# Word problem for groups and monoids

by

Boikanyo Makubate

A thesis submitted to the Faculty of Science, University of Glasgow, for the degree of Masters of Science

Department of Mathematics,

University of Glasgow

September 1998

# Contents

Acknowledgements

I would like to express my deepest thanks to my supervisor, Prof. S. J. Pride, for all his inspiration, guidance, and encouragement during the research and preparation of this work.

I also wish to express my gratitude to Dr. P. Fisher and the late Mr F. Bonang in University of Botswana for they first introduced me to the world of group theory; to Dr Fix Mothebe in University of Botswana for his kindness and his valueable advises during my studies in the University of Botswana.

Thanks are also due to the staff and all postgraduate students of the Department of Mathematics, University of Glasgow for all their kindness and help.

Also, I would like to thank all my friends for all assistance and support.

Finally, special thanks to my family; my mum Kgakgamatso, my brother Ludza and my two sisters MmaNeo and Thatayaone, whose love, support and understanding have made this thesis possible.

Summary

Chapter 1 defines basic ideas such as definition of monoids, homomorphisms of monoids, congruences, factor monoids, free monoids, monoid presentations (rewriting systems), homomorphisms of monoids defined by presentations into known monoids, equivalent rewriting system, Tietze transformation and noetherian induction.

In chapter 2 we give definitions of some properties of rewriting systems, eg noetherian, confluency, locally confluency and completeness. We also mention some well known reduction orderings. Some important theorems and lemmas are proved, which will later be used in the thesis. We define what is meant by a monoid to be left (right) $FP_{\infty}$.

In chapter 3 we constuct free groups, free product of two monoids, monoids with amalgamated submonoids, HNN-extension in monoids and finally monoids with commutative submonoids using the concept of monoid presentations (rewriting system). The irreducibles of each presentation is discussed. And in each presentation, we emphasize that the irreducibles are unique, using theorems and lemmas proved in chapter 2.

The word problem for monoids and groups is discussed in chapter 4. Examples of groups and monoids with solvable (unsolvable) word problem are given. We discuss residual properties of a monoid (group) and prove that residually finite monoids have solvable word problem.

Statement

In preparing this thesis, I have tried to emphasize the concept of rewriting systems (monoid presentations). I have used the concept of rewriting systems to solve some problems, solutions of which have been extensively discussed (in groups). In this thesis, mostly we will be working with monoids. Among the more significant problems are the following:

(1) Normal for theorems for free groups, free product of two monoids, free products of two monoids with amalgamated submonoids, HNN-extension in monoids, and monoids with commutative submonoids.

(2) Word problem for groups and monoids.

Chapter 1 covers basic material, mainly on monoids. This material can be found in [21], [29], [30], [50].

In Chapter 2 we consider some important theorems and lemmas concerning rewiting systems. These had earlier been discussed, for example in [4], [13], [30], [48], [61]. I have given my own proofs of the main results (Theorems 2.2.1, 2.3.1).

The aim of Chapter 3 (which is the main chapter of the thesis) is to give a unified approach to various normal form theorems for various group (and monoid) constructions by viewing the constructions as complete rewriting systems. Many of these normal form theorems can be found in standard texts on group theory, such as [14], [26], [44], [59]. The inspiration to consider complete rewriting systems came from one of the proofs of the normal form theorem for free groups in [14], and work of Dekov in [16, 17]. The proofs given here are my own work (the proof in Section 3.6 was obtained jointly with my supervisor). The results of Section 3.2 and Section 3.3, for groups can be found, for example in [14], [44], [59]. The results of Deko V. Dekov [16] are modified to prove the result of Section 3.5. The results of Section 3.6 can be found (alternatively) in Deko V. Dekov [17]. The result of Section 3.7 appears to be new and is my own work.

Chapter 4 covers topics such as the word problem for monoids and groups, residual properties of monoids (groups). This material can be found, for example, in [1], [2], [3], [11].

# Chapter 1

# Preliminaries

## 1.1 Monoids

A *monoid* is a set $M$ together with a binary operation called *multiplication* (denoted by $\cdot$) such that multiplication is associative, i.e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in M$. And $M$ contains an identity element $e$ such that $a \cdot e = e \cdot a = a$ for all $a \in M$. (Normally we omit the dot and just write $ab$ instead of $a \cdot b$.) We remark that the identity of $M$ is unique and we usually denote it by 1.

**Examples 1.1.1** *The set of positive integers under multiplication is a monoid with identity* 1.

**Example 1.1.2** *The set of non-negatives integers is a monoid under addition with identity* 0. *We denote this monoid by* $\mathbb{Z}^+$.

**Example 1.1.3** *Let* $R$ *be a ring with* 1. *Then* $M_n(R)$ *the set of* $n \times n$

*matrices over R is a monoid under multiplication. The identity is the* $n \times n$ *matrix* $I_n$.

**Example 1.1.4** *The set* $\mathcal{P}\mathfrak{T}(\mathbf{x})$ *of partial transformation on the set* $\mathbf{x}$ *is a monoid under partial composition. The identity is the function*

$$i : \mathbf{x} \longrightarrow \mathbf{x}$$

$$x \mapsto x \ (x \in \mathbf{x}).$$

**Example 1.1.5** *The set* $\mathfrak{T}(\mathbf{x})$ *of full transformation of* $\mathbf{x}$ *is a monoid.*

A subset $S$ of a monoid $M$ is called a *submonoid* if it is closed under multiplication and contains the identity of $M$.

**Example 1.1.6** *Let* $\mathbf{x} = \{1, 2\}$. *Then*

$$\mathcal{P}\mathfrak{T}(\mathbf{x}) = \{\begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ - & - \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 1 & - \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ - & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}\},$$

*is a monoid. And*

$$\mathfrak{T}(\mathbf{x}) = \{\begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}\}.$$

*is a submonoid of* $\mathcal{P}\mathfrak{T}(\mathbf{x})$.

**Lemma 1.1.1** *The intersection of submonoids* $(\bigcap_{i \in I} S_i)$ *is a submonoid.*

**Proof** Since $S_i$ for any $i \in I$ is a submonid, then $1 \in S_i$ for any $i \in I$. So $1 \in \bigcap_{i \in I} S_i$. For any $x, y \in \bigcap_{i \in I} S_i$ then $x, y \in S_i$ for all $i \in I$. So $xy \in S_i$ for all $i \in I$. Hence $xy \in \bigcap_{i \in I} S_i$. Thus $\bigcap_{i \in I} S_i$ is a submonoid.□

Let $A$ be a non-empty subset of a monoid $S$. Consider $\mathfrak{X} = \{T : T$ is a submonoid of $S$, $A \subseteq T\}$. Of course $\mathfrak{X}$ is not empty since $S \in \mathfrak{X}$, so we can form the intersection $\bigcap_{T \in \mathfrak{X}}$. This intersection contains $A$ as a subset, and is a submonoid of $S$ by Lemma 1.1.1. Hence $\bigcap_{T \in \mathfrak{X}}$ is one of the elements of $\mathfrak{X}$, and is the smallest submonoid of $S$ containing $A$. We denote the smallest submonoid by $< A >$ called the *submonoid generated by* $A$.

We say that $A$ *generates* $S$ if $< A >= S$.

**Example 1.1.7** *The monoid* $\mathbb{Z}^+$ *as in Example* 1.1.2 *is generated by* $\{1\}$.

**Theorem 1.1.2** $< A >$ *consists of* $1_S$, *together with all elements of* $S$ *which can be expressed as a product of the form*

$$a_1 a_2 \cdots a_m \ (m \geq 1, a_1, a_2, a_3, \cdots, a_m \in A).$$

**Proof** Let $B$ be the set containing $1_S$, and all elements of $S$ which can be written as a product of elements of $A$. We will show that $B =< A >$ . Since $A \subseteq< A >$ and since $< A >$ is a submonoid, we must have that any product of elements of $A$ is in $< A >$ . Also $1_S \in< A >$ . Thus $B \subseteq< A >$ . Now let $W, W' \in B$. If one of

$W, W' = 1_S$, then clearly $WW' \in B$. Otherwise we have

$$W = a_1a_2a_3 \cdots a_r,\ W' = a'_1a'_2a'_3 \cdots a'_s\ (a_1, a_2, \cdots, a_r, a'_1, a'_2, \cdots, a'_s \in A, r, s \geq 1).$$

Then $WW' = a_1a_2a_3 \cdots a_ra'_1a'_2a'_3 \cdots a'_s \in B$. Also by assumption $1_S \in B$. Thus $B$ is a submonoid containing $A$. But $< A >$ is the smallest monoid containing $A$, thus we must have $< A > \subseteq B$. Hence $< A > = B$.□

## 1.2 Homomorhisms of monoids

A *homomorphism* from a monoid $S$ to a monoid $T$ is a function

$$\phi : S \longrightarrow T$$

such that

$$\phi(1_S) = 1_T \text{ and } \phi(ss') = \phi(s)\phi(s') \text{ for all } s, s' \in S.$$

**Example 1.2.1** *Let $R$ be a ring with 1. Let $R^\times$ denote $R$ under multiplication. Then $R^\times$ is a monoid.*

$$\phi : M_n(R) \longrightarrow R^\times$$
$$m \mapsto det(m)\ (m \in M_n(R)),$$

*is a monoid homomorphism.*

**Lemma 1.2.1** *If*

$$\phi : S \longrightarrow T$$

*is a monoid homomorphism then*

$$Im\phi = \{\phi(s) : s \in S\}$$

*is a submonoid of T.*

**Proof** Let $t, t' \in Im\phi$, thus there exist $s, s' \in S$ such that

$$\phi(s) = t \text{ and } \phi(s') = t'.$$

Hence

$$tt' = \phi(s)\phi(s') = \phi(ss') \text{ (since } \phi \text{ is a homomorphism).}$$

Thus $tt' \in Im\phi$. Also $\phi(1_S) = 1_T$, thus $1_T \in Im\phi$. Hence $Im\phi$ is a submonoid of $T$.□

An *isomorphism* is a homomorphism that is also bijective.

If $\psi : S \longrightarrow T$ and $\phi : T \longrightarrow T'$ are homomorphisms, then so is the composition $\phi \circ \psi$.

A homomorphism $\phi : S \longrightarrow S$ is called an *endomorphism* of $S$. The set of all endomorphisms of $S$ denoted by $End(S)$ with multiplication defined as composition is a monoid.

**Theorem 1.2.2** (*Cayley's Theorem*) *Every finite monoid is isormorphic to a submonoid of a full transformation monoid* $\mathfrak{T}_n$, *for some* $n \in \mathbb{Z}^+$.

**Proof** Let $M$ be a monoid with $n$ elements $\{x_1, x_2, \cdots x_n\}$, and let $x_1 = 1_M$. Then for each $m \in M$

$$x_1m, x_2m, \cdots x_nm \in M, \text{ (since } M \text{ is closed under multiplication).}$$

Define the mapping

$$\theta : M \longrightarrow \mathfrak{T}(M)$$

$$m \mapsto \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1 m & x_2 m & \cdots & x_n m \end{bmatrix}.$$

Suppose

$$\theta(m_1) = \theta(m_2) \text{ (for some } m_1, m_2 \in M).$$

Then

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1 m_1 & x_2 m_1 & \cdots & x_n m_1 \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1 m_2 & x_2 m_2 & \cdots & x_n m_2 \end{bmatrix}$$

Thus $x_1 m_1 = x_1 m_2$. Since $x_1 = 1_M$, then $m_1 = m_2$. Hence $\theta$ is injective. For any $m_1, m_2 \in M$, we have

$$\theta(m_1 m_2) = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1 m_1 m_2 & x_2 m_1 m_2 & \cdots & x_n m_1 m_2 \end{bmatrix} =$$

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1 m_1 & x_2 m_1 & \cdots & x_n m_1 \end{bmatrix} \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1 m_2 & x_2 m_2 & \cdots & x_n m_2 \end{bmatrix} = \theta(m_1)\theta(m_2).$$

Clearly $\theta(1_M) = 1_{\mathfrak{T}(M)}$. Hence $\theta$ is an injective homomorphism, so $M$ is isomorphic to $Im\theta$ a submonoid of $\mathfrak{T}(M)$.□

**Example 1.2.2** *Let M be the monoid defined by the multiplication table below.*

| $\bullet$ | $1$ | $z$ | $x$ | $y$ |
|---|---|---|---|---|
| $1$ | $1$ | $z$ | $x$ | $y$ |
| $z$ | $z$ | $z$ | $z$ | $z$ |
| $x$ | $x$ | $y$ | $1$ | $z$ |
| $y$ | $y$ | $y$ | $y$ | $y$ |

*Then*

$$\theta : M \longrightarrow \mathfrak{T}(M)$$

is the mapping

$$1 \mapsto \begin{bmatrix} 1 & z & x & y \\ 1 & z & x & y \end{bmatrix}$$
$$z \mapsto \begin{bmatrix} 1 & z & x & y \\ z & z & y & y \end{bmatrix}$$
$$x \mapsto \begin{bmatrix} 1 & z & x & y \\ x & z & 1 & y \end{bmatrix}$$

*relation,* $\rho_\phi$ *on* $S$ *by* $x\rho_\phi y$ *if* $\phi(x) = \phi(y)$*. Then clearly* $\rho_\phi$ *is an equivalence relation. Now suppose* $x\rho_\phi y$ *and let* $s \in S$*. Thus* $\phi(x) = \phi(y)$*. We are to show that* $xs\rho_\phi ys$*, thus to show that* $\phi(xs) = \phi(ys)$*. But*

$$\begin{aligned} \phi(xs) &= \phi(x)\phi(s) \\ &= \phi(y)\phi(s) \\ &= \phi(ys). \end{aligned}$$

*Similarly* $sx\rho_\phi sy$*. Hence* $\rho_\phi$ *is a congruence.*

We call $\rho_\phi$ the *congruence determined by* $\phi$. (We remark that $\rho_\phi$ is also called the *kernel of* $\phi$, though we will not use this terminology.)

Congruences plays the role for monoids as normal subgroups do for groups. We remark that congruences are *relations* on the monoid $S$ whereas normal subgroups are *subobjects*.

Let $\rho$ be a congruence on the monoid $S$. For $s \in S$ let $[s] = \{x \in S : x\rho s\}$, thus the *congruence class* of $s$.

**Lemma 1.3.1** *If* $s\rho s_1$ *and* $s'\rho s'_1$, then $ss'\rho s_1 s'_1$.

**Proof** We have $s\rho s_1$ and since $\rho$ is a congruence, then $ss'\rho s_1 s'$. Similarly, since $s'\rho s'_1$, then $s_1 s'\rho s_1 s'_1$. Hence by transitivity $ss'\rho s_1 s'_1$.□

We define multiplication of congruence classes $[s], [s']$ as follows:

$$y \mapsto \begin{bmatrix} 1 & z & x & y \\ & & & \\ y & z & z & y \end{bmatrix}.$$

**Lemma 1.2.3** *Let $M$ be a monoid generated by a set $A$. Then if we have two homomorphisms*

$$\alpha, \beta : M \longrightarrow K \text{ (where } K \text{ is any monoid)}$$

*such that $\alpha|_A = \beta|_A$, then $\alpha = \beta$.*

**Proof** Let $m \in M$. If $m = 1_M$ then $\alpha(1_M) = \beta(1_M)$. If $m \neq 1_M$ then by Theorem 1.1.2, $m$ can be written as a product of elements of $A$. So suppose

$$m = a_1 a_2 a_3 a_4 \cdots a_{n-1} a_n \ (a_1, a_2, \cdots, a_n \in A, n \geq 1).$$

Thus

$$\begin{aligned} \alpha(m) &= \alpha(a_1)\alpha(a_2)\alpha(a_3)\alpha(a_3) \cdots \alpha(a_{n-1})\alpha(a_n) \text{ (since } \alpha \text{ is a homomorphism)} \\ &= \beta(a_1)\beta(a_2)\beta(a_3)\alpha(a_4) \cdots \beta(a_{n-1})\beta(a_n) \text{ (since } \alpha|_A = \beta|_A) \\ &= \beta(m) \text{ (since } \beta \text{ is a homomorphism).} \end{aligned}$$

Hence $\alpha = \beta$.□

## 1.3 Congruences and factor monoids

Let $S$ be a monoid. A *congruence* on $S$ is an equivalence relation $\rho$ with the property that whenever $x\rho y$ and $s \in S$, then $xs\rho ys$ and $sx\rho sy$.

**Example 1.3.1** *Let $\phi : S \longrightarrow T$ be a monoid homomorphism. Define a*

$$[s][s'] = [ss'] \ (s, s' \in S),$$

which is well defined by Lemma 1.3.1.

Let $S|_\rho$ be the set of congruence classes defined above.

**Lemma 1.3.2** *The congruence classes $S|_\rho$, under the multiplication defined above form a monoid. The identity is* $[1]$.

**Proof** The set $S|_\rho$ is closed under the defined multiplication. Now let $[s_1], [s_2], [s_3] \in S|_\rho$, then

$$\begin{aligned} ([s_1][s_2])[s_3] &= [s_1 s_2][s_3] \\ &= [(s_1 s_2) s_3] \\ &= [s_1 (s_2 s_3)] \\ &= [s_1][s_2 s_3] \\ &= [s_1]([s_2][s_3]). \end{aligned}$$

Now let $[s] \in S|_\rho$, then

$$\begin{aligned} [1][s] &= [1s] \\ &= [s]. \end{aligned}$$

Similarly $[s][1] = [s]$. Hence $S|_\rho$ is a monoid.□

We call $S|_\rho$ the *factor monoid* or *quotient monoid.*

**Theorem 1.3.3** (*First Isomorphism Theorem*) *Let*

$$\phi : S \longrightarrow T$$

*be a monoid homomorphism. Let* $\rho_\phi$ *be the congruence on* $S$ *determined by* $\phi$*, then* $S|_{\rho_\phi}$ and $Im\phi$ *are isomorphic.*

**Proof** Define

$$\phi_* : S|_{\rho_\phi} \longrightarrow T \text{ by}$$
$$[s] \mapsto \phi(s) \ (s \in S).$$

This is well defined since if we choose another representative $s'$ of the congruence class $[s]$, then $s\rho_\phi s'$ so $\phi(s) = \phi(s')$.

Now observe that $\phi_*$ is a homomorphism since for any $[s_1], [s_2] \in S|_{\rho_\phi}$, then

$$\begin{aligned}
\phi_*([s_1][s_2]) &= \phi_*([s_1 s_2]) \\
&= \phi(s_1 s_2) \\
&= \phi(s_1)\phi(s_2) \\
&= \phi_*([s_1])\phi_*([s_2]).
\end{aligned}$$

Also

$$\begin{aligned}
\phi_*([1_S]) &= \phi(1_S) \\
&= 1_T.
\end{aligned}$$

Thus $\phi_*$ is a homomorphism. Moreover, $\phi_*$ is injective. Since if

$$\phi_*([s_1]) = \phi_*([s_2]), \text{ then } \phi(s_1) = \phi(s_2).$$

Thus by definition of $\rho_\phi$, $s\rho_\phi s'$. Hence $[s] = [s']$. Of course $Im\phi_* = Im\phi$. Hence

$$\phi_* : S|_{\rho_\phi} \longrightarrow Im\phi$$

is an isomorphism.□

## 1.4 Free monoids

Let $\mathbf{x}$ be a non-empty set, then a *word* on $\mathbf{x}$ is just a finite sequence of elements of $\mathbf{x}$. In particular, we have the *empty* word containing no letters denoted by $\epsilon$. We remark that this notation is not universal, other notations are $1, \emptyset$. If $W', W''$ are words, then the word

$$W = W'W''$$

is the word obtained by *concatenation* ($W'$ followed by $W''$). We call $W'$ and $W''$ *left* and *right factors* of $W$ respectively.This multiplication is easily shown to be associative. Also for any word $W$, then

$$\epsilon W = W = W\epsilon,$$

so the empty word $\epsilon$ is an identity. Thus the set of words with the above defined multiplication (concatenation) is a monoid, called the *free monoid* on $\mathbf{x}$, and is denoted by $\mathbf{x}^*$. We denote the length of any word $W$ by $L(W)$. For any non-empty word

$$W = x_1x_2x_3\cdots x_n \ (x_1, x_2, \cdots, x_n \in \mathbf{x}, n \geq 1)$$

then $x_1$ and $x_n$ are called the *initial* and *terminal* letters of $W$ respectively. A word $Q$ is called a subword of $W$ if there exist a left factor $W'$ of $W$ and a right factor $W''$ of $W$ such that

$$W = W'QW''.$$

A word $W$ is *unborded* if none of its right factors is a left factor of $W$, except $W$ itself and the empty word.

**Theorem 1.4.1** (*Universal property of free monoids*) *Any function*

$$\psi : \mathbf{x} \longrightarrow M,$$

*where $M$ is a monoid, has a unique extension to a monoid homomorphism*

$$\psi_* : \mathbf{x}^* \longrightarrow M,$$

**Proof** Let $M$ be a monoid, and suppose we are given a function

$$\psi : \mathbf{x} \longrightarrow M$$

$$x \mapsto m_x \ (x \in \mathbf{x}, m_x \in M).$$

Then we can extend $\psi$ to a function $\psi_*$ as follows. Define

$$\psi_* : \mathbf{x}^* \longrightarrow M$$

$$\psi_*(\epsilon) = 1_M$$

and if $W = x_1 x_2 \cdots x_{n-1} x_n$ $(x_1, x_2, \cdots, x_n \in \mathbf{x}, n \geq 1)$ is a non-empty word then

$$\psi_*(W) = m_{x_1} m_{x_2} m_{x_3} \cdots m_{x_{n-1}} m_{x_n} \text{ (product in } M).$$

Then clearly $\psi_*$ is a homomorphism, and it agrees with $\psi$ on $\mathbf{x}$. Now suppose $\phi$ is another extension of $\psi$ ($\phi$ is a homomorphism). Then

$$\phi|_{\mathbf{x}} = \psi_*|_{\mathbf{x}} = \psi.$$

Since $\mathbf{x}$ generates $\mathbf{x}^*$ it follows from Lemma 1.2.3 that $\phi = \psi_*$.□

## 1.5 Monoid presentations (rewriting systems)

A *monoid presentation* or *rewriting system*

$$\mathcal{P} = [\mathbf{x};\mathbf{r}]$$

is a pair, where $\mathbf{x}$ is a set (the *generating symbols* or *alphabets*) and $\mathbf{r}$ consists of ordered pairs of words on $\mathbf{x}$ (*defining relations* or *rewriting rules*). A typical element of $\mathbf{r}$ will have the form $(R_{+1}, R_{-1})$ where $R_{+1}, R_{-1}$ are words on $\mathbf{x}$. We denote this by $R : R_{+1} = R_{-1}$ or simply by $R_{+1} = R_{-1}$. We say that $\mathcal{P}$ is *finite* if $\mathbf{x}$ and $\mathbf{r}$ are both finite (see also [63]).

