Whitehead's Decision Problems for Automorphisms of Free Group

by

Subhajit Mishra, BS., MS.

Department of Mathematics and Statistics,
McMaster University

supervised by

Professor Ian Hambleton

Department of Mathematics and Statistics,
McMaster University

A Thesis submitted to the School of Graduate Studies in Partial Fulfillment of the Requirements for the degree Master of Mathematics (Thesis)

To all the essential workers in the fight with Covid-19.

ACKNOWLEDGMENT

Gurur Brahma Gurur Vishnu,
Gurur Devo Maheswarah.
Gurur Sakshaat Param Brahma,
Tasmai Shree Gurave Namah.

Guru Gita, Uttarakhand section

First of all, I wish to express my sincere gratitude to my supervisor, Prof. Ian Hambleton, for allowing me to work on this thesis as a Master's student. His constant guidance, encouragement and useful critiques have been essential for the completion of this work. I thank him for being patient with me and giving me the freedom to portray my ideas.

I would like to thank Prof. McKenzie Wang and Prof. Andrew J. Nicas for being in the defense committee. Their comments, suggestions and encouragement have been invaluable. I thank all my professors for teaching me in the period of my Master's degree.

I wish to thank all my friends especially Jie, Elkin, Anthony, Uyen, Lorena, Robert, Tanmoy, Shouvik and Kuntal for allowing me to have a lot of discussions during the course of this work.

I would like to extend my gratitude toward my "jethumoni" Prof. Kalyan Chatterjee and my cousin Mr. Saradindu Kar for helping me in my difficult times.

I am thankful to the School of Graduate studies, McMaster University for providing me scholarship during my Master's degree.

Lastly, I am indebted to my parents for their unfailing support, constant encouragement and undeniable faith in me. This accomplishment would not have been possible without them.

ABSTRACT

Let F be a free group of finite rank. Given words $u, v \in F$, J.H.C. Whitehead [Whitehead, 1936b] solved the decision problem of finding an automorphism $\phi \in \mathrm{Aut}(F)$, carrying u to v. He used topological methods to produce an algorithm. Higgins and Lyndon [Higgins and Lyndon, 1974] gave a very concise proof of the problem based on the works of Rapaport [Rapaport, 1958].

We provide a detailed account of Higgins and Lyndon's proof of the peak reduction lemma and the restricted version of Whitehead's theorem, for cyclic words as well as for sets of cyclic words, with full explanation of each step. Then, we give an inductive proof of Whitehead's minimization theorem and describe Whitehead's decision algorithm.

Noticing that Higgins and Lyndon's work is limited to the cyclic words, we extend their proofs to ordinary words and sets of ordinary words.

In the last chapter, we mention an example given by Whitehead to show that the decision problem for finitely generated subgroups is more difficult, and outline an approach due to Gersten to overcome this difficulty.

We also give an extensive literature survey of Whitehead's algorithm.

TABLE OF CONTENTS

CHAPTER 1

OVERVIEW

- In this chapter, we give an overview of this thesis. Whitehead, in two famous papers [Whitehead, 1936a][Whitehead, 1936b], proved a decision problem for automorphism groups of free groups. We call this *Whitehead's first decision problem.*

  Given $U = \{u_1, \ldots, u_m\}$ and $V = \{v_1, \ldots, v_m\}$, two finitely ordered subsets of a free group of finite rank, F_n, to decide if there is an automorphism of F_n carrying U to V.

  Whitehead proved the problem by using topological methods. This provided an algorithm to find such an automorphism, called *Whitehead algorithm.* Later, Rapaport [Rapaport, 1958] proved the problem using purely algebraic methods and Higgins and Lyndon [Higgins and Lyndon, 1974] gave a simplified version of her proof.

- The goal of this thesis is to give a detailed account of Whitehead's first decision problem, following Higgins and Lyndon's proof. Their version of Whitehead's theorem [Lyndon and Schupp, 2001, Proposition 4.17, p. 32] is rather weak. We call this *restricted form* or *restricted version of Whitehead's theorem.* Though, Whitehead's proof works for both the cyclic words and ordinary words (true words, as per Whitehead), Higgins and Lyndon's proof is limited to cyclic words. We extend these proofs to ordinary words.

- In the second chapter, we provide a historical significance of this problem. We provide a brief survey from Nielsen's work on automorphism group of free groups in early 1900s to recent developments on computational complexity of the algorithm.

- In the third chapter, we introduce Whitehead automorphisms, product counts and some necessary preliminaries, and give a detailed proof of some properties of Whitehead automorphisms and product counts. Basically, this chapter consists of necessary materials for the build up of the theorem.

- The following chapter contains three sections.

  – In §4.1, we prove the restricted version of Whitehead's theorem for cyclic words. First, we prove the *peak reduction lemma.* We will see

that the proof of this lemma is quite long and consists of five cases. Then, using this lemma, we give a proof of the restricted version of the theorem.

  - §4.2 consists of the proof of Whitehead's main theorems: which are, finding a minimal word in the automorphic orbit and finding a sequence of Whitehead automorphisms between two equivalent minimal words. Then we show how this theorem provides Whitehead's decision algorithm. We don't emphasize the efficiency of the algorithms. For that, we refer to the appropriate papers.
  - In §4.3, we turn our attention to the finite sets of cyclic words. We give a detailed proof of the peak reduction lemma and the restricted version of Whitehead's theorem. Then, we notice that, given the lemma and the theorem, the main theorem follows when replacing cyclic words by sets of cyclic words.

- In chapter 5, we extend these proofs to ordinary words and the finite sets of ordinary words.
- In the following chapter, we briefly discuss Whitehead's counter example to the problem of finding a sequence of automorphisms for two equivalent finitely generated subgroups of free groups, and Gersten's idea to solve it.

CHAPTER 2

A BRIEF HISTORICAL SURVEY

The central goal of this section is to provide a historical survey on *Whitehead's decision problem* in the automorphisms of free groups. Before describing the problem itself, we shall go further back to discuss a few relevant works of Nielsen which are crucial for proving Whitehead's problem.

Nielsen, in **[Nielsen, 1917]**, proved that mapping class group of a *torus minus a point* is isomorphic to the automorphism classes of free group of rank 2, F_2. While proving this, Nielsen showed that $\mathrm{Aut}(F_2)$ is generated by some special automorphisms, called *Nielsen transformations* or *elementary Nielsen automorphisms*, which he generalized in his next papers **[Nielsen, 1918]**[**Nielsen, 1924**]. Readers may go to **[Magnus et al., 2004, Theorem 3.2, pp. 131]** for the proof of the theorem:

The elementary Nielsen automorphisms of F_n on the generators $x_1, x_2, \ldots, x_n$, n finite, are a finite set of generators for Aut(F_n).

In 1935, Whitehead proved that if a set of words, W forms a part of a basis of F_n, then the *Whitehead graph* of W is either not connected or has a cut vertex **[Whitehead, 1936a, lemma]**. This is known as *Whitehead's cut vertex lemma*, which provides an algorithm to find a basis of the free group. He proved this by representing words on three dimensional manifolds and introducing a new set of special automorphisms, called *Whitehead automorphisms*. Stong **[Stong, 1997]** and Stallings **[Stallings, 1999]** extended this to the *separability* of free groups. Stallings' proof uses Whitehead's techniques of representing words on manifolds. Hoare **[Hoare, 1988]** gave a combinatorial proof of the cut vertex lemma using Gersten's graph which was developed to study automorphism group of free groups in a series of papers **[Gersten, 1987]**[**Gersten, 1983**]**[Gersten, 1984a]**. A careful treatment of the lemma and an extension to *generalized cut-vertex lemma* was given recently by Warren Dicks **[Dicks, 2017b,** §4, §5]. Goldstein **[Goldstein, 1999]** used Whitehead's 3-manifold techniques to introduce a bound for length of a word. Later, using same techniques, Clifford and Goldstein **[Clifford and Goldstein, 2010]** provided an algorithm which determines whether a subgroup of a free group contains a primitive element, which was an open problem. Wade **[Wade, 2014]** produced an algorithm, based on Stallings foldings **[Stallings, 1983]**, to decompose an automorphism as a product of Whitehead automorphisms. Dicks **[Dicks, 2014]** gave an algorithm

that sandwich a subgroup of a free group between free product factors and obtained a simplified Clifford-Goldstein algorithm using Whitehead's cut-vertex lemma. Wilton **[Wilton, 2018]** used Whitehead's graph and cut vertex lemma to prove Gromov's question: *Does every one-ended hyperbolic group contain a surface subgroup?* Kim and Oum **[Kim and Oum, 2014]** formulated a stronger Whitehead graph to answer: *Does every one-ended double of a non-abelian free group have a hyperbolic surface subgroup?* Heusener and Weidmann **[Heusener and Weidmann, 2019]** showed that Whitehead's cut vertex lemma is a mere consequence of Stallings folds **[Stallings, 1983]**. Clay, Conant and Ramasubramanian **[Clay et al., 2014]** proved that for F_2, the probability of Whitehead graph with l edges is $1/l^2$.

In a subsequent paper **[Whitehead, 1936b]**, Whitehead gave an answer to the decision problem of finding an automorphism between two given words in a finely ranked free group. Whitehead's proof was based on the topological methods that he developed in the previous paper. Basically, in §3 of the paper, he showed that if a set of words (*cyclic* or *ordinary*) can be reduced by an automorphism then it can also be reduced by a random sequence of Whitehead automorphisms, and two equivalent minimal sets of words can be interchanged by Whitehead automorphisms, keeping the lengths fixed (*level transformations*). This provides an algorithm for the problem above, called *Whitehead's algorithm*.

Rapaport **[Rapaport, 1958]** reproved Whitehead's first problem using a purely algebraic method. Her effort was simplified further by Higgins and Lyndon **[Higgins and Lyndon, 1974]**. McCool **[McCool, 1974]** gave a refinement of the argument given by Higgins and Lyndon, and obtained a presentation for the automorphism group of a finitely generated free group and for certain stabilizers in a free group. Hoare **[Hoare, 1979]** described Whitehead automorphisms by cutting and pasting of *coinitial graphs*, and using this unified Higgins and McCool's work. Stallings **[Stallings, 1987]** first noticed a connection between Gersten's graphical representation of automorphisms and Whitehead's three dimensional model. This connection is explained in details with some added results by Goldstein and Turner **[Goldstein and Turner, 1984]**. Collins and Zieschang in a series of papers **[Collins and Zieschang, 1984a]** **[Collins and Zieschang, 1984b]** **[Collins and Zieschang, 1984c]** generalized Whitehead's algorithm to a free product of finitely many indecomposable factors. Culler and Vogtman **[Culler and Vogtmann, 1986]** gave a refinement of Higgins and Lyndon's peak-reduction lemma using graphical nature of Whitehead moves developed by Hoare, while studying outer automorphisms of free groups. Later, Clay and Forester generalized the notion of Whitehead moves from Culler and Vogtman's Outer space to G-trees **[Clay and Forester, 2009]**. Extensions of Whitehead's algorithm have been made to the surface groups by Levitt and Vogtmann **[Levitt and Vogtmann, 2000]**, the

torsion free hyperbolic groups by Bogopolski and Ventura **[Bogopolski and Ventura, 2011]**, the hyperbolic groups by Dahmani and Guirardel **[Dahmani and Guirardel, 2011]**, the toral relatively hyperbolic groups by Kharlampovich and Ventura **[Kharlampovich and Ventura, 2012]** and the right angled Artin groups by Day **[Day, 2009]**[**Day, 2014**]. In fact, Bogopolski and Ventura provided the algorithm for the mixed tuple of words (*cyclic and ordinary*), Dahmani and Guirardel's proof uses relative Grushko and JSJ decompositions which is a completely different approach to other proofs, and Day found a finite presentation for the automorphism group of Artin group that generalized the McCool's result on finite presentation. Kristić, Lustig and Vogtmann **[Krstić et al., 2001, Theroem 1.1]** produced an equivariant Whitehead algorithm, using which they solved the conjugacy problem for roots of Dehn twist automorphisms. Clarke and Goldstein proved certain stability of numerical invariants in a free group which they introduced in **[Clark and Goldstein, 2005]**, using Whitehead's 3D model. Lee **[Lee, 2002]** used Whitehead automorphisms and Whitehead graph to prove that an endomorphism of a free group that preserves automorphic orbits is necessarily an automorphism. In a later paper, using Whitehead's algorithm, the author **[Lee, 2007]** produced an algorithm to decide whether or not two cyclic words u and v have the property that the length of $\phi(u)$ and $\phi(v)$ is equal for every automorphism ϕ in F_2. Dicks **[Dicks, 2017a]** provided a graph theoretical argument and proved Whitehead's algorithm. Gutiérrez, Núñez and Ramírez **[Manjarrez-Gutiérrez et al., 2015]** used Whitehead's topological methods to construct circular handle decompositions of knot complements with free Seifert surfaces in the three-dimensional sphere. Chrona, Geller and Shpilrain **[Chorna et al., 2017]** gave an algorithm using peak-reduction lemma which says that if a sequence of $A(k)$ and $B(k)$ reduces complexity of a matrix $M \in SL_2(\mathbb{Z})$, then there is single such multiplication that reduces the complexity, where $A(k) = (1, k, 0, 1)$ and $B(k) = (1, 0, k, 1)$ are 2×2 matrices viewed as elements in $\mathbb{R}^4$.

There have also been efforts to improve the computational complexity of Whitehead's algorithm. It is well known that the reduction to minimal part of Whitehead algorithm is fast whereas, the second part (finding a path between two minimal words of same length) is very slow. Myasnikov and Shpilrain **[Myasnikov and Shpilrain, 2003]** improved the second part of the algorithm with polynomial time complexity and proved it for F_2. Lee **[Lee, 2006]** showed that the algorithm is bounded by polynomial time for free group of rank ≥ 2. Khan **[Khan, 2004]** further improved the algorithm to quadratic time complexity using Whitehead graphs. Haralick, Miasnikov and Myasnikov **[Haralick et al., 2005]**[**Miasnikov and Myasnikov, 2004**] showed by experimental methods that, for rank ≥ 2, Whitehead algorithm is very fast. Myasnikov and Haralick **[Myasnikov and Haralick, 2006]** produced a new algorithm for Whitehead minimiza-

tion problem, called a *hybrid search algorithm* in the sense that it employs several stochastic, as well as deterministic procedures based on the heuristic methods of **[Haralick et al., 2005]**. Kapovich, Schupp and Shpilrain **[Kapovich et al., 2006]** showed that for an exponentially generic input, first part of Whitehead's algorithm terminates immediately and the second part has linear time complexity. Roig, Ventura and Weil **[Roig et al., 2007]** produced first fully polynomial algorithm for Whitehead minimization problem. The authors showed that their algorithm is polynomial both in length of input words and in the rank of free group as opposed to the earlier algorithms by Whitehead and Gersten, which had an exponential dependency in the rank of free group. To prove this, the authors reduced the length reduction problem to classical MaxFlow-MinCUt problem in graph theory, which has polynomial time complexity, using Whitehead graph. Kapovich **[Kapovich, 2007]**, using geodesic current, gave a theoretical justification of some experimental results provided by Haralick, Miasnikov and Myasnikov via pattern recognition methods regarding Whitehead algorithm. It is still unknown if Whitehead's algorithm (second part) has polynomial time complexity for rank > 2.

Whitehead mentioned the generalization of his first problem to the finitely generated subgroups of free groups in **[Whitehead, 1936b, p. 800]** but did not find a solution. This problem remained unsolved for some time until Gersten **[Gersten, 1984b]** realized that it can be solved by using a different "complexity" to the length of the words. His main idea was to represent a free group as a fundamental group of wedge of circles, and any subgroup of the free group as a covering space. Kalajdžievski **[Kalajdžievski, 1992]** extended Gersten's idea to topography and proved that the centralizer of any finite subgroup of automorphism group of a finite rank free group is finitely presented. Using Gersten's idea, Diao and Feighn **[Diao and Feighn, 2005]** provided an algorithm which, given a finite graph of finite rank free groups, produces the Grushko decomposition of its fundamental group. Bogopolski **[Bogopolski, 2001]** extended this result for the finitely generated subgroups of fundamental groups of compact surfaces. Bassino, Nicaud and Weil **[Bassino et al., 2016]** showed that a finitely generated subgroup of a free group, chosen uniformly at random, is strictly Whitehead minimal with overwhelming probability.

CHAPTER 3

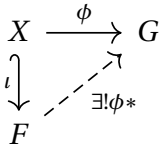
WHITEHEAD AUTOMORPHISMS

In §3.1 of the chapter, we review some preliminaries regarding free groups and fix some notations. In §3.2, we give equivalent definitions of Whitehead automorphisms and prove some properties. Then, in §3.3, we introduce the product count of two subsets of a basis for a cyclic word and a set of cyclic words. At last, in §3.4, we prove the necessary results for proving Whitehead's theorem.

3.1. Free groups

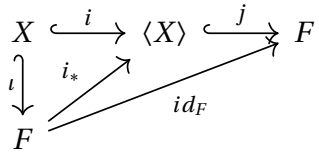
In this section, we discuss *free groups, cyclic words and elementary reduction* to avoid any confusion regarding the notions later on.

Definition 3.1.1. (**Free Group**) Let X be a subset of a group F and G be another group. We say F is a free group with basis X, if for any function $\phi : X \to G$ there exists a unique homomorphism $\phi^* : F \to G$ such that $\phi^*|_X = \phi$ i.e., the following diagram commutes.



Proposition 3.1.2. $F = \langle X \rangle$.

Proof. Notice that, we have $\langle X \rangle \leq F$. Let $j : \langle X \rangle \to F$ be the inclusion. Consider the following inclusion: $X \overset{i}{\hookrightarrow} \langle X \rangle$. Since F is free, we have a unique homomorphism $i_* : F \to \langle X \rangle$. Now, for the composition: $X \overset{i}{\hookrightarrow} \langle X \rangle \overset{j}{\hookrightarrow} F$, we have id_F. The following diagram makes the above argument clear.



From the diagram, we see that both $j \circ i_*$ and id_F are extensions of i. Therefore, $j \circ i_* = \mathrm{id}_F$. Since id_F is surjective, j is surjective. Therefore, $F = \langle X \rangle$. ■

A free group F, with basis X is denoted by $F(X)$. If X is finite with cardinality $n > 0$, we say $F(X)$ has rank n, and denote it by F_n or $F(n)$.

