ON THE SIMULTANEOUS CONJUGACY PROBLEM IN GARSIDE GROUPS

ARKADIUS KALKA, BOAZ TSABAN, AND GARY VINOKUR

Abstract. We solve the simultaneous conjugacy problem in Garside groups by means of an effectively computable invariant. This invariant generalizes the one-dimensional notion of super summit set of a conjugacy class. One key ingredient of our solution is the introduction of a provable high-dimensional version of the Birman–Ko–Lee cycling theorem. The complexity of this solution is a small degree polynomial in the cardinalities of our generalized super summit sets and the input parameters. Computer experiments suggest that the cardinality of this invariant, for a list of order $N$ independent elements of Artin’s braid group $B_N$, is generically close to 1.

1. Introduction

In 1911, Dehn formulated three fundamental algorithmic problems concerning groups: the Word Problem, the Conjugacy Problem, and the Group Isomorphism Problem. The Word Problem is that of deciding whether two words in given symmetric generators of a group represent the same element or, equivalently, whether a word in these generators represents the identity element. The Conjugacy Problem is that of deciding whether two group elements are conjugate. The Conjugacy Search Problem version of this problem is to find, given two conjugate group elements, a witness conjugator.

Throughout, for group elements $g$ and $x$ in $G$, we use the notation $g^x := x^{-1}gx$. The Simultaneous Conjugacy Problem (SCP) generalizes the Conjugacy Problem: $r$-tuples $(g_1, \ldots, g_r)$ and $(h_1, \ldots, h_r)$ of elements of a group $G$ are conjugate if there is an element $x \in G$ such that

$$(g_1, \ldots, g_r)^x := (g_1^x, \ldots, g_r^x) = (h_1, \ldots, h_r).$$

The (r-dimensional) SCP is that of deciding whether two $r$-tuples of group elements are conjugate. The definition of the Search SCP is analogous.

An external motivation for studying the SCP comes from cryptography. The security of a number of cryptographic protocols reduces to the Search SCP in Artin’s braid groups. In Section 2, we provide such reductions for prominent examples. In the case where $G$ is a braid group, there are by now polynomial-time, ad-hoc solutions of the problems that characterize the security of these protocols [5, 32, 2]. These solutions do not address the (formally harder) SCP. Moreover, for the lack of a general, polynomial-dimension representation theory for

Key words and phrases. Conjugacy problem, simultaneous conjugacy, Garside group, Braid group, minimal simple element, Birman-Ko-Lee presentation, summit set, super summit set.
Garside groups, the known solutions do not generalize to arbitrary Garside groups. From a heuristic point of view, practically all braid-based cryptographic protocols proposed thus far, including ones hitherto not cryptoanalyzed, are based on the difficulty of the SCP. In order to understand the potential of braid groups in cryptography, we must address the full-fledged SCP.

A number of computational problems in braid groups reduce to the SCP. For example, Dehornoy’s Shifted Conjugacy Problem \[8\] reduces to the SCP via a reduction to the Subgroup Conjugacy Problem for the braid group \(B_{N-1}\) in \(B_N\) \[21\]. More generally, the Subgroup Conjugacy Problem for \(B_M\) in \(B_N\) \((M < N)\) is reducible to the SCP \[16\]. In a sequel paper \[23\], we show that the Double Coset Problem for parabolic subgroups of braid groups reduces to the SCP. In particular, the present paper leads to the first solution of the Double Coset Problem.

Our main result is a deterministic, effective solution to the decision and search version of the SCP, in arbitrary Garside groups. Earlier, Lee and Lee provided a solution in Artin’s braid groups \[26\], that extends to Garside groups with weighted presentations. In contrast to the Lee–Lee solution, our solution provides a finite invariant of the conjugacy class of an \(r\)-tuple. Experimental results, in braid groups, show a considerable improvement over the earlier solution. We conclude this paper with open problems and indications for additional applications.

2. Reductions of some computational problems to the SCP

In the original instantiations of the problems below, the group \(G\) was Artin’s braid group. The protocols, problems and reductions in this section apply in arbitrary finitely generated groups. We assume, for simplicity, that each mentioned group is provided in terms of a generating set of cardinality \(r\).

The security of the Braid Diffie–Hellman protocol \[25\], is based on the difficulty of the following problem.

**Problem 2.1.** Let \(A\) and \(B\) be subgroups of a group \(G\) with \([A,B] = 1\), and let \(g \in G\) be given. Given a pair \((g^a, g^b)\), for \(a \in A\) and \(b \in B\), find \(g^{ab}\).

Problem 2.1 reduces to the Search SCP. Indeed, let \(b_1, \ldots, b_r\) be generators of the subgroup \(B\). Find an element \(\tilde{a} \in G\) such that

\[(g, b_1, \ldots, b_r)^{\tilde{a}} = (g^a, b_1, \ldots, b_r).
\]

Then \([\tilde{a}, B] = 1\), and

\[g^{ab} = (g^a)^b = (g^{\tilde{a}})^b = g^{\tilde{a}b} = g^{b\tilde{a}} = (g^{\tilde{a}})^b = (g^b)^{\tilde{a}},\]

which we can compute, having \(g^b\) and \(\tilde{a}\).

The Double Coset protocol \[6\] is a generalization of the Braid Diffie–Hellman protocol. Its security is based on the difficulty of the following problem.
Problem 2.2. Let $A_1, A_2, B_1$ and $B_2$ be subgroups of a group $G$ with $[A_1, B_1] = [A_2, B_2] = 1$, and let $g \in G$ be given. Given a pair $(a_1 ga_2, b_1 gb_2)$, for $a_i \in A_i$ and $b_i \in B_i$ for $i = 1, 2$, find $a_1 b_1 g a_2 b_2$.

To see that Problem 2.2 reduces to the Search SCP, let $b_1, \ldots, b_r$ be generators of the subgroup $B_i$ for $i = 1, 2$. For elements $b \in B_1$ of our choice, since $[a_1, B_1] = 1$, we know the element $b^{g a_2} = b^{a_1 g a_2}$. Find an element $\tilde{a}_2 \in G$ such that

$$(b_{11}^g, \ldots, b_{1r}^g, b_{21}, \ldots, b_{2r})^{\tilde{a}_2} = (b_{11}^{g a_2}, \ldots, b_{1r}^{g a_2}, b_{21}, \ldots, b_{2r}).$$

Then $[\tilde{a}_2, B_2] = 1$, and $[(g a_2)(g \tilde{a}_2)^{-1}, B_1] = 1$. Compute $\tilde{a}_1 = (a_1 g a_2)(g \tilde{a}_2)^{-1} = a_1(g a_2)(g \tilde{a}_2)^{-1}$. Then $[\tilde{a}_1, b_1] = 1$, and thus

$$\tilde{a}_1(b_1 gb_2)\tilde{a}_2 = b_1\tilde{a}_1 g \tilde{a}_2 b_2 = b_1 a_1 ga_2 b_2 = a_1 b_1 g a_2 b_2,$$

which we can compute from $b_1 gb_2$, $\tilde{a}_1$ and $\tilde{a}_2$.

The security of the Commutator protocol [1] is based on the difficulty of the following problem.

Problem 2.3. Let $A$ and $B$ be subgroups of a group $G$. Given $A^b$ and $B^a$, for $a \in A$ and $b \in B$, find the commutator $[a, b]$.

The reducibility of Problem 2.3 to the SCP remains open. Generically, the centralizer of subgroups of the braid group is equal to the center of the entire group, which is known. Problem 2.3 reduces to the conjunction of the Search SCP and computing the centralizer of a finite set of elements: Let $a_1, \ldots, a_r, b_1, \ldots, b_r, c_1, \ldots, c_r$ and $d_1, \ldots, d_r$ be generators of the subgroup $A$, $B$ and their centralizers $C(A)$ and $C(B)$, respectively. Find elements $\tilde{a}, \tilde{b} \in G$ such that

$$(a_1, \ldots, a_r, d_1, \ldots, d_r)^{\tilde{b}} = (a_1^b, \ldots, a_r^b, d_1, \ldots, d_r).$$

and

$$(b_1, \ldots, b_r, c_1, \ldots, c_r)^{\tilde{a}} = (b_1^a, \ldots, b_r^a, c_1, \ldots, c_r).$$

Then $a^{\tilde{b}} = a^b$. Also, $\tilde{a}a^{-1} \in C(B)$ and $[\tilde{b}, C(B)] = 1$. In particular, $[\tilde{b}, \tilde{a}a^{-1}] = 1$. Compute

$$\tilde{a}^{-1}\tilde{b}^{-1}\tilde{a}\tilde{b} = \tilde{a}^{-1}\tilde{b}^{-1}(\tilde{a}a^{-1})\tilde{a}\tilde{b} = \tilde{a}^{-1}(\tilde{a}a^{-1})\tilde{b}^{-1}\tilde{a}\tilde{b} = a^{-1}\tilde{a}^b = a^{-1}a^b = [a, b].$$

Finally, the security of the Centralizer protocol [30] is based on the following problem.

Problem 2.4. Let $g, a_1, b_2 \in G$, $C \leq C(a_1)$, $D \leq C(b_2)$, $a_2 \in D$ and $b_1 \in C$. Given $g, C$, $D$, $a_1 ga_2$ and $b_1 gb_2$, compute $a_1 b_1 g a_2 b_2$.

