Logspace computations for Garside groups of spindle type

Murray Elder and Arkadius Kalka*

October 29, 2013. Mathematics Subject Classification(2010): 20F36, 20F65, 68Q15.
Keywords: Logspace normal form, logspace conjugacy problem, braid group, Garside group

Abstract

M. Picantin introduced the notion of Garside groups *of spindle type*, generalizing the 3-strand braid group. We show that, for linear Garside groups of spindle type, a normal form and a solution to the conjugacy problem are logspace computable. For linear Garside groups of spindle type with *homogenous* presentation we compute a geodesic normal form in logspace.

1 Introduction and Outline

The word problem, conjugacy problem and geodesic problem are examples for classical problems in combinatorial group theory. Here we deal with the question which of these problems can be solved in *logarithmic space*. Our objects of interest are braid and Garside groups, certain generalizations of braid groups which admit a similar solution to the word and conjugacy problem. Since braid groups are linear [3, 20] the word problem is solvable in logspace [22]. Closely related to the word problem is the computation of a normal form. Here the problem seems to be much harder. In [14] it is shown that torus knot groups $\langle a, b \mid a^m = b^n \rangle$ for m, n positive integers have logspace normal forms, which includes the 3-strand braid group. Here we prove that Garside normal forms are logspace computable for a small class of simple Garside groups which includes B_3. Also, we use this result to solve the conjugacy problem and the shortest word problem for some special Garside groups in logspace. For $n \geq 4$, the braid groups are not of spindle type, and it is not known whether the Garside normal form (or any other normal form) is logspace computable. More generally, it is an open problem whether all linear (respectively automatic) groups have logspace computable normal forms, and also whether all biautomatic groups have conjugacy problem solvable in logspace, so since braid groups are biautomatic [16] and linear, they serve as important test cases.

In related work Diekert, Kausch and Lohrey consider logspace geodesic normal forms for right-angle Artin groups and Coxeter groups [11], and S. Vassileva

*Research supported by Australian Research Council grants DP110101104 and FT110100178

showed that the conjugacy problem for a large class of wreath products is solvable in logspace [29].

Outline. In Section 2 we introduce the basic notion of an *logspace transducer* and recall some basic examples and properties of logspace computable functions and normal forms. Section 3 deals with normal forms in Garside systems of spindle type. First we recall the definition of Garside systems (section 3.1) and their normal forms (section 3.2). In section 3.3 we refer to the basic Garside structures in braid groups. Section 3.4 introduces the main notion of so-called Garside groups *o*f spindle type. The main results on normal forms in Garside groups of spindle type are given in sections 3.5 and 4. In particular, we show that the Garside normal form is logspace computable for linear Garside groups of spindle type (section 3.5.1). Furthermore, we show that a geodesic normal form is logspace computable for linear Garside groups of spindle type with homogenous presentation (section 3.5.2). A logspace solution for the conjugacy problem in linear Garside groups of spindle type is given in section 4. In the final section we briefly consider a normal form for B_4, which we show cannot be computed in logspace.

2 Basic properties of logspace normal forms

We start with a precise definition of logspace computation, taken from [14].

Definition 2.1. *A* DETERMINISTIC LOGSPACE TRANSDUCER *consists of a finite state control and three tapes: the first* INPUT TAPE *is read only, and stores the input word; the second* WORK TAPE *is read-write, but is restricted to using at most $c \log n$ squares, where n is the length of the word on the input tape and c is a fixed constant; and the third* OUTPUT TAPE *is write-only, and is restricted to writing left to right only. A transition of the machine takes as input a letter of the input tape, a state of the finite state control, and a letter on the work-tape. On each transition the machine can modify the work tape, change states, move the input read-head, and write at most a fixed constant number of letters to the output tape, moving right along the tape for each letter printed.*

Since the position of the read-head of the input tape is an integer between 1 and n, we can store it in binary on the work tape.

Definition 2.2. *Let X, Y be finite alphabets. Let X^* denote the set of all finite length strings in the letters of X, including the empty string λ. We call $f : X^* \to Y^*$ a* LOGSPACE COMPUTABLE FUNCTION *(short: L-computable function) if there is a deterministic logspace transducer that on input $w \in X^*$ computes $f(w)$.*

In the sequel we make use of the following results on L-computable functions and normal forms. The first result is due to Lipton and Zalcstein [22].

Proposition 2.3. *All linear groups (groups of matrices with entries from a field of characteristic zero) have word problem solvable in logspace.*

Simon [27] extends this to linear groups over arbitrary fields.

Proposition 2.4. *(see Prop. 1 in [14]) Let $\langle a_1, \ldots, a_k \mid - \rangle$ be the free group of finite rank k with normal form the set of all freely reduced words over $X = \{a_i^{\pm 1}\}$. Then there is a logspace computable function $f : X^* \to X^*$ such that $f(w)$ is the normal form word for w.*

This result can be traced back to [23]. The next result shows that logspace computable functions are closed under composition.

Proposition 2.5. *(see Lemma 2 in [14]) If $f : X^* \to Y^*$ and $f : Y^* \to Z^*$ can both be computed in logspace, then their composition $f \circ g : X^* \to Z^*$ can also be computed in logspace.*

Lastly, we note that finding a logspace computable normal form for one finite generating set implies the existence of a logspace normal form for any other (see Prop. 5 in [14]).

3 Normal forms for Garside systems of spindle type

3.1 Basic definitions for Garside systems

This introductory subsection follows in exposition and terminology closely [26] and [17].

Let M be a monoid. For $a, b \in M$, we say that a is a *left divisor of* b, and b is a *right multiple of* a, denoted by $a \preceq b$, if there exists an element $c \in M$ such that $b = ac$. Similarly, for $a, b \in M$, we say that a is *right divisor of* b, and b is a *left multiple of* a, denoted by $b \succeq a$, if there exists an element $c \in M$ such that $b = ca$.

A monoid M is *atomic* (or *Noetherian*) if for every element $a \in M$ there exists an integer n such that the element cannot be expressed as the product of more than n elements distinct from 1. An element $a \neq 1$ in M is called an *atom* if $a = bc$ implies $b = 1$ or $c = 1$. An atomic monoid is necessarily generated by its atoms. Indeed, the subsets of M that generate M are exactly those subsets that include the set of all atoms. Furthermore, if M is a finitely generated atomic monoid then relations $\preceq$ and $\succeq$ are partial orders, and every element of M admits only finitely many left and right divisors [10]. We call an element $\Delta \in M$ *balanced* if the sets of left and right divisors coincide. In that case, this set is denoted by $\mathrm{Div}(\Delta)$.

A monoid M is *cancellative* if for all $a, b, b', c \in M$ $abc = ab'c$ implies $b = b'$.

An element $m \in M$ is a *least common right multiple* (or a *right lcm*) *of a and b* if it is a right multiple of both a and b, and $a \preceq c$ and $b \preceq c$ implies $m \preceq c$.

A *left lcm* is defined symmetrically using the relation $\succeq$. If they exist, right and left lcm's are, by definition, unique, and denoted by $a \vee b$ and $a \tilde{\vee} b$, respectively. If $a \vee b$ exists, and M is (left) cancellative, there exists a unique element c such that $a \vee b = ac$. This element is called the *right complement of a in b*, and it is denoted by $a \backslash b$. We define the *left complement* symmetrically. In particular, we have $a \vee b = a(a \backslash b) = b(b \backslash a)$, and $a \tilde{\vee} b = (b/a)a = (a/b)b$.

Definition 3.1. *A monoid M is an* LCM MONOID *if it is Noetherian, cancellative, and every pair of elements $a, b \in M$ admits a right and a left lcm.*

In an lcm monoid, for every pair of elements (a, b), the set of common left divisors of a and b is finite and it admits a right lcm, which is therefore the *greatest common left divisor* (or *left gcd*) *of* a *and* b, denoted by $a \wedge b$. The *right gcd* $a \tilde{\wedge} b$ is defined symmetrically. An lcm monoid is a lattice for the left and right divisibility relations $\preceq$ and $\succeq$.
If M is a lcm monoid, then M satisfies Ore's conditions [7], and it embeds in its group of right fractions, and, symmetrically, in its group of left fractions. These two groups coincide, and therefore we may speak of the group of fractions of an lcm monoid.

Definition 3.2. *[26, 17] Let G be a group. Denote by G^+ the submonoid of G generated by a given subset S of G. The pair (G, S) is called a* Garside system *if G^+ is an lcm monoid, G is its group of fractions, and there exists a balanced element $\Delta \in G^+$ such that $S = \mathrm{Div}(\Delta)$ is finite and it generates G. Then we call G a* Garside group*, G^+ a* Garside monoid*, and Δ a* Garside element*. The elements of S are called* simple elements*.*

S is closed under $\backslash, /, \vee, \tilde{\vee}, \wedge, \tilde{\wedge}$. Indeed, S is the closure of the atoms of G^+ under $\backslash$ and $\vee$. The functions $\partial : a \mapsto a\backslash\Delta$ and $\tilde{\partial} : a \mapsto \Delta/a$ map G^+ onto S, and the restrictions $\partial|_S$, $\tilde{\partial}|_S$ are bijections of S satisfying $\tilde{\partial}|_S = (\partial|_S)^{-1}$. In particular, we have $\partial^2(a) = \tau(a)$ and $\tilde{\partial}^2 = \tau^{-1}(a)$ for all $a \in S$, where τ denotes the inner automorphism of G defined by $a \mapsto \Delta^{-1}a\Delta$.
The partial orders $\preceq$ and $\succeq$ on G^+ naturally extend to partial orders on the whole Garside group G. Furthermore, we define for $a, b \in G$, $a \leq b$, if there exist $c, c' \in G^+$ such that $b = cac'$. By definition $\leq$ is always reflexive and transitive. For a Noetherian monoid, like G^+, $\leq$ is a partial order, i.e. also antisymmetric. Indeed, assume there exist $a, b \in G^+$ such that $a \leq b$ and $b \leq a$, i.e., there exist $c_1, c_2, c_1', c_2' \in G^+$ such that $b = c_1ac_2$ and $a = c_1'bc_2'$. Then repeated insertion, i.e., $b = c_1ac_2 = c_1(c_1'bc_2')c_2 = c_1c_1'(c_1ac_2)c_2'c_2 = \ldots$ contradicts Noetherianity except for the case $a = b$.