We define an *elementary transformation* as follows: if a word contains a sub-word $R_\varepsilon$ ($\varepsilon = \pm 1$), for some $R \in \mathbf{r}$, then replace that occurrence of $R_\varepsilon$ by $R_{-\varepsilon}$.

If a word $W'$ is obtained from a word $W$ by replacing $R_{+1}$ with $R_{-1}$, then we denote the process by $W \to_{\mathcal{P}} W'$ or simply $W \to W'$, and we say that $W'$ is obtained from $W$ by applying a single *positive transformation*. If $W'$ is obtained from $W$ by finitely applying positive transformations, then we denote the process by $W \to_{\mathcal{P}}^* W'$ or simply $W \to^* W'$. Similarly we have *negative* transformations.

If $W$ is obtained from $W'$ by applying a finite number of elementary transformations, we write $W \leftrightarrow_{\mathcal{P}}^* W$ or simply $W \leftrightarrow^* W$ (Note that $\leftrightarrow^*$ is an equivalence relation). And we say $W, W'$ are *equivalent*. We denote the equivalece class containing the word $W$ by $[W]_{\mathcal{P}}$ or simply $[W]$.

**Example 1.5.1** *Let* $\mathcal{P} = [a, b; ab = b^2, ba = a^2]$, *and let* $W, W'$ *be the words* $aba, ba^2$ *respectively. Then*

$$\underline{ab}a \to b\underline{ba} \to ba^2.$$

*So* $W \to^* W'$.

**Example 1.5.2** *The words*

$$W = b^2a \text{ and } W' = a^3$$

*are equivalent since*

$$\underline{bb}a \leftarrow a\underline{ba} \to a^3.$$

*So* $W \leftrightarrow^* W'$.

**Lemma 1.5.1** $\leftrightarrow^*$ *is a congruence.*

**Proof** Let $W, W', Y \in \mathbf{x}^*$ and suppose that $W \leftrightarrow^* W'$. We want to show that $WY \leftrightarrow^* W'Y$ and $YW \leftrightarrow^* YW'$.

**Special case:** Suppose $W'$ is obtained from $W$ by just applying a single elementary transformation, say

$$W = UR_{+\varepsilon}V \text{ and } W' = UR_{-\varepsilon}V \ (U, V \in \mathbf{x}^*).$$

Then

$$WY = UR_{+\varepsilon}VY \text{ and } W'Y = UR_{-\varepsilon}VY.$$

Hence $W'Y$ is obtained from $WY$ by applying a single elementary transformation. Thus

$$W'Y \leftrightarrow^* WY.$$

Similarly $YW' \leftrightarrow^* YW$.

**General case:** Suppose there exists a chain

$$W = W_0, W_1, W_2 \cdots W_n = W'$$

such that each $W_{i+1}$ is obtained from $W_i$ ($i = 0, 1, 2, \cdots, n-1$) by applying a single elementary transformation. Then by the special case each

$$W_iY \leftrightarrow^* W_{i+1}Y.$$

Hence by transitivity,

$$WY \leftrightarrow^* W'Y.$$

Similarly $YW \leftrightarrow^* YW'$. Hence the equivalence relation $\leftrightarrow^*$ is a congruence.□

By Lemma 1.3.2, $\mathbf{x}^*/\leftrightarrow^*$ is a monoid. We denote the factor monoid $\mathbf{x}^*/\leftrightarrow^*$ by $M(\mathcal{P})$. We call $M(\mathcal{P})$ *the monoid defined by* $\mathcal{P}$.

## 1.6 Homomorphisms of monoids defined by presentations into known monoids

Let

$$\mathcal{P} = [\mathbf{x};\mathbf{r}]$$

be a monoid presentation, and let $K$ be any arbitrary monoid. Suppose we have a function

$$\psi : \mathbf{x} \longrightarrow K$$

$$\psi(x) = k_x \ (x \in \mathbf{x}, k_x \in K).$$

By Lemma 1.2.3, there can be at most one homomorphism

$$(*) \qquad \psi_{\mathcal{P}} : M(\mathcal{P}) \longrightarrow K$$

$$\bar{x} = [x]_{\mathcal{P}} \mapsto k_x \ (x \in \mathbf{x}).$$

We give the necessary and sufficient conditions for such a homomorphism to exist. By Theorem 1.4.1 there is a unique monoid homomorphism

$$\mathbf{x}^* \longrightarrow K$$

extending $\psi$. We will denote here this homomorphism by the same letter $\psi$ (rather than using $\psi_*$).

**Lemma 1.6.1** *The following are equivalent;*

*(i) For all* $W, W' \in \mathbf{x}^*$ *if* $W \leftrightarrow^* W'$ *then* $\psi(W) = \psi(W')$;

*(ii)* $\psi(R_{+1}) = \psi(R_{-1})$ *for all* $R \in \mathbf{r}$.

**Proof** $(i) \Rightarrow (ii)$. Since $R_{+1} \leftrightarrow^* R_{-1}$ for all $R \in \mathbf{r}$, if $(i)$ holds then we must have $\psi(R_{+1}) = \psi(R_{-1})$.

$(ii) \Rightarrow (i)$. Let $W \leftrightarrow^* W'$.

**Special case:** Say $W = UR_{+\varepsilon}V$ and $W' = UR_{-\varepsilon}V$, where $R \in \mathbf{r}$ and $\varepsilon = \pm 1$, i.e $W$ is obtained from $W'$ by applying a single elementary transformation. Then

$$\begin{aligned} \psi(W) &= \psi(UR_{+\varepsilon}V) \\ &= \psi(U)\psi(R_{+\varepsilon})\psi(V) \\ &= \psi(U)\psi(R_{-\varepsilon})\psi(V) \\ &= \psi(UR_{-\varepsilon}V) \\ &= \psi(W'). \end{aligned}$$

**General case:** Suppose we have the sequence

$$W = W_0, W_1, W_2 \cdots W_n = W'$$

where $W_i$ is obtained from $W_{i+1}$ $(i = 0, 1, 2, \cdots, n-1)$ by applying a single elementary transformation. Then it follows from the special case that each

$$\psi(W_i) = \psi(W_{i+1}).$$

Hence by transitivity we will obtain that

$$\psi(W) = \psi(W'). \square$$

**Theorem 1.6.2** *The homomorphism $\psi_{\mathcal{P}}$ as in $(*)$ exists if and only if $\psi(R_{+1}) = \psi(R_{-1})$ for all $R \in \mathbf{r}$.*

**Proof** Suppose $\psi(R_{+1}) = \psi(R_{-1})$ for all $R \in \mathbf{r}$. Then by Lemma 1.6.1 the mapping

$$\psi_{\mathcal{P}} : M(\mathcal{P}) \longrightarrow K$$

$$[W] \mapsto \psi(W) \ (W \in \mathbf{x}^*)$$

is well defined. We show that $\psi_{\mathcal{P}}$ is a homomorphism. Let $[W], [W'] \in M(\mathcal{P}]$ then

$$\begin{aligned}\psi_{\mathcal{P}}([W][W']) &= \psi_{\mathcal{P}}([WW']) \\ &= \psi(WW') \\ &= \psi(W)\psi(W') \\ &= \psi_{\mathcal{P}}([W])\psi_{\mathcal{P}}([W']).\end{aligned}$$

We remark that $\psi(WW') = \psi(W)\psi(W')$ holds, since $\psi$ is a homomorphism. Also

$$\begin{aligned}\psi_*(1_{M(\mathcal{P})}) &= \psi(\epsilon) \\ &= 1_K.\end{aligned}$$

Hence $\psi_{\mathcal{P}}$ is a homomorphism.

Conversely, suppose there is a homomorphism

$$\psi_{\mathcal{P}} : M(\mathcal{P}) \longrightarrow K$$

$$[W] \mapsto \psi(W) \ (W \in \mathbf{x}^*).$$

We show that $\psi(R_{+1}) = \psi(R_{-1})$ for any $R \in \mathbf{r}$. Since $[R_{+1}] = [R_{-1}]$ and $\psi_{\mathcal{P}}$ is well defined, then

$$\psi_{\mathcal{P}}([R_{+1}]) = \psi_{\mathcal{P}}([R_{-1}]).$$

But

$$\psi_{\mathcal{P}}([R_{+1}]) = \psi(R_{+1}) \text{ (by definition of } \psi_{\mathcal{P}}).$$

Similarly,

$$\psi_{\mathcal{P}}([R_{-1}]) = \psi(R_{-1}).$$

Hence $\psi(R_{+1}) = \psi(R_{-1})$.$\square$

**Example 1.6.1** *Let*

$$\mathcal{P} = [a, b, ; ab = ba]$$

*Define*

$$\psi : a, b \longrightarrow M_3(\mathbb{Z})$$
$$a \longmapsto \begin{bmatrix} 1 & 2 & 2 \\ 0 & 2 & 2 \\ 0 & 0 & 0 \end{bmatrix}$$
$$b \longmapsto \begin{bmatrix} 0 & 2 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

*Then it is easily checked that* $\psi(ab) = \psi(ba)$. *Hence we have an induced homomorphism*

$$\psi_{\mathcal{P}} : M(\mathcal{P}) \longrightarrow M_3(\mathbb{Z})$$
$$[W] \mapsto \psi(W).$$

**Example 1.6.2** *Let* $\mathcal{P}' = [a, b; ab^2 = ba]$. *Define* $\psi$ *as in Example* 1.6.1. *Then*

$$\psi(ab^2) \neq \psi(ba).$$

*So there is no homomorphism*

$$\psi_{\mathcal{P}} : M[\mathcal{P}'] \longrightarrow M_3(\mathbb{Z})$$

*with* $\psi_{\mathcal{P}'}([a]) = \psi(a)$, $\psi_{\mathcal{P}'}([b]) = \psi(b)$.

## 1.7 Equivalent rewriting system, Tietze transformation

Two rewriting systems

$$\mathcal{P}_1 = [\mathbf{x}; \mathbf{r}],\ \mathcal{P}_2 = [\mathbf{y}; \mathbf{s}]$$

are said to be *equivalent* if $\mathbf{x} = \mathbf{y}$ and $\leftrightarrow^*_{\mathcal{P}_1}$, $\leftrightarrow^*_{\mathcal{P}_2}$ are the same congruence, in other words if

$$M(\mathcal{P}_1) = M(\mathcal{P}_2).$$

**Lemma 1.7.1** *Two rewriting systems* $\mathcal{P}_1 = [\mathbf{x}; \mathbf{r}]$, $\mathcal{P}_2 = [\mathbf{y}; \mathbf{s}]$ *are equivalent if and only if*

$(i)$ $\mathbf{x} = \mathbf{y}$;

$(ii)$ *for each* $R \in \mathbf{r}$, $[R_{+1}]_{\mathcal{P}_2} = [R_{-1}]_{\mathcal{P}_2}$;

$(iii)$ *for each* $S \in \mathbf{s}$, $[S_{+1}]_{\mathcal{P}_1} = [S_{-1}]_{\mathcal{P}_1}$.

**Proof** Suppose $\mathcal{P}_1$ and $\mathcal{P}_2$ are equivalent. Then $(i)$ holds. For $R \in \mathbf{r}$ we certainly have $R_{+1} \leftrightarrow^*_{\mathcal{P}_1} R_{-1}$, so since $\leftrightarrow^*_{\mathcal{P}_1}$ and $\leftrightarrow^*_{\mathcal{P}_2}$ are the same congruence, $R_{+1} \leftrightarrow^*_{\mathcal{P}_2} R_{-1}$. Hence $(ii)$ holds, and the fact that $(iii)$ holds is proved similarly.

Conversely, suppose $W \leftrightarrow^*_{\mathcal{P}_1} W'$ $(W, W \in \mathbf{x}^*)$. We want to show that $W \leftrightarrow^*_{\mathcal{P}_2} W'$.
**Special case** Suppose $W'$ is obtained from $W$ by an elementary transformation in $\mathcal{P}_1$. Then $W = UR_\epsilon V$, $W' = UR_{-\epsilon}V$ for some $R : R_\epsilon = R_{-\epsilon} \in \mathbf{r}$, $U, V \in \mathbf{x}^*$. Then from $(ii)$, $[W]_{\mathcal{P}_2} = [W]_{\mathcal{P}_2}$.

**General case** Suppose we have a chain

$$W = W_0, W_1, \cdots, W_n = W',$$

where each of the $W_i$, $W_{i+1}$ $(i = 0, 1, \cdots, n-1)$ is obtained from the other by an elementary transformation in $\mathcal{P}_1$. Then by special case,

$$[W_i]_{\mathcal{P}_2} = [W_{i+1}]_{\mathcal{P}_2}.$$

Hence by transitivity,

$$[W]_{\mathcal{P}_2} = [W']_{\mathcal{P}_2}.$$

Similarly we can show (using $(iii)$) that if $W \leftrightarrow^*_{\mathcal{P}_2} W'$ then $W \leftrightarrow^*_{\mathcal{P}_1} W'$.□

**Example 1.7.1** *Let*

$$\mathcal{P}_1 = [a, b; a^3 = a^2, b^2 = a^2 b]$$

$$\mathcal{P}_2 = [a, b; a^3 = a^2, b^2 = a^3 b].$$

*Then $\mathcal{P}_1$ and $\mathcal{P}_2$ are equivalent since*

$$\underline{b^2} \to_{\mathcal{P}_2} \underline{a^3} b \to_{\mathcal{P}_2} a^2 b.$$

*Thus*

$$[b^2]_{\mathcal{P}_2} = [a^2 b]_{\mathcal{P}_2}.$$

*Also we observe that*

$$\underline{b^2} \to_{\mathcal{P}_1} \underline{a^2} b \leftarrow_{\mathcal{P}_1} a^3 b.$$

*Thus*

$$[b^2]_{\mathcal{P}_1} = [a^3b]_{\mathcal{P}_1}.$$

A monoid $M$ can have many presentations. Given a presentation

$$\mathcal{P} = [\mathbf{x}; \mathbf{r}]$$

of a monoid $M$, we consider the following *transformations* :

($T_1$) If $P, Q$ are words on $\mathbf{x}$ such that $[P]_{\mathcal{P}} = [Q]_{\mathcal{P}}$ (ie. $P \leftrightarrow^* Q$), then add $P = Q$ to the defining relations.

($T_2$) If $U$ is a word on $\mathbf{x}$, then add $y$ to the generating symbols, and add $y = U$ to the defining relations (here $y$ is a letter not in $\mathbf{x}$).

We also have the *inverse transformations* ${T_1}^{-1}$ and ${T_2}^{-1}$. The transformations $T_1, {T_1}^{-1}, T_2, {T_2}^{-1}$ are called *Tietze transformations*. Each single transformation is called an *elementary Tietze transformation.*

**Lemma 1.7.2** *If the presentation $\mathcal{P}'$ is obtained from the presentation $\mathcal{P}$ by a Tietze transformation, then $M(\mathcal{P})$* is isomorphic to $M(\mathcal{P}')$.

**Proof** Let $\mathcal{P} = [\mathbf{x}; \mathbf{r}]$. Suppose $\mathcal{P}'$ is obtained from $\mathcal{P}$ by an elementary transformation $T_1$, so

$$\mathcal{P}' = [\mathbf{x}; \mathbf{r}, P = Q].$$

Define

$$\phi : \mathbf{x} \longrightarrow M(\mathcal{P}')$$

$$x \mapsto [x]_{\mathcal{P}'} \ (x \in \mathbf{x}).$$

Then for any $R \in \mathbf{r}$

$$\phi(R_{+1}) = [R_{+1}]_{\mathcal{P}'} = [R_{-1}]_{\mathcal{P}'} = \phi(R_{-1}),$$

so by Theorem 1.6.2, there exists a homomorphism

$$\phi_{\mathcal{P}} : M(\mathcal{P}) \longrightarrow M(\mathcal{P}')$$

$$[x]_{\mathcal{P}} \mapsto [x]_{\mathcal{P}'}.$$

Similarly define

$$\psi : \mathbf{x} \longrightarrow M(\mathcal{P})$$

$$x \mapsto [x]_{\mathcal{P}}.$$

Then for each $R \in \mathbf{r}$

$$\psi(R_{+1}) = [R_{+1}]_{\mathcal{P}} = [R_{-1}]_{\mathcal{P}} = \psi(R_{-1}).$$

Also

$$\psi(P) = [P]_{\mathcal{P}} = [Q]_{\mathcal{P}} = \psi(Q),$$

so by Theorem 1.6.2 there exists a homomorphism

$$\psi_{\mathcal{P}'} : M(\mathcal{P}') \longrightarrow M(\mathcal{P})$$

$$[x]_{\mathcal{P}'} \mapsto [x]_{\mathcal{P}}.$$

We observe that for all $x \in \mathbf{x}$,

$$\psi_{\mathcal{P}'}\phi_{\mathcal{P}}([x]_{\mathcal{P}}) = \psi_{\mathcal{P}'}([x]_{\mathcal{P}'}) = [x]_{\mathcal{P}} = id_{M(\mathcal{P})}([x]_{\mathcal{P}}).$$

Thus by the Lemma 1.2.3 $\psi_{\mathcal{P}'}\phi_{\mathcal{P}} = id_{M(\mathcal{P})}$. Also

$$\phi_{\mathcal{P}}\psi_{\mathcal{P}'}([x]_{\mathcal{P}'}) = \phi_{\mathcal{P}}([x]_{\mathcal{P}}) = id_{M(\mathcal{P}')}([x]_{\mathcal{P}'}).$$

Thus by the Lemma 1.2.3 $\phi_{\mathcal{P}}\psi_{\mathcal{P}'} = id_{M(\mathcal{P}')}$. Hence $M(\mathcal{P}')$ is isomorphic to $M(\mathcal{P})$.

Suppose $\mathcal{P}'$ is obtained from $\mathcal{P}$ by elementary transformation $T_2$, so

$$\mathcal{P}' = [\mathbf{x}, y; \mathbf{r}, y = U].$$

Define

$$\phi : \mathbf{x} \longrightarrow M(\mathcal{P}')$$

$$x \mapsto [x]_{\mathcal{P}'}.$$

Then for any $R \in \mathbf{r}$

$$\phi(R_{+1}) = [R_{+1}]_{\mathcal{P}'} = [R_{-1}]_{\mathcal{P}'} = \phi(R_{-1}),$$

so by Theorem 1.6.2 there exists a homomorphism

$$\phi_{\mathcal{P}} : M(\mathcal{P}) \longrightarrow M(\mathcal{P}')$$

$$[x]_{\mathcal{P}} \mapsto [x]_{\mathcal{P}'}.$$

Similarly define

$$\psi : \{\mathbf{x}, y\} \longrightarrow M(\mathcal{P})$$

$$x \mapsto [x]_{\mathcal{P}} \ (x \in \mathbf{x})$$

$$y \mapsto [U]_{\mathcal{P}}.$$

Then for any $R \in \mathbf{r}$

$$\psi(R_{+1}) = [R_{+1}]_{\mathcal{P}} = [R_{-1}]_{\mathcal{P}} = \psi(R_{-1}).$$

Also

$$\psi(y) = [U]_{\mathcal{P}} = \psi(U).$$

Hence by Theorem 1.6.2 there exists a homomorphism

$$\psi_{\mathcal{P}'} : M(\mathcal{P}') \longrightarrow M(\mathcal{P})$$

$$[x]_{\mathcal{P}'} \mapsto [x]_{\mathcal{P}} \ (x \in \mathbf{x})$$

$$[y]_{\mathcal{P}'} \mapsto [U]_{\mathcal{P}}.$$

We observe that

$$\phi_{\mathcal{P}}\psi_{\mathcal{P}'}([x]_{\mathcal{P}'}) = \phi_{\mathcal{P}}([x]_{\mathcal{P}}) = [x]_{\mathcal{P}'} \ (x \in \mathbf{x})$$

$$\phi_{\mathcal{P}}\psi_{\mathcal{P}'}([y]_{\mathcal{P}'}) = \phi_{\mathcal{P}}([U]_{\mathcal{P}}) = [U]_{\mathcal{P}'} = [y]_{\mathcal{P}'}.$$

Hence by the Lemma 1.2.3 it implies that $\phi_{\mathcal{P}}\psi_{\mathcal{P}'} = id_{M(P')}$. Also for any $x \in \mathbf{x}$

$$\psi_{\mathcal{P}'}\phi_{\mathcal{P}}([x]_{\mathcal{P}}) = \psi_{\mathcal{P}'}([x]_{\mathcal{P}'}) = [x]_{\mathcal{P}}.$$

Hence by the Lemma 1.2.3 it implies that $\psi_{\mathcal{P}'}\phi_{\mathcal{P}} = id_{M(P)}$. Thus $M(P)$ is isomorphic to $M(P')$.□

**Remark** *The isomorphism $\phi_{\mathcal{P}}$ is called a standard isomorphism.*

**Theorem 1.7.3** (*Tietze theorem*) *Let $\mathcal{P}, \mathcal{P}'$ be two finite monoid presentations such that $\eta : M(\mathcal{P}) \longrightarrow M(\mathcal{P}')$ is an isomorphism. Then there is a finite monoid presentation $\mathcal{R}$ and two sequences of finite monoid presentations*

$$\mathcal{P}_0 = \mathcal{P} \longrightarrow \mathcal{P}_1 \longrightarrow \mathcal{P}_2 \longrightarrow \cdots \longrightarrow \mathcal{P}_u = \mathcal{R}$$

$$\mathcal{P}'_0 = \mathcal{P}' \longrightarrow \mathcal{P}'_1 \longrightarrow \mathcal{P}'_2 \longrightarrow \cdots \longrightarrow \mathcal{P}'_v = \mathcal{R},$$

*where each step* $\mathcal{P}_i \longrightarrow \mathcal{P}_{i+1}$, $\mathcal{P}'_j \longrightarrow \mathcal{P}'_{j+1}$ $(0 \le i \le u-1,\ 0 \le j \le v-1)$, *is an elementary Tietze transformation* $T_1$ or $T_2$, *such that*

$$\eta = (\eta'_{v-1} \cdots \eta'_1 \eta'_0)^{-1} (\eta_{u-1} \cdots \eta_1 \eta_0),$$

*where* $\eta_i$ *and* $\eta'_j$ *are the standard isomorhisms*

$$\eta_i : M(\mathcal{P}_i) \longrightarrow M(\mathcal{P}_{i+1})$$

*and*

$$\eta'_j : M(\mathcal{P}_j) \longrightarrow M(\mathcal{P}'_{j+1})$$

*respectively.*

**Proof** Let

$$\mathcal{P} = [\mathbf{x}; \mathbf{r}]$$

$$\mathcal{P}' = [\mathbf{y}; \mathbf{s}].$$

If $\eta : M(\mathcal{P}) \longrightarrow M(\mathcal{P}')$ is an isomorphism, then there exists

$$\eta^{-1} = \gamma : M(\mathcal{P}') \longrightarrow M(\mathcal{P})$$

such that

$$\gamma\eta = id_{M(\mathcal{P})},$$

$$\eta\gamma = id_{M(\mathcal{P}')}.$$

Suppose

$$\eta([x]_{\mathcal{P}}) = [U_x]_{\mathcal{P}'} \ (x \in \mathbf{x}),$$

$$\gamma([y]_{\mathcal{P}'}) = [V_y]_{\mathcal{P}} \ (y \in \mathbf{y})$$

($U_x$ is a word on $\mathbf{y}$, $V_y$ is a word on $\mathbf{x}$).