Problem 2.4 reduces to the conjunction of the Search SCP and computing the centralizer of a finite set of elements: Let $c_1, \ldots, c_r$ and $e_1, \ldots, e_r$ be generators of the subgroup $C$ and $C(D)$, respectively. For each $c \in C$, we can compute $c^{g a_2} = c^{g a_2}$. Find $\tilde{a}_2 \in G$ such that

$$(c_1^g, \ldots, c_r^g, e_1, \ldots, e_r)^{\tilde{a}_2} = (c_1^{g a_2}, \ldots, c_r^{g a_2}, e_1, \ldots, e_r).$$
Let $\bar{a}_1 = (a_1 ga_2)(\tilde{g}a_2)^{-1}$. Then $\bar{a}_1 = a_1((ga_2)(\tilde{g}a_2)^{-1}) \in C(C)$, and thus $[\bar{a}_1, b_1] = 1$. Also, $[\bar{a}_2, C(D)] = 1$ and $b_2 \in C(D)$. Thus, $[\bar{a}_2, b_2] = 1$. It follows that

$$\bar{a}_1(b_1 gb_2)\bar{a}_2 = b_1\bar{a}_1 gb_2 b_2 = b_1 a_1ga_2 b_2 = a_1 b_1 ga_2 b_2.$$ 

3. Background on Garside groups

Garside groups [11] [28] form a generalization of braid groups where Garside’s solution to the conjugacy problem in braid groups applies. Many examples of Garside groups are known [10]. These include, in addition to Artin’s braid groups, all Artin groups of finite type and torus link groups [19].

Let $M$ be a monoid. An element $a \in M$ is a left divisor of an element $b \in M$ ($a \preceq b$) if $b \in aM$. An element $a$ is right divisor of an element $b$ ($b \succeq a$) if $b \in Ma$. It is a divisor of $b$ if it is a left or a right divisor of $b$. Div($b$) is the set of divisors of $b$. An element $b \in M$ is balanced if the left and right divisors of $b$ coincide.

A monoid $M$ is Noetherian if for each element $a \in M$ there is a natural number $n$ such that $a$ cannot be expressed as the product of more than $n$ nonidentity elements. An element $a \neq 1$ in $M$ is an atom if $a = bc$ implies $b = 1$ or $c = 1$. A set generates a Noetherian monoid $M$ if and only if it includes all atoms of $M$.

Let $M$ be a finitely generated, cancellative Noetherian monoid. The relations $\preceq$ and $\succeq$ are partial orders, and every element of $M$ admits only finitely many left and right divisors [11]. An element $m \in M$ is a right lcm of $a$ and $b$ if $a, b \preceq m$, and whenever $a \preceq c$ and $b \preceq c$, we have $m \preceq c$. The definition of left lcm is symmetric, using the relation $\succeq$. Right and left lcms of pairs $a$ and $b$ are unique, and are denoted $a \lor b$ and $a \land b$, respectively. If $a \lor b$ exists, then there is a unique element $c$ such that $a \lor b = ac$. This element $c$ is the right complement (or residue) of $a$ in $b$, denoted by $a \backslash b$. We define the left complement symmetrically. In particular, we have $a \lor b = a(a \backslash b) = b(b \backslash a)$, and $a \land b = (b/a)a = (a/b)b$.

A monoid $M$ is Gaussian if it is Noetherian, cancellative, and every pair of elements $a, b \in M$ admits a right and a left lcm. Let $M$ be a Gaussian monoid. For every pair of elements $a$ and $b$, the set of common left divisors of $a$ and $b$ is finite and admits a right lcm, which is therefore the greatest common left divisor of $a$ and $b$, denoted by $a \land b$. The definition of right $gcd$ $a \land b$ is symmetric. A Gaussian monoid $M$ is a lattice with respect to the relations $\preceq$ and $\succeq$. The groups of right fractions and left fractions of the monoid $M$ coincide, and form the group of fractions of $M$. The monoid $M$ embeds in this group.

**Definition 3.1.** A Garside group is a group $G$ equipped with a finite subset $S$ and an element $\Delta$ such that the monoid $G^+$ generated by $S$ is Gaussian with $G$ is its group of fractions, $\Delta \in G^+$ is a balanced element, and $S = \text{Div}(\Delta)$.

In this case, we say that $G^+$ is a Garside monoid, $\Delta$ the Garside element, and the elements of $S$ are the simple elements of $G$.

Let $G$ be a Garside group. There may be several choices of $S$ and $\Delta$ witnessing that, and we always assume, tacitly, that $S$ and $\Delta$ are fixed in the background. The set $S$ is closed under the operators $\setminus, /, \lor, \land$ and $\land$. Indeed, $S$ is the closure of the atoms of $G^+$ under
are the maximal elements \(a, b\) of \(G\) defined by the operators \(\partial: a \mapsto a \backslash \Delta\) 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 \(\tau\) denotes the inner automorphism of \(G\) defined by \(a \mapsto \Delta^{-1}a\Delta\).

The partial orders \(\leq\) and \(\geq\) on \(G^+\) extend naturally to partial orders on the whole Garside group \(G\). Define a partial order on \(G\) by \(a \leq b\) if there are \(c, c'\in G^+\) such that \(b = cac'\). For elements \(a, b \in G\) and \(k \in \mathbb{Z}\), we have \(a \leq \Delta^k \leq b\) if and only if \(b \geq \Delta^k \geq a\) if and only if \(a \leq \Delta^k \leq b\). For \(m, n \in \mathbb{Z}\), define the interval \([m, n] := \{a \in G: \Delta^m \leq a \leq \Delta^n\}\).

The infimum and the supremum of an element \(a \in G\), denoted \(\inf a\) and \(\sup a\), respectively, are the maximal \(m \in \mathbb{Z}\) and the minimal \(n \in \mathbb{Z}\) such that \(a \in [m, n]\). The canonical length of \(a\), denoted \(\text{cl}(a)\), is the difference \(\sup a - \inf a\).

Let \(G\) be a Garside group. The (left) normal form of an element \(a \in G^+\) is a unique decomposition \(a = s_1 \cdots s_t\) such that \(s_i = \Delta \land (s_i \cdots s_t) \in S\) for all \(i\), and \(s_t \neq 1\). The length \(l\) of this decomposition equals \(\sup a\). The (left) normal form of a general element \(a\) is obtained by expressing \(a = \Delta^{\inf a}\) for the unique element \(a_+ \in G^+\), and decomposing \(a_+\) to its (left) normal form.

4. THE BASIC SOLUTION

Picantin’s solution for the Conjugacy Problem in Garside groups \([28]\) extends to the SCP by choosing the appropriate coordinate-wise generalization of the involved notions. For a natural number \(r\), the standard partial order \(\leq\) of \(\mathbb{Z}\) extends to a partial order of \(\mathbb{Z}^r\) coordinate-wise: for elements \(p = (p_1, \ldots, p_r)\) and \(q = (q_1, \ldots, q_r)\) in \(\mathbb{Z}^r\), we define \(p \leq q\) if \(p_i \leq q_i\) for all \(i = 1, \ldots, r\). For an \(r\)-tuple \(a = (a_1, \ldots, a_r)\) of elements of a Garside group \(G\), let

\[
a^G := \{a^g : g \in G\} = \{(a_1^g, \ldots, a_r^g) : g \in G\},
\]

the (simultaneous) conjugacy class of \(a\). Define

\[
\inf a := (\inf a_1, \ldots, \inf a_r);
\]

\[
\sup a := (\sup a_1, \ldots, \sup a_r).
\]

For \(p, q \in \mathbb{Z}^r\) with \(p \leq q\), define the following interval:

\[
[p, q] = \{a \in G^r : p \leq \inf a \text{ and } \sup a \leq q\}
\]

\[
= \{(a_1, \ldots, a_r) \in G^r : p_i \leq \inf a_i \text{ and } \sup a_i \leq q_i \text{ for all } i = 1, \ldots, r\}.
\]

**Lemma 4.1.** Let \(G\) be a Garside group, and \(r\) be a natural number. For all tuples \(p, q \in \mathbb{Z}^r\), the interval \([p, q]\) is finite.

**Proof.** The one-dimensional case \((r = 1)\) is due to Picantin \([28]\). In the case \(r > 1\), the interval

\[
[p, q] = [p_1, q_1] \times \cdots \times [p_r, q_r]
\]
is finite, as a product of finitely many one-dimensional intervals.

Lemma 4.2 (28, Lemma 2.3). Let $G$ be a Garside group. Then $\Delta \leq \alpha \beta$ implies $\Delta \leq \alpha (\beta \wedge \Delta)$, for all $\alpha, \beta \in G^+$.

Since the set of simple elements $S$ in a Garside group is finite and the automorphism $\tau: S \to S$ a bijection, there is a natural number $k$ such that $\tau^k$ is the identity map. Then the element $\Delta^k$ is in the center of $G$. Assume that elements $a, c \in G$ are conjugate by an element $x \in G$. Then, for a large enough natural number $m$, the elements $a$ and $c$ are also conjugate by the element $x^+ := \Delta^m k x \in G^+$. It follows that the same holds for tuples $a, c \in G^r$, for an arbitrary dimension $r$.

Theorem 4.3 (Simultaneous Convexity). Let $G$ be a Garside group, $p, q \in \mathbb{Z}^r$, and $a, c \in [p, q]$. Assume that $c = a^x = a^{x^{-1}}$ for elements $x, \tilde{x} \in G^+$. Let $x_1 := \Delta \wedge x$ and $\tilde{x}_1 := x \wedge \tilde{\Delta}$, the leftmost and rightmost simple factors of $x$, respectively. Then $a^{x_1}, a^{\tilde{x}_1} \in [p, q]$.

Proof. The case $r = 1$ is due to Picantin [28, Propositions 3.2]. It follows that, for each $i = 1, \ldots, r$, we have $a_i^{x_1}, a_i^{\tilde{x}_1} \in [p_i, q_i]$, and thus $a^{x_1}, a^{\tilde{x}_1} \in [p, q]$. □

The one-dimensional version of the following corollary is due to Picantin [28, Propositions 3.3].

