ALGORITHMIC RECOGNITION OF QUASIPOSITIVE BRAIDS OF ALGEBRAIC LENGTH TWO

S.Yu. Orevkov

Abstract. We give an algorithm to decide if a given braid is a product of two factors which are conjugates of given powers of standard generators of the braid group. The same problem is solved in a certain class of Garside groups including Artin-Tits groups of spherical type. The solution is based on the Garside theory and, especially, on the theory of cyclic sliding developed by Gebhardt and González-Meneses. We show that if a braid is of the required form, then any cycling orbit in its sliding circuit set in the dual Garside structure contains an element for which this fact is immediately seen from the left normal form.

Introduction

Let Br_n be the braid group with n strings. It is generated by $\sigma_1,\dots,\sigma_{n-1}$ (called *standard* or *Artin* generators) subject to the relations

$$\sigma_i\sigma_j=\sigma_j\sigma_i \text{ for } |i-j|>1; \qquad \sigma_i\sigma_j\sigma_i=\sigma_j\sigma_i\sigma_j \text{ for } |i-j|=1$$

In this paper we give an algorithm (rather efficient in practice) to decide if a given braid is the product of two factors which are conjugates of given powers of standard generators. Since our solution is based on Garside theory, as a by-product we obtain a solution to a similar problem for a certain class of Garside groups which includes Artin-Tits groups of spherical type (we call them in this paper just Artin groups; note that Br_n is the Artin group of type A_{n-1}). The main ingredient of our solution is the theory of cyclic sliding developed by Gebhardt and González-Meneses in [17]. In fact, we show that if an element X is a product of two conjugates of atom powers, then its set of sliding circuits $\mathrm{SC}(X)$ contains an element for which this property is immediately seen from the left normal form. If the Garside structure is symmetric (which is the case for the dual structures on Artin groups), then any cycling orbit in $\mathrm{SC}(X)$ contains such an element.

When speaking of Garside groups, we use mostly the terminology and notation from [17]. All necessary definitions and facts from the Garside theory are given in §1 below. For readers familiar with the Garside theory, we just say here that by a Garside structure on a group G we mean a triple $(G,\mathcal{P},\Delta)$ were $\mathcal{P}$ is the submonoid of positive elements and Δ is the Garside element (see details in §1). The letter length function on $\mathcal{P}$ is denoted by $\|\ \|$ and the set of atoms is denoted by $\mathcal{A}$.

It is convenient also to give the following new definitions. We say that a Garside structure is *symmetric* if, for any two simple elements u,v, one has $(u\prec v)\Leftrightarrow(v\succ u)$. The main example is the dual Garside structure on Artin groups introduced by Bessis [1], see [1; §1.2]. In particular, the Birman-Ko-Lee Garside structure on the braid groups [4] is symmetric. Another example is the braid extension of the complex reflection group $G(e,e,r)$ with the Garside structure introduced in [2].

Following [6], we say that $X \in \mathcal{P}$ is *square free* if there do not exist $U, V \in \mathcal{P}$ and $x \in \mathcal{A}$ such that $X = Ux^2V$. A Garside structure is called *square free* if all simple elements are square free. We say that a Garside structure is *homogeneous* if $\|XY\| = \|X\| + \|Y\|$ for any $X, Y \in \mathcal{P}$, thus, $\|\ \|$ extends up to a unique homomorphism $e : G \to \mathbb{Z}$ such that $e|_{\mathcal{A}} = 1$. Both the standard and the dual Garside structure on Artin groups are square free and homogeneous.

The conjugacy class of an element X of a group G is denoted by X^G. We use Convention 1.8 (see §1 below) for the presentation of left (right) normal forms. Let us give the statements of the main results (the proofs are in §3 and in §4).

Theorem 1. *Let $(G, \mathcal{P}, \delta)$ be a symmetric homogeneous Garside structure of finite type with set of atoms $\mathcal{A}$. Let k, l be positive integers. When $k \geq 2$ in Part* (a) *or when* $\max(k,l) \geq 2$ *in Part* (b)*, we suppose in addition that the Garside structure is square free. Let $X \in G$ and $x, y \in \mathcal{A}$. Then:*

(a). *$X \in (x^k)^G$ if and only if the left normal form of X is*

$$\delta^{-n} \cdot A_n \cdot \ldots \cdot A_2 \cdot A_1 \cdot x_1^k \cdot B_1 \cdot B_2 \cdot \ldots \cdot B_n \tag{1}$$

where $n \geq 0$, $x_1 \in x^G \cap \mathcal{A}$ and A_i, B_i are simple elements such that

$$A_i \delta^{i-1} B_i = \delta^i, \qquad i = 1, \ldots, n. \tag{2}$$

(b). *$X \in (x^k)^G (y^l)^G$ if and only if either $X \in (x_1^k y_1^l)^G$ or* **any cycling orbit** *and* **any decycling orbit** *in the set of sliding circuits* $\mathrm{SC}(X)$ (*see Remark 1.13*) *contains an element whose left normal form is*

$$\delta^{-n} \cdot A_n \cdot \ldots \cdot A_2 \cdot A_1 \cdot x_1^k \cdot B_1 \cdot B_2 \cdot \ldots \cdot B_n \cdot y_1^l \tag{3}$$

where $n \geq 1$, $x_1 \in x^G \cap \mathcal{A}$, $y_1 \in y^G \cap \mathcal{A}$, and A_i, B_i are as in Part (a).

Thus, under the hypothesis of Theorem 1, we obtain the following algorithm to decide if a given $X \in G$ belongs to $(x^k)^G (y^l)^G$.

Step 1. Compute $\mathfrak{s}^i(X)$, $i = 1, 2, \ldots$ (see Definition 1.12) until $\mathfrak{s}^i(X) = \mathfrak{s}^j(X)$ for some $j < i$. Set $\tilde{X} = \mathfrak{s}^i(X)$. We have $\tilde{X} \in \mathrm{SC}(X)$.