We can successively add each letter $y \in \mathbf{y}$ to the generators and the corresponding relation $y = V_y$ to the defining relations, and obtain

$$\mathcal{Q}_1 = [\mathbf{x}, \mathbf{y}; \mathbf{r}, y = V_y(y \in \mathbf{y})].$$

Thus $\mathcal{Q}_1$ is obtained from $\mathcal{P}$ by $|\mathbf{y}|$ elementary Tietze transformations $T_2$. We let

$$\eta_0 : M(\mathcal{P}) = M(\mathcal{P}_0) \longrightarrow M(\mathcal{Q}_1)$$

$$[W]_{\mathcal{P}} \mapsto [W]_{\mathcal{Q}_1}$$

be the composition of the corresponding standard isomorphisms.

For any $S \in \mathbf{s}$

$$\gamma([S_{+1}]_{\mathcal{P}'}) = \gamma([S_{-1}]_{\mathcal{P}'}).$$

Since $\eta_0$ is an isomorphism then

$$\eta_0\gamma([S_{+1}]_{\mathcal{P}'}) = \eta_0\gamma([S_{-1}]_{\mathcal{P}'}).$$

Thus we obtain

$$[S_{+1}]_{\mathcal{Q}_1} = [S_{-1}]_{\mathcal{Q}_1}.$$

Hence for any $S \in \mathbf{s}$ then $S_{+1} \leftrightarrow^*_{\mathcal{Q}_1} S_{-1}$. Thus for each $S \in \mathbf{s}$ we can add $S_{+1} = S_{-1}$ to the defining relations, and obtain

$$\mathcal{Q}_2 = [\mathbf{x}, \mathbf{y}; \mathbf{r}, \mathbf{s}, y = V_y (y \in \mathbf{y})].$$

Thus $\mathcal{Q}_2$ is obtained from $\mathcal{Q}_1$ by $|\mathbf{s}|$ elementary Tietze transformations $T_1$. We let

$$\eta_1 : M(\mathcal{Q}_1) \longrightarrow M(\mathcal{Q}_2)$$

$$[W]_{\mathcal{Q}_1} \mapsto [W]_{\mathcal{Q}_2}$$

be the composition of the corresponding standard isomorphisms.

Then

$$\gamma\eta([x]_{\mathcal{P}}) = \gamma([U_x]_{\mathcal{P}'}) = [x]_{\mathcal{P}} \ (x \in \mathbf{x}).$$

We observe that

$$[x]_{\mathcal{P}} = [V_{U_x}]_{\mathcal{P}} = [V_{y_1}]_{\mathcal{P}}[V_{y_2}]_{\mathcal{P}} \cdots [V_{y_n}]_{\mathcal{P}} \ (y_1 ... y_n = U_x, \ y_1, y_2, \cdots y_n \in \mathbf{y}, x \in \mathbf{x})$$

Thus

$$\eta_1\eta_0\eta([x]_{\mathcal{P}}) = [x]_{\mathcal{Q}_2} = \eta_1\eta_0\eta([V_{U_x}]_{\mathcal{P}}) = [V_{U_x}]_{\mathcal{Q}_2} = [V_{y_1}]_{\mathcal{Q}_2}[V_{y_2}]_{\mathcal{Q}_2} \cdots [V_{y_n}]_{\mathcal{Q}_2}.$$

But in $M[\mathcal{Q}_2]$

$$[V_{y_1}]_{\mathcal{Q}_2}[V_{y_2}]_{\mathcal{Q}_2} \cdots [V_{y_n}]_{\mathcal{Q}_2} = [y_1]_{\mathcal{Q}_2}[y_2]_{\mathcal{Q}_2} \cdots [y_n]_{\mathcal{Q}_2}.$$

This implies that

$$[x]_{\mathcal{Q}_2} = [y_1]_{\mathcal{Q}_2}[y_2]_{\mathcal{Q}_2} \cdots [y_n]_{\mathcal{Q}_2} = [U_x]_{\mathcal{Q}_2}.$$

Hence $x \leftrightarrow^*_{\mathcal{Q}_2} U_x$ $(x \in \mathbf{x})$. Thus we can successively add the relations $x = U_x$ $(x \in \mathbf{x})$ to $\mathcal{Q}_2$, and obtain

$$\mathcal{R} = \mathcal{Q}_3 = [\mathbf{x}, \mathbf{y}; \mathbf{r}, \mathbf{s}, y = V_y (y \in \mathbf{y}), x = U_x (x \in \mathbf{x})].$$

Thus $\mathcal{R} = \mathcal{Q}_3$ is obtained from $\mathcal{Q}_2$ by $|\mathbf{x}|$ elementary Tietze transformations $T_1$. We let

$$\eta_2 : M(\mathcal{Q}_2) \longrightarrow M(\mathcal{Q}_3)$$

$$[W]_{\mathcal{Q}_2} \mapsto [W]_{\mathcal{Q}_3}$$

be the composition of the corresponding standard isomorphisms.

By symmetry we can also obtain a sequence

$$\mathcal{P}', \mathcal{Q}_1', \mathcal{Q}_2', \mathcal{Q}_3' = \mathcal{R}$$

and the compositions of the corresponding standard isomorphisms

$$\eta_0', \eta_1', \eta_2'.$$

$$\mathcal{P} \xrightarrow[|\mathbf{y}| - times]{T_2} \mathcal{Q}_1 \xrightarrow[|\mathbf{s}| - times]{T_1} \mathcal{Q}_2 \xrightarrow[|\mathbf{x}| - times]{T_1} \mathcal{R}$$

$$\mathcal{P}' \xrightarrow[|\mathbf{x}| - times]{T_2} \mathcal{Q}_1' \xrightarrow[|\mathbf{r}| - times]{T_1} \mathcal{Q}_2' \xrightarrow[|\mathbf{y}| - times]{T_1} \mathcal{R}$$

Indeed

$$\eta_2\eta_1\eta_0([x]_{\mathcal{P}}) = [x]_{\mathcal{R}} = [U_x]_{\mathcal{R}} \ (x \in \mathbf{x}),$$

and

$$\eta_2'\eta_1'\eta_0'\eta([x]_P) = [U_x]_{\mathcal{R}} \ (x \in \mathbf{x}).$$

Hence by Lemma 1.2.3, $\eta_2'\eta_1'\eta_0'\eta = \eta_2\eta_1\eta_0$. Thus $(\eta_2'\eta_1'\eta_0')^{-1}\eta_2\eta_1\eta_0 = \eta$.□

**Corollary 1.7.4** *Two finite presentation define isomorphic monoids if and only if one can be obtained from the other by a finite sequence of elementary Tietze transformations.*

**Proof** This is a consequence of Lemma 1.7.2 and Theorem 1.7.3.□

## 1.8 Noetherian induction

A relation $>$ on a set $A$ is an *ordering* if it is both irreflexive and transitive. An ordering is *noetherian* if for any $a \in A$ there is no infinite chain

$$a = a_0 > a_1 > a_2 > a_3 \cdots .$$

Let $A$ be a set and $>$ be a noetherian ordering. For each $a \in A$ assume we have a proposition $P(a)$.

**Theorem 1.7.1** (*Principal of noetherian induction*) *Suppose we can show that the following holds :*

(+) *If $a \in A$ and $P(b)$ is true for all $a > b$ then $P(a)$ is true.*

*Then we deduce that $P(a)$ is true for all $a \in A$.*

**Proof** Suppose $P(a)$ is not true for all $a \in A$. Choose $a_1$ such that $P(a_1)$ is false. From (+) it cannot be the case that $P(b)$ is true for all $a_1 > b$. So choose $a_1 > a_2$, such that $P(a_2)$ is false. So by (+) it cannot be the case that $P(b)$ is true for all $a_2 > b$. Choose $a_2 > a_3$ such that $P(a_3)$ is false. We continue, contradicting the fact that $>$ is noetherian. Hence $P(a)$ must be true for all $a \in A$.$\square$

# Chapter 2

# Complete rewriting systems

## 2.1 Definitions

Let

$$\mathcal{P} = [\mathbf{x};\mathbf{r}]$$

be a rewriting system on $\mathbf{x}$. Then

$(i)$ $\mathcal{P}$ is said to be *noetherian* if there exists no infinite sequence

$$W_0 \longrightarrow W_1 \longrightarrow W_2 \longrightarrow W_3 \longrightarrow \cdots \ (W_i \in \mathbf{x}^*, i = 0, 1, 2, \cdots).$$

$(ii)$ $\mathcal{P}$ is *confluent* if whenever we have

$$W \longrightarrow^* Y \text{ and } W \longrightarrow^* Z \ (W, Y, Z \in \mathbf{x}^*),$$

there exists a word $W'$ on $\mathbf{x}$, such that

$$Y \longrightarrow^* W' \text{ and } Z \longrightarrow^* W'.$$

$(iii)$ $\mathcal{P}$ is *locally confluent* if whenever we have

$$W \longrightarrow Y \text{ and } W \longrightarrow Z \ (W, Y, Z \in \mathbf{x}^*),$$

then there exists a word $W'$ on $\mathbf{x}$, such that

$$Y \longrightarrow^* W' \text{ and } Z \longrightarrow^* W'.$$

*(iv)* $\mathcal{P}$ is a *complete* rewriting system if $\mathcal{P}$ is both noetherian and confluent.

A word $W$ on $\mathbf{x}$ is said to be *irreducible* if no positive transformations can be applied to it.

**Example 2.1.1** *Let*

$$\mathcal{P} = [a, b; a^2ba = \epsilon, a^2b = ba].$$

*Then the word bab is irreducible, whereas the word* $ba^2ba$ *is not irreducible, since we can replace* $a^2b$ *by ba.*

**Lemma 2.1.1** *If* $\mathcal{P}$ *is noetherian then each equivalence class contains an irreducible.*

**Proof** Let $W$ be a word. If $W$ is irreducible then there is nothing to prove. Otherwise we apply an elementary positive transformation to $W$ to obtain a word $W_1$

$$W \to W_1.$$

If $W_1$ is irreducible then $W_1$ is an irreducible of the equivalence class $[W]$. Otherwise we apply an elementary positive transformation to $W_1$ to obtain a word $W_2$

$$W \to W_1 \to W_2.$$

If $W_2$ is irreducible then $W_2$ is an irreducible of the equivalence class $[W]$. Otherwise we apply an elementary positive transformation to $W_2$ to obtain a word $W_3$. We continue with this process. Since $\mathcal{P}$ is noetherian, we must eventually reach an irreducible word $W_n$

$$W \to W_1 \to W_2 \cdots W_n.$$

Hence $W_n$ is an irreducible of the equivalence class $[W]$.□

Let $>$ be an ordering on $\mathbf{x}^*$. Then the ordering is said to be:

$(i)$ *monotonic*, if whenever we have words $U, V, W, W'$ on $\mathbf{x}$ such that $W > W'$, then $UWV > UW'V$;

$(ii)$ *well-founded*, if there exists no infinite sequence such that

$$W_0 > W_1 > W_2 > W_3 > \cdots (W_i \in \mathbf{x}^*, i = 0, 1, 2, \cdots);$$

$(iii)$ *reduction*, if it is both monotonic and well-founded ;

$(iv)$ *compatible* with $\mathbf{r}$ if $R_+ > R_-$ for each defining relator.

$(v)$ *total* if whenever we have two words $W, W'$ on $\mathbf{x}$ exactly one of $W > W'$, $W' > W$, $W = W'$ hold.

$(vi)$ *partial* if there exist words $W, W'$ that can not be compared.

We give some well-known examples of reduction orderings:

$(a)$ *Length-reducing ordering* $(LO)$ : For any two words $W, W'$, then $W > W$ if and only if $L(W) > L(W')$.

(b) *Weight-reducing ordering* $(WO)$ : Let $\psi : \mathbf{x} \longrightarrow \mathbb{Z}^+$, such that $\psi(x) > 0$ for all $x \in \mathbf{x}$. By Theorem 1.4.1, $\psi$ can be extended to a unique homomorphism, $\mathbf{x}^* \longrightarrow \mathbb{Z}^+$ which by abuse of notation we also denote by $\psi$. For any word $W, W'$ then $W > W'$ if and only if $\psi(W) > \psi(W')$.

**Remark** : note that $LO$ is a special case of $WO$ when all letters have weight one.

(c) *Weight-plus-lexicographic ordering from the left* $(WLO - L)$ : For any word $W, W'$ then $W > W'$ if and only if either $\psi(W) > \psi(W')$ or $\psi(W) = \psi(W')$ and $W >_{Lex-L} W'$, where $>_{Lex-L}$ is the lexicographic ordering from the left on $\mathbf{x}^*$ induced by a well-founded total ordering on $\mathbf{x}$, called a *precedence* on $\mathbf{x}$.

Suppose $\mathbf{x} = \mathbf{y} \cup \mathbf{z}$, where $\mathbf{y}$, $\mathbf{z}$ are disjoint sets. Suppose we have precedences $\rhd_{\mathbf{y}}$, $\rhd_{\mathbf{z}}$ on $\mathbf{y}$, $\mathbf{z}$ respectively. Then we define a precedence on $\mathbf{x}$ by

$$x_1 \rhd x_2 \text{ if and only if}$$

$$\begin{array}{ll} \textit{either} & x_1, x_2 \in \mathbf{y} \text{ and } x_1 \rhd_{\mathbf{y}} x_2; \\ \textit{or} & x_1, x_2 \in \mathbf{z} \text{ and } x_1 \rhd_{\mathbf{z}} x_2; \\ \textit{or} & x_1 \in \mathbf{y}, x_2 \in \mathbf{z}. \end{array}$$

We say $\mathbf{y}$ has precedence over $\mathbf{z}$ and denote it by $\mathbf{y} \rhd \mathbf{z}$.

**Theorem 2.1.2** *A rewriting system*

$$\mathcal{P} = [\mathbf{x};\mathbf{r}]$$

*on* $\mathbf{x}$ *is noetherian if there exists a reduction ordering on* $\mathbf{x}^*$, *which is compatible with* $\mathbf{r}$.

**Proof** First we would show that for any words $W, W'$ on $\mathbf{x}$ if $W \longrightarrow W'$, then $W > W'$. But if $W \longrightarrow W'$ holds, it implies that we can have $W = UR_{+1}V$ and $W' = UR_{-1}V$, for some defining relator $R : R_{+1} = R_{-1}$. Then since $>$ is compatible with $\mathbf{r}$, $R_{+1} > R_{-1}$ holds. And since $>$ is a reduction ordering, then $>$ is monotonic. Thus $UR_{+1}V > UR_{-1}V$. Hence $W > W'$, as required.

Now suppose $\mathcal{P}$ is not noetherian. Thus there exists at least one word $W$ on $\mathbf{x}$ such that we have an infinite chain of positive transformations

$$W \longrightarrow W_1 \longrightarrow W_2 \longrightarrow W_3 \cdots.$$

By the above

$$W > W_1 > W_2 > W_3 > \cdots,$$

thus contradicting the assumption that $>$ is well-founded. Thus we conclude that $\mathcal{P}$ is noetherian.□

The converse of this theorm is also true (see D.S. Lankford [33] for more details).

**Example 2.1.2** *The rewriting system* $\mathcal{P}$ *as in Example* 2.1.1 *is noetherian, since LO is compatible with* $\mathbf{r}$.

Suppose there are distinct relators $R, S$ such that

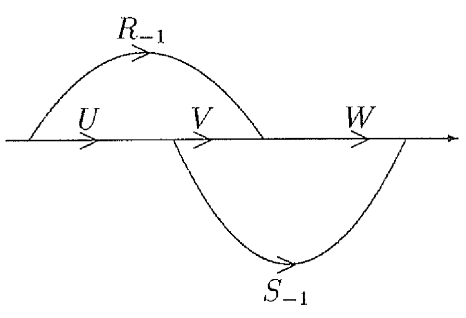
$$R_{+1} = UV,\ S_{+1} = VW$$

where $V$ is non-empty. Then the word $UVW$ is called an *overlap ambiguity* of $\mathcal{P}$ .

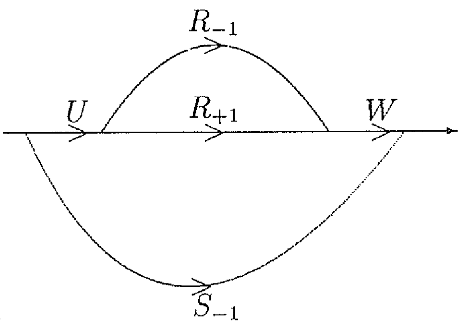
If

$$R_{+1} = V,\ S_{+1} = UVW\ (V \text{ non-empty})$$

then $UVW$ is called an *inclusion ambiguity*. The pair of words $(R_{-1}W, US_{-1})$ or $(UR_{-1}W, S_{-1})$, respectively, is called a *critical pair* corresponding to the ambiguity.




*Overlap ambiguity*




*Inclusion ambiguity*

A critical pair $(P, Q)$ is said to be *resolved* if there is a word $Z$ on $\mathbf{x}$ such that $P \longrightarrow^* Z$ and $Q \longrightarrow^* Z$, *unresolved* otherwise.

**Example 2.1.3** *Let* $\mathcal{P} = [a, b, c, d, e, f, g; ab^2ef = ca, efg^2c = d^3]$. *The overlap ambiguity is* $ab^2efg^2c$ *and the corresponding critical pair is* $(cag^2c, ab^2d^3)$.

**Example 2.1.4** *Let* $\mathcal{P}' = [a, b, c, d, e, f, g; ag = c^3b, b^2dagce = fg^2]$. *The inclusion ambiguity is* $b^2dagce$ *and the corresponding critical pair is* $(b^2dagce, b^2dc^3bce)$.

## 2.2 Fundamental theorem on rewriting systems

The following basic result is due to M. H. A. Newman [48].

**Theorem 2.2.1** *Let*

$$\mathcal{P} = [\mathrm{x};\mathrm{r}]$$

*be a noetherian rewriting system. Then the following conditions are equivalent* :

$(i)$ $\mathcal{P}$ *is locally confluent;*

$(ii)$ $\mathcal{P}$ *is confluent;*

$(iii)$ *If* $(P, Q)$ *is a critical pair and*

$$P \longrightarrow^* V, Q \longrightarrow^* U,$$

*where* $U$ and $V$ *are irreducibles* then $U = V$;

$(iv)$ *All critical pairs of* $\mathbf{r}$ *are resolvable.*

**Proof** $(i) \Rightarrow (ii)$. For $W \in \mathbf{x}^*$, let $P(W)$ be the following statement.

$P(W)$ : If whenever $W$ is such that

$$W \to^* Y \text{ and } W \to^* Z$$

then there exist a word $S \in \mathbf{x}^*$ such that

$$Y \to^* S \text{ and } Z \to^* S.$$

We show that if $\mathcal{P}$ is locally confluent then $P(W)$ holds for all $W$. We will show it by noetherian induction. Let $<$ be a relation defined on $\mathbf{x}^*$ by:

$U < V$ if $U$ is obtained from $V$ by at least one positive transformation ($U, V \in \mathbf{x}^*$). Clearly the defined relation is irreflexive for if we had a chain

$$U = U_0 \longrightarrow U_1 \longrightarrow U_2 \longrightarrow \cdots \longrightarrow U_n = U$$

with $n > 0$, then we can repeat this chain arbitrarily often

$$U = U_0 \longrightarrow U_1 \longrightarrow \cdots \longrightarrow U_n = U \to U_0 \longrightarrow U_1 \longrightarrow \cdots \longrightarrow U_n = U \to U_1 \cdots,$$

thus contradicting the fact that $\mathcal{P}$ is noetherian. Again $<$ is transitive since if we have chains

$$W = W_0 \longrightarrow W_1 \longrightarrow W_2 \longrightarrow \cdots \longrightarrow W_m = V$$

$$V = V_0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow \cdots \longrightarrow V_n = U$$

with $m, n > 0$ then we have the chain

$$W = W_0 \longrightarrow W_1 \longrightarrow \cdots \longrightarrow W_m = V = V_0 \longrightarrow V_1 \longrightarrow \cdots \longrightarrow V_n = U,$$

so $W < U$. The relation is noetherian, since $\mathcal{P}$ is noetherian.