Corollary 4.4. Let $G$ be a Garside group, and $p, q \in \mathbb{Z}^r$. For all conjugate tuples $a, c \in [p, q]$, there are a natural number $l$, tuples $v_0, v_1, \ldots, v_l \in [p, q]$, and simple elements $s_1, \ldots, s_l \in G$ such that $v_0 = a$, $v_l = c$, and $v_i s_i^{-1} = v_{i-1}$ for $i = 1, \ldots, l$; schematically:

$$a \xrightarrow{s_1} v_1 \xrightarrow{s_2} v_2 \xrightarrow{s_3} \cdots \xrightarrow{s_{l-1}} v_{l-1} \xrightarrow{s_l} c.$$  

Proof. There is an element $x \in G^+$ such that $a^x = c$. The assertion follows by applying the Simultaneous Convexity Theorem 4.3 sup $x$ times. □

We obtain an extension of Picantin’s result [28, Corollary 3.4] to the simultaneous setting.

Theorem 4.5. The SCP in Garside groups is solvable.

Proof. Given tuples $a, c \in G^r$, fix tuples $p, q \in \mathbb{Z}^r$ with $p \leq \inf a, \inf c$ and sup $a, \sup c \leq q$. Then $a, c \in [p, q]$, and the elements $a$ and $c$ are conjugate if and only if $c \in a^G \cap [p, q]$.

By Lemma 4.1, the set $a^G \cap [p, q]$ is finite. By Corollary 4.4, this set can be generated by starting with $a$ and iteratively conjugating with simple elements, keeping only the conjugates that remain in $[p, q]$, until we obtain no new elements of $[p, q]$ (Algorithm 1).

We solve the Search SCP by keeping track of the conjugating elements during the computation of the set $a^G \cap [p, q]$. □

For braid groups, a variation of the solution presented here was provided by Lee and Lee [26]. Their solution uses, instead of intervals $[p, q]$, intervals of the form

$$[p, \infty] = \{ a \in G^r : p \leq \inf a \}.$$
Algorithm 1 Compute the set $a^G \cap [p, q]$, for $p, q \in \mathbb{Z}^r$ and $a \in [p, q]$.

\[
W := \emptyset; \quad V := \{a\}
\]

repeat
    Take $v \in V$
    for all $s \in S$ do
        $u := (v^s_1, \ldots, v^s_r)$
        if $u \in [p, q]$ and $u \notin V$ then
            $V := V \cup \{u\}$
        end if
    end for
    $W := W \cup \{v\}$; $V := V \setminus \{v\}$
until $V = \emptyset$
return $W$

While these intervals are finite for braid groups, and more generally for so-called Garside groups with weighted presentation, they may potentially be infinite in some Garside groups, in which case the Lee–Lee solution to the SCP may not terminate in finite time.

The solution presented in this section is infeasible in practice, for two reasons: The intervals used are typically too large, and each step in the algorithm consists of conjugating by all simple elements. In the braid group $B_N$, there are exponentially (in $N$) many simple elements. We address these issues in the coming sections.

5. Simultaneous Cyclic Sliding

While cycling only affects the infimum of a braid, cyclic sliding affects infimum and supremum. We identify and establish a high-dimensional generalization of the latter. This plays a crucial role in our moving to minimal intervals in the next section.

Let $a \in G^r$. For each index $i = 1, \ldots, r$, represent the group element $a_i$ in normal form:

\[
a_i = \Delta^p_i P_i = \Delta^p_i s_1^{(i)} \cdots s_l^{(i)}.
\]

Assume that the interval $[p, q]$ is not minimal with respect to $a^G$, that is, there exists an element $b \in a^G$ such that $[p, q] \nsubseteq [\inf b, \sup b]$. Consider target intervals $[\tilde{p}, \tilde{q}]$ which are proper subintervals of $[p, q]$ such that $q_i - \tilde{q}_i \leq 1$ and $\tilde{p}_i - p_i \leq 1$ for all $i = 1, \ldots, r$. By definition, there are exactly $2r$ target intervals that are maximal with respect to $\leq$, namely those where the tuples $p$ and $\tilde{p}$—(exclusive) or $q$ and $\tilde{q}$—differ in exactly one coordinate. According to our assumption, there exists (among these $2r$ maximal target intervals) at least one such that $[\tilde{p}, \tilde{q}] \cap a^G \neq \emptyset$. We define simultaneous cyclic sliding with respect to a target interval $[\tilde{p}, \tilde{q}]$. 
5.1. Simultaneous cycling and decycling. Let \( b \in [\bar{p}, \bar{q}] \cap a^G \). Fix an element \( X \in G^+ \)
such that \( XaX^{-1} = b \). For \( i = 1, \ldots, r \), write
\[
    b_i = \Delta^{\bar{p}_i} \bar{b}_i = X \Delta^{p_i} P_i X^{-1},
\]
with \( \bar{b}_i \geq 1 \). The normal form of \( b_i \) need not be \( \Delta^{\bar{p}_i} \bar{b}_i \); in general, we have \( \inf(b_i) \geq \bar{p}_i \).
Multiplying Equation (1) on the left by \( \Delta^{-b_i} \), we have
\[
    \Delta \bar{b}_i = \Delta^{-(\bar{p}_i-1)} X \Delta^{p_i} P_i X^{-1} = \tau^{\bar{p}_i-1}(X) \Delta^{p_i-\bar{p}_i+1} P_i X^{-1} \geq \Delta.
\]
Since \( X \geq 1 \), we have \( \tau^{\bar{p}_i-1}(X) \Delta^{p_i-\bar{p}_i+1} P_i \geq \Delta \). For the index \( i \) with \( \bar{p}_i = p_i + 1 \), we have
\[
    \tau^{\bar{p}_i-1}(X) P_i \geq \Delta \quad \text{which by Lemma 4.2 implies that}
\]
\[
    \tau^{\bar{p}_i-1}(X)(P_i \land \Delta) = \tau^{\bar{p}_i-1}(X)s^{(i)}_1 \geq \Delta.
\]
By the invariance of the relation \( \geq \) under right multiplication, we have \( \tau^{\bar{p}_i-1}(X) \geq \Delta(s^{(i)}_1)^{-1} = \partial^{-1}(s^{(i)}_1) \). By invariance of \( \geq \) under \( \tau \)-automorphism, we have \( X \geq \tau^{-\bar{q}_i+1}(\partial^{-1}(s^{(i)}_1)) \).
Taking the left lcm for all \( i \) with \( \bar{p}_i = p_i + 1 \), we obtain
\[
    X \geq \vee_{i: \bar{p}_i = p_i + 1} \tau^{-\bar{q}_i+1}(\partial^{-1}(s^{(i)}_1)).
\]

**Definition 5.1.** In the above notation, the *simultaneous cycling* operation is the left conjugation of the tuple \( a \in G^r \) by the element in the right hand side of Equation (2).

We define simultaneous decycling analogously: Recall that \( q_i = \sup a_i = -\inf a_i^{-1} \). Let the normal form of the element \( a_i \) be \( \Delta^{-q_i} P'_i \). Since \( \sup b_i \leq \bar{q}_i \leq q_i \) and \( \inf b_i^{-1} = -\sup b_i \), we have \( \inf b_i^{-1} \geq -\bar{q}_i \). Thus, for each index \( i = 1, \ldots, r \), we can write
\[
    b_i^{-1} = \Delta^{-\bar{q}_i} \bar{b}_i' = X a_i^{-1} X^{-1} = X \Delta^{-q_i} P'_i X^{-1}
\]
for some element \( \bar{b}_i' \geq 1 \). In general, we have \( \inf(b_i^{-1}) \geq -\bar{q}_i \) and \( \Delta^{-\bar{q}_i} \bar{b}_i' \) need not be the normal form of \( b_i^{-1} \). Multiplying Equation (3) on the left by \( \Delta^{\bar{q}_i} \), we have
\[
    \Delta \bar{b}_i' = \Delta^{\bar{q}_i+1} X \Delta^{-q_i} P'_i X^{-1} = \tau^{-\bar{q}_i-1}(X) \Delta^{-q_i+\bar{q}_i+1} P'_i X^{-1} \geq \Delta.
\]
Since \( X \geq 1 \), we have \( \tau^{\bar{q}_i-1}(X) \Delta^{-q_i+\bar{q}_i+1} P'_i \geq \Delta \). For \( i \) with \( \bar{q}_i = q_i - 1 \), we have \( \tau^{-\bar{q}_i-1}(X) P'_i = \tau^{-q_i}(X) P'_i \geq \Delta \). By Lemma 4.2, we have \( \tau^{-q_i}(X)(P'_i \land \Delta) \geq \Delta \). The normal form of the element \( a_i^{-1} \) is related to that of \( a_i \). In particular, we have
\[
    P'_i \land \Delta = \tau^{-q_i}(\partial(s^{(i)}_{l_i})).
\]
Thus,
\[
    \tau^{-q_i}(X \partial(s^{(i)}_{l_i})) = \tau^{-q_i}(X(s^{(i)}_{l_i})^{-1}) \Delta \geq \Delta.
\]
By invariance of the relation \( \geq \) under right multiplication, we have \( \tau^{-q_i}(X) \geq \tau^{-q_i}(s^{(i)}_{l_i}) \). Invariance of the relation \( \geq \) under the automorphism \( \tau \) implies that \( X \geq s^{(i)}_{l_i} \) for all \( i \) with
\( \tilde{q}_i = q_i - 1 \). Finally, we can take the left lcm and obtain

\[
X \geq \bigvee_{i : \tilde{q}_i = q_i - 1} s_{i}^{(i)}.
\]

**Definition 5.2.** In the above notation, the *simultaneous decycling* operation is the left conjugation of the tuple \( a \in G^r \) by the element on the right hand side of Equation \( \text{(4)} \).