For example, $(\mathbb{Z}, +)$ is a free group of rank 1, with the generator 1.

In this project, we will only deal with free groups of finite rank.

Definition 3.1.3. (**Words, length of a word, length of a set of words, elementary reduction and reduced words**)

- Since F_n is generated by $X = \{x_1, \ldots, x_n\}$, any element $w \in F_n$ is given by $w = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$, for $1 \leq i_1, \ldots, i_n \leq n$ and $\varepsilon_i \in \{-1, 1\}$. Therefore, w is a finite sequence of basis elements. This w is said to be a *word* in F_n.

  From now on, we write the basis of F_n to be $X^{\pm 1} = X \cup X^{-1}$, where $X^{-1} = \{x_1^{-1}, \ldots, x_n^{-1}\}$. Therefore, a word, w is a finite sequence of the basis elements (called *letters*, by Whitehead), $w = a_1 \cdots a_m$, for $m \geq 0$ and $a_i \in X^{\pm 1}$.

  For $m = 0$, we write $w = 1$, the empty word or the identity element of F_n.

- A word w, may consists of forms aa^{-1} or $a^{-1}a$, for $a \in X^{\pm 1}$. An *elementary reduction* is deletion of these forms.

- We say a word w is *reduced* if it does not contain any of the forms aa^{-1} or $a^{-1}a$, for $a \in X^{\pm 1}$.

- The *length* of a word $|w|$, is defined to be the number of letters in it. For example, if $w = x_1 x_3 x_1^{-1}$ and $u = x_1 x_2 x_2^{-1}$, then $|w| = 3$ and $|u| = 3$. Notice, here u is an unreduced word.

- Given a set of words W, the *length* of W is given by $|W| = \sum_{w \in W} |w|$.

From now on, a word is always considered to be reduced, unless mentioned otherwise.

Words are divided into two types: *cyclic words* and *ordinary words* (*true words* as per Whitehead [Whitehead, 1936a]).

Definition 3.1.4. (**Cyclic Words**) A cyclic word of length k is an equivalence class of a cyclically ordered set of k letters a_i, for $i \in \mathbb{Z}_k$, where $\mathbb{Z}_k$ is the additive group of integer modulo k.

A cyclic word can also be thought of as an equivalence class of a set of k letters of above form, where equivalence relation is cyclic permutation. For example, we say $x_1 x_2 x_3 x_2^{-1}$ is a same cyclic words as that of $x_2 x_3 x_2^{-1} x_1$.

For us, a cyclic word is always reduced i.e., $a_i a_{i+1} \neq 1$, for $i \in \mathbb{Z}_k$, unless mentioned otherwise.

Definition 3.1.5. An *ordinary word*, w is defined to be a sequence of letters $xyz\ldots$, for $x, y, z \in X^{\pm 1}$ such that no consecutive pair of letters are inverses of each other.

For a detailed account of ordinary words see Chapter 5.

3.2. Whitehead Automorphisms

This section deals with some special kind of automorphisms, introduced by J.H.C. Whitehead [Whitehead, 1936b][Lyndon and Schupp, 2001, p. 31], called *Whitehead automorphisms*. We prove some properties of these automorphisms which will be useful to prove Whitehead's theorem.

Definition 3.2.1. Let F_n be a free group with basis $X^{\pm 1}$. A *Whitehead automorphism*, τ of F_n is defined to be one of the following two kinds:

(I) τ permutes the elements of $X^{\pm 1}$, *type (I) Whitehead automorphism*.

(II) For some fixed $a \in X^{\pm 1}$, τ maps each element $x \in X^{\pm 1}$ into one of x, xa, $a^{-1}x$, or $a^{-1}xa$, *type (II) Whitehead automorphism*. For a type (II) Whitehead automorphism, we write $\tau = (A, a)$, where the set A consists of all $x \in X^{\pm 1}$ such that $x\tau = xa$ or $x\tau = a^{-1}xa$, including a but excluding a^{-1}.

Let Ω denote the set of all Whitehead Automorphisms in F_n.

Here we give another definition of type (II) Whitehead automorphisms.

Definition 3.2.2. Given $a \in X^{\pm 1}$ and $A \subset X^{\pm 1}$ such that $a \in A$, $a^{-1} \notin A$, we define (A, a) as follows:

$$x(A,a) = \begin{cases} xa, & \text{if } x \in A, x^{-1} \notin A \\ a^{-1}xa, & \text{if } x, x^{-1} \in A \\ a^{-1}x, & \text{if } x \notin A, x^{-1} \in A \\ x, & \text{if } x, x^{-1} \notin A \end{cases} \tag{3.1}$$

for any $x \in X^{\pm 1}$, $x \neq a, a^{-1}$, and a, a^{-1} are fixed by (A, a).

Remark 1. Note that, it is necessary for (A, a) to fix a and a^{-1}. If possible, suppose that $a(A, a) = a^2$. Now any automorphism $F \to F$ induces an automorphism $\bar{F} \to \bar{F}$, where $\bar{F} = F/[F, F] \simeq \mathbb{Z}^n$. Also, note that $\mathrm{Aut}(\bar{F}) \simeq GL(n, \mathbb{Z})$. Now, $a \mapsto a^2$ induces $[a] \mapsto 2[a]$. So, the matrix of the induced automorphism will have a column $(2, 0, \ldots, 0)^T$. Therefore, the determinant of the matrix will never be ± 1. This is a contradiction. Hence, the only possibility is that $a(A, a) = a$ and similarly, $a^{-1}(A, a) = a^{-1}$.

Proposition 3.2.3. *Definition 3.2.1 and Definition 3.2.2 are equivalent, for type (II) Whitehead automorphisms.*

Proof. ($\Longrightarrow$) Let $A \subset X^{\pm 1}$ be the subset such that A consists of all $x \in X^{\pm 1}$ such that $x(A,a) = xa$ or $x(A,a) = a^{-1}xa$, including a but excluding a^{-1}.

- Let $x \mapsto xa$, for $x \in A$, $x \neq a$. So, $x^{-1} \mapsto a^{-1}x^{-1}$. Now, according to Definition 3.2.1, this suggests $x^{-1} \notin A$. Hence, we get, $x \mapsto xa$, for $x \in A, x^{-1} \notin A$, $x \neq a, a^{-1}$.

- Let $x \mapsto a^{-1}xa$. In that case, $x^{-1} \mapsto a^{-1}x^{-1}a$. Hence, from Definition 3.2.1, $x^{-1} \in A$.

- Let $x \notin A$. According to the definition of type (II) Whitehead automorphism, x is mapped into either $a^{-1}x$ or x by (A,a).

  Take $x \mapsto a^{-1}x$. Therefore, $x^{-1} \mapsto x^{-1}a$. Hence, according to Definition 3.2.1, $x^{-1} \in A$. So, $x \mapsto a^{-1}x$, for $x \notin A$ and $x^{-1} \in A$.

  Now, $x \mapsto x \implies x^{-1} \mapsto x^{-1}$. This means $x^{-1} \notin A$, according to Definition 3.2.1.

All these cases prove this direction.

($\Longleftarrow$) Given (A,a) in Definition 3.2.2, it is clear that A is indeed the set defined in Definition 3.2.1. ■

Remark 2. For computation purposes, we will always use Definition 3.2.2 as the definition for type (II) Whitehead automorphisms.

Remark 3. The action of an automorphism on a word is defined as follows. Let $w = xyz\cdots$ be a word. Then $w\tau := (x\tau)(y\tau)(z\tau)\cdots$.

3.2.1 Some properties of Whitehead Automorphism

(p-i) *Given* (A,a)*, we have* $(A,a)^{-1} = (A - a + a^{-1}, a^{-1})$.

PROOF. Let $S = (A - a + a^{-1}, a^{-1})$. Using Definition 3.2.2, for $x \neq a, a^{-1}$, we have,

$$x(A,a)S = \begin{cases} (xa)S = xa^{-1}a = x, \text{ if } x \in A, x^{-1} \notin A \\ (a^{-1}xa)S = a^{-1}axa^{-1}a = x, \text{ if } x, x^{-1} \in A \\ (a^{-1}x)S = a^{-1}ax = x, \text{ if } x \notin A, x^{-1} \in A \\ xS = x, \text{ if } x, x^{-1} \notin A \end{cases} \tag{3.2}$$

Since a, a^{-1} are fixed by both (A,a) and S, they are fixed by $(A,a)S$. Therefore, $(A,a)(A-a+a^{-1},a^{-1}) = id$, where id is the identity automorphism. Similarly, it can be shown that $(A-a+a^{-1},a^{-1})(A,a) = id$. Hence, $(A,a)^{-1} = (A-a+a^{-1},a^{-1})$. ■

(p-ii) *Let $A, B \subset X^{\pm 1}$ and $a \in X^{\pm 1}$. Suppose that, $A \cap B = \{a\}$. Then, $(A,a)(B,a) = (A \cup B, a)$.*

PROOF. We see that, a and a^{-1} are fixed by (A,a), (B,a) and $(A \cup B, a)$. Therefore, we only need to look at all $x \in X^{\pm 1}$, for $x \notin \{a, a^{-1}\}$.

(a) For $x \in A \cup B$ and $x^{-1} \notin A \cup B$,

$$x(A,a)(B,a) = \begin{cases} (xa)(B,a) = xa, & \text{if } x \in A, x^{-1} \notin A \cup B \\ x(B,a) = xa, & \text{if } x \in B, x^{-1} \notin A \cup B. \end{cases} \tag{3.3}$$

So, $x(A,a)(B,a) = xa$, for $x \in A \cup B$ and $x^{-1} \notin A \cup B$.

(b) For $x, x^{-1} \in A \cup B$,

$$x(A,a)(B,a) = \begin{cases} (a^{-1}xa)(B,a), & \text{if } x, x^{-1} \in A \\ (xa)(B,a) = a^{-1}xa, & \text{if } x \in A, x^{-1} \in B \\ (a^{-1}x)(B,a) = a^{-1}xa, & \text{if } x \in B, x^{-1} \in A \\ x(B,a) = a^{-1}xa, & \text{if } x, x^{-1} \in B. \end{cases} \tag{3.4}$$

So, we have $x(A,a)(B,a) = a^{-1}xa$, for $x, x^{-1} \in A \cup B$.

(c) For $x \notin A \cup B$ and $x^{-1} \in A \cup B$,

$$x(A,a)(B,a) = \begin{cases} (a^{-1}x)(B,a) = a^{-1}x, & \text{if } x \notin A \cup B, x^{-1} \in A \\ x(B,a) = a^{-1}x, & \text{if } x \notin A \cup B, x^{-1} \in B. \end{cases} \tag{3.5}$$

So, $x(A,a)(B,a) = a^{-1}x$, for $x \notin A \cup B$ and $x \in A \cup B$.

(d) For $x, x^{-1} \notin A \cup B$,

$$x(A,a)(B,a) = x(B,a) = x \tag{3.6}$$

So, from the four cases above, we see that $(A,a)(B,a) = (A \cup B, a)$. ■

(p-iii) *Let A' be the complement of A. Then $(A', a^{-1})(A,a)^{-1} = (X^{\pm 1} - a, a^{-1}) = \kappa$, where κ is the conjugation by a, i.e., $x\kappa = axa^{-1}$, for any $x \in X^{\pm 1}$.*

PROOF. By using (p-i) and (p-ii), we have,

$$(A', a^{-1})(A, a)^{-1} = (A', a^{-1})(A - a + a^{-1}, a^{-1}), \text{ (using (p-i))} \tag{3.7}$$

$$= (X^{\pm 1} - a, a^{-1}). \text{ (using (p-ii))} \tag{3.8}$$

Now, for any $x \in X^{\pm 1} - a$, we have $x^{-1} \in X^{\pm 1} - a$. Therefore, $x(X^{\pm 1} - a, a^{-1}) = axa^{-1}$. Since a, a^{-1} are fixed by $(X^{\pm 1} - a, a^{-1})$, we get $(X^{\pm 1} - a, a^{-1}) = \kappa$. ■

ALTERNATE PROOF. Using (p-i), basically, we want to show that $(A', a^{-1})(A - a + a^{-1}, a^{-1}) = \kappa$. For $x \neq a, a^{-1}$, we have,

$$x(A', a^{-1})(A - a + a^{-1}, a^{-1}) = \begin{cases} (xa^{-1})(A - a + a^{-1}), \text{ if } x \in A', x^{-1} \notin A' \\ (axa^{-1})(A - a + a^{-1}, a^{-1}), \text{ if } x, x^{-1} \in A' \\ (ax)(A - a + a^{-1}, a^{-1}), \text{if } x \notin A', x^{-1} \in A' \\ x(A - a + a^{-1}, a^{-1}), \text{ if } x, x^{-1} \notin A' \end{cases} \tag{3.9}$$

$$= \begin{cases} axa^{-1}, \text{ for } x \notin A, x^{-1} \in A \\ axa^{-1}, \text{ for } x, x^{-1} \notin A \\ axa^{-1}, \text{ for } x \in A, x^{-1} \notin A \\ axa^{-1}, \text{ for } x, x^{-1} \in A. \end{cases} \tag{3.10}$$

We know that a and a^{-1} are fixed by $(A', a^{-1})(A - a + a^{-1}, a^{-1})$. Now, $a\kappa = aaa^{-1} = a$ and $a^{-1}\kappa = aa^{-1}a^{-1} = a^{-1}$. Hence, $(A', a)(A, a)^{-1} = \kappa$.

Now, $A' \cap (A - a + a^{-1}) = \{a^{-1}\}$. So, from (p-ii), we have $(A', a)(A - a + a^{-1}, a^{-1}) = (A' \cup A - a + a^{-1}, a^{-1}) = (X^{\pm 1} - a, a^{-1})$. ■

(p-iv) *Let $A, B \subset X^{\pm 1}$. Suppose that $a \in A$ and $b \in B$, with $a \neq b$, for some $a, b \in X^{\pm 1}$. Moreover, let $a \notin B, a^{-1} \in B, b \in A$ and $b^{-1} \notin A$. If $A - \{a, b\} = B - \{a^{-1}, b\}$, then $(A, a)(B, b) = \pi(A - b + b^{-1}, a)$, where π is a permutation that maps a to b^{-1} and b to a with everything else fixed.*

PROOF. For $x = a$, we have,

$$a(A, a)(B, b) = a(B, b) = b^{-1}a, \tag{3.11}$$

and

$$a\pi(A - b + b^{-1}, a) = b^{-1}(A = b + b^{-1}, a) = b^{-1}a. \tag{3.12}$$

For $x = b$, we have,

$$b(A,a)(B,b) = (ba)(B,b) = bb^{-1}a = a, \tag{3.13}$$

and

$$b\pi(A - b + b^{-1}, a) = a(A - b + b^{-1}) = a. \tag{3.14}$$

Now,for $x \neq a, a^{-1}, b, b^{-1}$,

(a) Let $x \in A - b + b^{-1}$ and $x \notin (A - b + b^{-1})$. Since $A - \{a,b\} = B - \{a^{-1}, b\}$, $x \in A - b + b^{-1} \implies x \in B$, and $x^{-1} \notin A - b + b^{-1} \implies x^{-1} \notin B$.
So, we have,

$$x(A,a)(B,b) = (xa)(B,b) = xbb^{-1}a = xa. \tag{3.15}$$

and

$$x\pi(A - b + b^{-1}, a) = x(A - b + b^{-1}, a) = xa. \tag{3.16}$$

(b) Let $x, x^{-1} \in A - b + b^{-1}$. Therefore, $x, x^{-1} \in B$.
So, we have,

$$x(A,a)(B,b) = (a^{-1}xa)(B,b) = a^{-1}bb^{-1}xbb^{-1}a = a^{-1}xa. \tag{3.17}$$

and

$$x\pi(A - b + b^{-1}, a) = x(A - b + b^{-1}, a) = a^{-1}xa. \tag{3.18}$$

(c) Let $x \notin A - b + b^{-1}$ and $x^{-1} \in A - b + b^{-1}$. Therefore, $x \notin B$ and $x^{-1} \in B$.
So,

$$x(A,a)(B,b) = (a^{-1}x)(B,b) = a^{-1}bb^{-1}x = a^{-1}x, \tag{3.19}$$

and

$$x\pi(A - b + b^{-1}) = x(A - b + b^{-1}) = a^{-1}x. \tag{3.20}$$

(d) Let $x, x^{-1} \notin A - b + b^{-1}$. Therefore, $x, x^{-1} \notin A - b + b^{-1}$.
So,

$$x(A,a)(B,b) = x(B,b) = x, \tag{3.21}$$

and

$$x\pi(A - b + b^{-1}, a) = x(A - b + b^{-1}, a) = x. \tag{3.22}$$

Hence, $(A,a)(B,b) = \pi(A - b + b^{-1}, a)$. ■

(p-v) *Let $\sigma = (A,a)$ and τ be a permutation. Then, $\tau^{-1}\sigma\tau = (A\tau, a\tau)$.*

PROOF. (a) Suppose, $x \in A\tau, x^{-1} \notin A\tau$. Then, $x = y\tau$, some $y \in A$. Therefore,

$$x\tau^{-1}\sigma\tau = y\sigma\tau = \begin{cases} (ya)\tau = x(a\tau), & \text{if } y^{-1} \notin A \\ (a^{-1}ya)\tau = (a\tau)^{-1}x(a\tau). & \text{if } y^{-1} \in A \end{cases} \tag{3.23}$$

Now, since $x = y\tau$, $x^{-1} = y^{-1}\tau$. If $y^{-1} \in A$, then $x^{-1} \in A\tau$, a contradiction. Therefore, $y^{-1} \notin A$. Hence, from (3.23), we have,

$$x\tau^{-1}\sigma\tau = x(a\tau) \tag{3.24}$$

.