Suppose

$$W \to^* Y \text{ and } W \to^* Z$$

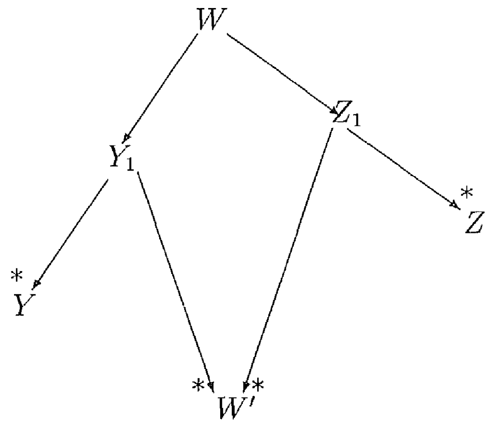
We show that there exists $S \in \mathbf{x}^*$, such that $Y \rightarrow^* S$ and $Z \rightarrow^* S$.

**Case 1:** If $W = Y$ then we let $S = Z$. Hence $P(W)$ is satisfied. Similarly if $W = Z$ then we let $S = Y$. Thus in both cases $P(W)$ is satisfied.

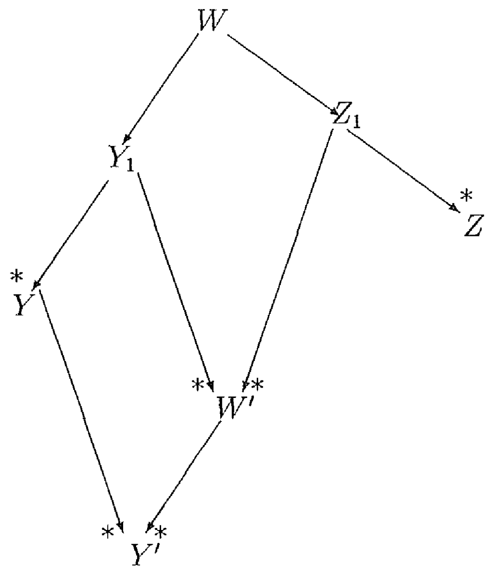
**Case 2:** Suppose $W \neq Y$, $W \neq Z$. Thus there exist words $Y_1, Z_1$ such that

$$Y \;{}^*\!\!\leftarrow Y_1 \leftarrow W \rightarrow Z_1 \rightarrow^* Z.$$

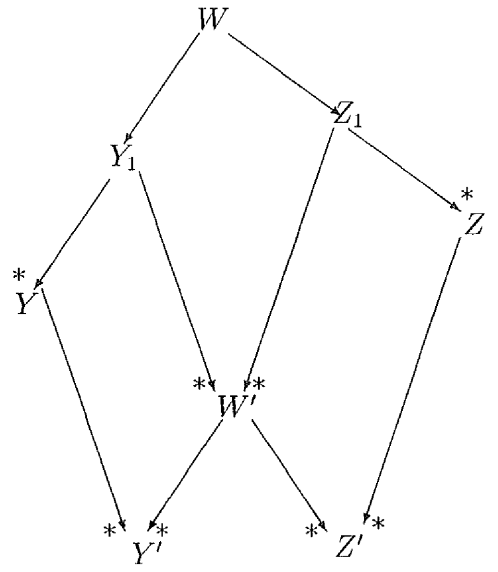
Since $\mathcal{P}$ is locally confluent then there exists a word $W'$ such that



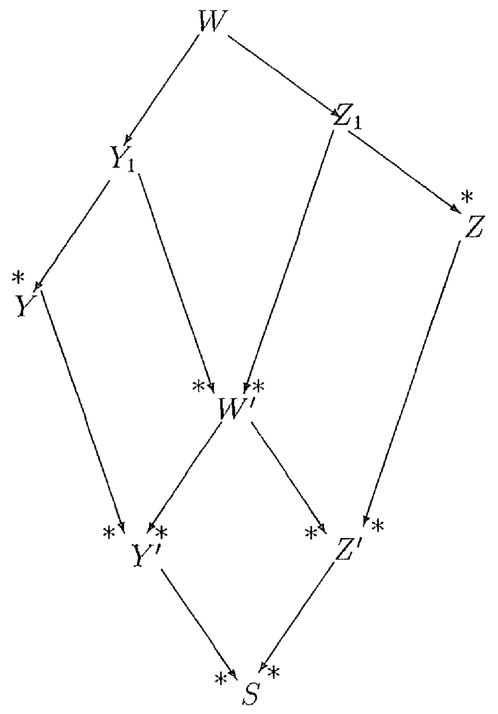

Since $Y_1 < W$, $P(Y_1)$ holds by the induction assumption. Thus there exists a word $Y'$ such that




Similarly, since $Z_1 < W$, $P(Z_1)$ holds by induction assumption, so there exists a word $Z'$ such that




By the same argument since $W' < W$, $P(W')$ is satisfied, so there exists a word $S \in X^*$, such that




Thus we have shown that if

$$W \to^* Y \text{ and } W \to^* Z,$$

then there exists a word $S \in X^*$, such that

$$Y \to^* S \text{ and } Z \to^* S.$$

Hence $P(W)$ is satisfied.

Thus by the principle of Noetherian induction $P(W)$ holds, for any word $W$ on $\mathbf{x}$. Hence $\mathcal{P}$ is confluent.

$(ii) \Rightarrow (iii)$. Suppose $(P, Q)$ is a critical pair. But $(P, Q)$ being a critical pair implies that there exists a word $W \in \mathbf{x}^*$, such that

$$W \to P \text{ and } W \to Q.$$

Suppose

$$P \to^* V \text{ and } Q \to^* U, \text{ where } U, V \text{ are irreducibles.}$$

Then we have

$$W \to P \to^* V \text{ and } W \to Q \to^* U.$$

Thus we have

$$W \to^* V \text{ and } W \to^* U.$$

Now since $\mathcal{P}$ is confluent, then there exists a word $S \in \mathbf{x}^*$, such that

$$V \to^* S \text{ and } U \to^* S.$$

But $U$ and $V$ are irreducibles. Thus $S = U = V$. Hence $V = U$ as required.

$(iii) \Rightarrow (iv)$. Suppose $(P, Q)$ is a critical pair. We show that there exists a word $W'$, such that

$$P \to^* W' \text{ and } Q \to^* W'.$$

But since $\mathcal{P}$ is noetherian, by Lemma 2.1.1, there exist irreducibles $Z$ and $Z'$, such that

$$P \to^* Z \text{ and } Q \to^* Z'.$$

Hence by $(iii)$, $Z = Z'$, so we can take $W'$ to be $Z$. Thus the critical pair is resolved.

$(iv) \Rightarrow (i)$. Let

$$W \to Y \text{ and } W \to Z \ (W, Y, Z \in \mathbf{x}^*).$$

We must prove that there exists $V \in \mathbf{x}^*$ such that

$$Y \to^* V \text{ and } Z \to^* V.$$

There are relators $R, S$ and words $Y_1, Y_3, Z_1, Z_3$ such that

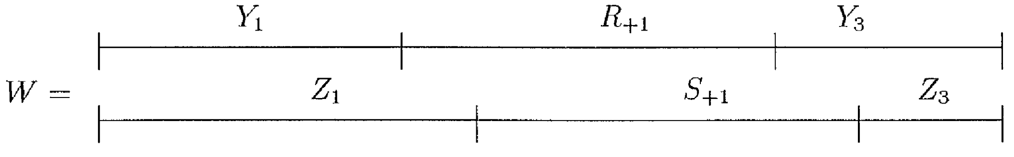
$$W = Y_1 R_{+1} Y_3, \ Y = Y_1 R_{-1} Y_3$$

$$W = Z_1 S_{+1} Z_3, \ Z = Z_1 S_{-1} Z_3.$$

There are two situations: the occurrence $R_{+1}, S_{+1}$ are disjoint or they are not.

We treat first the situation where they are not disjoint.

**Case (i):** Suppose there exist an overlap ambiguity between the occurrence of $R_{+1}$ and $S_{+1}$.




Then

$$R_{+1} = UV \text{ and } S_{+1} = VT$$

with $V$ non-empty. We then have $Z_1 = Y_1 U$, $Y_3 = T Z_3$ such that we have the overlap ambiguity $UVT$, and the critical pair $(R_{-1}T, US_{-1})$. So we have

$$W = Y_1 R_{+1} T Z_3 \to Y_1 R_{-1} T Z_3 = Y \text{ and } W = Y_1 U S_{+1} Z_3 \to Y_1 U S_{-1} Z_3 = Z.$$

But by $(iv)$ we know there exists a word $V \in \mathbf{x}^*$, such that

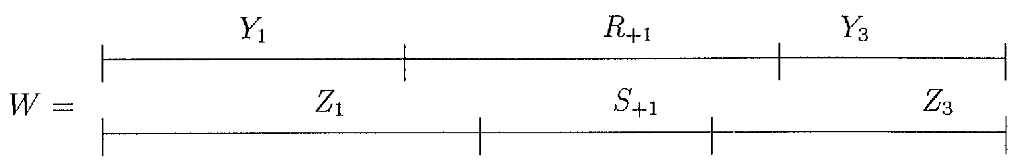
$$R_{-1}T \to^* V \text{ and } US_{-1} \to^* V.$$

Hence there exists a word $Y_2VZ_4 \in \mathbf{x}^*$, such that

$$Y \to^* Y_2VZ_4 \text{ and } Z \to^* Y_2VZ_4.$$

Thus local confluence is satisfied.

**Case (ii):** Suppose there exists an inclusion ambiguity.




Then

$$R_{+1} = UVT \text{ and } S_{+1} = V$$

with $V$ non-empty. We then have $Z_1 = Y_1U$, $Z_3 = TY_3$ such that we have the inclusion ambiguity $UVT$, and the critical pair $(R_{-1}, US_{-1}T)$. So we have

$$W = Y_1US_{+1}TY_3 \to Y_1US_{-1}TY_3 = Z \text{ and } W = Y_1US_{+1}TY_3 \to Y_1R_{-1}Y_3 = Z.$$

But by $(iv)$ we know there exists a word $V \in \mathbf{x}^*$, such that

$$R_{-1} \to^* V \text{ and } US_{-1}T \to^* V.$$

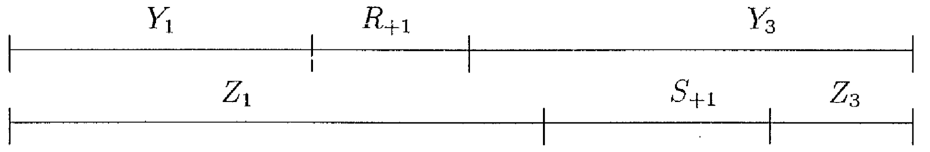
Hence there exists a word $Y_1VY_3 \in \mathbf{x}^*$, such that

$$Y \to^* Y_1VY_3 \text{ and } Z \to^* Y_1VY_3.$$

Thus local confluece is satisfied.

Now suppose that the occurrences of $R_{+1}$, $S_{+1}$ are disjoint.

$W =$




Then

$$Z_1 = Y_1R_{+1}K \text{ and } Y_3 = KS_{+1}Z_3 \text{ ($K$ is the partition between $Y_3$ and $Z_3$).}$$

So

$$W = Y_1R_{+1}KS_{+1}Z_3 \to Y_1R_{-1}KS_{+1}Z_3 = Y \to Y_1R_{-1}KS_{-1}Z_3$$

$$W = Y_1R_{+1}KS_{+1}Z_3 \to Y_1R_{+1}KS_{-1}Z_3 = Z \to Y_1R_{-1}KS_{-1}Z_3.$$

Hence local confluence is satisfied.□

**Example 2.2.1** *The rewriting system* $\mathcal{P} = [x, \theta; x\theta = \theta, \theta^2 = \theta]$ *it is noetherian, since is length-reducing. The critical pairs are* $(\theta^2, x\theta)$ $(\theta^2, \theta^2)$*. But* $\theta^2 \to \theta$ *and* $x\theta \to \theta$*. Thus the critical pairs are resolved, so by Theorem* 2.2.1 (*iv*), $\mathcal{P}$ *is* *confluent.*

**Example 2.2.2** *The rewriting system* $\mathcal{P}' = [x, \theta; x\theta = \theta, \theta^2 = x]$ *is noetherian, since it is length-reducing. We have the critical pair* $(\theta^2, x^2)$, *and* $\theta^2 \to^* x$. *Since* $x^2$, $x$ *are distinct irreducibles, by Theorem* 2.2.1 *(iii),* $\mathcal{P}'$ *is not confluent.*

## 2.3 A further characterization of complete rewriting system

**Theorem 2.3.1** *Suppose* $\mathcal{P}$ *is noetherian. Then the following are equivalent :*

*(i)* $\mathcal{P}$ *is complete;*

*(ii) each equivalence class contains a unique irreducible.*

We refer the reader to M. H. A. Newman [48], who originally proved the theorem.

**Proof** We first note that by Lemma 2.1.1 each equivalence class contains at least one irreducible.

$(i) \Rightarrow (ii)$. Suppose $W, W'$ are irreducibles belonging to $[W]$. We will show that $W$ and $W'$ are the same. Since $W \leftrightarrow^* W'$ there exists a sequence

$$W = W_0, W_1, W_2 \cdots W_n = W'$$

such that $W_{i+1}$ comes from $W_k$ $(i = 0, 1, 2, \cdots, n-1)$ by an elementary transformation. If $n = 0$ there is nothing to prove. Otherwise, since $W$ and $W'$ are irreducibles, then our sequence must be of the form

$$W \longleftarrow W_1 \leftrightarrow^* W_{n-1} \longrightarrow W'.$$

Thus there must exist at least one $k$ such that $W_{k-1}$ comes from $W_k$ by a single positive transformation and $W_{k+1}$ comes from $W_k$ $(k = 1, 2, \cdots, n-1)$ by a single positive transformation.

Hence there exist

$$0 < k_1 < k_2 < k_3 < k_4 < \cdots < k_m < n$$

such that

$$W \; {}^*\!\!\leftarrow W_{k_1} \rightarrow^* W_{k_2} \; {}^*\!\!\leftarrow W_{k_3} \rightarrow^* W_{k_4} \; {}^*\!\!\leftarrow \cdots {}^*\!\!\leftarrow W_{k_m} \rightarrow^* W'.$$

Since we have the subsequence

$$W \; {}^*\!\!\leftarrow W_{k_1} \rightarrow^* W_{k_2}$$

and $\mathcal{P}$ is confluent, there must exists a word $Z$ such that

$$W \rightarrow^* Z \text{ and } W_{k_2} \rightarrow^* Z.$$

But $W$ is irreducible, thus $W = Z$. Hence

$$W \; {}^*\!\!\leftarrow W_{k_2} \; {}^*\!\!\leftarrow W_{k_3} \rightarrow^* W_{k_4} \; {}^*\!\!\leftarrow \cdots {}^*\!\!\leftarrow W_{k_m} \rightarrow^* W'$$

holds. By the same argument we can find a word $Z'$ such that

$$W \rightarrow^* Z' \text{ and } W_{k_4} \rightarrow^* Z'.$$

Since $W$ is irreducible, then $W = Z'$. We continue eliminating the $k_i' s$ until we are left with

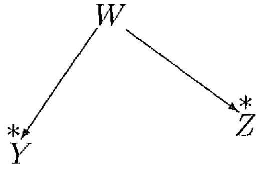
$$W \; {}^*\!\!\leftarrow W_{k_m} \rightarrow^* W'.$$

Since $\mathcal{P}$ is confluent there exists a word $Z''$ such that

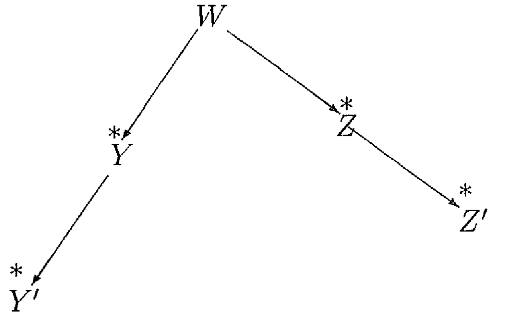
$$W \to^* Z'' \text{ and } W' \to^* Z''.$$

But $W, W'$ were chosen to be irreducibles, thus $W = Z'' = W'$.

$(ii) \Rightarrow (i)$. Let $W$ be a word such that




Since $\mathcal{P}$ is noetherian, by Lemma 2.1.1, there exist irreducibles $Y'$ and $Z'$, such that $Y \to^* Y'$ and $Z \to^* Z'$. Hence we have




But $Y'$ and $Z'$ are equivalent, and they are irreducibles in $\mathcal{P}$. Hence by $(ii)$, $Y' = Z'$. Thus $\mathcal{P}$ is confluent.□

## 2.4 Resolutions

Let $M$ be a monoid. Let $\mathbb{Z}$ denote the ring of (ordinary) integers and let $\mathbb{Z}M$ denote the monoid ring of $M$ with coefficients in $\mathbb{Z}$. We view $\mathbb{Z}$ as a left $\mathbb{Z}M$-module on which each element of $M$ acts as the identity: if $\lambda \in \mathbb{Z}$ and $m \in M$, then $m\lambda = \lambda$. Similarly we can view $\mathbb{Z}$ as a right $\mathbb{Z}M$-module on which each element of $M$ acts as the identity.

A *(right) left resolution* of $\mathbb{Z}$ is a sequence

$$\cdots \longrightarrow B_i \xrightarrow{\partial_i} B_{i-1} \longrightarrow \cdots \longrightarrow B_2 \xrightarrow{\partial_2} B_1 \xrightarrow{\partial_1} B_0 \xrightarrow{\partial_0} \mathbb{Z} \to 0$$

of (right) left $\mathbb{Z}M$-modules $B_i$ and (right) left $\mathbb{Z}M$-module homomorphisms $\partial_i$ (as indicated) such that $im\partial_{i+1} = ker\partial_i$ $(i = 0, 1, 2, \cdots)$, and we say the sequence is *exact*. The resolution is said to be of *finite length* if there exists $k$ such that $B_i = 0$ for all $i > k$. The resolution is called a *free resolution* if all the $B_i$ are free modules. Such a free resolution always exists.

The monoid $M$ is said to have the *(right) left $FP_n$ property* $(n \leq \infty)$ if there is a free resolution as above with $B_i$ finitely generated for $i \leq n$.

D. Cohen in [15] has shown that the properties of left $FP_\infty$ and right $FP_\infty$ are not related, by exhibiting a monoid $M$ with presentation

$$\mathcal{P} = [x_i(i \in \mathbb{N}); x_i x_j = x_i x_{j+1}(i, j \in \mathbb{N}, i < j)]$$

which is right $FP_\infty$ but not left $FP_1$. There will then also be a monoid which is left $FP_\infty$ but not right $FP_1$, namely the *opposite monoid* of $M$, which has the same underlying set as $M$ but with the multiplication $*$ defined by $u * v = vu$ $(u, v \in M)$.

**Theorem 2.4.1** *If a monoid $M$ has a finite complete rewriting system, then $M$ is both left and right $FP_\infty$.*

C.C Squier [61] has shown that if a monoid $M$ has a finite complete rewriting system, then $M$ is $FP_3$. Later it was shown by Kenneth S. Brown [13], Y.

Kobayashi [30] that if $M$ has a finite complete rewriting system then $M$ is both left and right $FP_\infty$. Then it was realised that in fact D.J Anick [4] had shown it earlier.

# Chapter 3

# Monoid and group constructions viewed as rewriting systems

## 3.1 Introduction

Free groups, free products of groups, free products of groups with amalgamated subgroups and $HNN$-extensions of groups are basic construction in combinatorial group theory and have been studied extensively. See the standard text books D. Cohen [14], A.G. Kurosh [32], Lyndon and Schupp [35], W. Magnus, A Karrass, and D. Solitar [44], J.J. Rotman [59]. For each of these construction there is a normal form for every element of the group. A lesser known construction is the free product with commutative subgroups (see [27], [28], [44]). In this chapter, we will study these costructions using monoids, and obtain the normal forms for each construction by viewing the construction as a rewriting system. D. Cohen [14], has shown that normal forms of free groups are unique using similar concept as the one from rewriting systems. Deko V. Dekov in [16] has discussed the normal forms of a special case of free products with amalgamation of monoids, and has shown that the normal forms are unique, using rewriting systems. Again in [17] Deko V. Dekov has discussed normal forms of $HNN$-extensions of monoids, using rewriting systems. We will show that normal forms of $HNN$-extensions of monoids are unique, using different method from the one used in [17]. We will need to discuss transversals of submonoids. A new normal form theorem for monoids with commutative submonids is proved.