3.2 Normal forms in Garside systems

Since Δ is quasi-central, we have for all $a, b \in G$ and $k \in \mathbb{Z}$, $a \preceq \Delta^k \preceq b$ iff $b \succeq \Delta^k \succeq a$ iff $a \leq \Delta^k \leq b$. If $\Delta^r \leq a \leq \Delta^s$, we denote $a \in [r, s]$. The maximal $r \in \mathbb{Z}$ and the minimal $s \in \mathbb{Z}$ such that $a \in [r, s]$ are called the *infimum* and the *supremum* of a, denoted by $\inf(a)$ and $\sup(a)$, respectively.
In Garside systems there exist natural normal forms. For every $a \in G^+$ there exists an unique $l \in \mathbb{N}$ and a unique decomposition $a = s_1 \cdots s_l$ where $s_i = \Delta \wedge (s_i \cdots s_l) \in S$ and $s_l \neq 1$. This decomposition is called the *left normal form* of $a \in G^+$ in (G, S), and the number l is called the *canonical length* or *gap*, denoted $cl(a)$. Using the decomposition $a = \Delta^{\inf(a)}\overline{a}$ for some unique $\overline{a} \in G^+$ we get the *left Δ-normal form* of a in (G, S). Note that $\overline{a}_1 = \overline{a} \wedge \Delta$ is a proper divisor of Δ. We define $cl(a) = cl(\overline{a})$.
Furthermore, we can associate with every element $g \in G$ an unique pair $(a, b) \in G^+ \times G^+$ such that $g = a^{-1}b$ and $a \wedge b = 1$. The left normal forms $a = t_1 \cdots t_m$ and $b = s_1 \cdots s_l$ give rise to the decomposition $g = (t_m^{-1} \cdots t_1^{-1})(s_1 \cdots s_l)$ which we call the *left fractional normal form* of g in (G, S). *Right fractional normal forms* are defined symmetrically.
For the sake of brevity, in the sequel we often simply refer to a Garside group G rather than a Garside system (G, S) with $S = \mathrm{Div}(\Delta)$.

3.3 Garside structures for the braid groups

For any Garside system $(G, \mathrm{Div}(\Delta)$ and every $k \in \mathbb{N}$, also $(G, \mathrm{Div}(\Delta^k)$ is a Garside system. This leads us to the following definition.

Definition 3.3. *A pair (G, S) is called a* Minimal Garside system *if (G, S) is a Garside system and there exists no proper subset S' of S such that (G, S') is also a Garside system.*

n-strand braid groups admit at least two minimal Garside structures. The first being the classical Garside structure $(B_n, \mathrm{Div}(\Delta_n))$ where the partial orders $\preceq$ and $\succeq$ (defining the divisors of Δ) are induced by the monoid generated by the atoms $\sigma_1, \ldots, \sigma_{n-1}$. Topologically, inside an Artin generator σ_k $(1 \leq k < n)$ the $(k+1)$-th strand crosses over the k-th strand, i.e., it is an half twist on 2 strands. The Garside element $\Delta_n = \sigma_1(\sigma_2\sigma_1)\cdots(\sigma_{n-1}\cdots\sigma_2\sigma_1)$ describes an half twist on all n strands. It has $n!$ positive divisors which are in one-to-one correspondence to permutations. Indeed, there exists a lattice isomorphism from $(\mathrm{Div}(\Delta_n), \prec)$ to S_n equipped with the weak order, where the fundamental braid Δ_n maps to the longest element.
The presentation with respect to the set of atoms is the classical Artin presentation [1]

$$B_n = \left\langle \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & \forall |i-j| > 1, \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} & \forall i = 1, \ldots, n-2 \end{array} \right\rangle.$$

The second, somehow dual (see [2]), Garside structure is induced by the *dual monoid* B_n^{+*} generated by the so-called *band generators*. Topologically, inside the band generator a_{st} the t-th strand crosses over the s-th strand 'behind' the strands $s+1, \ldots, t-1$, i.e., here the atoms correspond to all tranpositions (reflections) rather than only the nearest-neighbor transpositions (simple reflections). W.r.t. this generating set B_n admits the following complete set of relations [4].

$$\begin{aligned} a_{rs}a_{st} = a_{rt}a_{rs} = a_{st}a_{tr}, &\qquad 1 \leq r < s < t \leq n, \\ a_{st}a_{qr} = a_{qr}a_{st}, &\qquad (t-r)(t-q)(s-r)(s-q) > 0. \end{aligned}$$

We call this presentation the *dual presentation.*
The minimal Garside system induced by the dual braid monoid is $(B_n, \mathrm{Div}(\delta_n))$ with $\delta_n = a_{12}a_{23}\cdots a_{n-1,n}$. Here the dual Garside element corresponds to a Coxeter element in the Weyl group. The simple elements are characterized by non-crossing partitions, i.e., we have $|\mathrm{Div}(\delta)| = \frac{1}{n+1}\binom{2n}{n}$, the n-th Catalan number.
It is conjectured that for $n \geq 4$ (B_n, Δ_n) and (B_n, δ_n) are (up to automorphisms) the only minimal Garside systems for B_n.
The 3-strand braid group is exceptional as it admits further minimal Garside structures.

Proposition 3.4. *(a) Recall that $B_3 \equiv T(2,3) = \langle a, b \mid a^2 = b^3 \rangle$ where $a = \Delta_3$ and $b = \delta_3$ and consider the set $S_T = \{1, a, b, b^2, a^2\}$ of positive divisors of a^2 w.r.t the torus knot monoid $T^+ = T^+(2,3)$. Then (B_3, S_T) is a minimal Garside system.*
(b) B_3 also admits the non-standard presentation $\langle \sigma, b \mid \sigma b \sigma = b^2 \rangle$ where $\sigma = \sigma_1$ and $b = \delta_3$. Consider the set $\{1, \sigma, b, \sigma b, b^2, b\sigma, b\sigma b, b^3\}$ of divisors of b^3 w.r.t. the monoid defined by that presentation. Then $(B_3, \mathrm{Div}(b^3))$ is a minimal Garside system.

3.4 Garside systems of spindle type

Definition 3.5. *A Garside system (G,S) with $S=\mathrm{Div}(\Delta)$ is* OF SPINDLE TYPE *iff for every pair of elements $a,b\in S$ we have that $a\wedge b$ and $a\mathbin{\tilde{\wedge}}b$ lie in $\{a,b,1\}$.*

In particular, if neither $a\preceq b$ nor $b\preceq a$ then $a\wedge b=1$, and if neither $a\succeq b$ nor $b\succeq a$ then $a\mathbin{\tilde{\wedge}}b=1$.

Corollary 3.6. *Let (G,S) with $S=\mathrm{Div}(\Delta)$ be a Garside system of spindle type. For every pair of elements $a,b\in S$ we have that $a\vee b$ and $a\mathbin{\tilde{\vee}}b$ lie in $\{a,b,\Delta\}$.*

PROOF. The following formula holds for all $a,b,c,d\in G^+$ (see [26]):

$$ac=bd=(a\vee b)(c\mathbin{\tilde{\wedge}}d)=(a\wedge b)(c\mathbin{\tilde{\vee}}d).$$

In particular, if $\Delta=a\partial(a)=b\partial(b)=\partial^{-1}(c)c=\partial^{-1}(d)d$ then

$$\Delta=(a\vee b)(\partial(a)\mathbin{\tilde{\wedge}}\partial(b))=(\partial^{-1}(c)\wedge\partial^{-1}(d))(c\mathbin{\tilde{\vee}}d).$$

We conclude that if the (left and right) gcd's are 1 then the lcm's equal Δ. And if $a\wedge b$ (or $a\mathbin{\tilde{\wedge}}b$) lie in $\{a,b\}$, then a and b are comparable w.r.t the partial order in question, and we conclude that also $a\vee b$ (or $a\mathbin{\tilde{\vee}}b$) lies in $\{a,b\}$. □

This notion (with some additional height condition) was introduced by Picantin as *monoide de type fuseau* in [25].
Note that all Garside systems of spindle type are minimal.

Definition 3.7. *A group G is a* GARSIDE GROUP OF SPINDLE TYPE *iff it admits a Garside system of spindle type $(G,\mathrm{Div}(\Delta))$. A monoid M is* GARSIDE MONOID OF SPINDLE TYPE *iff it is generated by $S=\mathrm{Div}(\Delta)$ for some Garside system of spindle type (G,S).*

Examples. (1) The 3-strand braid group B_3 is a Garside group of spindle type. It admits the Garside monoids of spindle type B_3^+, $(B_3^*)^+$ and $T^+(2,3)$. However the Garside monoid $\langle\sigma,b\mid\sigma b\sigma=b^2\rangle^+$ from Proposition 3.4 (b) is not of spindle type since $aba\wedge ba=b\notin\{aba,ba,1\}$.
(2) All *torus knot groups* $T(p,q)=\langle a,b\mid a^p=b^q\rangle$ are Garside groups of spindle type.
(2a) More general *torus-type groups* $T(p_1,\ldots,p_k)=\langle a_1,\ldots,a_k\mid a_1^{p_1}=\ldots=a_k^{p_k}\rangle$ are Garside groups of spindle type.
(3) The Artin groups of type $I_2(m)$ (also called *dihedral Artin groups* $\mathcal{A}(I_2(m))$) are Garside groups of spindle type. Indeed, two Garside structures are known - the classical one induced by the monoid $\mathcal{A}^+(I_2(m))\langle a,b\mid\underbrace{aba\cdots}_{m}=\underbrace{bab\cdots}_{m}\rangle$, and the dual induced by the monoid $\mathcal{A}^+(I_2^*(m))=\langle\{\sigma_i\}_{1\leq i\leq m}\mid\sigma_1\sigma_m=\sigma_m\sigma_{m-1}=\ldots=\sigma_2\sigma_1\rangle$ where $\sigma_1=a$ and $\sigma_i=\underbrace{bab\cdots}_{i-1}=\underbrace{(bab\cdots)^{-1}}_{i-2}$ for $2\leq i\leq m$.
(4) The 3-strand pure braid group $P_3=\langle a,b,c\mid abc=bca=cab\rangle$ is a Garside group of spindle type. Recall that for $n\geq 4$ the pure braid groups P_n are not known to be Garside. In particular, the monoids induced by standard presentations are *not* Garside [21].

(5) P_3 is part of another infinite family of groups, namely the fundamental groups of the complement of a complex line arrangement whose graph is one multiple point of multiplicity $n \geq 2$. These fundamental groups admit presentations of the form

$$\langle a_1, \ldots, a_n \mid a_n a_{n-1} \cdots a_1 = a_{n-1} \cdots a_1 a_n = \ldots = a_1 a_n \cdots a_2 \rangle,$$

and they are all Garside groups of spindle type with Garside element $\Delta = a_1 \vee \ldots \vee a_n = a_n \cdots a_1$. Indeed, these groups are the *pure dihedral Artin groups of rank* n, denoted by $\mathcal{PA}(I_2(n))$. The monoid $\mathcal{PA}^+(I_2(n))$ is a submonoid of the dual dihedral monoid $\mathcal{A}^+(I_2^*(n))$ - the embedding is given by $a_i = \sigma_i^2$ for all $1 \leq i \leq n$.

Remark. All Garside groups of spindle type given in the examples (except for example (2a)) are known to be *linear*, i.e. they admit a faithful linear representation. This has been known for B_3 for many years. Indeed, for $n = 3$ the Burau representation is faithful [24]. The dihedral Artin groups are of finite type. Faithful linear representations for finite type Artin groups are certain generalizations of the Lawrence-Krammer representation [8, 12].

It can be shown that the torus knot groups are discrete subgroups of $\tilde{SL}_2(\mathbb{R})$ (see e.g. [28]).