**5.2. Simultaneous cyclic sliding.**

**Definition 5.3.** In the above notation, Equations \( \text{(2)} \) and \( \text{(4)} \) imply that

\[
X \geq \bigvee_{i : \tilde{p}_i = p_i + 1} \tau^{-\tilde{p}_i + 1}(s_i^{(i)}) \bigvee \bigvee_{i : \tilde{q}_i = q_i - 1} s_{i}^{(i)} =: x(0).
\]

The *simultaneous cyclic sliding* operation (with respect to the target interval \([\tilde{p}, \tilde{q}]\)) is the left conjugation of the tuple \( a \in G^r \) by the element \( x(0) \). Let \( \text{sl}(a) := x(0) ax(0)^{-1} \).

It is easy to verify that

\[
\tilde{p}_i - 1 \leq \inf(\text{sl}(a_i)) \leq \sup(\text{sl}(a_i)) \leq \tilde{q}_i + 1
\]

for all \( i = 1, \ldots, r \). In other words, the infimum and supremum of the element \( \text{sl}(a_i) \) are at most in distance one outside the target interval. Indeed, we have implicitly treated the difficult cases (where \( \tilde{p}_i = p_i + 1 \) or \( \tilde{q}_i = q_i - 1 \)) in the derivation above. The cases where \( \tilde{p}_i = p_i \) or \( \tilde{q}_i = q_i \) are clear, since conjugation by any simple element (in particular, by \( x(0) \)) can decrease (respectively, increase) the infimum (respectively, supremum) by at most 1.

For an element \( a \in G^r \) in a Garside group \( G \), let \( \|a\| \) be the maximum number of atoms in an expression of \( a \) as a product of atoms. The following theorem generalizes the Birman–Ko–Lee Cycling Theorem \[4\] to dimension \( r > 1 \). It asserts that if moving to a proper subinterval is possible, then this can be done in at most \( \|\Delta\| - 1 \) steps. As usual, for \( i \in \{1, \ldots, r\} \) let \( e_i \in \mathbb{Z}^r \) be the tuple with all coordinates 0 but the \( i \)-th, which is 1.

**Theorem 5.4 (Simultaneous Cyclic Sliding).** Let \( a \in G^r \cap [p, q] \). For each index \( i = 1, \ldots, r \) and each pair \((\tilde{p}, \tilde{q}) \in \{(p + e_i, q), (p, q - e_i)\} \) with \( a^G \cap [\tilde{p}, \tilde{q}] \neq \emptyset \), we have

\[
\text{sl}\|\Delta\|^{-1}(a) := \overbrace{\text{sl}(\text{sl}(\cdots \text{sl}(a)))}^{\|\Delta\|^{-1} \text{ times}} \in [\tilde{p}, \tilde{q}].
\]

**Proof.** Let \( a(0) := a \). For \( t = 0, 1, \ldots, \|\Delta\| - 2 \), let \( a(t + 1) = \text{sl}(a(t)) \). Let \( p_i(t) := \inf(a_i(t)) \), \( q_i(t) := \sup(a_i(t)) \), and \( l_i(t) := q_i(t) - p_i(t) \). Express the element \( a_i(t) \) in normal form:

\[
a_i(t) = \Delta^{p_i(t)} s_i^{(i)}(t) \cdots s_{l_i(t)}^{(i)}(t).
\]

Explicitly, \( a(t + 1) = x(t)a(t)x(t)^{-1} \), where

\[
x(t) := \bigvee_{i : \tilde{p}_i = p_i(t) + 1} \tau^{-\tilde{p}_i + 1}(s_i^{(i)}(t)) \bigvee \bigvee_{i : \tilde{q}_i = q_i(t) - 1} s_{l_i(t)}^{(i)}(t).
\]
Setting $X(t) := x(t)x(t-1)\cdots x(1)x(0)$, we have $a_i(t) = X(t)a_iX(t)^{-1}$.

Let $m$ and $X = X(m) \succeq 1$ be minimal (with respect to $\succeq$) such that $XaX^{-1} = a(m+1) \in [\tilde{p}, \tilde{q}]$. Let $X(t) := x(m)x(m-1)\cdots x(t)$, that is, decompose $X = X(m) = \tilde{X}(t)X(t-1)$ for all $t = 1, 2, \ldots, m$. For $t = 0$, we obtain $\tilde{X}(0) = X(m) = X$. Define

$$H(t) := \Delta \land \tilde{X}(t)$$

for $t = 0, 1, \ldots, m$. Then $H(t+1) \succeq H(t)$ for all $t = 0, 1, \ldots, m-1$.

By the minimality of the number $m$, we have $H(m) = x(m) \succ 1$. By the minimality of the element $X = X(m)$, we have $\inf X = 0$, and hence $H(0) = \Delta \land \tilde{X}(0) = \Delta \land X \preceq \Delta$. In order to prove that

$$1 \prec H(m) \prec \cdots \prec H(1) \prec H(0) \prec \Delta$$

it suffices to show that $H(t) \neq H(t+1)$ for all $t$. Then Equation (6) implies that

$$0 < \|H(m)\| < \cdots < \|H(1)\| < \|H(0)\| < \|\Delta\|,$$

and thus $m+1$, is bounded below $\|\Delta\| - 1$, which completes the proof.

We prove the inequality $H(1) \neq H(0)$; the proof of the inequality $H(t+1) \neq H(t)$ for $t = 1, \ldots, m-1$ is similar. Let $L := \text{cl}(X) = \text{sup}(X) \leq m+1$. Express in normal form $X = B_L \cdots B_2 B_1$. Then $H(0) = \tilde{X}(0) \land \Delta = X \land \Delta = B_L$. Assume, towards a contradiction, that $H(1) = H(0) = B_L$, that is, $\tilde{X}(1) \land \Delta = B_L$. Write $\tilde{X}(1) = x(m) \cdots x(1) = B_L R_1$ for some $R_1 \in G^+$. Then $X = B_L R_1 x(0)$ and $B_{L-1} \cdots B_1 = R_1 x(0)$. We prove that

$$\begin{align*}
(B_{L-1} \cdots B_1) a_i & \succeq \Delta^{\tilde{p}_i}, \\
(B_{L-1} \cdots B_1) a_i^{-1} & \succeq \Delta^{-\tilde{q}_i}
\end{align*}$$

For all $i = 1, \ldots, r$.

Proof of Equation (7). First, let $i$ be an index with $\tilde{p}_i = p_i+1$. According to Equation (2), we have $x(0) \succeq \tau^{-p_i}(\partial^{-1}(s_i^{(i)}))$. Write $x(0) = r_i \tau^{-p_i}(\partial^{-1}(s_i^{(i)}))$. Then

$$\begin{align*}
(B_{L-1} \cdots B_1) a_i &= R_1 x(0) \Delta^{p_i} P_i = R_1 r_i \tau^{-p_i}(\partial^{-1}(s_i^{(i)})) \Delta^{p_i} P_i \\
&= R_1 r_i \Delta^{p_i} \partial^{-1}(s_i^{(i)}) s_i^{(i)} \cdots s_i^{(i)} \succeq \Delta^{p_i+1} = \Delta^{\tilde{p}_i}.
\end{align*}$$

The case where $\tilde{p}_i = p_i$ is simpler:

$$(B_{L-1} \cdots B_1) a_i = R_1 x(0) \Delta^{p_i} P_i \succeq \Delta^{p_i} = \Delta^{\tilde{p}_i}.$$ 

Proof of Equation (8): Let $i$ be an index such that $\tilde{q}_i = q_i - 1$. According to Equation (4), we have $x(0) \succeq s_i^{(i)}$. Write $x(0) = r_i' s_i^{(i)}$. Since $a_i^{-1} = \Delta^{-q_i} \tilde{P}_i$ and $\tilde{P}_i \land \Delta = \tau^{-q_i}(\partial(s_i^{(i)}))$, we can write $\tilde{P}_i = \tau^{-q_i}(\partial(s_i^{(i)})) \tilde{P}_i'$. Thus,

$$\begin{align*}
(B_{L-1} \cdots B_1) a_i^{-1} &= R_1 x(0) \Delta^{-q_i} \tilde{P}_i = R_1 r_i' s_i^{(i)} \Delta^{-q_i} \tilde{P}_i \\
&= R_1 r_i' \Delta^{-q_i} \tau^{-q_i}(s_i^{(i)}) \tau^{-q_i}(\partial(s_i^{(i)})) \tilde{P}_i' \succeq \Delta^{-q_i+1} = \Delta^{-\tilde{q}_i}.
\end{align*}$$
The case where $\tilde{q}_i = q_i$ is simpler:

$$(B_{L-1} \cdots B_1) a_i^{-1} = R_1 x(0) \Delta^{-q_i} \bar{P}_i \geq \Delta^{-\tilde{q}_i} = \Delta^{-\tilde{q}_i}.$$  

Next, we prove that:

(9) \quad \inf((B_{L-1} \cdots B_1) a_i (B_{L-1} \cdots B_1)^{-1}) \geq \tilde{p}_i \text{ and}

(10) \quad \sup((B_{L-1} \cdots B_1) a_i (B_{L-1} \cdots B_1)^{-1}) \leq \bar{q}_i

For all $i = 1, \ldots, r$.