Step 2. If $\tilde{X} \in \mathcal{P}$, then check if $\tilde{X} \in (x_1^k y_1^l)^G$ for all pairs of atoms (x_1, y_1) in $(x^G) \times (y^G)$ and finish the computation.

Step 3. Compute $\mathbf{c}^i(\tilde{X})$, $i = 1, 2, \ldots$ (see Definition 1.10) until $\mathbf{c}^i(\tilde{X}) = \tilde{X}$. If some of $\mathbf{c}^i(\tilde{X})$ is of the form (3), then return YES. Otherwise return NO.

Theorem 2. *Let $(G, \mathcal{P}, \Delta)$ be the standard Garside structure on an Artin-Tits group of spherical type. Let k, l be positive integers, $X \in G$ and $x, y \in \mathcal{A}$. Then:*

(a). *$X \in (x^k)^G$ if and only if the left normal form of X is either x_1^k or*

$$\Delta^{-n} \cdot A_n \cdot \ldots \cdot A_2 \cdot A_1 \cdot x_1^{k-1} \cdot x_1 B_1 \cdot B_2 \cdot \ldots \cdot B_n \tag{4}$$

where $n \geq 1$, $x_1 \in x^G \cap \mathcal{A}$ and A_i, B_i are simple elements such that

$$A_i \Delta^{i-1} B_i = \Delta^i, \qquad i = 1, \ldots, n. \tag{5}$$

and

$$A_1 = A_1' x_1, \qquad A_1' \in \mathcal{P}. \tag{6}$$

(b). *$X \in (x^k)^G (y^l)^G$ if and only if either $X \in (x_1^k y_1^l)^G$ or the set of sliding circuits* $\mathrm{SC}(X)$ *contains an element whose left normal form is*

$$\Delta^{-n} \cdot A_n \cdot \ldots \cdot A_1 \cdot x_1^{k-1} \cdot x_1 B_1 \cdot B_2 \cdot \ldots \cdot B_{n-1} \cdot B_n y_1 \cdot y_1^{l-1} \tag{7}$$

where $n \ge 1$, $x_1 \in x^G \cap \mathcal{A}$, $y_1 \in y^G \cap \mathcal{A}$, and A_i, B_i are simple elements which satisfy (5), (6), *and*

$$A_n = \tilde{y}_1 A_n', \qquad \tilde{y}_1 \Delta^n = \Delta^n y_1, \quad A_n' \in \mathcal{P}. \tag{8}$$

When $n = 1$, the expression $x_1 B_1 \cdot B_2 \cdot \ldots \cdot B_n y_1$ in (7) *is understood as $x_1 B_1 y_1$ and conditions* (6) *and* (8) *should be replaced by*

$$A_1 = \tilde{y}_1 A_1'' x_1, \qquad \tilde{y}_1 \Delta = \Delta y_1, \quad A_1'' \in \mathcal{P}. \tag{9}$$

Corollary 3. *Under the hypothesis of Theorem 1 (resp. of Theorem 2), if $X \in (x^k)^G (y^l)^G$ and $\inf_s X < 0$, then $\ell_s(X) = -2\inf_s X + k + l$ (resp. $\ell_s(X) = -2\inf_s X + k + l - 2$), see Definition 1.9.*

Remarks. (1). In Theorem 1(b) we typed the words "any cycling/decycling orbit" in boldface because this is a very important difference between Theorems 1 and 2. A computation of a single cycling or decycling orbit is much easier than a computation of the whole set of sliding circuits. Moreover, though $\mathrm{SC}(X)$ for a random X is usually not very big, there are examples of reducible (see [17; Prop. 9]) and even rigid pseudo-Anosov (see [26]) braids $X \in \mathrm{Br}_n$ of letter length $l = O(n)$ such that $|\,\mathrm{SC}(X)|$ is exponentially large. In contrary, the size of a single cycling orbit of a rigid braid is, of course, bounded by l. It seems plausible that the size of any cycling orbit of any pseudo-Anosov braid is bounded by a polynomial in n, l.

(2). In applications for real algebraic curves, the standard Garside structure is more natural than the dual one. So, it would be interesting to prove the analog of Theorem 2(b) with any cyclic orbit instead of the whole $\mathrm{SC}(X)$.

(3). Theorem 2 extends to any square free homogeneous Garside structures for which Lemma 4.3, and Lemma 4.5 hold (the latter is not needed for Theorem 2(a)).

(4). It seems plausible that Theorem 1(b) (at least for the braid group) remains true if one replaces the words "any cycling orbit in $\mathrm{SC}(X)$" by "any cycling orbit in $\mathrm{USS}(X)$".

(5). We say that a braid in Br_n is *quasipositive* if it is a product of conjugates of standard generators. The *quasipositivity problem* (QPP) in Br_n is the algorithmic problem to decide if a given braid is quasipositive or not. This problem appears very naturally in the study of plane real or complex algebraic curves (see, e. g., [27], [19– 25]). It is solved for $n = 3$ in [22] (see §6).

(6). Let $e : \mathrm{Br}_n \to \mathbb{Z}$ be as above, i. e., $e\big(\prod_j \sigma_{i_j}^{k_j}\big) = \sum k_j$. Usually, $e(X)$ is called the *algebraic length* of X or the *exponent sum* of X. If a braid X is quasipositive, i. e., if $X = \prod_{j=1}^k a_j^{-1} \sigma_{i_j} a_j$, then evidently $k = e(X)$. So, in the case $e(X) < 0$ the braid X is never quasipositive; in the case $e(X) = 0$ it is quasipositive if and only if it is trivial (thus QPP is just the word problem), and if $e(X) = 1$, then QPP is a particular case of the conjugacy problem in Br_n which is solved by Garside [15] but in this case the solution is particularly fast. Indeed, by [5], ElRifai-Morton's algorithm [12] gives the result after $\le \|\delta\|\ell(X)$ cyclings where $\ell(X)$ is the canonical length of X (see Definition 1.7) and Theorem 1(a) shows that $\ell(X)/2$ cyclings is enough. The next case $e(X) = 2$ is covered by Theorem 1(b) or 2(b).