## 3.2 Free groups

Let $\mathbf{x}$ be a set, $\mathbf{x}^{-1}$ be a set (disjoint from $\mathbf{x}$) in 1 : 1 correspondence $x \leftrightarrow x^{-1}$ with $\mathbf{x}$. Consider the rewriting system

$$\mathfrak{F}(\mathbf{x}) = \mathfrak{F} = [\mathbf{x}, \mathbf{x}^{-1}; x^{\varepsilon}x^{-\varepsilon} = \epsilon \ (x \in \mathbf{x}, \varepsilon = \pm 1)].$$

**Lemma 3.2.1** *$M(\mathfrak{F})$ is a group.*

**Proof** We show that for any $[W] \in M(\mathfrak{F})$ there exists $[W'] \in M(\mathfrak{F})$ such that

$$[W][W'] = [W'][W] = 1_{M(\mathfrak{F})} = [\epsilon].$$

If $W = \epsilon$, then there is nothing to prove. Otherwise let

$$W = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \ (\varepsilon_i = \pm 1, x_i \in \mathbf{x}, n \geq i \geq 1)$$

be a word on $\mathbf{x} \cup \mathbf{x}^{-1}$. Then

$$W' = x_n^{-\varepsilon_n} x_{n-1}^{-\varepsilon_{n-1}} \cdots x_2^{-\varepsilon_2} x_1^{-\varepsilon_1}$$

is also a word in $\mathbf{x} \cup \mathbf{x}^{-1}$. And

$$\begin{aligned} WW' &= x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots \underline{x_n^{\varepsilon_n} x_n^{-\varepsilon_n}} x_{n-1}^{-\varepsilon_{n-1}} \cdots x_2^{-\varepsilon_2} x_1^{-\varepsilon_1} \\ &\to x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots \underline{x_{n-1}^{-\varepsilon_{n-1}} x_{n-1}^{-\varepsilon_{n-1}}} \cdots x_2^{-\varepsilon_2} x_1^{-\varepsilon_1} \\ &\to \cdots\cdots \\ &\to x_1^{\varepsilon_1} \underline{x_2^{\varepsilon_2} x_2^{-\varepsilon_2}} x_1^{-\varepsilon_1} \\ &\to \underline{x_1^{\varepsilon_1} x_1^{-\varepsilon_1}} \\ &\to \epsilon \end{aligned}$$

Thus $[W][W'] = [\epsilon]$. Similarly $[W'][W] = [\epsilon]$. Thus every element of $M(\mathfrak{F})$ has an inverse in $M(\mathfrak{F})$. Hence $M(\mathfrak{F})$ is a group, since $M(\mathfrak{F})$ is a monoid and every element of $M(\mathfrak{F})$ has an inverse in $M(\mathfrak{F})$.□

We call $M(\mathfrak{F})$ the *free group* on $\mathbf{x}$, denoted by $F(\mathbf{x})$.

**Theorem 3.2.2** *$\mathfrak{F}$ is a complete rewriting system.*

**Proof** We observe that $L(x^\varepsilon x^{-\varepsilon}) = 2 > L(\epsilon) = 0$. Thus $x^\varepsilon x^{-\varepsilon} >_{LO} \epsilon$. Since $LO$ is a reduction ordering, by Theorem 2.1.2, the rewriting system $\mathfrak{F}$ is noetherian.

There are no inclusion ambiguities. The overlap ambiguities are of the form $x^\varepsilon x^{-\varepsilon} x^\varepsilon$ ($x \in \mathbf{x}$, $\varepsilon = \pm 1$) [corresponding to the defining relations $R : x^\varepsilon x^{-\varepsilon} = \epsilon$, $S : x^{-\varepsilon} x^\varepsilon = \epsilon$]. Then

$$\underline{x^\varepsilon x^{-\varepsilon}} x^\varepsilon \to x^\varepsilon$$

and

$$x^{\varepsilon}\underline{x^{-\varepsilon}x^{\varepsilon}} \to x^{\varepsilon}.$$

Thus the critical pairs arising from overlap ambiguities are resolved. Hence by Theorem 2.2.1, $\mathfrak{F}$ is confluent. The rewriting system $\mathfrak{F}$ is complete since it is both noetherian and confluent.□

Since $\mathfrak{F}$ is complete, by Lemma 2.1.1, each equivalence class contains at least one irreducible. The irreducibles of $\mathfrak{F}$ are words $W$ such that $W$ does not contain a pair $x^{\varepsilon}x^{-\varepsilon}$ ($x \in \mathbf{x}$, $\varepsilon = \pm 1$). The words on $\mathbf{x} \cup \mathbf{x}^{-1}$ which are irreducible with respect to $\mathfrak{F}$ are called *freely reduced* words.

**Corollary 3.2.3** (*Normal form theorem for free groups*) *Each element of* $F(\mathbf{x})$ *is represented by a unique freely reduced word.*

**Proof** Since $\mathfrak{F}$ is complete, then by Theorem 2.3.1, every equivalence class in $\mathfrak{F}$ (element of $F(\mathbf{x})$) is represented by a unique irreducible.□

## 3.3 Free product of two monoids

Let $A$ and $B$ be monoids ($A \cap B = \emptyset$). Consider the rewriting system

$$\mathfrak{F}\mathcal{P}(A,B) = \mathfrak{F}\mathcal{P} = [A, B; 1_A = \epsilon, 1_B = \epsilon, aa' = a \cdot a' \ (a, a' \in A), bb' = b \cdot b' \ (b, b' \in B)].$$

Here $a \cdot a'$ denotes the product of $a$ and $a'$ in $A$ (similarly for $B$). We call $M(\mathfrak{F}\mathcal{P})$ the *free product* of $A$ and $B$, denoted by $A * B$. The monoids $A$ and $B$ are called the *free factors* of $A * B$.

**Lemma 3.3.1** *If $A, B$ are groups so is $A * B$.*

**Proof** We show that for any $[W] \in A * B$ there exists $W' \in A * B$ such that

$$[W][W'] = [W'][W] = 1_{A*B} = [\epsilon].$$

If $W = \epsilon$, then there is nothing to prove. Otherwise let

$$W = x_1 x_2 \cdots x_n \; (x_1, x_2, \cdots, x_n \in A \cup B, n \geq 1).$$

But each $x_i$ has an inverse $x_i^{-1}$ in the group $A$ or $B$ to which it belongs. Let

$$W' = x_n^{-1} x_{n-1}^{-1} \cdots x_2^{-1} x_1^{-1}$$

Then

$$
\begin{aligned}
WW' &= x_1x_2\cdots x_{n-1}\underline{x_nx_n^{-1}}x_{n-1}^{-1}\cdots x_2^{-1}x_1^{-1} \\
&\to x_1x_2\cdots x_{n-1}\underline{1}x_{n-1}^{-1}\cdots x_2^{-1}x_1^{-1} \quad \left\{ \begin{array}{l} \text{where 1 denotes the identity of the} \\ \text{group } A \text{ or } B \text{ to which } x_n \text{ belongs.} \end{array} \right. \\
&\to x_1x_2\cdots \underline{x_{n-1}x_{n-1}^{-1}}\cdots x_2^{-1}x_1^{-1} \\
&\to \cdots\cdots\cdots \\
&\to \cdots\cdots\cdots \\
&\to x_1\underline{x_2x_2^{-1}}x_1^{-1} \\
&\to x_1\underline{1}x_1^{-1} \\
&\to \underline{x_1x_1^{-1}} \\
&\to \underline{1} \\
&\to \epsilon.
\end{aligned}
$$

Thus $[W][W'] = [\epsilon]$. Similarly $[W'][W] = [\epsilon]$. Hence $A * B$ is a group since $A * B$ is a monoid and every element $[W] \in A * B$ has an inverse in $A * B$.□

Let $\mathcal{P}_A = [A; aa = a \cdot a' \ (a, a' \in A),\ 1_A = \epsilon]$. Consider the function

$$\psi : A \longrightarrow A$$
$$a \mapsto a \ (a \in A).$$

By Theorem 1.6.2 we get an induced homomorphism

$$\psi_{\mathcal{P}_A} : M(\mathcal{P}_A) \longrightarrow A$$
$$[a]_{\mathcal{P}_A} \mapsto a \ (a \in A),$$

since $\psi(aa') = \psi(a \cdot a')$ $(a, a' \in A)$ and $\psi(\epsilon) = \psi(1_A)$.

**Lemma 3.3.2** *$\mathcal{P}_A$ is a complete rewriting system, and $\psi_{\mathcal{P}_A}$ is an isomorphism.*

**Proof** Clearly $\psi_{\mathcal{P}_A}$ is surjective. We observe that $L(aa') = 2 > L(a \cdot a') = 1$ and $L(1_A) = 1 > L(\epsilon) = 0$. Thus $aa' >_{LO} a \cdot a'$ and $1_A >_{LO} \epsilon$. Since $LO$ is a reduction ordering, $\mathcal{P}_A$ is noetherian by Theorem 2.1.2. Hence by Lemma 2.1.1, each equivalence class contains an irreducible. The irreducibles of $\mathcal{P}_A$ are $a$ $(a \in A - \{1_A\})$ and $\epsilon$. Suppose there exist irreducibles $a, a'$ such that

$$[a] = [a'].$$

Then

$$\psi_{\mathcal{P}_A}([a]) = \psi_{\mathcal{P}_A}([a']).$$

Hence

$$a = a'.$$

Also

$$\psi_{\mathcal{P}_A}([\epsilon]) = \psi([\epsilon]) = 1_A.$$

Thus $\psi_{\mathcal{P}_A}$ is injective. Hence $\psi_{\mathcal{P}_A}$ is an isomorphism since it is a bijective homomorphism. Moreover each equivalence class contains a unique irreducible so $\mathcal{P}_A$ is complete by Theorem 2.3.1.□

We remark that we can similarly define $\mathcal{P}_B$ and show that it is a complete rewriting system.

**Theorem 3.3.3** *$\mathfrak{FP}$ is a complete rewriting system.*

**Proof** We observe that

$$\mathfrak{FP} = \mathcal{P}_A \cup \mathcal{P}_B.$$

But $\mathcal{P}_A$ and $\mathcal{P}_B$ do not intersect, and are both complete. Hence $\mathfrak{FP}$ is a complete rewriting system.□

A non-empty word

$$x_1x_2x_3x_4\cdots x_{n-1}x_n \ (n \geq 1, x_1, x_2, \cdots, x_n \in A \cup B)$$

on $A \cup B$ is said to be *irreducible* if no $x_i$ is $1_A$ nor $1_B$, and there exists no subsequence $x_ix_{i+1}$ $(i = 1, 2, \cdots, n-1)$, such that $x_i$ and $x_{i+1}$ are from the same free factor. The irreducible words with respect to $\mathfrak{FP}$ are usually just called *reduced* words.

**Corollary 3.3.4** (*Normal form theorem for free products*) *Every element of $M(\mathfrak{FP})$ is represented by a unique reduced word.*

**Proof** This is a consequence of Theorem 3.3.2 and Theorem 2.3.1.□

## 3.4 Transversals

A *right transversal* of a monoid $A$ with respect to a submonoid $H \subseteq A$ is a subset $T$ of $A$, such that $1_A \in T$ and for every $a \in A$, then $a$ can be uniquely expressed as a product $h_a \cdot a^*$ (for some $h_a \in H, a^* \in T$). Similarly we have *left transversals.* We remark that such a set $T$, may not exist, but if $A, H$ are groups, then $T$ always exist.

**Example 3.4.1** *Let $A$ be the symmetric group on $\{1,2,3\}$, and let $H$ be the subgroup of $A$ generated by* $(12)$. *One right transversal of $A$ with respect to $H$ is $\{1,(13),(23)\}$, which is also a left transversal. Another is $\{1,(13),(132)\}$, but this is not a left transversal.*

**Example 3.4.2** *Let $A_1$, $A_2$ be monoids, and let $A = A_1 \times A_2$ be the direct product of $A_1$ and $A_2$.*
*$\bar{A}_1 = \{(a_1, 1) : a_1 \in A\}$ is a (left or right) transversal of $A$ with respect to $\bar{A}_2 = \{(1, a_2) : a_2 \in A_2\}$.*

**Example 3.4.3** *Let $\mathcal{P}$ be as in Example* 2.2.1. *Elements of $M(\mathcal{P})$ are $[x^i]$, $[\theta x^i]$ $(i = 0, 1, 2, \cdots)$. Let $H = \{[x^i] : i = 0, 1, 2, \cdots\}$. Then $T = \{[\epsilon], [\theta]\}$ is a left transversal of $M(\mathcal{P})$ with respect to $H$. But there is no right transversal of $M(\mathcal{P})$ with respect to $H$.*

Suppose there exists a right transversal $T$ for $H$ in $A$. Let $\bar{T} = T - 1_A, \bar{A} =$

$A - (T \cup H)$,

Note that $\bar{T}, \bar{A}$ and $H$ form a partition for $A$.

As in the previous section, we let $\mathcal{P}_A = [A; aa' = a \cdot a' \ (a, a' \in A), 1_A = \epsilon]$.

Let $\mathcal{P}_A^* = [\bar{A}, H, \bar{T}; \mathbf{r}_A]$ where $\mathbf{r}_A$ is the following set of defining relations

$$(a) \quad hh' = h \cdot h' \ (h, h' \in H)$$

$$(b) \quad 1_A = \epsilon$$

$$(c) \quad a = h_a a^* \ (a \in \bar{A})$$

$$(d) \quad tt' = h_{t \cdot t'}(t \cdot t')^* \ (t, t' \in \bar{T})$$

$$(e) \quad tu = h_{t \cdot u}(t \cdot u)^* \ (t \in \bar{T}, u \in H).$$

We observe that the defining relations $\mathbf{r}_A$ of $\mathcal{P}_A^*$ are consequences of the defining relations of $\mathcal{P}_A$. This is clear for $(a)$, $(b)$ $(c)$. For $(d)$, $(e)$ we have

$$tt' \to t \cdot t' = h_{t \cdot t'} \cdot (t \cdot t')^* \leftarrow h_{t \cdot t'}(t \cdot t')^*;$$

$$tu \to t \cdot u = h_{t \cdot u} \cdot (t \cdot u)^* \leftarrow h_{t \cdot u}(t \cdot u)^*.$$

Consider the mapping

$$\theta : A \longrightarrow M(\mathcal{P}_A)$$

$$a \mapsto [a]_{\mathcal{P}_A} \ (a \in A).$$

Since each defining relation of $\mathcal{P}_A^*$ is a consequence of the defining relations of $\mathcal{P}_A$, by Theorem 1.6.2, we get an induced homomorphism

$$\theta_{\mathcal{P}_A^*} : M(\mathcal{P}_A^*) \longrightarrow M(\mathcal{P}_A)$$

$$[a]_{\mathcal{P}_A^*} \mapsto [a]_{\mathcal{P}_A} \ (a \in A).$$

Clearly $\theta_{\mathcal{P}_A^*}$ is surjective.

**Theorem 3.4.1** *$\mathcal{P}_A^*$ is complete and $\theta_{\mathcal{P}_A^*}$ is an isomorphism.*

**Proof** We first show that $\mathcal{P}_A^*$ *is noetherian.* Define the weight function

$$\beta(h) = 1 \ (h \in H),$$

$$\beta(t) = 2 \ (t \in \bar{T}),$$

$$\beta(a) = 4 \ (a \in \bar{A}).$$

Define a precedence on $A$ by assigning precedences on $\bar{T}$, $H$, $\bar{A}$, and using the precedence $\bar{T} \rhd H \rhd \bar{A}$. Let $>_{WLO-L}$ denote the corresponding weight-plus-lexicographic ordering from the left on $A^*$.

Then

$$\beta(hh') = 2 > \beta(h \cdot h') = 1 \Rightarrow hh' >_{WLO-L} h \cdot h' \ (h, h' \in H);$$

$$\beta(1_A) = 1 > \beta(\epsilon) = 0 \Rightarrow 1_A >_{WLO-L} \epsilon;$$

$$\beta(a) = 4 > \beta(h_a a^*) = 3 \Rightarrow a >_{WLO-L} h_a a^* \ (a \in \bar{A});$$

$$\beta(tt') = 4 > 3 \geq \beta(h_{t \cdot t'}(t \cdot t')^* \Rightarrow tt' >_{WLO-L} h_{t \cdot t'}(t \cdot t')^* \ (t, t' \in \bar{T});$$

$$\beta(tu) = 3 \geq \beta(h_{t \cdot u}(t \cdot u)^*) \text{ and since } t \rhd h_{t \cdot u} \Rightarrow tu >_{WLO-L} h_{t \cdot u}(t \cdot u)^*$$

$$(t \in \bar{T}, u \in H).$$

Thus for any $R : R_{+1} = R_{-1} \in \mathbf{r}_A$ then $R_{+1} >_{WLO-L} R_{-1}$. Since $>_{WLO-L}$ is a reduction ordering which is compatible with $\mathbf{r}$, by Theorem 2.1.2, $\mathcal{P}_A^*$ is noetherian.

The irreducibles in $\mathcal{P}_A^*$ are $(i)$ $t$ $(t \in \bar{T})$, $(ii)$ $h$ $(h \in \bar{H})$, $(iii)$ $\epsilon$, and $(iv)$ $ht$ $(h \in \bar{H},\, t \in \bar{T})$.

Let $\Phi = \psi_{\mathcal{P}_A}\theta_{\mathcal{P}_A^*}$ where

$$\psi_{\mathcal{P}_A} : M(\mathcal{P}_A) \longrightarrow A$$

$$[a]_{\mathcal{P}_A} \mapsto a \ (a \in A)$$

is as in Section 3.2.

We will show that if $U$, $V$ are distinct irreducibles in $\mathcal{P}_A^*$ then $\Phi([U]) \neq \Phi([V])$. We will show for the case when both $U$ and $V$ are of type $(iv)$, since for other cases it is similar or clear. Suppose we have irreducibles $ht$ *and* $h't'$ such that

$$[ht] = [h't'] \ (h \in \bar{H}, t \in \bar{T}).$$

Then

$$\psi_{\mathcal{P}_A}\theta_{\mathcal{P}_A^*}([ht]_{\mathcal{P}_A^*}) = \psi_{\mathcal{P}_A}([ht]_{\mathcal{P}_A}) = h \cdot t,$$

$$\psi_{\mathcal{P}_A}\theta_{\mathcal{P}_A^*}([h't']_{\mathcal{P}_A^*}) = \psi_{\mathcal{P}_A}([h't']_{\mathcal{P}_A}) = h' \cdot t'.$$

Since the products $h \cdot t$ and $h' \cdot t'$ are unique, then $h = h'$ and $t = t'$. Hence $ht = h't'$. Thus the irreducibles are unique. This implies that $\mathcal{P}_A^*$ is complete by Theorem 2.3.1. Also $\Phi$ is injective, so $\theta_{\mathcal{P}_A^*}$ is injective. Hence $\theta_{\mathcal{P}_A^*}$ is an isomorphism.□

**Lemma 3.4.2** *$\mathcal{P}_A$ and $\mathcal{P}_A^*$ are equivalent.*

**Proof** Since $\theta_{\mathcal{P}_A^*}$ is an isomorphism, then each defining relation of $\mathcal{P}$ is a consequence of the defining relation of $\mathcal{P}_A^*$. Hence by Lemma 1.7.1, $\mathcal{P}_A$ and $\mathcal{P}_A^*$ are equivalent.□

Now suppose we have a left transversal $S$ of a monoid $B$ with respect to a submonoid $K \subseteq B$. Let ${}^*\mathcal{P}_B = [\bar{B}, K, \bar{S}; {}^*\mathbf{r}_B]$ where ${}^*\mathbf{r}_B$ is the following set of defining relations

$$(a) \quad kk' = k \cdot k' \ (k, k' \in K)$$

$$(b) \quad 1_B = \epsilon$$

$$(c) \quad b = b^* k_b \ (b \in \bar{B})$$

$$(d) \quad ss' = (s \cdot s')^* k_{s \cdot s'} \ (s, s' \in \bar{S})$$

$$(e) \quad us = (s \cdot u)^* k_{s \cdot u} \ (s \in \bar{S}, u \in K).$$

We remark that we get similar results, as we did for right transversals.

## 3.5 Monoids with amalgamated submonoids

Let $A, B$ $(A \cap B = \emptyset)$ be monoids with submonoids $H, K$ respectively, such that there exists an isomorphism

$$\theta : H \longrightarrow K.$$

Consider the presentation

$$\mathcal{A} = \mathcal{A}(A,\, B,\, \theta) = [A,\, B;\, aa' = a \cdot a' \ (a, a' \in A),\, bb' = b \cdot b' \ (b, b' \in B),\, 1_A = \epsilon,\, 1_B = \epsilon,\, h = \theta(h) \ (h \in H)].$$

Then $M(\mathcal{A})$ is called the *free product of* $A, B$ *amalgamating* $H, K$, denoted by $A *_H B$.

**Lemma 3.5.1** *If* $A, B$ *are groups then so is* $A *_H B$.

**Proof** We will show that for any $[W] \in M(\mathcal{A})$, there exists $[W'] \in M(\mathcal{A})$ such that $[W][W'] = [\epsilon]$. If $W = \epsilon$, then there is nothing to prove. Otherwise let

$$W = x_1 x_2 \cdots x_n \ (n \geq 1, x_1, x_2, \cdots, x_n \in A \cup B).$$

Then the word

$$W' = x_n^{-1} x_{n-1}^{-1} \cdots x_2^{-1} x_1^{-1}$$

is also in $A \cup B$ (since $A, B$ are groups), where $x_i^{-1}$ is the inverse of $x_i$ in the group $A$ or $B$ to which it belongs. Thus $[W'] \in M(\mathcal{A})$, and by an argument similar to that in Lemma 3.3.1,

$$[W][W'] = [\epsilon] = [W'][W].\Box$$

Let $\mathbf{r}_A$ be as defined in the previous section, and let $\mathbf{r}_B$ be defined similarly (where $S$ is the right transversal of the submonoid $K \subseteq B$).