Proposition 3.8. *Let (G, S) with $S = \mathrm{Div}(\Delta)$ be a Garside system of spindle type, and let $X = \{a_1, \ldots, a_n\}$ be the set of atoms of S. Then G admits the group presentation*

$$\langle a_1, \ldots, a_n \mid a_1 \underline{\partial(a_1)} = a_2 \underline{\partial(a_2)} = \ldots = a_n \underline{\partial(a_n)} \rangle.$$

Proof. By induction over $\preceq$, it is easy to show that every Garside group G and every Garside monoid G^+ admits a *complemented presentation* in the sense of P. Dehornoy (see [10]), i.e. $G = \langle X \mid a_i w_{ij} = a_j w_{ji} \ \forall i \neq j \rangle$ for some $w_{kl} \in X^*$. with $\overline{w_{kl}} = a_k \backslash a_l$. In a Garside system of spindle type we have by Corollary 3.6 $a_k \backslash a_l = \partial(a_k)$ and $a_k \vee a_l = \Delta$ for all $1 \leq k \neq l \leq n$. □

Proposition 3.9. *Let (G, S) with $S = \mathrm{Div}(\Delta)$ be a Garside system of spindle type and X its set of atoms.*
(1) If $\Delta \preceq b$ then a word $D \in X^*$ for Δ is an infix of any word $w \in X^*$ with $\overline{w} = b$, i.e. there exist words $w_l, w_r \in X*$ s.t. $w \equiv w_l D w_r$.
(2) Let $b \in G^+ \setminus \Delta G^+$. Then there exists an unique word $w \in X^*$ representing b.
(3) Let $\Delta^q \preceq b$ for some $q \geq 0$. Then for every word $w \in X^*$ with $\overline{w} = b$ there exist $m, q_1, \ldots, q_m \in \mathbb{N}$, $u_1, D_1 \ldots, u_m, D_m, u_{m+1} \in X^*$ such that $\sum_{i=1}^m q_i = q$, $\overline{D_i} = \Delta^{q_i}$ $\forall i = 1, \ldots m$, and $w \equiv u_1 D_1 \cdots u_m D_m u_{m+1}$.

Proof. Let $w, w' \in X^*$ s.t. $\overline{w} = \overline{w'}$. Then w' can be transformed to w by application of positive relations only, i.e. by a sequence $\overline{w'} = \overline{w_1} = \ldots = \overline{w_m} = \overline{w}$ with $w_1, \ldots, w_m \in X^*$. Assume that a word for Δ is not an infix of w. Then, by Proposition 3.8, no relation is applicable and we conclude that w is the unique positive word representing b. Hence, we also get $\Delta \not\preceq \overline{w}$. Thus we

have proven (1) and (2).
The proof of (3) is rather technical and relies on (1): Consider a decomposition $w \equiv u_1 D_1 \cdots u_m D_m u_{m+1}$ such that $\overline{D_i} = \Delta^{q_i}\ \forall i = 1, \dots m$, and $\sum_{i=1}^m q_i$ is maximal among all such decompositions of the word w. Assume that $\sum_{i=j}^m q_i < q$. We will show that this leads to a contradiction. Define words $u'_j \equiv \tau^{\sum_{i=j}^m q_i}(u_j)$ for all $1 \leq j \leq m+1$, in particular $u'_{m+1} \equiv u_{m+1}$. Since

$$\overline{w} = \overline{u_1 D_1 \cdots u_m D_m u_{m+1}} = \Delta^{\sum_{i=j}^m q_i} \overline{u'_1} \cdots \overline{u'_{m+1}} \succeq \Delta^q,$$

we conclude that $\overline{u'_1} \cdots \overline{u'_{m+1}} \succeq \Delta$. By (1) it follows that an infix of the word $u'_1 \cdots u'_{m+1}$ represents Δ, i.e. there are two cases. Either there exists an $i_0 \in \mathbb{N}$ s.t. u'_{i_0} contains an infix representing Δ. Then so does u_{i_0}, and we conclude the decomposition $w \equiv u_1 D_1 \cdots u_{i_0} D_{i_0} \cdots u_m D_m u_{m+1}$ has not maximal $\sum_{i=1}^m q_i$. In the second case, there are numbers $i_0 < j_0 \in \mathbb{N}$ and words $u'^{(l)}_{i_0}, u'^{(r)}_{i_0}, u'^{(l)}_{j_0}, u'^{(r)}_{j_0}$ s.t. $u'^{(r)}_{i_0}$ is a postfix of u'_{i_0}, i.e. $u'_{i_0} \equiv u'^{(l)}_{i_0} u'^{(r)}_{i_0}$, $u'^{(l)}_{j_0}$ is a prefix of u'_{j_0}, i.e. $u'_{j_0} \equiv u'^{(l)}_{j_0} u'^{(r)}_{j_0}$, and $\overline{u'^{(r)}_{i_0} u'_{i_0+1} \cdots u'_{j_0-1} u'^{(l)}_{j_0}} = \Delta$. Decompose $u_{i_0} \equiv u^{(l)}_{i_0} u^{(r)}_{i_0}$ with $u^{(l),(r)}_{i_0} \equiv \tau^{-\sum_{i=i_0}^m q_i}(u'^{(l),(r)}_{i_0})$ and $u_{j_0} \equiv u^{(l)}_{j_0} u^{(r)}_{j_0}$ with $u^{(l),(r)}_{j_0} \equiv \tau^{-\sum_{i=j_0}^m q_i}(u'^{(l),(r)}_{j_0})$. Then $u^{(r)}_{i_0} D_{i_0} u_{i_0+1} D_{i_0+1} \cdots u_{j_0-1} D_{j_0-1} u^{(l)}_{j_0}$ represents

$$\Delta^{\sum_{i=i_0}^{j_0-1} q_i} \tau^{-\sum_{i=j_0}^m q_i} (\overline{u'^{(r)}_{i_0} u'_{i_0+1} \cdots u'_{j_0-1} u'^{(l)}_{j_0}}) = \Delta^{(\sum_{i=i_0}^{j_0-1} q_i)+1}.$$

Set $\tilde{D}_i \equiv D_i$ for $1 \leq i \leq i_0 - 1$, $\tilde{D}_{i_0} \equiv u^{(r)}_{i_0} D_{i_0} u_{i_0+1} D_{i_0+1} \cdots u_{j_0-1} D_{j_0-1} u^{(l)}_{j_0}$, and $\tilde{D}_j \equiv D_{j+j_0-i_0}$ for $i_0 + 1 \leq j \leq m - j_0 + i_0$. Then, for all $1 \leq i \leq m - j_0 + i_0$, $\overline{\tilde{D}_i} = \Delta^{\tilde{q}_i}$ for some $\tilde{q}_i \in \mathbb{N}$. Indeed, $\tilde{q}_i = q_i$ for $1 \leq i \leq i_0 - 1$, $\tilde{q}_{i_0} = (\sum_{i=i_0}^{j_0-1} q_i) + 1$, and $\tilde{q}_j = q_{j+j_0-i_0}$ for $i_0 + 1 \leq j \leq m - j_0 + i_0$. In addition, set $\tilde{u}_i = u_i$ for $1 \leq i \leq i_0 - 1$, $\tilde{u}_{i_0} = u^{(l)}_{i_0}$, $\tilde{u}_{i_0+1} = u^{(r)}_{j_0}$, and $\tilde{u}_j = u_{j+j_0-i_0-1}$ for $i_0 + 2 \leq j \leq m - j_0 + i_0 + 1$, and define $\tilde{m} := m - j_0 + i_0$. Then by construction

$$\tilde{u}_1 \tilde{D}_1 \cdots \tilde{u}_{\tilde{m}} \tilde{D}_{\tilde{m}} \tilde{u}_{\tilde{m}+1} \equiv u_1 D_1 \cdots u_m D_m u_{m+1} \equiv w$$

with $\sum_{i=1}^{\tilde{m}} \tilde{q}_i = (\sum_{i=1}^m q_i) + 1$ in contradiction with the maximality of $\sum_{i=1}^m q_i$.
□

3.5 Logspace normal forms for Garside systems of spindle type

3.5.1 Garside normal form

Proposition 3.10. *Let (G, S) with $S = \mathrm{Div}(\Delta)$ be a Garside system of spindle type. If G is a linear group, then the (left) Garside normal form of any element $b \in G$ can be computed by a logspace transducer.*

Proof. Let $X = \{a_1, \dots, a_n\}$ be the set of atoms of the given Garside system of spindle type $(G, \mathrm{Div}(\Delta))$. Assume that our input element is given as a word $w \in (X^{\pm})^*$. Recall that transforming a word v over another alphabet Y to a word $w \in (X^{\pm})^*$ can be done in logarithmic space. We will construct explicitly an L-computable function f over $(X^{\pm})^*$ that (on input w) returns

its (left) Garside normal form, i.e., a tuple $(p, s_1, \ldots, s_l) \in \mathbb{Z} \times (S \setminus \{1, \Delta\})^*$ such that $\overline{w} \overset{LNF}{=} \Delta^p s_1 \cdots s_l$. Indeed, f is the composition of four L-computable functions f_a, f_b, f_c, f_d.
(a) The function $f_a : (X^{\pm})^* \longrightarrow (X^{\pm})^*$ returns a freely reduced word w_a s.t $\overline{w_a} = \overline{w}$. Recall that free reduction in the rank n free group $\langle a_1, \ldots, a_n$ can be done in Logspace. Actually, step (a) is not really necessary, but we include it for convenience.
(b) The function $f_b : (X^{\pm})^* \longrightarrow \mathbb{N} \times X^*$ maps w_a to (k, w_b) s.t. $\overline{w_a} = \Delta^{-k}\overline{w_b}$. Here $k \geq 0$ is the number of occurences of negative generators in the word w_a. Let $w_a \equiv u_1 a_{i_1}^{-1} u_2 a_{i_2}^{-1} \cdots u_k a_{i_k}^{-1} u_{k+1}$ with $u_j \in X^*$ for $1 \leq j \leq k+1$. Replacing, for $1 \leq j \leq k$, each $a_{i_j}^{-1}$ by $\partial(a_{i_j})\Delta^{-1}$, and sliding the Δ^{-1}'s to the left, leads to the following word (equivalent to w_a):

$$\Delta^{-k}\tau^{-k}(u_1\partial(a_{i_1}))\tau^{-k+1}(u_1\partial(a_{i_2}))\cdots\tau^{-1}(u_1\partial(a_{i_k}))u_{k+1} \equiv \Delta^{-k}w_b.$$

It is easy to compute $f_b(w_a)$ in logarithmic space. First scan the word w_a and count the number of negative occurences of atoms, and output (and store) that number k whose bitlength is $O(\log |w_a|)$. Set a counter $j := k$. Scan again the word $w_a \equiv x_1 \cdots x_i \cdots x_{|w_a|}$ and do the following:

- If x_i is an atom, then output $\tau^{-j}(x_i)$.
- If x_i is the inverse of an atom, then output the letters of the unique word representing $\tau^{-k}(\partial(x_i^{-1})) \in S \setminus \{1, \Delta\}$, and decrement $j := j - 1$.

