Combinatorial Group Theory of Braid Groups

Name : Usman Ali

Year of Admission : 2004

Registration No. : 54-GCU-PHD-SMS-2004

Abdus Salam School of Mathematical Sciences

GC University Lahore, Pakistan

Combinatorial Group Theory of Braid Groups

Submitted to

Abdus Salam School of Mathematical Sciences

GC University Lahore, Pakistan

in the partial fulfillment of the requirements for the award of degree of

Doctor of Philosophy

in

Mathematics

By

Name : Usman Ali

Year of Admission : 2004

Registration No. : 54-GCU-PHD-SMS-2004

Abdus Salam School of Mathematical Sciences

GC University Lahore, Pakistan

DECLARATION

I, **Mr. Usman Ali** Registration No. **54-GCU-PHD-SMS-2004** student at **Abdus Salam School of Mathematical Sciences GC University** in the subject of **Mathematics**, hereby declare that the matter printed in this thesis titled

"Combinatorial Group Theory of Braid Groups"

is my own work and that

(i) I am not registered for the similar degree elsewhere contemporaneously.

(ii) No direct major work had already been done by me or anybody else on this topic; I worked on, for the Ph. D. degree.

(iii) The work, I am submitting for the Ph. D. degree has not already been submitted elsewhere and shall not in future be submitted by me for obtaining similar degree from any other institution.

Dated: ------------------------- -----------------------------------

Signature

<u>RESEARCH COMPLETION CERTIFICATE</u>

Certified that the research work contained in this thesis titled **"<u>Combinatorial Group Theory of Braid Groups</u>"** has been carried out and completed by Mr. **<u>Usman Ali</u>** Registration No. **54-GCU-PHD-SMS-2004** under my supervision.

-----------------------------   ------------------------------

Date   Supervisor

Dr. Barbu Berceanu

Submitted Through

<u>Dr. A. D. Raza Choudary</u>   -------------------------------

Director General
Abdus Salam School of
Mathematical Sciences,
GC University Lahore, Pakistan

Controller of Examination
GC University Lahore

To the memory of my benign Mother

Table of Contents

Acknowledgements

I would like to thank my supervisor, Professor Barbu Berceanu, for his guidance and precious time.

I would like to thank Professor Allah Ditta Raza Chaudhry who supported me through adverse times and gave me numerous encouragement.

My thanks are for all colleagues from Abdus Salam School of Mathematical Sciences. I especially thank colleagues of Batch I and II for the wonderful environment they created at ASSMS.

Of course, I am grateful to my wife, children, brothers, and sisters for their patience, support, and love. My special thanks go to my grandmother for her countless prayers.

Finally, I am thankful to the following: Zaffar Iqbal (for his collaboration); Dr. Syed Iqbal Hussain, Dr. Mubashir (for their professional support when I was severely depressed); Faiz Jailany (for his friendship); professor Usman Khalil (for his guidance); and Awais Naeem, Nauman for their office support.

ASSMS, Lahore — Usman Ali

March 11, 2009.

Introduction

Braid theory was first introduced by Emil Artin in 1925 ([2]). The Alexander theorem stating that "Every link (or knot) is equivalent to the closure of a braid" motivated mathematicians to study braids in order to solve problems in knot theory. The conjugacy problem of braid groups is related to the problem of isotopy of knots and links ([6]). If two braids are conjugate, their closures are isotopic links (or knots).

A *geometric braid* can be defined as finite family of continuous curves located between two parallel planes in the three-dimensional Euclidian space. The curves are not allowed to intersect; they start on a predefined set of distinct points, the starting points, on the first plane; and end on a similar set of points, the ending points, on the second plane. The curves (we call them strings) must go strictly downward. It can be assumed that the starting points and the ending points are the complex numbers $p_1, p_2, \ldots, p_n$. A braid with n strings is called an *n-braid.* Two braids are equivalent, if one can be continuously deformed into the other one through braids.

The multiplication of two braids is defined by concatenating the ending points of strings of one braid to the starting points of the other braid. The equivalence classes of braids under the above multiplication form a group known as *Artin braid group*, denoted by $\mathcal{B}_{n+1}$.

Braid groups are Artin groups whose corresponding Coxeter groups are symmetric groups. The larger class of Artin groups having finite Coxeter groups are called *spherical Artin groups.* Both the word and conjugacy problems are solvable in these groups [11] and [16].

In this thesis we study spherical Artin monoids, especially the braid monoids. The main focus is to find better solutions for the word and conjugacy problems in spherical Artin groups. We apply complete presentations (non-commutative Gröbner bases), in case of braid monoids, to obtain some new results which modify (or possibly improve) the algorithms to obtain Garside normal form and left-canonical form of a braid word.

Chapter 1 contains preliminaries and the classical solution for word and conjugacy problem of braid groups. This classical solution of word and conjugacy problem was given by Garside in ([18]); the problem was actually reduced to a problem in the corresponding braid monoid. The terminology and notations used in this chapter will be followed throughout this thesis. This first chapter does not contain original results.

Chapter 2 is devoted to the word problem of spherical Artin monoids. We introduce and characterize *relative Garside element* corresponding to an embedding $\Gamma_{n-1} \hookrightarrow \Gamma_n$ (i.e, the Coxeter graph Γ_n is obtained from Coxeter graph Γ_{n-1} by just adding one vertex to it). We compute this relative Garside element using its characterization. We also describe completely the Garside elements for spherical Artin monoids. Next we introduce *fragments* of relative Garside elements and apply these to find complete presentation for some spherical Artin monoids. This chapter is a result of joint work [4] with Zaffar Iqbal .

In chapter 3, we find unique representative in the conjugacy class of a 3-braid to give a complete solution to the conjugacy problem in $\mathcal{B}_3$, a braid group on three strings. As a consequence, a class formula corresponding to conjugacy classes is obtained and is proved that the number of conjugacy classes for a fixed length grows exponentially. Application to knot theory are given. This last chapter is part of my paper [24] accepted in the journal " Algebra Colloquium". The results of this paper was cited by Birman and Menasco in ([7]).

In chapter 4, we give a procedure to obtain divisors of Garside braid. Next we give a new method to compute initial set of these divisors. Morton and Elrifai [17] introduced the unique left-canonical form for braids. This left-canonical form provides a solution to the word problem in braid groups; it is also the key ingredient in most of the solutions to conjugacy problem given so for. We modify the method given in [17] to check the left-canonical form of braids. Here we also introduce an inductive way of finding exponent of a positive word.

Chapter 1

Preliminaries

1.1 Braid groups and monoids

The braid group $\mathcal{B}_{n+1}$ admits the following classical presentation given by Artin [3]:

$$\mathcal{B}_{n+1} = \left\langle x_1, x_2, \cdots, x_n : \begin{array}{l} x_{i+1}\, x_i\, x_{i+1} \ = \ x_i\, x_{i+1}\, x_i \\ x_i\, x_j \ = \ x_j\, x_i \text{ for } |i-j| \geq 2 \end{array} \right\rangle \tag{1.1.1}$$

The set of positive braids or the braid monoid, $\mathcal{MB}_{n+1}$ can be defined in two different ways:

(i) $\mathcal{MB}_{n+1} = \{W \in \mathcal{B}_{n+1} | W = x_{i_1}^{a_1} \cdots x_{i_k}^{a_k} | a_1, \ldots, a_k \geq 0\}$.

(ii) Let $F[X]$ be a free monoid generated by a finite ordered set $X = \{x_1, x_2, \cdots, x_n\}$. The braid monoid, $\mathcal{MB}_{n+1}$ is the quotient F/N of $F[X]$ for N being the congruence on F generated by the relations

$$\{(\ x_{i+1}\, x_i\, x_{i+1} = \ x_i\, x_{i+1}\, x_i), (\ x_i\, x_j \ = \ x_j\, x_i \text{ for } |i-j| \geq 2)\}.$$

Garside [18] proved that (i) and (ii) are equivalent. From definition (ii), it is clear that $\mathcal{MB}_{n+1}$ admits the presentation (1.1.1) as a monoid.

Notation: The signs $\equiv$ and $=$ represents the equality in free groups (monoids) and braid groups (monoids) respectively.

Definition 1.1.1. The set $D(W) = \{U \in F[X] \mid p(U) = W\}$ is called *the diagram* of a word $W \in \mathcal{MB}_{n+1}$, where p is the canonical map, $p : F[X] \to F/N$.

Definition 1.1.2. The set $St(W) = \{i \mid x_i U_i = W$ for some $U_i \in \mathcal{MB}_{n+1}\}$ is called *the initial set* of a word $W \in \mathcal{MB}_{n+1}$. Similarly, the set $Fl(W) = \{i \mid U_i x_i = W$ for some $U_i \in \mathcal{MB}_{n+1}\}$ is called *the final set* of a word $W \in \mathcal{MB}_{n+1}$.

Three natural partial orders $|$, $|_L$, and $|_R$ are defined on $\mathcal{MB}_{n+1}$. For each W, $U \in \mathcal{MB}_{n+1}$ we write, $W \mid U$ when $U = C_1 W C_2$ for some C_1, $C_2 \in \mathcal{MB}_{n+1}$ and W is called a *divisor* of U. Furthermore, W is called *left-divisor* of U denoted by $W \mid_L U$ if $U = WC$ for some $C \in \mathcal{MB}_{n+1}$ and W is called *right-divisor* of U denoted by $W \mid_R U$ if $U = CW$ for some $C \in \mathcal{MB}_{n+1}$. Let $|W|$ denotes length of a positive word W then the total order on the $F[X]$, called *the length-lexicographic order* $>$ is defined as: if $|W| > |U|$ then $W > U$ and, if $|W| = |U|$ we use lexicographic order given by $x_i > x_j$ if $i > j$.

The order $|_L$ will be used more frequently in the coming chapters. This order is a lattice order [11], i.e., for every W, $U \in \mathcal{MB}_{n+1}$ there exist a unique least common multiple $W \vee_L U$ and a unique greatest common divisor $W \wedge_L U$.

Definition 1.1.3. A word W is called *canonical form* if it is the smallest, length-lexicographically, in its diagram.

1.2 Garside braid and its properties

The element $\Delta_{n+1} = x_1(x_2x_1)\cdots(x_1x_2\cdots x_n)$ in $\mathcal{MB}_{n+1}$ is called *Garside braid* (*Garside element*). Geometrically, Δ_{n+1} is equivalent to a half-twist of identical braid. The Garside braid and its divisors play a key role in the solutions of the word and conjugcy problem in $\mathcal{B}_{n+1}$ given by Garside [18]. Apart from the fact that Δ_{n+1}^2

generates the center of $\mathcal{B}_{n+1}$ [14], it has some other useful properties discussed by Garside [18]:

1. Conjugation by Δ_{n+1} is given as $\alpha_\Delta(x_i) = \Delta_{n+1}x_i\Delta_{n+1}^{-1} = x_{n+1-i}$ and hence $\alpha_\Delta(W) = \widehat{W}$, where $\widehat{W} = x_{n+1-i_1}x_{n+1-i_2}\cdots x_{n+1-i_s}$ for $W = x_{i_1}x_{i_2}\cdots x_{i_s}$.

2. $\Delta_{n+1} \mid W$ implies $\Delta_{n+1} \mid_L W$ and $\Delta_{n+1} \mid_R W$. Similarly $W \mid \Delta_{n+1}$ implies $W \mid_L \Delta_{n+1}$ and $W \mid_R \Delta_{n+1}$.

3. $St(\Delta_{n+1}) = \{1, 2, \ldots, n\} = Fl(\Delta_{n+1})$.

4. Δ_{n+1} is the least common multiple of the set of generators $x_1, x_2, \cdots, x_3$.

5. Δ_{n+1} is square free (there is no generator x_i such that $x_i^2 \nmid \Delta_{n+1}$, though, in some cases Δ_{n+1} itself is a square: for example $\Delta_4 = x_1(x_2x_1)(x_3x_2x_1) = (x_1x_3x_2)^2$.) (see [16], [22].)

Definition 1.2.1. The set $\mathcal{MB}_{n+1}^+ = \mathcal{MB}_{n+1} \backslash \Delta_{n+1}\mathcal{MB}_{n+1}$ is called the set of *primes* to Δ_{n+1}.

Definition 1.2.2. a) A nonnegative integer k is called the *exponent* of a word V in $\mathcal{MB}_{n+1}$ if $\Delta_{n+1}^k \mid V$ but $\Delta_{n+1}^{k+1} \nmid V$; this will be be denoted by $exp_{n+1}(V)$.

b) An integer k is called the *exponent* of a word V in $\mathcal{B}_{n+1}$ if $V = \Delta_{n+1}^k W$, where $W \in \mathcal{MB}_{n+1}^+$.

1.3 Word and conjugacy problem

Two words of $\mathcal{MB}_{n+1}$ are equivalent if and only if they have the same diagrams. The solution of word and conjugacy problem in $\mathcal{B}_{n+1}$ was reduced [18] to a problem in $\mathcal{MB}_{n+1}$. Elements in $\mathcal{B}_{n+1}$ admit a unique *Garside normal form* $\Delta_{n+1}^r W$, where $r \in \mathbb{Z}$ and $W \in \mathcal{MB}_{n+1}^+$: two words of $\mathcal{B}_{n+1}$ are equivalent if and only if their normal forms coincide. Garside also proved that in a given conjugacy class, C (with some exceptions, i.e., the conjugacy class of trivial word and that of central elements of $\mathcal{B}_{n+1}$, C is an infinite set). The set of numbers r such that $\Delta_{n+1}^r W \in C$ has a least upper bound, $\exp(C)$. The *summit set* of a conjugacy class C is defined as:

$$SS(C) = \{\Delta_{n+1}^r W \in C \mid r = \exp(C)\}.$$

and this is a finite set. In this way, Garside's [18] solution of the conjugacy problem is to compute $SS(C)$: two elements in $\mathcal{B}_{n+1}$ are conjugate if and only if they have the same $SS(C)$.

Almost all the other solutions to the word and conjugacy problems in $\mathcal{B}_{n+1}$ [17],[19], and [20] adopt the same approach of Garside with a slight modification in order to have a faster algorithm of the Garside solution. In [17],[19], and [20] subsets of the summit set were introduced to have conjugacy invariants of smaller cardinality than the summit set. These conjugacy invariants are: *super summit set* [17], *ultra summit set* [19] and *reduced super summit set* [20].

In order to improve the Garside's solution [18] to the word and conjugacy problem in $\mathcal{B}_{n+1}$, Elrifai and Morton in [17] introduced the left-canonical form or left-greedy form for braids.

Definition 1.3.1. [17] A product A_1A_2 of two divisors A_1 and A_2 of Δ_{n+1} is called *left-weighted* if $A_1A_2 \wedge_L \Delta_{n+1} = A_1$.

Definition 1.3.2. [17] The word $V = \Delta_{n+1}^r A_1 A_2 \cdots A_s$ of $\mathcal{B}_{n+1}$ is said to be in *left-canonical form* if each A_i is a proper divisor of Δ_{n+1} and $A_iA_{i+1} \wedge_L \Delta_{n+1} = A_i$ for each pair A_iA_{i+1}.

Let $V = \Delta_{n+1}^r A_1 A_2 \cdots A_s$ be the left-canonical form of $V \in \mathcal{B}_{n+1}$. The number r is called the *infimum* of V and is denoted by $inf(V)$, $r+s$ is called the *supremum* and is denoted by $sup(V)$ and s is called the *canonical length* and is denoted by $l(V)$.

The above terminology [17] comes from the fact that r is the greatest number such that $\Delta_{n+1}^r \mid_L V$ and $r+s$ is the smallest number such that $V \mid_L \Delta_{n+1}^{r+s}$.

For the conjugacy class C of V in $\mathcal{B}_{n+1}$ the following are defined [17]:

$$\inf(C) = \max\{\inf(U) : U \in C\} \text{ and } \sup(C) = \min\{\sup(U) : U \in C\}.$$

The super summit set of conjugacy class C is defined as:

$$SSS(C) = \{U \in C : inf(U) = inf_C(V),\, sup(U) = sup_C(V)\}.$$

Definition 1.3.3. [17] Given $V = \Delta_{n+1}^r A_1 A_2 \cdots A_s$ written in left-canonical form, where $s > 0$, then the cycling of V is the conjugate, $c(V) = \Delta_{n+1}^r A_2 A_3 \cdots A_s \tau^{-r}(V)$ and decycling of V is the conjugate $d(v) = A_s \Delta_{n+1}^r A_1 A_2 \cdots A_{s-1}$, where τ is the inner automorphism defined by $\tau(x_i) = \Delta_{n+1}^{-1} x_i \Delta_{n+1}$.

The ultra summit set and reduced super summit set are defined as [19] and [20]:

$$USS(V) = \{U \in SSS(V) |\, c^m(U) = U \, \text{for some } \ m \geq 1\},$$

$$RSSS(V) = \{U \in SSS(V) |\, c^{m_1}(U) = U \, \text{and} \, d^{m_2}(U) = U \text{for some } \ m_1, m_2 \geq 1\}.$$

It is obvious that $RSSS(V) \subseteq USS(V) \subseteq SSS(V) \subseteq SS(V)$ for all $V \in \mathcal{B}_{n+1}$.

1.4 Coxeter groups and Artin groups

Let S be a set. A *Coxeter matrix* over S is a square matrix $M = (m_{st})_{s,t \in S}$ indexed by the the elements of S such that

- $m_{ss} = 1$ for all $s \in S$;
- $m_{st} = m_{ts} \in \{2, 3, 4, \ldots, \infty\}$ for all $s, t \in S$, $s \neq t$.

A *Coxeter graph* Γ is a labeled graph defined by the following data.

- S is a set of vertices of Γ.