(b) Suppose, $x, x^{-1} \in A\tau$. Then, $x = y\tau$, for some $y \in A$, and $x^{-1} = y^{-1}\tau$. So, $y^{-1} \in A$. Therefore,

$$x\tau^{-1}\sigma\tau = y\sigma^{-1}\tau = (a^{-1}ya)\tau = (a\tau)^{-1}x(a\tau). \tag{3.25}$$

(c) Suppose, $x \notin A\tau$ and $x^{-1} \in A\tau$. Let $x^{-1} = y\tau$, for some $y \in A$. So, $x = y^{-1}\tau$. Since $x \notin A\tau$, $y^{-1} \notin A$. So, we have,

$$x\tau^{-1}\sigma\tau = y^{-1}(A,a)\tau = (a^{-1}y^{-1})\tau = (a\tau)^{-1}x. \tag{3.26}$$

(d) Suppose, $x, x^{-1} \notin A\tau$. Therefore, $x\tau^{-1}, x^{-1}\tau^{-1} \notin A$. So, $x\tau^{-1}\sigma = x\tau^{-1}$. Therefore, we have

$$x\tau^{-1}\sigma\tau = x\tau^{-1}\tau = x. \tag{3.27}$$

Thus, we have $\tau^{-1}(A,a)\tau = (A\tau, a\tau)$, for any permutation τ. ■

(p-vi) *Let $\sigma = (A,a)$ and $\tau = (B,b)$, with $A \cap B = \varnothing$. Suppose that σ fixes b and b^{-1}, and τ fixes a as well as a^{-1}. Then $\tau^{-1}\sigma\tau = \sigma$ i.e., σ and τ commutes.*

PROOF. We observe that σ can fix b and b^{-1} if and only if $b^{-1} \notin A$. Similarly, a and a^{-1} are fixed by τ if and only if $a^{-1} \notin B$.

Now, we see that a, a^{-1}, b and b^{-1} are fixed by σ and τ. Therefore, the assertion holds for these letters. So, we are interested in the letters $x \neq a, a^{-1}, b, b^{-1}$.

(a) For $x \in A, x^{-1} \notin A$,

$$x\tau^{-1}\sigma\tau = \begin{cases} (bx)\sigma\tau = (bxa)\tau, \text{ if } x^{-1} \in B \\ x\sigma\tau = (xa)\tau, \text{ if } x^{-1} \notin B \cup A \end{cases} \tag{3.28}$$

$$= \begin{cases} bb^{-1}xa = xa, \text{ if } x^{-1} \in B \\ xa, \text{ if } x^{-1} \notin A \cup B \end{cases} \tag{3.29}$$

So, we have, $x\tau^{-1}\sigma\tau = xa$.

(b) For $x, x^{-1} \in A$,

$$x\tau^{-1}\sigma\tau = x\sigma\tau = (a^{-1}xa)\tau = a^{-1}xa \tag{3.30}$$

(c) For $x \notin A$, $x^{-1} \in A$,

$$x\tau^{-1}\sigma\tau = \begin{cases} (xb)\sigma\tau = (a^{-1}xb)\tau, \text{ if } x \in B \\ x\sigma\tau = (a^{-1}x\tau), \text{ if } x \notin B \cup A \end{cases} \tag{3.31}$$

$$= \begin{cases} a^{-1}xb^{-1}b = a^{-1}x, \text{ if } x \in B \\ a^{-1}x, \text{ if } x \notin B \cup A \end{cases} \tag{3.32}$$

So, $x\tau^{-1}\sigma\tau = a^{-1}x$.

(d) For $x, x^{-1} \notin A$,

$$x\tau^{-1}\sigma\tau = \begin{cases} (bxb^{-1})\sigma\tau = (bxb^{-1})\tau = bb^{-1}xbb^{-1} = x, \text{ if } x, x^{-1} \in B \\ (xb^{-1})\sigma\tau = (xb^{-1})\tau = xbb^{-1} = x, \text{ if } x \in B, x^{-1} \notin B \\ (bx)\sigma\tau = (bx)\tau = bb^{-1}x = x, \text{ if } x \notin B, x^{-1} \in B \\ x\sigma\tau = x\tau = x, \text{if } x, x^{-1} \notin B \end{cases} \tag{3.33}$$

So, $\tau^{-1}\sigma\tau = x$.

Hence, we have $\tau^{-1}\sigma\tau = \sigma$. ■

(p-vii) *Let $\sigma = (A, a)$ and $\tau = (B, b)$, with $A \cap B = \varnothing$. Suppose that, τ fixes both a and a^{-1}. Let $b^{-1} \in A$. Then, $\tau^{-1}\sigma\tau = (A + B - b, a)$.*

PROOF. First, we see that, a, a^{-1} are fixed by σ, τ and $(A + B - b, a)$. So, $\{a, a^{-1}\}\tau^{-1}\sigma\tau = \{a, a^{-1}\} = \{a, a^{-1}\}(A + B - b, a)$.

For $x = b$, we see that $b \xmapsto{\tau^{-1}} b \xmapsto{\sigma} a^{-1}b \xmapsto{\tau} a^{-1}b \equiv b(A+B-b, a)$. So, $b^{-1} \xmapsto{\tau^{-1}\sigma\tau} b^{-1}a \equiv b^{-1}(A + B - b, a)$.

Therefore, we look into the cases for $x \neq a, a^{-1}, b, b^{-1}$.

(i) For $x \in A+B-b$ and $x^{-1} \notin A+B-b$,

$$x\tau^{-1}\sigma\tau = \begin{cases} x\sigma\tau = (xa)\tau, \text{ if } x \in A, x^{-1} \notin A+B-b \\ (xb^{-1})\sigma\tau = (xb^{-1}a)\tau, \text{ if } x \in B-b, x^{-1} \notin A+b-b \end{cases} \tag{3.34}$$

$$= \begin{cases} xa, \text{ if } x \in A, x^{-1} \notin A+B-b \\ xbb^{-1}a = xa, \text{ if } x \in B-b, x^{-1} \in A+B-b \end{cases} \tag{3.35}$$

So, $x\rho_2^{-1} = xa$, for $x \in A+B-b$ and $x^{-1} \notin A+B-b$.

(ii) For $x, x^{-1} \in A+B-b$,

$$x\tau^{-1}\sigma\tau = \begin{cases} x\sigma\tau = (a^{-1}xa)\tau, \text{ if } x \in A, x^{-1} \in A \\ (bx)\sigma\tau = (a^{-1}bxa)\tau, \text{ if } x \in A, x^{-1} \in B-b \\ (xb^{-1})\sigma\tau = (a^{-1}xb^{-1}a)\tau, \text{ if } x \in B-b, x^{-1} \in A \\ (bxb^{-1})\sigma\tau = (a^{-1}bxb^{-1}a)\tau, \text{ if } x \in B-b, x^{-1} \in B-b \end{cases} \tag{3.36}$$

$$= \begin{cases} a^{-1}xa, \text{ if } x \in A, x^{-1} \in A \\ a^{-1}bb^{-1}xa = a^{-1}xa, \text{ if } x \in A, x^{-1} \in B-b \\ a^{-1}xbb^{-1}a = a^{-1}xa, \text{ if } x \in B-b, x^{-1} \in A \\ a^{-1}bb^{-1}xbb^{-1}a = a^{-1}xa, \text{ if } x \in B-b, x^{-1} \in B-b \end{cases} \tag{3.37}$$

So, $x\rho_2^{-1} = a^{-1}xa$, for $x, x^{-1} \in A+B-b$.

(iii) For $x \notin A+B-b$ and $x^{-1} \in A+B-b$,

$$x\tau^{-1}\sigma\tau = \begin{cases} x\sigma\tau = (a^{-1}x)\tau, \text{ if } x \notin A+B-b, x^{-1} \in A \\ (bx)\sigma\tau = (a^{-1}bx)\tau, \text{ if } x \notin A+B-b, x^{-1} \in B-b \end{cases} \tag{3.38}$$

$$= \begin{cases} a^{-1}x, \text{ if } x \notin A+B-b, x^{-1} \in A \\ a^{-1}bb^{-1}x = a^{-1}x, \text{ if } x \notin A+B-b, x^{-1} \in B-b \end{cases} \tag{3.39}$$

So, $x\rho_2^{-1} = a^{-1}x$, for $x \notin A+B-b$ and $x^{-1} \in A+B-b$.

(iv) For $x, x^{-1} \notin A+B-b$, both x and x^{-1} are fixed by τ and σ. So, we have,

$$x\tau^{-1}\sigma\tau = x\sigma\tau = x\tau = x. \tag{3.40}$$

Therefore, we see that, $\tau^{-1}\sigma\tau = (A+B-b, a)$, as desired. ■

(p-viii) *For a cyclic word w, we have $w(A', a^{-1}) = w(A, a)$.*

PROOF. If w is a cyclic word, then the inner automorphism does not change w. Therefore, from (p-iii), we have $w(A', a^{-1})(A, a)^{-1} = w$. This proves the result. ■

3.3. Product Counting

In this section, we define a function corresponding to a cyclic word and a set of cyclic words. The function counts the number of certain forms in the word or the set of words. We call this function the *product counting function*.

Definition 3.3.1. (**Product count corresponding to a cyclic word**)

- Let $A, B \subset X^{\pm 1}$. For a cyclic word w, we define a function $f_w : X^{\pm 1} \times X^{\pm 1} \to \mathbb{Z}$, such that, $f_w(x, y)$ = number of both the forms xy^{-1} and yx^{-1} in w. We denote $f_w(x, y)$ as $(x \cdot y)_w$, and call this the *product count* of x and y in w.

- For the sets $A, B \subset X^{\pm 1}$, we define the product count, $(A \cdot B)_w$, to be the number of forms xy^{-1} and yx^{-1} in w, for $x \in A$ and $y \in B$ i.e., $(A \cdot B)_w = \sum_{x \in A, y \in B} (x \cdot y)_w$.

Example 3.3.1. Let $w = xyz^{-1}$ be a cyclic word such that $x \in A, x^{-1} \in A'; y, y^{-1} \in A'$ and $z, z^{-1} \in A$. Then $(A \cdot A')_w = 3$. The counting goes as follows: 1 (for $xy \equiv x(y^{-1})^{-1}$) + 1 (for yz^{-1}) + 1 (for $z^{-1}x \equiv z^{-1}(x^{-1})^{-1}$).

Remark 4. In the calculation of $(A \cdot A')_w$, cyclic permutation has been taken to make the product count well-defined. To see this, we consider the following example.

Let $w = xyz^{-1}$ be a cyclic word such that $x \in A, x^{-1} \in A', y \in A', y^{-1} \in A, z \in A$ and $z^{-1} \in A$. Now, we calculate $A \cdot A'$ by not taking the cyclic permutation. So, $A \cdot A' = 1$. The counting goes as follows: 0 [for $x(y^{-1})^{-1}$] + 1 [for yz^{-1}].

Now, xyz^{-1} is the same word as $yz^{-1}x$. For $yz^{-1}x$, the counting goes as: 1 [for yz^{-1}] + 1 [for $z^{-1}(x^{-1})^{-1}$]. So, $A \cdot A' = 2$.

We often suppress the subscript w and write $x \cdot y$ or $A \cdot B$ for the product count, when it is clear that we are dealing with the word w.

3.3.1 Properties

Now we look into some properties of the product count.

(i) It is clear that for a cyclic word w, $A \cdot B \geq 0$.

(ii) The product count is symmetric i.e., $A \cdot B = B \cdot A$. This is true because $x \cdot y$ is symmetric, since we are counting either of the forms xy^{-1} or yx^{-1}.

(iii) Let $A, B, C \subseteq X^{\pm 1}$ and $A \cap B = \varnothing$, then product count is distributive i.e., $(A+B) \cdot C = A \cdot C + B \cdot C$, where $A+B$ is the disjoint union of A and B. The proof goes as follows,

$$\begin{aligned}(A+B) \cdot C &= \sum_{x \in A+B, y \in C} x \cdot y, \\ &= \sum_{x \in A \vee x \in B, y \in C} x \cdot y, \\ &= \sum_{x \in A, y \in C} x \cdot y + \sum_{x \in B, y \in C} x \cdot y, \text{ (since } A \cap B = \varnothing) \\ &= A \cdot C + B \cdot C.\end{aligned}$$

(iv) Since there can be no xx^{-1} or $x^{-1}x$ in a cyclic word for $x \in X^{\pm 1}$, we have $x \cdot x = 0$.

(v) We see that, for a fixed $a \in X^{\pm 1}$, $a \cdot X^{\pm 1} = \#$ of ax^{-1} and xa^{-1}, for $x \in X^{\pm 1}$. Therefore, it is clear that, $a \cdot X^{\pm 1}$ = total number of a and a^{-1} in the given word = $a^{-1} \cdot X^{\pm 1}$.

(vi) Let $B \subset A \subset X^{\pm 1}$. Then $(A-B) \cdot C = A \cdot C - B \cdot C$, where $A - B \equiv A \cap B'$, B' is the complement of B. We have, $A = (A-B) + B$. Therefore, using the distributive property, we get $A \cdot C = (A-B) \cdot C + B \cdot C$, which gives the desired result.

Definition 3.3.2. (**Product count for a set of cyclic words**) Let W be a finite set of cyclic words. For $x, y \in X^{\pm 1}$, we define, $(x \cdot y)_W = \sum_{w \in W} (x \cdot y)_w$. For $A, B \subset X^{\pm 1}$, we define, $(A \cdot B)_W = \sum_{w \in W} (A \cdot B)_w$.

Since $(A \cdot B)_W$ is the sum of $(A \cdot B)_w$, the above properties also hold for $(A \cdot B)_W$.

Lemma 3.3.3. *Let $A, B \subset X^{\pm 1}$ with $A \cap B \neq \varnothing$. Denote, $A_1 = A, A_2 = A', B_1 = B$ and $B_2 = B'$, where A' and B' are complements of A and B, respectively. Then,*

$$A \cdot A' + B \cdot B' = P_{11} \cdot P'_{11} + P_{22} \cdot P'_{22} + 2P_{12} \cdot P'_{21}, \tag{3.41}$$

where $P_{ij} = A_i \cap B_j$.

Proof. From the definition, we know that $A \cdot A'$= number of xy^{-1} and yx^{-1} in a cyclic word, for $x \in A$ and $y \in A'$. Now, $A = (A \cap B') + (A \cap B)$. Suppose, $(x \in A, y \in A')$ denote the number of xy^{-1} or yx^{-1} for $x \in A$ and $y \in A'$. Therefore, we can write,

$$A \cdot A' = (x \in A \cap B', y \in A') + (x \in A \cap B, y \in A'). \tag{3.42}$$

We also have $A' = A' \cap B + A' \cap B'$. So,

$$\begin{aligned} A \cdot A' = &(x \in A \cap B', y \in A' \cap B) \\ &+ (x \in A \cap B', y \in A' \cap B') + (x \in A \cap B, y \in A'). \end{aligned} \tag{3.43}$$

Similarly, we have,

$$\begin{aligned} B \cdot B' = &(x \in A' \cap B, y \in A \cap B') \\ &+ (x \in A' \cap B, y \in A' \cap B') + (x \in A \cap B, y \in B'). \end{aligned} \tag{3.44}$$

Now,

$$(x \in A \cap B', y \in A' \cap B) = (A \cap B') \cdot (A' \cap B) \equiv P_{12} \cdot P_{21}, \tag{3.45}$$

and

$$(x \in A' \cap B, y \in A \cap B') = (A' \cap B) \cdot (A \cap B') \equiv P_{21} \cdot P_{12} = P_{12} \cdot P_{21}. \tag{3.46}$$

For any sets X and Y, we have,

$$\#(X \cup Y) = \#X + \#Y - \#(X \cap Y). \tag{3.47}$$

Therefore,

$$\begin{aligned} (x \in A \cap B, y \in A' \cup B') = &(x \in A \cap B, y \in A') \\ &+ (x \in A \cap B, y \in B') - (x \in A \cap B, y \in A' \cap B') \end{aligned} \tag{3.48}$$

So,

$$\begin{aligned} (x \in A \cap B, y \in A') + (x \in A \cap B, y \in B') &= (x \in A \cap B, y \in A' \cup B') \\ &\quad + (x \in A \cap B, y \in A' \cap B') \\ &= (x \in A \cap B, y \in (A \cap B)') + (x \in A \cap B, y \in A' \cap B') \\ &\equiv P_{11} \cdot P'_{11} + (x \in A \cap B, y \in A' \cap B'). \end{aligned} \tag{3.49}$$

From $A = (A \cap B') + (A \cap B) + (A' \cap B)$, we have,

$$\begin{aligned} (x \in A \cap B', y \in A' \cap B') + (x \in A \cap B, y \in A' \cap B') &\\ + (x \in A' \cap B, y \in A' \cap B') &\\ = (x \in A \cup B, y \in A' \cap B') &\\ \equiv P'_{22} \cdot P_{22} \text{ (as } (A' \cap B')' = A \cup B). & \end{aligned} \tag{3.50}$$

Adding (3.43) and (3.44), and using (3.45),(3.46),(3.48),(3.49) & (3.50), we get,

$$A \cdot A' + B \cdot B' = P_{11} \cdot P'_{11} + P_{22} \cdot P'_{22} + 2P_{12} \cdot P_{21}, \tag{3.51}$$

which proves the lemma. ■

Remark 5. The proof of the lemma above can be simplified significantly by using $A = P_{11} + P_{12}$, $B = P_{21} + P_{11}$, $A' = P_{21} + P_{22}$, $B' = P_{12} + P_{22}$ and the distributive property of the product count.

3.4. Building up to the theorem

In this section, we give the proofs of some important results, which will be crucial for proving Whitehead's theorem in the following chapter.

Given a cyclic word w and $\tau = (A, a)$, we define $D(\tau, w) = |w\tau| - |w|$. In this section, our goal is to show,

$$D(\tau, w) = (A \cdot A')_{w\tau} - (a \cdot X^{\pm 1})_{w\tau}. \tag{3.52}$$

Let w' be the *unreduced cyclic word* obtained from w by replacing each letter x in w with $x\tau$ without any cancellation. For example, if $w = xy^{-1}x$, then $w' = xaa^{-1}y^{-1}xa$, for $x\tau = xa$ and $y^{-1}\tau = a^{-1}y^{-1}$.

Let w'' be the word resulting from deleting all the parts aa^{-1} and $a^{-1}a$ in w'. In the above example $w'' = xy^{-1}xa$.