(c) The function $f_c : \mathbb{N} \times X^* \longrightarrow \mathbb{N} \times X^* \times \mathbb{N}$ maps (k, w_b) to (k, w_c, q) such that $\overline{w_b} = \overline{w_c}\Delta^q$. and $q \geq 0$ is maximal such that $\Delta^q \preceq \overline{w_b}$. We conclude that $\inf(\overline{w}) = q - k$. To find q we have to extract the whole "Δ-content" from the positive word w_b.
Since "nesting" might occur as e.g. in the word *babbaababb* representing the 4-th power of the Garside element in $T(2,3)$, we cannot use Proposition 3.9 (a) by removing one Δ after the other for a logspace algorithm. However we can utilize Proposition 3.9 (c) which states that there exists a decomposition $w \equiv u_1 D_1 \cdots u_m D_m u_{m+1}$ with $u_1, D_1 \ldots, u_m, D_m, u_{m+1} \in X^*$, $\overline{D_i} = \Delta^{q_i}$ $\forall i = 1, \ldots m$, and $\sum_{i=1}^m q_i = q$. Indeed, the following algorithm utilizes such a decomposition with m minimal.
For a monoid element $b \in G^+$, we define the so-called "norm" by $||b|| = \max\{|w| \mid w \in X^*, \overline{w} = b\}$, and for any element $b \in G$, denote the geodesic length (w.r.t. the generating set X) $\ell(b) = \ell_X(b) = \min\{|w| \mid w \in (X^{\pm})^*, \overline{w} = b\}$. Let $w_b \equiv x_1 \cdots x_i \cdots x_{|w_b|}$ with $x_i \in X$.

Algorithm 1 checks for each letter x_i whether it is the first letter in some word representing a Δ-power. Only letters x_i not belonging to some Δ-power word (according to that procedure) are printed, but as $\tau^{-q}(x_i)$ (here we mean the current q-value during the runtime of the algorithm) because we have to move Δ^q through such letters to the right. For checking whether $x_i \cdots x_j \Delta^{-q_1} \overset{?}{=} 1$ we need to call the oracle for the word problem (WP) which is so far known to be logspace computable only for linear (!) Garside groups of spindle type.
For all $D \in X^*$ with $\overline{D} = \Delta$, we have $\ell(\Delta) \leq |D| \leq ||\Delta||$ which implies $q_1\ell(\Delta) \leq |D^{(q_1)}| \leq q_1||\Delta||$ for all words $D^{(q_1)} \in X^*$ representing Δ^{q_1}. We conclude that if $x_i \cdots x_j = \Delta^{q_1}$ then

$$(j - i + 1)/||\Delta|| \leq q_1 \leq (j - i + 1)/\ell(\Delta),$$

```
Input: $(k, w_b) \in \mathbb{N} \times X^*$.
Output: $(k, w_c, q) \in \mathbb{N} \times X^* \times \mathbb{N}$
Print $k$ on output tape;
Initialize counter $q := 0$;
Initialize $i := 1$;
while $i \leq |w_b|$ do
    for $j := |w_b|$ to 1 by -1 do
        $q_{\min} := \lceil (j-i+1)/||\Delta||\rceil$; $q_{\max} := \lfloor (j-i+1)/\ell(\Delta)\rfloor$;
        for $q_1 := q_{\min}$ to $q_{\max}$ do
            Check whether $x_i \cdots x_j \Delta^{-q_1} \overset{!}{=} 1$ calling the WP-oracle ;
            if $x_i \cdots x_j \Delta^{-q_1} = 1$ then
                $i := j$; $q := q + q_1$;
                break $j$;
            end
        end
    end
    if $x_i \cdots x_j \Delta^{-q_1} \neq 1$ for all $q_1 \in [q_{\min}(i,j), q_{\max}(i,j)]$ $\forall j : i \leq j \leq k$
    then Print $\tau^{-q}(x_i)$ on output tape;
    $i := i + 1$;
end
Print $q$ on output tape.
```

Algorithm 1: Function $f_c : \mathbb{N} \times X^* \longrightarrow \mathbb{N} \times X^* \times \mathbb{N}$.

and we may choose integer test values for q_1 from that interval $[q_{\min}, q_{\max}]$.
(d) The last function $f_d : \mathbb{N} \times X^* \times \mathbb{N} \longrightarrow \mathbb{Z} \times (S \setminus \{1, \Delta\})^*$ maps (k, w_c, q) to $(q-k, s_1, \ldots, s_l)$ such that $\Delta^{-k}\overline{w_c}\Delta^q \overset{LNF}{=} \Delta^{q-k}s_1 \cdots s_l$. Since $\inf(\overline{w_c}) = q - k$ $\overline{w_c}$ lies in $G^+ \setminus \Delta G^+$ and w_c is according to 3.9 the unique representative of $\overline{w_c}$ and it is (in some sense) its left and right Garside normal form (which coincide). The same holds for its automorphic image $\tau^q(w_c)$ - recall that $\Delta^{-k}\overline{w_c}\Delta^q = \Delta^{q-k}\tau^q(\overline{w_c})$.
Therefore, we only have to read off the simple elements from the word $\tau^q(w_c)$. Let $w_c = x_1 \cdots x_{|w_c|}$ with $x_i \in X$ for all i. Furthermore, let $\underline{S}$ be the set of unique representatives of the elements of $S \setminus \{1, \Delta\}$. We scan the word w_c for consecutive subwords, and we print $s \in S$ (or equivalently its unique representative $\underline{s} \in \underline{S}$) on the output tape iff $\tau^q(x_i) \cdots \tau^q(x_j) = s$ $(i < j < |w_c|)$, but the word $x_i \cdots x_j x_{j+1}$ lies not in $\underline{S}$. Of course, we also print the last simple element $s_l = \tau^q(x_{i_l}) \cdots \tau^q(x_{|w_c|})$ (for some minimal i_l). □

3.5.2 Geodesic normal form

Definition 3.11. *Let (G, S) be a Garside system and X the set of atoms of S. (G, S) is called a Garside system with* HOMOGENOUS PRESENTATION *iff G (or/and G^+) admits a presentation of the form $\langle X \mid R_1^{(l)} = R_1^{(r)}, \ldots R_m^{(l)} = R_m^{(r)} \rangle$ with $R_i^{(l)}, R_i^{(r)} \in X^*$ and $|R_i^{(l)}| = |R_i^{(r)}|$ for all $1 \leq i \leq m$.*

For a Garside system (G, S) with homogeneous presentation all words $w \in X^*$ representing a monoid element $p \in G^+$ have the same word length $|w| =$

$\ell(p) = ||p||$.

Definition 3.12. *Let (G, S) be a Garside system with homogeneous presentation and X the set of atoms of S. We define a Reduction operations* red, Red : $(X^{\pm})^* \longrightarrow (X^{\pm})^*$. *Consider the unique decomposition of a word $w \in (X^{\pm})^*$ into a form $w \equiv \Delta^r w_1 \cdots w_s$ with $w_i \in (S \setminus \{1, \Delta\})^{\pm}$ such that s is minimal. Then we define* $\mathrm{red}(w)$ *as follows:*
(1) If $r \geq 0$ or $w_i \preceq 1$ then set $\mathrm{red}(w) \equiv w$.
(2) Otherwise, choose a $w_k \succeq 1$ whose wordlength is maximal among $\{w_i \in (0,1) \mid 1 \leq i \leq s$, and define

$$\mathrm{red}(w) \equiv \Delta^{r+1}\tau(w_1) \cdots \tau(w_{k-1}) w'_k w_{k+1} \cdots w_s$$

where $w'_k \in (X^-)^*$ is a word of minimal length s.t. $\Delta\overline{w'_k} = \overline{w_k}$.
Now, we set $\mathrm{Red}(w) \equiv \mathrm{red}^{|r|}(w)$.

Note that although neither $\mathrm{red}(w)$ nor $\mathrm{Red}(w)$ is uniquely determined from a given decomposition of w, the word-length $|\mathrm{Red}(w)|$ is uniquely determined and $|\mathrm{Red}(w)| \leq |w|$.

Remark. We restricted Definition 3.12 to Garside systems with homogeneous presentation, because for Garside systems with non-homogeneous presentation Reduction might increase word length, i.e, $|\mathrm{Red}(w)| \leq |w|$ does not hold. Consider for example a torus knot group $\langle a, b \mid a^p = b^q \rangle$ with $p + 2 < q$. Here, reduction of the word $w \equiv a^{-p}b$ leads to the word $\mathrm{Red}(w) \equiv b^{-q+1}$ with $|\mathrm{Red}(w)| = q - 1 > |w| = p + 1$.

Definition 3.13. *The* SHORTEST (OR GEODESIC) WORD PROBLEM *(w.r.t. the generating set X) is the following problem. Given a word $w \in (X^{\pm})^*$, find $\ell(w) = \ell_X(w)$ and return a geodesic representative, i.e. a word w_g s.t. $|w_g| = \ell(w)$ and $\overline{w_g} = \overline{w}$.*

Lemma 3.14. *Let (G, S) be a Garside system of spindle type with homogeneous presentation and X the set of atoms of S. Let w_{LNF} be a word in LNF, i.e. $w_{LNF} \equiv D^p w_1 \cdots w_l$ with $D, w_1, \ldots, w_l \in X^*$ such that $\overline{D} = \Delta$, $\overline{w_i} = s_i \in S$ and $\Delta^p s_1 \cdots s_l$ is a (left) Garside normal form.*
Then, for all words $w \in (X^{\pm})^*$ such that $\overline{w} = \overline{w_{LNF}}$,

$$|\mathrm{Red}(w_{LNF})| \leq |w|.$$

PROOF. We start from a decomposition of w, say $w \equiv x_1 \cdots x_{|w|}$, where x_i is either an atom or an inverse of an atom. Recall that $|\mathrm{Red}(w)| \leq |w|$. If there is a factor, say x_k, which is an inverse of a generator, change w to

$$w' \equiv \Delta^{-1}\tau^{-1}(x_1) \cdots \tau^{-1}(x_{k-1}) w'_k x_{k+1} \cdots x_{|w|}$$

where w'_k is a word of minimal length such that $\Delta^{-1}\overline{w'_k} = x_k$, and therefore $w'_k \in X^*$. Then clearly, $|\mathrm{Red}(w')| \leq |\mathrm{Red}(w)|$. Continue this process until we get a decomposition $\Delta^r c_1 \cdots c_m$ with $c_i \in S \setminus \{1, \Delta\}$. To prove the lemma, it suffices to show that the value $|\mathrm{Red}(\cdot)|$ does not increase for all decompositions that arise during the transformation of $\Delta^r c_1 \cdots c_m$ into the left-canonical decomposition $\Delta^p s_1 \cdots s_l$. Let $c_i c_{i+1}$ be transformed to $c'_i c'_{i+1}$. It suffices to show that

$$\max\{|c'_i|, |c'_{i+1}|\} \geq \max\{|c_i|, |c_{i+1}|\} \quad (*)$$

which implies $|\mathrm{Red}(\Delta^q c'_i c'_{i+1})| \leq |\mathrm{Red}(\Delta^q c_i c_{i+1})|$ for all $q \in \mathbb{Z}$. Note that in Lemma 5.1. of [19] $(*)$ is proven for all homogeneous Garside systems with $||\Delta|| = 3$ (which implies $1 \leq |c_i|, |c_{i+1}| \leq 2$).
By definition of leftgreedy decomposition, we have $c_i c_{i+1} = c'_i c'_{i+1}$ with $c'_{i+1} = \Delta \wedge (c_i c_{i+1})$, i.e. $\forall e : e \preceq c_i c_{i+1} \Rightarrow e \preceq c'_i$, in particular $c_i \preceq c'_i$. Write $c'_i = c_i d$. Since G is of spindle type, this implies $d \preceq \partial(c_i)$. By left cancellativity, we conclude that $c_{i+1} = d c'_{i+1}$. In case of $d = 1$ we get $c'_i = c_i$ and $c'_{i+1} = c_{i+1}$, and $(*)$ holds trivially. Now, assume $1 \neq d \preceq \partial(c_i)$. Recall that c_{i+1} is simple, i.e. $c_{i+1} = d c'_{i+1} \preceq \partial(c_i)\partial(\partial(c_i)) = \Delta$. Here we conclude that either $d = \partial(c_i)$ and $c'_{i+1} \preceq \partial(\partial(c_i))$, or $d \neq \partial(c_i)$ and $c'_{i+1} = 1$. In both cases we have $|c'_i| \geq \max\{|c_i|, |c_{i+1}|\}$, validating $(*)$. □