(7). QPP is a particular case of the *class product problem* (CPP) – the algorithmic problem to decide if a given element of a group belongs to the product of a given collection of conjugacy classes. CPP in Br_n for conjugacy classes of the braids of algebraic singularities also naturally arises in the study of plane algebraic curves. So, our result is a solution of CPP in Br_n for the product of two braids of singularities of type A_n. Since the Artin group of type B_n is isomorphic to the group of braids with a distinguished string (see [8; Prop. 5.1]), this case is also important for applications to plane real algebraic curves, especially, when using the method of cubic resolvents (see [24; §4 and Apdx. A, C]).

Example. It is shown in [24; §4.4] that the arrangement of a real pseudoholomorphic quintic curve in $\mathbb{RP}^2$ with respect two lines shown in [24; Fig. 16.12 or Fig. 25.1] is algebraically unrealizable. The proof is based on the fact that $X \notin \sigma_1^G(\sigma_1^4)^G$ where $G = \mathrm{Br}_4$ and $X = \Delta^4\big(\sigma_3^2\sigma_1^{-1}\sigma_2\sigma_1\sigma_3^2\sigma_2^{-1}\sigma_1\sigma_2^3\sigma_3^2\sigma_2^4\sigma_3^2\sigma_1\sigma_2\sigma_1\big)^{-1}$. This fact was proven in [24] using a mixture of Burau and Gassner representations. We have $(\inf_s X, \ell_s(X)) = (-6, 12)$ for the standard Garside structure and $(-6, 14)$ for the dual one. Thus the result follows from Corollary 3 in both cases.

In §5 we give an example which shows the difficulties in the Garside-theoretical approach to QPP for $e(X) \ge 3$. In §6 we give an algorithm for QPP in Br_3 and a C program with its implementation. In §7 we prove a property of the dual Garside structures which we hope to be useful for QPP in the general case.

Acknowledgment. I am grateful to the referee for indicating some mistakes in the first version of the paper and for many very useful advises.

§1. Elements of Garside theory needed for the statement of Theorems 1 and 2

Given a group G and $x, y \in G$, we denote $x^y = y^{-1}xy$ and $x^G = \{x^z \mid z \in G\}$. Garside groups were introduced in [9, 10] as a class of groups to which the technique initiated by Garside [15] and further developed in [15, 6, 11, 7, 13, 12, 4, 5] can be extended. When speaking of Garside groups, we use mostly definitions and notation from [17]. For the reader's convenience we give a summary in this section. A group G is said to be a *Garside group* with *Garside structure* $(G, \mathcal{P}, \Delta)$ if it admits a submonoid $\mathcal{P}$ satisfying $\mathcal{P} \cap \mathcal{P}^{-1} = \{1\}$, called the monoid of *positive elements*, and a special element $\Delta \in P$ called the *Garside element*, such that the following properties hold:

- (G1) The partial order $\preccurlyeq$ defined on G by $a \preccurlyeq b \Leftrightarrow a^{-1}b \in \mathcal{P}$ (which is invariant under left multiplication by definition) is a lattice order. That is, for every $a, b \in G$ there exist a unique least common multiple $a \vee b$ and a unique greatest common divisor $a \wedge b$ with respect to $\preccurlyeq$.
- (G2) The set $[1, \Delta] = \{a \in G \mid 1 \preccurlyeq a \preccurlyeq \Delta\}$, called the set of *simple elements*, generates G.

(G3) Conjugation by Δ preserves $\mathcal{P}$. That is, $(X \in \mathcal{P}) \Longrightarrow (X^\Delta \in \mathcal{P})$.
(G4) For all $X \in \mathcal{P} \setminus \{1\}$, one has:

$$\|X\| = \sup\{k \mid \exists\, a_1, \dots, a_k \in \mathcal{P} \setminus \{1\} \text{ such that } X = a_1 \dots a_k\} < \infty.$$

If $1 \preccurlyeq a \preccurlyeq b$, then we say that a is a *prefix* of b. We write $a \prec b$ if $a \preccurlyeq b$ and $a \neq b$. Similarly to $[1, \Delta]$, we denote: $]1, \Delta] = [1, \Delta] \setminus \{1\}$, $[1, \Delta[= [1, \Delta] \setminus \{\Delta\}$, $]1, \Delta[= [1, \Delta[\setminus \{1\}$. We define the mappings

$$\tau : G \to G,\ \tau(X) = X^\Delta, \qquad \text{and} \qquad \partial : [1, \Delta] \to [1, \Delta],\ \partial A = A^{-1}\Delta.$$

We call ∂A and $\partial^{-1} A$ the *right* and the *left complement of* A respectively. It is clear that $\partial^2 = \tau|_{[1,\Delta]}$ and thus $\tau([1, \Delta]) = [1, \Delta] = \{a \in G \mid \Delta \succcurlyeq a \succcurlyeq 1\}$.

Definition 1.1. A Garside structure $(G, \mathcal{P}, \Delta)$ is said to be *of finite type* if the set of simple elements $[1, \Delta]$ is finite. A group G is called a *Garside group of finite type* if it admits a Garside structure of finite type.

All Garside structures considered in this paper are of finite type.

