \epsilon, ba = \epsilon \rangle$ is isomorphic to the additive monoid $(\mathbb{Z}, +)$.

Proposition 3.5. *Any monoid $(M, \cdot, 1_M)$ has a standard presentation (A, R), where A consists of one symbol a_x for each $x \in M$, and R is defined by $R = \{(a_{1_M}, \epsilon), (a_x a_y, a_{xy})$ for all $x, y \in M\}$. In particular, any finite monoid is finitely presented.*

Proof. Let $A = \{a_x, x \in M\}$ and $R = \{(a_{1_M}, \epsilon), (a_x a_y, a_{xy})$ for all $x, y \in M\}$, then for all $w \in A^*$, there exists $\{x_i, ..., x_j\} \subseteq M$ suth that $w = a_{x_i} ... a_{x_j}$ and $w \overset{*}{\underset{R}{\leftrightarrow}} a_{x_k}$, $x_k = x_i \cdot ... \cdot x_j$, therefore $A^* / \overset{*}{\underset{R}{\leftrightarrow}} = \left\{ [a_{x_k}]_{\overset{*}{\underset{R}{\leftrightarrow}}}, x_k \in M \right\}$. Then the isomorphism $\theta : M \longrightarrow A^* / \overset{*}{\underset{R}{\leftrightarrow}}$ is defined by: $\theta(x_k) = [w]_{\overset{*}{\underset{R}{\leftrightarrow}}}$, where $x_k = x_i \cdot ... \cdot x_j, w = a_{x_i} ... a_{x_j}, \{x_i, ..., x_j\} \subseteq M$.

The mapping θ is morphism because for all $(x_k, x_l) \in M^2$, we have $\theta(x_k x_l) = \theta(x_m) = [w]_{\overset{*}{\underset{R}{\leftrightarrow}}}$ where $x_m = x_k x_l$ and $w = a_{x_k} a_{x_l}$, then $[w]_{\overset{*}{\underset{R}{\leftrightarrow}}} = [a_{x_k} a_{x_l}]_{\overset{*}{\underset{R}{\leftrightarrow}}} = [a_{x_k}]_{\overset{*}{\underset{R}{\leftrightarrow}}} [a_{x_l}]_{\overset{*}{\underset{R}{\leftrightarrow}}} = \theta(x_k)\theta(x_l)$.

It is trivial that θ is onto. We show that θ is one-to-one, for all $(x_k, x_l) \in M^2$, there exists $\{x_i, ..., x_j\} \subseteq M, \{x_s, ..., x_t\} \subseteq M$ where $x_k = x_i \cdot ... \cdot x_j$ and $x_l = x_s \cdot ... \cdot x_t$, we have,

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

□

Example 3.6. Consider the monoid

$$M = \left\{ x_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, x_1 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, x_2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

provided with matrix multiplication. The Cayley table of 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 M satisfies the following two properties: for all $x_i \in M, x_i \cdot x_1 = x_1$ and $x_i \cdot x_2 = x_2$.

Lat $A=\{a_{x_i},x_i\in M,0\leq i\leq 2\}$ and $R=\left\{(a_{x_0},\epsilon),\left(a_{x_i}a_{x_j},a_{x_ix_j}\right),x_i,x_j\in M\right\}$. Then for all $w\in A^*$, there exists $\{x_i,...,x_j\}\subseteq M$ suth that $w=a_{x_i}...a_{x_j}$ and $w\underset{R}{\overset{*}{\leftrightarrow}}a_{x_k}$, with $x_k=x_i\cdot...\cdot x_j$. There is only three cases to be considered:

- If $w=ua_{x_1},u\in A^*$, in this case we have $w\underset{R}{\overset{*}{\leftrightarrow}}a_{x_1}$.
- If $w=ua_{x_2},u\in A^*$, in this case we have $w\underset{R}{\overset{*}{\leftrightarrow}}a_{x_2}$.
- If $w=a_{x_0}...a_{x_0}$, in this case we have $w\underset{R}{\overset{*}{\leftrightarrow}}\epsilon$.