Theorem 3.15. *Let (G, S) be a Garside system of spindle type with homogeneous presentation and X the set of atoms of S. If G is a linear group then we can solve the geodesic word problem w.r.t X with a logspace transducer. Indeed, we may always find some unique w_g, i.e. a* GEODESIC NORMAL FORM *in Logspace.*

PROOF. Given an instance word $w \in (X^{\pm})^*$, recall that Lemma 3.14 already solves the shortest WP w.r.t. to $\ell_X(\cdot)$ by providing the geodesic $w_g = \mathrm{Red}(LNF(w))$. It remains to make the reduction procedure unique and to show that it can be accomplished in logspace. First, according to Proposition 3.10, computing the (unique) left normal form $\Delta^p s_1 \cdots s_l$ can be done with logarithmic space. Let $w_{LNF} = D^p w_1 \cdots w_l$ be the (unique for Garside systems *of spindle type*) LNF word, i.e., $D, w_1, \ldots, w_l \in X^*$ s.t. $\overline{D} = \Delta$ and $\overline{w_i} = s_i$ for all $1 \leq i \leq l$. Now, if $p \geq 0$, then clearly $\mathrm{Red}(w_{LNF}) = w_{LNF}$. Also if $p < 0$ and $|p| \geq l$, then $\mathrm{Red}(w_{LNF}) = D^{p+l}\tau^l(w'_1)\tau^{l-1}(w'_2) \cdots \tau(w'_{l-1})w'_l$ is already unique, where $w'_k \in (X^-)^*$ is a word of minimal length s.t. $\Delta\overline{w'_k} = \overline{w_k}$ (see Def. 3.12).
Therefore, one may assume that $p < 0$ and $|p| < l$. Define a threshold value as the greatest number $t \in \mathbb{N}$ s.t. at least p of the words w_k have length $\geq t$, i.e $|\{w_k \mid 1 \leq k \leq l,\ |w_k| \geq t\}| \geq p$. This value t can be computed in logspace by running though all values $t = 1, \ldots, ||\Delta|| - 1$, and for each t checking whether $|\{w_k \mid 1 \leq k \leq l,\ |w_k| \geq t\}| \geq p$. Clearly this can be done with the help of two logspace counters. Note that one may improve that procedure by running only through all possible values of $||s|| = \ell(s)$ for all $s \in S \setminus \{1, \Delta\}$.
Now, we make our Red-operation unique my applying the red-operation to the $|p|$ leftmost words w_k with $|w_k| \geq t$, i.e let $1 \leq i_1 < \ldots < i_p$ with $|w_{i_k}| \geq t$ $\forall 1 \leq k \leq p$ and $\sum_{k=1}^{p} i_k$ minimal. Then one may decompose (in logspace) the LNF word as $w_{LNF} \equiv D^p u_0 w_{i_1} u_1 \cdots w_{i_p} u_p$ for some $u_0, \ldots, u_p \in X^*$. Recall that $w'_k \in (X^-)^*$ is a word of minimal length s.t. $\Delta\overline{w'_k} = \overline{w_k}$. Then we output the following geodesic word

$$w_g \equiv \tau^{|p|}(u_0)\tau^{|p|-1}(w'_{i_1} \cdot u_1) \cdots \tau(w'_{i_{|p|-1}} \cdot u_{|p|-1}) \cdot w'_{i_{|p|}} \cdot u_{|p|},$$

which can easily be accomplished with logarithmic space only. □

4 Conjugacy in Garside groups of spindle type

4.1 Cycling and Decycling

Let us recall some further definitions and facts in Garside theory.

Definition 4.1. *Let (G, S) with $S = \mathrm{Div}(\Delta)$ be a Garside system. Recall that $\tau : G \to G$ is defined by $a \mapsto \Delta^{-1}a\Delta$. The* ORDER OF A GARSIDE SYSTEM, *denoted by* $\mathrm{ord}(G, S)$*, is the minimal number $n \in \mathbb{N}$ such that $\tau^n = \mathrm{id}$. Analogeously, one may define for any $b \in G$ the* ORDER OF THE ELEMENT $\mathrm{ord}(b)$ *(w.r.t. that Garside system) as the minimal number $n \in \mathbb{N}$ such that $\tau^r(b) = b$. By definition,* $\mathrm{ord}(b)$ *is always a divisor of* $\mathrm{ord}(G, S)$.

In particular, the following definitions are fundamental for the study of conjugacy in Garside groups.

Definition 4.2. *Let (G, S) with $S = \mathrm{Div}(\Delta)$ be a Garside system and b an element in G. We define the* SUMMIT INFIMUM, *the* SUMMIT SUPREMUM *and the* SUMMIT CANONICAL LENGTH *(or* SUMMIT GAP*) as the maximal (or minimal) possible value of these quantities inside the conjugacy class of b, i.e.,*

$$\inf{}_s(b) := \max\{\inf(b') \mid b' \sim b\}, \quad \sup{}_s(b) := \min\{\sup(b') \mid b' \sim b\},$$

and $cl_s(b) := \sup_s(b) - \inf_s(b)$. For $p \leq q \in \mathbb{N}$, define intervals $[p, q] := \{a \in G \mid \Delta^p \preceq a \preceq \Delta^q\}$. Then the SUPER SUMMIT SET $SSS(b)$ *of an element $b \in G$ is defined as the intersection of the conjugacy class $C(b)$ with the interval* $[\inf_s(b), \sup_s(b)]$.

Summit infimum, supremum and gap are conjugacy invariants. The SSS is a full invariant, i.e., $b_1 \sim b_2$ if and only if $SSS(b_1) = SSS(b_2)$. A representative $\tilde{b}$ in $SSS(b)$ may be found by iterative application of a finite number of *cycling* and *decycling* operations c, d. Let $\Delta^p s_1 \cdots s_l$ be the LNF of b. Then

$$c(b) := \Delta^p s_2 \cdots s_l \cdot \tau^{-p}(s_1), \text{ and } \quad d(b) := \Delta^p \tau^p(s_l) \cdot s_1 \cdots s_{l-1}.$$

For a general Garside system $(G, \mathrm{Div}(\Delta))$, according to an improvement [5] of the *cycling theorem* [13] one must "cycle" (resp. "decycle") at most $||\Delta|| - 1$ times in order to either increase inf (resp. decrease sup) or to be sure that it is already maximal (resp. minimal) for the given conjugacy class. For Garside systems of spindle type the situation is even much simpler. Elements in the SSS can be characterized as follows.

Proposition 4.3. *Let (G, S) with $S = \mathrm{Div}(\Delta)$ be a Garside system of spindle type and b an element in G with left Garside normal form $\Delta^p s_1 \cdots s_l$. Then*

$$b \in SSS(b) \quad if\ and\ only\ if \quad \tau^{-p}(s_1) \wedge \partial(s_l) = 1.$$

In this case (if $\tau^{-p}(s_1) \wedge \partial(s_l) = 1$) we call the element b RIGID.
In particular, if b is a not rigid then

$$(a) \quad \inf(d(b)) = \inf(b) + 1 \quad or \quad \sup(d(b)) = \sup(b) - 1.$$

Proof. ($\Rightarrow$): Let $s_1' := s_1 \wedge \tau^p(\partial(s_l))$ and write $s_1 = s_1's_1''$. The negation of the r.h.s is equivalent to $s_1' \neq 1$. Since G is of spindle type, we conclude that $s_1' = s_1$ or $s_1' = \partial(\tau^p(s_l))$. If $s_1' = s_1$ then $s_1 \preceq \partial(\tau^p(s_l))$, and therefore $s := \tau^p(s_l)s_1 \preceq \Delta$. We conclude that $d(b) = b^{s_l} = \Delta^p s s_2 \cdots s_{l-1}$ has supremum $\sup(d(b)) = p + l - 1 = \sup(b) - 1$, and therefore $b \notin SSS(b)$.
Now, if $s_1' = \partial(\tau^p(s_l))$ then $d(b) = \Delta^{p+1}s_1''s_2 \cdots s_{l-1}$, i.e. $\inf(d(b)) = \inf(b) + 1$. Again we conclude that $b \notin SSS(b)$. Obeserve that we proved here also the second claim.
($\Leftarrow$): Now let b be rigid, i.e. $s_1 \wedge \tau^p(\partial(s_l)) = 1$, and assume that $b \notin SSS(b)$. Then, according to the cycling theorem [13], after applying finally many cyclings/decyclings one should increase/decrease the infimum/supremum of b. Since $s_1 \wedge \tau^p(\partial(s_l)) = 1 \Leftrightarrow \tau^p(s_l)s_1 \wedge \Delta = \tau^p(s_l)$ the pair $(\tau^p(s_l), s_1)$ is left-greedy. Therefore $\Delta^p\tau^p(s_l) \cdot s_1 \cdots s_{l-1}$ is already the left (and right) Garside normal form of $d(b)$.

By induction over k we may show that

$$d^k(b) = \Delta^p\tau^p(s_{l-k+1} \cdots s_l)s_1 \cdots s_{l-k} \quad \text{for} \quad 1 \leq k \leq l.$$

In particular, $d^l(b) = \Delta^p\tau^p(s_1 \cdots s_l) = \tau^p(b)$. Let $r = \mathrm{ord}(b) \mid \mathrm{ord}(G)$, then $d^{lcm(p,r)l/p}(b) = \tau^{lcm(p,r)}(b) = b$ for $p > 0$ and $d^l(b) = b$ for $p = 0$. Since, the supremum can not increase by applying decyclings, we conclude that $\sup d^k(b) = \sup(b)$ for all $k \in \mathbb{N}$. Analogeously, one may show for cyclings that

$$c^k(b) = \Delta^p s_{k+1} \cdots s_l\tau^{-p}(s_1 \cdots s_k) \quad \text{for} \quad 1 \leq k \leq l, \quad c^l(b) = \tau^{-p}(b),$$

and $c^{lcm(p,r)l/p}(b) = \tau^{-lcm(p,r}(b) = b$. Since, the infimum can not decrease by applying cyclings, we conclude that $\inf c^k(b) = \inf(b)$ for all $k \in \mathbb{N}$. Applying the cycling theorem leads to the conclusion that b has already maximal infimum and minimal supremum inside its conjugacy class, i.e. $b \in SSS(b)$. □

For a Garside groups of spindle type, if an element lies not inside its SSS, then we may find an element with bigger/smaller infimum/supremum by only one decycling. A similar statement holds for cyclings.