- Two vertices $s, t \in S, s \neq t$ are joined by an edge if $m_{st} \geq 3$. This edge is labeled by m_{st} if $m_{st} \geq 4$.

(A Coxeter matrix $M = (m_{st})_{s,t \in S}$ is usually represented by its Coxeter graph Γ.)

Definition 1.4.1. Let $M = (m_{st})_{s,t \in S}$ be the Coxeter matrix of the Coxeter graph Γ. Then the group defined by

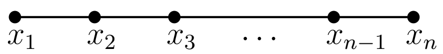
$$\mathcal{W}(\Gamma) = \Big\langle s \in S \,\Big|\; s^2 = 1\,, (st)^{m_{st}} = 1 \;\text{ for all } s, t \in S,\ s \neq t, \text{ and } m_{st} \neq \infty \Big\rangle$$

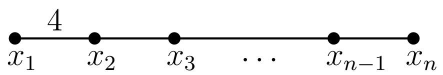
is called the *Coxeter Group* (of type Γ).

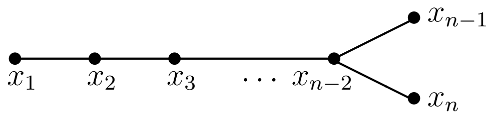
In a simple way we can write $\mathcal{W}(\Gamma) = \Big\langle s \in S \Big| \, s^2 = 1,\ \underbrace{sts\cdots}_{m_{st}\,\text{factors}} = \underbrace{tst\cdots}_{m_{st}\,\text{factors}} \Big\rangle$.

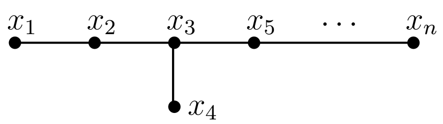
We call Γ_n, with n vertices, to be of *spherical type* if $\mathcal{W}(\Gamma_n)$ is finite.

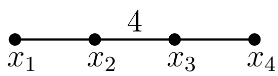
Theorem 1.4.1 ([10])**.** *The graph Γ_n is of spherical type if and only if Γ_n is of a finite union of graphs in the following list.*

$(A_n)_{n \geq 1}$:


$(B_n)_{n \geq 2}$:


$(D_n)_{n \geq 4}$:


$(E_n)_{n=6,7,8}$:


F_4 :


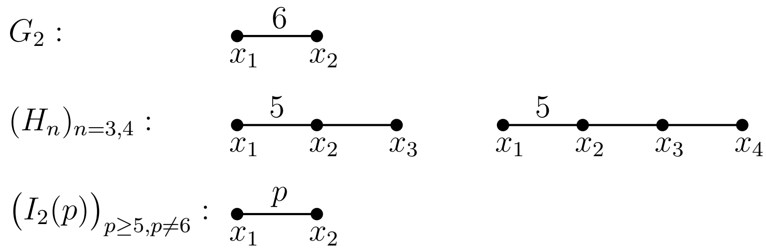


Figure 1.1. The connected spherical type Coxeter graphs.

Definition 1.4.2. If $\mathcal{W}(\Gamma_n)$ is a Coxeter group then the *Artin group associated to* $\mathcal{W}(\Gamma_n)$ is defined by

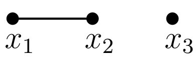
$$\mathcal{A}(\Gamma_n) = \left\langle s \in S \,\middle|\, \underbrace{sts\cdots}_{m_{st}\text{ factors}} = \underbrace{tst\cdots}_{m_{st}\text{ factors}} \right\rangle.$$

If $\mathcal{W}(\Gamma_n)$ is a finite group then $\mathcal{A}(\Gamma_n)$ is called an *Artin spherical group.*

Artin spherical monoids $\mathcal{M}(\Gamma_n)$ are defined corresponding to each $\mathcal{A}(\Gamma_n)$, analogous to the braid monoids $\mathcal{M}(A_n) = \mathcal{MB}_{n+1}$ defined by the same presentation of $\mathcal{B}_{n+1}$. All these monoids are Garside monoids, i.e, they are equipped with Garside element $\Delta(\Gamma_n)$, like $\mathcal{M}(A_n) = \mathcal{MB}_{n+1}$ is equipped with $\Delta(A_n) = \Delta_{n+1}$. The four order $|$, $|_L$, $|_R$, and $>$ can be defined on these monoids.

Definition 1.4.3. If all the labels in a Coxeter graphs are 2 or ∞ then the associated groups are called *right-angled* Artin spherical groups.

Remark 1.4.2. *We are using different convention for the graph associated to right angled Artin groups. For example in the literature, the graph*

$G:$ 

represents the group $\langle x_1, x_2, x_3 | x_1x_2 = x_2x_1\rangle$ *but in our convention the given graph* G *represents the group* $\langle x_1, x_2, x_3 | x_1x_3 = x_3x_1, x_2x_3 = x_3x_2\rangle$.

1.5 Complete presentation of braid monoids

All the following notions are in [1], [5], [9] , [12], [15] and [23] under different names: complete presentation, Gröbner bases, presentation with solvable ambiguities, rewriting system and so on.

Let $F[X]$ be a free monoid generated by $X = \{x_1, x_2, \ldots, x_n\}$. The *total order* on the set of generators given by $x_1 < x_2 < \cdots < x_n$ is extended to *length-lexicographic order* $<$. Let $\mathcal{M}$ be a monoid, constructed by defining some relations in $F[X]$. A defining relation $\mathcal{R}$ in $\mathcal{M}$ is written in the form $a_i = b_i$ where a_i is a monomial greater than b_i. Denote by $a_i(\mathcal{R})$ and $b_i(\mathcal{R})$ the terms a_i and b_i respectively of the given relation $\mathcal{R}$. For $W \in \mathcal{M}$, define two reduction rules:

$$L(W) = \begin{cases} W & \text{if } a_i(\mathcal{R}) \nmid W \text{ for all relations } \mathcal{R}, \\ L(\gamma b_j \delta) & \text{if } W = \gamma a_j \delta \text{ and if } W = \varepsilon a_k \eta \text{ then } |\gamma| < |\varepsilon|. \end{cases}$$

$$R(W) = \begin{cases} W & \text{if } a_i(\mathcal{R}) \nmid W \text{ for all relations } \mathcal{R}, \\ R(\gamma b_j \delta) & \text{if } W = \gamma a_j \delta \text{ and if } W = \varepsilon a_k \eta \text{ then } |\delta| < |\eta|. \end{cases}$$

In the monoid $\mathcal{M}$, a word containing the L.H.S. of a relation is called *reducible* and a word which does not contain the L.H.S. of a relation is called *irreducible*. The Diamond lemma (see [5] or [15]) says that if all the ambiguities are solvable (for any overlap $a_i = \gamma_i \delta, a_j = \delta \epsilon_j, \delta \neq 1$, reductions of $(\gamma_i \delta)\epsilon_j \to b_i \epsilon_j \to \cdots$ and $\gamma_i(\delta \epsilon_j) \to \gamma_i b_j \to \cdots$ give the same result), then the set of irreducible words is in bijection with the monoid with the presentation $\langle x_1, x_2, \ldots, x_n : a_i = b_i, i \in I \rangle$ (I could be an infinite set). The above presentation is called *complete presentation* and the irreducible words are called canonical forms. In this way the word problem in the monoid $\mathcal{M}$ is solved by computing the canonical forms.

With the notations $\alpha(i,j) = \alpha(x_i, x_{i+1}, \ldots, x_j)$ for arbitrary word in $x_i, x_{i+1}, \ldots, x_j$; $\Sigma\alpha(i,j) = \alpha(x_{i+1}, x_{i+2}, \ldots, x_{j+1})$; and $\lambda(i,j) = x_i x_{i-1} \cdots x_{j+1} x_j$, Bokut [9] gave the complete presentation (Gröbner bases) of $\mathcal{MB}_{n+1}$ and proved:

Theorem 1.5.1. [9] *A complete presentation (Gröbner- bases) of* $\mathcal{MB}_{n+1}$ *consists of the following relations:*

(i) $x_{i+1}x_i\alpha(i-1,1)\beta(j,i)\lambda(i+1,j) = x_ix_{i+1}x_i\alpha(i-1,1)\lambda(i,j)\Sigma\beta(j,i)$,

(ii) $x_sx_k = x_kx_s$, $s-k \geq 2$,

where $1 \leq i \leq n-1, 1 \leq j \leq i+1$

Definition 1.5.1. A complete presentation $\langle x_1, x_2, \ldots, x_n : a_i = b_i, i \in I\rangle$ of a monoid is called *reduced* if $a_j|a_i$ implies $i = j$.

Chapter 2

Relative Garside elements and complete presentation of some Artin monoids

2.1 Introduction

We describe *relative Garside element* in § 2.2, in order to construct Garside element $\Delta(\Gamma_{n-1})$ from $\Delta(\Gamma_n)$ for $\Gamma_{n-1} \subset \Gamma_n$, (i.e, Γ_n is obtained from Γ_{n-1} by just adding one vertex to it.) In § 2.3, we describe particular left-divisors (*fragments*) of relative Garside element. These fragments are important, because left side of each relation in complete presentation of $\mathcal{M}(\Gamma_n)$ is right-divisible by one of such fragments. Using computation (commutations or shifts) of fragments with generators $x_1, \ldots, x_n$, we give and prove complete presentation of $\mathcal{M}(A_n)$, $\mathcal{M}(B_n)$, and $\mathcal{M}(I_n(p))$.

2.2 Relative Garside elements

Suppose we have an inclusion of Coxeter graphs $\Gamma_{n-1} \subset \Gamma_n$ with the set of vertices $\{x_1, \ldots, x_{n-1}\}$, respectively $\{x_1, \ldots, x_n\}$. Using the general properties of Garside elements we have

$$\Delta(\Gamma_{n-1})|_L \Delta(\Gamma_n).$$

Definition 2.2.1. We define the relative Garside element $\Delta(\Gamma_n, \Gamma_{n-1})$ by

$$\Delta(\Gamma_n) = \Delta(\Gamma_{n-1})\Delta(\Gamma_n, \Gamma_{n-1}).$$

If there is no ambiguity related to the inclusion $\Gamma_{n-1} \subset \Gamma_n$, we denote in a simple form:

$$\Delta_n = \Delta_{n-1} T_n$$

Proposition 2.2.1. *The relative Garside element T_n for $\Gamma_{n-1} \subset \Gamma_n$, satisfies the following properties:*

1) *T_n is square free.*

2) *$x_i|_L T_n \Leftrightarrow i = n$.*

3) *there is a bijection $\sigma : \{1, \dots, n-1\} \to \{1, \dots, \widehat{m}, \dots, n\}$ such that $x_i T_n = T_n x_{\sigma(i)}$.*

4) *$x_j|_R T_n \Leftrightarrow j = m$.*

Proof. Let $\Delta_n = \Delta_{n-1} T_n$ then

1) T_n is square free because Δ_n is square free;

2) $x_i\,(1 \le i \le n-1)$ cannot be a left divisor of T_n: otherwise, $T_n = x_i U$. But $x_i|_R \Delta_{n-1}$ implies $\Delta_{n-1} = V x_i$. Therefore $\Delta_n = \Delta_{n-1} T_n = V x_i^2 U$, a contradiction.

3) Let $\sigma_{n-1} : \{1, \dots, n-1\} \to \{1, \dots, n-1\}$ and $\sigma_n : \{1, \dots, n\} \to \{1, \dots, n\}$ the bijection defined by conjugation with Δ_{n-1}, respectively Δ_n: $x_i \Delta_{n-1} = \Delta_{n-1} x_{\sigma_{n-1}(i)}$, $x_i \Delta_n = \Delta_n x_{\sigma_n(i)}$. Now

$$\Delta_{n-1} x_i T_n = x_{\sigma_{n-1}^{-1}(i)} \Delta_{n-1} T_n = x_{\sigma_{n-1}^{-1}(i)} \Delta_n = \Delta_n x_{\sigma_n \circ \sigma_{n-1}^{-1}(i)} = \Delta_{n-1} T_n x_{\sigma_n \circ \sigma_{n-1}^{-1}(i)},$$

therefore $x_i T_n = T_n x_{\sigma(i)}$, where $\sigma = \sigma_n \circ \sigma_{n-1}^{-1}$. The image of σ contains the elements $1, \dots, n$, but not $\sigma_n(n) = m$.

4) Let $x_j \neq x_m$ then there exists $i \in \{1, \ldots, n-1\}$ such that $j = \sigma(i)$ and $x_i T_n = T_n x_j$. Suppose $x_j \mid_R T_n$. Then $T_n = S x_j$. But $x_i T_n = T_n x_j = S x_j^2$, a contradiction, because $x_i T_n$ is a divisor of Δ_n. $\square$

Proposition 2.2.2. *If $U_n \in \mathcal{M}(\Gamma_n)$ satisfies:*

1) $x_m^2 \nmid U_n$;

2) $x_i|_L U_n \Leftrightarrow i = n$;

3) *there is a bijection* $\tau : \{1, \ldots, n-1\} \to \{1, \ldots, \widehat{k}, \ldots, n\}$ *such that* $x_i U_n = U_n x_{\tau(i)}$,

then $U_n = T_n$ *(and also* $k = m$, $\tau = \sigma$*).*

Proof. Let us define $D = \Delta_{n-1} U_n$. Because $x_i \mid_L \Delta_{n-1}, i = 1, \ldots, n-1$ and from 3) and 2) we have $x_n|_L D_n$, we obtain $x_i|_L \Delta_{n-1} U_n$ for any $i = 1, \ldots, n$, therefore $\Delta_n|_L D$. This implies that $\Delta_{n-1} T_n|_L \Delta_{n-1} U_n$, i.e., $T_n|_L U_n$. If $T_n \neq U_n$, then $T_n x_j W = U_n$. If $j \neq m$, then $j = \sigma_n(i)$ for some $i \in \{1, \ldots, n-1\}$, hence $U_n = T_n x_{\sigma(i)} W = x_i T_n W$ and this contradicts 2). If $j = m$, then $U_n = (S x_m) x_m W$ which contradicts 1). $\square$

Proposition 2.2.3. *If $U_n \in \mathcal{M}(\Gamma_n)$ satisfies:*

1) $x_n|_L U_n$;

2) *there is a bijection* $\tau : \{1, \ldots, n-1\} \to \{1, \ldots, \widehat{k}, \ldots, n\}$ *such that* $x_i U_n = U_n x_{\tau(i)}$;

3) U_n *has minimal length among the words satisfying* 2) *and* 3)*,*

then $U_n = T_n$ (and $also$ $k = m$, $\tau = \sigma$).

Proof. Let us define $D = \Delta_{n-1} U_n$. As in the previous proof, 1) and 2) implies $x_i|_L D$ for all $i = 1, \ldots, n$. Therefore $\Delta_n|_L D$, hence $T_n|_L U_n$. Because of 3), we have $|U_n| \leq |T_n|$ and T_n satisfies 1) and 2), therefore $T_n = U_n$. $\square$

Computation of Relative Garside and Garside Elements

1. Starting with A_1: 

and the Garside element $\Delta(A_1) = x_1$, we will construct, inductively, the Garside elements of the classical list.

2. If the graph Γ is disjoint union of Γ_1, Γ_2 then $\mathcal{M}(\Gamma) \cong \mathcal{M}(\Gamma_1) \times \mathcal{M}(\Gamma_1)$ and $\Delta(\Gamma) = \Delta(\Gamma_1).\Delta(\Gamma_2) = \Delta(\Gamma_2).\Delta(\Gamma_1)$.

3. Construction of $\Delta(A_n, A_{n-1})$:

Let us define $U_n = x_n x_{n-1} \cdots x_1$; then U_n satisfies the properties of the Proposition 2.2.2:

1) U_n is square free (U_n is rigid, i.e, there is unique word representing U_n);

2) $x_i|_L U_n \Leftrightarrow i = n$ for the same reason;

3) $x_i U_n = U_n x_{i+1}$, i.e., $\sigma(i) = i + 1$ where $i = 1, \ldots, n-1$.

Corollary 2.2.4. *(classical Garside element)*

$$\Delta_n(A) = x_1(x_2 x_1) \cdots (x_{n-1} \cdots x_1)(x_n \cdots x_1).$$

4. Construction of $\Delta(B_n, B_{n-1})$: For B_2 we have $\Delta(B_2) = x_1(x_2 x_1 x_1)$ (see construction $\Delta(I_2(p), A_1)$.) Let $U_n = x_n x_{n-1} \cdots x_2 x_1 x_2 \cdots x_n$. Then U_n satisfies the properties of the Proposition 2.2.2:

1) U_n is square free (obvious, because U_n is rigid);

2) $x_i|_L U_n \Leftrightarrow i = n$ for the same reason;

3) $x_i U_n = U_n x_i$, i.e., $\sigma(i) = i$ where $i = 1, \ldots, n-1$.

Corollary 2.2.5.

$$\Delta_n(B) = x_1(x_2 x_1 x_2)(x_3 x_2 x_1 x_2 x_3) \cdots (x_n x_{n-1} \cdots x_2 x_1 x_2 \cdots x_{n-1} x_n).$$

5. Construction of $\Delta(I_2(p), A_1)$:

Let us define $U_2(p) = x_2 x_1 x_2 \cdots$ ($p - 1$ factors). Then U_n satisfies Proposition 2.2.3:

1) clearly $x_2|_L U_2(p)$;

2) we have $x_1 U_2(2p+1) = U_2(2p+1)x_2$ and $x_1 U_2(2p) = U_2(2p)x_1$;

3) any relation $x_1 A = B x_{\sigma(1)}$ should involve the unique defining relation $x_1 x_2 \cdots = x_2 x_1 \cdots$ so the length of A is $\geq p-1$; so $U_2(p)$ has minimal length.