An element $a \in \mathcal{P} \setminus \{1\}$ is called an *atom* if $a = bc$ with $b, c \in \mathcal{P}$ implies either $a = 1$ or $b = 1$. We denote the set of atoms by $\mathcal{A}$. It is clear that if $X = a_1 \dots a_k$, $a_i \in \mathcal{P}$, $k = \|X\|$, then all a_i are atoms. So, $\mathcal{A}$ generates $\mathcal{P}$ and $\mathcal{A} \subset [1, \Delta]$.

Definition 1.2. A Garside structure $(G, \mathcal{P}, \Delta)$ is called *homogeneous* if for any $X, Y \in \mathcal{P}$ one has $\|XY\| = \|X\| + \|Y\|$. In this case we can define a group homomorphism $e : G \to \mathbb{Z}$ such that $e(\mathcal{A}) = \{1\}$ and $e(X) = \|X\|$ for any $X \in \mathcal{P}$.

Similarly to $\preccurlyeq$ we define the order $\succcurlyeq$ by $a \succcurlyeq b \Leftrightarrow ab^{-1} \in \mathcal{P}$. It is obvious that $a \preccurlyeq b$ is equivalent to $a^{-1} \succcurlyeq b^{-1}$. It follows that $\succcurlyeq$ is also a lattice order and $\mathcal{P} = \{X \mid 1 \preccurlyeq X\} = \{X \mid X \succcurlyeq 1\}$. We denote the lcm and gcd of a and b with respect to the lattice order $\succcurlyeq$ by $a \vee^{\!\rceil} b$ and $a \wedge^{\!\rceil} b$ respectively.

Definition 1.3. A Garside structure is called *symmetric* if for any simple elements u, v one has $u \preccurlyeq v \Leftrightarrow v \succcurlyeq u$.

Definition 1.4. $X \in \mathcal{P}$ is called *square free* if there do not exist $U, V \in \mathcal{P}$ and $x \in \mathcal{A}$ such that $X = Ux^2V$. A Garside structure is called *square free* if all simple elements are square free.

Till the end of this section we suppose that $(G, \mathcal{P}, \Delta)$ is a Garside structure with set of atoms $\mathcal{A}$.

Definition 1.5. Let $A \in \mathcal{P}$. As in [4, 12, 15], we define the *starting set* $S(A)$ and the *finishing set* $F(A)$:

$$S(A) = \{x \in \mathcal{A} \mid x \preccurlyeq A\}, \qquad F(A) = \{x \in \mathcal{A} \mid A \succcurlyeq x\}.$$

If, moreover, $A \in [1, \Delta]$, then, following [4], we define the *right complementary set* $R(A)$ and the *left complementary set* $L(A)$:

$$R(A) = \{x \in \mathcal{A} \mid Ax \preccurlyeq \Delta\}, \qquad L(A) = \{x \in \mathcal{A} \mid \Delta \succcurlyeq xA\}.$$

Or, equivalently, $R(A) = S(\partial A)$ and $L(A) = F(\partial^{-1} A)$.

Definition 1.6. Given two simple elements A, B, we say that the decomposition $AB = A\cdot B$ is *left weighted* if $A = AB\wedge\Delta$ which is equivalent to $B\wedge\partial A = 1$ or to $S(B)\cap R(A) = \varnothing$. We say that the decomposition $AB = A\cdot B$ is *right weighted* if $B = AB\wedge^{\!\!\curvearrowleft}\Delta$ which is equivalent to $A\wedge^{\!\!\curvearrowleft}\partial^{-1}B = 1$ or to $F(A)\cap L(B) = \varnothing$.

In particular, for any $A\in\,]1,\Delta[$, the decompositions $A\cdot 1$ and $\Delta\cdot A$ are left weighted whereas $A\cdot\Delta$ and $1\cdot A$ are not.

Definition 1.7. Given $X\in G$, we say that a decomposition

$$X = \Delta^p\cdot A_1\cdot A_2\cdot\ldots\cdot A_r \tag{10}$$

is the *left normal form* of X if $A_i\in\,]1,\Delta[$ for $i = 1,\ldots,r$ and $A_i\cdot A_{i+1}$ is left weighted for $i = 1,\ldots,r-1$. In this case we define the *infimum*, the *canonical length* and the *supremum* of X respectively by $\inf X = p$, $\ell(X) = r$, $\sup X = p+r$. In [15], $\inf X$ is called the *power* of X.

Convention 1.8. Given $A, B\in G$, we use both notations AB and $A\cdot B$ for the product in G. However, if a mixed notation is used (e. g., $X = AB\cdot C\cdot D$) and we say that this decomposition is left/right weighted or in left/right normal form, then we mean that the dots separate simple elements and each consecutive pair of these simple elements is left/right weighted. If x is an atom and an expression x^k appears in a left/right normal form (as in Theorems 1 and 2), then it stands for $x\cdot\ldots\cdot x$ (k times) and, of course, $A\cdot x^k\cdot B$ means $A\cdot B$ when $k = 0$.

Definition 1.9. Let $X\in G$. The *summit infimum*, the *summit supremum*, and the *summit length* of X are defined as $\inf_s X = \max\{\inf Y \mid Y\in X^G\}$, $\sup_s X = \min\{\sup Y \mid Y\in X^G\}$, $\ell_s(X) = \min\{\ell(Y)\mid Y\in X^G\}$. The *super summit set* of X is $\mathrm{SSS}(X) = \{Y\in X^G\mid \ell(Y) = \ell_s(X)\}$. It is shown in [12] that $\ell_s(X) = \sup_s X - \inf_s X$ and thus

$$\mathrm{SSS}(X) = \{Y\in X^G \mid \inf Y = \inf_s X \text{ and } \sup Y = \sup_s X\}.$$

Definition 1.10. Let $X\in G$, $\ell(X) > 0$, and let (10) be its left normal form. We define the *initial factor* and the *final factor* of X as $\iota(X) = \tau^{-p}(A_1)$ and $\varphi(X) = A_r$. So, we have $X = \iota(X)\Delta^p A_2\ldots A_{r-1}\varphi(X)$ when $r > 1$ and we have $X = \iota(X)\Delta^p = \Delta^p\varphi(X)$ when $r = 1$. We define the *cycling* and the *decycling* of X as $\mathbf{c}(X) = X^{\iota(X)} = \Delta^p A_2\ldots A_r\,\iota(X)$ and $\mathbf{d}(X) = \mathbf{c}(X^{-1})^{-1} = X^{\varphi(X)^{-1}} = A_r\Delta^p A_1\ldots A_{r-1}$.