**Proof of Equation (9):** Define, for $k = 0, 1, \ldots, L$ and $i = 1, \ldots, r$,

$$\alpha_i(k) := \inf[(B_{L-1} \cdots B_1) a_i \tau(B_1) \partial(B_2) \cdots \tau^{k-1}(\partial(B_k))].$$

Note that $\tau(B_1) \tau(B_2) \cdots \tau^{k-1}(\partial(B_k))$ is the normal form of $(B_k \cdots B_1)^{-1} \Delta^k$. By definition, for $i = 1, \ldots, r$ we have

$$\alpha_i(0) = \inf[(B_{L-1} \cdots B_1) a_i] \geq \tilde{p}_i,$$

$$\alpha_i(L) = \inf[(B_{L-1} \cdots B_1) a_i \tau(B_1) \partial(B_2) \cdots \tau^{L-1}(\partial(B_L))]$$

$$= \inf[B_k^{-1}(X a_i X^{-1}) \Delta^L] \geq -1 + \tilde{p}_i + L, \text{ and}$$

$$\alpha_i(k) \leq \alpha_i(k+1)$$

for all $k = 0, 1, \ldots L - 1$. By the lemma, we have $\alpha_i(k+1) \leq \alpha_i(k) + 1$ for all $k$ and $i$. Since $\partial(B_1) \tau(B_2) \cdots \tau^{k-1}(\partial(B_k))$ is in normal form, we have

$$\alpha_i(k) = \alpha_i(k+1) \quad \Rightarrow \quad \alpha_i(k) = \cdots = \alpha_i(L - 1) = \alpha_i(L).$$

Assume that there is an index $i$ such that $\alpha_i(L - 1) \leq \tilde{p}_i + L - 2$. Since $\alpha_i(0) \geq \tilde{p}_i$, there is a natural number $k$ such that $\alpha_i(k) = \alpha_i(k+1)$. Hence $\alpha_i(k) = \cdots = \alpha_i(L - 1) = \alpha_i(L) \leq \tilde{p}_i + L - 2$, in contradiction to the inequality $\alpha_i(L) \geq \tilde{p}_i + L - 1$. Thus, $\alpha_i(L - 1) \geq \tilde{p}_i + L - 1$ for all $i = 1, \ldots, r$, that is,

$$\inf[(B_{L-1} \cdots B_1) a_i \tau(B_1) \partial(B_2) \cdots \tau^{L-2}(\partial(B_{L-1}))] \geq \tilde{p}_i + L - 1,$$

or, equivalently, $\inf[(B_{L-1} \cdots B_1) a_i (B_{L-1} \cdots B_1)^{-1}] \geq \tilde{p}_i$ for all $i$.

**Proof of Equation (10):** Analogously, define

$$\alpha_i^-(k) := \inf[(B_{L-1} \cdots B_1) a_i^{-1} \tau(B_1) \partial(B_2) \cdots \tau^{k-1}(\partial(B_k))].$$

The element $\alpha_i^-(k)$ has the same properties as $\alpha_i(k)$, expect that we have to replace $\tilde{p}_i$ by $-\tilde{q}_i$. In particular, we have $\alpha_i^-(0) \geq -\tilde{q}_i$ and $\alpha_i^-(L) \geq -1 - \tilde{q}_i + L$. The proof proceeds as in the previous case, and we obtain

$$\inf[(B_{L-1} \cdots B_1) a_i^{-1} (B_{L-1} \cdots B_1)^{-1}] = -\sup[(B_{L-1} \cdots B_1) a_i (B_{L-1} \cdots B_1)^{-1}] \geq -\tilde{q}_i.$$
Equations (9) and (10) assert that the tuple \((B_{L-1} \cdots B_1) a (B_{L-1} \cdots B_1)^{-1}\) lies in the target interval \([\bar{p}, \bar{q}]\), in contradiction to the minimality of the element \(X = B_L B_{L-1} \cdots B_1\). We conclude that the assumption \(H(0) = H(1)\) is false.

\[\square\]

6. Moving to minimal intervals

Let \(G\) be a Garside group and \(a, c \in G^r\). The solution to the SCP for \(a\) and \(c\), described in section 4, is by choosing some interval \([p, q]\) containing \(a\) and \(c\) and computing the set \(a^G \cap [p, q]\). Increasing \(p\) or decreasing \(q\)—lexicographically—may reduce the cardinality of this set considerably.

Algorithm 2 conjugates an \(r\)-tuple into a prescribed interval, assuming that this is possible. For braid groups, with \([\inf c, \infty]\) (where \(c\) is conjugate to \(a\)) instead of \([p, q]\) (and \(M = \infty\)), this algorithm is similar to that of Lee and Lee \([26]\). Here, for example, we can take the smaller interval \([\inf c, \sup c]\). We note that a simultaneous cycling theorem was not established for the operation used by Lee and Lee; they did not conjugate by the \(\tilde{\vee}\)-join of all cyclings for components with infimum outside the target interval.

**Algorithm 2** Given tuples \(a \in G^r\) and \(p, q \in \mathbb{Z}^r\), find an element \(y \in G^+\) such that \(a^y^{-1} \in [p, q]\). Uses input parameter \(M \in \mathbb{N} \cup \{\infty\}\).

\[
\begin{align*}
\text{function } & \text{ConjugateToInterval}(a, p, q, M) \\
& \quad y := 1; \ c := a; \ i := 0 \\
& \quad \text{while } c \notin [p, q] \text{ and } i < M \text{ do} \\
& \quad \quad h := 1 \\
& \quad \quad \text{for } k := 1 \text{ to } r \text{ do} \\
& \quad \quad \quad \text{if } \inf c_k < p_k \text{ then} \\
& \quad \quad \quad \quad h := h \tilde{\vee} \Delta^{-\inf c_k} (\Delta^{-\inf c_k c_k})^{-1} \\
& \quad \quad \quad \text{end if} \\
& \quad \quad \quad \text{if } q_k < \sup c_k \text{ then} \\
& \quad \quad \quad \text{Bring } c_k \text{ in normal form } \Delta^{\inf c_k s_1 \cdots s_{\text{cl}(c_k)}} \\
& \quad \quad \quad h := h \tilde{\vee} s_{\text{cl}(c_k)} \\
& \quad \quad \text{end if} \\
& \quad \quad \end{for} \\
& \quad \quad y := h y, \ c := c^h \\
& \quad \quad i := i + 1 \\
& \quad \text{end while} \\
& \quad \text{return } y \quad \quad \triangleright \text{Successful if and only if } a^y^{-1} \in [p, q]. \\
\end{align*}
\]

By the Simultaneous Cyclic Sliding Theorem (Theorem 5.4), we have the following performance guarantee.
Corollary 6.1. Assume that $a \in G^r \cap [p, q]$, $i \in \{1, \ldots, r\}$, and $(\tilde{p}, \tilde{q}) \in \{(p+e_i, q), (p, q-e_i)\}$ is a pair with $a^G \cap [\tilde{p}, \tilde{q}] \neq \emptyset$. Let $y := \text{ConjugateToInterval}(a, p', q', ||\Delta|| - 1)$. Then $a^y \in [\tilde{p}, \tilde{q}]$.

Definition 6.2. Let $G$ be a Garside group, $r$ a natural number, $a \in G^r$, and $p, q \in \mathbb{Z}^r$ be tuples with $p \leq q$. The interval $[p, q]$ is minimal for the conjugacy class $a^G$ if $[p, q]$ intersects $a^G$, but no proper subinterval of $[p, q]$ intersects $a^G$.

Consider the one-dimensional case. For a Garside group $G$ and an element $a \in G$, the summit infimum and summit supremum of $a$ are the maximal infimum and minimal supremum, respectively, of an element of $a^G$. In this one-dimensional case, the interval $[\text{suminf}(a), \text{sumsup}(a)]$ is the only minimal interval with respect to $a$. Garside’s Summit Set \cite{15} and Elrifai–Morton’s Super Summit Set \cite{12} of $a$ are the sets

$$SS(a) = a^G \cap [\text{suminf} a, \infty];$$
$$SSS(a) = a^G \cap [\text{suminf} a, \text{sumsup} a],$$

respectively. These sets are complete conjugacy invariants. In higher dimensions, there are in general more than one minimal interval for a conjugacy class. Any canonical choice among them would provide a complete conjugacy invariant. We provide two variations of a complete invariant for simultaneous conjugacy classes. Since we use minimal intervals, these invariants generalize the classic Super Summit Sets to general dimension.

Definition 6.3. Let $G$ be a Garside group and $a \in G^r$. The lexicographically minimal interval for the conjugacy class $a^G$ is the unique interval $[p, q]$ with the following properties:

1. $p_1$ and $q_1$ are the summit infimum and summit supremum of $a_1$, respectively.
2. For $i = 2, 3, \ldots, r$, in this order: $p_i$ is maximal and $q_i$ is minimal (given $p_i$) with $(a_1, \ldots, a_i)^G \cap [(p_1, \ldots, p_i), (q_1, \ldots, q_i)] \neq \emptyset$.

The Lexicographic Super Summit Set of $a$, $\text{LSSS}(a)$, is the intersection of $a^G$ with its lexicographically minimal interval.

The lexicographically minimal interval for the conjugacy class $a^G$ is the unique interval $[p, q]$ with the following properties:

1. For $i = 1, \ldots, r$: $p_i$ is maximal with $(a_1, \ldots, a_i)^G \cap [(p_1, \ldots, p_i), \infty] \neq \emptyset$.
2. For $i = 1, \ldots, r$: $q_i$ is minimal with $(a_1, \ldots, a_i)^G \cap [(p_1, \ldots, p_i), (q_1, \ldots, q_i)] \neq \emptyset$.

The Lexicographic Super Summit Set of $a$, $\text{LSSS}'(a)$, is the intersection of $a^G$ with its lexicographically minimal interval.

If $[p, q]$ is the lexicographically minimal interval for a conjugacy class $a^G$, then the set $\text{LSS}(a) := a^G \cap [p, \infty]$ is also a complete invariant for $a^G$, but it is, in general, larger than $\text{LSSS}'(a)$.

Given a lexicographically minimal interval $[p, q]$ for an element $a \in G^r$, we can conjugate the element $a$ into $\text{LSSS}(a)$ using $\text{ConjugateToInterval}(a, p, q, ||\Delta|| - 1)$, and then compute the entire $\text{LSSS}(a)$ using Algorithm \[1\] \text{Algorithm \[3\]} computes the lexicographically minimal interval for an element $a$. Analogous assertions hold for $\text{LSSS}'(a)$. 