Corollary 2.2.6.

$$\Delta(I_2(p)) = x_1 x_2 x_1 x_2 \cdots \ (p\, factors).$$

6. We give (without proof) the relative Garside and Garside element of E_6, E_7 and E_8 as follow:

E_6;

$T_6(E) = x_6x_5x_4x_3x_2x_1x_4x_3x_2x_5x_3x_4x_6x_5x_3x_2x_1 = x_6T_5(D)x_6x_5x_3x_2x_1$.

$x_1T_6(E) = T_6(E)x_6$, $x_2T_6(E) = T_6(E)x_5$, $x_3T_6(E) = T_6(E)x_3$, $x_4T_6(E) = T_6(E)x_2$ and $x_5T_6(E) = T_6(E)x_4$.

$\Delta(E_6) = \Delta(D_4)T_6(E) = \Delta(A_4)T_5(D)T_6(E)$

$x_i\Delta(E_6) = \Delta(E_6)x_{7-i}$. for $i = 1, 2, 5, 6$ and $x_i\Delta(E_6) = \Delta(E_6)x_i$. for $i = 3, 4$

E_7;

$T_7(E) = x_7T_6x_7x_6x_5x_3x_2x_4x_3x_5x_6x_7$.

$x_iT_7(E) = T_7(E)x_{7-i}$. for $i = 1, 2, 5, 6$ and $x_iT_7(E) = T_7(E)x_i$. for $i = 3, 4$

$\Delta(E_7) = \Delta(E_6)T_7$

$x_i\Delta(E_7) = \Delta(E_7)x_i$

E_8;

$T_8(E) = x_8T_7x_8T_7x_8$.

$x_iT_8(E) = T_8(E)x_i$.

$\Delta(E_8) = \Delta(E_7)T_8$

$x_i\Delta(E_8) = \Delta(E_8)x_i$

2.3 Fragments of relative Garside elements

For a fixed word $W \in \mathcal{M}(\Gamma_n)$ let us consider the subsets of the generators $\{x_1, \ldots, x_n\}$

$$A(W) = \{x_i : x_i W = W x_{\sigma(i)}\}, B(W) = \{x_j : W x_j = x_{\sigma^{-1}(j)} W\}$$

where σ is a bijection. We also have $\Sigma : A(W) \approx B(W)$ (defined by $\Sigma(x_i) = x_{\sigma(i)}$) and the partitions $A(W) = C(W) \coprod S(W)$, $B(W) = C(W) \coprod T(W)$ where

$$C(W) = \{x_i | x_i W = W x_i\} \text{ (the fixed part)},$$

$$S(W) = A(W) \smallsetminus C(W) \text{ (the shifted part)},$$

$$T(W) = B(W) \smallsetminus C(W).$$

We also denote by σ, the restriction $\sigma : s(W) \to t(W)$, where $s(W) = \{i \in N : x_i W = W x_{\sigma(i)}\}$ and $t(W) = \{j \in N : W x_j = x_{\sigma^{-1}(j)} W\}$. For instance; in $\mathcal{M}(A_n)$, $C(x_1 x_2) = \{x_4, x_5, \ldots, x_n\}$, $S(x_1 x_2) = \{x_2\}$, $\sigma(2) = 1$. Lets denote the fragments F_* of the relative Garside element T_n by

A: $F_i = x_n x_{n-1} \cdots x_i, 1 \leq i \leq n.$

B: $F_i = x_n x_{n-1} \cdots x_i, 2 \leq i \leq n.$

B: $F_{ii} = x_n x_{n-1} \cdots x_2 x_1 x_2 \cdots x_i$, $2 \leq i \leq n$.

$I_2(p)$: $F_{(p)} = T_{(p)} = x_2 x_1 x_2 \cdots$ ($p - 1$ factors).

$C(F_*) =$ set of generators of $\mathcal{A}$ which commute with F_*.

$S(F_*) =$ set of generators of $\mathcal{A}$ which are shifted by F_* where the shift-map σ is given by $x_i F_* = F_* x_{\sigma(i)}$.

Monoid	Fragment	$C(F)$	$S(F)$
A, B	$F_i, 1 \leq i \leq n-1$	$\begin{cases} \{x_1, \ldots, x_{i-2}\}, i \geq 3 \\ \emptyset, \quad i < 3 \end{cases}$	$\{x_i, \ldots, x_{n-1}\}$
A, B	F_n	$\{x_1, \ldots, x_{n-2}\}$	$\emptyset$
B	$F_{ii}, 2 \leq i \leq n$	$\{x_1, \ldots, x_{i-1}\}$	$\{x_{i+1}, \ldots, x_{n-1}\}$
$I_2(p)$	$F_{(p)}, p = \text{odd}$	$\emptyset$	$\{x_1\}$
$I_2(p)$	$F_{(p)}, p = \text{even}$	$\{x_1\}$	$\emptyset$

Table1.1. Commutation relations for the fragments

Monoid	Fragment	$\sigma : s(F) \to t(F)$
A, B	$F_i, 1 \leq i \leq n-1$	$\sigma(j) = j+1$
B	$F_{ii}, 2 \leq i \leq n$	$\sigma(j) = j+1$

Table1.2. Shift relations for the fragments

2.4 Complete Presentation of Some Artin Monoids

For the reduced complete presentation we are using the following notations for the relations in $\mathcal{MB}_{n+1}$ and for $\alpha(n-2,1)$ we will write α.

- $\mathcal{R}_{nk}^{[n+1]} = \{x_n x_k = x_k x_n\}$ $(k \leq n-2)$.
- $\mathcal{R}_{\alpha;n}^{[n+1]} = \{x_n x_{n-1}\alpha\, x_n = x_{n-1}x_n x_{n-1}\alpha : x_{n-1}\alpha \in A^{[n]}\}$($\alpha$ can be empty).
- $\mathcal{R}_{\alpha,\beta;n-1}^{[n+1]} = \{x_n x_{n-1}\alpha\beta(n-1)x_n x_{n-1} = x_{n-1}x_n x_{n-1}\alpha\, x_{n-1}\Sigma\beta(n-1) :$ $x_{n-1}\alpha\beta(n-1) \in A^{[n]}$ and $\mathcal{R}^{[n]}, \mathcal{R}_{\alpha;n}^{[n+1]} \nmid x_n x_{n-1}\alpha\beta(n-1)x_n\}$.
- $\mathcal{R}_{\alpha,\beta;j}^{[n+1]} = \{x_n x_{n-1}\alpha\beta(n-1,j)x_n \cdots x_j = x_{n-1}x_n x_{n-1}\alpha\, x_{n-1}\cdots x_j\Sigma\beta(n-1,j) :$ $x_{n-1}\alpha\beta(n-1,j) \in A^{[n]}$ and $\mathcal{R}^{[n]}, \mathcal{R}_{\alpha;n}^{[n+1]}, \ldots, \mathcal{R}_{\alpha,\beta;j+1}^{[n+1]} \nmid x_n x_{n-1}\alpha\beta(n-1,j)x_n \cdots x_{j+1}\}$,

$1 \le j \le n-2$.

- The relations $\mathcal{R}^{[n+1]}$ are given inductively by $\mathcal{R}^{[1]} = \emptyset$ and

$$\mathcal{R}^{[n+1]} = \mathcal{R}^{[n]} \coprod \left(\coprod_{k=1}^{n-2} \mathcal{R}_{nk}^{[n+1]} \right) \coprod \mathcal{R}_{\alpha;n}^{[n+1]} \coprod \mathcal{R}_{\alpha,\beta;n-1}^{[n+1]} \coprod \cdots \coprod \mathcal{R}_{\alpha,\beta;1}^{[n+1]}.$$

Now we explain the reduced complete presentation of $\mathcal{MB}_{n+1}$ as a corollary of Theorem 1.5.1.

Corollary 2.4.1. *[13] The braid monoid $\mathcal{MB}_{n+1}$ have a reduced complete presentation $\left\langle x_1, \ldots, x_n \,|\, \mathcal{R}^{[n+1]} \right\rangle$.*

Proof. (of Corollary 2.4.1 and also another proof of Theorem 1.5.1)

We use induction to prove that the above reduced presentation of $\mathcal{MB}_{n+1}$ is complete. In first step we describe how the relations $\mathcal{R}^{[n+1]}$ are obtained from the defining relations and ambiguities between them. In second step we show that all the new ambiguities are solvable. For simplicity we will write $\mathcal{R}_*$ instead of $\mathcal{R}_*^{[n+1]}$. For $n = 2$ we prove that the presentation $\mathcal{MB}_3 = \langle x_1, x_2 : \mathcal{R}_{\emptyset,2}, \mathcal{R}_{\emptyset,1^r;1} \rangle$ is complete, where $\mathcal{R}_{\emptyset,2} : x_2x_1x_2 = x_1x_2x_1$ and $\mathcal{R}_{\emptyset,1^r;1} : x_2x_1^rx_2x_1 = x_1x_2x_1^2x_2^{r-1}$, $r \ge 2$. Let $i \le j$, $\mathcal{R}_{\emptyset,1^i;1} : x_2\, x_1^i\, x_2x_1 = x_1x_2x_1^2x_2^{i-1}$ and $\mathcal{R}_{\emptyset,1^j;1} : x_2\, x_1^j\, x_2x_1 = x_1x_2x_1^2x_2^{j-1}$. Then we have the following ambiguities:

$$\mathcal{R}_{\emptyset,2}\mathcal{R}_{\emptyset,2},\ \mathcal{R}_{\emptyset,2}\mathcal{R}_{\emptyset,1^i;1},\ \mathcal{R}_{\emptyset,1^i;1}\mathcal{R}_{\emptyset,2},\ \mathcal{R}_{\emptyset,1^i;1}R_{\emptyset,1^i;1},\ \mathcal{R}_{\emptyset,1^i;1}\mathcal{R}_{\emptyset,1^j;1},\ \mathcal{R}_{\emptyset,1^j;1}\mathcal{R}_{\emptyset,1^i;1}.$$

(we are not mentioning the overlap in the ambiguities) First we show that the relations $\mathcal{R}_{\emptyset,1^r;1}$ are satisfied in $\mathcal{MB}_3$. In the ambiguity $\mathcal{R}_{\emptyset,2}\mathcal{R}_{\emptyset,2} : x_2x_1x_2x_1x_2$, $L(\mathcal{R}_{\emptyset,2}\mathcal{R}_{\emptyset,2}) = x_1x_2\, x_1^2x_2$, $R(\mathcal{R}_{\emptyset,2}\mathcal{R}_{\emptyset,2}) = x_2x_1^2x_2x_1$, i.e., $\mathcal{R}_{\emptyset,2}\mathcal{R}_{\emptyset,2}$ gives the relation $\mathcal{R}_{\emptyset,1^2;1}$. The ambiguity $\mathcal{R}_{\emptyset,1^2;1}\mathcal{R}_{\emptyset,2}$ gives $\mathcal{R}_{\emptyset,1^3;1}$ and in general $\mathcal{R}_{\emptyset,1^{r-1};1}\mathcal{R}_{\emptyset,2}$ gives $\mathcal{R}_{\emptyset,1^r;1}$ which are satisfied in $\mathcal{MB}_3$. Now we show that all other ambiguities are solvable. In the ambiguity $\mathcal{R}_{\emptyset,2}\mathcal{R}_{\emptyset,1^i;1} : x_2x_1x_2\, x_1^i\, x_2x_1$; $L(\mathcal{R}_{\emptyset,2}\mathcal{R}_{\emptyset,1^i;1}) = L(x_1x_2x_1^{i+1}x_2x_1)$ and

$R(\mathcal{R}_{\emptyset,2}\mathcal{R}_{\emptyset,1^i;1}) = R(x_2x_1^2x_2x_1^2x_2^{i-1}) = R(x_1x_2x_1^{i+1}x_2x_1)$. Therefore this ambiguity is solvable. Generally for any i and j, in the ambiguity $\mathcal{R}_{\emptyset,1^i;1}\mathcal{R}_{\emptyset,1^j;1} : x_2x_1^ix_2x_1^jx_2x_1$;

$$L(\mathcal{R}_{\emptyset,1^i;1}\mathcal{R}_{\emptyset,1^j;1}) = L(x_1x_2x_1^2x_2^{i-1}x_1^{j-1}x_2x_1)$$

and

$$\begin{aligned} R(\mathcal{R}_{\emptyset,1^i;1}\mathcal{R}_{\emptyset,1^j;1}) &= R(x_2x_1^{i+1}x_2x_1^2x_2^{j-1}) = R(x_1x_2x_1^2x_2^ix_1x_2^{j-1}) \\ &= R(x_1x_2x_1^2x_2^{i-1}x_1^{j-1}x_2x_1). \end{aligned}$$

Therefore all the ambiguities are solvable. Hence the above reduced presentation is complete. Now suppose the relations are true for any n. We prove them for $n+1$ in the following way.

Step 1. i) Using induction we show that the relations $R_{\alpha;n}$ are satisfied in $\mathcal{MB}_{n+1}$. The ambiguity $\mathcal{R}_{\emptyset;n}\mathcal{R}_{n(n-2)}$ gives the relations $\mathcal{R}_{x_{n-2};n}$, $\mathcal{R}_{x_{n-2};n}\mathcal{R}_{n(n-2)}$ gives $\mathcal{R}_{x_{n-2}^2;n}$ and so on $\mathcal{R}_{x_{n-2}^r;n}\mathcal{R}_{n(n-2)}$ gives $\mathcal{R}_{\alpha(n-2);n}$. The ambiguity $\mathcal{R}_{\alpha(n-2);n}\mathcal{R}_{n(n-3)}$ gives the relations $\mathcal{R}_{\alpha(n-2)x_{n-3};n}$. The ambiguity $\mathcal{R}_{\alpha(n-2)x_{n-3};n}\mathcal{R}_{n(n-3)}$ gives $\mathcal{R}_{\alpha(n-2)x_{n-3}^2;n}$ and so on $\mathcal{R}_{\alpha(n-2)x_{n-3}^s;n}\mathcal{R}_{n(n-3)}$ gives $\mathcal{R}_{\alpha(n-2,n-3);n}$. Continuing this process, the ambiguity $\mathcal{R}_{\alpha(n-2;2);n}\mathcal{R}_{n.1}$ gives $\mathcal{R}_{\alpha(n-2,2)x_1;n}$, $\mathcal{R}_{\alpha(n-2,2)x_1;n}\mathcal{R}_{n.1}$ gives $\mathcal{R}_{\alpha(n-2,2)x_1^2;n}$ and so on $\mathcal{R}_{\alpha(n-2,2)x_1^t;n}\mathcal{R}_{n.1}$ gives the relations $\mathcal{R}_{\alpha;n}$ which are satisfied in $\mathcal{MB}_{n+1}$.

ii) The ambiguity $\mathcal{R}_{\alpha,n}\mathcal{R}_{\emptyset;n}$ gives $\mathcal{R}_{\alpha,x_{n-1};n-1}$, $\mathcal{R}_{\alpha,x_{n-1};n-1}\mathcal{R}_{\emptyset;n}$ gives $\mathcal{R}_{\alpha,x_{n-1}^2;n-1}$ and so on $\mathcal{R}_{\alpha,x_{n-1}^r;n-1}\mathcal{R}_{\emptyset;n}$ gives the relations $\mathcal{R}_{\alpha,\beta(n-1);n-1}$ which are satisfied in $\mathcal{MB}_{n+1}$.

iii) Using induction again we show that the relations $\mathcal{R}_{\alpha,\beta;1}$ are satisfied in $\mathcal{MB}_{n+1}$. The ambiguity $\mathcal{R}_{\alpha,\beta(n-1);n-1}\mathcal{R}_{\emptyset;n-1}$ gives the relations $\mathcal{R}_{\alpha,\beta(n-1)x_{n-2};n-2}$, $\mathcal{R}_{\alpha,\beta(n-1)x_{n-2};n-1}\mathcal{R}_{\emptyset;n-1}$ gives $\mathcal{R}_{\alpha,\beta(n-1)x_{n-2}^2;n-2}$ and so on $\mathcal{R}_{\alpha,\beta(n-1)x_{n-2}^s;n-1}\mathcal{R}_{\emptyset;n-1}$ gives $\mathcal{R}_{\alpha,\beta(n-1,n-2);n-2}$. Continuing the above process, the ambiguity $\mathcal{R}_{\alpha,\beta(n-1,2);2}\mathcal{R}_{\emptyset;2}$ gives $\mathcal{R}_{\alpha,\beta(n-1,2)x_1;1}$, $\mathcal{R}_{\alpha,\beta(n-1,2)x_1;1}\mathcal{R}_{\emptyset;2}$ gives $\mathcal{R}_{\alpha,\beta(n-1,2)x_1^2;1}$ and so on $\mathcal{R}_{\alpha,\beta(n-1,2)x_1^t;1}\mathcal{R}_{\emptyset;2}$ gives the relations $\mathcal{R}_{\alpha,\beta(n-1,1);1}$ which are satisfied in $\mathcal{MB}_{n+1}$.