Lemma 3.4.1. *w'' is a reduced word.*

Proof. Since w is reduced and w' is obtained from w by inserting a and a^{-1}, w' can contain parts xx^{-1} or $x^{-1}x$ only when $x = a$ i.e., in the form of aa^{-1} or $a^{-1}a$, where at least one of them is newly generated. Given $\tau = (A, a)$, a new a can arise only following a x, and a new a^{-1} can arise only preceding a x in w, for any $x \in X^{\pm 1}$, $x \neq a, a^{-1}$. *So, $a^{-1}a$ does not occur in w'.*
Now, we consider the following cases regarding the occurrence of aa^{-1}.

(i) Suppose that aa^{-1} arises from a part xy of w, $y \neq x^{-1}$, yielding $xaa^{-1}y$ in w'. Then xy in w'' is a reduced word.

(ii) Suppose that one of the letter in aa^{-1}, say a, was already present in w, while a^{-1} arises from the transformation. So, yax in w becomes either $yaa^{-1}x$; $y \neq x^{-1}, a^{-1}$ or $yaaa^{-1}x$; $y \neq a, a^{-1}$ in w', yielding yx or yax in w'', respectively. If a^{-1} was already present in w, $ya^{-1}x$ would become either $yaa^{-1}x$; $y \neq x^{-1}, a, a^{-1}$ or $yaa^{-1}a^{-1}x$; $y \neq a$, yielding yx or $ya^{-1}x$ in w'' respectively.

Therefore, we don't have any xx^{-1} or $x^{-1}x$ in w''. Hence, w'' is reduced. ■

Let D_1 = number of a or a^{-1} introduced while passing from w to w' that remain in w'', and D_2 = number of old a or a^{-1} in w that cancel with new a^{-1} or a while passing from w' to w''.

Lemma 3.4.2. $D(\tau, w) = D_1 - D_2$

Proof. By definition, we have $D(\tau, w) = |w''| - |w|$. Notice that, the extra length of $|w''|$ comes from the new letters a or a^{-1}. Suppose, some of old a or a^{-1} in w do not occur in w''. Therefore, $|w''|$= (number of new a or a^{-1} in w'')+$|w|$−(number of old a or a^{-1} which have canceled with a new a^{-1} or a in w'). So, $|w''| = D_1 + |w| - D_2$. Hence, the claim follows. ■

Lemma 3.4.3. $D_1 = (A - a) \cdot A'$

Proof. Our aim is to count the number of new a or a^{-1} that remain in w'' while passing from w to w'. We see that, new a or a^{-1} occur in w' from a letter $x \in A - a$ in w, $x \neq a, a^{-1}$, in the form of $x\tau = xa$ or $a^{-1}xa$.

Claim 3.4.4. *The newly introduced letter a, following $x \in A - a$ in the part xy^{-1} in w, fails to cancel if and only if $y \in A'$.*

Proof. ($\Longleftarrow$) Suppose, $y \in A'$ in xy^{-1} for $x \in A - a$. Then $y\tau$ is either $a^{-1}y$ or y. So, $y^{-1}\tau = y^{-1}a$ or y^{-1}. Therefore, $(xy^{-1})\tau$ is equal to either $xay^{-1}a$, xay^{-1}, $a^{-1}xay^{-1}$ or $a^{-1}xay^{-1}a$. We see that, in all the cases, the cancellation of a following x fails.

($\Longrightarrow$) We will prove this in contra-positive way. Suppose, $y \in A$ in xy^{-1} of w, with $x \in A - a$. Then $y\tau = ya$ or $a^{-1}ya$. So, $y^{-1}\tau = a^{-1}y^{-1}$ or $a^{-1}y^{-1}a$. Therefore, the a following x gets canceled in this case. q.e.d

Similarly, a new a^{-1} preceding x^{-1}, for $x \in A - a$, gets canceled in yx^{-1} of w if and only if $y \in A$. Indeed, if $y \in A$, then $y\tau = ya$ or $a^{-1}ya$. We have, $x\tau = xa$ or $a^{-1}xa$, for $x \in A - a$. Therefore, $x^{-1}\tau = a^{-1}x^{-1}$ or $a^{-1}x^{-1}a$. We see that in all the cases the said a^{-1} gets cancelled. So, we see that, it will not cancel if $y \in A'$.

Therefore, from Claim 3.4.4 and the above paragraph, we see that, $D_1 = (A - a) \cdot A$. ■

Lemma 3.4.5. $D_2 = (A - a) \cdot a$

Proof. We want to count the number of old a or a^{-1} those cancel with new a^{-1} or a in w'.

Claim 3.4.6. *An old a in w cancels with a new a^{-1} in w' if and only if it occurs as a part of ax^{-1} for $x \in A - a$ in w.*

Proof. If a occurs as a part of ax^{-1} for $x \in A-a$. Then under (A, a), x maps into xa or $a^{-1}xa$ i.e., $ax^{-1} \mapsto aa^{-1}x^{-1}$ or $aa^{-1}x^{-1}a$, respectively. Hence, the cancellation happens. On the other hand, if a occurs in ax^{-1} but $x \notin A - a$. Then under (A, a), ax^{-1} maps to ax^{-1} or $ax^{-1}a$, failing to cancel the old a. ■

Similarly, a^{-1} in w cancels with a new a in w' if and only if it occurs as a part of xa^{-1} for $x \in A - a$.
Therefore, from Claim 3.4.6 and the above sentence, we see that, $D_2 = a \cdot (A - a)$. ■

Now, we prove (3.52) as the following proposition.

Proposition 3.4.7. *Let w be a cyclic word and $\tau = (A, a)$. Then, $D(\tau, w) = (A \cdot A')_{w\tau} - (a \cdot X^{\pm 1})_{w\tau}$.*

Proof. We have,

$$\begin{aligned} D(\tau, w) &= D_1 - D_2, \text{ (from Lemma 3.4.2)} \\ &= (A - a) \cdot A' - a \cdot (A - a), \text{ (using Lemma 3.4.3 and 3.4.5)} \\ &= A \cdot A' - a \cdot (A + A') + a \cdot a, \text{ (using the properties of the product count)} \\ &= A \cdot A' - a \cdot X^{\pm 1}, \text{ as } (a \cdot a = 0). \end{aligned}$$

■

CHAPTER 4

WHITEHEAD'S THEOREM FOR CYCLIC WORDS

In this chapter, we prove Whitehead's theorem, which solved the minimization and decision problem. In the first section, we prove a rather restricted version of the theorem following Higgins and Lyndon [Higgins and Lyndon, 1974]. The second section contains the proof of Whitehead's theorem and the decision algorithm. In the last section, we prove Whitehead's theorem for a finite set of cyclic words.

4.1. Whitehead's theorem (restricted version)

First, we prove the following lemma, which is crucial for proving the main theorem. This lemma is also known as the *peak reduction lemma*. The following picture is the schematic of the lemma. We see that the name *peak reduction* is justified.

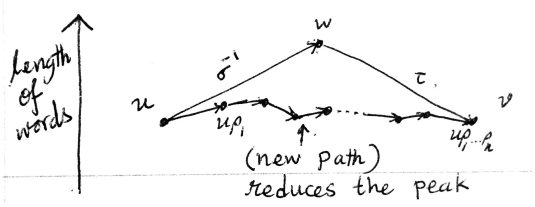


Figure 4.1: Schematic diagram for the peak reduction lemma

Lemma 4.1.1. *(**Peak reduction lemma**) Let w be a fixed cyclic word and $u = w\sigma, v = w\tau$ where $\sigma, \tau \in \Omega$. Assume that $|u| \leq |w|$ and $|v| \leq |w|$ with at least one of inequality strict. Then $v = u\rho_1 \cdots \rho_n$, $n \geq 0$, where $\rho_1, \ldots, \rho_n \in \Omega$, and for $0 < i < n, |u\rho_1 \cdots \rho_i| < |w|$.*

Proof. We write $u_i = u\rho_1 \cdots \rho_i$, for $0 \leq i \leq n$. From the assumptions of the statement of the lemma, we have, either $|u| < |w|$ or $|v| < |w|$. So,

$$|w| > \frac{1}{2}(|u| + |v|) \tag{4.1}$$

We will prove the lemma by going through several cases.

Case 1. (***τ is a permutation***) Since a permutation automorphism does not change the length of a word, we get $|u\tau| = |u|$ and $|v| = |w|$. We know that, $v = w\tau$. We rewrite v as follows,

$$v = w\tau = u\sigma^{-1}\tau = u\tau(\tau^{-1}\sigma^{-1}\tau). \tag{4.2}$$

Letting $\rho_1 = \tau$ and $\rho_2 = \tau^{-1}\sigma^{-1}\tau$, we have $v = u\rho_1\rho_2$, with $\rho_1 = \tau \in \Omega$, $\rho_2 = ((A - a + a^{-1})\tau, a^{-1}\tau) \in \Omega$ (from (p-v)), and $|u\rho_1| = |u\tau| = |u| < |w|$.

In view of the previous case, we can assume that, neither σ nor τ are permutations. Let $\sigma = (A, a), \tau = (B, b)$.

Case 2. (***A*** $\cap$ ***B*** $= \varnothing$**, and** ***b*** $= a^{-1}$) We have, $v = w\tau = u\sigma^{-1}\tau$. Letting $\sigma^{-1}\tau = \rho_1$, we have $v = u\rho_1$. Now, $\sigma^{-1}\tau = (A - a + a^{-1}, a^{-1})(B, a^{-1})$. We observe that $(A - a + a^{-1}) \cap B = \{a^{-1}\}$. Therefore, using (p-ii), we get, $\rho_1 = \sigma^{-1}\tau = (A + b - a, a^{-1}) \in \Omega$. So, with $n = 1$, $|u_i| < |w|$ is vacuously true for $0 < i < 1$.

Case 3. (***A*** $\cap$ ***B*** $= \varnothing$ **and** $a^{-1} \in B'$) First, we will show the following.

Claim 4.1.2. $|u\tau| < |w|$.

proof. Let w' and u' be the unreduced cyclic words obtained from action of τ on w and u, respectively. First, we show that,

$$|u'| - |u| = |w'| - |w|. \tag{4.3}$$

proof of **(4.3)**. Under σ, any x in w with $x \in B - b$, maps to $a^{-1}x$ or x in u. Therefore, there are one to one correspondences between the occurrences of all the letters $x \in B - b$ in w and the letters $x \in u$. Now, under τ, the letters $x \in B - b$ in both the words w and u will map into either xb or $b^{-1}xb$ in w' and u', while a, a^{-1} and b will remain fixed, since $a, a^{-1} \notin B$. So, $|u'| - |u| = \#$ of new b or b^{-1} introduced $= |w'| - |w|$. ■

Let $w\tau$ and $u\tau$ be the words obtained from deleting bb^{-1} from w' and u', respectively. We will show from (4.3) that $|u\tau| - |u| = |w\tau| - |w|$. We only consider bb^{-1} because, as seen earlier, there are no $b^{-1}b$ in u' or w'. Now, bb^{-1} can only occur in w' as $xbb^{-1}, bb^{-1}y^{-1}$ or $xbb^{-1}y^{-1}$ from xb^{-1}, by^{-1} or xy^{-1}, respectively, for $x, y \in B - b$. Since x, y, b are not in A, under σ, any $z \in \{x, y, b\}$ is mapped into $a^{-1}z$ or z. Therefore, the parts xb^{-1}, by^{-1} and xy^{-1} from w are preserved in u. Hence, this gives rise to bb^{-1} in u'. So, there are as many cancellations of bb^{-1} in u' as in w'. Now, since $u = w\sigma$ was already reduced in terms of deletion of aa^{-1}, we see that only possible cancellations from u' to $u\tau$ are bb^{-1}. Thus, from (4.3), we have, $|u\tau| - |u| = |w\tau| - |w|$. Now, using $w\tau = v$ and $|u| + |v| < 2|w|$ from (4.1), we get $|u\tau| < |w|$. ■

Now, rewriting $v = w\tau$, we get $v = u\tau\tau^{-1}\sigma^{-1}\tau$. Letting $\rho_1 = \tau$ and $\rho_2 = \tau^{-1}\sigma^{-1}\tau$, we have $v = u\rho_1\rho_2$. From Claim 4.1.2, we get, $|u\rho_1| = |u\tau| < |w|$. It only remains to show that $\rho_2 \in \Omega$.

Claim 4.1.3. $\rho_2 = \tau^{-1}\sigma^{-1}\tau \in \Omega$.

proof. We consider two cases depending on where b^{-1} is located.

(c-i) $\underline{\boldsymbol{b^{-1} \in A'}:}$ We see that a, a^{-1} are fixed by τ and b, b^{-1} are fixed by σ. Therefore, using (p-vi), we have $\tau^{-1}\sigma^{-1}\tau = \sigma^{-1}$, whence, $\rho_2 \in \Omega$.

(c-ii) $\underline{\boldsymbol{b^{-1} \in A}:}$ To prove $\rho_2 \in \Omega$, we will show that, $\rho_2^{-1} = \tau^{-1}\sigma\tau = (A + B - b, a)$. Therefore, we will have $\rho_2 = (A + B - b - a + a^{-1}, a^{-1})$, proving $\rho_2 \in \Omega$.

Since a, a^{-1} are fixed by τ and $b^{-1} \in A$, from (p-vii), we see that $\rho_2^{-1} = \tau^{-1}\sigma\tau = (A + B - b, a)$.

Thus, in view of the cases above, we get $\rho_2 \in \Omega$. ■

Case 4. ($\boldsymbol{A \cap B = \varnothing}$) This is the general case for $A \cap B = \varnothing$. In the view of Case 2, we can assume that $a \neq b^{-1}$, and by Case 3, we assume that $a^{-1} \in B$, $b^{-1} \in A$. Since A and B are disjoint, we have $a \neq b$.

Let $\sigma' = (A, b^{-1})$ and $\tau' = (B, a^{-1})$. We will show that, for the word w, $D(\sigma') + D(\tau') = D(\sigma) + D(\tau)$. Indeed, using $a^{-1} \cdot X^{\pm 1} = a \cdot X^{\pm 1}$ and $b \cdot X^{\pm 1} = b^{-1} \cdot X^{\pm 1}$, we have,

$$D(\sigma') + D(\tau') = A \cdot A' - b^{-1} \cdot X^{\pm 1} + B \cdot B' - a^{-1} \cdot X^{\pm 1} \tag{4.4}$$

$$= A \cdot A' - b \cdot X^{\pm 1} + B \cdot B' - a \cdot X^{\pm 1} \tag{4.5}$$

$$= A \cdot A' - a \cdot X^{\pm 1} + B \cdot B' - b.X^{\pm 1} \tag{4.6}$$

$$= D(\sigma) + D(\tau). \tag{4.7}$$

Now, we see that,

$$D(\sigma') + D(\tau') = D(\sigma) + D(\tau) = |w\sigma| - |w| + |w\tau| - |w| \tag{4.8}$$

$$= |u| + |v| - 2|w| < 0, \text{ from (4.1)}. \tag{4.9}$$

Therefore, at least one of $D(\sigma')$ and $D(\tau')$ has to be negative. Without loss of generality, suppose, $D(\tau') < 0$. This implies, $|w\tau'| < |w|$. Now, rewriting v, we have, $v = w\tau = u\sigma^{-1}\tau'\tau'^{-1}\tau$. Letting $\rho_1 = \sigma^{-1}\tau'$ and $\rho^* = \tau'^{-1}\tau$, we have, $v = u\rho_1\rho^*$. Now, from (p-ii), we see that, $\rho_1 = \sigma^{-1}\tau' = (A + B - a, a^{-1})$. Hence, $\rho_1 \in \Omega$, and from (p-iv), we see that, $\rho^* = \pi(A - b + b^{-1}, a)$, where π is the permutation that maps a to b^{-1} and b to a, with everything else fixed.

Letting $\rho_2 = \pi$ and $\rho_3 = (A - b + b^{-1}, a)$, we get $v = u\rho_1\rho_2\rho_3$ with $\rho_1, \rho_2, \rho_3 \in \Omega$. We have, $|u\rho_1\rho_2| = |u\rho_1|$, since ρ_2 is a permutation. Now, $|u\rho_1| = |w\sigma\sigma^{-1}\tau'| = |w\tau'| < |w|$.

Case 5. ($\boldsymbol{A \cap B \neq \varnothing}$) This is the general case. We will reduce this to Case 4. From (4.9), we have $D(\sigma) + D(\tau) < 0$, which gives,

$$A \cdot A' + B \cdot B' - a \cdot X^{\pm 1} - b \cdot X^{\pm 1} < 0. \tag{4.10}$$

We write $A_1 = A, A_2 = A', B_1 = B, B_2 = B'$ and $P_{ij} = A_i \cap B_j$, for $i, j \in \{1,2\}$. Now, from (3.41) of Lemma 3.3.3, we have,

$$A \cdot A' + B \cdot B' = P_{11} \cdot P'_{11} + P_{22} \cdot P'_{22} + 2P_{12} \cdot P'_{21} \tag{4.11}$$

Since $P_{12} \cdot P_{21} \geq 0$, we have,

$$A \cdot A' + B \cdot B' \geq P_{11} \cdot P'_{11} + P_{22} \cdot P'_{22}. \tag{4.12}$$

From (4.12), interchanging B and B', we have,

$$A \cdot A' + B' \cdot B \geq P_{12} \cdot P'_{12} + P_{21} \cdot P'_{21}. \tag{4.13}$$

Now, subtracting $a \cdot X^{\pm 1} + b \cdot X^{\pm 1}$ from the inequalities (4.12) and (4.13), and using (4.10), we get the following inequalities, respectively,

$$P_{11} \cdot P'_{11} + P_{22} \cdot P'_{22} - a \cdot X^{\pm 1} - b \cdot X^{\pm 1} < 0, \tag{4.14}$$

$$P_{12} \cdot P'_{12} + P_{21} \cdot P'_{21} - a \cdot X^{\pm 1} - b \cdot X^{\pm 1} < 0. \tag{4.15}$$

Let x stand for one of the a, a^{-1}, b and b^{-1}, which need not all be distinct. Let $P(x)$ denote the set P_{ij} to which x belongs i.e., $P(x) = P_{ij}$, if and only if $x \in P_{ij}$. It is clear that $x^{-1} \notin P(x)$. To see this, lets look at an example. Suppose $x = a$ and $a \in P_{11}$, then a^{-1} can not be in P_{11} because of the construction of the set A for Whitehead automorphism (A, a).