Definition 1.11. Let $X\in G$. The *ultra summit set* of X is

$$\mathrm{USS}(X) = \{Y\in\mathrm{SSS}(X)\mid \mathbf{c}^k(Y) = Y \text{ for some } k > 0\}.$$

The *restricted super summit set* of X is

$$\mathrm{RSSS}(X) = \{Y\in\mathrm{SSS}(X)\mid \mathbf{c}^k(Y) = \mathbf{d}^m(Y) = Y \text{ for some } k, m > 0\}.$$

If $Y\in\mathrm{USS}(X)$, we define the *cycling orbit* of Y as $\{\mathbf{c}^k(Y)\mid k\geq 0\}$. Similarly, if $\mathbf{d}^k(Y) = Y$ for some $k>0$, then we define the *decycling orbit* of Y as $\{\mathbf{d}^k(Y)\mid k\geq 0\}$.

Definition 1.12. Let $X \in G$ and let (10) be its left normal form. The *preferred prefix* of X is $\mathfrak{p}(X) = \iota(X) \wedge \partial(\varphi(X))$. In other words, $\mathfrak{p}(X)$ is the greatest positive u such that $u \preccurlyeq \iota(X)$ and $\varphi(X)u \preccurlyeq \Delta$. The *cyclic sliding* of X is $\mathfrak{s}(X) = X^{\mathfrak{p}(X)}$. The *set of sliding circuits* of X is

$$\mathrm{SC}(X) = \{Y \in X^G \mid \mathfrak{s}^m(Y) = Y \text{ for some } m > 0\}.$$

Remark 1.13. By [17; Prop. 2], we have $\mathrm{SC}(X) \subset \mathrm{RSSS}(X)$ and if $\ell_s(X) > 1$, then $\mathrm{SC}(X) = \mathrm{RSSS}(X)$. Thus, $\mathrm{SC}(X)$ is a disjoint union of cycling orbits as well as a disjoint union of decycling orbits.

§2. Elements of Garside theory used in the proofs of Theorems 1 and 2

Let $(G, \mathcal{P}, \Delta)$ be a Garside structure of finite type with set of atoms $\mathcal{A}$.

Lemma 2.1. *Let $A \in [1, \Delta]$ and $B = \partial A$, i. e., $AB = \Delta$. Then $S(B) = R(A)$ and $F(A) = L(B)$.*

Proof. $x \in S(B) \Leftrightarrow (\exists B' \in \mathcal{P},\ B = xB') \Leftrightarrow (\exists B' \in \mathcal{P},\ \Delta = AxB') \Leftrightarrow x \in R(A)$. Thus $S(B) = F(A)$. Symmetrically, $F(A) = L(B)$. □

Lemma 2.2. [12; p. 482]. *For any $X, Y \in G$ one has $\ell(XY) \le \ell(X) + \ell(Y)$.* □

Lemma 2.3. [7; Lemma 2.4]. *Let $X, Y \in \mathcal{P}$ and let $Y_1 = \Delta \wedge Y$. Then $\Delta \wedge (XY) = \Delta \wedge (XY_1)$.* □

Lemma 2.4. *Suppose that $X = X_1 \cdot \ldots \cdot X_n$ is right weighted and $Y = Y_1 \cdot \ldots \cdot Y_m$ is left weighted. If $\Delta \preccurlyeq XY$, then $\Delta \preccurlyeq X_n Y_1$.*

Proof. The condition $\Delta \preccurlyeq XY$ can be rewritten as $\Delta \wedge (XY) = \Delta$. Hence, by Lemma 2.3, we have $\Delta = \Delta \wedge (XY) = \Delta \wedge (XY_1)$, i. e., $\Delta \preccurlyeq XY_1$ and hence $XY_1 \succcurlyeq \Delta$. Then the analog of Lemma 2.3 for $\wedge^{\urcorner}$ yields $\Delta = \Delta \wedge^{\urcorner} (XY_1) = \Delta \wedge^{\urcorner} (X_n Y_1)$. □

Definition 2.5. The *local sliding* is the mapping $\mathfrak{ls} : [1, \Delta]^2 \to [1, \Delta]^2$ defined by $\mathfrak{ls}(u, v) = (us, s^{-1}v)$ where $s = v \wedge \partial u$. Thus, if $(u', v') = \mathfrak{ls}(u, v)$, then $u'v' = uv$ and $u' \cdot v'$ is left weighted.

Lemma 2.6. [7; Prop. 3.1]. *Suppose that $X = A_1 \cdot A_2 \cdot \ldots \cdot A_r$ is in left normal form and let A_0 be a simple element. Then the decomposition $A_0 X = A'_0 \cdot A'_1 \cdot \ldots \cdot A'_r$ is left weighted where the A'_i's are defined recursively together with simple elements $t_0, \ldots, t_r$ by $t_0 = A_0$, $(A'_{i-1}, t_i) = \mathfrak{ls}(t_{i-1}, A_i)$, $i = 1, \ldots, r$, and $A'_r = t_r$. We have $A'_i \ne \Delta$ for $i > 0$ and $A'_i \ne 1$ for $i < r$ (but it is possible that $A'_0 = \Delta$ or $A'_r = 1$).*

Thus, if we set $s_i = A_i \wedge \partial t_{i-1}$, then we have $A_i = s_i t_i$ and $A'_{i-1} = t_{i-1} s_i$ for $1 \le i \le r$, and the left normal forms of X and $A_0 X$ are:

$$\begin{aligned} X &= \quad s_1 t_1 \cdot s_2 t_2 \cdot \ \ \ldots \ \ \cdot s_r t_r \\ A_0 X &= t_0 s_1 \cdot t_1 s_2 \cdot \ldots \cdot t_{r-1} s_r \cdot t_r \end{aligned}$$

where the last factor t_r should be removed if it is equal to 1.

