Word problems on balanced semigroups and balanced groups

by

Dong Wook Won

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

2008

UMI Number: 3296964

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirements for the degree of Doctor of Philosophy.

Alexei Myasnikov

Date — Chair of Examining Committee

Józef Dodziuk

Date — Executive Officer

Alexei Myasnikov

Vladimir Shpilrain

Roman Kossak

Supervisory committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

Word problems on balanced semigroups and balanced groups

by

Dong Wook Won

Advisor: Professor Alexei Myasnikov

We study the word problems on a certain type of semigroups and groups, for which we know that there is no algorithm to solve the word problem. We find some common characteristics on those algebraic structures. Then we find a generic solution of the word problem on those structures including famous known examples of groups and semigroups where the word problem is undecidable.

Acknowledgments

First and foremost I would like to thank my advisor Prof. Alexei Myasnikov for his generous time, support, advice, and help throughout the doctoral study. His knowledge and passion for group theory as well as mathematics in general influenced me greatly and will certainly influence me more in the future.

I would like to thank supervisory committee members, Prof. Vladimir Shpilrain and Prof. Roman Kossak for their time and feedbacks on my dissertation.

I am grateful to faculty members of Mathematics Department who taught me mathematics during my study at the Graduate Center, especially Prof. Joel Hamkins and Prof. Roman Kossak.

I would like to thank the executive officer of Mathematics Department Prof. Józef Dodziuk for helping me on registrations and various occasions and Robert Landsman for his excellent service as assistant program officer.

I wish to thank all friends I met at the Graduate Center. I especially thank Alexander Ushakov for his many valuable suggestions and helps on this research.

I am very grateful to two uncles Sayoon Kim and Sachol Edward Kim. Without Sayoon Kim, I would not be able to start my doctoral study. Without Sachol Kim, I would not even start studying Mathematics. I thank both of you deeply from my bottom of heart.

I would like to thank uncle Daeyun Won for his constant care and support.

I would like to thank Ms. Hye-kyung Choi for her generous understanding and kind emotional support.

I would like to thank my friends for their understanding and support, especially Jonghee Lee, Joshua Biehn, Youngkwon Kim, Euiseok Kim, and Jongwook Park.

Finally, my special thanks go to my parents, Do-yeon Won and Sung-ae Kim, and my sister, Jinyoung Won, for their support throughout this very long process.

Table of Contents

Introduction

Decision problem is the problem of finding, for a given class of questions which depend on certain parameters, an algorithm that answers, for a given input, "Yes" or "No" correctly. It is, by nature, an algorithmic problem. One of the most outstanding algorithmic problems in group theory and semigroup theory is the word problem.

The word problem in group theory(similarly semigroup theory) asks whether there exists an algorithm that answers correctly if any two words are equivalent in the group(respectively semigroup). The word problem was first stated by M. Dehn in 1910 for groups. For semigroups, A. Thue in 1914 first stated the word problem.(See [1]) Since then many mathematicians have made huge efforts to resolve this problem. For example, Dehn himself solved the word problem for the trefoil knot group in 1914. In 1926 E. Artin solved the word problem for braid groups. In 1932 W. Magnus solved the word problem for one relator groups.(See [22]) But the general question of whether the word

problem is solvable on any group or any semigroup turns out to have a negative answer. The history of this negative aspect of the word problem goes back to the 1930's.

In 1936, Turing introduced his model of computation, the Turing machine. The Turing machine, which is equipped with an infinite tape and a tape head with a finite alphabet and a finite set of tape head states, has been accepted as a computation model that captures the core of human computation. With Church's thesis, the Turing machine is used to prove the unsolvability of algorithmic problems.

In 1936 Turing proved that there is a decision problem that no algorithm on the Turing machine can solve. This was a special case of the halting problem and later it was realized that the halting problem on the Turing machine can not be decided by any Turing machine, hence the halting problem is undecidable.

In 1947, Markov and Post independently constructed finitely presented semigroups with unsolvable word problems. They were able to construct the semigroups by simulating the computation of the Turing machine in their semigroups and they were the first algebraic structures that contained an undecidable decision problem. The presentation of the semigroup is not

simple, since it contains a huge number of generators and relations. However, several mathematicians showed later that there are even much more simply presented semigroups where the word problem is unsolvable. For example, Tseitin, Makaninn, and Matiyasevich all came up with much more simply presented semigroups with unsolvable word problems.

The undecidability result on semigroups could not be applied to groups directly. For example, Post's semigroup can not be embedded in a group. For groups, it was in 1955 that Novikov constructed the first group that contains an unsolvable word problem, and one year later Boone constructed his group with an unsolvable word problem. Thus the word problem for semigroups and groups has, as we all know now, a negative solution, unsolvable in general.

So far the decidability of the word problem has been the main question. But with the rapid development of the computer and complexity theory, other aspects of the word problem have been considered by many mathematicians, such as, 'when the word problem on an algebraic structure is decidable how fast can one solve the word problem?' This question addresses the practical solvability of the word problem with current computational devices. Several groups which have the solvable word problem have a fast algorithm - we mean an algorithm whose complexity is polynomial in the length of input, for

example, word-hyperbolic groups and linear groups over the field of rational numbers. However, for some groups where the word problem is decidable, it is very difficult to analyze the complexity of the algorithm; the famous example is the Magnus' algorithm for the word problem for one relator group, whose complexity is still unknown.

When one runs a computer program to solve a problem, one often experiences the cases that for "most" inputs the program runs quite fast but for some small number of inputs the program runs very slowly. From this observation one can classify the inputs into two categories: the set of inputs where the algorithm answers quickly(or in a reasonable amount of time) and the set of inputs where the algorithm answers quite slowly and even possibly don't answer. This classification has been applied in group theory, and [9] Kapovich, Myasnikov, Shupp, and Shpilrain proposed the following approach to the word problem for groups and semigroups : given a finitely generated group(or semigroup) $G = \langle X \mid R \rangle$, decide whether the word problem is solvable on a generic subset of $X^* \times X^*$ with a suitable measure ρ on X. If one can find such an procedure, then we say the word problem on G is generically decidable. In [9], the authors note that this approach could be adapted to algebraic structures where the word problem is known to be unsolvable.

The idea of this approach is, although one may not solve the word problem completely on certain difficult algebraic structures, one may be able to answer the question of word problem on 'most' cases by measuring the set of inputs where the word problem is solvable.

The aim of this thesis is to show that several semigroups and groups with unsolvable word problems do have generic solutions of the word problem. In chapter 1, we review the Turing machine, undecidable problems on the Turing machine, semigroups and groups with undecidable word problems, and the generic-case complexity of a decision problem. In chapter 2, we define first a certain type of presentation of semigroups, called a balanced presentation, then show that the word problem is generically solvable for semigroups that have those presentations. Then we observe that several well-known semigroups with unsolvable word problem, such as Post semigroup, Tseitin semigroup, Makaninn's semigroup and Matiyasevich semigroup, do have balanced presentations, hence the word problem is generically solvable for these semigroups. In chapter 3, we extend the idea of balanced presentation to groups and show that the word problem for a finitely generated group with a balanced presentation is generically solvable. Then we observe that many well-known groups with unsolvable word problem, such as Novikov's group,

Boone's group, Borisov's group and Collins' group, do have balanced presentations as well, hence the word problem is generically solvable for these groups.

In the last chapter we show a generic solution of the conjugacy problem on HNN extension using the blackhole. This work is based on the paper [5]. In [5], the authors show a generic solution of the conjugacy problem for amalgamated products using the blackhole. In chapter 4, we show that a similar approach to the HNN-extensions using blackhole solves the conjugacy problem generically.

Chapter 1

Decision problems and generic case complexity

1.1 Turing machines and the halting problem

In this section we introduce Turing's computational model, the Turing machine and an undecidable problem on the Turing machine.

A Turing machine is assumed to have a tape and a tape head. The tape of a Turing machine is assumed to be infinite in both directions and it has infinitely many cells in it. Each cell in the tape can contain a tape letter symbol from a finite set of symbols or can be blank. The tape contains only a finite string as an input and the rest of the cells in the tape are blank. At each moment of the computation, the tape head scans a cell in the tape, reads the tape letter in a cell at the current position and can change the

tape letter as well as move the position of tape head back or forth. To direct the movement of the tape head, Turing realized that it needs only a finite number of internal states. To describe a Turing machine completely, one needs a finite set of tape symbols Σ, a finite set of internal states Q, a transition function (or a program) $P : Q \times \Sigma \to Q \times (\Sigma \cup \{L, R\})$, which directs the movement of the tape head with L being the symbol to move the tape head one cell to the left and R being the symbol to move the tape head one cell to the right, a starting state from Q, which we denote by q_1 and an halting state from Q, which we denote by q_0. The formal definition of a Turing machine is the following:

Definition 1.1.1. A Turing machine is a 5-tuple, (Q, Σ, P, q_0, q_1), where Q, Σ are all finite sets and

1. $Q = \{q_0, q_1 \cdots q_l\}$ is the set of internal states,
2. $\Sigma = \{e_0, e_1, \cdots e_m\}$ is the tape alphabet, where e_0 is used to denote the blank symbol,
3. $P : Q \times \Sigma \to Q \times (\Sigma \cup \{L, R\})$ is the transition function,
4. $q_1 \in Q$ is the start state,
5. $q_0 \in Q$ is the halting state.

The core of a Turing machine is the transition function P, which describes how to move the tape head of the machine at any moment during the computation. It is the instructions as below:

For any $(q_i, e_j) \in Q \times \Sigma$ with $i > 0$, the transition function P of Turing machine is defined as below;

1. $P(q_i, e_j) = (q_k, e_r)$, which means if the tape letter in the scanned cell in the tape of Turing machine is e_j with current internal state q_i, then change the letter e_j to e_r and the state q_i to q_k.

2. $P(q_i, e_j) = (q_k, L)$, which means if the tape letter in the scanned cell in the tape is e_j with current state q_i, then change the state q_i to q_k and move the tape head one cell to the left.

3. $P(q_i, e_j) = (q_k, R)$, which means if the tape letter in the scanned cell in the tape is e_j with current state q_i, then change the state q_i to q_k and move the tape head one cell to the right.

At any moment during the computation, the sequence of letters of the form Kq_ia_jM where q_i is the current tape head state, a_j is the scanned tape letter inside the cell in the tape, and $K, M \in \Sigma^*$ are the sequences of letters to the left and to the right of the current cell in the tape respectively,

describes the next move of the Turing machine. We call this word Kq_ia_jM, the configuration of the Turing machine at the current state.

Once a Turing machine starts, the computation proceeds according to the rules described by the transition function. The computation continues until the tape head enters the halting state. If it does not occur, the machine goes on forever. If a Turing machine begins in a configuration q_1A and halts in a configuration Bq_0C then we say the Turing machine accepts a word BC.

We say an algorithmic problem is decidable if there exists an algorithm of a Turing machine that answers correctly "Yes" or "No" for a given input.

Turing machines are powerful computational models that do everything computers do, but as it was shown, the following problem can not be decided by any Turing machine.

Halting problem : For a given Turing machine $T = (Q, \Sigma, P, q_0, q_1)$ and an input $u \in \Sigma^*$, find an algorithm that decides whether T halts.

The halting problem of Turing machines is algorithmically unsolvable implies the following theorem:

Theorem 1.1.1. *There is a Turing machine for which no algorithm solves the halting problem.*

For detail and history of the halting problem of Turing machines, see [1]

and [22].

1.2 Semigroups and groups with unsolvable word problem

In 1914, A. Thue first proposed the way of defining a semigroup in terms of generators and defining relations: Let A be a set. A word on A is a finite sequence $a_1a_2\cdots a_k$, where each a_i, $1 \leq i \leq k$, is an element in A. Let A^* be the set of all finite words generated by elements of A. Then A^* together with concatenation operation of two words called a free semigroup generated by A. We denote this semigroup by $\langle A \mid - \rangle$ or simply $\langle A \rangle$.

A relation in a semigroup is an ordered pair of words. If (u, v) is a relation in $\langle A \rangle$ where $u, v \in A^*$, we denote it by $u = v$. Let $\mathcal{R}$ be a set of relations. One can define an equivalence relation with $\mathcal{R}$ on $\langle A \rangle$, that is, for $w_1, w_2 \in A^*$, we say w_1 is equivalent to w_2 if and only if w_1 can be transformed into w_2 through a finite number of applications of relations in $\mathcal{R}$. Then the set of equivalence classes on $\langle A \rangle$ with respect to $\mathcal{R}$ with induced concatenation operation on the equivalence classes is a semigroup and denoted by $\langle A \mid \mathcal{R} \rangle$. We say the semigroup $\langle A \mid \mathcal{R} \rangle$ is generated by the generating set A and the

set of defining relations $\mathcal{R}$.

For a group presentation, let A be a set and, for each $a \in A$, let a^{-1} be a new symbol, which we call the inverse of a. Let A^{-1} be the set of all inverse symbols of elements of A, i.e. $A^{-1} = \{a^{-1} \mid a \in A\}$. The empty word is denoted by 1. For each $a \in A$ relations of the form $aa^{-1} = 1, a^{-1}a = 1$ are called trivial relations. Then

$$F_A = \left\langle A \cup A^{-1} \mid a_i a_i^{-1} = 1, a_i^{-1} a_i = 1 \text{ for all } a_i \in A \right\rangle$$

is a group and we call F_A a free group generated by A, simply denote it by $F_A = \langle A \mid - \rangle$ or $\langle A \rangle$. A relation is an equation of the form $W(a_1, a_2, \cdots, a_k) = 1$ where $W(a_1, a_2, \cdots, a_k)$ is a word on $A \cup A^{-1}$. Let $\mathcal{R}_G$ be a set of relations. Then one can define an equivalence relation with respect to $\mathcal{R}_G$ on F_A, that is, two words $w_1, w_2 \in (A \cup A^{-1})^*$ are equivalent if and only if w_1 can be transformed into w_2 through a finite number of applications of trivial relations and relations in $\mathcal{R}_G$. The set of equivalence classes on F_A with respect to $\mathcal{R}_G$ with induced group operation on equivalence classes is a group and is denoted by $\langle A \mid \mathcal{R}_G \rangle$. We say the group $\langle A \mid \mathcal{R}_G \rangle$ is generated by the generating set A and the set of defining relations $\mathcal{R}_G$. The generating set of a semigroup or a group is sometimes called an alphabet.