Algorithm 3 Compute the lexicographically minimal interval \([p, q]\) for an element \(a \in G^r\)

\begin{algorithm}
\begin{algorithmic}
\For{\(i = 1, \ldots, r\)}
\State \(p_i := \inf a_i\).
\Repeat
\State \(y := \text{CONJUGATETOINTERVAL}((a_1, \ldots, a_i), (p_1, \ldots, p_i + 1), (q_1, \ldots, q_{i-1}, \infty), \|\Delta\| - 1)\)
\If{\((a_1, \ldots, a_i)^{y^{-1}} \in [(p_1, \ldots, p_i + 1), (q_1, \ldots, q_{i-1}, \infty)]\)}
\State \(p_i := p_i + 1\)
\State \(a := a^{y^{-1}}\)
\State \(\text{flag} := \text{true}\)
\Else
\State \(\text{flag} := \text{false}\)
\EndIf
\Until{\(\text{flag} = \text{false}\)}
\State \(q_i := \sup a_i\).
\Repeat
\State \(y := \text{CONJUGATETOINTERVAL}((a_1, \ldots, a_i), (p_1, \ldots, p_i), (q_1, \ldots, q_i - 1), \|\Delta\| - 1)\)
\If{\((a_1, \ldots, a_i)^{y^{-1}} \in [(p_1, \ldots, p_i + 1), (q_1, \ldots, q_i - 1)]\)}
\State \(q_i := q_i - 1\)
\State \(a := a^{y^{-1}}\)
\State \(\text{flag} := \text{true}\)
\Else
\State \(\text{flag} := \text{false}\)
\EndIf
\Until{\(\text{flag} = \text{false}\)}
\EndFor
\State \(\text{return } p, q\)
\end{algorithmic}
\end{algorithm}

The following proposition summarizes the relations among the introduced invariants.

**Proposition 6.4.** Let \(G\) be a Garside group and \(i \in \{1, \ldots, r\}\). Let \(\text{proj}_i\) denote the projection on the first \(i\) coordinates. For each tuple \(a \in G^r\), the following relations hold:

\[
\begin{align*}
\text{LSS}((a_1, \ldots, a_i)) &= \text{proj}_i(\text{LSS}(a)), \\
\text{LSSS}((a_1, \ldots, a_i)) &= \text{proj}_i(\text{LSSS}(a)), \\
\text{LSSS}'((a_1, \ldots, a_i)) &\subseteq \text{proj}_i(\text{LSSS}'(a)), \\
\text{LSSS}'(a) &\subseteq \text{LSS}(a).
\end{align*}
\]

In particular, we have \(\text{SS}(a_1) = \text{proj}_1(\text{LSS}(a))\) and

\[
\text{SSS}(a_1) = \text{proj}_1(\text{LSSS}(a)) \subseteq \text{proj}_1(\text{LSSS}'(a)).
\]
Our invariants are computable in finite time: detecting the lexicographically minimal interval \([p, q]\) of an element of this set, and then computing \(a^G \cap [p, q]\). Also, note that finite invariants of conjugacy classes imply canonical representatives: The lexicographically minimal element of the invariant. However, the computational complexity of computing such a canonical representative remains proportional to the cardinality of the initial invariant.

This completes our treatment of interval minimization. We next address the second and last problem: Removing the need to conjugate by all simple elements in each step of our algorithms. This will be done by extending the method of minimal simple elements to our situation.

### 7. Minimal simple elements

We apply the technique of minimal simple elements, introduced by González–Meneses and Franco [13], in order to make the computation of the sets \(a^G \cap [p, q]\) more efficient. The propositions and algorithms in this section are natural generalizations of earlier algorithms [13, 19, 22].

**Proposition 7.1.** Let \(G\) be a Garside group. Let \(v \in G^r\) be a tuple with \(v \in [p, q]\), for \(p, q \in \mathbb{Z}^r\). For \(i = 1, \ldots, r\), express \(v_i = \Delta^p_i w_i = z_i \Delta^p_i\) with \(w_i, z_i \in G^+\) and \((w_i^{-1} \Delta^q_i)\), \((\Delta^q_i) \in G^+\). Let \(s \in S\). Then:

1. \(v^s \in [p, q]\) if and only if
   \[\tau^{p_i}(s) \leq w_is\text{ and }\tau^{-q_i}(s) \leq (\Delta^{q_i-1}z_i^{-1})s\]
   for all \(i = 1, \ldots, r\).
2. \(v^{s^{-1}} \in [p, q]\) if and only if
   \[sz_i \geq \tau^{-p_i}(s)\text{ and }s(w_i^{-1} \Delta^{q_i}) \geq \tau^{q_i}(s)\]
   for all \(i = 1, \ldots, r\).

**Proof.** (1) For \(i = 1, \ldots, r\), we have \(\Delta^p_i \leq v_i \leq \Delta^q_i\) if and only if \(\Delta^p_i \leq v_i^s \leq \Delta^q_i\). Since \(\leq\) is invariant under left multiplication, we have \(\Delta^p_i \leq s^{-1} \Delta^p_i w_is\) if and only if \(\tau^{p_i}(s) \leq w_is\), and \(s^{-1} z_i \Delta^p_i s \leq \Delta^q_i\) is equivalent to \(s \leq \Delta^{-p_i} z_i^{-1} \Delta^q_i = \tau^q_i(\Delta^{-p_i} z_i^{-1})s\). By invariance of \(\leq\) under the automorphism \(\tau\), we have \(\tau^{-q_i}(s) \leq (\Delta^{q_i-1}z_i^{-1})s\).

(2) Here, for \(i = 1, \ldots, r\), we use that \(\Delta^p_i \leq v_i^{s^{-1}} \leq \Delta^q_i\) if and only if \(\Delta^{q_i} \geq v_i^{s^{-1}} \geq \Delta^p_i\). Since \(\geq\) is invariant under right multiplication, we conclude that \(sz_i \Delta^p_i s^{-1} \geq \Delta^p_i\) if and only if \(sz_i \geq \tau^{-p_i}(s)\), and \(\Delta^q_i \geq s \Delta^p_i w_is^{-1}\) is equivalent to \(\Delta^q_i w_i^{-1} \Delta^{-p_i} = \tau^{-q_i}(sw_i^{-1} \Delta^{q_i-p_i}) \geq s\). By invariance of \(\geq\) under \(\tau\), we have \(s(w_i^{-1} \Delta^{q_i-p_i}) \geq \tau^{q_i}(s)\). \(\square\)

**Lemma 7.2.** Assume that a set \(A \subseteq S\) is closed under the operation \(\land\) (respectively, \(\lor\)). Let \(x \in A\). If the set \(\{s \in A : x \preceq s\}\) (respectively, \(\{s \in A : s \succeq x\}\)) is nonempty, then it has a unique minimal element with respect to the relation \(\preceq\) (respectively, \(\succeq\)).

**Proof.** Every interval \(\{x \in G^+ : a \preceq x \preceq b\}\) in the poset \((G^+, \preceq)\) is closed under the operations \(\land\) and \(\lor\). The intersection of sets closed under \(\land\) and \(\lor\) is also closed under these operations. Uniqueness follows. \(\square\)
**Definition 7.3.** Let $G$ be a Garside group, $p, q \in \mathbb{Z}^r$, and $v \in [p, q]$. The set $S^{[p,q]}_{\text{right}}(v)$ consists of all $\preceq$-minimal elements $s \in S$ such that $v^s \in [p, q]$. Similarly, the set $S^{[p,q]}_{\text{left}}(v)$ consists of all $\succeq$-minimal elements $s \in S$ such that $v^{s^{-1}} \in [p, q]$.

Analogously to the proof of González–Meneses [19] Proposition 2.2, we prove the following result.

**Theorem 7.4.** Let $G$ be a Garside group, and $a, c \in [p, q] \subseteq G^r$. The following assertions are equivalent:

1. The tuples $a$ and $c$ are conjugate.
2. There exist a natural number $l$, elements $\tilde{w}_1, \ldots, \tilde{w}_{l-1} \in a^G \cap [p, q]$, and elements $\tilde{s}_i \in S^{[p,q]}_{\text{right}}(\tilde{w}_i)$, for $i = 1, \ldots, l$, such that
   \[
   a \xleftarrow{\tilde{s}_1} \tilde{w}_1 \xleftarrow{\tilde{s}_2} \cdots \xleftarrow{\tilde{s}_{l-1}} \tilde{w}_{l-1} \xleftarrow{\tilde{s}_l} c.
   \]
   
3. There exist a natural number $l$, elements $w_1, \ldots, w_{l-1} \in a^G \cap [p, q]$, and elements $s_i \in S^{[p,q]}_{\text{left}}(w_i)$, for $i = 1, \ldots, l$, such that
   \[
   a \xrightarrow{s_1} w_1 \xrightarrow{s_2} \cdots \xrightarrow{s_{l-1}} w_{l-1} \xrightarrow{s_l} c. \]

The set \{ $s \in S : v^s \in [p, q]$, \} is closed under $\wedge$. It follows [13] Corollary 4.3] that for each $s \in S^{[p,q]}_{\text{right}}(v)$ there is an atom $x \in S$ such that $s$ is the unique $\preceq$-minimal element of the set \{ $a \in S : x \preceq a$ and $v^a \in [p, q]$, \}. Similarly, each element of $S^{[p,q]}_{\text{left}}(v)$ is the unique $\succeq$-minimal element of the set \{ $a \in S : a \succeq x$ and $v^a \in [p, q]$, \} for some atom $x \in S$. It follows that, in Algorithm 11 the computation of $a^G \cap [p, q]$ can be done with $S$ replaced by $S^{[p,q]}_{\text{right}}(v)$, a set not larger than the number of atoms in $S$. For example, the Artin groups of type $A_n$, $B_n$, and $D_n$, respectively, have $(n+1)!$, $n!2^n$, and $n!2^{n-1}$ simple elements, but only $n$ atoms.

Algorithms 4, 5, and 6 build on earlier algorithms [13] [19] [22].