**Theorem 3.5.2** *Let* $\mathcal{A}^* = [\bar{A}, H, \bar{T}, \bar{B}, K, \bar{S}; \mathbf{r}_A, \mathbf{r}_B, h = \theta(h)\ (h \in H)]$. *Then* $\mathcal{A}^*$ *is equivalent to* $\mathcal{A}$, *and* $\mathcal{A}^*$ *is a complete rewriting system.*

**Proof** $\mathcal{A}$, $\mathcal{A}^*$ are equivalent since

$$\mathcal{A} = \mathcal{P}_A \cup \mathcal{P}_B \cup \{h = \theta(h); h \in H\} \text{ and}$$

$$\mathcal{A}^* = \mathcal{P}_A^* \cup \mathcal{P}_B^* \cup \{h = \theta(h); h \in H\}$$

But $\mathcal{P}_A$, $\mathcal{P}_A^*$ are equivalent. Also $\mathcal{P}_B$, $\mathcal{P}_B^*$ are equivalent. Hence by Lemma 1.7.1, the rewriting systems $\mathcal{A}$, $\mathcal{A}^*$ are equivalent.

Define the weight fuction

$$\psi(h) = \psi(k) = 1 \ (h \in H, \, k \in K),$$

$$\psi(t) = \psi(s) = 2 \ (t \in \bar{T}, \, s \in \bar{S}),$$

$$\psi(a) = \psi(b) = 4 \ (a \in \bar{A}, \, b \in \bar{B}).$$

Define a precedence on $A \cup B$ by assigning precedences on $\bar{T}$, $H$, $\bar{A}$, $\bar{S}$, $K$, $\bar{B}$, and using the precedence $\bar{T} \rhd H \rhd \bar{S} \rhd K \rhd \bar{A} \rhd \bar{B}$. Let $>_{WLO-L}$ denote the corresponding weight-plus-lexicographic ordering from the left on $\mathcal{A}^*$. We observe that for any $R : R_{+1} = R_{-1}$, an element of the set of defining relations of $\mathcal{A}^*$, we have $R_{+1} >_{WLO-L} R_{-1}$. Since $WLO$-$L$ is a reduction ordering, then by Theorem 2.1.2, the rewiting system $\mathcal{A}^*$ is noetherian.

Since $\mathcal{P}_A^*$ and $\mathcal{P}_B^*$ are complete, then by Lemma 2.2.1, the critical pairs arising from $\mathbf{r}_A$ and $\mathbf{r}_B$ are respectively resolved. We observe that there are no critical pairs arising between $\mathbf{r}_A$ and $\mathbf{r}_B$. Similarly there are no critical pairs arising from $\mathbf{r}_B$ and $\{h = \theta(h); h \in H\}$. Thus we have critical pairs arising from the defining relators of $\mathcal{P}_A^*$ only, critical pairs arising from the defining relators of $\mathcal{P}_B^*$ only, and the critical pairs arising from

$$hh' = h \cdot h' \text{ and } h = \theta(h) \ (h, h' \in H)$$

$$tu = h_{t \cdot u}(t \cdot u)^* \text{ and } u = \theta(u) \ (t \in \bar{T},\ u \in H)$$

$$1_A = \epsilon \text{ and } 1_A = \theta(1_A).$$

But

$$\underline{hh'} \to h \cdot h' \text{ and } \underline{h}h' \to \theta(h)h' = \underline{m}h' \to \theta^{-1}(m)h' = \underline{hh'} \to h \cdot h'$$

Thus the critical pairs arising between the defining relators $hh' = h \cdot h'$ and $h = \theta(h)$ are resolved.

Also

$$\underline{tu} \to h_{t \cdot u}(t \cdot u)^* \text{ and } t\underline{u} \to \underline{t\theta(u)} \to \underline{t\theta^{-1}\theta(u)} \to h_{t \cdot u}(t \cdot u)^*$$

Thus the critical pairs arisising from the defining relators $tu = h_{t \cdot u}(t \cdot u)^*$ and $u = \theta(u)$ are resolved. Finally

$$\underline{1_A} \to \epsilon \text{ and } \underline{1_A} \to \underline{\theta(1_A)} \to \underline{\theta^{-1}\theta(1_A)} \to \epsilon$$

Thus the critical pairs arising from the defining relators $1_A = \epsilon$ and $1_A = \theta(1_A)$ are resolved. All the critical pairs of $\mathcal{A}^*$ are resolved since critical pairs arising from $\mathbf{r}_A$ only and critical pairs arising from $\mathbf{r}_B$ only are resolved. Thus by Theorem 2.2.1 $\mathcal{A}^*$ is confluent. The rewriting system $\mathcal{A}^*$ is complete since it is both noetherian and confluent.□

A *normal form* is a word in $A \cup B$ of the form

$$k\bar{a_1}\bar{a_2}\bar{a_3}\bar{a_4}\cdots\bar{a_n}$$

where $k \in K, n \geq 0, a_1, a_2, \cdots, a_n \in S \cup T$, and adjacent $a's$ lie in distinct monoids.

**Corollary 3.5.3** (*Normal form theorem for free products with amalgamated submonoids*) *Every equivalence class in $M(\mathcal{A})$ is represented by a unique normal form.*

**Proof** Since the $\mathcal{A}^*$ irreducible sequences are exactly the normal forms, and since $\mathcal{A}^*$ is complete, then by Theorem 2.3.4, there is exactly one reduced sequence representing each element of $M(\mathcal{A}^*)$. But $M(\mathcal{A}^*) = M(\mathcal{A})$, hence every equivalence class in $M(\mathcal{A})$ contains a unique reduced sequence.□

We also refer the reader to Dekov V. Dekov [16] who proved a special case of Corollary 3.5.3. He has proved the case when the subgroups $H$ and $K$ are the same.

## 3.6 HNN-extensions

Let $A$ be a monoid, and $H, K$ be submonoids of $A$. Suppose there exists an isomorphism

$$\theta : H \longrightarrow K.$$

Consider the rewriting system

$$\mathcal{H} = [x, x^{-1}, A; \mathbf{r}_{\mathcal{H}}],$$

where $\mathbf{r}_{\mathcal{H}}$ is the following set of defining relations

$$(i)\quad aa' = a \cdot a' \ (a, a' \in A);$$

$$(ii)\quad x^{\varepsilon}x^{-\varepsilon} = \epsilon \ (\varepsilon = \pm 1);$$

$$(iii)\quad x^{-1}h = \theta(h)x^{-1} \ (h \in H);$$

$$(iv)\quad xk = \theta^{-1}(k)x \ (k \in K);$$

$$(v)\quad 1_A = \epsilon.$$

Then $M(\mathcal{H})$ is called the *HNN-extension* of $A$ with *associated submonoids* $H, K$, denoted by $A *_{H=K}$.

Suppose there exist right transerversals $T$ and $S$ for $H$ in $A$ and $K$ in $A$ respectively. Let $\mathcal{H}^* = [A, x, x^{-1}; \mathbf{r}_{\mathcal{H}^*}]$ where $\mathbf{r}_{\mathcal{H}^*}$ is $\mathbf{r}_{\mathcal{H}}$ together with the following set of defining relations;

$$x^{-1}a = \theta(h)x^{-1}t;\ h \in H - \{1_A\},\ t \in T - \{1_A\},\ \text{and } a = h \cdot t$$

$$xa = \theta^{-1}(k)xs;\ k \in K - \{1_A\},\ s \in S - \{1_A\},\ \text{and } a = k \cdot s$$

**Lemma 3.6.1** *$\mathcal{H}^*$ and $\mathcal{H}$ define the same monoid.*

**Proof** The defining relations of $\mathcal{H}$ are already in $\mathbf{r}_{\mathcal{H}^*}$, the defining relations of $\mathcal{H}^*$. Now we will only show that $x^{-1}a \leftrightarrow^*_{\mathcal{H}} \theta(h)x^{-1}t$ and $xa \leftrightarrow^*_{\mathcal{H}} \theta^{-1}(k)xs$. But

$$\begin{aligned} x^{-1}a &= x^{-1}(h \cdot t) \\ &\leftrightarrow^*_{\mathcal{H}} \underline{x^{-1}h}t \\ &\leftrightarrow^*_{\mathcal{H}} \theta(h)x^{-1}t. \end{aligned}$$

Also

$$\begin{aligned} xa &= x(m \cdot k) \\ &\leftrightarrow^*_{\mathcal{H}} \underline{xm}k \\ &\leftrightarrow^*_{\mathcal{H}} \theta^{-1}(m)xk \end{aligned}$$

Thus by Lemma 1.7.1, $\mathcal{H}$ and $\mathcal{H}^*$ are equivalent. Hence $M(\mathcal{H}) = M(\mathcal{H}^*)$.□

**Lemma 3.6.2** *$\mathcal{H}^*$ is noetherian.*

**Proof** Let

$$\mathcal{P}_A = [A; aa' = a \cdot a' \ (a, a' \in A), \ 1_A = \epsilon].$$

For $U, V$ words on $A$, write $U \rhd_H V$ if

$$\begin{aligned} &\textit{either}: && U \rightarrow_{\mathcal{P}_A} V \\ &\textit{or}: && U = hV \text{ (for some } h \in H) \\ &\textit{or}: && U = aW \text{ (for some } a \text{ not in } H \cup T \text{ and } V = a^*W), \end{aligned}$$

where, as usual,

$$a = h_a \cdot a^*, h_a \in H, a^* \in \bar{T}.$$

Let $\succ_H$ denote the transitive closure of $\rhd_H$ . Clearly there is no infinite chain

$$U_1 \rhd_H U_2 \rhd_H U_3 \rhd_H \cdots,$$

so $\succ_H$ is noetherian. Hence $\succ_H$ is irreflexive for if we had a chain

$$U_1 \succ_H U_2 \succ_H U_3 \succ_H \cdots \succ_H U_n = U_1$$

with $n > 0$, then we can repeat this chain arbitrarily often

$$U_1 \succ_H U_2 \succ_H \cdots \succ_H U_n = U_1 \succ_H U_2 \succ_H \cdots \succ_H U_n = U_1 \succ_H U_2 \cdots ,$$

thus contradicting the fact that $\succ_H$ is noetherian. Hence $\succ_H$ is an ordering. Similarly, we have the ordering $\succ_K$ .

Now consider the rewriting system $\mathcal{H}^*$. If $W$ is a word on $A \cup \{x, x^{-1}\}$ then we let $W^\circ$ be the word on $\{x, x^{-1}\}$ obtained by deleting all letters from $A$. We write $U > V$ if

*either* : $V^\circ$ is obtained from $U^\circ$ by deleting a subword $x^\varepsilon x^{-\varepsilon}$ $(\varepsilon = \pm 1)$

*or* : $U^\circ = V^\circ$ and

$$U = U_{n+1} x^{\varepsilon_n} \cdots U_3 x^{\varepsilon_2} U_2 x^{\varepsilon_1} U_1$$

$$V = V_{n+1} x^{\varepsilon_n} \cdots V_3 x^{\varepsilon_2} V_2 x^{\varepsilon_1} V_1$$

where there exists $1 \leq i \leq n+1$ such that

$$U_1 = V_1, U_2 = V_2, \cdots U_{i-1} = V_{i-1}$$

and

*either* $i < n+1$ and $U_i \prec_H V_i$ (if $\varepsilon_i = -1$) or $U_i \prec_K V_i$ (if $\varepsilon_i = +1$)

*or* $i = n+1$, $U_i \neq V_i$ and $U_i \rightarrow^*_{\mathcal{P}_A} V_i$.

The ordering $>$ is monotonic. Clearly there can be no infinite descending chain

$$W_0 > W_1 > W_2 > \cdots .$$

Hence $>$ is a reduction ordering on $\mathcal{H}^*$. It can be easily shown that $>$ is compatible with the defining relations of $\mathcal{H}^*$. Thus by Theorem 2.1.2, $\mathcal{H}^*$ is noetherian.□

Since $\mathcal{H}^*$ is noetherian, by Lemma 2.1.1, each equivalence class contains at least one irreducible. An *irreducible* in $\mathcal{H}^*$ is either the empty word $\epsilon$ or a word $x^m$ $m \in \mathbb{Z} - \{0\}$ or is a word

$$a_0 x^{k_1} a_1 x^{k_2} a_2 \cdots x^{k_n} a_n \ (n \geq 0)$$

where

$(i)$ $K_1, k_2, \cdots k_n$ are non-zero integers.

$(ii)$ $a_0 \in A - \{1_A\}$.

$(iii)$ If $k_i < 0$, then $a_i \in \bar{T}$ $(i = 1, 2, \cdots n)$.

$(iv)$ If $k_i > 0$, then $a_i \in \bar{S}$ $(i = 1, 2, \cdots n)$.

**Theorem 3.6.3** *Each equivalence class in $M(\mathcal{H})$ has a unique irreducible.*

**Proof** It can be shown that the critical pairs of $\mathcal{H}^*$ are resolved. This is long but straightforward and we omit the details. Then by Lemma 3.6.2 and Theorem 2.3.1, each equivalence class in $M(\mathcal{H}^*)$ contains a unique irreducible. Since $M(\mathcal{H}) = M(\mathcal{H}^*)$, then every equivalence class in $M(\mathcal{H})$ has a unique irreducible.

## 3.7 Monoids with commutative submonoids

Let $A$ and $B$ be monoids with submonoids $H$ and $K$ respectively. Define

$$\mathcal{K} = [A, B; aa' = a \cdot a' \ (a, a' \in A),\ bb' = b \cdot b' \ (b, b' \in B),\ kh = hk \ (h \in H, k \in K)].$$

Then $M(\mathcal{K})$ is called the *free product of $A$ and $B$ with commutative submonoids* $H$ and $K$.

Suppose there exist a right transversal $T$ and a left transversal $S$ for $H$ in $A$ and $K$ in $B$ repectively. Let

$$\mathcal{P}_A^* = [\bar{A}, H, \bar{T}; \mathbf{r}_A]$$

$${}^*\mathcal{P}_B = [\bar{B}, K, \bar{S}; {}^*\mathbf{r}_B]$$

as in Section 3.4.

**Theorem 3.7.1** *$\mathcal{K}^* = [\bar{A}, H, \bar{T}, \bar{B}, M, \bar{K}; \mathbf{r}_A, {}^*\mathbf{r}_B, 1_A = \epsilon, 1_B = \epsilon, kh = hk$ $(h \in H, k \in K)]$ is equivalent to $\mathcal{K}$, and $\mathcal{K}^*$ is complete.*

**Proof** $\mathcal{K}$, $\mathcal{K}^*$ are equivalent since

$$\mathcal{K} = \mathcal{P}_A \cup \mathcal{P}_B \cup \{1_A = \epsilon, 1_B = \epsilon, kh = hk; h \in H, k \in K\} \text{ and}$$

$$\mathcal{K}^* = \mathcal{P}_A^* \cup {}^*\mathcal{P}_B \cup \{1_A = \epsilon, 1_B = \epsilon, kh = hk; h \in H, k \in K\}.$$

But $\mathcal{P}_A$, $\mathcal{P}_A^*$ are equivalent. Also $\mathcal{P}_B$, ${}^*\mathcal{P}_B$ are equivalent. Hence by Lemma 1.7.1, the rewriting systems $\mathcal{K}$, $\mathcal{K}^*$ are equivalent.

Define the weight fuction

$$\psi(h) = \psi(k) = 1 \ (h \in H, \, k \in K),$$

$$\psi(t) = \psi(k) = 2 \ (t \in \bar{T}, \, s \in \bar{S}),$$

$$\psi(a) = \psi(b) = 4 \ (a \in \bar{A}, \, b \in \bar{B}).$$

Define a precedence on $A \cup B$ by assigning precedences on $\bar{T}$, $H$, $\bar{A}$, $\bar{S}$, $K$, $\bar{B}$, and using the precedence $K \rhd H \rhd \bar{T} \rhd \bar{S} \rhd \bar{A} \rhd \bar{B}$. Let $>_{WLO-L}$ denote the corresponding weight-plus-lexicographic ordering from the left on $\mathcal{A}^*$. We observe that for any defining relation $R : R_{+1} = R_{-1}$ of $\mathcal{K}^*$, $R_{+1} >_{WLO-L} R_{-1}$. Since $WLO$-$L$ is a reduction ordering, by Theorem 2.1.2, $\mathcal{K}^*$ is noetherian.

Now we observe that the introduction of the defining relation $kh = hk$ $(h \in H, k \in K)$ yields new overlap ambiguities of the following forms

$(i)$ $kh_1h_2$ corresponding to the relations $R : h_1h_2 = h_1 \cdot h_2$, $S : kh_1 = h_1k$ $(h_1, h_2 \in H, k \in K)$;

$(ii)$ $k_1k_2h$ corresponding to the relations $R : k_2h = hk_2$, $S : k_1k_2 = k_1 \cdot k_2$ $(h \in H, k_1, k_2 \in K)$. But

$$\underline{kh_1}h_2 \to h_1\underline{kh_2} \to \underline{h_1h_2}k \to (h_1 \cdot h_2)k$$

and

$$k\underline{h_1h_2} \to \underline{k(h_1 \cdot h_2)} \to (h_1 \cdot h_2)k.$$

Similarly

$$k_1\underline{k_2h} \to \underline{k_1h}k_2 \to h\underline{k_1k_2} \to h(k_1 \cdot k_2)$$

and

$$\underline{k_1k_2}h \to \underline{(k_1 \cdot k_2)h} \to h(k_1 \cdot k_2).$$

Hence the critical pairs arising from the above overlap ambiguities are resolved. Thus all critical pairs of $\mathcal{K}^*$ are resolved (see Section 3.4). Hence by Theorem 2.3.1, $\mathcal{K}^*$ is confluent. The rewriting system $\mathcal{K}^*$ is complete since it is both noetherian and confluent.□

An *irreducible* in $\mathcal{K}$ is a word on $H \cup K \cup T \cup S$ of the form

$$x_1 x_2 \cdots x_n \ (n \geq 0),$$

such that

$(i)$ none of the $x_i's$ $(i = 1, 2, \cdots, n)$ is $1_A$ nor $1_B$;

$(ii)$ whenever we have $x_i \in K$, then $x_{i+1} \in \bar{T}$ $(i = 1, 2, \cdots n-1)$;

$(iii)$ whenever we have $x_i \in H$, then $x_{i-1} \in \bar{S}$ $(i = 2, 3, \cdots n)$;

$(iv)$ whenever we have $x_i \in \bar{T}$, then $x_{i+1}$ can not belong to $H$ $(i = 1, 2, \cdots, n-1)$;

$(v)$ whenever we have $x_i \in \bar{S}$, then $x_{i-1}$ can not belong to $K$ $(i = 1, 2, \cdots, n-1)$;

$(vi)$ there does not exist any subsequence $x_i x_{i+1}$ $(i = 1, 2, \cdots n-1)$ such that both $x_i$ and $x_{i+1}$ belong to the same submonoid or to the same transversal.

**Corollary 3.7.2** *Every equivalence class in $M(\mathcal{K}^*)$ contains a unique irreducible.*

**Proof** This is a consequence of Theorem 3.5.1.□

# Chapter 4

# Word problem for monoids and groups

## 4.1 Word problem for monoids

Through out this chapter all monoid presentations will be assumed to be finite. Let

$$\mathcal{P} = [\mathbf{x}; \mathbf{r}]$$

be a monoid presentation. We say that the *word problem* for $\mathcal{P}$ is *decidable* or *solvable* if there exists an algorithm which determines, for all $W, W' \in \mathbf{x}^*$, whether or not

$$[W]_{\mathcal{P}} = [W']_{\mathcal{P}}.$$

**Theorem 4.1.1** *If two presentations $\mathcal{P}$, $\mathcal{P}'$ define the same monoid, and if one has a solvable word problem, then so does the other.*

**Proof** Since $\mathcal{P}$ and $\mathcal{P}'$ define the same monoid, by Corollary 1.7.4 $\mathcal{P}'$ can be obtained from $\mathcal{P}$ by a finite application of elementary Tietze transformations.

**Special case 1** Let $\mathcal{P} = [\mathbf{x}; \mathbf{r}]$ and $\mathcal{P}' = [\mathbf{x}; \mathbf{r}, U{=}V]$ where $U \leftrightarrow^*_{\mathcal{P}} V$ $(U, V \in \mathbf{x}^*)$. By Lemma 1.7.1, $\mathcal{P}$ and $\mathcal{P}'$ are equivalent. Thus $\leftrightarrow^*_{\mathcal{P}}$ and $\leftrightarrow^*_{\mathcal{P}'}$ are the same congruence. Hence if one of the presentations $\mathcal{P}$, $\mathcal{P}'$ has the solvable word problem, then so does the other.

**Special case 2** Let $\mathcal{P} = [\mathbf{x}; \mathbf{r}]$ and $\mathcal{P}' = [\mathbf{x}, y; \mathbf{r}, y = Z]$, where $Z$ is any word on $\mathbf{x}$. Suppose $\mathcal{P}'$ has a solvable word problem. Since $\mathcal{P}'$ has a solvable word problem, it implies that for any two words $W$, $W'$ on $\mathbf{x}$, there is an algorithm to decide whether or not $[W]_{\mathcal{P}'} = [W']_{\mathcal{P}'}$. By Lemma 1.7.2, the monoids defined by $\mathcal{P}$ and $\mathcal{P}'$ are isomorphic. Hence the word problem for $\mathcal{P}'$ is solved in this way, if $[W]_{\mathcal{P}'} = [W']_{\mathcal{P}'}$, then $[W]_{\mathcal{P}} = [W']_{\mathcal{P}}$. Otherwise $[W]_{\mathcal{P}} \neq [W']_{\mathcal{P}}$.

Now suppose $\mathcal{P}$ has a solvable word problem. If $W$, $W'$ are words on $\mathbf{x}$ only, then we can use the same algorithm used on $\mathcal{P}$ to decide whether or not $[W]_{\mathcal{P}'} = [W']_{\mathcal{P}'}$.

If $W$, $W'$ are words on $\mathbf{x} \cup y$, then we convert $W$, $W'$ to words on $\mathbf{x}$ only, by replacing $y$ with $Z$. Then use the same algorithm used on $\mathcal{P}$. Hence $\mathcal{P}'$ has a solvable word problem.