Step 2. Here we show that all other ambiguities are solvable. In the ambiguity $\mathcal{R}_{\alpha;n}\mathcal{R}_{\gamma;n} : x_n x_{n-1}\alpha x_n x_{n-1}\gamma(n-2,1)x_n$;

$$\begin{aligned} L\big(\mathcal{R}_{\alpha;n}\mathcal{R}_{\gamma;n}\big) &= L\big(x_{n-1}x_n x_{n-1}\alpha x_{n-1}\gamma(n-2,1)x_n\big), \\ R\big(\mathcal{R}_{\alpha;n}\mathcal{R}_{\gamma;n}\big) &= R\big(x_n x_{n-1}\alpha x_{n-1}x_n x_{n-1}\gamma(n-2,1)\big) \\ &= R\big(x_{n-1}x_n x_{n-1}\alpha x_{n-1}x_n\gamma(n-2,1)\big) \\ &= R\big(x_{n-1}x_n x_{n-1}\alpha x_{n-1}\gamma(n-2,1)x_n\big). \end{aligned}$$

Therefore this ambiguity is solvable. In the ambiguity

$\mathcal{R}_{\alpha;n}\mathcal{R}_{\gamma,\delta;j} : x_n x_{n-1}\alpha x_n x_{n-1}\gamma(n-2,1)\delta(n-1,j)x_n x_{n-1}\cdots x_j$;

$L\big(\mathcal{R}_{\alpha;n}\mathcal{R}_{\gamma,\delta;j}\big) = L\big(x_{n-1}x_n x_{n-1}\alpha x_{n-1}\gamma(n-2,1)\delta(n-1,j)x_n x_{n-1}\cdots x_j\big)$ and

$$\begin{aligned} R\big(\mathcal{R}_{\alpha;n}\mathcal{R}_{\gamma,\delta;j}\big) &= R\big(x_n x_{n-1}\alpha x_{n-1}x_n x_{n-1}\gamma(n-2,1)x_{n-1}\cdots x_j\Sigma\delta(n-1,j)\big) \\ &= R\big(x_{n-1}x_n x_{n-1}\alpha x_{n-1}x_n\gamma(n-2,1)x_{n-1}\cdots x_j\Sigma\delta(n-1,j)\big) \\ &= R\big(x_{n-1}x_n x_{n-1}\alpha x_{n-1}\gamma(n-2,1)x_n x_{n-1}\cdots x_j\Sigma\delta(n-1,j)\big) \\ &= R\big(x_{n-1}x_n x_{n-1}\,\alpha\, x_{n-1}\,\gamma(n-2,1)\,\delta(n-1,j)x_n x_{n-1}\cdots x_j\big). \end{aligned}$$

Therefore this ambiguity is also solvable. In general let the ambiguity

$\mathcal{R}_{\alpha,\beta;j}\mathcal{R}_{\gamma(k-2,1),\delta(k-1,i);i} : x_n x_{n-1}\alpha\beta(n-1,j)x_n\cdots x_{k+1}x_k x_{k-1}\cdots x_j\,\gamma(k-2,1)$ $\delta(k-1,i)x_k\cdots x_i$ overlaps at $x_k\cdots x_j$ and $i \le j \le k$. Then

$L\big(\mathcal{R}_{\alpha,\beta;j}\mathcal{R}_{\gamma,\delta;i}\big) = L\big(x_{n-1}x_n x_{n-1}\alpha\, x_{n-1}\cdots x_j\Sigma\beta(n-1,j)\gamma(k-2,1)\delta(k-1,i)x_k\cdots x_i\big)$

and

$R\big(\mathcal{R}_{\alpha,\beta;j}\mathcal{R}_{\gamma,\delta;i}\big)$

$$= R\big(x_n x_{n-1}\alpha\beta(n-1,j)x_n\cdots x_{k+1}x_{k-1}x_k\cdots x_j\gamma(k-2,1)x_{k-1}\cdots x_i\Sigma\delta(k-1,i)\big)$$

$$= R\big(x_n x_{n-1}\alpha\{\beta(n-1,j)x_{k-1}\}x_n\cdots x_j\gamma(k-2,1)x_{k-1}\cdots x_i\Sigma\delta(k-1,i)\big)$$

$$= R\big(x_{n-1}x_nx_{n-1}\alpha\, x_{n-1}\cdots x_j\Sigma\beta(n-1,j)x_k\gamma(k-2,1)x_{k-1}\cdots x_i\Sigma\delta(k-1,i)\big)$$
$$= R\big(x_{n-1}x_nx_{n-1}\alpha\, x_{n-1}\cdots x_j\Sigma\beta(n-1,j)\gamma(k-2,1)x_k\cdots x_i\Sigma\delta(k-1,i)\big)$$
$$= R\big(x_{n-1}x_nx_{n-1}\alpha\, x_{n-1}\cdots x_j\Sigma\beta(n-1,j)\gamma(k-2,1)\delta(k-1,i)x_k\cdots x_i\big).$$

Therefore this ambiguity is solvable too. Hence the reduced presentation of $\mathcal{MB}_{n+1}$ is complete. □

Next we give the complete presentations of the monoids $\mathcal{M}(B_n)$ and $\mathcal{M}\big(I_2(p)\big)$. We are using the following notations for the relations in $\mathcal{M}(B_n)$ and for $\alpha_*(n-2,1)$ we will write α_*.

- $\mathcal{R}^{[k]}$ = set of relations in $\mathcal{M}(B_k)$.
- $\mathcal{R}^{[n]}_{nk} = \big\{x_nx_k = x_kx_n\big\}$ $(k \le n-2)$.
- $\mathcal{R}^{[n]}_{n;i} : x_nx_{n-1}\alpha\beta(n-1,i)x_nx_{n-1}\cdots x_i = x_{n-1}x_nx_{n-1}\alpha x_{n-1}\cdots x_i\Sigma\beta(n-1,i)$.
- $\mathcal{R}^{[n]}_{n;ii} : x_nx_{n-1}\alpha_1\beta_1(n-1,2)\alpha_2(i-1,1)\beta_2(n-1,i+1)x_n\cdots x_1x_2\cdots x_i =$
$x_{n-1}x_nx_{n-1}\alpha_1x_{n-1}\cdots x_1\Sigma\beta_1(n-1,2)x_2\cdots x_i\alpha_2(i-1,1)\Sigma\beta_2(n-1,i+1)$.
- The relations $\mathcal{R}^{[n]}$ are given inductively by $\mathcal{R}^{[1]} = \emptyset$ and

$$\mathcal{R}^{[n]} = \mathcal{R}^{[n-1]} \coprod \left(\coprod_{k=1}^{n-2} \mathcal{R}^{[n]}_{nk}\right) \coprod \mathcal{R}^{[n]}_{n;i} \coprod \mathcal{R}^{[n]}_{n;ii}.$$

Theorem 2.4.2. *The monoid $\mathcal{M}(B_n)$ have a complete presentation*

$$\big\langle x_1, \ldots, x_n \,|\, \mathcal{R}^{[n]} \big\rangle\,.$$

Proof. We will check here few ambiguities only. For example in the ambiguity $\mathcal{R}^{[n]}_{n;ii}\mathcal{R}^{[k]}_{k;jj} : x_nx_{n-1}\alpha_1\beta_1(n-1,2)\alpha_2(i-1,1)\beta_2(n-1,i+1)x_n\cdots x_{k+1}x_k\cdots x_i\cdots x_1\cdots x_i$ $\alpha_3(k-2,1)\beta_3(k-1,2)\alpha_4(j-1,1)\beta_4(k-1,j+1)x_k\cdots x_1\cdots x_j$;

$L\big(\mathcal{R}^{[n]}_{n;ii}\mathcal{R}^{[k]}_{k;jj}\big) = L\big(x_{n-1}x_nx_{n-1}\alpha_1x_{n-1}\cdots x_1\Sigma\beta_1(n-1,2)x_2\cdots x_i\alpha_2(i-1,1)\Sigma\beta_2(n-1,i+1)$
$\alpha_3(k-2,1)\beta_3(k-1,2)\alpha_4(j-1,1)\beta_4(k-1,j+1)x_k\cdots x_1\cdots x_j\big)$,

$R\big(\mathcal{R}^{[n]}_{n;ii}\mathcal{R}^{[k]}_{k;jj}\big) = R\big(x_nx_{n-1}\alpha_1\beta_1(n-1,2)\alpha_2(i-1,1)\beta_2(n-1,i+1)x_n\cdots x_{k+1}x_{k-1}x_kx_{k-1}$

$x_{k-2}\cdots x_1\cdots x_i\alpha_3(k-2,1)x_{k-1}\cdots x_1\Sigma\beta_3(k-1,2)x_2\cdots x_j\alpha_4(j-1,1)\Sigma\beta_4(k-1,j+1)\big)$

$= R\big(x_nx_{n-1}\alpha_1\beta_1(n-1,2)\alpha_2(i-1,1)\{\beta_2(n-1,i+1)x_{k-1}\}x_n\cdots x_1\cdots x_i\alpha_3(k-2,1)$

$x_{k-1}\cdots x_1\Sigma\beta_3(k-1,2)x_2\cdots x_j\alpha_4(j-1,1)\Sigma\beta_4(k-1,j+1)\big)$

$= R\big(x_{n-1}x_nx_{n-1}\alpha_1x_{n-1}\cdots x_1\Sigma\beta_1(n-1,2)x_2\cdots x_i\alpha_2(i-1,1)\Sigma\beta_2(n-1,i+1)x_k\alpha_3(k-2,1)$

$x_{k-1}\cdots x_1\Sigma\beta_3(k-1,2)x_2\cdots x_j\alpha_4(j-1,1)\Sigma\beta_4(k-1,j+1)\big)$

$= R\big(x_{n-1}x_nx_{n-1}\alpha_1x_{n-1}\cdots x_1\Sigma\beta_1(n-1,2)x_2\cdots x_i\alpha_2(i-1,1)\Sigma\beta_2(n-1,i+1)\alpha_3(k-2,1)$

$x_k\cdots x_1\Sigma\beta_3(k-1,2)x_2\cdots x_j\alpha_4(j-1,1)\Sigma\beta_4(k-1,j+1)\big)$

$= R\big(x_{n-1}x_nx_{n-1}\alpha_1x_{n-1}\cdots x_1\Sigma\beta_1(n-1,2)x_2\cdots x_i\alpha_2(i-1,1)\Sigma\beta_2(n-1,i+1)\alpha_3(k-2,1)$

$\beta_3(k-1,2)x_k\cdots x_1x_2\cdots x_j\alpha_4(j-1,1)\Sigma\beta_4(k-1,j+1)\big)$

$= R\big(x_{n-1}x_nx_{n-1}\alpha_1x_{n-1}\cdots x_1\Sigma\beta_1(n-1,2)x_2\cdots x_i\alpha_2(i-1,1)\Sigma\beta_2(n-1,i+1)\alpha_3(k-2,1)$

$\beta_3(k-1,2)\alpha_4(j-1,1)\beta_4(k-1,j+1)x_k\cdots x_1\cdots x_j\big).$

Therefore this ambiguity is solvable. Also in the ambiguity

$\mathcal{R}^{[n]}_{n;kk}\mathcal{R}^{[k]}_{k;ii} : x_nx_{n-1}\alpha_1\beta_1(n-1,2)\alpha_2(k-1,1)\beta_2(n-1,k+1)x_n\cdots x_1\cdots x_{k-1}x_kx_{k-1}$

$\alpha_3(k-2,1)\beta_3(k-1,2)\alpha_4(i-1,1)\beta_4(k-1,i+1)x_k\cdots x_1\cdots x_i;$

$L\big(\mathcal{R}^{[n]}_{n;kk}\mathcal{R}^{[k]}_{k;ii}\big) = L\big(x_{n-1}x_nx_{n-1}\alpha_1x_{n-1}\cdots x_1\Sigma\beta_1(n-1,2)x_2\cdots x_k\alpha_2(k-1,1)$

$\Sigma\beta_2(n-1,k+1)x_{k-1}\alpha_3(k-2,1)\beta_3(k-1,2)\alpha_4(i-1,1)\beta_4(k-1,i+1)x_k\cdots x_1\cdots x_i\big)$

$= L\big(x_{n-1}x_nx_{n-1}\alpha_1x_{n-1}\cdots x_1\Sigma\beta_1(n-1,2)x_2\cdots x_k\alpha_2(k-1,1)x_{k-1}\Sigma\beta_2(n-1,k+1)$

$\alpha_3(k-2,1)\beta_3(k-1,2)\alpha_4(i-1,1)\beta_4(k-1,i+1)x_k\cdots x_1\cdots x_i\big),$

$R\big(\mathcal{R}^{[n]}_{n;kk}\mathcal{R}^{[k]}_{k;ii}\big) = R\big(x_nx_{n-1}\alpha_1\beta_1(n-1,2)\alpha_2(k-1,1)\beta_2(n-1,k+1)x_n\cdots x_k\cdots x_1\cdots$

$x^2_{k-1}x_kx_{k-1}\alpha_3(k-2,1)x_{k-1}\cdots x_1\Sigma\beta_3(k-1,2)x_2\cdots x_i\alpha_4(i-1,1)\Sigma\beta_4(k-1,i+1)\big)$

$= R\big(x_nx_{n-1}\alpha_1\beta_1(n-1,2)\alpha_2(k-1,1)\beta_2(n-1,k+1)x_n\cdots x_1\cdots x_{k+1}x_{k-1}x_kx_{k-1}x_{k-2}\cdots$

$x_1\cdots x_{k-1}x^2_k\alpha_3(k-2,1)x_{k-1}\cdots x_1\Sigma\beta_3(k-1,2)x_2\cdots x_i\alpha_4(i-1,1)\Sigma\beta_4(k-1,i+1)\big)$

$= R\big(x_nx_{n-1}\alpha_1\beta_1(n-1,2)\{\alpha_2(k-1,1)x_{k-1}\}\beta_2(n-1,k+1)x_n\cdots x_1\cdots x_k\alpha_3(k-2,1)$

$x_k\cdots x_1\Sigma\beta_3(k-1,2)x_2\cdots x_i\alpha_4(i-1,1)\Sigma\beta_4(k-1,i+1)\big)$

$= R\big(x_{n-1}x_nx_{n-1}\alpha_1x_{n-1}\cdots x_1\Sigma\beta_1(n-1,2)x_2\cdots x_k\alpha_2(k-1,1)x_{k-1}\Sigma\beta_2(n-1,k+1)$

$\alpha_3(k-2,1)\beta_3(k-1,2)\cdots x_1\cdots x_i\alpha_4(i-1,1)\Sigma\beta_4(k-1,i+1)x_k\big)$

$= R\big(x_{n-1}x_nx_{n-1}\alpha_1x_{n-1}\cdots x_1\Sigma\beta_1(n-1,2)x_2\cdots x_k\alpha_2(k-1,1)x_{k-1}\Sigma\beta_2(n-1,k+1)$

$\alpha_3(k-2,1)\beta_3(k-1,2)\alpha_4(i-1,1)\beta_4(k-1,i+1)x_k\cdots x_1\cdots x_i\big).$

Therefore this ambiguity is solvable too. Hence the above presentation is complete.

□

Theorem 2.4.3. *The complete presentations of the monoid* $\mathcal{M}\big(I_2(p)\big)$ *are*

1) $\mathcal{M}\big(I_2(2k+1)\big) = \big\langle x_1, x_2 \mid \mathcal{P}_{2k+1}, x_2x_1^r\Delta = \Delta x_1x_2^r, r \geq 1\big\rangle$ *and*

2) $\mathcal{M}\big(I_2(2k)\big) = \big\langle x_1, x_2 \mid \mathcal{P}_{2k}, x_2x_1^r\Delta = \Delta x_2x_1^r, r \geq 1\big\rangle$, *where*

$\mathcal{P}_l : x_2x_1x_2x_1\cdots$ *(l factors)* $= x_1x_2x_1x_2\cdots$ *(l factors).*

Proof. 1) Let

$$\mathcal{R}(r) : x_2x_1^r\underbrace{x_2x_1x_2\cdots x_2x_1}_{2k\,\text{factors}} = \underbrace{x_1x_2x_1\cdots x_2}_{2k\,\text{factors}}x_1^2x_2^{r-1}, r \geq 2$$

and

$$\mathcal{R}(s) : x_2x_1^s\underbrace{x_2x_1x_2\cdots x_2x_1}_{2k\,\text{factors}} = \underbrace{x_1x_2x_1\cdots x_2}_{2k\,\text{factors}}x_1^2x_2^{s-1}, s \geq 2$$

be the relations in $\mathcal{M}\big(I_2(2k+1)\big)$. We will check the ambiguity $\mathcal{R}(r)\mathcal{R}(s)$ only. Other cases are similar. In the ambiguity

$$\mathcal{R}(r)\mathcal{R}(s) : x_2x_1^r\underbrace{x_2x_1x_2\cdots x_2x_1}_{2k\,\text{factors}}x_1^{s-1}\underbrace{x_2x_1x_2\cdots x_2x_1}_{2k\,\text{factors}};$$

$$\begin{aligned} L\big(\mathcal{R}(r)\mathcal{R}(s)\big) &= L\big(x_2x_1^{r-1}\Delta x_1^{s-2}\Delta\big) \\ &= L\big(\Delta x_1x_2^{r-1}x_1^{s-2}\Delta\big) \\ &= L\big(\Delta x_1x_2^{r-2}\Delta x_1x_1^{s-2}\big) \\ &= L\big(\Delta x_1\Delta x_1^{r-1}x_2^{s-2}\big), \end{aligned}$$

$$\begin{aligned}
R\big(\mathcal{R}(r)\mathcal{R}(s)\big) &= R\big(x_2x_1^r \underbrace{x_2x_1x_2\cdots x_2x_1}_{2k-2\,\text{factors}} x_2x_1^{s-1}\Delta\big) \\
&= R\big(x_2x_1^r \underbrace{x_2x_1x_2\cdots x_2x_1}_{2k-2\,\text{factors}} \Delta x_1x_2^{s-1}\big) \\
&= R\big(x_2x_1^r \underbrace{x_2x_1x_2\cdots x_2x_1}_{2k-4\,\text{factors}} \Delta x_1x_2x_1x_2^{s-1}\big) \\
&\qquad\vdots \\
&= R\big(x_2x_1^r\Delta \underbrace{x_1x_2x_1\cdots x_2x_1}_{2k-1\,\text{factors}} x_2^{s-1}\big) \\
&= R\big(\Delta x_1x_2^r\Delta' x_2^{s-2}\big) \quad \Big(\Delta' = \underbrace{x_1x_2\cdots x_2}_{2k\,\text{factors}} \text{ and } x_2^r\Delta' = \Delta' x_1^r\Big) \\
&= R\big(\Delta x_1\Delta' x_1^r x_2^{s-2}\big) \\
&= R\big(\Delta x_1\Delta x_1^{r-1}x_2^{s-2}\big).
\end{aligned}$$

Therefore this ambiguity is solvable. Hence the presentation 1) is complete. Similarly we can prove that the presentation of $\mathcal{M}\big(I_2(2k)\big)$ is complete. $\square$

Chapter 3

Conjugacy classes of 3-braid group

3.1 Introduction

As described in chapter 1 for the general case, the *summit set* of a conjugacy class C of $\mathcal{B}_3$ is defined as

$$SS(C) = \{\Delta_3^r W \in C \,|\, r = \exp(C)\,\}\,.$$

and this is a finite set. The set of elements $W \in \mathcal{MB}_3^+$ such that $\Delta_3^r W \in SS(C)$ is called the *base-summit set* of the class C. In this way, Garside's [18] solution of the conjugacy problem is to compute $\exp(C)$ and the base-summit set: two elements in $\mathcal{B}_3$ are conjugate if and only if their conjugacy classes have the same exponents and the same base-summit sets. It is easy to see that all the (positive) elements in a base-summit set have the same length and for two exponents which are congruent mod 2, the corresponding base summit sets coincide or are disjoint. So we will treat separately the two types of base summit sets: *E-summit set* corresponding to even exponents and *O-summit sets* corresponding to odd exponents.