The word problem on semigroup and group can be formulated as below.

Semigroup Let A be a finite alphabet that generates a semigroup $S = \langle A \mid R \rangle$. The word problem with respect to the generating set A is:

For any two words $u, v \in A^*$, construct an algorithm to determine whether or not u and v are equivalent in S.

Group Let A be a set of generators for a finitely generated group $G = \langle A \mid R_G \rangle$. The word problem with respect to the generating set A for G is defined as below :

For an arbitrary word $w \in (A \cup A^{-1})^*$, construct an algorithm to determine whether or not w is equivalent to the identity element in G.

In 1947, Post and Markov independently constructed a semigroup with unsolvable word problem. The semigroup is constructed from a Turing machine with undecidable halting problem and we briefly show below the Post's construction of his semigroup:

Let $T = (Q, \Sigma, P, q_0, q_1)$ be a Turing machine where $Q = \{q_0, \cdots, q_l\}$ is the set of internal states, $\Sigma = \{e_0, \cdots, e_m, L, R\}$ is the set of tape letter symbols with left move and right move symbols, P is the transition function and q_1 is the start state. From a Turing machine $T = (Q, \Sigma, P, q_0, q_1)$, one can construct a semigroup S_T in the following way; S_T is generated by $Q \cup \Sigma \cup \{h\}$

and defining relations R_{S_T} of S_T are presented below;

(i) For each instruction in the program of T of the form $P(q_i, e_j) = (q_k, e_l)$, include a relation $q_i e_j = q_k e_l$.

(ii) For each instruction in the program of T of the form $P(q_i, e_j) = (q_k, L)$, include relations $e_s q_i e_j = q_k e_s e_j$ for all $s = 0, 1, \ldots, m$ and one more relation $h q_i e_j = h q_k e_0 e_j$.

(iii) For each instruction in the program of T of the form $P(q_i, e_j) = (q_k, R)$, include the relations $q_i e_j e_s = e_j q_k e_s$ for all $s = 0, 1, \ldots, m$ and one more relation $q_i e_j h = e_j q_k e_0 h$.

(iv) $q_0 e_i = q_0, e_i q_0 = q_0$ for all $0 \leq i \leq m$ and $h q_0 h = q_0$.

We call a semigroup constructed from a Turing machine in this way a Post semigroup.

Post showed that if $T_u = (Q, \Sigma, P, q_1, q_0)$ is a Turing machine with undecidable halting problem then the semigroup S_{T_u} constructed from T_u as shown above has an unsolvable word problem. Markov also proved the same result independently in a similar way.

Theorem 1.2.1 (Markov, Post)**.** *Let T_u be a Turing machine with undecidable halting problem. Let S_{T_u} be a semigroup constructed from T_u by the*

method described above. Then the problem of deciding whether an arbitrary word w generated by letters from the generators of S_{T_u} is equal to q_0 in S_{T_u} is unsolvable.

For groups, in 1955, Novikov constructed the first group with unsolvable word problem.

Theorem 1.2.2 (Novikov)**.** *Let $\Gamma =< g_1, g_2, \cdots, g_n \mid L_1 = R_1, \cdots, L_m = R_m >$ be a semigroup such that L_i, R_i for $1 \leq i \leq m$ are not the empty word and, for some word u, the problem of deciding whether $X = u$ is unsolvable. Let G be a group presented by $G = < g_1, \cdots, g_n, l, r, c, t, k \mid R_G >$ where R_G consists of the following relations;*

$$g_i l = l^{m+1} g_i, \quad r g_i = g_i r^{m+1} \text{ for } 1 \leq i \leq n,$$

$$c g_i = g_i c, \quad (l^i L_i r^i) c = c(l^i R_i r^i) \text{ for } 1 \leq i \leq m,$$

$$ct = tc, \quad lt = tl, \quad ck = kc, \quad kr = kr, \quad (q^{-1}tq)k = k(q^{-1}tq).$$

Then G has an unsolvable word problem.

1.3 Generic-case complexity

Computational complexity measures how much time, space or other resources are required to solve a given decision problem. The computational complexity of a decision problem depends on the model of computation, for instance, whether it is a single-tape Turing machine or a multi-tape Turing machine, and the mode of computation, for instance, whether the Turing machine is deterministic or nondeterministic. In this paper all computational complexities are assumed to be measured with a multi-tape deterministic Turing machine and we are only concerned with the time complexity of the machine.

Definition 1.3.1. Let T be a multi-tape deterministic Turing machine that halts on all inputs. The time complexity of T is defined by the function $r : \mathbb{N} \to \mathbb{N}$, where $r(n)$ is the maximal number of steps that takes for T to reach the halting state on an input of length n.

The generic-case complexity of a decision problem measures how fast an algorithm solves a given decision problem on "most" inputs. For this approach to a decision problem we need a measure to say "most" inputs. We use an asymptotic density as a measure for that, which is suggested in [9].

Definition 1.3.2. Let X be a finite set of letters. We define the length

of $(u, v) \in X^* \times X^*$ to be $|u| + |v|$. Let $U \subset X^* \times X^*$. For any positive integer n, let S_n be the set of all ordered pairs in $X^* \times X^*$ of length n, $S_n = \{(u, v) \in X^* \times X^* | \ |u| + |v| = n\}$. The asymptotic density $\rho(U)$ for U is defined by

$$\rho(U) = limsup_{n\to\infty}\rho_n(U),$$

where

$$\rho_n(U) = \frac{|U \cap S_n|}{|S_n|}.$$

If $lim_{n\to\infty}\rho_n(U)$ exists, we denote it by $\hat{\rho}(U)$.

We say a set $U \subseteq X^* \times X^*$ is generic if $\hat{\rho}(U) = 1$ and a set $V \subseteq X^* \times X^*$ is negligible if $(X^* \times X^*) \setminus V$ is generic.

Having this probability function ρ on $X^* \times X^*$, we define the generic-case complexity of the word problem.

Definition 1.3.3. Let $WP \subseteq X^* \times X^*$ be the word problem on X and let C be a complexity class. Let P be a partial algorithm for WP on X . We say that P solves WP with generic-case complexity C if there is a generic subset $U \subseteq X^* \times X^*$ such that P solves WP on all inputs from U within the complexity bound C.

Chapter 2

Balanced semigroup

2.1 Balanced semigroup presentation

In this section we define a certain type of presentation of semigroups, which we call a balanced semigroup presentation, and we present a generic solution of the word problem for finitely generated semigroups with balanced presentations.

Let Π be a semigroup presented by a finite alphabet X and a set of defining relations $R = \{l_i = r_i \mid i \in I\}$, where $l_i, r_i \in X^*$ and $|I| < \infty$. For $a \in X$ and $w \in X^*$, let us denote by $\sigma_a(w)$ the number of occurrences of a in w. We call the set of defining relations R a-balanced if, for every $i \in I$,

$\sigma_a(l_i) = \sigma_a(r_i)$. If a semigroup Π is presented by a set of a-balanced relations R, then we say Π is a-balanced and a is a balanced letter.

Lemma 1. *Let X be a finite set and let $a \in X$. Let $\Pi = \langle X \mid R \rangle$ be an a-balanced semigroup and let $u, v \in X^*$. If $u =_\Pi v$ then $\sigma_a(u) = \sigma_a(v)$.*

Proof. Obvious. □

Hence two equivalent words in a balanced semigroup have the same number of balanced letters. This property of equivalent words turns out to be a sufficient condition to solve the word problem for a balanced semigroup generically:

Let $a \in X$ and let $B \subset X^* \times X^*$ be a set of all a-balanced pairs of words, i.e.

$$B = \{(u, v) \in X^* \times X^* \mid \sigma_a(u) = \sigma_a(v)\}$$

We claim that the set B is negligible in $X^* \times X^*$.

Let $S(n) = \{(u, v) \in X^* \times X^* | \ |u| + |v| = n \ \}$ be the sphere of radius n in $X^* \times X^*$. We show that

$$\frac{|B \cap S(n)|}{|S(n)|} \to 0$$

as $n \to \infty$.

Observe that a pair of words $(u, v) \in X^* \times X^*$ can be represented by a pair of one word and a natural number $(w, n) \in X^* \times \mathbb{N}$, where w is the concatenation of u and v and n is the length of u, i.e. $(w, n) = (uv, |u|)$. We say the latter presentation $(w, n) \in X^* \times \mathbb{N}$ is a-balanced if there exists $u, v \in X^*$ such that $w = uv$ and $\sigma_a(u) = \sigma_a(v)$. Hence there is a one to one correspondence between balanced pair of words $(u, v) \in X^* \times X^*$ and balanced pairs $(w, n) \in X^* \times \mathbb{N}$.

When we count the cardinality of $B \cap S(n)$, we use the latter presentation $(w, n) \in X^* \times \mathbb{N}$ for a pair of words $(u, v) \in X^* \times X^*$. Then $S(n)$ is equinumerous to the set S_n where

$$S_n = \{(w, r) \in X^* \times \mathbb{N} \mid |w| = n,\ 0 \leq r \leq n\}$$

and to count $|B \cap S(n)|$, we count the a-balanced pair of words in S_n.

Let W_n be the set of all words on X with the length n and let $w \in W_n$. Let $\gamma_a(w)$ be the length of a longest factor of w which contains no a symbol.

Lemma 2. *Let X be a finite set containing at least two letters and let $a \in X$. Let w be a word on X. There are at most $\gamma_a(w) + 1$ a-balanced ordered pairs in $(w, 0), \ldots, (w, |w|)$.*

Proof. Obvious. □

We say a word w' is a factor of a word w if $w = uw'v$.

Lemma 3. *Let X be a finite set containing at least two letters and let $a \in X$. Let $W_n = \{w \in X^* \mid |w| = n\}$. Then, for any positive integer $k \leq n$,*

$$|\{w \in W_n \mid \gamma_a(w) \geq k\}| \leq (n-k)(|X|-1)^k |X|^{n-k}.$$

Proof. Let $w \in W_n$ and let w' be a factor of w of the maximal length which does not contain a. Assume that w' is located at the beginning of w. Then the number of words w's that have initial factor w' of length at least k, is $(|X|-1)^k|X|^{n-k}$. w' can be placed in any $n-k$ positions in w and the same formula works for each positions, thus adding all together gives an upper bound of $|\{w \in W_n \mid \gamma_a(w) \geq k\}|$ in the statement of the proposition. □

Lemma 4. *Let X be a finite set containing at least two letters and let $a \in X$. Let $B_n = \{(w, r) \in S_n \mid w = w_1w_2$ for some $w_1, w_2 \in X^*, |w_1| = r$ and $\sigma_a(w_1) = \sigma_a(w_2)\}$. Then, for any positive integer n such that $\lceil (log_2 n)^2 \rceil \leq n$, the following inequality holds:*

$$|B_n| \leq \lceil (log_2 n)^2 \rceil |X|^n + (n+1)(n - \lceil (log_2 n)^2 \rceil)(|X|-1)^{\lceil (log_2 n)^2 \rceil} |X|^{n - \lceil (log_2 n)^2 \rceil}.$$

Proof. We partition $W_n = \{w \in X^* \mid |w| = n\}$ into two classes

$$W_n = \{w \in W_n \mid \gamma_a(w) < \lceil (log_2 n)^2 \rceil\} \cup \{w \in W_n \mid \gamma_a(w) \geq \lceil (log_2 n)^2 \rceil\}.$$

Then

$$S_n = W_n \times \{0, \ldots, n\}$$

$$= \{w \in W_n \mid \gamma_a(w) < \lceil (log_2 n)^2 \rceil\} \times \{0, \ldots, n\} \cup$$

$$\{w \in W_n \mid \gamma_a(w) \geq \lceil (log_2 n)^2 \rceil\} \times \{0, \ldots, n\}.$$

Every w in $(w,0), \cdots, (w,n)$ in the first set has $\gamma_a(w) < \lceil (log_2 n)^2 \rceil$, thus by the Lemma 2, there are at most $\lceil (log_2 n)^2 \rceil$ many a-balanced pairs in $(w,0), \cdots, (w,n)$ for each w in $\{w \in W_n \mid \gamma_a(w) < \lceil (log_2 n)^2 \rceil\}$ of the first set. Hence the number of a-balanced pairs from the first set is bounded above by $\lceil (log_2 n)^2 \rceil |X|^n$. The number of a-balanced pairs from the second set is bounded above by $(n+1)(n - \lceil (log_2 n)^2 \rceil)(|X|-1)^{\lceil (log_2 n)^2 \rceil} |X|^{n - \lceil (log_2 n)^2 \rceil}$ by Lemma 3 since this is the case when $k = \lceil (log_2 n)^2 \rceil$. □

Now we can show that $B = \{(u,v) \in X^* \times X^* \mid \sigma_a(u) = \sigma_a(v)\}$ is negligible in $X^* \times X^*$.