Proposition 4.4. *Let (G, S) with $S = \mathrm{Div}(\Delta)$ be a Garside system of spindle type. Consider a non-rigid element $b \overset{LNF}{=} \Delta^p s_1 \cdots s_l$. If $\tau^p(s_l)s_1 \neq \Delta$, then $d(b) \in SSS(b)$.*

Proof. Again denote $s_1' := s_1 \wedge \tau^p(\partial(s_l))$. Since (G, S) is of spindle type and $s_1' \neq 1$ (b is non-rigid), we have two cases to consider.
(a) Either we have $s_1' = s_1$ which implies $s_1 \preceq \partial(\tau^p(s_l))$. Since $\tau^p(s_l)s_1 \neq \Delta$ we conclude that $\tau^p(s_l)s_1 \prec \Delta$. The left-greedy condition for the pair (s_{l-1}, s_l) is equivalent to $\tau^p(s_l) \wedge \partial(\tau^p(s_{l-1})) = 1$. We conclude that $\tau^p(s_l)s_1 \wedge \partial(\tau^p(s_{l-1})) = 1$. Since the LNF of $d(b)$ is $\Delta^p s s_2 \cdots s_{l-1}$ with $s = \tau^p(s_l)s_1$, this is exactly the rigidity condition for $d(b)$. By Proposition 4.3 we conclude that $d(b) \in SSS(b)$.
(b) The other case is $s_1' = \partial(\tau^p(s_l))$. Hence $\Delta \preceq \tau^p(s_l)s_1 = \Delta s_1''$ with $s_1 = s_1's_1''$, and

$$1 \neq s_1'' \preceq \partial(s_1') = \partial(\partial(\tau^p(s_l))) = \tau^{p+1}(s_l).$$

The left-greedy condition for the pair (s_{l-1}, s_l) is equivalent to $\tau^{p+1}(s_l) \wedge \partial(\tau^{p+1}(s_{l-1})) = 1$. We conclude that $d \wedge \partial(\tau^{p+1}(s_{l-1})) = 1$ for all positive left divisors $d \preceq \partial(\tau^{p+1}(s_{l-1}))$. In particular, this holds for $d = s_1''$, i.e. $s_1'' \wedge \partial(\tau^{p+1}(s_{l-1})) = 1$ Since the LNF of $d(b)$ is $\Delta^{p+1}s_1''s_2\cdots s_{l-1}$, this is exactly the rigidity condition for $d(b)$. By Proposition 4.3 we conclude that $d(b) \in SSS(b)$. □

Lemma 4.5. *Let (G,S) with $S = \operatorname{Div}(\Delta)$ be a Garside system of spindle type. Consider a non-rigid element $b \overset{LNF}{=} \Delta^p s_1 \cdots s_l$. Assume that the summit infimum is $\inf_s(b) = p + p_0$. Then, for $1 \leq k \leq p_0$,*

$$d^k(b) = \begin{cases} \Delta^{p+k}s_{k+1}\cdots s_{l-k}, & k < p_0 \\ \Delta^{p+p_0}s''_{p_0}s_{p_0+1}\cdots s_{l-p_0}, & k = p_0. \end{cases}$$

Proof. We prove by induction over k. Assume $k+1 < p_0$, then

$$d^{k+1}(b) \overset{IH}{=} d(\Delta^{p+k}s_{k+1}\cdots s_{l-k}) = \Delta^{p+k}\tau^{p+k}(s_{l-k})s_{k+1}\cdots s_{l-k-1}.$$

Since $k+1 < p_0$ we have $\inf(d^{k+1}(b)) \leq p+k+1 < p+p_0 = \inf_s(b)$, i.e. $d^{k+1}(b) \notin SSS(b)$. By Proposition 4.4 we conclude that $\tau^{p+k}(s_{l-k})s_{k+1} = \Delta$. Hence $d^{k+1}(b) = \Delta^{p+(k+1)}s_{(k+1)+1}\cdots s_{l-(k+1)}$.

Note that $d^k(b)$ may not be in $SSS(b)$. Indeed it is if and only if the pair $(\tau^{p+k}(s_{l-k}), s_{k+1})$ is left-greedy. If it is not, then we obtain an SSS-element by one more decycling which decreases the supremum.

In the case $k+1 = p_0$ we also may show by induction that

$$\begin{aligned} d^{p_0}(b) &= d(d^{p_0-1}(b)) \overset{IH}{=} d(\Delta^{p+p_0-1}s_{p_0}\cdots s_{l-p_0+1}) \\ &= \Delta^{p+p_0-1}\tau^{p+p_0-1}(s_{l-p_0+1})s_{p_0}s_{p_0+1}\cdots s_{l-p_0}. \end{aligned}$$

We conclude that $\Delta \preceq \tau^{p+p_0-1}(s_{l-p_0+1})s_{p_0}$ - otherwise $\inf_s(b) = p+p_0-1$ by Propositions 4.3 and 4.4. Write $\tau^{p+p_0-1}(s_{l-p_0+1})s_{p_0} = \Delta s''_{p_0}$ and we get the assertion.

Note that here are still two cases to consider. If $s''_{p_0} \neq 1$ then $d^{p_0}(b) \in SSS(b)$ according to Proposition 4.4. But if $s''_{p_0} = 1$ then $d^{p_0}(b)$ is in $SSS(b)$ if and only if the pair $(\tau^{p+p_0}(s_{l-p_0}), s_{p_0+1})$ is left-greedy. Now if that pair is not left-greedy, then we may obtain an SSS-element by one more decycling which decreases the supremum. □

4.2 Super Summit Set

Inside $SSS(b)$ (or $C(b)$) two elements can be conjugated by a sequence of conjugations by simple elements $s \in S$. Therefore, one may define a conjugacy graph whose vertices are the elements of a conjugacy class (or of $SSS(b)$) and the edges are conjugations by simple elements $s \in S$. In general, the SSS might be quite big. Certainly no polynomial bound (in $\ell(b)$) on the size (or even on the diameter) of the SSS graph is known. But in the case of Garside systems *of spindle type* the situation is fortunately simpler. Proposition 4.6 completely describes the structure of SSS graphs in Garside systems of spindle type.

Proposition 4.6. *Let (G,S) with $S = \operatorname{Div}(\Delta)$ be a Garside system of spindle type. Let $b \in SSS(b) \subset G$, and let $r = \operatorname{ord}(b)$ and $p = \inf(b)$.*
(a) Define $m = l \cdot lcm(p,r)/p$ for $p > 0$ and $m = l$ for $p = 0$. Then the SSS-graph of b is a quotient graph of the graph shown in Figure 1. Note that we only

$$\begin{tikzcd}
 & {} \arrow[d, "c"] & {} \arrow[d, "c"] & {} \arrow[d, "c"] & {} \arrow[d, "c"] & \\
{} \arrow[r, "\Delta"] & b \arrow[r, "\Delta"] \arrow[d, "c"] & \tau(b) \arrow[r, "\Delta"] \arrow[d, "c"] & {} \arrow[r, dotted, no head] \arrow[d, "c"] & \tau^{r-1}(b) \arrow[r, "\Delta"] \arrow[d, "c"] & {} \\
{} \arrow[r, "\Delta"] & c(b) \arrow[r, "\Delta"] \arrow[d, dotted, no head] & c(\tau(b)) \arrow[r, "\Delta"] \arrow[d, dotted, no head] & {} \arrow[r, dotted, no head] \arrow[d, dotted, no head] & c(\tau^{r-1}(b)) \arrow[r, "\Delta"] \arrow[d, dotted, no head] & {} \\
{} \arrow[r, "\Delta"] & c^{l-1}(b) \arrow[r, "\Delta"] \arrow[d, "c"] & c^{l-1}(\tau(b)) \arrow[r, "\Delta"] \arrow[d, "c"] & {} \arrow[r, dotted, no head] \arrow[d, "c"] & c^{l-1}(\tau^{r-1}(b)) \arrow[r, "\Delta"] \arrow[d, "c"] & {} \\
{} \arrow[r, "\Delta"] & \tau^{-p}(b) \arrow[r, "\Delta"] \arrow[d, dotted, no head] & \tau^{1-p}(b) \arrow[r, "\Delta"] \arrow[d, dotted, no head] & {} \arrow[r, dotted, no head] \arrow[d, dotted, no head] & \tau^{r-p-1}(b) \arrow[r, "\Delta"] \arrow[d, dotted, no head] & {} \\
 & {} & {} & {} & {} &
\end{tikzcd}$$

Figure 1: SSS-graph

draw cyclings $\alpha \xrightarrow{c} \beta$ *, but this always implies also a decycling* $\alpha \xleftarrow{d} \beta$ *. Also the graph is to be viewed as drawn on a torus.*
(b) We have the following bound on the size of the SSS: $|SSS(b)| \leq l \cdot \operatorname{ord}(b)$ *with* $l = cl(b)$*.*

Proof. (a) First we show that in Garside systems of spindle type the conjugacy graph of the SSS may be obtained by repeated cyclings (conjugation by $\tau^{-p}(s_1)$) and τ-automorphisms (conjugation by Δ) only. It is well known that positive simple conjugations suffice. For $s \in S$ and $b \overset{LNF}{=} \Delta^p s_1 \cdots s_l \in SSS(b)$, consider the conjugate $b^s = \Delta^{p-1}\partial^{2p-1}(s)s_1 \cdots s_l \cdot s$. We want to determine for which simple elements s, except for 1 and Δ, b^s also belongs to $SSS(b)$. For $b^s \in SSS(b)$, we have $\inf(b^s) = p$. Therefore $\Delta \preceq \partial^{2p-1}(s)s_1 \cdots s_l \cdot s$. we conclude that either (a1) $\Delta \preceq \partial^{2p-1}(s)s_1$ or (a2) $\Delta \preceq s_l s$.
(a1) If $\partial^{2p-1}(s)s_1 = \Delta s_1''$ with $s_1 = s_1's_1''$, we get $s_1' = \partial(\partial^{2p-1}(s)) = \tau^p(s) \Leftrightarrow s = \tau^{-p}(s_1')$. Hence

$$b^s = \Delta^{p-1}\partial^{2p-1}(\tau^{-p}(s_1'))s_1 \cdots s_l\tau^{-p}(s_1') = \Delta^p s_1''s_2 \cdots s_l\tau^{-p}(s_1').$$

It remains to show that $s_1'' = 1$, i.e. $s_1 = s_1'$. Then $b^s = b^{\tau^{-p}(s_1)} = c(b)$ is cycling.
Now, assume $s_1'' \neq 1$. Since $s_1' = \tau^p(s)$ and we consider $s \neq 1$, s_1' is a nontrivial left divisor of s_1. Hence the pair $(s_l, \tau^{-p}(s_1'))$ is left-greedy iff $(s_l, \tau^{-p}(s_1))$ is a left-greedy pair. And this is the case since b is rigid as an element inside $SSS(b)$. Also all other consecutive pairs in the product $s_1''s_2 \cdots s_l\tau^{-p}(s_1')$ are left-greedy except for the first. Indeed, if (s_1'', s_2) were left-greedy, then $cl(b^s) = l+1$ in contradiction with $b^s \in SSS(b)$. $\partial(s_1'') \wedge s_2 \neq 1$ implies either $\partial(s_1'') \wedge s_2 = \partial(s_1'')$ or $\partial(s_1'') \wedge s_2 = s_2$. In the first case we get $\partial(s_1'') \preceq s_2$, hence $\Delta \preceq s_1''s_2$ and $\inf(b^s) = p+1$ in contradiction to $b^s \in SSS(b)$. In the latter case we have $s_2 \preceq \partial(s_1'')$, i.e. $s_1''s_2 \in S$. Now, since $1 \neq s_1'' \preceq \partial(s_1')$, we have $\partial(s_1') \wedge (s_1''s_2) \neq 1$.