K. Murasugi [21] gave seven different classes of $\mathcal{B}_3$ (not in Garside normal form) and showed that an arbitrary word is conjugate to an unique element of these seven classes. Using *band presentation* of $\mathcal{B}_3$, P. J. Xu [25] described explicitly the normal and summit forms of words in $\mathcal{B}_3$ and found a unique representative in the summit set of words (see §3).

In this chapter we describe explicitly the words in classical generators which are:
(i) in the Garside normal form;
(ii) *summit words* (elements of summit set);
(iii) *super summit words* (elements of super summit set);
(iv) *smallest summit words* (smallest elements in a given summit set). The results of Th 3.1.1 and Th 3.1.2 seem to be well known by the experts, but I could not find these statements in the literature.

Garside normal form of elements in $\mathcal{B}_3$ are given by the following result:

Theorem 3.1.1. *For* $s_i > 0$ *and* $i_j \neq i_{j+1}$, $\Delta_3^r x_{i_1}^{s_1} x_{i_2}^{s_2} \cdots x_{i_h}^{s_h}$ *is in the normal form if and only if :*
(i) $h \leq 2$, *either*
(ii) $h \geq 3$ *and all the exponents are* ≥ 2, *with the possible exceptions of* s_1 *or* s_h.

The next result describes the elements of $\mathcal{B}_3$ in summit sets:

Theorem 3.1.2. *A word* $\Delta_3^r W = \Delta_3^r x_{i_1}^{s_1} x_{i_2}^{s_2} \cdots x_{i_h}^{s_h}$ *in normal form is summit word if and only if:*
(0) $\Delta_3^r W$ *is the word:* Δ_3^{even} *or* $\Delta_3^{odd} x_i$ *or* $\Delta_3^{even} x_{i_1} x_{i_2}$, *or*
(i) $h + 1 \equiv r (\mod 2)$, *or*
(ii) $s_j \geq 2$, *for all* $1 \leq j \leq h$.

The following theorem describes the elements of $\mathcal{B}_3$ in super summit sets:

Theorem 3.1.3. *A summit word* $\Delta_3^r W = \Delta_3^r x_{i_1}^{s_1} x_{i_2}^{s_2} \cdots x_{i_h}^{s_h}$ *is super summit word if and only if:*

(0) $\Delta_3^r W$ *is the word:* Δ_3^{even} *or* $\Delta_3^{odd} x_i$ *or* $\Delta_3^{even} x_{i_1} x_{i_2}$*, or*

(i) $h + 1 \equiv r (\mod 2)$.

The smallest elements of $\mathcal{B}_3$ in summit sets are described by the next theorem:

Theorem 3.1.4. *A summit word* $\Delta_3^r W = \Delta_3^r x_{i_1}^{s_1} x_{i_2}^{s_2} \cdots x_{i_h}^{s_h}$ *is the smallest in its summit set if and only if:*

(0) $\Delta_3^r W$ *is the word:* Δ_3^{odd} *or* $\Delta_3^{even} x_1^{s_1}$ $(s_1 \geq 0)$ *either*

$\Delta_3^r W$ *satisfies the following conditions:*

(a) $x_{i_1} = x_1$ *and*

(b) $h \equiv r (\mod 2)$ *and*

(c) $(s_1, \ldots, s_h)$ *satisfies* max-min condition.

(See §2 for max-min condition). We also give in §2 an algorithm to compute this smallest element.

As an application in knot theory, in §3 we find the unique representative in the conjugacy classes according to Birman-Menasco [8, 7] classification of links with braid index ≤ 3 and invertibility of 3-closed braid.

Next we compute the number C_n of base-summit sets containing elements W of length n; we denote the generating functions by $H^*(t) = \sum C_n t^n$, where $*$ has only two values, E or O. In the next formulas μ is the classical Möbius function:

Theorem 3.1.5. *(a) The Hilbert series of even base-summit sets is given by*

$$H^E(t) = 1 + t + 2t^2 + \sum_{n \geq 3} \left[1 + \sum_{k=1}^{[\frac{n}{4}]} \frac{1}{2k} \sum_{d|a} d \sum_{\delta|d} \mu(\frac{d}{\delta}) \binom{\delta(c-b)-1}{\delta b - 1} \right] t^n$$

where $a = gcd(n, 2k)$, $n = ac$ and $2k = ab$.

(b) The Hilbert series of odd base-summit sets is given by

$$H^O(t) = \sum_{n=0}^{5} t^n + \sum_{n\geq 6} \Big[1 + \sum_{k=1}^{[\frac{n-2}{4}]} \frac{1}{2k+1} \sum_{d|a} d \sum_{\delta|d} \mu(\frac{d}{\delta}) \binom{\delta(c-b)-1}{\delta b - 1}\Big] t^n$$

where $a = gcd(n, 2k+1)$, $n = ac$ and $2k+1 = ab$.

Remark 1: Given a, b, c positive integers such that $(b, c) = 1$, and ab =even, we can reconstruct n and $2k$.

3.2 Normal form and summit set

The unique smallest word in the summit set of a given word V in $\mathcal{B}_3$ can be described completely. A word in normal form is called *summit word* if it belongs to its summit set of its conjugacy class and it is called *super summit word* if it belongs to its super summit set.

Definition 3.2.1. A summit word $\Delta_3^r W$ is called the smallest summit word if W is the smallest (in length-lexicographic order) in the its base-summit set.

Proof of the Theorem 3.1.1: Let $h \geq 3$ and $s_j \geq 2$ for $1 < j < h$ or $h \leq 2$, then $W = x_{i_1}^{s_1} x_{i_2}^{s_2} \cdots x_{i_h}^{s_h}$ does not contain $x_1x_2x_1$ or $x_2x_1x_2$, so W is unique in its diagram and $\Delta_3^r x_{i_1}^{s_1} x_{i_2}^{s_2} \cdots x_{i_h}^{s_h}$ is the normal form. Conversely, let $\Delta_3^r x_{i_1}^{s_1} x_{i_2}^{s_2} \cdots x_{i_h}^{s_h}$ is the normal form. If $h \geq 3$ and there is a j satisfying $1 < j < h$ and $s_j = 1$, then $x_{i_1}^{s_1} x_{i_2}^{s_2} \cdots x_{i_h}^{s_h}$ contains $x_1x_2x_1$ or $x_2x_1x_2$, so the word W is divisible by Δ_3 and we have a contradiction. □

Remark 3: As a consequence of the proof the set of words in $\mathcal{MB}_3$ primes to Δ_3, i.e, $\mathcal{MB}_3^+$ is a subset of k-vector basis of the algebra $k\langle\mathcal{MB}_3\rangle$ for a field k. But this is not true for braid monoid $\mathcal{MB}_n$, $n \geq 4$.

In order to find the conjugacy class (and then the summit set) of the word $\Delta_3^r W$, Garside [18] proved that the conjugacy relation is generated by conjugations with the divisors of Δ_3: $Div = \{1, x_1, x_2, x_1x_2, x_2x_1, \Delta_3\}$.

Definition 3.2.2. A word V in normal form is called *special* if it is one of the form: Δ_3^{odd} or $\Delta_3^{odd}x_i$ or $\Delta_3^{even}x_{i_1}x_{i_2}$ or $\Delta_3^{even}x_1^{s_1}$ $(s_1 \geq 0)$. Otherwise V in normal form is a *general* word.

Lemma 3.2.1. ***(Computation)***

(a) Let $\Delta_3^{2m}W = \Delta_3^{2m}x_{i_1}^{s_1}x_{i_2}^{s_2}\cdots x_{i_h}^{s_h}$ *is normal form of a general word with* $s_j \geq 2$ *and* $i_1 \neq i_h$*, then, for any* A *such that* $A^{\pm 1} \in Div$ *the conjugate* $A\Delta_3^{2m}WA^{-1}$ *has exponent* $< 2m$ *or belongs to the set:*

$$\Delta_3^{2m}CSSS^E \coprod \Delta_3^{2m}BSSS^E,$$

where

$$CSSS^E = \{x_{i_k}^{s_k}\cdots x_{i_h}^{s_h}x_{i_1}^{s_1}\cdots x_{i_{k-1}}^{s_{k-1}}, \widehat{x}_{i_k}^{s_k}\cdots\widehat{x}_{i_h}^{s_h}\widehat{x}_{i_1}^{s_1}\cdots\widehat{x}_{i_{k-1}}^{s_{k-1}}\}_{k=\overline{1,h}}$$

and

$$BSSS^E = \{x_{i_k}^{s_k-j}x_{i_{k+1}}^{s_{k+1}}\cdots x_{i_{k-1}}^{s_{k-1}}x_{i_k}^{j}, \widehat{x}_{i_k}^{s_k-j}\widehat{x}_{i_{k+1}}^{s_{k+1}}\cdots\widehat{x}_{i_{k-1}}^{s_{k-1}}\widehat{x}_{i_k}^{j}\}_{k=\overline{1,h},j=\overline{1,s_k-1}}$$

or

$$BSSS^E = \{W \in \text{E-summit set} | \text{ W has minimal canonical-length}\}$$

(b) Let $\Delta_3^{2m+1}W = \Delta_3^{2m+1}x_{i_1}^{s_1}x_{i_2}^{s_2}\cdots x_{i_h}^{s_h}$ *is normal form of a general word with* $s_j \geq 2$ *and* $i_1 = i_h$*, then, for any* A *such that* $A^{\pm 1} \in Div$ *the conjugate* $A\Delta_3^{2m+1}WA^{-1}$ *has*

exponent $< 2m+1$ *or belongs to the set:*

$$\Delta_3^{2m+1} CSSS^O \coprod \Delta_3^{2m+1} BSSS^O,$$

where

$$CSSS^O = \{x_{i_k}^{s_k} \cdots x_{i_h}^{s_h} \widehat{x}_{i_1}^{s_1} \cdots \widehat{x}_{i_{k-1}}^{s_{k-1}}, \widehat{x}_{i_k}^{s_k} \cdots \widehat{x}_{i_h}^{s_h} x_{i_1}^{s_1} \cdots x_{i_{k-1}}^{s_{k-1}}\}_{k=\overline{1,h}}$$

and

$$BSSS^O = \{x_{i_k}^{s_k-j} x_{i_{k+1}}^{s_{k+1}} \cdots x_{i_{k-1}}^{s_{k-1}} \widehat{x}_{i_k}^{j}, \widehat{x}_{i_k}^{s_k-j} \widehat{x}_{i_{k+1}}^{s_{k+1}} \cdots \widehat{x}_{i_{k-1}}^{s_{k-1}} x_{i_k}^{j}\}_{k=\overline{1,h}, j=\overline{1,s_k-1}}$$

or

$$BSSS^O = \{W \in \text{O-summit set} |\, \text{W has minimal canonical-length}\}$$

Proof. (a) This is just a mater of computation. One has to compute and verify $A\Delta_3^{2m}WA^{-1}$ for all $A^{\pm 1} \in Div$. For example we verify $A\Delta_3^{2m}WA^{-1}$ for $A = x_1$: There are two cases (i) $x_{i_h} = x_1$; and (ii) $x_{i_h} = x_2$.

For (i) we have

$$x_1 \Delta_3^{2m} W x_1^{-1} = \Delta_3^{2m} x_1 x_2^{s_1} x_1^{s_2} \cdots x_1^{s_h - 1}.$$

For (ii) we have

$$x_1\Delta_3^{2m}Wx_1^{-1} = \Delta_3^{2m}x_1^{s_1+1}x_2^{s_2}\cdots x_2^{s_h}\Delta_3^{-1}x_1x_2 = \Delta_3^{2m-1}x_2^{s_1+1}x_1^{s_2}\cdots x_1^{s_h+1}x_2,$$

the exponent $< 2m$. Similarly it is true for all other $A^{\pm 1} \in Div$.

(b) We also verify $A\Delta_3^{2m+1}WA^{-1}$ only for $A = x_1$: There are again two cases (i) $x_{i_h} = x_1$; and (ii) $x_{i_h} = x_2$.

For (i) we have

$$x_1\Delta_3^{2m+1}Wx_1^{-1} = \Delta_3^{2m+1}\widehat{x}_1 x_1^{s_1} x_2^{s_2} \cdots x_1^{s_h-1} = \Delta_3^{2m+1} x_2 x_1^{s_1} x_2^{s_2} \cdots x_1^{s_h-1}.$$

And (ii) give us

$$x_1\Delta_3^{2m+1}Wx_1^{-1}{=}\Delta_3^{2m+1}\widehat{x}_1x_2^{s_1}x_1^{s_2}\cdots x_2^{s_h}\Delta_3^{-1}x_1x_2 = \Delta_3^{2m}x_1^{s_1+1}x_2^{s_2}\cdots x_1^{s_h+1}x_2,$$

the exponent $< 2m+1$. □

For example the sets $CSSS^E$ and $BSSS^E$ for $V = \Delta_3^4x_2^4x_1^2$ are given as below:
$CSSS^E = \{x_2^4x_1^2, x_1^2x_2^4, x_1^4x_2^2, x_2^2x_1^4\}$;
$BSSS^E = \{x_2^3x_1^2x_2, x_2^2x_1^2x_2^2, x_2x_1^2x_2^3, x_1x_2^4x_1, x_1^3x_2^2x_1, x_1^2x_2^2x_1^2, x_1x_2^2x_1^3, x_2x_1^4x_2\}$. The following Corollary is a consequence of the Lemma 3.2.1.

Corollary 3.2.2. *Let $\Delta_3^rW = \Delta_3^rx_{i_1}^{s_1}x_{i_2}^{s_2}\cdots x_{i_h}^{s_h}$ be normal form of a general word; then W belongs to a base-summit set if one of the following conditions is satisfied:*
(i) $h+1 \equiv r(\mod 2)$ or
(ii) $s_j \geq 2$, for all $1 \leq j \leq h$.

Proof of the Theorem 3.1.2: Let $\Delta_3^rW = \Delta_3^rx_{i_1}^{s_1}x_{i_2}^{s_2}\cdots x_{i_h}^{s_h}$ in $\mathcal{B}_3$ be a summit word. Suppose that $h \equiv r(\mod 2)$ and $s_1 = 1$ then $x_{i_h}\Delta_3^rWx_{i_h}^{-1} = \Delta_3^{r+1}W_1$, but W belongs to a base-summit set so we obtain contradiction. The converse is true by Corollary 3.2.2. It is also easy to check that Δ_3^{even}, $\Delta_3^{odd}x_i$ and $\Delta_3^{even}x_{i_1}x_{i_2}$ are summit words. □

Definition 3.2.3. For a positive $W = x_{i_1}^{s_1}x_{i_2}^{s_2}\cdots x_{i_h}^{s_h}$ (all $s_i \geq 1$), h is called the syllable length of W denoted by $l_s(W)$.

Lemma 3.2.3. *Let $W = x_{i_1}^{s_1}x_{i_2}^{s_2}\cdots x_{i_h}^{s_h}$ belongs to $CSSS^*$ then the syllable length and canonical length are given by the table:*

	$CSSS^*$	$BSSS^*$
$l_s(W)$	h	$h+1$
$l(W)$	L	$L-1$

where $L = \sum s_j - (h-1)$ *and* $* \in \{E, O\}$.

Proof. The description of $BSSS^*$ in Lemma 3.2.1 implies $l_s(W) = h+1$. W is written as a product of divisors of Δ_3 as below:

$$\underbrace{(x_{i_1})(x_{i_1})\cdots(x_{i_1})}_{s_1-1\ times}(x_{i_1}x_{i_2})\underbrace{(x_{i_2})(x_{i_2})\cdots(x_{i_2})}_{s_2-2\ times}(x_{i_2}x_{i_3})\cdots\underbrace{(x_{i_h})(x_{i_h})\cdots(x_{i_h})}_{s_h-1\ times}.$$

Therefore $l(W)$ of $CSSS^* = \sum s_h - (h-1)$ and obviously $l(W)$ of $BSSS^* = \sum s_h - (h-2)$ ($BSSS^*$ has one more divisors of length 2 than $CSSS^*$). □

Proof of the Theorem3.1.3: By Lemma 3.2.3 the super summit words of a general word are precisely the words of $BSSS^*$ and hence they must satisfy (i) of Th 3.1.2. It is also easy that Δ_3^{even}, $\Delta_3^{odd}x_i$ and $\Delta_3^{even}x_{i_1}x_{i_2}$ are super summit words. □

Super summit set and ultra summit set are the same in $\mathcal{B}_3$ [19]. Therefore the Theorem 3.1.3 is also valid for ultra summit words.