Proposition 1. *Let X be a finite set containing at least two letters and let $a \in X$. Then the set B of all a-balanced pairs of words on X is negligible in $X^* \times X^*$.*

Proof. Let $S(n) = \{(u,v) \in X^* \times X^* \mid |u| + |v| = n\}$, the sphere of radius n in $X^* \times X^*$ and let $B(n) = \{(u,v) \in S(n) \mid \sigma_a(u) = \sigma_a(v)\}$, the set of all

pairs of a-balanced words in $S(n)$, hence $B(n) = B \cap S(n)$. As we mentioned before, $S(n)$ is equinumerous to S_n and $B(n)$ is equinumerous to B_n. Hence $\frac{|B(n)|}{|S(n)|} = \frac{|B_n|}{|S_n|}$. By Lemma 4,

$$\begin{aligned}\frac{|B_n|}{|S_n|} &\leq \frac{\lceil (log_2 n)^2 \rceil |X|^n + (n+1)(n - \lceil (log_2 n)^2 \rceil)(|X|-1)^{\lceil (log_2 n)^2 \rceil} |X|^{n - \lceil (log_2 n)^2 \rceil}}{(n+1)|X|^n} \\ &= \frac{\lceil (log_2 n)^2 \rceil}{n+1} + \frac{(n - \lceil (log_2 n)^2 \rceil)(|X|-1)^{\lceil (log_2 n)^2 \rceil} |X|^{n - \lceil (log_2 n)^2 \rceil}}{|X|^n} \\ &= \frac{\lceil (log_2 n)^2 \rceil}{n+1} + (n - \lceil (log_2 n)^2 \rceil)\left(\frac{|X|-1}{|X|}\right)^{\lceil (log_2 n)^2 \rceil}.\end{aligned}$$

Since both $\frac{\lceil (log_2 n)^2 \rceil}{n+1}$ and $(n - \lceil (log_2 n)^2 \rceil)\left(\frac{|X|-1}{|X|}\right)^{\lceil (log_2 n)^2 \rceil}$ converge to 0 as $n \to \infty$, B is negligible in S. □

Theorem 2.1.1. *Let X be a finite set containing at least two letters and let $a \in X$. Let $\Pi = < X \mid R >$ be a finitely presented a-balanced semigroup. Then the word problem on Π is generically solvable by a linear time partial algorithm.*

Proof. Let u, v be two words in Π. The algorithm counts the number of occurrences of balanced letter a in u and v and compares them. If $\sigma_a(u) \neq \sigma_a(v)$ then the algorithm concludes that $u \neq_\Pi v$. Certainly this process can be done in linear time on $|u| + |v|$. Since $B = \{(u, v) \in X^* \times X^* \mid \sigma_a(w_1) = \sigma_a(w_2)\}$ is negligible in $X^* \times X^*$ by Proposition 1, the set $\{(u, v) \in X^* \times X^* \mid$

$\sigma_a(w_1) \neq \sigma_a(w_2)\}$, where the algorithm works, is generic in $X^* \times X^*$ and, hence, this algorithm solves the WP for Π generically. $\square$

2.2 Post semigroup

As we saw in section 1.2, the Post's construction of a semigroup is based on a Turing machine. For a semigroup with unsolvable word problem, they constructed a semigroup from a Turing machine with undecidable halting problem. In this section we show that the algorithm which counts the balanced letter in the presentation described in the previous section solves the word problem for the Post semigroup generically.

Let $T_u = (Q_u, \Sigma_u, P_u, q_0, q_1)$ be a Turing machine with undecidable halting problem where $Q_u = \{q_0, q_1, \cdots, q_{l-1}\}$ is the set of internal states and $\Sigma = \{e_0, e_1, \cdots, e_{m-1}\}$ is the set of tape letter symbols. Let S_{T_u} be the Post semigroup constructed from T_u by the construction described in section 1.2. The presentation of the Post semigroup S_{T_u} does not have a balanced letter in general, but the number of Q_u symbols in both sides of the relations are the same. Hence we can apply the method in the section 1.2 to solve the word problem generically for S_{T_u}.

Theorem 2.2.1. *Let T_u be a Turing machine with an undecidable halting problem and let S_{T_u} be a Post semigroup constructed from T_u. The word problem in S_{T_u} is generically solvable by a linear time partial algorithm.*

Proof. Let $T_u = (Q_u, \Sigma_u, P_u, q_0, q_1)$ be a Turing machine with undecidable halting problem where $Q_u = \{q_0, q_1, \cdots, q_{l-1}\}$ is the set of internal states and $\Sigma = \{e_0, e_1, \cdots, e_{m-1}\}$ is the set of tape letters. Let S_{T_u} be a Post semigroup presented by $\langle\ e_0, \ldots, e_{m-1}, q_0, \ldots, q_{l-1}, h \mid \mathcal{R}_T\ \rangle$ where $\mathcal{R}_t$ consists of the relations of the type described in section 1.2. Although S_{T_u} may not have a balanced letter in its relations, the number of q_i symbols in both sides of relations are the same. Thus if two words in S_{T_u} are equivalent then they have the same number of q_i symbols. We show that counting q_i symbols in a word $w \in S_{T_u}$ solves the word problem on S_{T_u} generically:

Let $S = \{e_0, e_1, \ldots, e_{m-1}, q_0, q_1, \ldots, q_{l-1}, h\}$ and let $Q = \{q_0, \cdots, q_{l-1}\}$. For $w \in S^*$, we denote by $\sigma_Q(w)$ the number of $q_i \in Q$ symbols in w. Let $B = \{(w_1, w_2) \in S^* \times S^* \mid \sigma_Q(w_1) = \sigma_Q(w_2)\}$. We claim that B is negligible in $S^* \times S^*$. As in the previous section, we will work with the pair $(w, r) \in S^* \times \mathbb{N}$ for a pair of words $(w_1, w_2) \in S^* \times S^*$, where $w = w_1 w_2$ and $r = |w_1|$, to show that B is negligible in $S^* \times S^*$. We say a pair (w, r) is Q-balanced if $w = w_1 w_2$ for some w_1, w_2 in Q^* and $\sigma_Q(w_1) = \sigma_Q(w_2)$. For each $w \in S^*$,

let us define $\gamma_Q(w)$ to be the length of a maximal factor in w which does not contain any q_i symbols in Q.

Lemma 5. *Let S be a finite set containing at least two letters and let Q be a proper subset of S. Let w be a word on S. There are at most $\gamma_Q(w)+1$ Q-balanced pairs in $(w,0),\ldots,(w,|w|)$.*

Proof. Obvious. □

Lemma 6. *Let $S=\{e_0,e_1,\ldots,e_{m-1},q_0,q_1,\ldots,q_{l-1},h\}$ and let $W_n=\{w\in S^* \mid |w|=n\}$. Then*

$$|\{w\in W_n \mid \gamma_Q(w)\geq k\}|\leq (n-k)(|S|-l)^k|S|^{n-k}.$$

In particular, for a sufficiently large positive integer n, that is for every $n\geq \lceil(log_2 n)^2\rceil$,

$$|\{w\in W_n \mid \gamma_Q(w)\geq \lceil(log_2 n)^2\rceil\}|\leq (n-\lceil(log_2 n)^2\rceil)(|S|-l)^{\lceil(log_2 n)^2\rceil}|S|^{n-\lceil(log_2 n)^2\rceil}.$$

Proof. The proof is almost the same as the proof of Lemma 3 when one replaces $|X|$ with $|S|$ and $|X|-1$ with $|S|-l$ where $l=|Q|$. □

A sphere of radius n in $S^*\times S^*$, $S(n)$, is equinumorous to the set

$$S_n=\{(w,r)\mid w\in S^*, |w|=n,\ 0\leq r\leq n\}\equiv\{w\in S^*\mid |w|=n\}\times\{0,\ldots,n\}.$$

Let $B_n = \{(w, r) \in S_n \mid w = w_1 w_2$ for some $w_1, w_2 \in S^*, |w_1| = r$ and $\sigma_Q(w_1) = \sigma_Q(w_2)\}$. Combining Lemma 5 and Lemma 6, one obtains the following upper bound for the number of pairs of balanced words in S_n:

$$|B_n| \leq \lceil (log_2 n)^2 \rceil |S|^n + (n+1)(n - \lceil (log_2 n)^2 \rceil)(|S| - l)^{\lceil (log_2 n)^2 \rceil} |S|^{n - \lceil (log_2 n)^2 \rceil}.$$

Hence

$$\frac{|B_n|}{|S_n|} \leq \frac{\lceil (log_2 n)^2 \rceil |S|^n + (n+1)(n - \lceil (log_2 n)^2 \rceil)(|S| - l)^{\lceil (log_2 n)^2 \rceil} |S|^{n - \lceil (log_2 n)^2 \rceil}}{(n+1)|S|^n} \tag{2.2.1}$$

$$= \frac{\lceil (log_2 n)^2 \rceil}{(n+1)} + (n - \lceil (log_2 n)^2 \rceil) \left(\frac{|S| - l}{|S|} \right)^{\lceil (log_2 n)^2 \rceil} \tag{2.2.2}$$

Since (2) converges to 0 as $n \to \infty$, B is negligible in $S^* \times S^*$. This proves the Theorem. □

2.3 Other semigroups with unsolvable word problems

The Post semigroup S_{T_u} constructed in the previous section has a huge number of generators and relations that come from the Turing machine T_u. After the construction of S_{T_u}, Tseitin, Makaninn and Matiyasevich showed

that there are much more simply presented semigroups with unsolvable word problem. These semigroups have much smaller numbers of generators and relations, although some of the relations might be quite long. Interestingly, many of these semigroups have a balanced letter in their presentations, so that one can solve the word problem generically for those semigroups.

Example 2.3.1. *In 1956, Tseitin constructed an amazingly simply presented semigroup T_s with 5 generators and 7 relations that has an unsolvable word problem.*

$$T_s = < a, b, c, d, e \mid ac = ca, ad = da, bc = cd, bd = db, ce = eca, de = edb, cca = ccae >$$

Example 2.3.2. *In 1966, G. Makanin constructed a semigroup Π_6^4 presented by four generators and six relations with unsolvable word problem.*

$$\Pi_6^4 =< \ a, b, c, d, \ \mid ab = ba, add = dda, dab = bda, cba = bc, cddda = ddc, aabb = aabbc >$$

Proposition 2. *The word problems on T_s and Π_6^4 are generically solvable by a linear time partial algorithm.*

Proof. T_s has balanced letters c, d in its presentation. Π_6^4 has a balanced letter b. Thus the word problems on these semigroups are generically solvable by Theorem 2.1.1. □

2.4 Matiyasevich semigroup

In 1966, Yu. Matiyasevich constructed a semigroup with unsolvable word problem. What is remarkable about this semigroup is that it has only two generators and three defining relations. This is the best known example of a semigroup so far in terms of numbers of generators and relations. To see the presentation of Matiyasevich semigroup, let us follow the construction of the semigroup.

Let T_0 be a Turing machine with undecidable halting problem and let S_{T_0} be the Post semigroup constructed from T_0. Then we make the relations in S_{T_0} of the form $L_i = R_i$, where $|L_i| = 1$ and $|R_i| = 2$. We also make this semigroup have 2^k many relations for some positive integer k where 2^k is greater than the number of generators of S_{T_0}. We call this semigroup Π_1;

$$\Pi_1 =< g_1, g_2, \cdots, g_n \mid L_1 = R_1, \cdots, L_m = R_m >$$

where $|L_i| = 1$, $|R_i| = 2$, $m = 2^k$ for some integer k and $m > n + 3$.

Now let us define a map Ψ from Π_1 to $\{a, b\}^*$ recursively by

$$\Psi(g_i) = a^2 b^i a b^{m-i-3} \quad \text{for} \quad i = 1, 2, \ldots, n, \quad \text{and}$$

$$\Psi(XY) = \Psi(X)\Psi(Y) \quad \text{for} \quad X, Y \in \{g_1, \cdots, g_n\}^*.$$

Let us denote the image of L_i and R_i under Ψ by

$$\Psi(L_i) = l_{i1}l_{i2}\cdots\cdots l_{im},$$

$$\Psi(R_i) = r_{i1}r_{i2}\cdots\cdots r_{i2m}.$$

Now let A and B be two words in $\{a,b\}^*$ defined by

$$A = l_{11}l_{21}\cdots l_{m1}l_{12}l_{22}\cdots l_{m2}\cdots l_{1m}l_{2m}\cdots l_{mm},$$

$$B = r_{11}r_{21}\cdots r_{m1}r_{12}r_{22}\cdots r_{m2}\cdots r_{12m}r_{22m}\cdots r_{m2m}.$$

Then the semigroup Π_2 is defined as

$$\Pi_2 =< \ a,b,c \mid ac = caa, ac = cba, bc = cab, bc = cbb, A = B \ >$$

Let us define a map τ from Π_2 to $\{\alpha,\beta\}^*$ recursively by

$$\tau(a) = \beta, \tau(b) = \beta\alpha, \tau(c) = \alpha\alpha, \tau(1) = 1, \ \text{ and}$$

$$\tau(XY) = \tau(X)\tau(Y) \ \text{ for } \ X, Y \in \{a,b,c\}^*$$

Observe that τ transforms the relations in Π_2,

$$ac = caa, \ ac = cba, \ bc = cab, \ bc = cbb, \ A = B,$$

to

$$\alpha\alpha\beta\alpha\beta = \beta\alpha\alpha, \ \alpha\alpha\beta\beta = \beta\alpha\alpha, \ \alpha\alpha\beta\alpha\beta\alpha = \beta\alpha\alpha, \ \alpha\alpha\beta\beta\alpha = \beta\alpha\alpha\alpha, \ \tau(A) = \tau(B)$$

Matiyasevich semigroup Π_3 is then defined as

$$\Pi_3 = < \ \alpha, \beta \mid \alpha\alpha\beta\beta = \beta\alpha\alpha, \ \beta\alpha\alpha = \alpha\alpha\beta\alpha\beta, \ \tau(A) = \tau(B) \ > .$$

Theorem 2.4.1 (Matiyasevich)**.** *The word problem on* Π_3 *is unsolvable.*

Matiyasevich semigroup is a little different from the previous semigroups with unsolvable word problems. Observe that in the presentation of Π_3 none of the generating letters is balanced in the defining relations of Π_3. However, one can observe that the first two defining relations of Π_3 have the same number of $\alpha\alpha$'s. Since $\tau(A)$ and $\tau(B)$ do not have a $\alpha\alpha$ inside, the number of $\alpha\alpha$'s is the same in both sides of all defining relations of Π_3. Hence if two words u and v are equivalent in Π_3 then the number of $\alpha\alpha$'s in both u and v are the same, i.e. two words have a balanced word $\alpha\alpha$. We show below that a slightly modified balanced letter argument in 2.1 solves the word problem on Π_3 generically.