We denote Whitehead automorphism $(P(x), x)$ as φ_x.
We shall deduce that φ_x decreases the length of w. First, we show the following claim.

Claim 4.1.4. *$D(\varphi_x) < 0$, for some x, where $\varphi_x = (P(x), x)$.*

proof. We consider the following two cases.

(cs-i) (***Each $\boldsymbol{P_{ij}}$ contains one of $\boldsymbol{a, a^{-1}, b, b^{-1}}$***) Using $a \cdot X^{\pm 1} = a^{-1} \cdot X^{\pm 1}$ and $b \cdot X^{\pm 1} = b^{-1} \cdot X^{\pm 1}$, we have,

$$\sum_x D(\varphi_x) = \sum_{i,j} P_{ij} \cdot P'_{ij} - \sum_x x \cdot X^{\pm 1} \tag{4.16}$$

$$= \sum_{i,j} P_{ij} \cdot P'_{ij} - 2(a \cdot X^{\pm 1} + b \cdot X^{\pm 1}) \tag{4.17}$$

$$< 0, \quad \text{(adding (4.14) and (4.15))}. \tag{4.18}$$

Therefore, at least one of $D(\varphi_x) < 0$, for some x.

(cs-ii) (***One of the P_{ij} does not contain any a, a^{-1}, b, b^{-1}***) Suppose, P_{ij} does not contain any a, a^{-1}, b, b^{-1}. Denote $a_1 = a, a_2 = a^{-1}, b_1 = b$, and $b_2 = b^{-1}$. Now, we have, $a_i \in A_i = (A_i \cap B) + (A \cap B') = P_{i1} + P_{i2}$. So, $a_i \in P_{ik}$, for $k \neq j$. Similarly, $b_j \in B_j = P_{1j} + P_{2j}$. Therefore, $b_j \in P_{lj}$, for $l \neq i$. We have,

$$D(\varphi_{a_i}) + D(\varphi_{b_j}) = P_{ik} \cdot P'_{ik} + P_{lj} \cdot P'_{lj} - a_i \cdot X^{\pm 1} - b_j \cdot X^{\pm 1}. \tag{4.19}$$

Since $i, j, k, l \in \{1, 2\}$, we have $k = i \iff l = j$, using $k \neq j$ and $l \neq i$. So, from (4.19), we get,

$$D(\varphi_{a_i}) + D(\varphi_{b_j}) = P_{ii} \cdot P'_{ii} + P_{jj} \cdot P'_{jj} - a_i \cdot X^{\pm 1} - b_j \cdot X^{\pm 1} \tag{4.20}$$

$$< 0, \quad \text{(by (4.14))}, \tag{4.21}$$

for $i \neq j$.
For $i = j$, we have $k = l$, since $i, j, k, l \in \{1, 2\}$. So, from (4.19), we get,

$$D(\varphi_{a_i}) + D(\varphi_{b_i}) = P_{ik} \cdot P'_{ik} + P_{ki} \cdot P'_{ki} - a_i \cdot X^{\pm 1} - b_i \cdot X^{\pm 1} \tag{4.22}$$

$$< 0, \quad \text{(by (4.15))}, \tag{4.23}$$

Thus, $D(\varphi_x) < 0$, for some x.

■

Now, we prove the following proposition.

Proposition 4.1.5. *At least one of the Whitehead automorphisms $\varphi_x \equiv (P(x), x)$ decreases the length of w.*

proof. We assume that x is either a or a^{-1}. Notice that,

$$a \in P_{11} + P_{12} = A, \tag{4.24}$$

and

$$a^{-1} \in P_{21} + P_{22} = A'. \tag{4.25}$$

We deduce that, we can assume $x = a$. This is possible because $w(A, a) = w(A', a^{-1})$ (from (p-viii)). Therefore, replacing (A, a) with (A', a^{-1}) does not change the action on w.

Assuming $x = a$, we get $P(x)$ to be P_{11} or P_{12}, from (4.24). Similarly, from (p-viii), we can replace (B, b) with (B', b^{-1}). Now, with this replacement, we get, $P(x) = P_{12} = A \cap B'$. So, we have, $a \in B'$, and by Claim 4.1.4, $D(\varphi_a) \equiv D(A \cap B', a) < 0$. Therefore, $|w\varphi_a| < |w|$. ■

Denote, $w_1 = w\varphi_a$. Using $w(A,a) = w(A', a^{-1})$ (from (p-viii)) and $u = w(A,a)$, we have $w = u(A', a^{-1})^{-1} = u(A' - a^{-1} + a, a)$. Hence, $w_1 = w\varphi_a = u(A' - a^{-1} + a, a)\varphi_a = u\rho_1$, with $\rho_1 = (A' - a^{-1} + a, a)(A \cap B', a)$. Now, using (p-ii), we have, $(A' - a^{-1} + a, a)(A \cap B', a) = ((A' - a^{-1}) \cup (A \cap B'), a) = ((X^{\pm 1} - a^{-1}) \cap (A' \cup B' - a^{-1}), a) = (A' \cup B' - a^{-1}, a)$, whence, $\rho_1 \in \Omega$.

Now, with $w_1 = w(A \cap B', a)$, $v = w\tau$, $|w_1| < |w|$ and $(A \cap B') \cap B = \varnothing$, we are reduced to Case 4. Therefore, we get, at most three Whitehead automorphisms ρ_2, ρ_3, ρ_4 such that $v = w_1\rho_2\rho_3\rho_4$, where, $|w_1\rho_2|, |w_1\rho_2\rho_3| < |w|$. Substituting, $w_1 = u\rho_1$, we get, $v = u\rho_1\rho_2\rho_3\rho_4$, with length of all the intermediate words less than w, proving the lemma for this case.

This finishes proof of the peak reduction lemma. ■

Remark 6. Notice that, our choice of $x = a$ and Whitehead automorphisms (A, a) and (B', b^{-1}) gave us $(A \cap B', a)$ as a length decreasing automorphism for w.

So, depending on the choices of x, we have automorphisms $(A \cap B, a)$, $(A' \cap B, a^{-1})$ and $(A' \cap B', a^{-1})$ which decrease length of w. We observe that, since $(A' \cap B') \cap B = \varnothing$, $(A' \cap B', a^{-1})$ is the only automorphism that will work in the proof of the above proposition, other than $(A \cap B', a)$. Note that, using $(A' \cap B', a^{-1})$ corresponds to replacing a with a^{-1}.

Since both $A \cap B$ and $A' \cap B$ are not disjoint with B, using these we can not reduce the above case to Case 4. Hence, they can not be used in the proof.

Note. If x is either b or b^{-1}, we interchange $a \leftrightarrow b$ and $A \leftrightarrow B$, which amounts to switching $\sigma = (A, a)$ and $\tau(B, b)$. Then proceed similarly.

Now, using the above lemma, we prove a rather restricted version of Whitehead's theorem.

Theorem 4.1.6. *Let w and $\bar{w}$ be cyclic words, let $\bar{w} = w\alpha$ for some $\alpha \in Aut(F)$, and suppose that $|\bar{w}|$ is an automorphic minimal word of w. Then, there exist $\tau_1, \ldots, \tau_n \in \Omega$, $n \geq 0$, finite, such that, for $0 \leq i \leq n$, writing $w_i = w\tau_1 \cdots \tau_i$, one has $w_n = \bar{w}$, and*

$$|w_i| \leq |w|, \text{ for } 1 \leq i < n, \tag{4.26}$$

with strict inequality unless w also has the minimum length i.e., $|w| = |\bar{w}|$.

Proof. Let w and $\bar{w} = w\alpha$ be given and satisfy the hypothesis of the theorem. Since the Nielsen transformation is subset of Whitehead automorphisms, and generates $\mathrm{Aut}(F)$ [Nielsen, 1918][Nielsen, 1924][Wade, 2014], for $\alpha \in \mathrm{Aut}(F)$, we can write $\alpha = \tau_1 \cdots \tau_n$, for some $\tau_1, \ldots, \tau_n \in \Omega$. If this α satisfies (4.26), then we are done.

If not, then we proceed as follows. Let $m = \max\{|w_i| : 0 < i < n\}$, where $w_i = w\tau_1 \cdots \tau_i$. Since α does not satisfy (4.26), we have[1] $n \geq 2$ and $m \geq |w| > |\bar{w}|$ or $m > |w| = |\bar{w}|$. The idea is to use the peak reduction lemma and get a new path which completely avoids the words of length m.

Let i be the largest index such that $|w_i| = m$. Then, we get[2] $|w_{i-1}| \leq |w_i|$ and $|w_{i+1}| < |w_i|$. We have $w_{i-1} = w_i\tau_i^{-1}$ (from $w_i = w_{i-1}\tau_i$) and $w_{i+1} = w_i\tau_{i+1}$. Now, applying Lemma 4.1.1 we get,

$$w_{i+1} = w_{i-1}\rho_1 \cdots \rho_k, \;\; k > 0, \rho_j \in \Omega \text{ for all } j, \tag{4.27}$$

with

$$|w_{i-1}\rho_1 \cdots \rho_j| < |w_i| = m, \;\; \text{for } 0 < j < k. \tag{4.28}$$

Therefore, we get a new path,

$$\tau_1 \cdots \tau_{i-1}\rho_1 \cdots \rho_k\tau_{i+2} \cdots \tau_n, \tag{4.29}$$

between w and $\bar{w}$, avoiding w_i. So, we see that by introducing a new path, the number of words of length m go down exactly by one.

Now, suppose that there exists $l < i$ maximal such that, $|w_l| = m$. Then, similarly, the peak reduction lemma gives us a new path, which avoids w_l altogether. We repeat this process to eliminate all the words of length m. This gives us $m' \leq m$, where m', similar to m, is the maximum of all the intermediate words corresponding to path (4.29).

We repeat this whole procedure first on the number of words of lengths m and then on m, until we reach $\widetilde{m} \leq |w|$. This proves the theorem. ■

We get the following corollaries from the equality part of the theorem.

Corollary 4.1.7. *Let w be a cyclic word. Suppose that w_1 and w_2 be automorphic minimal words i.e., $|w_1|, |w_2| \leq |w|$ and $|w_1| = |w_2|$. Then, there exist finitely many Whitehead automorphisms $t_1, \ldots, t_n$, such that, $|w_1| = |w_1 t_1| = \cdots = |w_1 t_1 \cdots t_n|$ and $w_2 = w_1 t_1 \cdots t_n$.*

Corollary 4.1.8. *Let u and v be cyclic words. Suppose, u_{min} and v_{min} be automorphic minimal words of u and v, respectively. Suppose there exists $\alpha \in Aut(F)$, such that $u_{min}\alpha = v_{min}$, then α can be written as a product of finitely many Whitehead automorphisms $t_1, \ldots, t_n$ such that $|u_{min}| = |u_{min}t_1| = \cdots = |u_{min}t_1 \cdots t_n|$, with $u_{min}t_1 \cdots t_n = v_{min}$.*

[1] Since $n = 1$ implies $\alpha = \tau_1$, we get $w\tau_1 = w\alpha = \bar{w}$. Therefore, $|\bar{w}| = |w\tau_1| \leq |w|$ is always true, for $n = 1$. The conditions for m follows by noticing, as per (4.26), that $|w_i| < |w|$, when $|\bar{w}| < |w|$ and $|w_i| = |w|$, when $|\bar{w}| = |w|$.

[2] It is possible that $|w_{i-1}|$ is also equal to m. Hence, the inequality $|w_{i-1} \leq |w_i|$. Now, it follows from the maximality of i and m that, $|w_{i+1}| < |w_i|$.

Note. Corollary 4.1.8 will help us to produce the *finite sequence algorithm* in the following section.

4.2. Whitehead's Minimization Theorem and Algorithm

In this section, we will discuss the decidability problem which says that given two cyclic words in a free group of finite rank to decide whether there exists an automorphism carrying the word to the other. First, we prove the theorem, then we discuss the algorithm.

Theorem 4.2.1. *(**Whitehead's minimization theorem for cyclic words**) Let w be a cyclic word in F. Suppose that $\bar{w}$ is an automorphic minimal word i.e., length of $\bar{w}$ is minimum among the orbit of w. Then, there exist Whitehead automorphisms $\tau_0, \tau_1, \ldots, \tau_n$, for some integer n, such that $\bar{w} = w\tau_0 \cdots \tau_n$ and*

$$|w\tau_0 \cdots \tau_n| \leq |w\tau_0 \cdots \tau_{n-1}| \leq \cdots \leq |w\tau_0| \leq |w|. \tag{4.30}$$

Proof. Define, $\text{dist}(w, \bar{w}) := |w| - |\bar{w}|$. Note that, $\text{dist}(w, \bar{w})$ is a non negative integer. We prove the theorem by induction.
Let S_m be the following statement :

If $0 \leq \text{dist}(w, \bar{w}) \leq m$, for some $m \in \mathbb{N}$, then there exist $\tau_1, \ldots, \tau_n$, such that $\bar{w} = w\tau_1 \cdots \tau_n \in \Omega$ and $|w\tau_1 \cdots \tau_n| \leq |w\tau_1 \cdots \tau_{n-1}| \leq \cdots \leq |w\tau_1| \leq |w|$.

Suppose, $0 \leq \text{dist}(w, \bar{w}) \leq 1$. Corollary 4.1.7 takes care of the case $\text{dist}(w, \bar{w}) = 0$. For $0 < \text{dist}(w, \bar{w}) \leq 1$, by Theorem 4.1.6, there exists at least one Whitehead automorphism, $\rho_0 \in \Omega$ such that $|w\rho_0| < |w|$. Therefore, we must have $|w\rho_0| = |\bar{w}|$, since dist(-, -) ≥ 0. Now, from Corollary 4.1.7, there exist $\rho_1, \ldots, \rho_k$ such that $\bar{w} = (w\rho_0)\rho_1 \cdots \rho_k$ and $|(w\rho_0)\rho_1 \cdots \rho_i| = |w\rho_0|$, for $1 \leq i \leq k$.

Assume, S_m to be true.

Now, proving S_{m+1} will prove the theorem. Let $0 \leq \text{dist}(w, \bar{w}) \leq m+1$. By Theorem 4.1.6, there exists at least one Whitehead automorphism, say τ_0, such that, $|w\tau_0| \leq |w|$. This implies $0 \leq \text{dist}(w\tau_0, \bar{w}) \leq m$. Therefore, from S_m, we get $\tau_1, \ldots, \tau_n \in \Omega$, such that, $\bar{w} = w\tau_0\tau_1 \cdots \tau_n$ and $|w\tau_0| \geq |w\tau_0\tau_1| \geq \cdots | \geq |w\tau_0\tau_1 \cdots \tau_n|$. Since $|w| \geq |w\tau_0|$, we get (4.30). ■

4.2.1 Algorithms

The algorithm consists of two parts. We call the first part, as *Whitehead Minimization algorithm* and the second part, as the *Finite Sequence algorithm*, and

together it is called *Whitehead algorithm.*

We have seen in the first chapter that there have been a lot of efforts to improve the algorithm. We provide the algorithm without keeping the computational complexity in mind.

Whitehead Minimization algorithm

Given a cyclic word w, the problem is to produce an algorithm to find an automorphic minimal word by applying a sequence of Whitehead automorphisms. The following algorithm follows from Haralick, Miasnikov and Myasnikov [Haralick et al., 2005]. We refer to §2 of the paper and [Miasnikov and Myasnikov, 2004] and [Myasnikov and Haralick, 2006] for the improved version of the algorithm.

- Let $w \in F_n$ be the given cyclic word, and Ω be the set of all Whitehead automorphisms, which is a finite set.
- *Whitehead Length Reduction Routine (WLR):* For each $t \in \Omega$, if $|wt| < |w|$, then set $t_1 = t$ and $w_1 = wt_1$. Otherwise, stop and set $w_{\min} = w$.
- Now, we repeat WLR on w, w_1 and so on, until for some $m+1$ steps, we get $w_{\min} = wt_1t_2\cdots t_m$ with $|w| > |w_1| > \cdots > |w_m|$. Therefore, $t_1\cdots t_m$ is the required automorphism

Remark 7. One uses classical greedy descent method to determine the successful directions t_1 from w, t_2 from w_1 and so on.

Remark 8. Notice that, Whitehead's Minimization theorem (4.2.1) and the finiteness of Ω guarantee that the algorithm will terminate. Also, note that, $m \leq |w|$.

Finite Sequence algorithm

First, we prove a lemma, which gives the necessary condition for existence of an automorphism between two automorphic minimal words.

Lemma 4.2.2. *Let u_{min} and v_{min} be the automorphic minimal words of u and v, respectively. Then there can not exist an automorphism between u_{min} and v_{min} unless $|u_{min}| = |v_{min}|$.*

Proof. Let $u_{\min} = u\alpha$ and $v_{\min} = v\beta$ with $\alpha, \beta \in \mathrm{Aut}(F)$. Suppose, there exists an automorphism γ taking $u_{\min}$ to $v_{\min}$.

Therefore, we have, $u_{\min} = v\beta\gamma^{-1}$ i.e., $u_{\min}$ is in the automorphism orbit of v. So, $|v_{\min}| \leq |u_{\min}|$. Similarly, we also have $|u_{\min}| \leq |v_{\min}|$. Hence, $|u_{\min}| = |v_{\min}|$. ■

Now, we provide an algorithm to decide if there exists a finite sequence of Whitehead automorphisms between two automorphically minimal words of same length such that in each step the length of the intermediate words do not change.

- Let $u_{\min}$ and $v_{\min}$ be cyclic words with $|u_{\min}| = |v_{\min}| = n$. Let $\Omega = \{t_1, \ldots, t_n\}$ be the set of Whitehead automorphisms.

- Consider $\{u_{\min}\}$ as a graph with a single vertex and no edges.

- Now, check the length of $u_{\min} t_i$, for each $t_i \in \Omega$. If $|u_{\min} t_i| = n$ and $u_{\min} t_i \neq u_{\min}$, then we join an edge between $u_{\min}$ and $u_{\min} t_i$. Denote this graph as Γ_1.

- Apply Ω to each vertex of the form $u_{\min} t_i$ in Γ_1, and check if the length of resulting words are n. Now, by discarding the new words, if they belong to the vertex set Γ_1, form a new graph Γ_2 using same procedure as above i.e., adding an edge between $u_{\min} t_i$ and $u_{\min} t_i t_j$.