The following Corollaries are consequences of the above Lemma 3.2.3.

Corollary 3.2.4. *The following are true for a general summit word* $\Delta_3^r W$*:*

(a) If $\Delta_3^r W_1$ *is in summit set of* $\Delta_3^r W$ *then* $| l_s(W_1) - l_s(W) | \leq 1$*;*

(b) The summit set of $\Delta_3^r W$ *has at least one element* $\Delta_3^r W_2$ *such that* $l_s(W_2) \equiv r($ mod 2)*;*

(c) The summit set of $\Delta_3^r W$ *has at least one element* $\Delta_3^r W_3$ *such that* $l_s(W_3) \equiv r+1($ mod 2)*.*

Corollary 3.2.5. *If $\Delta_3^r W_1$ and $\Delta_3^r W_2$ are general words from the same summit set then $l_s(W_1) > l_s(W_2)$ if and only if $l(W_1) < l(W_2)$.*

Remark 4: If $SSS(C)$ of a word in $\mathcal{B}_3$ is a proper subset of its $SS(C)$ then the smallest summit word lies in the complement of $SSS(C)$.

Remark 5: The cardinality of $SSS(C) \geq$ the cardinality of its complement. For example if $\Delta_3^{2m} W = \Delta_3^{2m} x_{i_1}^{s_1} x_{i_2}^{s_2} \cdots x_{i_h}^{s_h}$ for $h = even$ is a general summit word such that the set of s_i is nonperiodical then the cardinality of $SSS(C)$ is precisely $2\sum_{i=1}^{h}(s_i - 1)$ which is much greater than the cardinality $2\sum_{i=1}^{h} 1 = 2h$ of its complement.

The smallest summit word in the summit set of a general summit word $\Delta_3^r W = \Delta_3^r x_{i_1}^{t_1} x_{i_2}^{t_2} \cdots x_{i_l}^{t_l}$ is found in the following way:

Algorithm 3.2.6. *By Corrollary 3.2.4 $\Delta_3^r W$ is conjugate to $\Delta_3^r x_{i_1}^{s_1} x_{i_2}^{s_2} \cdots x_{i_h}^{s_h}$ such that $h \equiv r (\mod 2)$.*

step(1) *Find $s_k = \max\{s_j\}_{j=\overline{1,h}}$. If s_k is unique, then GO TO step 2. Otherwise find s_k such that $s_{k+1} < s_{l+1}$ for all $s_l = \max\{s_j\}$ and if s_{k+1} is unique, GO TO step 2. If this is not the case, then find s_{k+1} minimal with s_k maximal such that $s_{k+2} > s_{l+2}$ for all $s_l = \max\{s_j\}$ and if s_{k+2} is unique, GO TO step 2. Otherwise repeat the process; if the sequence of exponents is periodical, apply the above algorithm for a single period. Since $\{s_j\}$ is finite the process is also finite.*

step(2) *If r is even then $\Delta_3^r x_1^{s_k} x_2^{s_{k+1}} \cdots x_{i_h}^{s_h} x_{i_1}^{s_1} \cdots x_2^{s_{k-1}}$ is the smallest, if r is odd $\Delta_3^r x_1^{s_k} x_2^{s_{k+1}} \cdots x_{i_h}^{s_h} x_{i_1}^{s_1} \cdots x_1^{s_{k-1}}$ is the smallest.*

Definition 3.2.4. The words obtained as out-puts of the previous algorithm are said to satisfy *max-min condition.*

Proof of the Theorem3.1.4: The conditions (a), (b) and (c) of the theorem are obvious consequences of the description of $CSSS^*$ and $BSSS^*$ for $* \in \{E, O\}$. It is also easy to see that the smallest summit word in the summit set of Δ_3^{odd} and $\Delta_3^{even} x_i^{s_1}$ $(s_1 \geq 1)$ is Δ_3^{odd} and $\Delta_3^{even} x_1^{s_1}$ respectively. $\square$

The word obtained by algorithm 3.2.6 satisfied conditions of Theorem 3.1.4 and compute the smallest summit word of a given summit word. For example the summit words $V = \Delta_3^{2m} x_1^2 x_2^4 x_1^3 x_2^5 x_1^2 x_2^4 x_1^5 x_2^3 x_1$ and $W = \Delta_3^{2m} x_2^2 x_1^5 x_2^3 x_1^2 x_2^5 x_1^3$. By Corrolary 3.2.4, $V \sim \Delta_3^{2m} x_1^3 x_2^4 x_1^3 x_2^5 x_1^2 x_2^4 x_1^5 x_2^3$ and the sequence of exponents is nonperiodical so the smallest word in its summit set is $\Delta_3^{2m} x_1^5 x_2^2 x_1^4 x_2^5 x_1^3 x_2^3 x_1^4 x_2^3$. On the other hand the sequence of exponents in W is periodical, so the smallest word in its summit set is $\Delta_3^{2m} x_1^5 x_2^3 x_1^2 x_2^5 x_1^3 x_2^2$.

Definition 3.2.5. The unique representative $(r; (s_1, s_2, \cdots, s_h))$ of a summit set of a word V corresponding to the smallest summit word $\Delta_3^r W = \Delta_3^r x_{i_1}^{s_1} x_{i_2}^{s_2} \cdots x_{i_h}^{s_h}$. This unique representative(conjugacy invariant) of summit set is called *Artin-invariant* and it is denoted by $A^*(V)$.

Testing Conjugacy of Elements: Conjugacy of elements α and β of $\mathcal{B}_3$ can be tested as follow:

Step 1. Write α and β in normal form: $\alpha = \Delta_3^{r_1} W_1$, $\beta = \Delta_3^{r_2} W_2$.

Step 2. Check wether α and β are summit words or not according to Theorem 3.1.2. If they are not summit words then conjugate with $A^{\pm 1} \in Div$ and increase the exponents, like Garside done in [18].

Step 3. If the summit words of α and β have different exponents, then they are not conjugate. Otherwise find the Artin-invariants of both of them. If they have the same Artin-invariants then α and β are conjugates, otherwise not.

3.3 Knots of braid index less or equal three

Birman and Menasco [8, 7] gave the following classification theorem and invertibility theorem about 3-closed braids:

Theorem 3.3.1. *(**Birman and Menasco [8, 7]**) Let $\mathcal{L}$ be a link type which is represented by the closure of a 3-braid L. Then of the following holds:*
(a) $\mathcal{L}$ has braid index 3 and every 3-braid which represents $\mathcal{L}$ is conjugate to L.
(b) $\mathcal{L}$ has braid index 3, and is represented by exactly two distinct conjugacy classes of closed 3-braids. This happens if and only if the conjugacy class of L contains a braid whose associated (open) braid is conjugate to $x_1^u x_2^v x_1^w x_2^\varepsilon$ for some $u,\ v,\ w \in \mathbb{Z},\ \varepsilon = \pm 1$.
(c) The braid L is conjugate to $x_1^k x_2^{\pm 1}$ for some $k \in \mathbb{Z}$. These are precisely the links which are defined by closed 3-braids, but have index less than 3.

Theorem 3.3.2. *(**Birman and Menasco [8, 7]**) Let $\mathcal{K}$ be a link of braid index 3 with oriented 3-braid representative $\overrightarrow{K}$. Then $\mathcal{K}$ is non-invertible if and only if $\overrightarrow{K}$ and $\overleftarrow{K}$ are in distinct conjugacy classes, and the class of $\overrightarrow{K}$ does not contain a representative whose associated (open) braid is conjugate to $x_1^u x_2^v x_1^w x_2^\varepsilon$ for some $u,\ v,\ w \in \mathbb{Z},\ \varepsilon = \pm 1$.*

In [25] P.J Xu defined a unique representative (*Xu-invariant*) in the summit set of a word following the band presentation given as:

$$\mathcal{B}_3 = \left\langle a_1, a_2, a_3 : \quad a_2\, a_1 = a_3\, a_2 \ = a_1\, a_3 \right\rangle, \tag{3.3.1}$$

where $a_1 = x_1$, $a_2 = x_2$ and $a_3 = x_1^{-1}x_2x_1$. Like Xu-invariant, we defined Artin-invariant in the classical generators in the previous section. The advantage of working with Artin-invariant $A^*(V)$ instead of Xu-invariant $X^*(V)$ or vise versa is not completely understood. A computer program for finding the Artin-invariant of an arbitrary word in $\mathcal{B}_3$ is already available at [26]. These invariants are important for the implementation of classification and invertibility theorems mentioned above. The following Tables I and II given by Birman and Menasco [8] in Xu-invariants are translated in terms of the Artin-invariants.

Notation: 2^k stands for k-tuples of the form $(2, 2, \cdots, 2)$ in the following tables.

V	smallest summit word	$A^*(V)$
x_2	x_1	$(0; (1))$
x_1x_2	x_1x_2	$(0; (1,1))$
$x_1^kx_2$, $k \geq 2$	$\Delta_3 x_1^{k-2}$	$(1; (k-2))$
$x_1^kx_2^{-1}$, $k \geq 0$	$\Delta_3^{-1}x_1^{k+2}$	$(-1; (k+2))$
$x_1^kx_2$, $k < 0$	$\Delta_3^{-k}x_1^3 \underbrace{x_2^2x_1^2\cdots}_{\vert k\vert-1\ times}$	$(k; (3, 2^{\vert k\vert-1}))$
$x_1^{-1}x_2^{-1}$	$\Delta_3^{-1}x_1$	$(-1; (1))$
$x_1^{-2}x_2^{-1}$	Δ^{-1}	$(-1; \emptyset)$
$x_1^{-3}x_2^{-1}$	$\Delta_3^{-2}x_1x_2$	$(-2; (1,1))$
$x_1^{-4}x_2^{-1}$	$\Delta_3^{-2}x_1$	$(-2; (1))$
$x_1^kx_2^{-1}$, $k \leq -5$	$\Delta_3^{k+2}x_1^3 \underbrace{x_2^2x_1^2\cdots}_{\vert k\vert-5\ times}$	$(k+2; (3, 2^{\vert k\vert-5}))$

Table I: Artin-invariants of links of braid index ≤ 3.

ε	V	$A^*(V)$
+	$x_1^p x_2^q x_1^r x_2$	$(1;(p-1,q,r-1))$ or $(1;(q,r-1,p-1))$ or $(1;(r-1,p-1,q))$
+	$x_1^{-p} x_2^q x_1^r x_2$	$(-p;(r,2^p,q+1))$ for $r \geq q+1$ and $(-p;(q+1,r,2^p))$ for $r < q+1$
+	$x_1^p x_2^{-q} x_1^r x_2$	$(-q+1;(p,2^{q-1},r))$ for $p \geq r$ and $(-q+1;(r,p,2^{q-1}))$ for $p < r$
+	$x_1^p x_2^q x_1^{-r} x_2$	$(-r;(q+1,2^r,p))$ for $q+1 \geq p$ and $(-r;(p,q+1,2^r))$ for $q+1 < p$
-	$x_1^p x_2^q x_1^r x_2^{-1}$	$(-1;(p+1,q,r+1))$ or $(-1;(q,r+1,p+1))$ or $(-1;(r+1,p+1,q))$
-	$x_1^{-p} x_2^q x_1^r x_2^{-1}$	$(-p;(r+2,2^{p-2},q+1))$ for $r+1 \geq q$ and $(-p;(q+1,r+2,2^{p-2}))$ for $r+1 < q$
-	$x_1^p x_2^{-q} x_1^r x_2^{-1}$	$(-q-1;(p+2,2^{q-1},r+2))$ for $p \geq r$ and $((-q-1;(r+2,p+2,2^{q-1}))$ for $p < r$
-	$x_1^p x_2^q x_1^{-r} x_2^{-1}$	$(-r;(q+1,2^{r-2},p+2))$ for $q \geq p+1$ and $(-r;(p+2,q+1,2^{r-2}))$ for $q < p+1$

Table II: Artin-invariants of links in Th 3.3.1b and Th 3.3.2.

3.4 Hilbert series of conjugacy classes

The number of both smallest E-summit words and smallest O-summit words in $\mathcal{B}_3$ for a given length n are computed in this section. Hilbert series corresponding to conjugacy classes are then obtained as Theorem 3.1.5. The growing functions of these series is discussed at the end of the section. In [25] Xu gave Hilbert series for the conjugacy classes of minimal word length which are different of the series given in this section.

Definition 3.4.1. For a positive integer d, the function $\mu(d)$ given as below is called the classical Möbius function:

$$\mu(d) = \begin{cases} 1, & \text{when d is product of an even number of distinct primes ;} \\ -1, & \text{when d is product of an odd number of distinct primes;} \\ 0, & \text{when d is not square free.} \end{cases}$$

Theorem 3.4.1. *If $\mu(d)$ is a Möbius function then the following holds:*

(i) $\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1; \\ -0, & \text{otherwise} \end{cases}$

(ii) Let $f(n)$ and $g(n)$ be function defined for every positive integer n satisfying that $f(n) = \sum_{d|n} g(d)$ then $g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$

Proposition 3.4.2. *The number of* smallest E-summit words W *of length* $\mid W \mid = n \geq 3$ *is given by*

$$1 + \sum_{k=1}^{[\frac{n}{4}]} \frac{1}{2k} \sum_{d|a} d \sum_{\delta|d} \mu(\frac{d}{\delta}) \binom{\delta(c-b)-1}{\delta b - 1},$$

where $a = gcd(n, 2k)$, $n = ac$ and $2k = ab$.

Proof. Let $W = x_{i_1}^{s_1} x_{i_2}^{s_2} \cdots x_{i_h}^{s_h}$, $\mid W \mid = n \geq 3$ be a smallest E-summit word, then the following are true by Theorem 3.1.4:

(i) either $h = 1$ or $h = 2k$, $k \in \mathbb{Z}^+$;

(ii) for $h = 1$, there is only one smallest E-summit word: $\{x_1^n\}$;

(iii) $s_i \geq 2 \ \forall \ 1 \leq j \leq 2k$;

(iv) $\sum_{j=1}^{2k} s_j = n$.

Now we calculate the number of smallest E-summit words for a fixed k. First the cardinality of the following set of exponents

$$E(n,k) = \Big\{(s_1, s_2, \ldots, s_{2k-1}, s_{2k}) \in \mathbb{N}^{2k} \ \mid s_i \geq 2 \text{ and } \sum_{j=1}^{2k} s_j = n\Big\}$$

is given by

$$e(n,k) = \binom{n-2k-1}{2k-1} = \binom{a(c-b)-1}{ab-1}$$

(look at the equation $\sum_{i=1}^{2k}(s_i - 1) = n - 2k$, where $(s_i - 1)$ are positive integers). Now we replace the pair (n, k) by the triple (a, b, c), where $(b, c) = 1$, and, accordingly,

$E(n,k)$ by $E(a,b,c)$, and $e(n,k)$ by $e(a,b,c)$. Letting $2k = qp$ we introduce two new sets:

$$E(a,b,c,q) = \Big\{(s_1, s_2, \dots, s_{2k}) \in E(a,b,c) \text{ with minimal period of length } p\Big\},$$

(if $q \nmid ab$ or $q \nmid ac$, this set is empty), and also:

$$M(b,c,q) = \Big\{(s_1, s_2, \dots, s_p) \text{ is not periodic and } \sum_{i=1}^{p} s_i = c\frac{p}{b}\Big\}.$$

Now it is clear that $E(a,b,c) = \coprod_{d|a} E(a,b,c,d)$ and the bijection between $E(a,b,c,q)$ and $M(b,c,q)$ implies a bijection between $E(a,b,c)$ and $\coprod_{d|a} M(b,c,d)$. Therefore $e(a,b,c) = \sum_{d|a} m(b,c,d)$, where $m(b,c,d)$ is the cardinality of $M(b,c,d)$. By applying Möbius inversion formula, we have

$$m(b,c,d) = \sum_{\delta|d} \mu(\frac{d}{\delta}) e(\delta,b,c) = \sum_{\delta|d} \mu(\frac{d}{\delta}) \binom{\delta(c-b)-1}{\delta b - 1}.$$

$C_{n,k}$, the set of non-periodic sequences of length $b(\frac{a}{d})$, up to cyclic permutations, has the cardinality given by

$$c_{n,k} = \frac{1}{b}\frac{d}{a} \sum_{\delta|d} \mu(\frac{d}{\delta}) \binom{\delta(c-b)-1}{\delta b - 1}.$$

Hence the number of smallest E-summit words of length ≥ 3

$$1 + \sum_{k=1}^{[\frac{n}{4}]} \frac{1}{2k} \sum_{d|a} d \sum_{\delta/d} \mu(\frac{d}{\delta}) \binom{\delta(c-b)-1}{\delta b - 1}$$

□

Proposition 3.4.3. *The number of* smallest O-summit words *of length W of length $\mid W \mid = n \geq 6$ is given by*

$$1 + \sum_{k=1}^{[\frac{n-2}{4}]} \frac{1}{2k+1} \sum_{d|a} d \sum_{\delta|d} \mu(\frac{d}{\delta}) \binom{\delta(c-b)-1}{\delta b - 1},$$

where $a = gcd(n, 2k+1)$, $n = ac$ and $2k+1 = ab$.