Let $X = \{\alpha, \beta\}$. For $w \in X^*$, we count the number of $\alpha\alpha$'s in w in such a way that two occurrences of $\alpha\alpha$'s in w should not have a common α. For example, we count 1 $\alpha\alpha$ in $\alpha\alpha\alpha$. Let $B = \{(w_1, w_2) \in X^* \times X^* \mid \sigma_{\alpha^2}(w_1) = \sigma_{\alpha^2}(w_2)\}$. We claim that B is negligible in $X^* \times X^*$. As before, we work with the pair $(w, r) \in X^* \times \mathbb{N}$ for $(w_1, w_2) \in X^* \times X^*$ where $w = w_1 w_2$ and

$r = |w_1|$. We say a pair $(w, r) \in X^* \times \mathbb{N}$ α^2-balanced if $w = w_1 w_2$ for some $w_1, w_2 \in X^*$ and $\sigma_{\alpha^2}(w_1) = \sigma_{\alpha^2}(w_2)$. For each $w \in X^*$, define $\gamma_{\alpha^2}(w)$ to be the length of a maximal factor in w which does not contain $\alpha\alpha$'s.

Lemma 7. *Let $X = \{\alpha, \beta\}$. Let w be a word on X of length n. There are at most $\gamma_{\alpha^2}(w) + 1$ many α^2-balanced pairs in $(w, 0), \ldots, (w, n)$.*

Proof. Let w be a word on X of length n. If $(w, i) \in X^* \times \mathbb{N}$ is an α^2-balanced pair then w is a word of the form $w = uw'v$ where w' is a maximal factor between u and v that does not contain α^2 and u and v are factors of w such that $\sigma_{\alpha^2}(u) = \sigma_{\alpha^2}(v)$ or $\sigma_{\alpha^2}(u) = \sigma_{\alpha^2}(v) - 1$ or $\sigma_{\alpha^2}(u) = \sigma_{\alpha^2}(v) + 1$. If $\sigma_{\alpha^2}(u) = \sigma_{\alpha^2}(v)$ then there are at most $|w'| + 1$, which is less than $\gamma_{\alpha^2}(w) + 1$, many α^2-balanced pairs in $(w, 0), \cdots, (w, n)$. If $\sigma_{\alpha^2}(u) = \sigma_{\alpha^2}(v) - 1$ or $\sigma_{\alpha^2}(u) = \sigma_{\alpha^2}(v) + 1$ then there are at most $|w'|$, which is less than $\gamma_{\alpha^2}(w)$, many α^2-balanced pairs in $(w, 0), \cdots, (w, n)$. □

Lemma 8. *Let $X = \{\alpha, \beta\}$ and let $W_n = \{w \in X^* \mid |w| = n\}$. Then, for any positive integer $k \leq n$,*

$$|\{w \in W_n \mid \gamma_{\alpha^2}(w) \geq k\}| \leq 4(n-k)\left(\frac{1+\sqrt{5}}{2}\right)^k 2^{n-k}.$$

In particular, for a sufficiently large positive integer n, that is for every $n \geq$

$\lceil (log_2 n)^2 \rceil$,

$$|\{w \in W_n \mid \gamma_{\alpha^2}(w) \geq \lceil (log_2 n)^2 \rceil\}| \leq 4(n - \lceil (log_2 n)^2 \rceil) \left(\frac{1+\sqrt{5}}{2}\right)^{\lceil (log_2 n)^2 \rceil} 2^{n - \lceil (log_2 n)^2 \rceil}.$$

Proof. Let w be a word of length n in X^* and let w' be a factor of w of the maximal length which does not contain $\alpha\alpha$'s. Assume that the length of w' is k. Let us count the number of words of length k which does not contain $\alpha\alpha$, which we denote by u_k. If $k = 1$ then there are only two words α and β, hence the number of $u_1 = 2$. If $k = 2$ then there are three words which do not contain an $\alpha\alpha$, that is, $\alpha\beta, \beta\alpha, \beta\beta$, hence $u_2 = 3$. Suppose $k \geq 3$. Let a_k be the number of factors w' of the length k which ends with α, i.e, the last letter of the factor is α, and let b_k be the number of factors w' of length k which ends with β, so $u_k = a_k + b_k$. Observe that $b_k = u_{k-1}$ and $a_k = b_{k-1}$, hence $a_k = u_{k-2}$. Therefore $u_k = u_{k-1} + u_{k-2}$, which is the Fibonacci sequence whose first two terms are $u_1 = 2$ and $u_2 = 3$ and, hence, the formula of u_k is

$$u_k = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^{k+3} - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^{k+3}.$$

Since

$$u_k \leq \frac{2}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^3 \left(\frac{1+\sqrt{5}}{2}\right)^k \leq 4 \left(\frac{1+\sqrt{5}}{2}\right)^k,$$

the number of factors w' of length k which does not contain $\alpha\alpha$'s is bounded above by $4\left(\frac{1+\sqrt{5}}{2}\right)^k$.

Assume now that w' that does not contain $\alpha\alpha$'s is placed at the beginning of w. Then the number of words in X^* with initial factor w', which has a length at least k, is bounded above by $4\left(\frac{1+\sqrt{5}}{2}\right)^k 2^{n-k}$. w' can be placed in any $n-k$ position and the same upper bound works for each position. Hence the Lemma is true. □

Proposition 3. *Let* Π_3 *be the Matiyasevich semigroup presented by*

$$\Pi_3 = <\ \alpha, \beta \mid \alpha\alpha\beta\beta = \beta\alpha\alpha,\ \beta\alpha\alpha = \alpha\alpha\beta\alpha\beta,\ \tau(A) = \tau(B)\ > .$$

The word problem on Π_3 *is generically solvable by a linear time partial algorithm.*

Proof. Let $X = \{\alpha, \beta\}$. We show that $B = \{(w_1, w_2) \in X^* \times X^* \mid \sigma_{\alpha^2}(w_1) = \sigma_{\alpha^2}(w_2)\}$ is negligible in $X^* \times X^*$, hence counting $\alpha\alpha$s in words $w_1, w_2 \in X^*$ solves the word problem generically.

A sphere of radius n in $X^* \times X^*$, $S(n)$, is equinumerous to the set

$$S_n = \{(w, r) \mid w \in X^*, |w| = n,\ 0 \leq r \leq n\} = \{w \in X^* \mid |w| = n\} \times \{0, \ldots, n\}.$$

Let $B_n = \{(w, r) \in S_n \mid w = w_1 w_2$ for some $w_1, w_2 \in X^*, |w_1| = r$ and $\sigma_{\alpha^2}(w_1) = \sigma_{\alpha^2}(w_2)\}$. By Lemma 7 there are at most $\gamma_{\alpha^2}(w) + 1$ pairs of α^2-balanced

words in $(w,0),\cdots,(w,n)$. Combining that fact and Lemma 8, one obtains the following upper bound for the number of pairs of balanced words in S_n:

$$|B_n| \leq \lceil (log_2 n)^2 \rceil 2^n + 4(n+1)(n - \lceil (log_2 n)^2 \rceil) \left(\frac{1+\sqrt{5}}{2} \right)^{\lceil (log_2 n)^2 \rceil} 2^{n - \lceil (log_2 n)^2 \rceil}.$$

Hence

$$\frac{|B_n|}{|S_n|} \leq \frac{\lceil (log_2 n)^2 \rceil 2^n + 4(n+1)(n - \lceil (log_2 n)^2 \rceil) \left(\frac{1+\sqrt{5}}{2} \right)^{\lceil (log_2 n)^2 \rceil} 2^{n - \lceil (log_2 n)^2 \rceil}}{(n+1)2^n} \tag{2.4.1}$$

$$= \frac{\lceil (log_2 n)^2 \rceil}{(n+1)} + 4(n - \lceil (log_2 n)^2 \rceil) \left(\frac{1+\sqrt{5}}{4} \right)^{\lceil (log_2 n)^2 \rceil} \tag{2.4.2}$$

Since (2.4.1) converges to 0 as $n \to \infty$, B is negligible in $X^* \times X^*$. This proves the proposition. □

Chapter 3

Balanced group

3.1 Introduction

For groups, we cannot use the method on the word problem for semigroups to find a generic solution because of inverse elements. For example, the relation $ab = ba^2$ has a balanced letter b, but an equivalent relation $b^{-1}ab = a^2$ doesn't have a balanced letter. So we don't have a 'semigroup type' balanced letter of defining relations in groups. However, we can define a balanced letter for groups, that is, a letter whose sum of positive exponents and negative exponents in the left hand side of the relation is the same as that of the right hand side of the relation, as b in $b^{-1}ab = a^2$. We define the balanced letter

in groups more precisely as follows.

3.2 Balanced group presentations

Let X be a finite set of letters that contains at least two letters. Let $a \in X$. Let l and r be freely reduced words on X. In groups, the relation $l = r$ is equivalent to $lr^{-1} = 1$, so we will consider only the relations of the type $r = 1$. We define a balanced relation in a group in the following way: we say a relation $r = 1$ is a-balanced and a is a balanced letter if $\sigma_a(r) = \sigma_{a^{-1}}(r)$, i.e, r has the same number of a's and a^{-1}'s in it. Observe that if r coincides graphically with $r_1 r_2$ and r is a-balanced, then $\sigma_a(r_1) - \sigma_{a^{-1}}(r_1) = \sigma_a(r_2^{-1}) - \sigma_{a^{-1}}(r_2^{-1})$, thus if $l = l'$ is a relation that is equivalent to an a-balanced relation $r = 1$ then the difference of the number of a's and a^{-1}'s in l is the same as the one in l'.

Let R be a set of defining relations of the form $R = \{r_i = 1 \mid i \in I\}$, where r_i are words from X and $|I| < \infty$. If all relations $r_i = 1$ in R are a-balanced relations, we call R a-balanced. If G is a group presented by $G = < X \mid R >$ with a-balanced R , then we call G a-balanced.

Lemma 9. *Let X be a finite set, not empty, and let $a \in X$. Let $G = < X \mid R >$ be an a-balanced group and let u be a word on X. If $u =_G 1$ then $\sigma_a(u) = \sigma_{a^{-1}}(u)$.*

Proof. If $u =_G 1$, there is a finite sequence of transformations of words $u = u_1 \to u_2 \to \cdots \to u_k = 1$ where $u_i \to u_{i+1}$ means that u_{i+1} is obtained from u_i by applying a relation that is equivalent to $r_j = 1 \in R$. Since $\sigma_a(u_i) - \sigma_{a^{-1}}(u_i) = \sigma_a(u_{i+1}) - \sigma_{a^{-1}}(u_{i+1})$ for $1 \leq i \leq k-1$ and $\sigma_a(1) - \sigma_{a^{-1}}(1) = 0$, the lemma is true. □

As in semigroups, it turns out that the word problem on groups which have 'group type' balanced relations is generically solvable. Interestingly, among these groups are groups with unsolvable word problem including Novikov's group.

In groups, the word problem is equivalent to the identity problem, so we consider the identity problem instead of the word problem.

Proposition 4. *Let X be a finite set containing at least two letters and let $a \in X$. Let $B_a^X := \{u \in (X \cup X^{-1})^* \mid \sigma_a(u) = \sigma_{a^{-1}}(u)\}$. Then B_a^X is negligible in $(X \cup X^{-1})^*$.*

Proof. Let $S(n) = \{u \in (X \cup X^{-1})^* \mid |u| = n)\}$ and let $(B_a^X)_n = \{v \in$

$S(n) \mid \sigma_a(v) = \sigma_{a^{-1}}(v)\}$. Suppose $X = \{a, a_2, \cdots, a_k\}$ with $k \geq 2$. The number of all group words u randomly generated from $X \cup X^{-1}$ with the length n is $(2k)^n$ and the number of all group words u on $X \cup X^{-1}$ such that its length is n and $\sigma_a(u) = \sigma_{a^{-1}}(u) = i$ is $\binom{n}{i}\binom{n-i}{i}(2k-2)^{n-2i}$. Thus the number of all group words u whose length is n and $\sigma_a(u) = \sigma_{a^{-1}}(u)$ is

$$\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{i}\binom{n-i}{i}(2k-2)^{n-2i}.$$

If we show that

$$\frac{\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{i}\binom{n-i}{i}(2k-2)^{n-2i}}{(2k)^n} \to 0$$

as $n \to \infty$ then we are done. Since $\binom{n}{i}\binom{n-i}{i} = \binom{n}{2i}\binom{2i}{i}$,

$$\frac{\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{i}\binom{n-i}{i}(2k-2)^{n-2i}}{(2k)^n} = \frac{\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i}\binom{2i}{i}(2k-2)^{n-2i}}{(2k)^n} \tag{3.2.1}$$

Since $2k - 2 \geq 2$, the righthand side of (3.2.1) converges to 0 as $n \to \infty$ by the following Lemmas.