**General case** Suppose there is a sequence $\mathcal{P} = \mathcal{P}_0, \mathcal{P}_1, \mathcal{P}_2, \cdots \mathcal{P}_n = \mathcal{P}'$ $(n \geq 0)$, where $\mathcal{P}_{i+1}$ is obtained from $\mathcal{P}_i$ $(i = 0, 1, 2, \cdots, n-1)$ by an elementary Tietze transformation. If $\mathcal{P}_i$ has a solvable word problem by special cases $\mathcal{P}_{i+1}$ has a solvable word problem. Hence if $\mathcal{P}$ has a solvable word problem, then by transitivity $P'$ has a solvable word problem.$\square$

The above theorem shows that the concept of having solvable word problem depends only on the monoid and not on a (finite) presentation of it. We may therefore talk about a monoid with solvable word problem. A monoid $M$ is said to have a *decidable* or a *solvable* word problem if $M$ has a presentation with decidable word problem.

## 4.2 Word problem for groups

A *group presentation*

$$\mathcal{P} = <\mathbf{x}; \mathbf{r}>$$

is a pair, where $\mathbf{x}$ is a set, and $\mathbf{r}$ is a set of words in $\mathbf{x} \cup \mathbf{x}^{-1}$ (where $\mathbf{x}^{-1}$ is a set disjoint from $\mathbf{x}$ in $1:1$ correspondence $x \leftrightarrow x^{-1}$). We say $\mathcal{P}$ is finite if both $\mathbf{x}$ and $\mathbf{r}$ are finite. The elements of $\mathbf{x}$ are called (group) *generators*, and those of $\mathbf{r}$ *defining relators*. Note that we will use angular brackets $< \cdots >$ for group presentations, and square brakets $[\cdots]$ for monoid presentations.

We define elementary transformations as follows:

$(i)$ If $W$ is a word on $\mathbf{x} \cup \mathbf{x}^{-1}$, such that $W$ contains a subword $R \in \mathbf{r}$, then delete that occurrence of $R$.

$(ii)$ If $W$ contains a subword $x^{\varepsilon}x^{-\varepsilon}$ $(x \in \mathbf{x},\ \varepsilon = \pm 1)$ then delete that occurrence of $x^{\varepsilon}x^{-\varepsilon}$.

We remark that we also allow the inverses of the above elementary transformations. We say a word $W'$ is *equivalent* to a word $W$, if $W'$ can be obtained from $W$ by applying a finite number of elementary transformations $(i)$, $(ii)$, and their inverses, and we denote it by $W \sim_{\mathcal{P}} W'$. It can be easily shown that the relation $\sim_{\mathcal{P}}$ is an equivalence relation.

For every group presentation

$$\mathcal{P} = < \mathbf{x}; \mathbf{r} >$$

there is an associated monoid presentation

$$\hat{\mathcal{P}} = [\mathbf{x}, \mathbf{x}^{-1}; x^{\varepsilon}x^{-\varepsilon} = \epsilon \ (x \in \mathbf{x}, \varepsilon = \pm 1), \ R = \epsilon \ (R \in \mathbf{r})].$$

**Lemma 4.2.1** *$W \sim_{\mathcal{P}} W'$ if and only if $W \leftrightarrow^*_{\hat{\mathcal{P}}} W'$.*

**Proof** We observe that $W'$ is obtained from $W$ by an elementary transformations $(i)$ or $(ii)$, if and only if $W \to_{\hat{\mathcal{P}}} W'$. Suppose $W \sim_{\mathcal{P}} W'$. Then there exists a finite sequence

$$W = W_0, W_1, W_2, W_3, \cdots, W_{n-1}, W_n = W' \ (n \geq 0)$$

such that one of $W_i$, $W_{i+1}$ $(i = 0, 1, 2, \cdots, n-1)$ is obtained from the other by an elementary transformations $(i)$ or $(ii)$. Then by the above observation,

$$W_i \leftrightarrow^*_{\hat{\mathcal{P}}} W_{i+1} \ (i = 0, 1, 2, \cdots, n-1).$$

Hence by transitivity

$$W \leftrightarrow^*_{\hat{\mathcal{P}}} W'.$$

Conversely, suppose $W \leftrightarrow^*_{\hat{\mathcal{P}}} W'$. Then there exists a finite sequence

$$W = W_0, W_1, W_2, W_3, \cdots, W_{m-1}, W_m = W' \ (m \geq 0)$$

such that $W_i \to_{\hat{\mathcal{P}}} W_{i+1}$ or $W_{i+1} \to_{\hat{\mathcal{P}}} W_i$ $(i = 0, 1, 2, \cdots, m-1)$. Then by the above observation,

$$W_i \sim_{\mathcal{P}} W_{i+1} \ (i = 0, 1, 2, \cdots, m-1).$$

Hence by transitivity

$$W \sim_{\mathcal{P}} W'. \square$$

We define $G(\mathcal{P})$ to be $M(\hat{\mathcal{P}})$.

**Lemma 4.2.2** *$G(\mathcal{P})$ is a group.*

**Proof** By Theorem 2.2.2, $M(\hat{\mathcal{P}})$ is a monoid. Hence $G(\mathcal{P})$ is a monoid. We will show that for any $[W] \in G(\mathcal{P})$ then there exists $[W'] \in G(\mathcal{P})$ such that

$$[W][W'] = [W'][W] = [\epsilon].$$

If $W = \epsilon$, then there is nothing to prove. Otherwise let

$$W = x_1 x_2 x_3 \cdots x_n \ (n \geq 1, x_1, x_2, \cdots, x_n \in \mathbf{x} \cup \mathbf{x}^{-1})$$

be a word on $\mathbf{x} \cup \mathbf{x}^{-1}$. Then

$$W' = x_1^{-1} x_{n-1}^{-1} \cdots x_3^{-1} x_2^{-1} x_1^{-1}$$

is also a word on $\mathbf{x} \cup \mathbf{x}^{-1}$. And, by the argument similar to that in Lemma 3.1.1,

$$[W][W'] = [W'][W] = [\epsilon] = 1.$$

Thus $G(\mathcal{P})$ is a group, since it is a monoid and every element in $G(\mathcal{P})$ has an inverse.□

We say $\mathcal{P}$ has a *solvable word problem* if and only if $\hat{\mathcal{P}}$ does. Thus by Theorem 4.1.1, we observe that if $\mathcal{P}_1$, $\mathcal{P}_2$ are two group presentations which define isomorphic groups, and if one has a solvable word problem then so does the other.

**Lemma 4.2.3** *$\mathcal{P}$ has solvable word problem if and only if there is an algorithm to decide for any word $W$ on $\mathbf{x} \cup \mathbf{x}^{-1}$ whether or not $W \sim_{\mathcal{P}} \epsilon$.*

**Proof** Suppose $\mathcal{P}$ has solvable word problem. Thus in particular there is an algorithm to decide for any word $W$ on $\mathbf{x} \cup \mathbf{x}^{-1}$ whether or not $W \sim_{\mathcal{P}} \epsilon$. Conversely, suppose there is an algorithm to decide for any word $W$ on $\mathbf{x} \cup \mathbf{x}^{-1}$ whether or not $W \sim_{\mathcal{P}} \epsilon$. Let $U, V$ be any abitrary words on $\mathbf{x} \cup \mathbf{x}^{-1}$. We let $W = UV^{-1}$, then apply the avalaible algorithm on $W$. If $W \sim_{\mathcal{P}} \epsilon$, then $U \sim_{\mathcal{P}} V$. Otherwise $U$ is not equivalent to $V$. Thus $\mathcal{P}$ has solvable word problem.□

## 4.3 Some solvability and unsolvability results

**Theorem 4.3.1** *If*

$$\mathcal{P} = [\mathbf{x};\mathbf{r}]$$

*is a complete rewriting system, then $\mathcal{P}$ has a solvable word problem.*

**Proof** Let $W, W'$ be words on $\mathbf{x}$. Since $\mathcal{P}$ is complete, by Theoreom 2.3.1, each equivalence class contains a unique irreducible. We apply a finite number of positive elementary transformations on $W$ to obtain the unique irreducible $Irr(W)$ of the equivalence class containing $W$. Similarly we apply a finite number of positive elementary transformations on $W'$ to obtain the unique irreducible $Irr(W')$ of the equivalence class containing $W'$. Then the word problem is solved in this way, if $Irr(W) = Irr(W')$, then $[W]_{\mathcal{P}} = [W']_{\mathcal{P}}$. Otherwise $[W]_{\mathcal{P}} \neq [W']_{\mathcal{P}}$.□

The question of whether a monoid with soluble word problem must have a finite complete rewriting system, had been answered by C. Squier [61]. He provided an example of a monoid (even a group) that is not $FP_3$, but has a solvable word problem. Hence by Theorem 2.4.1, the example answers (in the negative) the question.

Generally speaking, the word problem for finitely presented monoids is undecidable, (see [41], [42], [53]). In [39] Matjasevitch even gives a presentation with two generators and three relations whose word problem is undecidable.

There are groups with unsolvable word problem (see [11], [12], [49]). The example in [12] is particularly noteworthy since it is the free product with amalgamations of groups with solvable word problems. (See also W. Magnus, A Karrass and D. Solitar [44], J. J. Rotman [59].)

The word problem for monoids which have a monoid presentation with a single relation is suspected to be decidable, though it is still open. The word problem for groups which have a group presentation with a single relator was shown to be decidable in [37]. Using this result, Adjan [1] proved the decidability of the word problem for the so-called *special* monoid presentations, that is presentations of the form

$$\mathcal{P} = [\mathrm{x}; R = \epsilon].$$

He also proved the decidability of the problem for presentations of the form

$$\mathcal{P} = [\mathrm{x}; R = S]$$

where $R$ and $S$ have different initial letters and different terminal letters. In [64] it is shown that the word problem is decidable for presentations of the form

$$\mathcal{P} = [a, b; b^m a^n = aUa],\ U \in \{a, b\}^*,\ m, n > 0.$$

In [2] first, then in [3], it was shown that the word problem for any presentation can be reduced to the word problem for a presentation

$$\mathcal{P} = [\mathrm{x}; R = S]$$

where $R$ and $S$ have different initial letters. In [3] it is also shown that for any presentation of the form

$$\mathcal{P} = [\mathrm{x}; R = S]$$

where $S$ is an unbordered word which is a factor of $R$, the word problem is decidable.

Although one-relator groups have a solvable word problem and are of type $FP_\infty$ [36], it is still an open question whether they have complete rewriting systems. Some examples of one -relator groups with complete rewriting systems are known.

Below we will give some examples of one-relator groups with complete rewriting systems (for more examples we refer the reader to Philippe Le Chenadec [52], or Deko V. Dekov [18]).

**Example 4.3.1** (*The surface groups*) *The group with the presentation*

$$\mathcal{P}_m =< a_1, a_2, \cdots, a_{2m}; a_1 a_2 \cdots a_{2m} a_1^{-1} a_2^{-1} \cdots a_{2m}^{-1} >$$

*is shown to have a finite complete rewriting system in* [52]. *The finite complete rewriting system for the group* $G(\mathcal{P}_m)$ *is*

$$\hat{\mathcal{P}_m} = [a_1, a_2, \cdots, a_{2m}, a_1^{-1}, a_2^{-1}, \cdots, a_{2m}^{-1}; \mathbf{r}]$$

*where* $\mathbf{r}$ *is the following set of defining relations*

$$a_{2k} \cdots a_{2m} a_1^{-1} \cdots a_{2k-1}^{-1} = a_{2k-1}^{-1} \cdots a_1^{-1} a_{2m} \cdots a_{2k};$$

$$a_{2k} \cdots a_1 a_{2m}^{-1} \cdots a_{2k+1}^{-1} = a_{2k+1}^{-1} \cdots a_{2m}^{-1} a_1 \cdots a_{2k};$$

$$a_{2k}^{-1} \cdots a_1^{-1} a_{2m} \cdots a_{2k+1} = a_{2k+1} \cdots a_{2m} a_1^{-1} \cdots a_{2k}^{-1};$$

$$a_{2k}^{-1} \cdots a_{2m}^{-1} a_1 \cdots a_{2k-1} = a_{2k-1} \cdots a_1 a_{2m}^{-1} \cdots a_{2k}^{-1},$$

$(k = 1, 2, \cdots, m)$. See [52] *for more details.*

**Example 4.3.2** (*The Greendlinger group*) *In* 1984, *F. Otto* [51], *gave a finite complete rewriting system for the group with presentation*

$$\mathcal{P} =< a, b, c; abc = cba > .$$

*The finite complete rewriting system for* $G(\mathcal{P})$ *is*

$$\hat{\mathcal{P}} = [a, b, c, a^{-1}, b^{-1} c^{-1}; a^{\varepsilon} a^{-\varepsilon} = \epsilon, b^{\varepsilon} b^{-\varepsilon} = \epsilon, c^{\varepsilon} c^{-\varepsilon} = \epsilon \ (\varepsilon = \pm 1),$$

$$ac^{-1} = b^{-1} c^{-1} ab, a^{-1} b^{-1} = c^{-1} b^{-1} a^{-1} c, abc = cba, a^{-1} cb = bca^{-1}].$$

*In* 1986, *Ph. Le Chenadec gave another finite complete rewriting system for the Greendlinger group* $G(\mathcal{P})$ *(see* [18], [51], [52] *for more details).*

**Example 4.3.3** *The group with the presentation*

$$\mathcal{P} =< a, b; aba = bab >$$

*has a finite complete rewriting system. The finite complete rewriting system for* $G(\mathcal{P})$ *is*

$$\hat{\mathcal{P}} = [a, b, c, a^{-1}, b^{-1}, c^{-1}; a^{-1} = c^{-1}a^2, b^{-1} = c^{-1}b, c^{\varepsilon}c^{-\varepsilon} = \epsilon \ (\varepsilon = \pm 1),$$
$$a^3 = c, b^2 = c, ac = ca, ac^{-1} = c^{-1}a, bc = cb, bc^{-1} = c^{-1}b].$$

*(For more details see* [56].)

**Example 4.3.4** *In* 1997 *Dekov* [18], *using the method of Pedersen and Yonder* [56] *gave a finite complete rewriting system for the group with presentation*

$$\mathcal{P} =< a, b; a^n = b^m >,$$

*where* $m, n > 1$. *The finite complete rewriting system for* $G(\mathcal{P})$ *is*

$$\hat{\mathcal{P}} = [a, b, c, a^{-1}, b^{-1}, c^{-1}; c^{\varepsilon}c^{-\varepsilon} = \epsilon \ (\varepsilon = \pm 1), \ a^{-1} = c^{-1}a^{n-1}, b^{-1} = c^{-1}b^{m-1}, a^n =$$
$$c, b^m = c, ac = ca, ac^{-1} = c^{-1}a, bc = cb, bc^{-1} = c^{-1}b].$$

*(For more details see* [18].)

**Theorem 4.3.2** *Finitely generated linear groups have solvable word problem.*

For finitely generated groups which are linear over a field, this result is proved in Rabin [57] but also follows from an older result of Malcev [40].

The following classes of groups also have solvable word problem (we will refer the reader to [10] for more examples).

$(i)$ *Automatic* group. For the definition and examples of automatic group, we refer the reader to [20];

$(ii)$ Finitely presented residually finite groups. This will be shown in Section 4.5.

## 4.4 Residual finiteness

Let $\mathfrak{X}$ be a property of monoids. A monoid $M$ is *residually-*$\mathfrak{X}$ if given any two distinct elements $m_1, m_2$ of $M$, there exists a homomorphism $\psi_{m_1,m_2}$ (depending on $m_1$ and $m_2$) of $M$ onto a monoid $K$ with property $\mathfrak{X}$ such that

$$\psi(m_1) \neq \psi(m_2).$$

Thus we say a monoid $M$ is *residually-finite* if given two distinct elements $m_1, m_2 \in M$ there exists a finite monoid $K$ and a homomorphism $\psi_{m_1,m_2}$ (depending on $m_1$ and $m_2$) of $M$ onto $K$ such that

$$\psi_{m_1,m_2}(m_1) \neq \psi_{m_1,m_2}(m_2).$$

A monoid $M$ is said to be *n-residually-*$\mathfrak{X}$ ($n \in \mathbb{Z}^+$) if given any finite subset $S$ of $M$ with $|S| \leq n$, then there exists a homomorphism $\psi$ (depending on the subset $S$) of $M$ onto a monoid $K$ (with property $\mathfrak{X}$), such that $\psi$ is injective on $S$. We say $M$ is *fully residually-*$\mathfrak{X}$ if $M$ is *n-residually-*$\mathfrak{X}$ for any $n \in \mathbb{Z}^+$.

**Remark:** *If $M$ is fully residually-$\mathfrak{X}$ then $M$ is residually-$\mathfrak{X}$.*

**Lemma 4.4.1** *Suppose $\mathbb{X}$ and $\mathbb{Y}$ are the collection of monoids with properties $\mathfrak{X}$ and $\mathfrak{Y}$ respectively. Suppose each monoid of $\mathbb{X}$ is residually-$\mathfrak{Y}$. Then if a monoid $M$ is residually-$\mathfrak{X}$, then $M$ is residually-$\mathfrak{Y}$.*

**Proof** Suppose a monoid $M$ is residually-$\mathfrak{X}$, then it implies that for every two distinct elements $m_1, m_2 \in M$, we can find a homomorphism $\psi_{m_1,m_2}$ of $M$ onto a monoid $K$ in $\mathbb{X}$ such that

$$\psi_{m_1,m_2}(m_1) \neq \psi_{m_1,m_2}(m_2).$$

Since $K$ is residually-$\mathfrak{Y}$ there exists a homomorphism $\phi_{\psi_{m_1,m_2}(m_1),\psi_{m_1,m_2}(m_2)}$ of $K$ onto a monoid $T$ of $\mathbb{Y}$, such that

$$\phi_{\psi_{m_1,m_2}(m_1),\psi_{m_1,m_2}(m_2)}(\psi_{m_1,m_2}(m_1)) \neq \phi_{\psi_{m_1,m_2}(m_1),\psi_{m_1,m_2}(m_2)}(\psi_{m_1,m_2}(m_2)).$$

Thus the composition $\phi\psi$ is a homomorphism of $M$ onto $T$ such that

$$\phi\psi(m_1) \neq \phi\psi(m_2).$$

Hence $M$ is residually-$\mathfrak{Y}$.□

**Lemma 4.4.2** *Suppose every submonoid of an $\mathfrak{X}$-monoid is an $\mathfrak{X}$-monoid. Then every submonoid of a residually $\mathfrak{X}$-monoid is a residually $\mathfrak{X}$-monoid.*

**Proof** Let $M$ be a residually $\mathfrak{X}$-monoid and $S$ be a submonoid of $M$. We choose two distinct elements $s, s'$ of $S$. Since $M$ is residually-$\mathfrak{X}$ there exists a homomorphism $\psi_{s,s'}$ (depending on $s, s'$) of $M$ into an $\mathfrak{X}$-monoid $M'$ such that

$$\psi_{s,s'}(s) \neq \psi_{s,s'}(s').$$

The map $\psi_{s,s'}|_S$, restriction on $S$ is a homomorphism of $S$ onto $Im(\psi_{s,s'}|_S)$, a submonoid of $M'$ such that

$$\psi_{s,s'}|_S(s) \neq \psi_{s,s'}|_S(s').$$

Hence $S$ is residually-$\mathfrak{X}$ since the monoid $Im(\psi_{s,s'}|_S)$ is an $\mathfrak{X}$−monoid.□

**Lemma 4.4.3** *$M$ is residually-$\mathfrak{X}$ if and only there is an embedding*

$$\psi : M \longrightarrow \prod_{j \in J} Y_j$$

*of $M$ into a cartesian product of monoids $Y_j$ ($j \in J$) with property $\mathfrak{X}$ such that $\pi_i \psi$ is surjective for all $i, j \in J$* (here

$$\pi_i : \prod_{j \in J} Y_j \longrightarrow Y_i$$

*is the projection onto $Y_i$.)*

**Proof** Suppose $M$ is residually-$\mathfrak{X}$. List all pairs of elements of $M$. Since $M$ is residually-$\mathfrak{X}$, then for each pair $p = \{m_1, m_2\}$, ($m_1, m_2$ distinct elements of $M$) we have an epimorphism

$$\phi_p : M \longrightarrow X_p \ (X_p \text{ is an } \mathfrak{X}\text{-monoid})$$

such that

$$\phi_p(m_1) \neq \phi_p(m_2).$$

Let

$$X = \prod_p X_p$$

be the cartesian product of the $X_p's$. The mapping

$$\phi : M \longrightarrow X$$

$$\phi(m) = (\cdots, \phi_p(m), \cdots)\ (m \in M).$$

is a homomorphism since the $\phi_p's$ are homomorphisms, and clearly $\pi_p\phi$ is surjective for all $p$. Also $\phi$ is injective since for any distinct elements $m_1, m_2$ of M, we consider the pair $q = \{m_1, m_2\}$. Then

$$\phi(m_1) = (\cdots, \phi_q(m_1), \cdots) \text{ and } \phi(m_2) = (\cdots, \phi_q(m_2), \cdots).$$