- Repeat this process until one hits $v_{\min}$. A path between $u_{\min}$ and $v_{\min}$ gives a sequence of Whitehead automorphisms with required properties.

- If no sequence is found which connect $u_{\min}$ to $v_{\min}$, one concludes there is no automorphism. Notice that, the set of words of length n in the free group of finite rank is finite. Also, the set of Whitehead automorphisms Ω is a finite set. Therefore, the process terminates after some finite iteration.

Algorithm 1 Finite sequence algorithm

Let F be the free group of finite rank and $\Omega = \{t_1, \ldots, t_m\}$ be the set of Whitehead automorphisms.
Let u and v be cyclic words such that $|u| = |v| = n$.
Let $V_0 = \{u\}$. Let Γ_0 be the graph of V_0, which is just a vertex. Let $V = V_0$
while $t_i \in \Omega$ **do**
    if $|ut_i| = |u|$ and $ut_i \notin V$ **then**
        create a new list V_1 consisting ut_i's, and a graph Γ_1 with vertices $V_0 \cup V_1$ and edges t_i from u to ut_i, and set $V = \mathrm{Vert}(\Gamma_1)$
    end if
end while
repeat
    the above process for each $ut_i \in V_1$ and so on
until we find a sequence of path that hits v.
if we don't find such a sequence to v **then**
    then we conclude there is no path, hence no automorphisms from u to v.
end if

Whitehead algorithm

Finally, we are in the position to describe the algorithm for the decision problem of the existence of an automorphism between two given words.

Proposition 4.2.3. *(**Decision Problem**) Let u and v be cyclic words in a finitely generated free group F. Then it is decidable whether there is an automorphism, φ, carrying u to v.*

Proof. The algorithm goes as follows: given two words u and v, we find $u_{\min}$ and $v_{\min}$, respectively, using Whitehead's Minimization algorithm. Then, we check the lengths of the minimal words. If $|u_{\min}| \neq |v_{\min}|$, then by Lemma 4.2.2 we conclude that there does not exist an automorphism. If $|u_{\min}| = |v_{\min}|$, we use the finite sequence algorithm to decide the existence of a sequence of Whitehead automorphisms. ■

Whitehead algorithm can be described in a single theorem along with a pictorial description, as follows [Collins and Zieschang, 1984a]:

Theorem 4.2.4. *Let u and v be cyclic words. Let α be an automorphism such that $u\alpha = v$. Then one can write $\alpha = t_1 \cdots t_n$, for $t_1, \ldots, t_n \in \Omega$ such that for some p, q and $1 \leq p \leq q \leq n$,*

(i) $|ut_1 \cdots t_{i-1}| > |ut_1 \cdots t_i|$, *for* $1 \leq i \leq p$, *with* $ut_1 \cdots t_p = u_{min}$,

(ii) $|ut_1 \cdots t_{j-1}| = |ut_1 \cdots t_j|$, *for* $p+1 \leq j \leq q$, *with* $ut_1 \cdots t_q = v_{min}$, *and*

(iii) $|ut_1 \cdots t_{k-1}| < |ut_1 \cdots t_k|$, *for* $q+1 \leq k \leq n$ *with* $ut_1 \cdots t_n = v$.

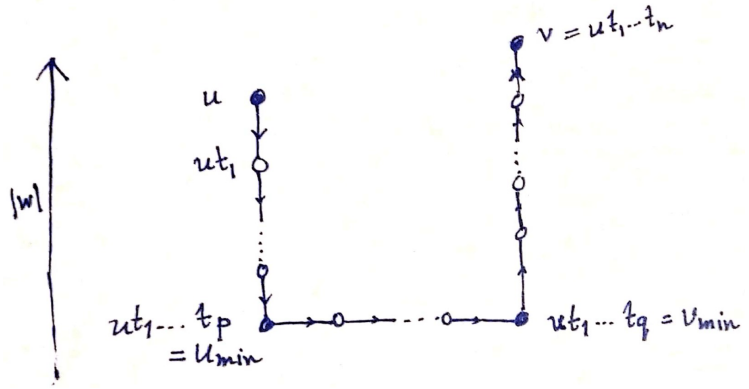


Figure 4.2: The pictorial description of Whitehead algorithm

4.3. Whitehead's theorem for a finite set of cyclic words

In this section, we provide a proof of the peak reduction lemma for a set of cyclic words (analogue of Lemma 4.1.1), and using that we prove the weak version of Whitehead's theorem (analogue of theorem 4.1.6). After establishing these two results, the analogue of section 4.2 follows exactly by replacing each cyclic word with a set of cyclic words. First, we define some basic notions.

Remark 9. Let W be a set of words. The action of an automorphism τ, on the set is defined as: $W\tau = \{w\tau | w \in W\}$.

We define the analogue $D(\tau, W)$, of $D(\tau, w)$ in a similar fashion as follows.

Definition 4.3.1. Let W be a set of words, and $\tau \in \mathrm{Aut}(F_n)$. We define, $D(\tau, W) = |W\tau| - |W|$.

Lemma 4.3.2. $D(\tau, W) = \sum_{w \in W} D(\tau, w)$.

Proof. We have,

$$\begin{aligned} D(\tau, W) &= |W\tau| - |W| \\ &= \sum_{w \in W} (|w\tau| - |w|) \\ &= \sum_{w \in W} D(\tau, w) \end{aligned}$$

■

The analogue of the Proposition 3.4.7 is as follows.

Proposition 4.3.3. *Let W be a set of cyclic words, and $\tau = (A, a)$. Then $D(\tau, W) = (A \cdot A')_{W\tau} - (a \cdot X^{\pm 1})_{W\tau}$.*

Proof. We have,

$$D(\tau, W) = \sum_{w \in W} D(\tau, w) \tag{4.31}$$

$$= \sum_{w \in W} [(A \cdot A')_{w\tau} - (a \cdot X^{\pm 1})_{w\tau}] \tag{4.32}$$

$$= (A \cdot A')_{W\tau} - (a \cdot X^{\pm 1})_{W\tau}. \tag{4.33}$$

This proves the proposition. ■

Now, we prove the peak reduction lemma.

Lemma 4.3.4. *(**Peak Reduction**) Let W be a finite set of cyclic words, and $U = W\sigma$, $V = W\tau$, for $\sigma, \tau \in \Omega$. Assume that $|U| \leq |W|$ and $|V| \leq |W|$ with at least one of the inequality strict. Then $V = U\rho_1 \cdots \rho_n$, $n \geq 0$, where $\rho_1, \ldots, \rho_n \in \Omega$, and for $0 < i < n$, $|U\rho_1 \cdots \rho_i| < |W|$.*

Proof. The proof the lemma follows similar pattern of that of Lemma 4.1.1. We discuss the modifications in each of the cases.

Case 1. (**τ is a permutation**) τ being a permutation, we have $|V| = \sum_{v \in V} |v| = \sum_{w \in W} |w\tau| = \sum_{w \in W} |w| = |W|$. Similarly, $|U\tau| = |U|$. From the case 1 of proof of Lemma 4.1.1, we have $V = U\rho_1\rho_2$ with $\rho_1, \rho_2 \in \Omega$, and $|U\rho_1| = |U\tau| = |U| < |W|$.

Therefore, as in the previous proof, we may assume that σ and τ are type (II) Whitehead automorphisms. Let $\sigma = (A, a)$ and $\tau = (B, b)$.

Case 2. (**$A \cap B = \varnothing$, and $b = a^{-1}$**) Replacing w, u, v with W, U, V respectively, the proof follows exactly that of the case 2 of Lemma 4.1.1.

Case 3. ($A \cap B = \varnothing$ **and** $a^{-1} \in B'$) First we see that, $|U\tau| < |W|$. From the proof of Lemma 4.1.1, we have, $|u\tau| - |u| = |w\tau| - |w|$. So, $|U\tau| - |U| = \sum_{u \in U}(|u\tau| - |u|) = \sum_{w \in W} |w\tau| - |w| = |W\tau| - |W| = |V| - |W|$, since by definition $W\tau = V$. Therefore, $|U\tau| = |U| + |V| - |W| < |W|$, since $|U| + |V| < 2|W|$ (as $|U| < |W|$ or $|V| < |W|$).

Now, taking ρ_1, ρ_2 as in Case 3 of the proof of Lemma 4.1.1 and following the proof, we get $V = U\rho_1\rho_2$, and $|U\rho_1| = |U\tau| < |W|$.

Case 4. ($A \cap B = \varnothing$) As in the case 4 of the proof of Lemma 4.1.1, we assume that $a^{-1} \in B$ and $b^{-1} \in A$. Let $\sigma' = (A, b^{-1})$ and $\tau' = (B, a^{-1})$. It is easy to see that $D(\sigma', W) + D(\tau', W) = D(\sigma, W) + D(\tau, W)$, using Proposition 4.3.3, as follows:

$$\begin{aligned} D(\sigma', W) + D(\tau', W) &= A \cdot A' - b^{-1} \cdot X^{\pm 1} + B \cdot B' - a^{-1} \cdot X^{\pm 1} && (4.34)\\ &= A \cdot A' - b \cdot X^{\pm 1} + B \cdot B' - a \cdot X^{\pm 1} \quad {\scriptstyle (a \cdot X^{\pm 1} = a^{-1} \cdot X^{\pm 1})} && (4.35)\\ &= (A \cdot A' - a \cdot X^{\pm 1}) + (B \cdot B' - b \cdot X^{\pm 1}) && (4.36)\\ &= D(\sigma, W) + D(\tau, W). && (4.37) \end{aligned}$$

Now, we have

$$D(\sigma', W) + D(\tau', W) = D(\sigma, W) + D(\tau, W) = |U| + |V| - 2|W| < 0 \tag{4.38}$$

Assuming $D(\tau', W) < 0$, we get $|W\tau'| < |W|$. Taking ρ_1, ρ_2, ρ_3 as in case 4 of the proof of Lemma 4.1.1 and following the proof, we get $V = U\rho_1\rho_2\rho_3$, and $|U\rho_1\rho_2| = |U\rho_1| = |W\tau'| < |W|$.

Case 5. ($A \cap B \neq \varnothing$) We will use exactly the same notation as that of the proof of the case 5 of Lemma 4.1.1. Similar to that proof, we will show that at least one of the automorphisms $\varphi_x = (P(x), x)$ decreases length of W, for some x, where x stands for one of a, a^{-1}, b, b^{-1}.

Like earlier, we can assume that $x = a$. Then, for each $w \in W$, $|w\varphi_a| < |w|$, using Proposition 4.1.5, where $\varphi_a = (A \cap B', a)$. Therefore, $|W\varphi_a| = \sum_{w \in W} |w\varphi_a| < \sum_{w \in W} |w| = |W|$. Now, from $U = W(A, a) = W(A', a^{-1})$ ((p-viii)), we have, $W = U(A', a^{-1})^{-1} = (A' - a^{-1} + a, a)$. So, $W_1 = W\varphi_a = U(A' - a^{-1} + a, a)(A \cap B', a) = U(A' \cup B' - a^{-1}, a)$.

Now, we have, $W_1 = W(A \cap B', a)$, $V = W(B, b)$, $|W_1| < |W|$ and $(A \cap B') \cap B = \varnothing$. Therefore, applying case 4 from above, we get at most three automorphisms, $\rho_2, \rho_3, \rho_4 \in \Omega$ such that $V = W_1\rho_2\rho_3\rho_4$, with $|W_1\rho_2|, |W_1\rho_2\rho_3|$ strictly lesser than $|W|$. Replacing W_1, with $U(A \cup B' - a^{-1}, a)$, we have, $V = U\rho_1\rho_2\rho_3\rho_4$ with $|U\rho_1|, |U\rho_1\rho_2|, |U\rho_1\rho_2\rho_3| < |W|$, where $\rho_1 = (A \cup B' - a^{-1}, a)$.

Hence, the lemma is proved. ■

Now, we state the restricted version of the theorem (analogue of Theorem 4.1.6) for a set of cyclic words.

Theorem 4.3.5. *Let $W = \{w_1, \cdots, w_r\}$ and $\bar{W} = \{\bar{w}_1, \cdots, \bar{w}_r\}$ be two finite sets of cyclic words. Let $\bar{W} = W\alpha$, for some $\alpha \in Aut(F)$, and suppose that $|\bar{W}| \leq |W|$ (i.e., $\bar{W}$ is automorphic minimal). Then there exist $\tau_1, \cdots, \tau_n \in \Omega$ $(n \geq 0)$, such that, writing $W_i = W\tau_1 \cdots \tau_i$, for $0 \leq i \leq n$, one has $W_n = \bar{W}$, and $|W_i| \leq |W|$, for $1 \leq i \leq n$, with strict inequality unless $|W| = |\bar{W}|$.*

Proof. The proof will exactly be same as that of the Theorem 4.1.6. We briefly discuss it here.

For $\alpha \in \mathrm{Aut}(F)$, we get $\alpha = \tau_1 \cdots \tau_n$, for some $\tau_1, \cdots, \tau_n \in \Omega$ (since Nielsen transformations generate the automorphism group, and are subset of Whitehead automorphisms).

Let $m = \max\{|W_i| : 0 < i < n\}$. If α does not satisfy the conclusion, then $n \geq 2$ and $m \geq |W| > |\bar{W}|$ or $m > |W| = |\bar{W}|$. Choosing i maximal for $|W_i| = m$, we get $|W_{i-1}| \leq |W|$ and $|W_{i+1}| < |W|$. Now, applying Lemma 4.3.4 to $W_{i-1} = W_i\tau_i^{-1}$ and $W_{i+1} = W_i\tau_i$, we get a new path $\rho_1 \cdots \rho_k$ from W_{i-1} to W_{i+1}, such that,

$$W_{i+1} = W_{i-1}\rho_1 \cdots \rho_k, \;\; k > 0, \rho_j \in \Omega \text{ for all } 1 \leq j \leq k, \tag{4.39}$$

with

$$|W_{i-1}\rho_1 \cdots \rho_j| < |W_i| = m, \;\; \text{for } 0 < j < k. \tag{4.40}$$

Now, we did in the proof of theorem 4.1.6, we apply induction first on number of $|W_i|$ of value m, and then on m, until we reach $|W| \leq m$. This proves the theorem. ■

This gives the corollaries analogous to Corollary 4.1.7 and 4.1.8. We state the following corollary which is analogous to Corollary 4.1.8.

Corollary 4.3.6. *Let $U = \{u_1, \ldots, u_r\}$ and $V = \{v_1, \ldots, v_r\}$ be two finite sets of cyclic words. Suppose, U_{min} and V_{min} be automorphic minimal sets of U and V, respectively. Suppose there exists $\alpha \in Aut(F)$, such that $U_{min}\alpha = V_{min}$, then, α can be written as a product of finitely many Whitehead automorphisms $t_1, \ldots, t_n$ such that $|U_{min}| = |U_{min}t_1| = \cdots = |U_{min}t_1 \cdots t_n|$, with $U_{min}t_1 \cdots t_n = V_{min}$.*

Now, we state Whitehead's minimization theorem for the finite set of cyclic words.

Theorem 4.3.7. *(**Whitehead's theorem for finite sets of cyclic words**) Let W be a finite set of cyclic words in F. Suppose that $\bar{W}$ is an automorphic minimal set i.e., length of $\bar{W}$ is minimum among the orbit of w. Then, there exist finitely many Whitehead automorphisms $\tau_0, \tau_1, \ldots, \tau_n$,, for some integer n, such that $\bar{W} = W\tau_0 \cdots \tau_n$ and $|W\tau_0 \cdots \tau_n| \leq |W\tau_0 \cdots \tau_{n-1}| \leq \cdots \leq |W\tau_0| \leq |W|$.*

As mentioned earlier, by replacing cyclic words with the set of cyclic words, in the proof Theorem 4.2.1, we get the theorem above.

Now, following similar procedure as section 4.2.1, we get the decision algorithm for Whitehead's problem.

Proposition 4.3.8. *(**Decision problem**) Let $U = \{u_1, \ldots, u_r\}$ and $V = \{v_1, \ldots, v_r\}$ be finite sets of cyclic words in a finitely generated free group F. Then it is decidable whether there is an automorphism, φ, carrying U to V i.e., $u_i\varphi = v_i$, for $1 \leq i \leq r$.*

CHAPTER 5

WHITEHEAD'S THEOREM FOR ORDINARY WORDS

We define ordinary words or true words (in terms of Whitehead), as follows.

Definition 5.1. (**Ordinary Words**) Let F_n be a free group of rank n with basis $X^{\pm 1} = \{x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}\}$. An *ordinary word, w* is defined to be a sequence of letters $xyz\ldots$, for $x, y, z \in X^{\pm 1}$ such that no consecutive pair of letters are inverses of each other. For example, $x_1 x_5 x_1^{-1}$, $x_4 x_2^{-1} x_4$ are ordinary words.

Any ordinary word is thought to be reduced unless mentioned.. Length of an ordinary word w, denoted by $|w|$, is the number of letters in the word.

Remark 10. Notice that, an ordinary word is quiet different than a cyclic word. For example, ab and ba are both same as cyclic word, whereas they are not as ordinary word. Another example, $cabc^{-1}$ and ab are different ordinary words, whereas they are same cyclic word.

Note. It only suffices to prove the peak reduction lemma (analogue to Lemma 4.1.1), since the restricted form of Whitehead's theorem follows from the peak reduction lemma exactly same way as before. Also, it is clear that the proof of Theorem 4.1.6 does not depend on the cyclic nature of words. Therefore, Corollaries 4.1.7, 4.1.8, Whitehead minimization theorem and Whitehead algorithm do not depend on the nature of words.

Remark 11. One can not prove the peak reduction lemma for ordinary words in the same way as cyclic words, because of the following reason:

Ordinary words are not conjugation invariant unlike cyclic words (see the above remark).

This means, ordinary words do not satisfy the conjugation relation in (p-viii). But this is crucial for proving the peak reduction lemma.

We introduce the following trick to solve this issue. Basically, for an ordinary word w in F_n, we define a corresponding cyclic word in F_{n+1}. Then, using those cyclic words we prove the lemma. Note that, McCool also uses a similar trick in [McCool, 1974].