This again splits in two cases. $\partial(s_1') \wedge (s_1'' s_2)$ is either $\partial(s_1')$ or $s_1''s_2$. In the first case we have $\partial(s_1') \preceq s_1''s_2$, hence $\Delta \preceq s_1 s_2$ in contradiction to $\inf(b) = p$. In the latter case we get $s_1''s_2 \preceq \partial(s_1')$, hence $s_1 s_2 \preceq \Delta$ in contradiction with $\sup s_1 s_2 = 2$. Thus we have proven $s_1'' = 1$.

(a2) If $\Delta \preceq s_l s$ we write $s = s's''$ with $s' = \partial(s_l)$. Hence $s'' \preceq \partial(s') = \tau(s_l)$ and we write $s_l = s_l'' s_l'$ with $s'' = \tau(s_l'')$. Thus

$$\partial^{2p-1}(s) = \tau^{p-1}(\partial(s)) = \tau^{p-1}((s'')^{-1}\partial(s')) = \tau^{p-1}((s'')^{-1}\tau(s_l)) = \tau^p(s_l'),$$

and we obtain

$$b^s = \Delta^{p-1}\tau^p(s_l')s_1 \cdots s_{l-1}\Delta s'' = \tau[\Delta^p \tau^p(s_l')s_1 \cdots s_{l-1}s_l''].$$

Now if $s_l' = 1$ then $b^s = \tau(b)$, and if $s_l'' = 1$ then we get $b^s = \tau(d(b))$, i.e. decycling up to a τ-automorphism. Analogeously as in (a1) one may show that the case $s_1' \neq 1$ and $s_1'' \neq 1$ contradicts to b, b^s lying inside $SSS(b)$.

Thus we have shown that cycling, decycling and τ-operations suffice to enumerate $SSS(b)$. Recall that, for $r = \mathrm{ord}(b)$ and $p > 0$, we have $c^{lcm(p,r)l/p}(b) = \tau^{-lcm(p,r)}(b) = b$. Hence $c^{lcm(p,r)l/p-1}(b) = c^{-1}(b) = d(b)$ for $p > 0$, and $c^{l-1} = d(b)$ for $p = 0$. We conclude that cyclings and τ-operations suffice. Since decyclings are inverse cyclings, obviously also only decyclings and τ-operations suffice.

The assertion on the structure of the SSS-graph as well as claim (b) are simple corollaries of this result and the identities $c^l(b) = \tau^{-p}(b)$ and $\tau^r(b) = b$. □

Theorem 4.7. *Let (G, S) with $S = \mathrm{Div}(\Delta)$ be a Garside system of spindle type. If G is a linear group, then the conjugacy problem is solvable in logspace.*

Proof. Let X be the set of atoms of the Garside system of spindle type (G, S). We construct an L-computable function $f : (X^{\pm 1})^2 \longrightarrow \{\text{true/false}\}$ that on input (w, w') decides whether $\overline{w}$ and $\overline{w}'$ are conjugated in G. f is the composition of three L-computable functions f_a, f_b and f_c.

(a) Denote $S_{prop} = S \backslash \{1, \Delta\}$. The function $f_a : (X^{\pm 1})^2 \longrightarrow (\mathbb{Z} \times S_{prop})^2$ returns the left Garside normal forms of $\overline{w}$ and $\overline{w}'$, i.e., $(p, (s_1, \ldots, s_l), p', (s_1', \ldots, s_{l'}'))$ such that $\Delta^p s_1 \cdots s_l = \overline{w}$ and $\Delta^{p'} s_1' \cdots s_{l'}' = \overline{w}'$ for some $l, l' \in \mathbb{N}$.

(b) Given the LNF's of $\overline{w}$ and $\overline{w}'$, the function $f_b : (\mathbb{Z} \times S_{prop})^2 \longrightarrow (\mathbb{Z} \times S_{prop})^2$ computes the LNF's of elements $b, b' \in G$ such that $b \in SSS(\overline{w})$ and $b' \in SSS(\overline{w}')$. Consider, for example, the left normal form for $\overline{w}$, and assume that $\inf_s(\overline{w}) = p + p_0$. Lemma 4.5 implies then that $\tau^p(s_{l-p_0+1} \cdots s_l)s_1 \cdots s_{p_0-1}s_{p_0}' = \Delta^{p_0}$ for some $s_{p_0}' \preceq s_{p_0} = s_{p_0}'s_{p_0}''$. Furthermore (see proof of Lemma 4.5), if $s_{p_0}'' \neq 1$ then $\Delta^{p+p_0}s_{p_0}''s_{p_0+1} \cdots s_{l-p_0}$ provides a left normal decomposition of an element in $SSS(\overline{w})$, namely of $d^{p_0}(\overline{w})$. But if $s_{p_0}'' = 1$ then $d^{p_0}(\overline{w}) = \Delta^{p+p_0}s_{p_0+1} \cdots s_{l-p_0} \in SSS(\overline{w})$ if $(\tau^{p+p_0}(s_{l-p_0}), s_{p_0+1})$ is left-greedy, and

$$d^{p_0+1}(\overline{w}) = \Delta^{p+p_0}(\tau^{p+p_0}(s_{l-p_0})s_{p_0+1}) \cdot s_{p_0+2} \cdots s_{l-p_0-1} \in SSS(\overline{w})$$

if it is not, i.e. $(\tau^{p+p_0}(s_{l-p_0})s_{p_0+1}) \in S$. Therefore, given the LNF of $\overline{w}$, in order to compute the LNF of an element $b \in SSS(\overline{w})$ one may perform the following steps.

(b1) Check, for convenience whether $\overline{w}$ is rigid. If yes, return $\overline{w}$ - otherwise proceed with (b2).

(b2) Check for all $p_0 = l \operatorname{div} 2, \ldots, 1$ and for all prefixes $s'_{p_0} \preceq s_{p_0}$ whether $\tau^p(s_{l-p_0+1} \cdots s_l)s_1 \cdots s_{p_0-1}s'_{p_0} \overset{?}{=} \Delta^{p_0}$. This can be done by the given WP-oracle. Note that there exists a unique positive word for the proper simple elements s_{p_0}. When found compute $s''_{p_0} = (s'_{p_0})^{-1}s_{p_0}$.
(b3) If $s''_{p_0} \neq 1$ return $(p + p_0, s''_{p_0}, s_{p_0+1}, \ldots, s_{l-p_0})$. If $s''_{p_0} = 1$ then check whether $(\tau^{p+p_0}(s_{l-p_0}), s_{p_0+1})$ is left-greedy and return the LNF as explained above.
(c) The function $f_c : (\mathbb{Z} \times S_{prop})^2 \longrightarrow \{\text{true/false}\}$ checks whether $b' \in SSS(b)$. In abuse of notation $(p, (s_1, \ldots, s_l), p', (s'_1, \ldots, s'_{l'}))$ encodes now the LNF's of b and b', respectively. For convenience, we may first compare (p, l) with (p', l') and return false if they differ. If not we compare for all $j = 0, 1, \ldots, l-1$ and for all $i = 0, 1, \ldots, r-1$ the LNF's of $\Delta^{-p}b'$ with the LNF of $\Delta^{-p}c^j(\tau^i(b))$, i.e we compare $(s'_1, \ldots, s'_{l'})$ with $(\tau^i(s_{j+1}, \ldots, \tau^i(s_l), \tau^{i-p}(s_1), \ldots, \tau^{i-p}(s_j))$. If we found a match, we return true, otherwise false. □

Remark. It is easy to modify the algorithm in order to show that we may also solve the corresponding witness problem, namely the *conjugacy search problem* for linear Garside groups of spindle type, in logspace.

5 Normal forms related to HNN extensions

The commutator subgroup $[B_n, B_n]$ of the n-strand braid group is the kernel of the abelianizer map $\mathcal{A}$ which sends every Artin generator σ_i to $t = \sigma_1$, i.e., we have the following short exact sequence.

$$[B_n, B_n] \longrightarrow B_n \xrightarrow{\mathcal{A}} \langle t \rangle.$$

Indeed, $\langle \sigma_1 \rangle \leq B_n/[B_n, B_n]$ is obvious, and the commutator relations $\sigma_i\sigma_{i+1} = \sigma_{i+1}\sigma_i$ (for $i = 1, \ldots, n-2$) imply that $\sigma_1 = \sigma_2 = \ldots \sigma_{n-1}$ holds in $B_n/[B_n, B_n]$. Gorin and Lin computed the commutator subgroups $[B_n, B_n]$ for all n [18] (see also [6]).

For $n = 3$, $[B_3, B_3] \cong F_2$ is freely generated, e.g. by $a = [\sigma_2, \sigma_1^{-1}] = \sigma_1\sigma_2\sigma_1^{-2}$ and $b = [\sigma_1, \sigma_2] = \sigma_2\sigma_1^{-1}$. The $t^{\pm 1}$-action (by conjugation) on $\langle a, b \rangle$ is given by [6]:

$$t^{-1}a^{\pm 1}t = b^{\pm 1}, \quad t^{-1}b^{\pm 1}t = (ba^{-1})^{\pm 1}, \quad ta^{\pm 1}t^{-1} = (b^{-1}a)^{\pm 1}, \quad tb^{\pm 1}t^{-1} = a^{\pm 1}.$$

In particular, B_3 admits the following presentation as an HNN extension over F_2.

$$B_3 = \langle a, b, t \mid at = tb, \quad bt = tba^{-1} \rangle.$$

Now, given a word over $\{a, b, t\}^{\pm 1}$ representing a braid, we may bring all powers off t to the left.

Definition 5.1. *For every 3-strand braid $\beta \in B_3$ there exists an unique representation $t^p \cdot V(a, b)$ where $p \in \mathbb{Z}$ and $V = V(a, b)$ is a reduced group word over $\{a, b\}$. We call this representation the (left) HNN normal form of β.*

One can show that this normal form is L-computable. Since we already know B_3 has logspace normal form for any finite generating set, we omit the details for this specific normal form here.