Proof. Let $W = x_{i_1}^{s_1} x_{i_2}^{s_2} \cdots x_{i_h}^{s_h}$, $\mid W \mid = n \geq 6$ be a smallest O-summit word, then the following are true by Theorem 3.1.4:

(i) either $h = 1$ or $h = 2k + 1$, $k \in \mathbb{Z}^+$;

(ii) for $h = 1$, there is only one smallest O-summit word: $\{x_1^n\}$;

(iii) $s_i \geq 2$, $\forall\ 1 \leq j \leq 2k + 1$;

(iv) $\sum\limits_{j=1}^{2k+1} s_j = n$.

Now the number of smallest O-summit words for a fixed k can be calculated as in proposition 1. □

Proof of the Theorem 3.1.5: The only E-summit set for $\mid W \mid$=0 is $\{e\}$, the E-summit set for $\mid W \mid$=1 is $\{x_1, x_2\}$ and for $\mid W \mid$=2, the two E-summit sets are $\{x_1^2, x_2^2\}$ and $\{x_1x_2, x_2x_1\}$. This list of E-summit sets and proposition 3.4.2 implies Theorem 3.1.5a.

Similarly, the O-summit sets for $\mid W \mid$=0, 1, 2, 3, 4 and 5 are $\{e\}$, $\{x_1, x_2\}$, $\{x_1^2, x_1x_2, x_2x_1, x_2^2\}$, $\{x_1^3, x_1^2x_2, x_1x_2^2, x_2x_1^2, x_2^2x_1, x_2^3\}$, $\{x_1^4, x_1^3x_2, x_1^2x_2^2, x_1x_2^3, x_2x_1^3, x_2^2x_1^2, x_2^3x_1, x_2^4\}$ and $\{x_1^5, x_1^4x_2, x_1^3x_2^2, x_1^2x_2^3, x_1x_2^4, x_2x_1^4, x_2^2x_1^3, x_2^3x_1^2, x_2^4x_1, x_2^5\}$ respectively. This list of O-summit sets and proposition 3.4.3 implies Theorem 3.1.5b. □

The first few terms of the two series are :

$$H^E(t) = 1 + t + 2t^2 + t^3 + 2t^4 + 2t^5 + 3t^6 + 3t^7 + 5t^8 + 5t^9 + 8t^{10} + 10t^{11} + 17t^{12} + \cdots$$

and

$$H^O(t) = 1 + t + t^2 + t^3 + t^4 + t^5 + 2t^6 + 2t^7 + 3t^8 + 5t^9 + 7t^{10} + 9t^{11} + 14t^{12} + \cdots$$

Next the nature of growth of these Hilbert series is discussed. All the symbols and notations used onward are those of Theorem 3.1.5a and the proof of Proposition 3.4.2.

Lemma 3.4.4. *The following holds for $n \geq 8$:*

$$(i)\ \frac{2^{2[\frac{n}{8}]-1}}{[\frac{n}{8}](2[\frac{n}{8}]+1)} \leq \sum_{k=1}^{[\frac{n}{4}]} \frac{1}{2k} e(n,k)\,;$$

$$(ii)\ \sum_{k=1}^{[\frac{n}{4}]} e(n,k) \leq 2^{n-3}\,.$$

Proof. Since $e(n,[\frac{n}{8}])$ is a part of $\sum_{k=1}^{[\frac{n}{4}]} e(n,k)$ so

$$e(n,[\frac{n}{8}]) \leq \sum_{k=1}^{[\frac{n}{4}]} e(n,k)$$

Now we prove that

$$\binom{2[\frac{n}{8}]}{[\frac{n}{8}]} \leq e(n,[\frac{n}{8}]). \tag{3.4.1}$$

Let $[\frac{n}{8}] = m$ then $n \in \{8m, 8m+1, \cdots, 8m+7\}$. First (3.4.1) is true for $n = 8m$, i.e.,

$$\binom{n-2[\frac{n}{8}]-1}{2[\frac{n}{8}]-1} = \binom{6m-1}{2m-1} \geq \binom{6m-1}{m} \geq \binom{2m}{m}.$$

The inequality (3.4.1) holds for all $n \in \{8m, 8m+1, \cdots, 8m+7\}$ because $[\frac{n}{8}]$ is constant and for $n < n'$ we have $e(n,[\frac{n}{8}]) < e(n',[\frac{n'}{8}])$. The inequality $\frac{2^{2m}}{2m+1} \leq \binom{2m}{m}$ completes the proof (i) of the Lemma.

By the inequality

$$\binom{n}{k} \leq 2^{n-1}$$

We have

$$\sum_{k=1}^{[\frac{n}{4}]} e(n,k) \leq \sum_{k=1}^{[\frac{n}{4}]} 2^{n-2k-2} \leq 2^{n-3}\,.$$

□

Corollary 3.4.5. *The Hilbert series $H^E(t)$ and $H^O(t)$ grow exponentially.*

Proof. Consider the finite set $E(n,k,q)$ of sequences of exponents having minimal period $p \leq 2k$ given by

$$E(n,k,q) = \{(s_1, s_2, \ldots, s_{2k-1}, s_{2k}) \in \mathbb{N}^{2k} \ \ | \, s_i \geq 2 \text{ and } \sum_{j=1}^{2k} s_j = n\}$$

where $|E(n,k,q)| = e(n,k,q)$. By definition $c_{n,k,q}$ is given by $\frac{e(n,k,q)}{p}$. We also know that $e(n,k) = \sum_{q|a} e(n,k,q)$, where $a = gcd(n,2k)$ and $2k = qp$. Therefore we have:

$$\frac{1}{2k} e(n,k) \leq c_{n,k} \leq e(n,k).$$

The above inequality clearly shows that the coefficient C_n of $H^E(t)$ satisfy

$$\sum_{k=1}^{[\frac{n}{4}]} \frac{1}{2k} e(n,k) \leq C_n \leq \sum_{k=1}^{[\frac{n}{4}]} e(n,k).$$

The result follows by Lemma 3.4.4. Similarly, it can be proved that $H^O(t)$ also grows exponentially. $\square$

Chapter 4

Complete presentation and left-canonical form

4.1 Introduction

Using the complete presentation of $\mathcal{M}(A_n) = \mathcal{MB}_{n+1}$, we find the canonical form of a positive braid. Having Δ_{n+1} in canonical form in § 4.2, we give a procedure of deleting some part from Δ_{n+1} to obtain an arbitrary divisor of it .

To find the Garside normal form of elements in braid group $\mathcal{B}_{n+1}$, it is necessary to decide what is the maximal exponent of Δ_{n+1} in a given positive word. An inductive way of deciding this exponent of a positive word W is given in § 4.3.

The left-canonical form for braids was defined in [17] and was also proved:

Theorem 4.1.1. *[17] There is unique expression for a positive* W *as* $W = A_1A_2 \cdots A_r$ *with* $A_i|\Delta_{n+1}$, $A_i \neq e$ *and* $St(A_{i+1}) \subseteq Fl(A_i)$ *for each* i.

Using the above theorem, an algorithm was developed in [17] to obtain the left-canonical form for braids. According to Lemma 2.4 in the same paper, the corresponding permutation of A_i is used to find $St(A_i)$. In § 4.4, we prove a result which enables us to compute $St(A_i)$ using only canonical forms, independent of the permutation corresponding to A_i

4.2 Divisors of Δ_{n+1}

Lemma 4.2.1. *Canonical form of Garside braid is given by*

$$\Delta_{n+1} = x_1(x_2x_1)(x_3x_2x_1)\cdots(x_nx_{n-1}\cdots x_1) \tag{4.2.1}$$

Proof. The left hand side of each relation (other than commutation relation) is of the form $x_k\alpha(1, k-1)x_kx_{k-1}\cdots x_{j+1}x_j$, $1 \leq j \leq k$. It is clear by inspection that 4.2.1 is not divisible by any left hand side of a relation in complete presentation of $\mathcal{MB}_{n+1}$. □

We write the canonical form of Δ_{n+1} simply by

$$\Delta_{n+1} = \lambda(1,1)\lambda(2,1)\cdots\lambda(n,1),$$

where $\lambda(k,1) = x_kx_{k-1}\cdots x_1$. In general, $\lambda(k,m) = x_kx_{k-1}\cdots x_m$ and $\lambda(m,k) = x_mx_{m+1}\cdots x_k$ for $1 \leq m \leq k \leq n$ and any other Greek or English alphabet, e.g, $\pi(1,k)$ or $P(1,k)$ represents an arbitrary word in $\mathcal{MB}_{k+1}$.

Definition 4.2.1. Cutting the entire $\lambda(k,m)$ or a right divisor of it in canonical form of Δ_{n+1} is called *permissible cut.*

Proposition 4.2.2. *The following statements are true:*

(a) A word obtained through permissible cut or cuts is a divisor of Δ_{n+1}.

(b) Divisors obtained through different permissible cuts are different.

(c) Every divisor of Δ_{n+1} *can be obtained through permissible cut or cuts.*

Proof. (a) We know that $x_j\lambda(k,1) = \lambda(k,1)x_{j+1}$ for all $1 \le j \le k-1$. The entire $\lambda(k,1)$ or its right divisor can be moved (as shifted word) to the right most in Δ_{n+1}. If more than one such moves are required then we move the left most $\lambda(k,1)$ or its right divisor first, and keep this convention till all the moves are finished. (b) By the proof of Lemma 4.2.1 the word obtained through permissible cut or cuts is also in canonical form. Therefore two different such cuts can not give the same divisor of Δ_{n+1}. (c) We apply induction on n. For $n = 2$, $Div(\Delta_3) = \{1, x_1, x_2, x_1x_2, x_2x_1, \Delta_3\}$ and all of them can be obtained through permissible cut or cuts. Let the claim is true for Δ_n, i.e, all the divisors A_i of Δ_n can be obtained through permissible cut or cuts. Obviously each A_i is a divisor of Δ_{n+1}. Since $B_j = A_i\lambda(n,j)$ for $1 \le j \le n$ can be obtained through permissible cut or cuts (by induction hypothesis) and hence B_j is a divisor of Δ_{n+1} (by (b)). We can easily count the cardinality of $\{A_i\}\coprod\{B_j\}$ to be $(n+1)!$ which is exactly the number of divisors of Δ_{n+1}. $\square$

Proposition 4.2.2 enables us to find an arbitrary divisor of Δ_{n+1} in the canonical form

$$\Lambda(K,M) \equiv \lambda(k_1,m_1)\lambda(k_2,m_2)\cdots\lambda(k_s,m_s),$$

where $K = \{k_1,\ldots,k_s\}$, $k_l < k_{l+1}$ and $M = \{m_1,\ldots,m_s\}$, $m_l \le k_l$.

4.3 Computing the exponents

If $W \in \mathcal{MB}_{n+1} \setminus \mathcal{MB}_n$ the canonical form of W can be written in a unique way $W = \alpha(1,n-1)\gamma(1,n)$, where $\gamma(1,n)$ starts with x_n.

Theorem 4.3.1. *a) If $W \in \mathcal{MB}_n \subset \mathcal{MB}_{n+1}$, then:*

$$exp_{n+1}(W) = 0.$$

b) If $W = \alpha(1, n-1)\gamma(1, n) \in \mathcal{MB}_{n+1}$ *is in canonical form, then either*

$$W = \alpha(1, n-1)[\lambda(n, 1)\lambda(1, n)]^p \beta(1, n), \;\; where$$

$$\beta = 1 \, or \, \beta = \lambda(n, i), \; i \geq 2 \, or \, \beta = \lambda(n, i)x_i\beta'(1, n);$$

or

$$W = \alpha(1, n-1)[\lambda(n, 1)\lambda(1, n)]^p \lambda(n, 1)\beta(1, n), \;\; where$$

$$\beta = 1 \, or \, \beta = \lambda(1, i), \; i \geq n-1 \, or \, \beta = \lambda(1, i)x_i\beta'(1, n).$$

c) In the first case

$$exp_{n+1}(W) = min\{exp_n(\alpha), \, 2p\},$$

and in the second case

$$exp_{n+1}(W) = min\{exp_n(\alpha), \, 2p+1\}.$$

Proof. a) For $x_n \notin \mathcal{MB}_n$ and $x_n \mid \Delta_{n+1}$ we must have $exp_{n+1}(W) = 0$.

b) We apply induction on length of γ to show

$$\gamma = [\lambda(n, 1)\lambda(1, n)]^p \beta(1, n), \;\; where$$

$$\beta = 1 \, or \, \beta = \lambda(n, i), \; i \geq 2 \, or \, \beta = \lambda(n, i)x_i\beta'(1, n);$$

or

$$\gamma = [\lambda(n, 1)\lambda(1, n)]^p \lambda(n, 1)\beta(1, n), \;\; where$$

$$\beta = 1 \, or \, \beta = \lambda(1, i), \; i \geq n-1 \, or \, \beta = \lambda(1, i)x_i\beta'(1, n).$$

For $|\gamma| = 1$, $\gamma = x_n$ which is of the form $[\lambda(n, 1)\lambda(1, n)]^0\lambda(n, n)$. Let $\gamma = \gamma_1(1, n)x_j$ and suppose the claim is true for length $\leq |\gamma_1|$. We consider the following cases to complete the induction:

Case *1*: $\gamma_1 = [\lambda(n,1)\lambda(1,n)]^p\beta_1(1,n)$;

(1.1) $\beta_1 = 1$, *(1.2)* $\beta_1 = \lambda(n,i)$, $i \geq 2$ and *(1.3)* $\beta_1 = \lambda(n,i)x_i\beta'_1(1,n)$.

Case *2*: $\gamma_1 = [\lambda(n,1)\lambda(1,n)]^p\lambda(n,1)\beta_1(1,n)$;

(2.1) $\beta_1 = 1$, *(2.2)* $\beta_1 = \lambda(1,i)$, $i \geq n-1$ and *(2.3)* $\beta_1 = \lambda(1,i)x_i\beta'_1(1,n)$.

For *(1.1)*, $\gamma = \gamma_1 x_j$ implies $x_j = x_n$ otherwise $x_j \in St(\gamma)$ (because $[\lambda(n,1)\lambda(1,n)]^p x_j = x_j[\lambda(n,1)\lambda(1,n)]^p$). In this subcase $\gamma = [\lambda(n,1)\lambda(1,n)]^p x_n$. For *(1.2)*, $\gamma = \gamma_1 x_j$ implies $\gamma = [\lambda(n,1)\lambda(1,n)]^p\lambda(n,i)x_j$ for $i \geq 2$. If $j = i$ or $j = i-1$ then γ is of the required form. For $j < i-1$, we have $x_j|_L\gamma$ (because $[\lambda(n,1)\lambda(1,n)]^p\lambda(n,i)x_j = x_j[\lambda(n,1)\lambda(1,n)]^p\lambda(n,i)$), for $j > i$, we have $x_{j-1}|_L\gamma$ because $[\lambda(n,1)\lambda(1,n)]^p\lambda(n,i)x_j = x_{j-1}[\lambda(n,1)\lambda(1,n)]^p\lambda(n,i)$, contradicts $St(\gamma) = \{x_n\}$. *(1.3)* is obvious as $\beta'_1(1,n)x_j = \beta'(1,n)$. Similarly all the subcases of case *2* can be checked.

c) Let us denote by V_n the braid $V_n = x_n(x_{n-1}x_n)\cdots(x_2\cdots x_n)$ (this is not the canonical form!). By definition and basic properties of Δ_{n+1} we have

$$V_n\Delta_{n+1} = V_n\lambda(1,n)\Delta_n = \Delta_n\lambda(n,1)\Delta_n = \Delta_{n+1}\Delta_n$$

$$V_n\lambda(1,n) = \Delta_n\lambda(n,1) = \Delta_{n+1}, \tag{4.3.1}$$

$$\Delta_n^q\Delta_{n+1} = \Delta_{n+1}V_n^q, \tag{4.3.2}$$

$$V_n^q\Delta_{n+1} = \Delta_{n+1}\Delta_n^q, \tag{4.3.3}$$

We know that

$$\alpha = \Delta_n^{exp_n(\alpha)}\alpha_1(1,n-1) = \overline{\alpha}_1(1,n-1)\Delta_n^{exp_n(\alpha)},$$

where $\alpha_1 \in \mathcal{MB}_n^+$, $\overline{\alpha}_1 = \alpha_1$ for even $exp_n(\alpha)$ and $\overline{\alpha}_1 = \widehat{\alpha}_1$ for odd $exp_n(\alpha)$.

Case *1*: If $W = \overline{\alpha}_1\Delta_n^{exp_n(\alpha)}[\lambda(n,1)\lambda(1,n)]^p\beta$. We have two subcases:

(1.1) $2p = min\{exp_n(\alpha), 2p\}$ and *(1.2)* $exp_n(\alpha) = min\{exp_n(\alpha), 2p\}$.