Then $A^*/\underset{R}{\overset{*}{\leftrightarrow}}=\left\{[\epsilon]_{\underset{R}{\overset{*}{\leftrightarrow}}},[a_{x_1}]_{\underset{R}{\overset{*}{\leftrightarrow}}},[a_{x_2}]_{\underset{R}{\overset{*}{\leftrightarrow}}}\right\}$ and we define the isomorphism λ : $M\longrightarrow A^*/\underset{R}{\overset{*}{\leftrightarrow}}$ by:

$\lambda(x_0)=[\epsilon]_{\underset{R}{\overset{*}{\leftrightarrow}}},\lambda(x_1)=[a_{x_1}]_{\underset{R}{\overset{*}{\leftrightarrow}}},\lambda(x_2)=[a_{x_2}]_{\underset{R}{\overset{*}{\leftrightarrow}}}$. Finally $M\cong A^*/\underset{R}{\overset{*}{\leftrightarrow}}$.

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

Proposition 3.7. *We consider two systems of rewriting $S_1=(A_1,R_1)$, $S_2=(A_2,R_2)$ and $f:A_1^*\longrightarrow A_2^*$ is a morphism of monoids such that for all $(r,s)\in R_1$: $[f(r)]_{\underset{R_2}{\overset{*}{\leftrightarrow}}}=[f(s)]_{\underset{R_2}{\overset{*}{\leftrightarrow}}}$, then there exists a unique morphism $\psi:A_1^*/\underset{R_1}{\overset{*}{\leftrightarrow}}\longrightarrow A_2^*/\underset{R_2}{\overset{*}{\leftrightarrow}}$ with $\psi\circ\pi_{R_1}=\pi_{R_2}\circ f$.*

Proof. We have for all $(r,s)\in R_1:[f(r)]_{\underset{R_2}{\overset{*}{\leftrightarrow}}}=[f(s)]_{\underset{R_2}{\overset{*}{\leftrightarrow}}}$, then the morphism $\pi_{R_2}\circ f$ satisfies the following property: for all $(r,s)\in R_1,(\pi_{R_2}\circ f)(r)=(\pi_{R_2}\circ f)(s)$, then there exists a unique morphism $\psi:A_1^*/\underset{R_1}{\overset{*}{\leftrightarrow}}\longrightarrow A_2^*/\underset{R_2}{\overset{*}{\leftrightarrow}}$ with $\psi\circ\pi_{R_1}=\pi_{R_2}\circ f$. $\square$

Example 3.8. Let $S_1=(A_1,R_1)$ and $S_2=(A_2,R_2)$ be two systems of rewriting, where,

$$\left\{\begin{array}{c}A_1=\{a,b\}\\ R_1=\{(ab,a),(ba,a)\}\end{array}\right.\text{ and }\left\{\begin{array}{c}A_2=\{c,d,e\}\\ R_2=\{(ec,c),(de,d)\}\end{array}\right..$$

We consider the morphism $f:A_1^*\longrightarrow A_2^*$, with $\left\{\begin{array}{c}f(a)=cd\\ f(b)=e\end{array}\right.$.

We have $\pi_{R_2}:A_2^*\longrightarrow A_2^*/\underset{R_2}{\overset{*}{\leftrightarrow}}$ satisfies the following equalities: $\pi_{R_2}(ec)=\pi_{R_2}(c)$ and $\pi_{R_2}(de)=\pi_{R_2}(d)$.

Now we show that for all $(r,s)\in R_1,(\pi_{R_2}\circ f)(r)=(\pi_{R_2}\circ f)(s)$, we have

$(\pi_{R_2}\circ f)(ab)=\pi_{R_2}(cde)=\pi_{R_2}(c)\pi_{R_2}(de)=\pi_{R_2}(c)\pi_{R_2}(d)=\pi_{R_2}(cd)=(\pi_{R_2}\circ f)(a)$.

$(\pi_{R_2}\circ f)(ba)=\pi_{R_2}(ecd)=\pi_{R_2}(ec)\pi_{R_2}(d)=\pi_{R_2}(c)\pi_{R_2}(d)=\pi_{R_2}(cd)=(\pi_{R_2}\circ f)(a)$.

Consequently there exists a unique morphism $\psi:A_1^*/\underset{R_1}{\overset{*}{\leftrightarrow}}\longrightarrow A_2^*/\underset{R_2}{\overset{*}{\leftrightarrow}}$ with $\psi\circ\pi_{R_1}=\pi_{R_2}\circ f$.