**Proposition 7.5.** Let $G$ be a Garside group, $p, q \in \mathbb{Z}^r$, $v \in [p, q] \subseteq G^r$, and $x \in S$. Algorithm 2 terminates and provides the correct output.

**Proof.** By Proposition 7.1 (1), we need to find the smallest element $r_x$ such that for all $i = 1, \ldots, r, x \preceq r_x$, $\tau^{p_k}(s) \preceq w_is$ and $\tau^{q_k}(s) \preceq w'_is$ with $w'_i = \Delta^{q_k-p_k}z_{i}^{-1}$. We take a simple element $s$ such that $x \preceq s \preceq r_x$, initializing with $s := x$. Then, for $k$ such that $\tau^{p_k}(s) \not\preceq w_ks$ or $\tau^{q_k}(s) \not\preceq (\Delta^{q_k-p_k}z_{k}^{-1})s$, we compute $s_1, s_2 \in G$ such that $\tau^{p_k}(s) \lor w_ks = w_ks_1$ and $\tau^{q_k}(s) \lor w'_ks = w'_ks_2$. If $s' := s_1 \lor s_2 = 1$, then $s_1 = s_2 = 1$, and we have $\tau^{p}(s) \preceq ws$ and $\tau^{q}(s) \preceq w's$, in contradiction to the choice of $k$. Thus, $s' \not= 1$. $s \preceq r_x$ implies that $\tau^{p_k}(s) \preceq \tau^{p_k}(r_x) \preceq w_ksr_x$, and by left-invariance of $\preceq$, it also implies that $w_ks \preceq w_ksr_x$, that is, $\tau^{p_k}(s), w_ks \preceq w_ksr_x$. By the definition of right lcm, we have that $\tau^{p_k}(s) \lor w_ks = w_ks_1 \preceq w_ksr_x$, and therefore $ss_1 \preceq r_x$.

Furthermore, $s \preceq r_x$ implies that $\tau^{q_k}(s) \preceq \tau^{q_k}(r_x) \preceq w'_ksr_x$, and by left-invariance of the relation $\preceq$ it also implies $w'_ks \preceq w'_ksr_x$, that is, $\tau^{q_k}(s), w'_ks \preceq w'_ksr_x$. By the definition of right lcm, $\tau^{q_k}(s) \lor w'_ks = w'_ks_2 \preceq w'_ksr_x$, and therefore $ss_2 \preceq r_x$. 
Algorithm 4 Compute the minimal element in the set \( \{ a \in S : x \preceq a \text{ and } v^a \in [p, q] \} \), for an atom \( x \).

Express \( v_i = \Delta^{p_i} w_i = z_i \Delta^{p_i} \)

\( s := x \)

\textbf{while} There is an index \( k \in \{1, \ldots, r\} \) with \( \tau^{p_k}(s) \not\lesssim w_k s \) or \( \tau^{-q_k}(s) \not\gtrsim (\Delta^{q_k} - p_k z_k^{-1})s \) \textbf{do}

Choose such an index \( k \)

Compute \( s_1 \in S \) such that \( \tau^{p_k}(s) \lor w_k s = w_k s s_1 \)

\( w'_k := \Delta^{q_k} - p_k z_k^{-1} \)

Compute \( s_2 \in S \) such that \( \tau^{-q_k}(s) \lor w'_k s = w'_k s s_2 \)

\( s' := s_1 \lor s_2 \)

\( s := s s' \)

\( r_x := s \)

\textbf{end while}

\textbf{return} \( r_x \)

From \( ss_1 \preceq r_x \) and \( ss_2 \preceq r_x \) we conclude that \( ss_1 \lor ss_2 = s(s_1 \lor s_2) = ss' \preceq r_x \).

So, if \( s \) is not equal to \( r_x \), then Algorithm 4 gives an element \( ss' \neq 1 \) such that \( s \preceq ss' \preceq r_x \), and it starts again checking whether \( ss' = r_x \). Since the number of left divisors of \( r_x \) is finite, this process must stop. Therefore, Algorithm 4 finds the requested minimal element in finite time.

Algorithm 5 Compute the minimal element of the set \( \{ a \in S : x \succeq a \text{ and } v^a \in [p, q] \} \), for an atom \( x \in S \).

Express \( v_i = \Delta^{p_i} w_i = z_i \Delta^{p_i} \)

\( s := x \)

\textbf{while} There is \( k \) with \( s z_k \not\gtrsim \tau^{-p_k}(s) \) and \( s(w_k^{-1} \Delta^{q_k} - p_k) \succeq \tau^{-q_k}(s) \) \textbf{do}

Compute \( s_1 \in S \) such that \( \tau^{-p_k}(s) \lor s z_k = s_1 s z_k \)

\( w'_k := w_k^{-1} \Delta^{q_k} - p_k \)

Compute \( s_2 \in S \) such that \( \tau^{p_k}(s) \lor s w'_k = s_2 s w'_k \)

\( s' := s_1 \lor s_2 \)

\( s := s s' \)

\textbf{end while}

\( r_x := s \)

\textbf{return} \( r_x \)

The sets of minimal simple elements \( S^{[p, q]\text{left}}(v) \) and \( S^{[p, q]\text{right}}(v) \) can be computed by comparing the elements \( r_x \), for all atoms \( x \) of \( G^+ \), and keeping the minimal ones. Since it is faster to check whether an atom divides a simple element than to compare two simple elements, we prefer to use Algorithm 3 (see Proposition 5.3 there).

We conclude by pointing out that, since our invariants are preserved by the automorphism \( \tau \), it is natural to consider them \( \textit{modulo} \ \tau \), that is, to maintain only one representative (for
Algorithm 6 Compute $S^{[p,q]}_{\text{right}}(v)$ or $S^{[p,q]}_{\text{left}}(v)$, respectively.

Let $x_1, \ldots, x_m$ be the atoms of $G$

\[ R := \emptyset \]

for $i = 1, \ldots, m$ do

Compute $r_{x_i}$ using Algorithm 4 (or 5, respectively)

\[ J_i := \{ j : j \in R \text{ and } x_j \preceq r_{x_i} \text{ (or } r_{x_i} \preceq x_j \} \]

\[ K_i := \{ j : j > i \text{ and } x_j \preceq r_{x_i} \text{ (or } r_{x_i} \preceq x_j \} \]

if $J_i = K_i = \emptyset$ then

\[ R := R \cup \{i\} \]

end if

end for

return \{ $r_{x_i} : i \in R$ \}

example, the lexicographically minimal one) out of each $\tau$-orbit. For example, the order of $\tau$ for two known Garside structures in braid groups $B_N$ with $N \geq 4$ strands, namely, the Artin–Garside structure with Garside element $\Delta = \Delta_N$ and the dual or Birman–Ko–Lee structure with $\Delta = \delta_N$, are 2 and $N$, respectively.

8. Experimental results in Artin’s braid groups

We have conducted extensive experiments checking the cardinalities of the finite sets that can be used for solving the SCP. The experiments are on Artin’s braid groups $B_N$, with their two known Garside structures (Artin and BKL). For a tuple $a \in B^*_N$, the set $a^{B_N} \cap [\inf a, \infty]$ is the one proposed by Lee and Lee [26]. The set $a^{B_N} \cap [\inf a, \sup a]$ is its natural subset introduced here. Both of these sets are not invariants of the conjugacy class. The sets $\text{LSS}(a)$ and $\text{LSSS}(a)$ are the invariants introduced here, namely the lexicographic summit set and the lexicographic super summit set.

We did not notice substantial differences between the cardinalities of the two variations of $\text{LSSS}$ introduced here. Thus, we used in the experiments the second variation, so that $\text{LSSS}(a)$ is always a subset of $\text{LSS}(a)$. This allows the use of a smaller number of experiments, while avoiding problems arising from the large variance.

To give the two sets that are not invariants a fair chance, we considered them for solving the Search SCP: We constructed conjugate $a, c \in B^*_N$ by choosing $b \in B^*_N$ and $x, y \in B_N$, and setting $a = b^x$ and $c = b^y$. We then computed, instead of $a^{B_N} \cap [\inf a, \infty]$, the typically smaller set $a^{B_N} \cap [\inf c, \infty]$, and similarly for the other set.

Random elements of $B_N$ were generated as products of random $2N \log N$ generators, each inverted in probability $1/2$. Such products are, with high probability, fully supported in the group.

We summarize the results in Table 8 which demonstrates the following typical inequalities:

\[ |\text{LSSS}(a)| < |\text{LSS}(a)| \ll |a^{B_N} \cap [\inf c, \sup c]| < |a^{B_N} \cap [\inf c, \infty]|. \]
The symbol $\ll$ indicates a dramatic improvement when moving to the invariants. An additional observation is that the BKL presentation provides much smaller sets, often one-element sets!