Then $\phi(m_1)$ and $\phi(m_2)$ differ in the $q^{th}$ coordinate since

$$\phi_q(m_1) \neq \phi_q(m_2),$$

so

$$\phi(m_1) \neq \phi(m_2).$$

Conversely, suppose we have an injective homomorphism

$$\psi : M \longrightarrow \prod_{j \in J} Y_j = Y$$

such that

$$\pi_i \psi : M \longrightarrow Y_i$$

is surjective for all $i \in J$. Let $m_1, m_2$ be distinct elements of $M$. Since $\psi$ is injective,

$$\psi(m_1) \neq \psi(m_2).$$

Thus there must exist a $j$ such that the $j^{th}$ coordinate of $\psi(m_1)$ is different from the $j^{th}$ coordinate of $\psi(m_2)$. Thus

$$\pi_j\psi(m_1) \neq \pi_j\psi(m_2),$$

so $\pi_j\psi$ is a homomorphism from $M$ onto $Y_j$, such that

$$\pi_j\psi(m_1) \neq \pi_j\psi(m_2).$$

Hence $M$ is residually-$\mathfrak{X}$.$\square$

**Lemma 4.4.4** *A monoid is residually finite if and only if it is fully residually finite.*

**Proof** If $M$ is fully residually finite, then $M$ is residually finite. Conversely assume $M$ is residually finite. Let

$$S = \{m_1, m_2, \cdots, m_n\}$$

be a subset of the monoid $M$. Since $M$ is residually finite, for every distinct elements $m_i, m_j$ $(1 \leq i < j \leq n)$ of $S$ there exists a homomorphism

$$\psi_{i,j} : S \longrightarrow X_{i,j}$$

where $X_{i,j}$ is a finite monoid, such that

$$\psi_{i,j}(m_i) \neq \psi_{i,j}(m_j).$$

Let $X$ be the direct product $\prod_{1 \leq i < j \leq n} X_{i,j}$. Then $X$ is finite. The mapping

$$\psi : M \longrightarrow X$$

$$\psi(m) = (\psi_{1,2}(m), \psi_{1,3}(m), \cdots \psi_{n-1,n}(m)) \ (m \in M)$$

is a homomorphism, since the $\psi_{i,j}'s$ are homomorphisms. For any distinct $m_i, m_j \in S$ $(1 \leq i < j \leq n)$ then

$$\psi_{i,j}(m_i) \neq \psi_{i,j}(m_j).$$

Hence $\psi(m_i) \neq \psi(m_j)$. Thus $\psi$ is injective on $S$. Hence $M$ is fully residually finite.□

**Lemma 4.4.5** *Every free monoid* $\mathbf{x}^*$ *is residually finite.*

**Proof** Let $\mathbf{x}^*$ be a free monoid on $\mathbf{x}$. Let $W, W'$ be distinct words on $\mathbf{x}$.

**Case 1** Suppose $W'$ is the initial subword of $W$. So $W = W'aV$ $(a \in \mathbf{x}, V \in \mathbf{x}^*)$. Let $n = L(W')$. Let $\mathfrak{T}(\mathbf{y})$ be the full transformation monoid on the set

$$\mathbf{y} = \{0, 1, 2, 3, \cdots, n, *\}.$$

By Theorem 1.4.1, the mapping

$$\psi_{W,W'} : \mathbf{x} \longrightarrow \mathfrak{T}(\mathbf{y})$$

$$x \mapsto \begin{bmatrix} 0 & 1 & 2 & \cdots & n-1 & n & * \\ 1 & 2 & 3 & \cdots & n & * & * \end{bmatrix} = \tau_x \ (x \in \mathbf{x})$$

induces a homomorphism $\psi_{(W,W')*}$ from $\mathbf{x}^*$ into $\mathfrak{T}(\mathbf{y})$. For any word $U = x_1x_2\cdots x_m$ $(m \geq 1, x_i \in \mathbf{x}, i = 1, 2, \cdots, m)$ on $\mathbf{x}$ then $\tau_U$ is the composition $\tau_{x_1}\tau_{x_2}\cdots\tau_{x_m}$. We observe that

$$0\tau_W = n\tau_a\tau_V = *\tau_V = *$$

$$0\tau_{W'} = n.$$

Hence $\psi_{(W,W')*}(W) \neq \psi_{(W,W')*}(W')$.

**Case 2** Suppose $W'$ is not the initial subword of $W$. So $W = UaV$ and $W' = UbV'$, where $a, b$ are distinct elements of $\mathbf{x}$, and $U, V, V'$ are words on $\mathbf{x}$. Let $n = L(U)$. Let $\mathfrak{T}(\mathbf{y})$ be the full transformation monoid on the set

$$\mathbf{y} = \{0, 1, 2, \cdots, n, *, +\}.$$

By Theorem 1.4.1, the mapping

$$\psi_{W,W'} : \mathbf{x} \longrightarrow \mathfrak{T}(\mathbf{y})$$

$$a \mapsto \begin{bmatrix} 0 & 1 & 2 & \cdots & n-1 & n & * & + \\ 1 & 2 & 3 & \cdots & n & * & * & + \end{bmatrix} = \tau_a$$

$$x \mapsto \begin{bmatrix} 0 & 1 & 2 & \cdots & n-1 & n & * & + \\ 1 & 2 & 3 & \cdots & n & + & * & + \end{bmatrix} = \tau_x \ (x \neq a \in \mathbf{x}),$$

induces a homomorphism $\psi_{(W,W')*}$ from $\mathbf{x}^*$ into $\mathfrak{T}(\mathbf{y})$. And

$$0\tau_W = n\tau_a\tau_V = *\tau_V = *$$

$$0\tau_{W'} = n\tau_b\tau_{V'} = +\tau_{V'} = +.$$

Hence $\psi_{(W,W')*}(W) \neq \psi_{(W,W')*}(W')$. Thus $\mathbf{x}^*$ is residually finite.□

**Lemma 4.4.6** *A group $G$ is residually-$\mathfrak{X}$ if and only if for any element $g \neq 1_G$ of $G$, there exists a homomorphism $\psi_g$ of $G$ onto an $\mathfrak{X}$-group such that $\psi_g(g) \neq 1$.*

**Proof** Suppose $G$ is residually-$\mathfrak{X}$. In particular, for any $g \neq 1_G$ there exists a homomorphism $\psi_{g,1_G} = \psi_g$ of $G$ onto a $\mathfrak{X}$-group $H$ such that

$$\psi_{g,1_G}(g) \neq \psi_{g,1_G}(1_G) = 1_H.$$

Now suppose that for any $g \neq 1_G$ there exists a homomorphism $\psi_{g,1_G}$ of $G$ onto an $\mathfrak{X}$-group, such that $\psi_{g,1_G}(g) \neq \psi_{g,1_G}(1_G)$. Let $g_1, g_2$ be any abitrary distinct elements of $G$. We let $g = g_1 g_2^{-1}$. By the assumption there exists $\psi_g = \psi_{g_1 g_2^{-1}}$ a homomorphism of $G$ onto an $\mathfrak{X}$-group such that

$$\psi_g(g_1 g_2^{-1}) \neq \psi_g(1_G).$$

Thus

$$\psi_g(g_1) \neq \psi_g(g_2)$$

Hence $\psi_g$ is a homomorphism of $G$ onto an $\mathfrak{X}$-group such that

$$\psi_g(g_1) \neq \psi_g(g_2).$$

Thus $G$ is residually-$\mathfrak{X}$.□

Theorem 4.4.6 is normally used as a definition for residual finiteness in groups (see [26], [35] and [44]). For the residual properties of groups we refer the reader to G. Baumslag [7], [6] and [8], D. L. Johnson [26], K. W. Gruenberg [22], Lyndon and P. E. Schupp [35], W. Magnus, A Karrass and D. Solitar [44].

**Example 4.4.1** *Free groups are residually finite* (see [34]).

**Example 4.4.2** *Finitely generated abelian groups are residually finite (see [6]).*

**Example 4.4.3** *Every polycyclic group is residually finite (see [44]).*

**Example 4.4.4** *The automorphism group of a finitely generated residually finite group is again residually finite (see [7]).*

**Example 4.4.5** *A direct product of a family of residually finite groups, is residually finite* (*see* [59], [44]).

**Example 4.4.6** *Baumslag* [9] *has shown that if $A$ and $B$ are nilpotent and finitely generated groups, then the free product of $A$ and $B$ amalgamating a cyclic subgroup $H$ is residually finite.*

**Example 4.4.7** *A finite extension of a residually finite group is residually finite* (*see* [6]).

**Example 4.4.8** *A cyclic extension of a finitely generated residually finite group is residually finite* (*see* [6]).

## 4.5 Residual finiteness and the word problem

**Theorem 4.5.1** *A finitely presented residually finite monoid has a solvable word problem.*

We remark that the proof of these theorem can also be found in [10] and [35]

**Proof** Let

$$\mathcal{P} = [\mathbf{x};\mathbf{r}]$$

be a finite presentation for a residually finite monoid $M(\mathcal{P})$. To decide whether any arbitrary words $W, W'$ defines the same element or not, in $M(\mathcal{P})$, we effectively enumerate two lists:

**List 1** This list consist of all homomorphisms of $M(\mathcal{P})$ into finite monoids. Since by Theorem 1.2.2, every finite monoid is isomorphic to a submonoid of a full transformation monoid $\mathfrak{T}_n$ for some $n \in \mathbb{Z}^+$, it is enough to find all homomorphisms from $M(\mathcal{P})$ into $\mathfrak{T}_n$ for each $n$. For any function

$$\eta : \mathbf{x} \longrightarrow \mathfrak{T}_n \ (n \in \mathbb{Z}^+)$$

one can effectively check whether $\eta$ induces a homomorphism $\eta_{\mathcal{P}}$ of $M(\mathcal{P})$ into $\mathfrak{T}_n$, by checking if for any $R_{+1} = R_{-1} \in \mathbf{r}$, $\eta(R_{+1}) = \eta(R_{-1})$. If it holds, then by Theorem 1.6.2, $\eta$ induces a homomorphism $\eta_{\mathcal{P}}$ of $M(\mathcal{P})$ into $\mathfrak{T}_n$, otherwise $\eta$ does not induce a homomorphism of $M(\mathcal{P})$ into $\mathfrak{T}_n$. Thus for each $n \in \mathbb{Z}^+$ we can enumerate all mappings $\eta$ which induce homomorphisms of $M(\mathcal{P})$ into $\mathfrak{T}_n$. We let $K_n$ $(n \in \mathbb{Z}^+)$ be the set of all such mappings.

**List 2** For any word $W$ of length $n$ $(n \in \mathbb{Z}^+)$, apply $\leq n$ elementary transformations on the word $W$, to obtain a chain

$$W = W_0, W_1, W_2, \cdots, W_m \ (m \leq n),$$

where $W_{i+1}$ is obtained from $W_i$ $(i = 0, 1, 2, \cdots, m-1)$ by an elementary transformation. Thus for each word $W$ of length $n$ $(n \in \mathbb{Z}^+)$ we can enumerate all chains

$$W = W_0, W_1, W_2, \cdots, W_m \ (m \leq n),$$

where $W_{i+1}$ is obtained from $W_i$ $(i = 0, 1, 2, \cdots, m-1)$ by an elementary transformation. For all words $W$ of length $n \in \mathbb{Z}^+$, we let $S_n$ be the set of all the constructed chains. We observe that if two words $W$, $W'$ are chosen, such that $[W]_{\mathcal{P}} = [W']_{\mathcal{P}}$, then there must exist $S_n$ $(n \in \mathbb{Z}^+)$ with a chain such that both $W$ and $W'$ are in that chain.

Then the word problem is solved in the following way:

Take two distinct words $W$, $W'$. We compute $\eta(W), \eta(W')$ for every $\eta \in K_1$. If there exist $\eta \in K_1$ such that $\eta(W) \neq \eta(W')$, then $[W]_{\mathcal{P}} \neq [W']_{\mathcal{P}}$, else we go to $S_1$ and check if there is a chain in $S_1$ such that both $W$ and $W'$ are in that chain. If there is such a chain, then $[W]_{\mathcal{P}} = [W']_{\mathcal{P}}$, otherwise we go to $K_2$ and check if there is an $\eta$ from $K_2$ such that $\eta(W) \neq \eta(W')$. If there is such an $\eta$, then $[W]_{\mathcal{P}} \neq [W']_{\mathcal{P}}$, otherwise we go to $S_2$ and check if there is a chain from $S_2$ with both $W$ and $W'$ in that chain. If there is such a chain, then $[W]_{\mathcal{P}} = [W']_{\mathcal{P}}$, else we go to $K_3$. We continue the process in that manner. And in this way we can solve the word problem. Since if $[W]_{\mathcal{P}} \neq [W']_{\mathcal{P}}$, then there must be a $K_i$ ($i \in \mathbb{Z}^+$) with $\eta$, such that $\eta(W) \neq \eta(W')$, since $M(\mathcal{P})$ is residually finite. And if $[W]_{\mathcal{P}} = [W']_{\mathcal{P}}$, then there must exist an $S_n$ ($n \in \mathbb{Z}^+$) with a chain such that both $W$ and $W'$ are in that chain. Thus in that manner, the word problem can be solved.□

# Bibliography


[1] S.I. Adjan, *Defining relations and algorithmics problems for groups and semigroups*, Trudy Math. Inst. Steklov, Akad. Nauk SSSR, **85** (1966) 1-124.

[2] S.I. Adjan and G.U. Oganesjan, *On the problem of equality and divisibility in semigroups with one defining relation*, Izv. Akad. Nauk SSSR, Ser. Math, **42** 2 (1978) 219-225 (Russian).

[3] S.I. Adjan and G.U. Oganesjan, *Problems of equality and divisibility in semigroups with one defining relation*, Matem. Zametki, **41** (1987) 412-421 (Russian).

[4] D.J. Anick, *On the cohomology of the associative algebras*, Trans. Amer. Math. Soc. **296** (1986) 641-649.

[5] E. Artin, *The free product of groups*,Amer. J. Math, **69** (1947) 1-4.

[6] G. Baumslag, *Topics in Combinatorial Group Theory, Birkhäuser Verlag, 1993.*

[7] G. Baumslag, *Automorphism groups of residually finite groups*, J. London Math. Soc, **38**, (1963), 117-118.

[8] G. Baumslag, *On the residual finiteness of the generalised free products of nilpotent groups*, Trans. Amer. Math. Soc, **106**, (1963), 193-209.

[9] G. Baumslag, *Wreath products and extensions*, Math. Z, **81**, (1963), 286-299.

[10] G. Baumslag and C. F. Miller *III*, *Algorithms and classifications in combinatorial group theory*, Mathematical Sciences Research Institute Pubications, no 23, Springer-Verlag, 1992.

[11] W.W. Boone, *Certain simple unsolvable problems of group theory*, Indig. Math, **16**, (1955), 231-237.

[12] J.L. Britton, *The word problem for groups*, Proc. London Math Soc, **8**, No 32 (3rd Series), (1958), 493-506.

[13] Kenneth S. Brown, *The geometry of rewriting systems: a proof of the Anick-Groves-Squier theorem*, in: G. Baumslag and C.F Miller, eds. Algorithms and Classification in Combinatorial Group Theory MSRI publications, **23**, (Springer, New York, 1992) 137-164.

[14] D.E. Cohen, *Combinatorial group theory: a topological approach*, London Mathematical Society Student Texts, **14**, Cambridge University, 1989.

[15] D. Cohen, *A monoid which is right $FP_\infty$ but not $FP_1$*, Bull. London Math. Soc. **24** (1992) 340-342.

[16] Deko V. Dekov, *Free products with amalgamation of monoids*, Journal of Pure and Applied Algebra, **125**(1988) 129-133.

[17] Deko V. Dekov, *Rewriting systems for HNN extension of groups*, preprint.

[18] Deko V. Dekov, *Finite complete rewriting systems for groups*, Communications in Algebra, **25(12)**, (1997) 4023-4028.

[19] Deko V. Dekov, *Finite complete rewriting systems for semigroups*, preprint.

[20] D. B. A. Epstein, *Word processing in groups,* Jones and Bartlett Publishers, 1992.

[21] V.S Guba and S.J Pride, *Low-dimensional (co)homology of free Burnside monoids*, Journal of Pure and Applied Algebra, **108** (1996) 61-79.

[22] K. W. Gruenberg, *Residual properties of infinite soluble groups*, Proc. London Math. Soc, (3), **7**, (1957), 29-62.

[23] M. Hall, *Subgroups of free products*, Pacific J. Math, **3**, (1953) 115-120.

[24] D. Hofbauer and C. Lautemann, *Termination proofs and the length of derivations*, N. Dershowitz Edition, Rewriting Techniques and Applications, Lecture Notes in Computer Science, **355** (Springer-Verlag, Berlin, 1989) 167-177.

[25] M. Hall, jr, and T. Rado, *On Schreier systems in free groups,* Trans. Amer. Math. Soc. **64,** (1948), 386-408.

[26] D.L. Johnson, *Presentations of groups*, London Mathematical Society Texts, **15**, Cambridge University, 1990.

[27] R.D Hurwitz, *On the conjugancy problem in a free product with commuting subgroups,* Math. Ann, **221,** (1976), no 1, 1-8.

[28] R.D. Hurwitz, *On cyclic subgroups and the conjugancy problem,* Proc. Amer. Math. Soc, **79,** (1980), no 1, 1-8.

[29] Y. Kobayashi, *Complete rewriting system and cohomology of monoid algebras*, J. Pure Appl. Algebra, **65** (1990) 263-275.

[30] Y. Kobayashi, *A finitely presented monoid which has solvable word problem but has no regular complete presentation*, Theoretical Computer Science, **146** (1995) 321-329.

[31] A. Karass and D. Solitar, *On free products*, Proc. Amer. Math. Soc, **9**, (1958) 217-221.

[32] A.G. Kurosh, *The theory of groups*, **2** Chelsea, 1956.

[33] D.S. Lankford, *Some approaches to equality for computational logic: A survey and assessment*, Report ATP-36, Department of Mathematics and computer Science, University of Texas at Austin, (1977).

[34] F. Levi, *Über die Untergruppen der freien Gruppen*, Math. Z. **37**, (1933), 90-97.

[35] R.C. Lyndon and P.E. Schupp, *Combinatorial group theory*, Springer-Verlag, 1977.

[36] R.C. Lyndon, *Cohomology theory of groups with a single defining relation*, Ann. Math. **55**, (1950), 650-665.

[37] W. Magnus, *Identitäts-problem für Gruppen mit einer definierenden Relation*, Math. Ann, **106** (1932), 295-307.

[38] I.D. Macdonald, *The theory of groups*, Oxford, 1968.

[39] J. Matjasevitch, *Simple examples of unsolvable associative calculi*, Dokl. Akad. Nauk SSSR, **173** (1967) 1264-1266 (Russian).

[40] A. I. Malcev, *On isomorphic matrix representations of infinite groups,* Mat. Sb, **8**, (1940), 405-422.

[41] A.A. Markov, *On the imposssibility of certain algorithms in the theory of associative systems*, Dolk. Akad. Nauk SSSR, **55** (1947) 587-590 (Russian).

[42] A.A. Markov, *On the imposssibility of certain algorithms in the theory of associative systems*, Dolk. Akad. Nauk SSSR, **58** (1947) 353-356 (Russian).

[43] J. McCammond, *On the solution to the word problem for the relatively free semigroup satisfying* $T^a = T^{a+b}$ *with* $a \geq 6$, Internat. J. Algebra. Comput, **1** (1991) 1-32.

[44] W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory: presentations of groups in terms of generators and relations*, New York, 1966.

[45] C. F. Miller III and P. E. Schupp, *The geometry of Higmann-Neumann-Neumann extensions,* Comm. Pure Appl. Math, **26**, (1973), 787-802.

[46] H. Neumann, *Generalised free products with amalgamated subgroups*, Amer. J. Math, **70**, (1948), 590-625.

[47] H. Neumann, *Generalised free products with amalgamated subgroups*, Amer. J. Math, **71**, (1949) 491-540.

[48] M. H. A. Newman, *On theories with a combinatorial definition of "equivalence"* , Ann. of Math, **43**, (1942), 223-243.

[49] P. S. Novikov, *On the algorithmic unsolvability of the word problem in group theory*, Trudy Mat. Inst. im Steklov, **44** (1955), 143.

[50] F. Otto and Y. Koboyashi, *Properties of monoids that are presented by finite convergent string-rewriting systems-a survey*, preprint

[51] F. Otto, *Finite complete rewriting systems for the Jantzen monoid and the Greendlinger group*, Theoret. Comput. Sci, **32**, (1984), 249-260.

[52] Philippe Le Chenadec, *A catalogue of complete group presentations*, Journal of Symbolic Computation, **2** (1986) 363-381.

[53] E.L. Post, *Recursive unsolvability of a problem of Thue,* Journal of Symbolic Logic, **12** (1947) 1-11.

[54] ——— *Low-dimensional homotopy theory for monoids,* preprint, University of Glasgow, 1993.

[55] Stephen J. Pride, *Geometric methods in combinatorial semigroup theory,* J. Fountain(ed.), Semigroups, Formal Langusges and groups, (Kluwer academic, Dordrecht, 1995) 215-232.

[56] J. Pedersen and M. Yonder, *Term rewriting for the conjugacy problem of the braid groups*, J. symbolic computation, **18**, (1994), 563-572.

[57] M. O. Rabin, *Computable algebra, general theory and theory of computable fields,* Trans. Amer. Math. Inst. Steklov, **44**, (1960), 341-360.

[58] D.J.S. Robinson *Finiteness conditions and generalised soluble groups*,**Part 2** Springer-Verlag Berlin Heidelberg New York (1972).

[59] J.J. Rotman, *An introduction to the theory of groups*, **Third Edition,** 1934.

[60] O. Schreier, *Die Untergruppen der freien gruppen*, Abh. Math. Sem, Hamburgischen University, **5**, (1926), 161-183.

[61] C.C Squier, *Word problems and a homological finiteness condition for monoids*, Journal of Pure and Applied Algebra, **49** (1987) 201-217.

[62] M. Takahasi, *Bererkungen über denUntergruppensatz in freien produckten*, Proc. Acad. Tokyo, **20**, (1944) 589-594.

[63] X. Wang, *Second order dehn functions of finitely presented groups and monoids*, Ph.D thesis, University of Glasgow, 1996.

[64] G. Waiter, *Left-divisibility and word problems in single relation monoids*, Semigroup Forum, **53** (1996) 194-207.