Corollary 2.7. *Let the notation be as in Lemma 2.6. Suppose that A_j is an atom for some $j < r$. Then $\varphi(t_0X) = A_r$.*

Proof. Let A'_i, s_i and t_i, $1 \le i \le r$, be as in Lemma 2.6. Since $A_j = s_jt_j$ is an atom, we have either $s_j = 1$ or $t_j = 1$.

If $s_j = 1$, then $t_j = A_j$. Since $A_j \cdot A_{j+1} = t_j \cdot s_{j+1}t_{j+1}$ is left weighted, it follows that $s_{j+1} = 1$, and we obtain by induction that $A'_i = A_i$ for $i \ge j$, hence $\varphi(t_0X) = A'_r = A_r$.

If $t_j = 1$, then $A'_j = s_{j+1}$, hence $t_{j+1} = 1$ because otherwise $A'_j \cdot A'_{j+1} = s_{j+1} \cdot t_{j+1}s_{j+2}$ would not be left weighted. Hence $A'_j = A_{j+1}$ and we obtain by induction $A'_i = A_{i+1}$, $j \le i < r$, and $A'_r = 1$. Thus $\varphi(t_0X) = A'_{r-1} = A_r$. $\square$

Informally speaking, Lemma 2.6 means that if a product of elements is left weighted everywhere except the first pair of elements, then it can be put into left normal form in one passage from the left to the right: first we make left weighted the leftmost pair of elements, then the next pair, and so on. Similarly, the next lemma shows that if a product of elements is left weighted everywhere except the last pair of elements, then it can be put into the left normal form in one passage from the right to the left.

Lemma 2.8. [7; Prop. 3.3]. *Suppose that $X = A_1 \cdot A_2 \cdot \ldots \cdot A_r$ is in left normal form and let A_{r+1} be a simple element. Then the decomposition $XA_{r+1} = A''_1 \cdot \ldots \cdot A''_{r+1}$ is left weighted where the A''_i's are defined recursively together with simple elements $A'_1, \ldots, A'_r$ by $A'_{r+1} = A_{r+1}$, $(A'_i, A''_{i+1}) = \mathfrak{ls}(A_i, A'_{i+1})$, $i = r, \ldots, 1$, $A''_1 = A'_1$. We have $A''_i \ne \Delta$ for $i > 1$ and $A''_i \ne 1$ for $i \le r$ (but it is possible that $A''_1 = \Delta$ or $A''_{r+1} = 1$).*

Thus one has

$$\begin{aligned}
XA_{r+1} &= (A_1 \cdot A_2 \cdot A_3 \cdot \ldots \cdot A_{r-2} \cdot A_{r-1} \cdot A_r)\; A_{r+1} \\
&= (A_1 \cdot A_2 \cdot A_3 \cdot \ldots \cdot A_{r-2} \cdot A_{r-1})(A'_r \cdot A''_{r+1}) \\
&= (A_1 \cdot A_2 \cdot A_3 \cdot \ldots \cdot A_{r-2})(A'_{r-1} \cdot A''_r \cdot A''_{r+1}) \\
&\qquad\qquad \cdots\cdots\cdots \\
&= \;\; A_1\,(A'_2 \cdot A''_3 \cdot \ldots \cdot A''_{r-2} \cdot A''_{r-1} \cdot A''_r \cdot A''_{r+1}) \\
&= (A''_1 \cdot A''_2 \cdot A''_3 \cdot \ldots \cdot A''_{r-2} \cdot A''_{r-1} \cdot A''_r \cdot A''_{r+1})
\end{aligned}$$

where all the products in the parentheses are left weighted. In particular, the left normal form of XA_{r+1} is the last line with the factor A''_{r+1} removed if it is equal to 1. $\square$

Corollary 2.9. *Let* (10) *be the left normal form of X. Let $\tilde{A}_1 = \tau^{-p}(A_1)$.*

(a). *Suppose that $2 \le j \le r$. Let $Y = A_j \ldots A_r\, \tilde{A}_1$ and let $A''_j \cdot \ldots \cdot A''_r \cdot \tilde{A}''_1$ be the left weighted decomposition of Y. Then $\mathfrak{s}(X) = \Delta^p A''_1 A_2 \ldots A_{j-1} A''_j \ldots A''_r$ where $A''_1 = \tau^p(\tilde{A}''_1)$.*

(b). *Suppose that $3 \le j \le r$ and $A_{j-1} = BC$ where $B, C \in \mathcal{P}$ and $C \cdot A_j$ is left weighted. Let $Y = CA_j \ldots A_r\, \tilde{A}_1$ and let $C'' \cdot A''_j \cdot \ldots \cdot A''_r \cdot \tilde{A}''_1$ be the left weighted decomposition of Y. Then $\mathfrak{s}(X) = \Delta^p A''_1 A_2 \ldots A_{j-2} BC'' A''_j \ldots A''_r$ where $A''_1 = \tau^p(\tilde{A}''_1)$.* $\square$