Proposition 3.9. *Let $S_1 = (A_1, R_1)$, $S_2 = (A_2, R_2)$ be two systems canonicals and $f : A_1^* \longrightarrow A_2^*$ is a isomorphism of monoids where for all $(r, s) \in R_1$: $[f(r)]_{\underset{R_2}{\overset{*}{\leftrightarrow}}} = [f(s)]_{\underset{R_2}{\overset{*}{\leftrightarrow}}}$ and $f(Irr(R_1)) \subseteq Irr(R_2)$, we have,*

$$A_1^*/ \underset{R_1}{\overset{*}{\leftrightarrow}} \cong A_2^*/ \underset{R_2}{\overset{*}{\leftrightarrow}}.$$

Proof. We have for all $(r, s) \in R_1$: $[f(r)]_{\underset{R_2}{\overset{*}{\leftrightarrow}}} = [f(s)]_{\underset{R_2}{\overset{*}{\leftrightarrow}}}$, then for all $(r, s) \in R_1, (\pi_{R_2} \circ f)(r) = (\pi_{R_2} \circ f)(s)$, then there exists a unique morphism $\psi : A_1^*/ \underset{R_1}{\overset{*}{\leftrightarrow}} \longrightarrow A_2^*/ \underset{R_2}{\overset{*}{\leftrightarrow}}$ with $\psi \circ \pi_{R_1} = \pi_{R_2} \circ f$. Specifically the morphism ψ is defined by:

$\psi\left([x]_{\underset{R_1}{\overset{*}{\leftrightarrow}}}\right) = [f(x)]_{\underset{R_2}{\overset{*}{\leftrightarrow}}}$. We show that ψ is one-to-one: Let $[x]_{\underset{R_1}{\overset{*}{\leftrightarrow}}}, [y]_{\underset{R_1}{\overset{*}{\leftrightarrow}}} \in A_1^*/ \underset{R_1}{\overset{*}{\leftrightarrow}}$, since $S_1 = (A_1, R_1)$ is canonical, then there exists $u, v \in Irr(R_1)$ suth that $[x]_{\underset{R_1}{\overset{*}{\leftrightarrow}}} = [u]_{\underset{R_1}{\overset{*}{\leftrightarrow}}}$ and $[x]_{\underset{R_1}{\overset{*}{\leftrightarrow}}} = [v]_{\underset{R_1}{\overset{*}{\leftrightarrow}}}$.

We have $\psi\left([x]_{\underset{R_1}{\overset{*}{\leftrightarrow}}}\right) = \psi\left([y]_{\underset{R_1}{\overset{*}{\leftrightarrow}}}\right) \Longleftrightarrow \psi\left([u]_{\underset{R_1}{\overset{*}{\leftrightarrow}}}\right) = \psi\left([v]_{\underset{R_1}{\overset{*}{\leftrightarrow}}}\right) \Longleftrightarrow [f(u)]_{\underset{R_2}{\overset{*}{\leftrightarrow}}} = [f(v)]_{\underset{R_2}{\overset{*}{\leftrightarrow}}}$, since $f(Irr(R_1)) \subseteq Irr(R_2)$ and $S_2 = (A_2, R_2)$ is canonical, we have $f(u) = f(v)$, then $u = v$ because f is one-to-one, which shows that $[x]_{\underset{R_1}{\overset{*}{\leftrightarrow}}} = [y]_{\underset{R_1}{\overset{*}{\leftrightarrow}}}$. □

Now we show that ψ is onto: since f is onto, then for all $y \in A_2^*$, there exists $x \in A_1^*$, suth that $y = f(x)$, which allows to write $[y]_{\underset{R_2}{\overset{*}{\leftrightarrow}}} = [f(x)]_{\underset{R_2}{\overset{*}{\leftrightarrow}}} = \psi\left([x]_{\underset{R_1}{\overset{*}{\leftrightarrow}}}\right)$. Finally $A_1^*/ \underset{R_1}{\overset{*}{\leftrightarrow}} \cong A_2^*/ \underset{R_2}{\overset{*}{\leftrightarrow}}$.