For *(1.1)*, by (4.3.1), (4.3.2) and (4.3.3) we have

$$W = \overline{\alpha}_1 \Delta_n^{exp_n(\alpha)}[\lambda(n,1)\lambda(1,n)]^p \beta = \Delta_{n+1}^{2p}\overline{\alpha}_1 \Delta_n^{exp_n(\alpha)-2p}\beta.$$

In order to show that $exp_{n+1}(W) = 2p$, it is enough to show that $\overline{\alpha}_1 \Delta_n^{exp_n(\alpha)-2p}\beta$ is prime to Δ_{n+1}. On the contrary, if $\Delta_{n+1}|\overline{\alpha}_1 \Delta_n^{exp_n(\alpha)-2p}\beta$ then $\lambda(n,1)|_L\beta$ which contradicts $W = \overline{\alpha}_1 \Delta_n^{exp_n(\alpha)}[\lambda(n,1)\lambda(1,n)]^p\beta$. For *(1.2)*, again by (4.3.1), (4.3.2) and (4.3.3) we have

$$W = \begin{cases} \Delta_{n+1}^{exp_n(\alpha)}\overline{\alpha}_1[\lambda(n,1)\lambda(1,n)]^{p-\frac{exp_n(\alpha)}{2}}\beta, & exp_n(\alpha) \text{ is even;} \\ \Delta_{n+1}^{exp_n(\alpha)}\widehat{\overline{\alpha}}_1[\lambda(n,1)\lambda(1,n)]^{p-\frac{exp_n(\alpha)-1}{2}}\lambda(n,1)\beta, & exp_n(\alpha) \text{ is odd.} \end{cases}$$

For $W = \Delta_{n+1}^{exp_n(\alpha)}\overline{\alpha}_1[\lambda(n,1)\lambda(1,n)]^{p-\frac{exp_n(\alpha)}{2}}\beta$, if $exp_{n+1}(W) > exp_n(\alpha)$ then

$$\overline{\alpha}_1[\lambda(n,1)\lambda(1,n)]^{p-\frac{exp_n(\alpha)}{2}}\beta = \Delta_{n+1}^{exp_{n+1}(W)-exp_n(\alpha)}\pi(1,n)$$

implies $\Delta_n|\overline{\alpha}_1$ which contradicts $\alpha_1 \in \mathcal{MB}_n^+$. Similarly for

$$W = \Delta_{n+1}^{exp_n(\alpha)}\widehat{\overline{\alpha}}_1[\lambda(n,1)\lambda(1,n)]^{p-\frac{exp_n(\alpha)-1}{2}}\lambda(n,1)$$

we have $exp_{n+1}(W) = exp_n(\alpha)$. In the same way, in case *2*

$$W = \overline{\alpha}_1\Delta_n^{exp_n(\alpha)}[\lambda(n,1)\lambda(1,n)]^p\lambda(n,1)\beta$$

the $exp_{n+1}(W)$ is $min\{exp_n(\alpha), 2p\}$. □

4.4 Left-canonical form

Lemma 4.4.1. ***(Garside)*** *If a word $\pi(1,n)$ starts with x_i and x_j then $\pi(1,n)$ also starts with x_ix_j for $| j - i | \geq 2$ and with $x_ix_jx_i$ for $| j - i | = 1$.*

Lemma 4.4.2. *For $k \leq n$ and $i \neq k$, $x_i\pi(1,n) = \lambda(k,m)\gamma(1,n)$ implies $\pi(1,n) = \lambda(k,m)\mu(1,n)$.*

Proof. We prove the lemma by induction on $|\lambda(k,m)|$ and considered the following three cases:

(i) $i - k \geq 1$ (ii) $k - i = 1$ and (iii) $k - i \geq 2$.

Case(i): For $|\lambda(k,m)| = 1$ $x_i\pi(1,n) = x_k\gamma(1,n)$ implies $\pi(1,n) = x_k\mu(1,n)$ (by Lemma 4.4.1). Let the claim is true for $|\lambda(k,m)| = k-m$, i.e., $x_i\pi(1,n) = \lambda(k\text{-}1,m)\gamma(1,n)$ implies $\pi(1,n) = \lambda(k\text{-}1,m)\mu(1,n)$. For $|\lambda(k,m)| = k-m+1$, $x_i\pi(1,n) = \lambda(k,m)\gamma(1,n)$ implies (by Lemma 4.4.1):

$$\pi(1,n) = x_k\phi_1(1,n), \tag{4.4.1}$$

$$\lambda(k\text{-}1,m)\gamma(1,n) = x_i\phi_1(1,n). \tag{4.4.2}$$

From (4.4.2) $\phi_1(1,n) = \lambda(k\text{-}1,m)\mu(1,n)$ (by inductive hypothesis) and so from (4.4.1) we have $\pi(1,n) = \lambda(k,m)\mu(1,n)$.

Case(ii): Here $i = k - 1$ and $x_{k\text{-}1}\pi(1,n) = \lambda(k,m)\gamma(1,n)$ implies (by Lemma 4.4.1):

$$\pi(1,n) = x_k x_{k\text{-}1}\phi_2(1,n), \tag{4.4.3}$$

$$\lambda(k\text{-}2,m)\gamma(1,n) = x_k\phi_2(1,n). \tag{4.4.4}$$

From (4.4.4) $\phi_2(1,n) = \lambda(k\text{-}2,m)\mu(1,n)$ (by Case (i)). So from (4.4.3) $\pi(1,n) = \lambda(k,m)\mu(1,n)$.

Case(iii): For $|\lambda(k,m)| = 1$ $x_i\pi(1,n) = x_k\gamma(1,n)$ implies $\pi(1,n) = x_k\mu(1,n)$ (by Lemma 4.4.1). Let the claim is true for $|\lambda(k,m)| = k-m$, i.e., $x_i\pi(1,n) = \lambda(k\text{-}1,m)\gamma(1,n)$ implies $\pi(1,n) = \lambda(k\text{-}1,m)\mu(1,n)$. For $|\lambda(k,m)| = k-m+1$, $x_i\pi(1,n) = \lambda(k,m)\gamma(1,n)$ implies (by Lemma 4.4.1):

$$\pi(1,n) = x_k\phi_3(1,n), \tag{4.4.5}$$

$$\lambda(k\text{-}1, m)\gamma(1, n) = x_i\phi_3(1, n). \tag{4.4.6}$$

From (4.4.6) two subcases are dealt, i.e., (a) If $(k-1) - i = 1$ then $\phi_3(1, n) = \lambda(k\text{-}1, m)\mu(1, n)$ (by case (ii)) and (b) if $(k-1)-i > 1$ then $\phi_3(1, n) = \lambda(k\text{-}1, m)\mu(1, n)$ is again true (by inductive hypothesis). Hence from (4.4.5) $\pi(1, n) = \lambda(k, m)\mu(1, n)$.
□

The next lemma determines the left-least common multiple $\vee_L$ of x_i and $\lambda(k, m)$:

Lemma 4.4.3.

$$x_i \vee_L \lambda(k, m) = \begin{cases} x_i\lambda(k, m) = \lambda(k, m)x_i, & i \leq m-2 \\ x_{m-1}\lambda(k, m-1) = \lambda(k, m-1)x_m, & i = m-1; \\ x_i\lambda(k, m) = \lambda(k, m)x_{i+1}, & m \leq i \leq k-1; \\ \lambda(k, m), & i = k; \\ \lambda(k, m)\lambda(k+1, m) = \lambda(k+1, m)\lambda(k+1, m+1), & i = k+1; \\ \lambda(k, m)x_i = x_i\lambda(k, m), & i \geq k+2. \end{cases}$$

Proof. Let W be an arbitrary left- common multiple of x_i and $\lambda(k, m) = x_k x_{k-1} \cdots x_m$. We show that W is left-divisible by all the six words mentioned in the lemma corresponding to the cases:

(a) $i \leq m-2$, (b) $i = m-1$, (c) $m \leq i \leq k-1$, (d) $i = k$, (e) $i = k+1$ and (f) $i \geq k+2$.

For (a), (c) and (f), it is an immediate consequence of Lemma 4.4.2 that W is left-divisible by $x_i\lambda(k, m)$, which is the required least common multiple in the above three cases. For (d), the result is obvious as W is left-divisible by $\lambda(k, m)$. Let us consider the case (b). Since W is left-divisible by x_{m-1} and $\lambda(k, m)$, therefore

$$W = x_{m-1}Q_1(1, n) = \lambda(k, m)Q_2(1, n) \tag{4.4.7}$$

and $W = x_{m-1}\lambda(k,m)Q_3(1,n)$ (by Lemma 4.4.2). Using the fact that x_{m-1} commutes with x_j for $j \geq m+1$, we have

$$W = \lambda(k,m)x_{m-1}x_mQ_3(1,n). \tag{4.4.8}$$

From (4.4.7) and (4.4.8) we have $x_mQ_2(1,n) = x_{m-1}x_mQ_3(1,n)$, implies $x_mQ_2(1,n) = x_mx_{m-1}x_mQ_4(1,n)$(by Lemma 4.4.1), which further implies $Q_2(1,n) = x_{m-1}x_mQ_4(1,n)$. Put $Q_2(1,n) = x_{m-1}x_mQ_4(1,n)$ into (4.4.7) to have $W = \lambda(k,m-1)x_mQ_4(1,n)$ which implies W is left-divisible by $\lambda(k,m-1)x_m$. For (e), apply induction on the length of $\lambda(k,m)$. For $\lambda(k,k) = x_k$, $x_{k+1}|_LW$ and $x_k|_LW$ means $W = x_{k+1}P_1(1,n) = x_kP_2(1,n)$ which implies $W = x_{k+1}x_kx_{k+1}P_3(1,n)$ (by Lemma 4.4.1) and the result follows. Let the claim is true for $\lambda(k,m+1)$, i.e, if $x_{k+1}|_LW$ and $\lambda(k,m+1)|_LW$ then $\lambda(k,m+1)\lambda(k+1,m+1)|_LW$. Now $x_{k+1}|_LW$ and $\lambda(k,m)|_LW$ implies

$$W = x_kP_4(1,n) = \lambda(k,m)P_5(1,n). \tag{4.4.9}$$

Since $\lambda(k,m)|_LW$, obviously $\lambda(k,m+1)|_LW$ and by inductive hypothesis,

$$W = \lambda(k,m+1)\lambda(k+1,m+1)P_6(1,n). \tag{4.4.10}$$

From (4.4.9) and (4.4.10), $x_mP_5(1,n) = \lambda(k+1,m+1)P_6(1,n)$, which implies $x_mP_5(1,n) = x_m\lambda(k+1,m)P_7(1,n)$ (by case (b)) and $P_5(1,n) = \lambda(k+1,m)P_7(1,n)$. Put $P_5(1,n) = \lambda(k+1,m)P_7(1,n)$ into (4.4.9) to have $W = \lambda(k,m)\lambda(k+1,m)P_7(1,n)$. Which means W is left-divisible by $\lambda(k,m)\lambda(k+1,m)$. □

Now we give a new method to compute the initial set of a divisor of Δ_{n+1}, $\Lambda(K,M)$ (written in canonical form $\Lambda(K,M) \equiv \lambda(k_1,m_1)\lambda(k_2,m_2)\cdots\lambda(k_s,m_s)$ the sequence $k = (k_1,\ldots,k_s)$ is strictly increased and the sequence $M = (m_1,\ldots,m_s)$ satisfy $m_i \leq k_i$).

Proposition 4.4.4. *For $\Lambda(K, M)$. Define*

$$K_1 = \{k \in K | k-1 \notin K\}$$

and

$$K_2 = \{k \in K | k-1 \in K \text{ and } m_l \le m_{l-1}\}.$$

Then $x_i \mid_L \Lambda(K, M) \Leftrightarrow i \in K_1 \coprod K_2$.

Proof. " $\Leftarrow$ " If $i \in K_1$ then x_i commutes with all x_j to the left of it (by definition of $\Lambda(K, M)$) and we have $x_i|_L\Lambda(K, M)$. Also if $i \in K_2$ then $\lambda(k_{l-1}, m_{l-1})\lambda(i, m_l) = \lambda(i, m_l) \sum \lambda(k_{l-1}, m_{l-1})$ (as $m_l \le m_{l-1}$), now x_i commutes with all x_j to its left and we have $x_i|_L\Lambda(K, M)$.

" $\Rightarrow$ " Let $x_i|_L\Lambda(K, M)$. Apply induction on s. For $s = 1$, $x_i|_L\lambda(k_1, m_1)$ implies $i = k_1$ because $\lambda(k_1, m_1)$ is unique in its diagram. Let the claim is true for $s - 1$. The following different cases are considered to complete the induction on s.
(a) $i \le m_1 - 2$, (b) $i = m_1 - 1$, (c) $m_1 \le i \le k_1 - 1$, (d) $i = k_1$, (e) $i = k_1 + 1$ and (f) $i \ge k_1 + 2$: For (a), $\Lambda(K, M) = \lambda(k_1, m_1)x_iQ(1, n)$ (by Lemma 4.4.3) and

$$\lambda(k_2, m_2) \cdots \lambda(k_s, m_s) = x_iQ(1, n),$$

contradicting the fact that $\lambda(k_2, m_2) \cdots \lambda(k_s, m_s)$ is canonical form because $k_2 > k_1 \ge i$. Therefore $i \le m_1 - 2$ is not possible.
(b) $i = m_1 - 1$ and (c) $m_1 \le i \le k_1 - 1$ are also not possible by the same argument used in (a). Case (d) is obvious as $i = k_1$. For (e), $\Lambda(K, M) = \lambda(k_1, m_1)\lambda(k_1+1, m_1)P(1, n)$ (by Lemma 4.4.3) and

$$\lambda(k_2, m_2) \cdots \lambda(k_s, m_s) = \lambda(k_1 + 1, m_1)P(1, n).$$

Now $k_1+1 < k_2$ is not possible (again by the argument used in (a)). So $k_1+1 = k_2$, if $m_2 \leq m_1$ then $k_2 \in K_2$ otherwise $\lambda(k_3, m_3)\cdots\lambda(k_s, m_s) = \lambda(m_2-1, m_1)P(1, n)$ but $\lambda(k_s, m_s)\cdots\lambda(k_s, m_s)$ is canonical form and $x_{m_2-1} < x_{k_3}$ which is impossible. Finally for (f), $\Lambda(K, M) = \lambda(k_1, m_1)x_iT(1, n)$ (by Lemma 4.4.3) and

$$\lambda(k_2, m_2)\cdots\lambda(k_s, m_s) = x_iT(1, n).$$

Let $\widetilde{K}_1$ and $\widetilde{K}_2$ be the sets defined in the lemma corresponding to the divisor

$$\lambda(k_2, m_2)\cdots\lambda(k_s, m_s)$$

of Δ_{n+1}. By induction $i \in \widetilde{K}_1 \coprod \widetilde{K}_2$, where $\widetilde{K}_2 \subseteq K_2$ and $\widetilde{K}_1 = K_1 \backslash \{k_1\} \coprod \{k_2\}$. If $i = k_2$ then $k_2 \geq k_1 + 2$ implies $k_2 \in K_1$. Hence $i \in K_1 \coprod K_2$ in any case. $\square$

Bibliography

[1] D. J. Anick, *on the homolgy of associative algebras*, Trans. Amer. Math. Soc. 296(1986), pp. 641-659.

[2] E. Artin, *Theorie der Zopfe*, Ahb. Math. Sem. 4(1925), 47-72.

[3] E. Artin, *Theory of braids*. Ann. Math. 48(1947), 101-126.

[4] B. Berceanu, A. Usman, Z. Iqbal, *Relative Garside elements of Artin monoids* $\mathcal{MB}_{n+1}$ (in preparation).

[5] G. Bergman, *The diamond lemma for ring theory*, Adv. in Math 29(1978), pp. 178-218.

[6] J. S. Birman, *Braids links and mapping-class groups*. Annals of Math. Studdies. Princeton University Press, 12(1974).

[7] J. S. Birman and W. W. Menasco, *A note on closed 3-braids*, Communications in Contemporary Mathematics. 10(2008), 1033-1047.

[8] J. S. Birman and W. W. Menasco, *Studying links via closed braids III: Classifying links which are closed 3-braids*, Pacific Journal of Mathematics. 161 (1993), 25-113. Math. Studdies. Princton University Press, 12(1974).

[9] L. A. Bokut, Y. Fong, W. F. Ke, and L. S. Shiao , *Gröbner-Shirshov bases for the braid semigroup*. In advances in algebra, world Sci. Publ. 2003, 60-72.

[10] N. Bourbaki, *Groupes et algèbres de Lie*, Chapitres 4-6, Elem. Math., Hermann, 1968.

[11] E. Brieskorn and K. Saito, *Artin-Gruppen and Coxeter-Gruppen*, Invent. Math. 17(1972), 245-271.

[12] K. S. Brown, *The geometry of rewriting systems:a proof of Anick-Groves-Squeir theorem,* in: Algorithms and Classification in Combinatorial Group Theory (G. Baumslag, C.F. Miller, eds.), MSRI Publications 23, Springer, New York, 1992, pp.137-164.

[13] Z. Iqbal, *Hilbert series of positive braids* (to appear in Algebra Colloquium).

[14] W. L. Chow, *On the algebraic braid group*. Ann. of Math. 49, pp. 654-658.

[15] P. M. Cohn, *Further Algebra and Applications*, Springer (India), 2004.

[16] P. Deligne, *Les immeubles des groupes de tresses généralisés*, Invention math. 17(1972), 273-302.

[17] E. A. Elrifai and H. R. Morton , *Algorithms for positive braids*, Quart. J. Math. Oxford Ser. 2, 45(1994), 479-497.

[18] F. A. Garside, *The braid groups and other groups*, Quat. J. Math. Oxford, ser. 20(1969), 235-254.

[19] V. Gebhardt, *A new approach to the conjugacy problem in the Garside groups*, preprint, arXiv:math.GT/0306199 v2, 21 October 2003.

[20] S. J. Lee, Algoritmmic solutions to decision problems in braid groups, Ph.D. Thesis in KAIST, (2000).

[21] K. Murasugi, *On closed 3-braids*, Memoirs of the AMS 151, 1974.

[22] L. Paris, *Braid groups and Artin groups*, arxiv: 0711.2372VI [math. GR], 2007.

[23] V. A. Ufnarovskij, *Combinatorial and Asymptotic Methods in Algebra*, in Encyclopaedia of Mathematical Sciences, vol. 57, Algebra VI, Springer-Verlag, 1995.

[24] A. Usman, *Conjugacy classes of 3-braid group* (accepted for publication in Algebra Colloquium)

[25] P.J. Xu, *The genus of closed 3-braid*, J. of Knots Theory and its Ramifications. 1(1992), 303-326.

[26] www.sms.edu.pk/software.php