5.1 HNN normal form for B_4

The 4-strand braid group B_4 admits a description as tower of HNN extensions of the 2-rank free group, namely [6]

$$F_2 = \langle a, b\rangle \subset [B_4, B_4] = \langle a, b, t_1, t_2\rangle \subset B_4 = \langle a, b, t_1, t_2, t\rangle$$

where $t_1 = \sigma_1\sigma_2\sigma_1^{-2} = [\sigma_2, \sigma_1^{-1}]$, $t_2 = \sigma_2\sigma_1^{-1} = [\sigma_1, \sigma_2]$, $a = \sigma_1\sigma_2\sigma_1^{-1}\sigma_3\sigma_2^{-1}\sigma_1^{-1} = [\sigma_2\sigma_1^{-1}, \sigma_3] = [\sigma_3\sigma_1^{-1}, \sigma_2^{-1}]$, and $b = \sigma_3\sigma_1^{-1} = [\sigma_2^{-1}\sigma_1^{-1}\sigma_3\sigma_2\sigma_3^2\sigma_1^{-2}, \sigma_1^{-1}]$.
The commutator subgroup $[B_4, B_4]$ is a semidirect product of the free group $\langle a, b\rangle$ with the free group $\langle t_1, t_2\rangle \cong [B_3, B_3]$. And $\langle a, b\rangle$ is the kernel of the homomorphism $B_4 \longrightarrow B_3$ [18] given by

$$t \mapsto t, \quad t_1 \mapsto t_1, \quad t_2 \mapsto t_2, \quad a \mapsto 1, \quad b \mapsto 1.$$

With respect to these *Gorin-Lin generators* the 4-strand braid group admits the following presentation [6].

$$B_4 = \langle a, b, t_1, t_2, t \mid t_1 t = t t_2 = t_2 t t_1, [a, t_1] = [b, t] = 1, b a t_2 = t_2 b\rangle.$$

From that presentation one may derive the $t_1^{\pm 1}$- and $t_2^{\pm 1}$-action on $\langle a, b\rangle$ and the $t^{\pm 1}$-action on a, b, t_1, and t_2. For the explicit equations we refer to [6]. The conjugation action implies that one may bring the $t^{\pm 1}$'s to the very left, and the $t_1^{\pm 1}$'s and $t_2^{\pm 1}$'s to the left of the a and b's.

Definition 5.2. *For every 4-strand braid β there exists an unique representation $t^p \cdot VW$ where $p \in \mathbb{Z}$ and $V = V(t_1, t_2)$, $W = W(a, b)$ are reduced group words over $\{t_1, t_2\}$, $\{a, b\}$, respectively. We call this representation the (left) HNN normal form of $\beta \in B_4$.*

In the following we show that the HNN normal form of a 4-strand braid is *not* an L-computable function.

Lemma 5.3. *Consider the family of 4-strand braids in $\langle a, b\rangle \subset B_4$ given by the action of t_1-powers upon b, i.e. the family $(b^{t_1^m})_{m\in\mathbb{N}}$. Let $|\cdot|_A$ denote the word length of the unique reduced free group word over the alphabet $A = \{a, b\}$. Then we have*

$$|(b)^{t_1^m}|_A = \Phi^{2m+1} - \Phi^{-(2m+1)} \quad \textit{where} \quad \Phi = (1+\sqrt{5})/2$$

denotes the golden ratio.

Proof. The $t_1^{\pm 1}$-action on $\langle a, b\rangle$ is given by

$$(a^{\pm 1})^{t_1} = b^{\pm 1},\ (b^{\pm 1})^{t_1} = (ba^{-1}b^2)^{\pm 1},\ (a^{\pm 1})^{t_1^{-1}} = (a^2b^{-1}a)^{\pm 1},\ (b^{\pm 1})^{t_1^{-1}} = a^{\pm 1}.$$

We observe that a reduced word for $b^{t_1^m}$ is a (semigroup) word over $\{a^{-1}, b\}$ only. Indeed, under the t_1-action b is mapped to $ba^{-1}b^2$ and a^{-1} to b^{-1} which is always cancelled with some letter b since each occurence of a^{-1} is always between two letters b. Denote by $\bar{\alpha}_m$ and β_m the number of occurences of letters a^{-1} and b, inside the unique reduced word representing $b^{t_1^m}$. We conclude that the following (recurrence) equations hold: $\bar{\alpha}_m = \beta_{m-1}$ (for $m \geq 1$) and

$$\beta_m = 3\beta_{m-1} - \bar{\alpha}_{m-1} = 3\beta_{m-1} = 3\beta_{m-1} - \beta_{m-2} \quad \forall m \geq 2.$$

Since $|b^{t_1^m}| = \bar{\alpha}_m + \beta_m$, also $(|b^{t_1^m}|_A)_{m\geq 0}$ satisfies the recurrence relation $|b^{t_1^m}|_A = 3|b^{t_1^{m-1}}|_A - |b^{t_1^{m-2}}|_A$ for $m \geq 2$ with initial values $|b|_A = 1$, $|b^{t_1}|_A = 4$.
Now, it is an easy exercise to show that $|(b)^{t_1^m}|_A = \Phi^{2m+1} - \Phi^{-(2m+1)}$. □

Remark. This sequence (starting with $1, 4, 11, 29, 76, 199, 521, 1364, \ldots$) is also known as *Bisection of Lucas sequence* (see OEIS A002878).

Theorem 5.4. *The HNN normal form in $t^p V(t_1, t_2) W(a, b)$ of a 4-strand braid is not logspace computable.*

Proof. Indeed, we show a slightly stronger result, namely that there exists no logspace transducer that computes the HNN normal form $V(t_1, t_2)W(a, b)$ of any 4-strand braid inside the commutator subgroup $[B_4, B_4]$. Indeed, the family of braids $(b^{t_1^m})_{m\in\mathbb{N}}$ has, according to Lemma 5.3, HNN normal forms of exponential length (w.r.t. the alphabet $\{t_1, t_2, a, b\}^{\pm 1}$) in m. Therefore, the time complexity for printing the HNN normal form of $b^{t_1^m}$ is not in P $= DTIME(poly(m))$. Since $DSPACE(\log(m)) = \mathrm{L} \subseteq \mathrm{P}$, we conclude that there exists no such logspace transducer. □

It may be shown that, for any braid $\beta \in B_4$, we can find in logspace $p \in \mathbb{Z}$ and a group word $U = U(t_1, t_2, a, b)$ such that $\beta = t^p\overline{U}$. The problem remains to find a unique form for U that could be computed in logspace.

Remark. One may show that several other classical normal forms for the 3-strand braid group can be also computed in logspace. In particular the following normal forms are L-computable.

- Alternating normal form of B_3 (see e.g. chapter VII in [9]).
- Rotating normal form of B_3 (see e.g. chapter VIII in [9]).
- σ-positive/negative geodesic normal form for nontrivial braids in B_3.
- Artin's combed normal form for P_3.

Furthermore, one may show that the natural normal form which we get from embedding B_3 in $Aut(F_3)$ is not L-computable. Details are given in an extended version of this article uploaded to `arXiv` [15][1].

References

[1] E. Artin. Theory of braids. *Ann. of Math. (2)*, 48:101–126, 1947.

[2] David Bessis. The dual braid monoid. *Ann. Sci. École Norm. Sup. (4)*, 36(5):647–683, 2003.

[3] Stephen J. Bigelow. Braid groups are linear. *J. Amer. Math. Soc.*, 14(2):471–486 (electronic), 2001.

[1] In this earlier version we used another terminology. In particular, we called Garside groups of spindle type *rigid Garside groups.*

[4] Joan Birman, Ki Hyoung Ko, and Sang Jin Lee. A new approach to the word and conjugacy problems in the braid groups. *Adv. Math.*, 139(2):322–353, 1998.

[5] Joan S. Birman, Ki Hyoung Ko, and Sang Jin Lee. The infimum, supremum, and geodesic length of a braid conjugacy class. *Adv. Math.*, 164(1):41–56, 2001.

[6] Leonid Bokut and Andrei Vesnin. Gröbner-Shirshov bases for some braid groups. *J. Symbolic Comput.*, 41(3-4):357–371, 2006.

[7] A. H. Clifford and G. B. Preston. *The algebraic theory of semigroups. Vol. I.* Mathematical Surveys, No. 7. American Mathematical Society, Providence, R.I., 1961.

[8] Arjeh M. Cohen and David B. Wales. Linearity of Artin groups of finite type. *Israel J. Math.*, 131:101–123, 2002.

[9] Patrick Dehornoy, Ivan Dynnikov, Dale Rolfsen, and Bert Wiest. *Ordering braids*, volume 148 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2008.

[10] Patrick Dehornoy and Luis Paris. Gaussian groups and Garside groups, two generalisations of Artin groups. *Proc. London Math. Soc. (3)*, 79(3):569–604, 1999.

[11] Volker Diekert, Jonathan Kausch, and Markus Lohrey. Logspace computations in Coxeter groups and graph groups. In *Computational and combinatorial group theory and cryptography*, volume 582 of *Contemp. Math.*, pages 77–94. Amer. Math. Soc., Providence, RI, 2012.

[12] François Digne. On the linearity of Artin braid groups. *J. Algebra*, 268(1):39–57, 2003.

[13] Elsayed A. El-Rifai and H. R. Morton. Algorithms for positive braids. *Quart. J. Math. Oxford Ser. (2)*, 45(180):479–497, 1994.

[14] Murray Elder, Gillian Elston, and Gretchen Ostheimer. On groups that have normal forms computable in logspace. *J. Algebra*, 381:260–281, 2013.

[15] Murray Elder and Arkadius Kalka. Logspace computations for rigid Garside groups. Arxiv:1310.0933.

[16] David B. A. Epstein, James W. Cannon, Derek F. Holt, Silvio V. F. Levy, Michael S. Paterson, and William P. Thurston. *Word processing in groups.* Jones and Bartlett Publishers, Boston, MA, 1992.

[17] Eddy Godelle. Parabolic subgroups of Garside groups. *J. of Algebra*, 317:1–16, 2007.

[18] E. A. Gorin and V. Ja. Lin. Algebraic equations with continuous coefficients, and certain questions of the algebraic theory of braids. *Mat. Sb. (N.S.)*, 78 (120):579–610, 1969.

[19] Eun Sook Kang, Ki Hyoung Ko, and Sang Jin Lee. Band-generator presentation for the 4-braid group. *Topology Appl.*, 78(1-2):39–60, 1997. Special issue on braid groups and related topics (Jerusalem, 1995).

[20] Daan Krammer. Braid groups are linear. *Ann. of Math. (2)*, 155(1):131–156, 2002.

[21] Eon-Kyung Lee. A positive presentation for the pure braid group. *Journal of the Chungcheong Mathematical Society*, 23(3):555–561, 2010.

[22] Richard J. Lipton and Yechezkel Zalcstein. Word problems solvable in logspace. *J. Assoc. Comput. Mach.*, 24(3):522–526, 1977.

[23] Markus Lohrey and Nicole Ondrusch. Inverse monoids: decidability and complexity of algebraic questions. *Inform. and Comput.*, 205(8):1212–1234, 2007.

[24] Wilhelm Magnus and Ada Peluso. On a theorem of V. I. Arnol′d. *Comm. Pure Appl. Math.*, 22:683–692, 1969.

[25] Matthieu Picantin. *Petites groupes gaussiens*. PhD thesis, Université de Caen, 2000.

[26] Matthieu Picantin. The conjugacy problem in small Gaussian groups. *Comm. Algebra*, 29(3):1021–1039, 2001.

[27] Hans-Ulrich Simon. Word problems for groups and contextfree recognition. In *Fundamentals of computation theory (Proc. Conf. Algebraic, Arith. and Categorical Methods in Comput. Theory, Berlin/Wendisch-Rietz, 1979)*, volume 2 of *Math. Res.*, pages 417–422. Akademie-Verlag, Berlin, 1979.

[28] Valdemar Tsanov. Triangle groups, automorphic forms, and torus knots. *L'Enseignement Mathématique*, 59(3-4):73–113, 2013.

[29] Svetla Vassileva. The conjugacy problem in wreath products is decidable in log-space. April 2013. AMS Sectional Meeting, Boston College.

E-mail addresses: murrayelder@gmail.com, arkadius.kalka@rub.de