Example 3.10. Let $S_1 = (A_1, R_1)$ and $S_2 = (A_2, R_2)$ be two systems of rewriting, where,

$$\begin{cases} A_1 = \{a\} \\ R_1 = \{(aa, \epsilon)\} \end{cases} \text{and} \begin{cases} A_2^* = \mathbb{N} = \langle 1 \rangle \\ R_2 = \{(0+0, 0), (0+1, 1), (1+0, 1), (1+1, 0)\} \end{cases}.$$

We consider the isomorphism of length $f : A_1^* \longrightarrow \mathbb{N}$, $w \longmapsto |w|$.

We have $(\pi_{R_2} \circ f)(aa) = \pi_{R_2}(2) = \pi_{R_2}(0) = (\pi_{R_2} \circ f)(\epsilon)$, and $Irr(R_1) = \{\epsilon, a\}, f(Irr(R_1)) = \{0, 1\} = Irr(R_2)$.

$$\text{Finally } A_1^*/ \underset{R_1}{\overset{*}{\leftrightarrow}} \cong \mathbb{N}/ \underset{R_2}{\overset{*}{\leftrightarrow}}.$$

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 3.11. *Let $f : A^* \longrightarrow M$ be a monoids morphism and R is a binary relation on a set A^* suth that for all $(r, s) \in R, f(r) = f(s)$. Then for all $w \in$*

A^*, the congruence generated by R is included in the syntactic congruence of the equivalence class of w modulo $Ker\ f$ .i.e, $\overset{*}{\underset{R}{\leftrightarrow}} \subseteq \equiv_{[w]_{Ker\ f}}$.

Proof. Since for all $(r,s) \in R, f(r) = f(s)$, we have $R \subseteq Ker\ f$, then $\overset{*}{\underset{R}{\leftrightarrow}} \subseteq Ker\ f$. Now we show that $\overset{*}{\underset{R}{\leftrightarrow}} \subseteq \equiv_{[w]_{Ker\ f}}$, let $(u,v) \in A^* \times A^*$ suth that $u \overset{*}{\underset{R}{\leftrightarrow}} v$, we check that $u \equiv_{[w]_{Ker\ f}} v$, i.e, for all $(x,y) \in A^* \times A^* : xu\mathrm{y} \in [w]_{Ker\ f} \Longleftrightarrow xv\mathrm{y} \in [w]_{Ker\ f}$

We have $xu\mathrm{y} \in [w]_{Ker\ f} \Longleftrightarrow xu\mathrm{y} \in \bigcup_{i\in I} [c_i]_{\overset{*}{\underset{R}{\leftrightarrow}}}$, because $\overset{*}{\underset{R}{\leftrightarrow}} \subseteq Ker\ f$. $\Longleftrightarrow \exists i_0 \in I$ suth that $xu\mathrm{y} \in [c_{i_0}]_{\overset{*}{\underset{R}{\leftrightarrow}}}$, then $xu\mathrm{y} \overset{*}{\underset{R}{\leftrightarrow}} c_{i_0}$. Furthermore $u \overset{*}{\underset{R}{\leftrightarrow}} v$ implies that $xu\,y \overset{*}{\underset{R}{\leftrightarrow}} xvy$. We have $\begin{cases} xu\mathrm{y} \overset{*}{\underset{R}{\leftrightarrow}} c_{i_0} \\ xu\,y \overset{*}{\underset{R}{\leftrightarrow}} xvy \end{cases} \Longrightarrow xv\mathrm{y} \overset{*}{\underset{R}{\leftrightarrow}} c_{i_0}$, then $xv\mathrm{y} \in [w]_{Ker\ f}$.

A similar argument shows that if $xv\mathrm{y} \in [w]_{Ker\ f}$ then $xu\mathrm{y} \in [w]_{Ker\ f}$. Finally $\overset{*}{\underset{R}{\leftrightarrow}} \subseteq \equiv_{[w]_{Ker\ f}}$. □

Example 3.12. Let $A = \{a,b\}$, $R = \{(ab,ba)\}$ and $f : A^* \longrightarrow \mathbb{N}, f(u) = |u|$.