### Table 1.
Cardinalities of sets (modulo $\tau$) associated to the SCP, for dimension $r = 8$. Each cell lists the minimum, median, and maximum cardinality encountered, as well as the percentage of failures, out of 100 experiments. $\infty$ means $> 100,000$.

| $N$ | $\mathcal{B}_N \cap [\inf c, \infty]$ | $\mathcal{B}_N \cap [\inf c, \sup c]$ | LSS$(a)$ | LSSS$(a)$ |
|-----|-------------------------------------|-----------------------------------|----------|------------|
|     | Artin | BKL | Artin | BKL | Artin | BKL | Artin | BKL |
| 4   | 1     | 1   | 1     | 1   | 1     | 1   | 1     | 1   |
| 116 | 54    | 37  | 17    | 1   | 1     | 1   | 1     | 1   |
| 80,438 | 27,786 | 14,318 | 3,441 | 8   | 3     | 5   | 1     |
| 0%  | 0%    | 0%  | 0%    | 0%  | 0%    | 0%  | 0%    |
| 8   | $\infty$ | $\infty$ | 40,630 | 872 | 1     | 1   | 1     | 1   |
| $\infty$ | $\infty$ | $\infty$ | $\infty$ | 63  | 2     | 5   | 1     |
| $\infty$ | $\infty$ | $\infty$ | $\infty$ | 3,732 | 966 | 160  | 17   |
| 100% | 100% | 98% | 96% | 0% | 0% | 0% | 0% |
| 16  | $\infty$ | $\infty$ | $\infty$ | $\infty$ | 69,534 | 2 | 68 | 1 |
| $\infty$ | $\infty$ | $\infty$ | $\infty$ | $\infty$ | 740 | 76,509 | 6 |
| $\infty$ | $\infty$ | $\infty$ | $\infty$ | $\infty$ | $\infty$ | 28,025 |
| 100% | 100% | 100% | 100% | 99% | 10% | 76% | 0% |

We have tested, for the BKL presentation, the effect of increasing the dimension. Table 2 summarizes the results. We observe that the cardinality of the invariant LSSS tends to 1 with the increase of the dimension, and suggests that when $r = O(N)$ and the elements of the $r$-tuple are “generic” and independent, the invariant tends to have cardinality 1.

### Table 2.
The effect of increasing the dimension $r$ on the cardinality of the Birman–Ko–Lee Lexicographic SSS invariant (modulo $\tau$), for braid index $N = 32$. Each cell lists the minimum, median, and maximum cardinality encountered, out of 100 experiments. $\infty$ means $> 100,000$.

| $r$ | Minimum | Median | Maximum | Failures  |
|-----|---------|--------|---------|-----------|
| 4   | $\infty$ | $\infty$ | 720     | 100%      |
| 8   | 3       | 95     | 75      | 75%       |
| 16  | 1       | 2      | 4       | 0%        |
| 32  | 1       | 1      | 1       | 0%        |
| 64  | 1       | 1      | 1       | 0%        |
9. Open problems and further work

In Section 2 we reduced several problems to the conjunction of the Search SCP and the computation of the centralizer of a set. At present, there are no efficient algorithms for the computation of the centralizers of sets with more than one element in the braid groups. In addition to rectifying this specific issue, we have the following, more general problem.

**Problem 9.1.** Does the computation of the centralizer of a set in a group reduce to the Search SCP?

The computation of the centralizer of a single elements in braid groups involves methods used to solve the Conjugacy Problem in these groups [14]. These invariants depend on the order of entries in the \( r \)-tuple.

**Problem 9.2.** Is there an invariant, computable in comparable time, that does not depend on the order of the entries?

Our invariants may be huge. In the one-dimensional case, there are the much better (essentially, equivalent) invariants of Ultra Summit Sets and Sliding Circuits. Our methods provide candidates for high-dimensional generalizations, but some gaps must be filled.

**Problem 9.3.** Is there a generalization of Ultra Summit Sets or Sliding Circuits to the high-dimensional setting?

Dehornoy pointed out to us that some of the conditions in the definition of Garside groups, like being Noetherian, are often not needed to establish results about them. In particular, the normal form exists whenever there is a “Garside family” [9, 10]. Much that was done for Garside groups extends to Garside families, and it is natural to expect that our work can be extended to arbitrary Garside families.

It is also natural to consider potential applications of this work to cryptanalysis. As we can see in [2] the reductions to the Search SCP provide highly biased instances. The dependency among the entries renders the invariants too large to be of any direct use. To this end, the invariants must be combined with heuristic shortcuts, like ones used earlier [20]. The Search SCP has the following heuristic speedup: We compute LSSS(\(a\)) and LSSS(\(c\)) in parallel, until we find an element in the intersection. Heuristically, this has the potential to reduce the running time from \( n := |\text{LSSS}(a)| \) to about \( \sqrt{n} \). However, in our experiments we did not observe the expected speedup. An investigation of this phenomenon may help addressing Problem 9.3.

**Acknowledgments.** We thank Patrick Dehornoy for providing us information about representation theory of Garside groups and Garside families. We thank David Garber for useful discussions. The research of the first named author is partially supported by the Minerva Foundation of Germany.
References

[1] I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public-key cryptography, Mathematical Research Letters 6 (1999), 287–291.
[2] A. Ben-Zvi, A. Kalka, B. Tsaban, Cryptanalysis via algebraic spans, IACR eprint IACR eprint 2014/041.
[3] J. Birman, K. Ko, S. Lee, New approaches to the word and conjugacy problem in the braid groups, Advances in Mathematics 139 (1998), 322–353.
[4] J. Birman, K. Ko, S. Lee, The infimum, supremum and geodesic length of a braid conjugacy class, Advances in Mathematics 164 (2001), 41–56.
[5] J. Cheon, B. Jun, A polynomial time algorithm for the braid Diffie–Hellman conjugacy problem, CRYPTO 2003, Lecture Notes in Computer Science 2729 (2003), 212–224.
[6] J. Cha, K. Ko, S. Lee, J. Han, J. Cheon, An efficient implementation of braid groups, ASIACRYPT 2001, Lecture Notes in Computer Science 2248 (2001), 144–156.
[7] John Crisp, Injective maps between Artin groups, in: Geometric Group Theory Down Under, Walter deGruyter, 1999, 119–137.
[8] P. Dehornoy, Using shifted conjugacy in braid-based cryptography, Contemporary Mathematics 418 (2006), 65–73.
[9] P. Dehornoy, F. Digne, J. Michel, Garside families and Garside germs, Journal of Algebra 380 (2013), 109–145.
[10] P. Dehornoy, with F. Digne, E. Godelle, J. Michel, Foundations of Garside Theory, EMS Tracts in Mathematics, volume 22, xviii + 690 pages, European Mathematical Society, 2015.
[11] P. Dehornoy, L. Paris, Gaussian groups and Garside groups, two generalizations of Artin groups, Proceedings of the London Mathematical Society 79 (1999), 569–604.
[12] E. Elrifai, H. Morton, Algorithms for positive braids, Quarterly Journal of Mathematics 45 (1994), 479–497.
[13] N. Franco, J. González-Meneses, Conjugacy problem for braid groups and Garside groups, Journal of Algebra 266 (2003), 112–132.
[14] N. Franco, J. González-Meneses, Computation of Centralizers in Braid groups and Garside Groups, Rev. Mat. Iberoamericana 19 (2003), 367–384.
[15] F. Garside, The braid group and other groups, Quarterly Journal of Mathematics 20 (1969), 235–254.
[16] D. Garber, A. Kalka, E. Liberman, M. Teicher, Double Centralizers of Parabolic Subgroups of Braid Groups, arXiv eprint 1310.0936
[17] V. Gebhardt, J. González–Meneses, The cyclic sliding operation in Garside groups, Mathematische Zeitschrift 265 (2010), 85–114.
[18] E. Godelle, Parabolic subgroups of Garside groups, Journal of Algebra 317 (2007), 1–16.
[19] J. González–Meneses, Improving an algorithm to solve Multiple Simultaneous Conjugacy Problem in braid groups, Contemporary Mathematics 372 (2005), 35–42.
[20] D. Hofheinz, R. Steinwandt, A practical attack on some braid group based cryptographic primitives, PKC 2003, Lecture Notes in Computer Science 2567 (2002), 187–198.
[21] A. Kalka, E. Liberman, M. Teicher, A Note on the Shifted Conjugacy Problem in Braid Groups, Groups Complexity Cryptology 1 (2009), 227–230.
[22] A. Kalka, E. Liberman, M. Teicher, Solution to the subgroup conjugacy problem for Garside subgroups of Garside groups, Groups Complexity Cryptology 2 (2010), 157–174.
[23] A. Kalka, M. Teicher, B. Tsaban, On the Double Coset Problem for parabolic subgroups of Artin’s braid groups, arXiv eprint 1402.5541
[24] C. Kassel, V. Turaev, Braid Groups, Graduate Texts in Mathematics 247, Springer, New York, 2008.
[25] K. Ko, S. Lee, J. Cheon, J. Han, J. Kang, C. Park, New public-key cryptosystem using braid groups, CRYPTO 2000, Lecture Notes in Computer Science 1880 (2000), 166–183.
[26] S. Lee, E. Lee, Potential weaknesses of the commutator key agreement protocol based on braid groups, EUROCRYPT 2002, Lecture Notes in Computer Science 2332 (2002), 14–28.

[27] M. Picantin, Petites groupes gaussiens, Thèse de Doctorat de l’Université de Caen, 2000.

[28] M. Picantin, The conjugacy problem in small Gaussian groups, Communications in Algebra 29 (2001), 1021–1039.

[29] M. Picantin, Automatic structures for torus link groups, Journal of Knot Theory and its Ramifications 12, no. 5 (2003), 1–34.

[30] V. Shpilrain, A. Ushakov, A new key exchange protocol based on the decomposition problem, in: L. Gerritzen, D. Goldfeld, M. Kreuzer, G. Rosenberger and V. Shpilrain, eds., Algebraic Methods in Cryptography, Contemporary Mathematics 418 (2006), 161–167.

[31] William Thurston, Braid groups, chapter 9 in: D. Epstein, J. Cannon, D. Holt, S. Levy, M. Paterson, W. Thurston, Word processing in groups, Jones and Bartlett, 1992.

[32] B. Tsaban, Polynomial-time solutions of computational problems in noncommutative algebraic cryptography, Journal of Cryptology 28 (2015), 601–622.

(Kalka, Vinokur) Department of Mathematics, Bar-Ilan University, Ramat Gan 5290002, Israel
E-mail address: Arkadius.Kalka@rub.de, vinokur777@gmail.com

(Tsaban) Department of Mathematics, Bar-Ilan University, Ramat Gan 5290002, Israel; and Faculty of Mathematics, Weizmann Institute of Science, Rehovot 7610001, Israel
E-mail address: tsaban@math.biu.ac.il