Lemma 10 (Chebyshev's sum inequality)**.** *If $\{a_i\}_{i=1}^n, \{b_i\}_{i=1}^n$ are sequences of positive numbers such that $a_1 \geq a_2 \geq \cdots \geq a_n$ and $b_1 \geq b_2 \geq \cdots \geq b_n$ then*

$$n\sum_{i=1}^{n} a_i b_i \geq \sum_{i=1}^{n} a_i \cdot \sum_{i=1}^{n} b_i.$$

If $\{a_i\}_{i=1}^n, \{b_i\}_{i=1}^n$ *are sequences of positive numbers such that* $a_1 \geq a_2 \geq \cdots \geq a_n$ *and* $b_1 \leq b_2 \leq \cdots \leq b_n$ *then*

$$\sum_{i=1}^{n} a_i b_i \leq \frac{\sum_{i=1}^n a_i \cdot \sum_{i=1}^n b_i}{n}.$$

Lemma 11. *For any real number* $k \geq 1$,

$$\lim_{n\to\infty} \frac{\sum_{i=0}^{[\frac{n}{2}]} \binom{n}{2i}\binom{2i}{i}(2k)^{n-2i}}{(2k+2)^n} = 0. \tag{3.2.2}$$

Proof.

$$\frac{\sum_{i=0}^{[\frac{n}{2}]} \binom{n}{2i}\binom{2i}{i}(2k)^{n-2i}}{(2k+2)^n} = \frac{\sum_{i=0}^{[\frac{n}{2}]} \binom{n}{2i} k^{n-2i} \frac{\binom{2i}{i}}{2^{2i}}}{(k+1)^n}$$

Observe that

$$\frac{\binom{2i}{i}}{2^{2i}} \leq \frac{1}{\sqrt{2i+1}}$$

since

$$\begin{aligned}
\frac{\binom{2i}{i}}{2^{2i}} &= \frac{(2i)!}{(i!)^2} \cdot \frac{1}{2^{2i}} = \frac{2i-1}{2i} \cdot \frac{2i-3}{2i-2} \cdots \frac{1}{2} \\
&\leq \sqrt{\frac{2i-1}{2i} \cdot \frac{2i-3}{2i-2} \cdots \frac{1}{2}} \sqrt{\frac{2i}{2i+1} \cdot \frac{2i-2}{2i-1} \cdots \frac{2}{3}} \\
&= \frac{1}{\sqrt{2i+1}}
\end{aligned}$$

Hence

$$\frac{\sum_{i=0}^{[\frac{n}{2}]} \binom{n}{2i} k^{n-2i} \frac{\binom{2i}{i}}{2^{2i}}}{(k+1)^n} \leq \frac{\sum_{i=0}^{[\frac{n}{2}]} \binom{n}{2i} k^{n-2i} \frac{1}{\sqrt{2i+1}}}{(k+1)^n} \tag{3.2.3}$$

Consider the ratio of two terms in $\sum_{i=0}^{[\frac{n}{2}]} \binom{n}{2i} k^{n-2i}$.

$$\frac{\binom{n}{2i+2} k^{n-2i-2}}{\binom{n}{2i} k^{n-2i}} = \frac{(n-2i)(n-2i-1)}{(2i+2)(2i+1)} \cdot \frac{1}{k^2}.$$

Thus if $\frac{n-2i}{2i+2} > k \geq 1$, then, from $\frac{n-2i}{2i+2} > 1$, $\frac{n-2i-1}{2i+1} > \frac{n-2i}{2i+2} > k$ and hence

$$\frac{\binom{n}{2i+2}k^{n-2i-2}}{\binom{n}{2i}k^{n-2i}} > k \cdot k \cdot \frac{1}{k^2} = 1. \tag{3.2.4}$$

By (3.2.4), for each i satisfying $\frac{n-2i}{2i+2} > k$, that is, $i < \lfloor \frac{\frac{n}{2}+1}{k+1} - 1 \rfloor$, $\binom{n}{2i}k^{2i} < \binom{n}{2i+2}k^{n-2i-i}$. Hence,

$$k^n < \binom{n}{2}k^{n-2} < \cdots < \binom{n}{2\lfloor \frac{\frac{n}{2}+1}{k+1} \rfloor}k^{n-2\lfloor \frac{\frac{n}{2}+1}{k+1} \rfloor}. \tag{3.2.5}$$

Now the numerator of the right-hand side of (3.2.3) is

$$\sum_{i=0}^{[\frac{n}{2}]} \binom{n}{2i}k^{n-2i}\frac{1}{\sqrt{2i+1}} = \tag{3.2.6}$$

$$k^n + \binom{n}{2}k^{n-2}\frac{1}{\sqrt{3}} + \cdots + \binom{n}{2\lfloor \frac{\frac{n}{2}+1}{k+1} \rfloor}k^{n-2\lfloor \frac{\frac{n}{2}+1}{k+1} \rfloor}\frac{1}{\sqrt{2\lfloor \frac{\frac{n}{2}+1}{k+1} \rfloor + 1}} \tag{3.2.7}$$

$$+ \binom{n}{2\lfloor \frac{\frac{n}{2}+1}{k+1} \rfloor + 2}k^{n-2\lfloor \frac{\frac{n}{2}+1}{k+1} \rfloor - 2}\frac{1}{\sqrt{2\lfloor \frac{\frac{n}{2}+1}{k+1} \rfloor + 3}} + \cdots + \binom{n}{2\lfloor \frac{n}{2} \rfloor}k^{n-2\lfloor \frac{n}{2} \rfloor}\frac{1}{\sqrt{2\lfloor \frac{n}{2} \rfloor + 1}}$$

$$\tag{3.2.8}$$

Since

$$1 > \frac{1}{\sqrt{3}} > \frac{1}{\sqrt{5}} > \cdots > \frac{1}{\sqrt{2\lfloor \frac{\frac{n}{2}+1}{k+1} \rfloor + 1}}, \tag{3.2.9}$$

by combining (3.2.5) and (3.2.9) with Chebyshev's sum inequality, one obtains an upperbound for (3.2.7);

$$k^n + \binom{n}{2}k^{n-2}\frac{1}{\sqrt{3}} + \cdots + \binom{n}{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor}k^{n-2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor}\frac{1}{\sqrt{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+1}} \tag{3.2.10}$$

$$\leq \left(\frac{1}{\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+1}\right)\left(1+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+1}}\right)$$
$$\left(k^n + \binom{n}{2}k^{n-2} + \cdots\cdots + \binom{n}{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor}k^{n-2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor}\right)$$
$$\leq \frac{\sqrt{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+3}}{\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+1}\left(k^n + \binom{n}{2}k^{n-2} + \cdots + \binom{n}{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor}k^{n-2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor}\right) \tag{3.2.11}$$

since

$$\begin{aligned}1+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+1}} &< 1+\int_1^{\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+1}\frac{dx}{\sqrt{2x+1}}\\ &= \sqrt{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+3}-\sqrt{3}+1\\ &< \sqrt{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+3}\end{aligned} \tag{3.2.12}$$

On the other hand, it is obvious that the summation (3.2.8) has an upperbound as below;

$$\binom{n}{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+2}k^{n-2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor-2}\frac{1}{\sqrt{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+3}} + \cdots + \binom{n}{2\lfloor\frac{n}{2}\rfloor}k^{n-2\lfloor\frac{n}{2}\rfloor}\frac{1}{\sqrt{2\lfloor\frac{n}{2}\rfloor+1}}$$
$$\leq \frac{1}{\sqrt{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+3}}\left(\binom{n}{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+2}k^{n-2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor-2} + \cdots + \binom{n}{2\lfloor\frac{n}{2}\rfloor}k^{n-2\lfloor\frac{n}{2}\rfloor}\right) \tag{3.2.13}$$

Hence, combining (3.2.12) and (3.2.13), we obtain an upperbound of (3.2.6);

$$\sum_{i=0}^{[\frac{n}{2}]} \binom{n}{2i} k^{n-2i} \frac{1}{\sqrt{2i+1}}$$

$$\begin{aligned}
&\leq Max\{\frac{\sqrt{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+3}}{\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+1}, \frac{1}{\sqrt{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+3}}\}\{k^n + \binom{n}{2}k^{n-2} + \cdots + \binom{n}{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor}k^{n-2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor} \\
&+ \binom{n}{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+2}k^{n-2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor-2} + \cdots + \binom{n}{2\lfloor\frac{n}{2}\rfloor}k^{n-2\lfloor\frac{n}{2}\rfloor}\} \\
&= \frac{\sqrt{2\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+3}}{\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+1}\sum_{i=0}^{[\frac{n}{2}]}\binom{n}{2i}k^{n-2i} \leq \sqrt{\frac{3}{\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+1}}\sum_{i=0}^{[\frac{n}{2}]}\binom{n}{2i}k^{n-2i}
\end{aligned}$$

Now,

$$\frac{\sum_{i=0}^{[\frac{n}{2}]}\binom{n}{2i}k^{n-2i}\frac{1}{\sqrt{2i+1}}}{(k+1)^n} \leq \frac{\sum_{i=0}^{[\frac{n}{2}]}\binom{n}{2i}k^{n-2i}\frac{1}{\sqrt{2i+1}}}{\sum_{i=0}^{[\frac{n}{2}]}\binom{n}{2i}k^{n-2i}} \leq \sqrt{\frac{3}{\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+1}} \tag{3.2.14}$$

Since $\sqrt{\frac{3}{\lfloor\frac{\frac{n}{2}+1}{k+1}\rfloor+1}} \to 0$ as $n \to \infty$, this proves the lemma. □

Hence the Proposition 4 is true.

□

By the Proposition 4, we have the following theorem.

Theorem 3.2.1. *Let G be a finitely generated group with balanced relations. The word problem in G is generically solvable by a linear time partial algorithm.*

3.3 Groups with unsolvable word problem

We list groups with unsolvable word problem which have balanced relations. Using Proposition 4, one can determine the word problem for these groups generically.

Example 3.3.1. *In 1955, P.S. Novikov first constructed a group G_N with unsolvable word problem as follows; Let $\Gamma =< g_1, g_2, \cdots, g_n \mid L_1 = R_1, \cdots, L_m = R_m >$ be a semigroup such that L_i, R_i for $1 \leq i \leq m$ are not the empty word and, for some word u, the problem of deciding whether $X = u$ is unsolvable. Let G_N be a group presented by $G_N = < g_1, \cdots, g_n, l, r, c, t, k \mid R_{G_N} >$ where R_{G_N} consists of the following relations;*

$$g_i l = l^{m+1} g_i, \quad r g_i = g_i r^{m+1} \text{ for } 1 \leq i \leq n,$$

$$c g_i = g_i c, \quad (l^i L_i r^i)c = c(l^i R_i r^i) \text{ for } 1 \leq i \leq m,$$

$$ct = tc, \quad lt = tl, \quad ck = kc, \quad kr = kr, \quad (q^{-1}tq)k = k(q^{-1}tq).$$

Then G_N has an unsolvable word problem.

Example 3.3.2. *In 1956, Boone constructed a finitely presented group with unsolvable word problem as the following;*

Let S_B be a semigroup with unsolvable word problem presented as below.

$$S_B =< s_1, \cdots, s_M, q_1, \cdots, q_N, q \mid \Sigma_1 = \Gamma_1, \cdots, \Sigma_P = \Gamma_P >,$$

where each Σ_i *and* $\Gamma_i, i = 1, \cdots, P$, *is of the form* $\Delta q_\alpha \Pi$, Δ *and* Π *being words on* $s_1, \cdots, s_M$ *and* q_α *being* $q_1, \cdots q_N$, *or* q. *Let* $X_B = \{s_1, \cdots, s_M, q_1, \cdots, q_N, q\}$ *and let* $R_B = \{\ \Sigma_1 = \Gamma_1, \cdots, \Sigma_P = \Gamma_P\}$. *The group* G_{BN} *is presented as below.*

$$G_{BN} = <X_B, t_1, t_2, k, x, y, l_i, r_i \mid R_B,\ \Sigma_i = l_i\Gamma_i r_i,\ s_\beta l_i = y l_i y s_\beta,\ s_\beta y = yys_\beta,$$
$$t_\alpha l_i = l_i t_\alpha,\ t_\alpha y = y t_\alpha,\ r_i s_\beta = s_\beta x r_i x,\ x s_\beta = s_\beta x x,\ r_i k = k r_i,$$
$$xk = kx,\ kq^{-1}t_1^{-1}q = q^{-1}t_1^{-1}t_2 qk > .$$

Example 3.3.3. *Borisov constructed a group with unsolvable word problem with* 10 *generators and* 27 *relations:*

$$G_{BR} = \langle a, b, c, d, e, p, q, r, t, k \mid p^{10}a = ap,\ p^{10}b = bp,\ p^{10}c = cp,\ p^{10}d = dp,$$
$$p^{10}e = ep,\ qa = aq^{10},\ qb = bq^{10},\ qc = cq^{10},\ qd = dq^{10},\ qe = eq^{10},\ ra = ar,$$
$$rb = br,\ rc = cr,\ rd = dr,\ re = er,\ pacqr = rpcaq,\ p^2adq^2r = rp^2daq^2,$$
$$p^3bcq^3r = rp^3cbq^3,\ p^4bdq^4r = rp^4dbq^4,\ p^5ceq^5r = rq^5ecaq^5,$$
$$p^6deq^6r = rp^6edbq^6,\ p^7cdcq^7r = p^7cdceq^7,\ p^8caaaq^8r = rp^8aaaq^8,$$
$$p^9daaaq^9r = rp^9aaaq^9,\ pt = tp,\ qt = tq,\ k(aaa)^{-1}t(aaa) = (aaa)^{-1}t(aaa)k\rangle. \tag{3.3.1}$$