We have $A^*/\overset{*}{\underset{R}{\leftrightarrow}} = \left\{ [b^m a^n]_{\overset{*}{\underset{R}{\leftrightarrow}}}, (m,n) \in \mathbb{N}\times\mathbb{N} \right\}$ and for all $w \in A^*, [w]_{Ker\ f} = \{x \in A^* : |x| = |w|\}$. Now we show that $\overset{*}{\underset{R}{\leftrightarrow}} \subseteq \equiv_{[w]_{Ker\ f}}$, let $(u,v) \in A^* \times A^*$ suth that $u \overset{*}{\underset{R}{\leftrightarrow}} v$, then there exists $(p,q) \in \mathbb{N}\times\mathbb{N} : u \overset{*}{\underset{R}{\leftrightarrow}} b^p a^q$ and $v \overset{*}{\underset{R}{\leftrightarrow}} b^p a^q$, there ($|u|_a = |v|_a = q$ and $|u|_b = |v|_b = p$), we check that $u \equiv_{[w]_{Ker\ f}} v$, i.e, for all $(x,y) \in A^* \times A^* : xu\mathrm{y} \in [w]_{Ker\ f} \Longleftrightarrow xv\mathrm{y} \in [w]_{Ker\ f}$. Let $(x,y) \in A^* \times A^*$, we have
$xu\mathrm{y} \in [w]_{Ker\ f} \Longleftrightarrow |xu\mathrm{y}| = |w| \Longleftrightarrow |xv\mathrm{y}| = |w| \Longleftrightarrow xv\mathrm{y} \in [w]_{Ker\ f}$, because ($|u|_a = |v|_a = q$ and $|u|_b = |v|_b = p$).

Finally $\overset{*}{\underset{R}{\leftrightarrow}} \subseteq \equiv_{[w]_{Ker\ f}}$.

In the following proposition we give also a specific relation R on A^* making the quotient monoid $A^*/\overset{*}{\underset{R}{\leftrightarrow}}$ a group.

Proposition 3.13. *Let $A = \{a_1, ..., a_n\}$ and $R = \{(a_i a_i, \epsilon), 1 \le i \le n\}$.*

We have the quotient monoid $A^*/\overset{*}{\underset{R}{\leftrightarrow}}$ is a group.

Proof. It suffices to show that every element of $A^*/\overset{*}{\underset{R}{\leftrightarrow}}$ is invertible, let $w = a_{i_1}...a_{i_k} \in A^*$, and $[w]_{\overset{*}{\underset{R}{\leftrightarrow}}} \in A^*/\overset{*}{\underset{R}{\leftrightarrow}}$.

we take $\left([w]_{\overset{*}{\underset{R}{\leftrightarrow}}}\right)^{-1} = [\widetilde{w}]_{\overset{*}{\underset{R}{\leftrightarrow}}}$, there $\widetilde{w}$ is The reverse of a word w, we have $[w]_{\overset{*}{\underset{R}{\leftrightarrow}}} \cdot [\widetilde{w}]_{\overset{*}{\underset{R}{\leftrightarrow}}} = [\widetilde{w}]_{\overset{*}{\underset{R}{\leftrightarrow}}} \cdot [w]_{\overset{*}{\underset{R}{\leftrightarrow}}} = [\epsilon]_{\overset{*}{\underset{R}{\leftrightarrow}}}$. □

Example 3.14. Let $A = \{a\}$ and $R = \{(aa, \epsilon)\}$, we have $A^*/\overset{*}{\underset{R}{\leftrightarrow}} = \left\{[\epsilon]_{\overset{*}{\underset{R}{\leftrightarrow}}}, [a]_{\overset{*}{\underset{R}{\leftrightarrow}}}\right\}$, there

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

The Cayley table of $A^*/\overset{*}{\underset{R}{\leftrightarrow}}$ is defined as follows (see Table 1)

		$[\epsilon]_{\overset{*}{\underset{R}{\leftrightarrow}}}$	$[a]_{\overset{*}{\underset{R}{\leftrightarrow}}}$
2	$[\epsilon]_{\overset{*}{\underset{R}{\leftrightarrow}}}$	$[\epsilon]_{\overset{*}{\underset{R}{\leftrightarrow}}}$	$[a]_{\overset{*}{\underset{R}{\leftrightarrow}}}$
	$[a]_{\overset{*}{\underset{R}{\leftrightarrow}}}$	$[a]_{\overset{*}{\underset{R}{\leftrightarrow}}}$	$[\epsilon]_{\overset{*}{\underset{R}{\leftrightarrow}}}$

We have the groups $A^*/\overset{*}{\underset{R}{\leftrightarrow}}$ and $(\mathbb{Z}/2\mathbb{Z}, \oplus)$ are isomorphic.