Trick:

We represent an ordinary word w of F_n as a cyclic word in F_{n+1}, where F_{n+1} is generated by $X_{n+1} = X^{\pm 1} \cup \{x_{n+1}, x_{n+1}^{-1}\}$, as follows: define $w_1 = wx_{n+1}$. We see

that w_1 can be thought of as a cyclic word in F_{n+1}, because the end letters are not inverses of each other.

As for the automorphisms, we embed $\mathrm{Aut}(F_n) \hookrightarrow \mathrm{Aut}(F_{n+1})$, and for any $\psi \in \mathrm{Aut}(F_n)$, extend ψ on F_{n+1} by defining $x_{n+1}\psi = x_{n+1}$. We denote Ω_{n+1} as the set of Whitehead automorphisms in F_{n+1}.

Lemma 5.2. *(**Peak Reduction**) Let w be an ordinary word. Let $\sigma, \tau \in \Omega$. Suppose, $u = w\sigma$ and $v = w\tau$ with $|u| \leq |w|$ and $|v| \leq |w|$ with at least one of the inequalities strict. Then there exist $\rho_1, \ldots, \rho_n \in \Omega$ such that $v = u\rho_1 \cdots \rho_n$, and $|u\rho_1 \cdots \rho_i| < |w|$.*

Proof. Let F_{n+1} be the free group generated by $X_{n+1} = X^{\pm 1} \cup \{x_{n+1}, x_{n+1}^{-1}\}$. We embed $\mathrm{Aut}(F_n) \hookrightarrow \mathrm{Aut}(F_{n+1})$, and for any $\psi \in \mathrm{Aut}(F_n)$, extend ψ on F_{n+1} by defining $x_{n+1}\psi = x_{n+1}$, as mentioned above.

Let $w_1 = wx_{n+1}, u_1 = ux_{n+1}$ and $v_1 = vx_{n+1}$ be cyclic words in F_{n+1} corresponding to w, u and v, respectively. Since $\sigma, \tau \in \Omega$ fixes x_{n+1}, we get

$$w_1\sigma = (wx_{n+1})\sigma = w\sigma x_{n+1} = ux_{n+1} = u_1, \tag{5.1}$$

and similarly $w_1\tau = v_1$.

Notice that, $|w_1| = |w| + 1$, $|u_1| = |u| + 1$ and $|v_1| = |v| + 1$. Therefore, from $|u| \leq |w|$ and $|v| \leq |w|$, we get $|u_1| \leq |w_1|$ and $|v_1| \leq |w_1|$, respectively. So, from the hypothesis of the lemma, we have at least one of the inequalities is strict. Therefore, we get,

$$|u_1| + |v_1| < 2|w_1| \tag{5.2}$$

We will go through several cases analogous to the proof of Lemma 4.1.1 to prove this lemma. At each step we will verify that the necessary automorphisms fix x_{n+1} and therefore lie in Ω.

Case 1 (τ is a permutation). For τ a permutation, we get $|v| = |w\tau| = |w|$. Therefore, $|v_1| = |v| + 1 = |w| + 1 = |w_1|$. Now,

$$v_1 = w_1\tau = u_1\sigma^{-1}\tau = u_1\tau\tau^{-1}\sigma^{-1}\tau = (ux_{n+1})\tau\tau^{-1}\sigma^{-1}\tau \tag{5.3}$$

$$\implies vx_{n+1} = u\tau\tau^{-1}\sigma^{-1}\tau x_{n+1}, \text{ (since } \sigma,\tau \text{ fix } x_{n+1}) \tag{5.4}$$

$$\implies v = u\tau\tau^{-1}\sigma^{-1}\tau \text{ (multiplying } x_{n+1}^{-1}). \tag{5.5}$$

Taking $\rho_1 = \tau$ and $\rho_2 = \tau^{-1}\sigma^{-1}\tau$, we get $v = u\rho_1\rho_2$. We have seen in Lemma 4.1.1 that for this ρ_1 and ρ_2 we get $\rho_1, \rho_2 \in \Omega$, and $|u\rho_1| = |u| < |w|$.

So, we assume that none of σ and τ are permutations. Let $\sigma = (A, a)$ and $\tau = (B, b)$.

Case 2 ($A \cap B = \varnothing, b = a^{-1}$)**.** We have $v_1 = w_1\tau = u_1\sigma^{-1}\tau$. It follows that $v = u\sigma^{-1}\tau$. Taking $\rho_1 = \sigma^{-1}\tau$, the conclusion is vacuously true, as seen earlier in Lemma 4.1.1.

Case 3 ($A \cap B = \varnothing, a^{-1} \in B'$)**.** We have $w_1, u_1 = w_1\sigma$ and $v_1 = w_1\tau$ as cyclic words and the inequality $|u_1| + |v_1| < 2|w_1|$. So, from Claim 4.1.2, we get $|u_1\tau| < |w_1|$. Hence, $|u\tau| < |w|$.

Now, we have, $v_1 = w_1\tau = u_1\tau\tau^{-1}\sigma^{-1}\tau$. Letting $\rho_1 = \tau$ and $\rho_2 = \tau^{-1}\sigma^{-1}\tau$, we have $v_1 = u_1\rho_1\rho_2$ with $\rho_1, \rho_2 \in \Omega$. Since ρ_1, ρ_2 fix x_{n+1}, we get $v = u\rho_1\rho_2$ with $|u\rho_1| = |u\tau| < |w|$.

For the cyclic words w_1, u_1 and v_1, the proof of the following two cases are similar to that of Lemma 4.1.1. We briefly discuss the proofs here.

Case 4 ($A \cap B = \varnothing$)**.** As before, we assume that $a^{-1} \in B$ and $b^{-1} \in A$. Let $\sigma' = (A, b^{-1})$ and $\tau' = (B, a^{-1})$. Now, for the cyclic word w_1, we have, $D(\sigma', w_1) = (A \cdot A')_{w_1} - (b^{-1} \cdot X_{n+1})_{w_1}$. Using $a \cdot X_{n+1} = a^{-1} \cdot X_{n+1}$ and $b \cdot X_{n+1} = b^{-1} \cdot X_{n+1}$, we get, $D(\sigma', w_1) + D(\tau', w_1) = D(\sigma, w_1) + D(\tau, w_1) < 0$. So, at least one of $D(\sigma', w_1)$ or $D(\tau', w_1)$ is negative. As before, let's assume $D(\tau', w_1) < 0$. So, we get, $|w_1\tau'| < |w_1|$. Since $\tau' \in \Omega \subset \mathrm{Aut}(F_n)$, we have $x_{n+1}\tau' = x_{n+1}$. Therefore, from $|w_1\tau'| < |w_1|$, we get $|w\tau'| < |w|$. We follow exactly the same procedure as of Lemma 4.1.1 for the cyclic words w_1, u_1 and v_1 to get $v_1 = u_1\rho_1\rho_2\rho_3$ with $\rho_1 = \sigma^{-1}\tau', \rho_2 = \pi, \rho_3 = (A - b + b^{-1}, a) \in \Omega$. Therefore, we get $v = u\rho_1\rho_2\rho_3$. Now, $|u\rho_1\rho_2| = |u\rho_1|$, as ρ_2 is a permutation, and $|u\rho_1| = |w\tau| < |w|$.

Case 5 ($A \cap B \neq \varnothing$)**.** We have, $D(\sigma, w_1) = (A \cdot A')_{w_1} - (a \cdot X_{n+1})_{w_1}$. So, by replacing $X^{\pm 1}$ by X_{n+1} in the case 5 of the proof of Lemma 4.1.1 and proceeding exactly the same way, we get the analogues of 4.14 and 4.15. Now, taking x as one of a, a^{-1}, b, b^{-1}, we get $\varphi_x = (P(x), x)$ as a Whitehead automorphism. Therefore, for the cyclic word w_1, we get the analogue of Claim 4.1.4 i.e., $D(\varphi_x, w_1) < 0$, for some x. Now, proceeding exactly as that of the proof of Lemma 4.1.1, we get $D(\varphi_a, w_1) = D((A \cap B', a), w_1) < 0$. This implies, $|w_1(A \cap B', a)| < |w_1|$, which is the analogue of Proposition 4.1.5.

Since w_1 is a cyclic word and a conjugation does not change cyclic words, we have $w_1(A, a) = w_1(A', a^{-1})$. Therefore, $u_1 = w_1(A', a^{-1})$, hence, $w_1 = u_1(A', a^{-1})^{-1}$. Now, $w_1' = w_1(A \cap B', a) = u_1(A', a^{-1})(A \cap B, a) = u_1(A' \cup B' - a^{-1}, a)$, as seen in the proof of Lemma 4.1.1. So, we have, $w_1' = w_1(A \cap B', a), v_1 = w_1\tau, |w_1(A \cap B', a)| < |w_1|$ and $(A \cap B') \cap B = \varnothing$. Since $(A \cap B', a), \tau \in \Omega$, they fix x_{n+1}. So, $w_1(A \cap B', a) = w(A \cap B', a)x_{n+1}$.

Let $w' = w(A \cap B', a)$. From $|w(A \cap B', a^{-1})x_{n+1}| < |wx_{n+1}|$, we get $|w(A \cap B', a)| < |w|$. Also, from $v_1 = w_1\tau$, we get $v = w\tau$. Therefore, we have, $w' = w(A \cap B', a), v = w(B, b), |w'| < |w|$ and $(A \cap B') \cap B = \varnothing$. Hence, it is reduced to

case 4 above. So, we get at most three automorphisms such that $v = w'\rho_2\rho_3\rho_4 = u\rho_1\rho_2\rho_3\rho_4$, with all the intermediate words having length less than $|w|$, where $\rho_1 = (A' \cup B' - a^{-1}, a)$.

Hence, we have proved the lemma. ■

Now, following a similar procedure to the proof of Theorem 4.1.6, we can prove the restricted version of Whitehead's theorem.

Theorem 5.3. *Let w be an ordinary word. Suppose that w' is an automorphic minimal word in the orbit of w. Let $w' = w\alpha$, for some $\alpha \in Aut(F_n)$. Then there exist $\tau_1, \ldots, \tau_n \in \Omega$ such that $w' = w\tau_1 \cdots \tau_n$, and writing $w_i = w\tau_1 \cdots \tau_i$, we get, $|w_i| \leq |w|$, $0 < i < n$ with strict inequality unless w is also minimal.*

5.1. Whitehead's theorem for a finite set of ordinary words

In the following section, we prove the theorem for a finite set of ordinary words. First, we prove the lemma analogue to 5.2. Then using this, we prove the theorem.

Lemma 5.1.1. *Let W be a finite set of ordinary words, and $U = W\sigma$, $V = W\tau$, for $\sigma, \tau \in \Omega$. Suppose that, $|U| \leq |W|$ and $|V| \leq |W|$, with at least one of the inequality strict. Then $V = U\rho_1 \cdots \rho_n$. $n \geq 0$, where $\rho_1, \ldots, \rho_n \in \Omega$, and for $0 < i < n$, $|U\rho_1 \cdots \rho_n| < |W|$.*

Proof. We start with defining set of cyclic words corresponding to the set of ordinary words as follows,

$$W' = \{w_1 x_{n+1}, \ldots, w_k x_{n+1}\}, \tag{5.6}$$
$$U' = \{u_1 x_{n+1}, \ldots, u_k x_{n+1}\}, \tag{5.7}$$
$$V' = \{v_1 x_{n+1}, \ldots, v_k x_{n+1}\}. \tag{5.8}$$

Since σ and τ fix x_{n+1}, we see that $U' = W'\sigma$ and $V' = W'\tau$, with $|U'| \leq |W'|$ and $|V'| \leq |W'|$.

Proofs of the first three cases are exactly same as that of the proof of Lemma 4.3.4. We only write case 4 and case 5.

Case 4. ($\boldsymbol{A \cap B = \varnothing}$) Like before, we assume that $a^{-1} \in B$ and $b^{-1} \in A$. Let $\sigma' = (A, b^{-1})$ and $\tau' = (B, a^{-1})$. Now,

$$D(\sigma', W') + D(\tau', W') = \sum_{w' \in W'} (D(\sigma', w') + D(\tau', w') \tag{5.9}$$

$$= \sum_{w' \in W'} (D(\sigma, w') + D(\tau, w')) \text{ (using (4.7))} \tag{5.10}$$

$$= D(\sigma, W') + D(\tau, W') = |W'\sigma| - |W'| + |W'\tau| - |W'| \tag{5.11}$$

$$= |U'| + |V'| - 2|W'| < 0. \tag{5.12}$$

Therefore, at least one of $D(\sigma', W')$ or $D(\tau', W')$ is less than zero. Without loss of generality, let's assume $D(\tau', W') < 0$. This implies, $|W'\tau'| < |W'|$. Since $\tau' \in \Omega$ fixes x_{n+1}, we have $|W\tau'| < |W|$. Now, as previously, with $\rho_1 = \sigma^{-1}\tau'$, $\rho_2 = \pi$ and $\rho_3 = (A - b^{-1} + b, a)$, we see that $V = U\rho_1\rho_2\rho_3$, where $|U\rho_1\rho_2| = |U\rho_1| = |W\sigma\sigma^{-1}\tau| = |W\tau| < |W|$.

Case 5. ($\boldsymbol{A \cap B \neq \varnothing}$) Similar to the case 4 above, we consider the sets of cyclic words W', U' and V' corresponding to the sets of ordinary words W, U and V, respectively. We also have $U' = W'\sigma$, $V' = W'\tau$, $|U'| \leq |W'|$ and $|V'| \leq |W'|$.

Now, following exactly same as that of the proof of the case 5 of the Lemma 4.3.4, we get $|W'(A \cap B', a)| < |W'|$, $W' = U'(A' - a^{-1} + a, a)$ and $\widetilde{W} = W'(A \cap B', a) = U'(A \cup B' - a^{-1}, a)$. Now, $W'(A \cap B', a) = W(A \cap B', a)x_{n+1}$. Let $W_1 = W(A \cap B', a)$. So, from, $|\widetilde{W} = W'(A \cap B', a)| < |W'|$, we get $|W_1| < |W|$, and from $V' = W'(B, b)$, we get $V = W(B, b)$.

Therefore, we have, $W_1 = W(A \cap B', a)$, $V = W(B, b)$, $|W_1| < |W|$ and $(A \cup B') \cap B = \varnothing$. Hence, we are reduced to the case 4 above. So, there exist at most three automorphisms that connect V to W_1, with all the intermediate words having length less than $|W|$. Replacing W_1, with $U(A \cup B' - a^{-1}, a)$, we get a path from V to U with at most four steps, where all the intermediate words have length less than the length of W. Hence, the lemma is proved. ■

We write a detailed proof of the restricted form of Whitehead's theorem, which will be similar to the previous proofs.

Theorem 5.1.2. *Let $W = \{w_1, \cdots, w_r\}$ and $\bar{W} = \{\bar{w}_1, \cdots, \bar{w}_r\}$ be two finite sets of ordinary words. Let $\bar{W} = W\alpha$, for some $\alpha \in Aut(F_n)$, and suppose that $|\bar{W}| \leq |W|$. Then there exist $\tau_1, \ldots, \tau_n \in \Omega$ $(n \geq 0)$, such that, writing $W_i = W\tau_1 \cdots \tau_i \equiv \{w_1\tau_1 \cdots \tau_i, \cdots, w_r\tau_1 \cdots \tau_i\}$, for $0 \leq i \leq n$, one has $W_n = \bar{W}$, and $|W_i| \leq |W|$, for $1 \leq i \leq n$, with strict inequality unless $|W| = |\bar{W}|$.*

Proof. Since Nielsen transformations generate the automorphism group, and are contained in the set of Whitehead automorphisms, we see that for any $\alpha \in$

$\mathrm{Aut}(F_n)$, there exist $\tau_1, \ldots, \tau_n \in \Omega$ such that $\alpha = \tau_1 \cdots \tau_n$, for $n \geq 0$. Now, if $\tau_1, \ldots, \tau_n$ satisfy $|W_i| \leq |W|$, for $1 \leq i \leq n$, then we are done.

Let $m = \max\{|W_i| : 0 < i < n\}$, where $W_i = W\tau_1 \cdots \tau_i$. Since α does not satisfy the conclusion, we must have $n \geq 2$ and either $m > |W| = |W'|$ or $m \geq |W| > |W'|$. Let i be the maximal integer such that $|W_i| = m$. Therefore,

$$|W_{i-1}| \leq |W_i| \text{ and } |W_{i+1}| < |W_i|. \tag{5.13}$$

We also have

$$W_{i-1} = W_i\tau_i^{-1} \text{ and } W_{i+1} = W_i\tau_{i+1}. \tag{5.14}$$

From the justification in Theorem 5.3, we see that, given W a set of ordinary words, W_i is a set of ordinary words, for all i. So, from (5.13) and (5.14), we see that, they satisfy Lemma 5.1.1. Therefore, there exist $\rho_1, \ldots, \rho_k \in \Omega$, for some $k \geq 0$, such that

$$W_{i+1} = W_{i-1}\rho_1 \cdots \rho_k, \tag{5.15}$$

and for $1 \leq j < k$,

$$|W_{i-1}\rho_1 \cdots \rho_j| < |W_i| = m. \tag{5.16}$$

We know that,

$$\begin{aligned} W' &= W\tau_1 \cdots \tau_n && (5.17)\\ &= W_{i+1}\tau_{i+2} \cdots \tau_n && (5.18)\\ &= W_{i-1}\rho_1 \cdots \rho_k\tau_{i+1} \cdots \tau_n \text{ (using (5.16))} && (5.19)\\ &= W\tau_1 \cdots \tau_{i-1}\rho_1 \cdots \rho_k\tau_{i+1} \cdots \tau_n. && (5.20) \end{aligned}$$

So, from (5.20), we see that $\tau_1 \cdots \tau_{i-1}\rho_1 \cdots \rho_k\tau_{i+1} \cdots \tau_n$ is the new path that connects W to W', and also notice that, by doing so, we have removed W_i. Therefore, we conclude that by introducing the new path, the number of words of length m go down exactly by one.

Now, suppose that, there exists $l < i$, maximal, such that, $|W_l| = m$. Then we repeat the same process to get a new path where we don't have the word W_l. So, by repeating this process, we eventually eliminate all the words of length m and get a new path from W' to W corresponding to $m' \leq m$.