Example 3.3.4. *Collins constructed a group with 14 defining relations that has an unsolvable word problem. Collins' construction is as below:*

Let $S = < s_1, \cdots, s_M \mid L_1 = R_1, \cdots, L_N = R_N >$ *be a Thue system with* M *generators and* N *defining relations. From* S*, we define a Thue system* $S_* = < s_1, \cdots, s_M, q \mid L_1 q = qR_1, \cdots,\ qL_N = qR_N,\ s_1 q = qs_1, \cdots,\ s_M q = qs_M\ >$ *. Let* u_0 *be a word in* S*. Then Collins' group has the following presentation:*

$$
\begin{aligned}
G_C = < s_1, \cdots, s_M, q, k, t, a, d \mid & \\
& as_1 = s_1 a,\ \cdots,\ as_M = s_M a, \\
& ds_1 = s_1 d^{M+N+1} a d^{M+N+1},\ \cdots,\ ds_M = s_M d^{M+N+1} a d^{M+N+1}, \\
& \overline{L_i} q = d^{-i} a^{-1} d^{-1} q R_i d^i a d^i,\ \textit{for } 1 \le i \le M+N \\
& s_i^{-1} q = d^{-i} a^{-1} d^{-1} q s_i d^i a d^i,\ \textit{for } 1 \le i \le M+N \\
& ta = at, \qquad td = dt, \\
& ka = ak, \qquad kd = dk, \\
& k(u_0^{-1} q^{-1} t q u_0) = (u_0^{-1} q^{-1} t q u_0) k >
\end{aligned}
$$

where $\overline{L_i}$ *is obtained from* L_i *by replacing* s_j*'s by* s_j^{-1} *for* $1 \le j \le M$*.*

Collins showed that G_C *has an unsolvable word problem if the individual word problem to decide whether* $w = u_0$ *is unsolvable in* S*. Observe that* G_C *has* $3M + N + 5$ *defining relations. By choosing* S *to be a Matiyasevich semigroup, which has two generators and three defining relations, Collins*

obtained a group with 14 defining relations which has an unsolvable word problem.

Proposition 5. *The word problem for groups G_N, G_{BN}, G_{BR} and G_C in example 3.3.1, 3.3.2, 3.3.3 and 3.3.4 are generically solvable by a linear time partial algorithm.*

Proof. In G_N, the letters c, t, k among generators of G_N act as balanced letters. In G_{BN}, the letters q and k are balanced letters In G_{BR}, the letters t and k are balanced letters. In G_C, q, k, t are balanced letters. Hence, by Theorem 3.2.1, the word problem for G_N, G_{BR}, G_{BN} and G_C is generically solvable. □

Chapter 4

Conjugacy problem in HNN extensions

In this chapter we present an algorithm to compute a normal form and cyclically reduced normal form of an element in an HNN extension of a finitely presented group provided that the base group accepts an algorithm. After that we define the black hole in the HNN-extension and show that the conjugacy problem is decidable for 'regular type' elements in the HNN-extension of a group provided that the HNN extension accepts a few algorithms.

4.1 Some preliminary definitions and theorems in HNN extensions

Let G be a finitely presented group, let A, B be subgroups of G and let $\phi : A \to B$ be an isomorphism. Let $G^* = \langle\ G, t \mid t^{-1}at = \phi(a), a \in A\ \rangle$ be an HNN-extension of G. In this chapter G^* is used as an HNN-extension of G as above unless otherwise stated. Some preliminary definitions and theorems about HNN extensions of groups are the following;

Definition 4.1.1. Let $G^* = \langle\ G, t \mid t^{-1}at = \phi(a), a \in A\ \rangle$ be an HNN-extension of a group G and let $g \in G^*$. We say g is reduced if either $g \in G$ or g is a word of the form $g = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots t^{\varepsilon_n} g_n$ where

1. $\varepsilon_i = 1$ or -1 for all $i \in \{1, 2, \cdots, n\}$.

2. If $\varepsilon_i = -1$ and $\varepsilon_{i+1} = 1$ then $g_i \notin A$. If $\varepsilon_i = 1$ and $\varepsilon_{i+1} = -1$ then $g_i \notin B$.

For each reduced word $g = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots t^{\varepsilon_n} g_n \in G^*$, we define the length of g to be $\sum_{i=1}^{n} |\varepsilon_i|$, which we denote by $|g|$.

Lemma 12 (Britton's lemma)**.** *Let G^* be an HNN-extension of a group G and let $g \in G^*$. If $g = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots t^{\varepsilon_n} g_n$ is reduced and $n \geq 1$ then $g \neq 1$*

in G^*.

Definition 4.1.2. Let $G^* = \langle\ G, t \mid t^{-1}at = \phi(a), a \in A\ \rangle$ be an HNN-extension of a group G and let $g \in G^*$. We say g is a normal form if either $g \in G$ or g is a word of the form $g = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots t^{\varepsilon_n} g_n$ where

1. $\varepsilon_i = 1$ or -1 for all $i \in \{1, 2, \cdots, n\}$.
2. $g_0 \in G$.
3. If $\varepsilon_i = -1$ then g_i is a coset representative of A in G.
4. If $\varepsilon_i = 1$ then g_i is a coset representative of $B = \phi(A)$ in G.
5. If $\varepsilon_i \varepsilon_{i+1} = -1$ then $g_i \neq 1$.

Theorem 4.1.1 (The Normal Form Theorem for HNN Extension)**.** *Every element g in G^* has a unique representation as a normal form $g = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_1} \cdots t^{\varepsilon_n} g_n$ $(n \geq 0)$.*

Definition 4.1.3. An element $g = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_1} \cdots t^{\varepsilon_n}$ in G^* is called cyclically reduced if all cyclic permutations of $g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_1} \cdots t^{\varepsilon_n}$ with respect to g_i, t^{ε_j}'s are reduced.

Theorem 4.1.2 (The Conjugacy Theorem for HNN Extension)**.** *Let*

$$G^* = \left\langle\ G, t \mid t^{-1}at = \phi(a), a \in A\ \right\rangle$$

be an HNN-extension of a group G. Let $u = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_1} \cdots t^{\varepsilon_n}$, $n \geq 1$ and v be two cyclically reduced elements in G^*. If u, v are conjugate in G^*, then $|u| = |v|$ and u can be obtained from v by taking a suitable cyclic permutation of v, which ends in t^{ε_n}, and then conjugating by an element z, where $z \in A$ if $\varepsilon_n = -1$ and $z \in B$ if $\varepsilon_n = 1$.

4.2 Algorithms to compute normal forms and cyclically reduced normal forms

Let

$$\begin{aligned} G^* &= \langle\ G, t \mid t^{-1}at = \phi(a), a \in A\ \rangle \\ &= \langle\ X, t \mid R_G = 1, t^{-1}at = \phi(a), a \in A\ \rangle, \end{aligned}$$

where $G = \langle\ X \mid\ R_G = 1\ \rangle$ is a finitely presented group and A is a subgroup of G.

In this section we describe an algorithm to compute a normal form of an element in G^* provided that the Coset Representatives Search Problem (CRSP) Algorithm for A and $B = \phi(A)$ in G are given.

Algorithm 4.2.1 (Computing normal form)**.** INPUT: $g \in F(X \cup t)$.

OUTPUT: $g = g_0 t^{\varepsilon_1} g_1 \cdots t^{\varepsilon_n} g_n$, *which is reduced,* $g_0 \in G, \varepsilon_i \in \{1, -1\}$, g_i*'s,* $i \geq 1$, *are coset representatives of* G *modulo* A *or* B *depending on* ε_i *and* $g_i \neq 1$ *if* $\varepsilon_i \varepsilon_{i+1} = -1$ *for* $1 \leq i \leq n-1$.

SIGNATURE: $Normalform(g)$

COMPUTATIONS:

1. *Present* g *as a word of the form* $g = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} \cdots t^{\varepsilon_k} g_k$ *where each* $g_i, 1 \leq i \leq k$, *is a reduced word in* X, $\varepsilon_i \in \{\pm 1\}$.

   Induction on i*:* i *runs from* k *to* 1.

2. *If* $\varepsilon_i = -1$ *then rewrite* $g_i = a_i u_i$ *(using the CRSP algorithm) where* $a_i \in A$ *and* $u_k \in S$, S *is a set of representatives of coset of* A *in* G. *Then put* $t^{\varepsilon_i} g_i = t^{-1} a_i u_i =: \phi(a_i) t^{-1} u_i$.

   If $u_i = 1$ *and* $\varepsilon_{i+1} = 1$ *then put* $t^{\varepsilon_i} g_i t^{\varepsilon_{i+1}} g_{i+1} =: \phi(a_i) g_{i+1}$.

3. *If* $\varepsilon_i = 1$ *then rewrite* $g_i = b_i v_i$ *(using the CRSP algorithm) where* $b_i \in B$ *and* $v_k \in S'$, S' *is a set representatives coset of* B *in* G. *Then put* $t^{\varepsilon_i} g_i = t b_i v_i =: \phi^{-1}(b_i) t v_i$.

   If $v_i = 1$ *and* $\varepsilon_{i+1} = -1$ *then put* $t^{\varepsilon_i} g_i t^{\varepsilon_{i+1}} g_{i+1} =: \phi^{-1}(b_i) g_{i+1}$.

4. *Run 1 to 3 again until the number of* $t^{\pm 1}$ *can not be reduced further.*

Algorithm 4.2.2 (Computing cyclically reduced normal form)**.** INPUT: $g \in F(X \cup t)$.

OUTPUT: $g = g_0 t^{\varepsilon_1} g_1 \cdots g_{n-1} t^{\varepsilon_n}$ *is reduced,* $g_0 \in G, \varepsilon_i \in \{1, -1\}$*,* g_i*'s,* $i \geq 1$*, are coset representatives of* G *modulo* A *or* B *depending on* ε_i*, and* $\varepsilon_1 \varepsilon_n = 1$.

SIGNATURE: $CycNormalform(g)$

COMPUTATIONS:

1. *Put* $g := Normalform(g)$ *using algorithm 4.2.1. Let* $g = g_0 t^{\varepsilon_1} g_1 \cdots g_{k-1} t^{\varepsilon_n} g_n$.

2. *Put* $g_0 := g_n g_0$*, reduce* g_0 *and* $g =: g_0 t^{\varepsilon_1} g_1 \cdots g_{n-1} t^{\varepsilon_n}$.

   If $k \geq 2$ *then*

3. *If* $\varepsilon_1 \varepsilon_n = -1$ *then*

   (a) *If* $g_0 = 1$ *then put* $g := g_{n-1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-2} t^{\varepsilon_{n-1}}$. *Return to 2.*

   (b) *If* $g_0 = a_0 \in A \backslash \{1\}$ *and* $\varepsilon_n = -1$ *then put* $g := \phi(a_0) g_1 t^{\varepsilon_2} \cdots t^{\varepsilon_{n-1}} g_{n-1}$.

   Return to 2.

   (c) *If* $g_0 = b_0 \in B \backslash \{1\}$ *and* $\varepsilon_n = 1$ *then put* $g := \phi^{-1}(b_0) g_1 t^{\varepsilon_2} \cdots t^{\varepsilon_{n-1}} g_{n-1}$.

   Return to 2.

4.3 Regular elements in HNN extensions

In this section we define and study regular elements in G^*. They are elements that accept a good algorithm for conjugacy search problem, which is the subject of the next section. We conclude this section by showing that regularity of elements in G^* is decidable provided that G^* accepts a few algorithms.

Definition 4.3.1. $(s, g) \in G^* \times G^*$ is called a bad pair if $s \in A \cup B$, $g \in G^* \setminus (A \cup B)$, and $gsg^{-1} \in A \cup B$.

Lemma 13. *Let $s \in A \cup B \setminus \{1\}$ and let $g \in G^* \setminus (A \cup B)$. If $g = g_0 t^{\varepsilon_1} g_1 \cdots g_{n-1} t^{\varepsilon_n}, n \geq 1$, is a word of cyclically reduced normal form in G^* then (s, g) is a bad pair if and only if the following system of equations $S_{g,g}$ has a solution $(s, s_2, \cdots, s_{2n+1})$ in $\prod_{n=1}^{2n+1} S_i$ where $S_i = A$ or B for $1 \leq i \leq 2n$ and $S_{2n+1} = A \cup B$.*

$$t^{\varepsilon_n} x_1 t^{-\varepsilon_n} = x_2 \tag{4.3.1}$$

$$g_{n-1} x_2 g_{n-1}^{-1} = x_3$$

$$t^{\varepsilon_{n-1}} x_3 t^{-\varepsilon_{n-1}} = x_4$$

$$\vdots$$

$$t^{\varepsilon_1} x_{2n-1} t^{-\varepsilon_1} = x_{2n}$$

$$g_0 x_{2n} g_0^{-1} = x_{2n+1}$$

Proof. Directly follows from the Lemma 14 when g' is replaced by g in the Lemma 14. □

Definition 4.3.2. Let G be a group and let A be a set of G. The generalized normalizer of A in G, which we denote by $N_G^*(A)$, is the set defined as $N_G^*(A) = \{\ g \in G \mid A \cap A^g \neq 1\ \}$

Definition 4.3.3. The set $BH = N_{G^*}^*(A \cup B)$ is called a black hole. Elements in BH are called singular, and elements that are not singular are called regular.