4. Application on the notion of word problem in public key cryptography

In this work, we are interested in **ATS-monoid** protocol (proposed by **P. J. Abisha, D. G. Thomas G. and K. Subramanian**, the idea of this protocol is to transform a system of **Thue** $S_1 = (A, R)$ for which the word problem is undecidable a system of **Thue** $S_2 = (\Delta, R_\theta)$ or $\theta \subseteq \Delta \times \Delta$ for which the word problem is decidable in linear time.

4.1. The ATS-monoid protocol. **P. J. Abisha**, **D. G. Thomas** and **K. G. Subramanian**, use the theorem of **R. Cori** and **D. Perrin**. To build the ATS-monoid protocol,the idea is transform a system of **Thue** $S_1 = (A, R)$ for which the word problem is undecidable in a **Thue** system $S_2 = (\Delta, R_\theta)$ with $\theta \subseteq \Delta \times \Delta$ and $R_\theta = \{(ab, ba) : (a, b) \in \theta\}$ for which the word problem is decidable in linear time.

Public-Key (pK)**:** A **Thue** system $S_1 = (A, R)$ and two words w_0, w_1 of A^*. (A, R, w_0, w_1) constitute a public-key.

Secret-key (sK)**:** A **Thue** system $S_2 = (\Delta, R_\theta)$ where Δ alphabet of size smaller than A, a morphism h from A^* to Δ^*, such that for all $(r, s) \in R$:

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

Therefore:

$$\text{for all } u, v \in A^*, u \longleftrightarrow_R^* v \Longrightarrow h(u) \longleftrightarrow_{R_\theta}^* h(v).$$

thus if $h(u)$ and $h(v)$ are not equivalent with respect to $\longleftrightarrow_{R_\theta}^*$, then u and v are not equivalent with respect to $\longleftrightarrow_R^*$.

And, we also we have two words x_0, x_1 of Δ^* such that $x_0 \longleftrightarrow_{R_\theta}^* h(w_0), x_1 \longleftrightarrow_{R_\theta}^* h(w_1)$ with $h(w_0)$ and $h(w_1)$ are not equivalent with respect to $\longleftrightarrow_{R_\theta}^*$. $(\Delta, R_\theta, h \in Hom\,(A^*, \Delta^*))$ constitute a secret-key.

Encryption: for encrypt a bit $b \in \{0, 1\}$, **Bob** chooses a word c of A^* in the equivalence class of w_b with respect to $\longleftrightarrow_R^*$, i. e, $c \in [w_b]_{\longleftrightarrow_R^*}$ where $[w_b]_{\longleftrightarrow_R^*}$ denotes the equivalence class of w_b with respect to $\longleftrightarrow_R^*$ and then sent to **Alice**.

Decryption: Upon receipt of a word c of A^*, **Alice** calculated $h(c) \in \Delta^*$, since $c \longleftrightarrow_R^* w_b$ and according to the result for all $u, v \in \Sigma^*, u \longleftrightarrow_R^* v \Longrightarrow$

$h(u) \longleftrightarrow^*_{R_\theta} h(v)$ we have $h(c) \longleftrightarrow^*_{R_\theta} h(w_b)$, for example if $h(c) \longleftrightarrow^*_{R_\theta} x_0$ the message is decrypted 0.

Example :

Public-Key (pK)**:**

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

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

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

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

Secret-key (sK):

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

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

We have $R_\theta = \{(ab, ba), (ac, ca)\}$, $h(w_0) = x_0 = acbabc$ and $h(w_1) = x_1 = acbca$.

Now we verify the following conditions :

1. $h(w_0)$ et $h(w_0)$ are not equivalent with respect to $\longleftrightarrow^*_{R_\theta}$.

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

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

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 $\longleftrightarrow^*_{R_\theta}$.

For condition 2. we have $R = \{(\sigma_2\sigma_3, \sigma_3\sigma_2), (\sigma_2\sigma_4, \sigma_4\sigma_2), (\sigma_1\sigma_3, \sigma_3\sigma_1)\}$ then $(h(\sigma_2\sigma_3), h(\sigma_3\sigma_2)) = (ab, ba) \in R_\theta$, $(h(\sigma_2\sigma_4), h(\sigma_4\sigma_2)) = (ac, ca) \in R_\theta$, $(h(\sigma_1\sigma_3), h(\sigma_3\sigma_1)) = (b, b)$ (we have $h(\sigma_1\sigma_3) = h(\sigma_3\sigma_1)$.