Lemma 2.10. (See [17; Lemma 4]). If $\ell(X) \ge 2$ and either $\ell(\mathbf{c}(\mathbf{d}(X)) = \ell(X)$ or $\ell(\mathbf{d}(\mathbf{c}(X)) = \ell(X)$, then $\mathbf{c}(\mathbf{d}(X)) = \mathbf{d}(\mathbf{c}(X)) = \mathfrak{s}(X)$. □

Corollary 2.11. *If $\ell(X) \ge 2$ and $X \in \mathrm{SC}(X)$, then $\mathbf{c}(\mathbf{d}(X)) = \mathbf{d}(\mathbf{c}(X)) = \mathfrak{s}(X)$.*

Lemma 2.12. $\mathrm{SC}(X)$ *is invariant under τ, $\mathbf{c}$, and $\mathbf{d}$.*

Proof. If $\ell_s(X) = 1$, then the statement is evident. If $\ell_s(X) \ge 2$, then it follows from the fact that $\mathrm{SC}(X) = \mathrm{RSSS}(X)$ (see Remark 1.13) combined with Corollary 2.11. □

Lemma 2.13. [17; Prop. 7]. *Let $X \in G$ and let s, t be elements of G such that $X^s \in \mathrm{SC}(X)$ and $X^t \in \mathrm{SC}(X)$. Then $X^{s\wedge t} \in \mathrm{SC}(X)$.*

Definition 2.14. Let $X \in G$ and $s \in \mathcal{P} \setminus \{1\}$. We say that s is an SC-*minimal conjugator* for X if $X^s \in \mathrm{SC}(X)$ and $X^t \notin \mathrm{SC}(X)$ for any t such that $1 \prec t \prec s$. Since $Y \in \mathrm{SC}(X) \Rightarrow Y^\Delta \in \mathrm{SC}(X)$, it follows from Lemma 2.13 that all SC-minimal conjugators for the elements of $\mathrm{SC}(X)$ are simple elements. We define the *sliding circuits graph* $\mathrm{SCG}(X)$ as the directed graph whose set of vertices is $\mathrm{SC}(X)$ and whose arrows starting at a vertex Y are the SC-minimal conjugators for Y. If s is an SC-minimal conjugator for Y, then the corresponding arrow connects Y to Y^s.

The following statement is an analog of [3; Th. 2.5] for $\mathrm{SC}(X)$ instead of $\mathrm{USS}(X)$.

Lemma 2.15. *Let $X \in \mathrm{SC}(X)$ and let s be an* SC-*minimal conjugator for X. Then one and only one of the following conditions holds:*

(1) *$\varphi(X)s$ is a simple element.*
(2) *$\varphi(X) \cdot s$ is left weighted.*

Proof. Repeat word-by-word the proof of [3; Th. 2.5] replacing USS by SC and using Lemma 2.12 and Lemma 2.13 instead of [3; Lemma 2.5] and [3; Th. 1.13] respectively. □

Corollary 2.16. *Let $X \in \mathrm{SC}(X)$ with $\ell(X) > 0$ and let s be an* SC-*minimal conjugator for X. Then s is a prefix of either $\iota(X)$ or $\partial\varphi(X)$, or both.*

Proof. Repeat word-by-word the proof of [3; Cor. 2.7]. □

Similarly to [3; §2], we distinguish two kinds of arrows of the graph $\mathrm{SCG}(X)$. We say that an arrow s starting at Y is *black* if s is a prefix of $\iota(Y)$, and *grey* if it is a prefix of $\partial\varphi(Y)$ or, equivalently, if $\varphi(Y)s$ is a simple element. Note that some arrows may be both black and grey.

Definition 2.17. Let $X \in G$ and $u \in \mathcal{P}$. We define the $\mathbf{c}$-*transport* of u at X as $\mathbf{c}_X(u) = \iota(X)^{-1} u\, \iota(X^u)$, thus $\mathbf{c}(X^u) = \mathbf{c}(X)^{u'}$ for $u' = \mathbf{c}_X(u)$. Similarly we define the $\mathfrak{s}$-*transport* of u at X as $\mathfrak{s}_X(u) = \mathfrak{p}(X)^{-1} u\, \mathfrak{p}(X^s)$, thus $\mathfrak{s}(X^u) = \mathfrak{s}(X)^{u'}$ for $u' = \mathfrak{s}_X(u)$, i. e., the following diagrams commute (arrows are conjugations):

$$\begin{array}{ccc} X & \xrightarrow{\iota(X)} & \mathbf{c}(X) \\ u\downarrow & & \downarrow \mathbf{c}_X(u) \\ X^u & \xrightarrow[\iota(X^u)]{} & \mathbf{c}(X^u) \end{array} \qquad \begin{array}{ccc} X & \xrightarrow{\mathfrak{p}(X)} & \mathfrak{s}(X) \\ u\downarrow & & \downarrow \mathfrak{s}_X(u) \\ X^u & \xrightarrow[\mathfrak{p}(X^u)]{} & \mathfrak{s}(X^u) \end{array}$$

It is pointed out in [17; p. 98] that $\mathrm{SC}(X)$ can be viewed as a category and then $\mathfrak{s}$ becomes a functor which is a category isomorphism. The same is true for $\mathbf{c}$. Let us give precise definitions and statements.

Definition 2.18. For $X \in G$ we define the *sliding circuits category* $\mathcal{SC}(X)$. The set of objects is $\mathrm{SC}(X)$. Given $Y, Z \in \mathrm{SC}(X)$, we define the set of morphisms from Y to Z as $\mathrm{Hom}(Y,Z) = \{u \in \mathcal{P} \mid Y^u = Z\}$.