Hence if (g, c) is a bad pair then both g and c are in the set BH.

Lemma 14. *Let $g = g_0 t^{\varepsilon_1} g_1 \cdots g_{n-1} t^{\varepsilon_n}$ and $g' = g'_0 t^{\delta_1} g'_1 \cdots g'_{n-1} t^{\delta_n}, (n \geq 1)$ be two words of cyclically reduced normal form in G^*. Then the equation $gx = x'g'$ has a solution $s, s' \in A \cup B$ if and only if the following system of equations $S_{g,g'}$ has a solution $(s_1, s_2, \cdots, s_{2n}, s_{2n+1}) = (s, s_2, \cdots, s_{2n}, s')$ in*

$\prod_{n=1}^{2n+1} S_i$, *where* $S_i = A$ *or* B *for* $1 \leq i \leq 2n$ *and* $S_{2n+1} = A \cup B$;

$$t^{\varepsilon_n} x_1 = x_2 t^{\delta_n} \tag{4.3.2}$$

$$g_{n-1} x_2 = x_3 g'_{n-1}$$

$$t^{\varepsilon_{n-1}} x_3 = x_4 t^{\delta_{n-1}}$$

$$\vdots$$

$$t^{\varepsilon_1} x_{2n-1} = x_{2n} t^{\delta_1}$$

$$g_0 x_{2n} = x_{2n+1} g'_0$$

Proof. Let s, s' be a solution of $gx = x'g'$. Then $gs = s'g'$, which is

$$g_0 t^{\varepsilon_1} g_1 \cdots g_{n-1} t^{\varepsilon_n} s = s' g'_0 t^{\delta_1} g'_1 \cdots g'_{n-1} t^{\delta_n}. \tag{4.3.3}$$

Note that the right hand side of the equation 4.3.3 is already a cyclically reduced normal form. Thus applying the Algorithm 4.2.1, we can rewrite the left hand side of the equation 4.3.3 into its canonical normal form. That process is to find a solution $(s, s_2, \cdots, s_{2n}, s')$ of the system of equation $S_{g,g'}$. Note that $s_i \in A$ or B depending on ε_i. Conversely, if $(s_1, s_2, \cdots, s_{2n+1})$ is a solution of $S_{g,g'}$ then (s_1, s_{2n+1}) would be a solution of $gx = x'g'$. □

We use the following definition and lemma for characterizing the solution set of the system $S_{g,g'}$.

Definition 4.3.4. Let G be a group and let M be a subset of G. If $u, v \in G$ then uMv is called a G-shift of M. For a set μ of subgroups of G denote by $\Phi(\mu, G)$ the least set of subsets of G which contains μ and is closed under G-shift and intersections.

Lemma 15. *Let G be a group and let A be a subgroup of G. If $D \in \Phi(\{A\}, G)$ and $D \neq \emptyset$ then D is a set of the form $D = (A^{g_1} \cap \cdots \cap A^{g_n})k$ for some $g_1, \cdots, g_n, k \in G$. In particular, nonempty sets in $\Phi(\{A\}, G)$ are particular cosets from G.*

Proof. Induction on the number of operations that are used for D.

Observe that if C, D are two subgroups of G, $g, g' \in G$ and $h \in Cg \cap Dg'$ then $Cg \cap Dg' = (C \cap D)h$.

Now if $D = aAb$ for some $a, b \in G$ then $D = A^{a^{-1}}ab$. If $D = A^a h_1 \cap A^b h_2$ where $a, b, h_1, h_2 \in G$ and $h \in A^a h_1 \cap A^b h_2$ then $D = (A^a \cap A^b)h$.

Suppose $D = (A^{g_1} \cap \cdots \cap A^{g_m})k$ and $D' = (A^{g'_1} \cap \cdots \cap A^{g'_l})k'$ where $g_1, \cdots, g_m, g'_1, \cdots, g'_l, k \in G$. Then

$$\begin{aligned} aDb &= a(A^{g_1} \cap \cdots \cap A^{g_m})kb \\ &= (A^{g_1 a^{-1}} \cap \cdots \cap A^{g_m a^{-1}})akb \end{aligned}$$

and if $h \in (A^{g_1} \cap \cdots \cap A^{g_m})k \cap (A^{g'_1} \cap \cdots \cap A^{g'_l})k'$ then

$$\begin{aligned} D \cap D' &= (A^{g_1} \cap \cdots \cap A^{g_m})k \cap (A^{g'_1} \cap \cdots \cap A^{g'_l})k' \\ &= (A^{g_1} \cap \cdots \cap A^{g_m} \cap A^{g'_1} \cap \cdots \cap A^{g'_l})h. \end{aligned}$$

□

The following lemma characterizes the solution set of the system of equations $S_{g,g'}$.

Lemma 16. *Let G^* be an HNN-extension of a group G. Let $g = g_0 t^{\varepsilon_1} g_1 \cdots g_{n-1} t^{\varepsilon_n}$ and $g' = g'_0 t^{\delta_1} g'_1 \cdots g'_{n-1} t^{\delta_n}, (n \geq 1)$, be two elements of cyclically reduced normal form in G^*. Let $E_{g,g'}$ be the set of all $s \in A \cup B$ for which $S_{g,g'}$ has a solution $(s, s_2, \cdots, s_{2n}, s_{2n+1}) \in \prod_{j=1}^{2n+1} S_j$ where $S_i = A$ or B for $0 \leq i \leq 2n$ and $S_{2n+1} = A \cup B$. Then*

$$E_{g,g'} = S_1 \cap p_1^{-1} S_2 p'_1 \cap \cdots \cap p_1^{-1} p_2^{-1} \cdots p_{2n}^{-1} S_{2n+1} p'_{2n} \cdots p'_2 p'_1,$$

where $p_i = \begin{cases} g_{n-\frac{i}{2}}, & \text{if } i \text{ is even} \\ t^{\epsilon_n - \frac{i-1}{2}}, & \text{if } i \text{ is odd} \end{cases}$ *and* $p'_i = \begin{cases} g'_{n-\frac{i}{2}}, & \text{if } i \text{ is even} \\ t^{\delta_n - \frac{i-1}{2}}, & \text{if } i \text{ is odd} \end{cases}$.

In particular, if $E_{g,g'} \neq \emptyset$ then $E_{g,g'} = A_{g,g'} a_{g,g'}$ for some $A_{g,g'} < A$, $a_{g,g'} \in A$ or $E_{g,g'} = B_{g,g'} b_{g,g'}$ for some $B_{g,g'} < B, b_{g,g'} \in B$.

Proof. The system of equations $S_{g,g'}$ for $g = g_0 t^{\varepsilon_1} g_1 \cdots g_{n-1} t^{\varepsilon_n}$ and $g' = g'_0 t^{\delta_1} g'_1 \cdots g'_{n-1} t^{\delta_n}$, is the following:

$$t^{\varepsilon_n} x_1 = x_2 t^{\delta_n}$$

$$g_{n-1} x_2 = x_3 g'_{n-1}$$

$$t^{\varepsilon_{n-1}} x_3 = x_4 t^{\delta_{n-1}}$$

$$\vdots$$

$$t^{\varepsilon_1} x_{2n-1} = x_{2n} t^{\delta_1}$$

$$g_0 x_{2n} = x_{2n+1} g'_0$$

Denote by V_i the set of all solutions $(s_1, \cdots, s_{i+1}) \in \prod_{j=1}^{i+1} S_j$ of the system formed by the first i equations of $S_{g,g'}$. Let D^i_m be the projection of V_i onto its m^{th} component. The first equation of $S_{g,g'}$ is $t^{\varepsilon_n} x_1 t^{-\delta_n} = x_2$. Thus $D^1_2 = t^{\varepsilon_n} S_1 t^{-\delta_n} \cap S_2, D^1_1 = t^{-\varepsilon_n} D^1_2 t^{\delta_n}$ and $(s_1, s_2) \in V_1$ if and only if $s_2 \in D^1_2$ and $s_1 = t^{-\varepsilon_n} s_2 t^{\delta_n}$. Note that $D^1_1, D^1_2 \in \Phi(\{A\}, G^*)$ or $\Phi(\{B\}, G^*)$ (if $S_1 = A$ then replace B in S_i, i is even, by $t^{-1}At$ and similarly if $S_1 = B$ then replace A in S_i, i is odd, by tBt^{-1}) Now rewrite the i^{th} equation($i \geq 1$)) in $S_{g,g'}$ in the form of $p_i s_i {p'}_i^{-1} = s_{i+1}$ where

$$p_i = \begin{cases} g_{n-\frac{i}{2}}, & \text{if } i \text{ is even} \\ t^{\epsilon_n - \frac{i-1}{2}}, & \text{if } i \text{ is odd} \end{cases} \text{ and } p'_i = \begin{cases} g'_{n-\frac{i}{2}}, & \text{if } i \text{ is even} \\ t^{\delta_n - \frac{i-1}{2}}, & \text{if } i \text{ is odd} \end{cases}.$$

Then $D^i_{i+1} = p_i D^{i-1}_i {p'}^{-1}_i \cap S_{i+1}$ for $i = 1, \cdots, 2n$ when we set $D^0_1 := S_1$. In particular $D^{2n}_{2n+1} = p_{2n} D^{2n-1}_{2n} {p'}^{-1}_{2n} \cap S_{2n+1}$. Hence $(s_1, s_2, \cdots, s_{2n+1})$ is a solution of $S_{g,g'}$ if and only if $s_{2n+1} \in D^{2n}_{2n+1}$ and $s_i = p_i^{-1} s_{i+1} p'_i$ for $i = 2n$ to 1. More precisely, since $D^{2n}_i = p_i^{-1} D^{2n}_{i+1} p'_i$ for $1 \leq i \leq 2n$ it follows that

$$
\begin{aligned}
&D^{2n}_{(2n+1)-i} = p^{-1}_{(2n+1)-i} D^{2n}_{(2n+1)-i+1} p'_{(2n+1)-i} \\
&= p^{-1}_{(2n+1)-i} (p^{-1}_{(2n+1)-i+1} D^{2n}_{(2n+1)-i+2} p'_{(2n+1)-i+1}) p'_{(2n+1)-i} \\
&= \cdots \\
&= p^{-1}_{(2n+1)-i} p^{-1}_{(2n+1)-i+1} \cdots p^{-1}_{(2n+1)-1} D^{2n}_{2n+1} p'_{(2n+1)-1} \cdots p'_{(2n+1)-i+1} p'_{(2n+1)-i} \\
&= p^{-1}_{(2n+1)-i} p^{-1}_{(2n+1)-i+1} \cdots p^{-1}_{(2n+1)-1} (p_{2n} D^{2n-1}_{2n} {p'}^{-1}_{2n} \cap S_{2n+1}) p'_{(2n+1)-1} \\
&\cdots p'_{(2n+1)-i+1} p'_{(2n+1)-i} \\
&= \cdots \\
&= D^{(2n)-i}_{(2n+1)-i} \cap p^{-1}_{(2n+1)-i} S_{(2n+1)-i+1} p'_{(2n+1)-i} \cap \cdots \\
&\cap p^{-1}_{(2n+1)-i} p^{-1}_{(2n+1)-i+1} \cdots p^{-1}_{(2n+1)-1} S_{2n+1} p'_{(2n+1)-1} \cdots p'_{(2n+1)-i+1} p'_{(2n+1)-i}.
\end{aligned}
$$

By Lemma 15, after the replacement of A's in S_i's with tBt^{-1} or B's in S_i's with $t^{-1}At$, $D^{2n}_1 = S_1 \cap p_1^{-1} S_2 p'_1 \cap \cdots \cap p_1^{-1} p_2^{-1} \cdots p_{2n}^{-1} S_{2n+1} p'_{2n} \cdots p'_2 p'_1 = Hu$ for some $H < G^*$ and $u \in G^*$. If $S_1 = A$ then $E_{g,g'} = A_{g,g'} a_{g,g'}$ for some $A_{g,g'} < A$ and $a_{g,g'} \in A$. Similarly, if $S_1 = B$ then $E_{g,g'} = B_{g,g'} b_{b,b'}$ for some

$B_{g,g'} < B$ and $b_{g,g'} \in B$. $\square$

Denote by $Sub(A)$ the set of all subgroups of A. Then by Lemma 15 nonempty subsets of $\Phi(Sub(A), G^*)$ are some cosets of subgroups of G^*.

The **Cardinality Search Problem** for $\Phi(\mu, G)$ is the following decision problem: Let μ be a set of finitely generated subgroups of G. For a given set $B \in \Phi(\mu, G)$ determine whether B is empty, finite, or infinite and if B is finite, then list all elements of B.