Therefore:

$$\text{for all } u, v \in A^*, u \longleftrightarrow^*_R v \Longrightarrow h(u) \longleftrightarrow^*_{R_\theta} h(v).$$

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

we have $w_0 = \sigma_1\sigma_2\sigma_4\sigma_3\sigma_1\sigma_2\sigma_3\sigma_4 \longleftrightarrow^*_R \sigma_1\sigma_4\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3\sigma_4 \longleftrightarrow^*_R \sigma_1\sigma_4\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3\sigma_4$.

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 $h(c) \longleftrightarrow^*_{R_\theta} h(w_0)$. 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 the 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 $h(c) \longleftrightarrow^*_{R_\theta} h(w_0) = x_0$ and the word is decrypted 0.

5. Conclusion

In this paper, we determine some conditions on the two relations that ensure the existence of a morphism between the two quotient monoids. We give also a specific relation R on A^* making the quotient monoid $A^*/\underset{R}{\overset{*}{\leftrightarrow}}$ a group.

References

[1] Gross, L.: Abstract Wiener spaces, in: *Proc. 5th Berkeley Symp. Math. Stat. and Probab.* **2**, part 1 (1965) 31–42, University of California Press, Berkeley.

[2] Itô, K.: Stochastic integral, *Proc. Imp. Acad. Tokyo* **20** (1944) 519–524.

[3] McKean, H. P.: *Stochastic Integrals*, Academic Press, New York, 1969.

[4] J. Berstel & D. Perrin. "Theoryofcodes", *Academic Press* (1984).

[5] M. Benois, Application de l'étude de certaines congruences à un problème de décidabilité, *Séminaire Dubreil* , n^o 7, (1972).

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

[7] N. Dershowitz, Termination of Rewriting, *Jornal of Symbolic Computation*,vol 3, pp. $69 - 116$, (1987).

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

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

[10] R. Floyd, R. Beigel, Traduction de D. Krob, Le langage des machines, *International Thomson France, paris*, (1995).

[11] Y. Metivier, Calcul de longueurs de chaînes de réécriture dans le monoïde libre", *Theoretical Computer Science*, vol 35, pp. $71 - 87$, (1985).

[12] L. Perret, Etude d'outils algébriques et combinatoires pour la cryptographie à clef publique,*thèse de doctorat, Universite de Marne–la–Vallée*, (2005).

[13] H. Phan, P. Guillot, Preuves de sécurité des schémas cryptographiques, *université Paris 8*, (2013).

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

[15] Y. Lafont, A new finiteness condition for monoids presented by complete rewriting systems (after Craig C. Squier)", *Journal of Pur and Applied Algebra*, vol 98, pp. $229 - 244$, (1995).

[16] Y. Lafont, Réécritue et problème du mot, *Gazette des Mathématiciens*, pp. $27 - 38$, (2009).

[17] M. Lohrey, The Compressed Word Problem for Groups, *Springer* (2014).

[18] M. Nivat. Sur le noyau d'un morphisme du monoïde libre, *Proceedings de Séminaire Schutzenberger*, vol 1, pp. $1 - 6$, (1970).

[19] D. Kapur and P. Narendran,A Finite Thue System With Decidable Word Problem And Without Equivalent Finite Canonical System, *Theoretical Computer Science*, vol 35, pp. $337 - 344$, (1985).

[20] S. Qiao, W. Han, Y. Li and L. Jiao, Construction of Extended Multivariante Public Key Cryptosystems, *International Journal of Network Security*, Vol. 18, No.1, pp. 60-67, (2016).

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

[22] R. V. Book, H. N. Liu, Rewriting Systems and Word Problems in a Free Partially Commutative Monoid, *Information Processing Letters* n^o 26, p. 29-32, (1987).

NACER GHADBANE: LABORATORY OF PURE AND APPLIED MATHEMATICS, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF M'SILA, ALGERIA.
E-mail address: nacer.ghadbane@yahoo.com

DOUADI MIHOUBI: LABORATORY OF PURE AND APPLIED MATHEMATICS, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF M'SILA, ALGERIA
E-mail address: mihoubi_douadi@yahoo.fr