We keep repeating this process until we reach $\widetilde{m} \leq |W|$. Therefore, we get a path from W' to W with all the intermediate words having length less than $|W|$, proving the theorem. ■

Therefore, we get the corollaries analogous to 4.1.7 and 4.1.8.

Corollary 5.1.3. *Let $U = \{u_1, \ldots, u_r\}$ and $V = \{v_1, \ldots, v_r\}$ be two finite sets of ordinary words. Suppose, U_{min} and V_{min} be automorphic minimal sets of U and V, respectively. Suppose there exists $\alpha \in Aut(F)$, such that $U_{min}\alpha = V_{min}$, then, α can be written as a product of finitely many Whitehead automorphisms $t_1, \ldots, t_n$ such that $|U_{min}| = |U_{min}t_1| = \cdots = |U_{min}t_1 \cdots t_n|$, with $U_{min}t_1 \cdots t_n = V_{min}$.*

The proof of Whitehead's minimization theorem follows using the same procedure as that of Theorem 4.2.1.

Theorem 5.1.4. *(**Whitehead's theorem for the finite sets of ordinary words**) Let W be a finite set of ordinary words in F. Suppose that $\bar{W}$ is an automorphic minimal set i.e., length of $\bar{W}$ is minimum among the orbit of w. Then, there exist finitely many Whitehead automorphisms $\tau_0, \tau_1, \ldots, \tau_n$,, for some integer n, such that $\bar{W} = W\tau_0 \cdots \tau_n$ and $|W\tau_0 \cdots \tau_n| \leq |W\tau_0 \cdots \tau_{n-1}| \leq \cdots \leq |W\tau_0| \leq |W|$.*

Corollary 5.1.3 and Theorem 5.1.4 allow us to produce an algorithm for the decision problem in a similar fashion. Hence, we have the following solution to the decision problem for finite sets of ordinary words.

Proposition 5.1.5. *(**Decision problem**) Let U, V be the finite sets of ordinary words. Then it is decidable if there exists an automorphism carrying U to V.*

CHAPTER 6

WHITEHEAD'S SECOND PROBLEM

Whitehead [Whitehead, 1936b, p. 800] stated the extension of decision algorithm to the finitely generated free groups as an open problem. Explicitly, the problem is to decide whether there exists an automorphism between two finitely generated subgroups of free groups. Gersten [Gersten, 1984b] solved this problem using a different kind of complexity other than the length of the words.

In this chapter, we discuss Whitehead's counter example, and comment on Gersten's correction.

Take $F(a,b)$, the free group with two generators. Let G be a subgroup generated by

$$p = (ab^{-1})^2 b^{-2} (ab^{-1})^2 a^3, \quad q = a^{-3}b^{-5}$$

and H be a subgroup generated by

$$r = a^2 b^{-2} a^2 b^{-5}, \quad s = (ab)^{-3} b^{-5}.$$

We will see that these two subgroups are equivalent by Whitehead automorphism $t = (\{a,b\}, b)$. Notice that, under t, $a \mapsto ab$ and $b \mapsto b$. So,

$$\begin{aligned} pt &= a\underbrace{bb^{-1}}a\underbrace{bb^{-1}}b^{-1}b^{-1}a\underbrace{bb^{-1}}a\underbrace{bb^{-1}}ababab && (6.1)\\ &= a^2b^{-2}a^2(ab)^3 \equiv \alpha && (6.2)\end{aligned}$$

and

$$qt = (ab)^{-3}b^{-5} \equiv \beta. \tag{6.3}$$

Therefore, $\langle p,q\rangle t = \langle \alpha, \beta\rangle$. Now, we see that, $r = \alpha\beta$. So, $\langle r,s\rangle = \langle \alpha\beta, \beta\rangle$. But the group generated by $\alpha\beta$ and β is same as the group generated by α and β. Hence, we see that $\langle p,q\rangle$ and $\langle r,s\rangle$ are equivalent under the automorphism $t = (\{a,b\}, b)$.

Now, there are no possible reductions of these two sets of words $\{p,q\}$ and $\{r,s\}$, by means of Whitehead. Define the length of a subgroup to be the sum of the length of generators. So, we get that $|G| = 21$ and $|H| = 22$. Therefore, there does not exist any Whitehead automorphism which fix length in each intermediate steps (in Whitehead's terminology these are called *level transformations*).

So, with this example, we see that, even though two subgroups are equivalent by an automorphism, it is not always possible to use Whitehead's minimizing algorithm and the finite sequence algorithm, contrary to Whitehead's first decision problem.

Gersten [Gersten, 1984b] came up with a new notion length, called *complexity*, of subgroups. We briefly discuss Gersten's notion of complexity.

- Realize a free group of finite rank, F, as the fundamental group of wedge of circles, which can be thought of as a one vertex graph. Denote this graph as Y.

- Let S be a conjugacy class of finitely generated subgroups of $F \simeq \pi_1(Y)$. Corresponding to S, find a covering space $X_1 \xrightarrow{p_1} Y$ such that $p_{1*}(\pi_1(X_1, x))$ is in S. This is possible because of the existence theorem of covering spaces [Massey, 1977, Theorem 10.2, p. 175]. Since covering space of a graph is a graph, X_1 is a graph [Massey, 1977, Thereom 7.1, p.201].

- Take the *core graph*, X of X_1. A core graph can be thought of a graph where the fundamental group is concentrated. The core graph, X, can be found, using the generators of the fundamental groups of X_1 [Massey, 1977, Theorem 7.2, pp. 197-198]. Restriction of p_1 to X defines an *immersion* $X \xrightarrow{j} Y$ such that $j_*(\pi_1(X, x))$ belongs to S.

- Define the complexity of S, denoted by $c(S)$ to be the number of vertices of the core graph i.e., $c(S) = \#V(X)$. Note that $c(S)$ is well-defined due to the following reason. Let $X_2 \xrightarrow{p_1} Y$ be another covering space such that $p_{2*}(\pi_1(X_2, x_2))$ belongs to S. Therefore, both the covering spaces are isomorphic [Massey, 1977, Theorem 6.6, p. 159]. Hence, the core graph X is unique up to isomorphism.

Using this notion of the complexity, Gersten [Gersten, 1984b, p. 284] announced the solution of Whitehead's second decision problem one solves the problem [Gersten, 1984b, p. 284]. However, complete details of this approach do not seem to be in the literature (see [Kalajdžievski, 1992, section 10] and [Balle Pigem, 2009, Chapter 3] for alternative arguments).

BIBLIOGRAPHY

[Balle Pigem, 2009] Balle Pigem, B. D. (2009). Extensions de l'algorisme clàssic de Whitehead (*Master's Thesis*). Universitat Politècnica de Catalunya.

[Bassino et al., 2016] Bassino, F., Nicaud, C., and Weil, P. (2016). On the genericity of Whitehead minimality. *J. Group Theory*, 19(1):137–159.

[Bogopolski and Ventura, 2011] Bogopolski, O. and Ventura, E. (2011). On endomorphisms of torsion-free hyperbolic groups. *Internat. J. Algebra Comput.*, 21(8):1415–1446.

[Bogopolski, 2001] Bogopolski, O. V. (2001). The automorphic conjugacy problem for subgroups of fundamental groups of compact surfaces. *Algebra Logika*, 40(1):30–59, 120–121.

[Chorna et al., 2017] Chorna, A., Geller, K., and Shpilrain, V. (2017). On two-generator subgroups in $SL_2(\mathbb{Z})$, $SL_2(\mathbb{Q})$, and $SL_2(\mathbb{R})$. *J. Algebra*, 478:367–381.

[Clark and Goldstein, 2005] Clark, A. and Goldstein, R. (2005). Stability of numerical invariants in free groups. *Comm. Algebra*, 33(11):4097–4104.

[Clay et al., 2014] Clay, M., Conant, J., and Ramasubramanian, N. (2014). Whitehead graphs and separability in rank two. *Involve*, 7(4):431–452.

[Clay and Forester, 2009] Clay, M. and Forester, M. (2009). Whitehead moves for G-trees. *Bull. Lond. Math. Soc.*, 41(2):205–212.

[Clifford and Goldstein, 2010] Clifford, A. and Goldstein, R. Z. (2010). Subgroups of free groups and primitive elements. *J. Group Theory*, 13(4):601–611.

[Collins and Zieschang, 1984a] Collins, D. J. and Zieschang, H. (1984a). On the Whitehead method in free products. In *Contributions to group theory*, volume 33 of *Contemp. Math.*, pages 141–158. Amer. Math. Soc., Providence, RI.

[Collins and Zieschang, 1984b] Collins, D. J. and Zieschang, H. (1984b). Rescuing the Whitehead method for free products. I. Peak reduction. *Math. Z.*, 185(4):487–504.

[Collins and Zieschang, 1984c] Collins, D. J. and Zieschang, H. (1984c). Rescuing the Whitehead method for free products. II. The algorithm. *Math. Z.*, 186(3):335–361.

[Culler and Vogtmann, 1986] Culler, M. and Vogtmann, K. (1986). Moduli of graphs and automorphisms of free groups. *Invent. Math.*, 84(1):91–119.

[Dahmani and Guirardel, 2011] Dahmani, F. and Guirardel, V. (2011). The isomorphism problem for all hyperbolic groups. *Geom. Funct. Anal.*, 21(2):223–300.

[Day, 2009] Day, M. B. (2009). Peak reduction and finite presentations for automorphism groups of right-angled Artin groups. *Geom. Topol.*, 13(2):817–855.

[Day, 2014] Day, M. B. (2014). Full-featured peak reduction in right-angled Artin groups. *Algebr. Geom. Topol.*, 14(3):1677–1743.

[Diao and Feighn, 2005] Diao, G.-A. and Feighn, M. (2005). The Grushko decomposition of a finite graph of finite rank free groups: an algorithm. *Geom. Topol.*, 9:1835–1880.

[Dicks, 2014] Dicks, W. (2014). On free-group algorithms that sandwich a subgroup between free-product factors. *J. Group Theory*, 17(1):13–28.

[Dicks, 2017a] Dicks, W. (2017a). A graph-theoretic proof for Whitehead's second free-group algorithm. *arXiv preprint arXiv:1706.09679*.

[Dicks, 2017b] Dicks, W. (2017b). On Whitehead's first free-group algorithm, cutvertices, and free-product factorizations. *arXiv preprint arXiv:1704.05338*.

[Gersten, 1983] Gersten, S. M. (1983). On fixed points of automorphisms of finitely generated free groups. *Bull. Amer. Math. Soc. (N.S.)*, 8(3):451–454.

[Gersten, 1984a] Gersten, S. M. (1984a). Addendum: "On fixed points of certain automorphisms of free groups". *Proc. London Math. Soc. (3)*, 49(2):340–342.

[Gersten, 1984b] Gersten, S. M. (1984b). On Whitehead's algorithm. *Bull. Amer. Math. Soc. (N.S.)*, 10(2):281–284.

[Gersten, 1987] Gersten, S. M. (1987). Fixed points of automorphisms of free groups. *Adv. in Math.*, 64(1):51–85.

[Goldstein, 1999] Goldstein, R. Z. (1999). The length and thickness of words in a free group. *Proc. Amer. Math. Soc.*, 127(10):2857–2863.

[Goldstein and Turner, 1984] Goldstein, R. Z. and Turner, E. C. (1984). Automorphisms of free groups and their fixed points. *Invent. Math.*, 78(1):1–12.

[Haralick et al., 2005] Haralick, R. M., Miasnikov, A. D., and Myasnikov, A. G. (2005). Heuristics for the Whitehead minimization problem. *Experiment. Math.*, 14(1):7–14.

[Heusener and Weidmann, 2019] Heusener, M. and Weidmann, R. (2019). A remark on Whitehead's cut-vertex lemma. *J. Group Theory*, 22(1):15–21.

[Higgins and Lyndon, 1974] Higgins, P. J. and Lyndon, R. C. (1974). Equivalence of elements under automorphisms of a free group. *J. London Math. Soc. (2)*, 8:254–258.

[Hoare, 1979] Hoare, A. H. M. (1979). Coinitial graphs and Whitehead automorphisms. *Canadian J. Math.*, 31(1):112–123.

[Hoare, 1988] Hoare, A. H. M. (1988). On automorphisms of free groups. I. *J. London Math. Soc. (2)*, 38(2):277–285.

[Kalajdžievski, 1992] Kalajdžievski, S. (1992). Automorphism group of a free group: centralizers and stabilizers. *J. Algebra*, 150(2):435–502.

[Kapovich, 2007] Kapovich, I. (2007). Clusters, currents, and Whitehead's algorithm. *Experiment. Math.*, 16(1):67–76.

[Kapovich et al., 2006] Kapovich, I., Schupp, P., and Shpilrain, V. (2006). Generic properties of Whitehead's algorithm and isomorphism rigidity of random one-relator groups. *Pacific J. Math.*, 223(1):113–140.

[Khan, 2004] Khan, B. (2004). The structure of automorphic conjugacy in the free group of rank two. In *Computational and experimental group theory*, volume 349 of *Contemp. Math.*, pages 115–196. Amer. Math. Soc., Providence, RI.

[Kharlampovich and Ventura, 2012] Kharlampovich, O. and Ventura, E. (2012). A Whitehead algorithm for toral relatively hyperbolic groups. *Internat. J. Algebra Comput.*, 22(8):1240004, 9.

[Kim and Oum, 2014] Kim, S.-h. and Oum, S.-i. (2014). Hyperbolic surface subgroups of one-ended doubles of free groups. *J. Topol.*, 7(4):927–947.

[Krstić et al., 2001] Krstić, S., Lustig, M., and Vogtmann, K. (2001). An equivariant Whitehead algorithm and conjugacy for roots of Dehn twist automorphisms. *Proc. Edinb. Math. Soc. (2)*, 44(1):117–141.

[Lee, 2002] Lee, D. (2002). Endomorphisms of free groups that preserve automorphic orbits. *J. Algebra*, 248(1):230–236.

[Lee, 2006] Lee, D. (2006). Counting words of minimum length in an automorphic orbit. *J. Algebra*, 301(1):35–58.

[Lee, 2007] Lee, D. (2007). An algorithm that decides translation equivalence in a free group of rank two. *J. Group Theory*, 10(4):561–569.

[Levitt and Vogtmann, 2000] Levitt, G. and Vogtmann, K. (2000). A Whitehead algorithm for surface groups. *Topology*, 39(6):1239–1251.

[Lyndon and Schupp, 2001] Lyndon, R. C. and Schupp, P. E. (2001). *Combinatorial group theory*. Classics in Mathematics. Springer-Verlag, Berlin. Reprint of the 1977 edition.

[Magnus et al., 2004] Magnus, W., Karrass, A., and Solitar, D. (2004). *Combinatorial group theory*. Dover Publications, Inc., Mineola, NY, second edition. Presentations of groups in terms of generators and relations.

[Manjarrez-Gutiérrez et al., 2015] Manjarrez-Gutiérrez, F., Núñez, V., and Ramírez-Losada, E. (2015). Circular handle decompositions of free genus one knots. *Pacific J. Math.*, 275(2):361–407.

[Massey, 1977] Massey, W. S. (1977). *Algebraic topology: an introduction*. Springer-Verlag, New York-Heidelberg. Reprint of the 1967 edition, Graduate Texts in Mathematics, Vol. 56.

[McCool, 1974] McCool, J. (1974). A presentation for the automorphism group of a free group of finite rank. *J. London Math. Soc. (2)*, 8:259–266.

[Miasnikov and Myasnikov, 2004] Miasnikov, A. D. and Myasnikov, A. G. (2004). Whitehead method and genetic algorithms. In *Computational and experimental group theory*, volume 349 of *Contemp. Math.*, pages 89–114. Amer. Math. Soc., Providence, RI.

[Myasnikov and Haralick, 2006] Myasnikov, A. D. and Haralick, R. M. (2006). A hybrid search algorithm for the Whitehead minimization problem. *J. Symbolic Comput.*, 41(7):818–834.

[Myasnikov and Shpilrain, 2003] Myasnikov, A. G. and Shpilrain, V. (2003). Automorphic orbits in free groups. *J. Algebra*, 269(1):18–27.

[Nielsen, 1917] Nielsen, J. (1917). Die Isomorphismen der allgemeinen, unendlichen Gruppe mit zwei Erzeugenden. *Math. Ann.*, 78(1):385–397.

[Nielsen, 1918] Nielsen, J. (1918). Über die Isomorphismen unendlicher Gruppen ohne Relation. *Math. Ann.*, 79(3):269–272.

[Nielsen, 1924] Nielsen, J. (1924). Die Isomorphismengruppe der freien Gruppen. *Math. Ann.*, 91(3-4):169–209.

[Rapaport, 1958] Rapaport, E. S. (1958). On free groups and their automorphisms. *Acta Math.*, 99:139–163.

[Roig et al., 2007] Roig, A., Ventura, E., and Weil, P. (2007). On the complexity of the Whitehead minimization problem. *Internat. J. Algebra Comput.*, 17(8):1611–1634.

[Stallings, 1983] Stallings, J. R. (1983). Topology of finite graphs. *Inventiones mathematicae*, 71:551–565.

[Stallings, 1987] Stallings, J. R. (1987). Graphical theory of automorphisms of free groups. In *Combinatorial group theory and topology (Alta, Utah, 1984)*, volume 111 of *Ann. of Math. Stud.*, pages 79–105. Princeton Univ. Press, Princeton, NJ.

[Stallings, 1999] Stallings, J. R. (1999). *Whitehead graphs on handlebodies*. Geometric group theory down under (Canberra, 1996).

[Stong, 1997] Stong, R. (1997). Diskbusting elements of the free group. *Math. Res. Lett.*, 4(2-3):201–210.

[Wade, 2014] Wade, R. D. (2014). Folding free-group automorphisms. *Q. J. Math.*, 65(1):291–304.

[Whitehead, 1936a] Whitehead, J. H. C. (1936a). On Certain Sets of Elements in a Free Group. *Proc. London Math. Soc. (2)*, 41(1):48–56.

[Whitehead, 1936b] Whitehead, J. H. C. (1936b). On equivalent sets of elements in a free group. *Ann. of Math. (2)*, 37(4):782–800.

[Wilton, 2018] Wilton, H. (2018). Essential surfaces in graph pairs. *J. Amer. Math. Soc.*, 31(4):893–919.