Corollary 1. *Let G^* be an HNN-extension of a group G. Let $g = g_0 t^{\varepsilon_1} g_1 \cdots g_{n-1} t^{\varepsilon_n}$ and $g' = g'_0 t^{\delta_1} g'_1 \cdots g'_{n-1} t^{\delta_n}, (n \geq 1)$, be two elements of cyclically reduced normal form in G^*. If the Cardinality Search Problem is decidable for $\Phi(Sub(A), G^*)$ and $\Phi(Sub(B), G^*)$ then one can effectively find the set $E_{g,g'}$. In particular, one can effectively check whether or not $E_{g,g'}$ is empty, singleton, or infinite.*

Proof. Since $E_{g,g'} = D_1^{2n+1} = p_1^{-1} p_2^{-1} \cdots p_{2n}^{-1} D_{2n+1}^{2n} p'_{2n} \cdots p'_2 p'_1$, it suffices to solve the cardinality search problem for D_{2n+1}^{2n}. From $D_{i+1}^i = p_i D_i^{i-1} p_i'^{-1} \cap S_{i+1}$ for $1 \leq i \leq 2n$ and Lemma 15, one can see that each D_{i+1}^i is a coset of the type $S_{D_i} s_{D_i}$ where $S_{D_i} < A$ and $s_{D_i} \in A$ or $S_{D_i} < B$ and $s_{D_i} \in B$. Now observe that if K, H are subgroups of G and $a, b \in G$ then $Ka \cap Hb = (K \cap H)h$ for some $h \in Ka \cap Hb$. Thus one can effectively write D_{i+1}^i as $S_{D_i} s_{D_i}$ by finding

s_{D_i} as suggested in the method of finding h in $Ka \cap Hb = (K \cap H)h$ for some $h \in Ka \cap Hb$. Furthermore one can effectively find the cardinality of S_{D_i}, which is a subgroup of A or B, with the algorithm for Cardinality Search Problem for $\Phi(Sub(A), G^*)$ and for $\Phi(Sub(B), G^*)$. Thus one can solve the cardinality search problem for D^i_{i+1} for each $i \in \{0, \cdots, 2n\}$ and hence for $E_{g,g'}$. □

Lemma 17. *Let $g, g' \in G^*$. If $|g| = |g'| \geq 1$ and $S_{g,g'}$ has more than one solution in $A \cup B$ then g, g' are singular.*

Proof. Let $(s_1, \cdots, s_{2n+1})$ and $(s'_1, \cdots, s'_{2n+1})$ be two distinct solutions of $S_{g,g'}$. Then

$$t^{\varepsilon_n} s_1 = s_2 t^{\delta_n}, \quad t^{\varepsilon_n} s'_1 = s'_2 t^{\delta_n}$$

$$g_{n-1} s_2 = s_3 g'_{n-1}, \quad g_{n-1} s'_2 = s'_3 g'_{n-1}$$

$$t^{\varepsilon_{n-1}} s_3 = s_4 t^{\delta_{n-1}} \quad t^{\varepsilon_{n-1}} s'_3 = s'_4 t^{\delta_{n-1}}$$

$$\vdots \qquad\qquad \vdots$$

$$t^{\varepsilon_1} s_{2n-1} = s_{2n} t^{\delta_1}, \quad t^{\varepsilon_1 s'_{2n-1}} = s'_{2n} t^{\delta_1}$$

$$g_0 s_{2n} = s_{2n+1} g'_0, \quad g_0 s'_{2n} = s'_{2n+1} g'_0.$$

Rewrite both systems of equations for t^{δ_i}'s and g'_j's;

$$t^{\delta_n} = s_2^{-1} t^{\varepsilon_n} s_1, \quad t^{\delta_n} = {s'}_2^{-1} t^{\varepsilon_n} s'_1$$

$$g'_{n-1} = s_3^{-1} g_{n-1} s_2, \quad g'_{n-1} = {s'}_3^{-1} g_{n-1} s'_2$$

$$t^{\delta_{n-1}} = s_4^{-1} t^{\varepsilon_{n-1}} s_3 \quad t^{\delta_{n-1}} = {s'}_4^{-1} t^{\varepsilon_{n-1}} s'_3$$

$$\vdots \qquad\qquad \vdots$$

$$t^{\delta_1} = s_{2n}^{-1} t^{\varepsilon_1} s_{2n-1}, \quad t^{\delta_1} = {s'}_{2n}^{-1} t^{\varepsilon_1} s'_{2n-1}$$

$$g'_0 = s_{2n+1}^{-1} g_0 s_{2n}, \quad g'_0 = {s'}_{2n+1}^{-1} g_0 s'_{2n}.$$

Now equate both equations;

$$s_2^{-1} t^{\varepsilon_n} s_1 = {s'}_2^{-1} t^{\varepsilon_n} s'_1$$

$$s_3^{-1} g_{n-1} s_2 = {s'}_3^{-1} g_{n-1} s'_2$$

$$s_4^{-1} t^{\varepsilon_{n-1}} s_3 = {s'}_4^{-1} t^{\varepsilon_{n-1}} s'_3$$

$$\vdots$$

$$s_{2n}^{-1} t^{\varepsilon_1} s_{2n-1} = {s'}_{2n}^{-1} t^{\varepsilon_1} s'_{2n-1}$$

$$s_{2n+1}^{-1} g_0 s_{2n} = {s'}_{2n+1}^{-1} g_0 s'_{2n}.$$

We can rewrite this system as below;

$$t^{\varepsilon_n} s_1 {s'}_1^{-1} t^{-\varepsilon_n} = s_2 {s'}_2^{-1},$$

$$g_{n-1} s_2 {s'}_2^{-1} g_{n-1}^{-1} = s_3 {s'}_3^{-1},$$

$$\vdots$$

$$t^{\varepsilon_1} s_{2n-1} {s'}_{2n-1}^{-1} t^{-\varepsilon_1} = s_{2n} {s'}_{2n}^{-1},$$

$$g_0 s_{2n} {s'}_{2n}^{-1} g_0^{-1} = s_{2n+1} {s'}_{2n+1}^{-1}.$$

Since (all or some but definitely at least one) $s_i {s'}_i^{-1}$ are nontrivial, g is singular by the Lemma 13. g' is also a singular element for a similar reason. □

Let G be a group and let H be a subgroup of G. We say H is malnormal if $H \cap H^g = 1$ for all $g \in G \setminus H$. Then the **Malnormality Problem** for H in G is the problem of deciding whether a given subgroup H is malnormal in G.

Lemma 18. *Let G^* be an HNN-extension of a finitely presented group G. Assume that G^* allows algorithms for the following problems;*

1. *Coset Representatives Search Problems for the subgroup A and B.*
2. *Cardinality Search Problem for $\Phi(Sub(A), G^*)$ and $\Phi(Sub(B), G^*)$.*
3. *Malnormality Problem for $A \cup B$ in G.*

Then regularity of elements of G^* is decidable.

Proof. Let $g \in G^*$. We compute the cyclically reduced normal form of g using the Algorithm 4.2.2. If $|g| \geq 1$ then g is singular if and only if $S_{g,g}$ has a nontrivial solution of the form $(s, s_2, \cdots, s_{2n}, s_{2n+1})$ in $\prod_{n=1}^{2n+1} S_i$, where $S_i = A$ or B for $0 \leq i \leq n$ and $S_{2n+1} = A \cup B$ for some $s \in (A \cup B) \setminus \{1\}$. If $S_{g,g}$ has no solution of the form $(s, s_2, \cdots, s_{2n+1})$ then g is regular. If $S_{g,g}$ has one solution $(s, s_2, \cdots, s_{2n+1})$ then we can check whether it is a trivial solution or not, hence we can determine whether g is regular or not. If $S_{g,g}$ has more than one solution of the form $(s, s_2, \cdots, s_{2n+1})$ then one of them will be nontrivial, thus g is singular. If $|g| = 0$, i.e, $g \in G$ then we need to determine whether $g \in N_G^*(A \cup B)$. Since the Malnormality Problem for $A \cup B$ in G is decidable, we can determine the regularity of g. □

4.4 Conjugacy Search Problem for Regular Elements

The conjugacy search problem for a given set of pairs of elements Θ is defined as following: Let Θ be a set of pairs of elements of a group G. For a given $(g, h) \in \Theta$ determine whether g is a conjugate of h in G and if it is, find a

conjugator.

Lemma 19. *Let G^* be an HNN extension of a finitely presented group G and let $g \in G^*$ be a cyclically reduced regular element. Assume that G^* allows algorithms for the following problems;*

1. *Coset Representatives Search Problems for the subgroup A and $B = (\phi(A))$.*

2. *Cardinality Search Problem for $\Phi(Sub(A), G^*)$ and $\Phi(Sub(B), G^*)$.*

Then the Conjugacy Search Problem in G^* is decidable for g of length $l(g) \geq 1$.

Proof. Let g be a regular cyclically reduced element of G^*, and let g' be an arbitrary element of G^*. We can rewrite them into their cyclically reduced normal forms $g = g_0 t^{\varepsilon_1} g_1 \cdots g_{n-1} t^{\varepsilon_n}$, $g' = g'_0 t^{\delta_1} g'_1 \cdots g'_{m-1} t^{\delta_m}$ using Algorithm 4.2.2. By Theorem 4.1.2, g and g' are conjugate if and only if $n = m$ and $x^{-1}\pi(g')x = g$ has a solution s in A or B (depending on ε_n) where $\pi(g')$ is a cyclic permutation of g'. By Lemma 14 the equation $x^{-1}\pi(g')x = g$ has a solution s in A or B if and only if the system of equations $S_{\pi(g'),g}$ has a solution $(s, s_1, \cdots, s_{2n}, s)$ in $\prod_{i=0}^{2n+1} S_i$ where $S_i = A$ or B. Since g is regular and $l(g) \geq 1$, $S_{\pi(g'),g}$ has at most one solution in A or B by Lemma 17.

Now using the Algorithm for Cardinality Search Problem for $\Phi(Sub(A), G^*)$ and $\Phi(Sub(B), G^*)$, one can find first $E_{\pi(g'),g}$, the set of all $s \in A$ or B for which $S_{\pi(g'),g}$ has a solution $(s, s_1, \cdots, s_{2n+1})$ and, then, one can check whether $S_{\pi(g'),g}$ has a solution and if it does, one can find the solution. Now in case $S_{\pi(g'),g}$ has a solution one can check whether this solution is of the form $(s, s_1, \cdots, s_{2n}, s)$. If it is, then $x^{-1}\pi(g')x = g$ has a solution s in A or B and if it is not, then $x^{-1}\pi(g')x = g$ has no solution in A or B. □

Lemma 20. *Let G^* be an HNN extension of a finitely presented group G. If G^* allows an algorithm for the conjugacy Search Problem in G then the Conjugacy Search Problem in G^* is decidable for cyclically reduced regular elements g of length $l(g) = 0$.*

Proof. Proved as it is stated. □

Theorem 4.4.1. *Let G^* be an HNN extension of a finitely presented group G and let $g \in G^*$ be a cyclically reduced regular element. Assume that G^* allows algorithms for the following problems;*

1. *Coset Representatives Search Problems for the subgroup A and $B = (\phi(A))$*

2. *Cardinality Search Problem for $\Phi(Sub(A), G^*)$ in G^* and*

for $\Phi(Sub(B), G^*)$ *in* G^*

3. *Conjugacy Search Problem in* G

4. *Malnormality Problem for the subgroup* A *and* B *in* G^*

Then Conjugacy Search Problem in G^* *is decidable for* g.

Proof. Follows from Lemma 19 and Lemma 20. □

Bibliography

[1] S. I. Adian, V. G. Durnev, "Decision problems for groups and semigroups", RUSS MATH SURV, 2000, 55 (2), 207-296; English Transl.

[2] W. Boone, " The word problem", Ann. of Math.(2) 70, 207-265

[3] A. Borovik, A. Myasnikov, V. Shpilrain, "Measuring sets in infinite groups", Computational and Statistical Group Theory. Amer. Math. Soc., Contemporary Math. 298(2002), 21-42.

[4] A. Borovik, A. Myasnikov, V. Remeslennikov, "Multiplicative measures on free groups", Internat. J. Algebra Comput., 13(2003) No. 6, 705-731.

[5] A. Borovik, A. Myasnikov, V. Remeslennikov, "The conjugacy problem in amalgamated products I : Regular elements and Blanck holes", preprint, 2005

[6] D.J. Collins, "A simple presentation of a group with unsolvable word problem", Illinois Journal of Mathematics, Volume 30, Number 2, Summer 1986, 230 - 234

[7] S. Cooper, "Computability Theory", Chapman and Hall/CRC Mathematics, 2003

[8] R. Gilman, A. Myasnikov, A. Miasnikov, A. Ushakov, "Generic complexity of algorithmic problems", Preprint.

[9] I. Kapovich, A. Myasnikov, P. Shupp, V. Shpilrain, "Generic-case complexity and decision problems in group theory and random walks", J. of Algebra, 264(2003), 665-694.

[10] I. Kapovich, A. Myasnikov, P. Shupp, V. Shpilrain, "Averate-case complexity for the word and membership problems in group theory", Advances in Mathematics 190(2005), No 2, 343-359.

[11] G.H. Hardy, J.E. Littlewood and G. Po'lya, "Inequalities", 2nd ed. Cambridge, England: Cambridge University Press, 1988, 43-44.

[12] M. Lothaire, "Algebraic combinatorics on words", Cambridge, U.K.; New York: Cambridge University Press, 2002.

[13] R. Lyndon, P. Schupp, "Combinatorial Group Theory", Berlin; New York : Springer-Verlag, 1977.

[14] G. S. Makanin, "The identity problem in finitely presented semigroups", Dokl, Akad, Nauk, SSSR 171(1966), 285-287; English Transl., Soviet Math Dokl 7 (1966), 1478- 1480.

[15] A. Myasnikov, A. Rybolov, "On generically undecidable problems", preprint, 2006

[16] A. Myasnikov, "Asymptotic group theory", Lecture note, 2000

[17] A. Myasnikov and A. Ushakov, "Random van kampen diagrams and algorithmic problems in groups"

[18] C. Papadimitriou, "Computational complexity", Addison-Wesley 1994

[19] G. Polya, "Über eine Aufgabe betreffend die Irrfahrt im Strassennetz", Math. Ann., 84:149-160, 1921

[20] Robert I. Soare, "Recursively enumerable sets and degrees: a study of computable functions and computably enumerable sets", Springer-verlag, 1987

[21] M. Sipser, "Introduction to the theory of computation", PWS Publishing Company, 1997

[22] J. Stillwell, "The word problem and the isomorphism problem for groups", Bulletin of the American Mathematically Society, Volume 6, Number 1, January 1982, 33-56