Proposition 2.19. (a). *The mappings* $\mathbf{c}, \mathfrak{s} : \mathrm{SC}(X) \to \mathrm{SC}(X)$ *and*

$$\mathbf{c}_Y : \mathrm{Hom}(Y,Z) \to \mathrm{Hom}(\mathbf{c}(Y), \mathbf{c}(Z)), \qquad \mathfrak{s}_Y : \mathrm{Hom}(Y,Z) \to \mathrm{Hom}(\mathfrak{s}(Y), \mathfrak{s}(Z))$$

define functors of $\mathcal{SC}(X)$ *to itself.*

(b). *These functors are automorphisms of the category* $\mathcal{SC}(X)$.

Proof. (a). Follows from the invariance of $\mathrm{SC}(X)$ under $\mathbf{c}$ and $\mathfrak{s}$ (see Lemma 2.12). . (b). Follows from [16; Lemma 2.6] and [17; Lemma 8]. $\square$

Since the functors $\mathbf{c}|_{\mathrm{SC}(X)}$ and $\mathfrak{s}|_{\mathrm{SC}(X)}$ are bijective, we may define their inverses which we denote by $\mathbf{c}^{-1}$ and $\mathfrak{s}^{-1}$. If $\ell(X) \ge 2$, then we may define the functor $\mathbf{d} : \mathcal{SC}(X) \to \mathcal{SC}(X)$ by setting $\mathbf{d} = \mathfrak{s} \circ \mathbf{c}^{-1}$. By Corollary 2.11, the restriction of this functor to the set of object $\mathrm{SC}(X)$ coincides with the decycling operator $\mathbf{d}$ defined above.

Remark. In fact, we could define the functor $\mathbf{d}$ as $\mathbf{c}^{-1} \circ \mathfrak{s}$ as well. We do not know if these definitions are equivalent or not but any of them is equally good for our purposes (for the proof of Part (b) of Lemma 3.7).

Let $M(X) = \{(Y,u) \in \mathrm{SC}(X) \times \mathcal{P} \mid Y^u \in \mathrm{SC}(X)\}$ – all morphisms of $\mathcal{SC}(X)$. Let us define $\mathbf{c}_*, \mathfrak{s}_* : M(X) \to M(X)$ by setting $\mathbf{c}_*(X,s) = (\mathbf{c}(X), \mathbf{c}_X(s))$ and $\mathfrak{s}_*(X,s) = (\mathfrak{s}(X), \mathfrak{s}_X(s))$. Proposition 2.19 implies that these mappings are invertible, so we may define $\mathbf{d}_*$ as $\mathfrak{s}_* \circ \mathbf{c}_*^{-1}$.

Corollary 2.20. *Let* $X \in \mathrm{SC}(X)$ *and let* s *be an* SC*-minimal conjugator for* X. *Let* (X', s') *be* $\mathbf{c}_*^m(X,s)$, $\mathbf{d}_*^m(X,s)$, *or* $\mathfrak{s}_*^m(X,s)$, $m \in \mathbb{Z}$. *Then* s' *is an* SC*-minimal conjugator for* X'.

In particular, $\mathbf{c}_*^m$, $\mathbf{d}_*^m$, *and* $\mathfrak{s}_*^m$ *define automorphisms of the graph* $\mathrm{SCG}(X)$. $\square$

3. Symmetric homogeneous case: proof of Theorem 1

Let $(G, \mathcal{P}, \delta)$ be a **symmetric homogeneous** Garside structure of finite type with set of atoms $\mathcal{A}$. The following simple observation will be used again and again in this section.

Lemma 3.1. *Let* x *be an atom and* A *a simple element. If* $x \in L(A)$, *then there exists* $x_1 \in x^G \cap \mathcal{A}$ *such that* $xA = Ax_1$ *and hence* $x^k A = A x_1^k$ *for any* k.

If $x \in R(A)$, *then there exists* $x_1 \in x^G \cap \mathcal{A}$ *such that* $Ax^k = x_1^k A$ *for any* k.

Proof. Let $x \in L(A)$. Then xA is a simple element. Since the Garside structure is symmetric, we have $A \preccurlyeq xA$, i. e., $xA = Ax_1$ for some $x_1 \in \mathcal{P}$. Since, moreover, the Garside structure is homogeneous, we have $\|x_1\| = \|Ax_1\| - \|A\| = \|xA\| - \|A\| = \|x\| = 1$, thus $x_1 \in \mathcal{A}$. Since $x_1 = x^A$, we have $x_1 \in x^G$. The case $x \in R(L)$ is similar. $\square$

Note that for any $u \in G$, $k \in \mathbb{Z}$, we have $(x^k)^u = (x_1^k)^P$ where $u = \delta^{\inf u} P$ (thus $\inf P = 0$) and $x_1 = \tau^{\inf u}(x) \in x^G \cap \mathcal{A}$. Hence, Part (a) of Theorem 1 is an immediate consequence from the following fact.

Lemma 3.2. *Under the hypothesis of Theorem 1, suppose that $X = (x_1^k)^P$ with $x_1 \in x^G \cap \mathcal{A}$ and $\inf P = 0$. Let $P = B_1 \cdot \ldots \cdot B_n$, $n \geq 1$, be the left normal form of P and let $A_1, \ldots, A_n$ be defined by (2). Then either (1) is the left normal form of X or there exist $x_2 \in x^G \cap \mathcal{A}$ and $Q \in \mathcal{P}$ such that $X = (x_2^k)^Q$, $\|Q\| < \|P\|$, and $\ell(Q) \leq \ell(P)$.*

Proof. Suppose that such x_2 and Q do not exist. Let us show that (1) is left weighted. We should check that if C_1 and C_2 are two successive factors in (1) (not including δ^{-n}), then $R(C_1) \cap S(C_2) = \varnothing$. We consider all possible cases for (C_1, C_2).

Case 1. $(C_1, C_2) = (B_i, B_{i+1})$. Follows from the fact that $B_1 \cdot \ldots \cdot B_n$ is the left normal form of P.

Case 2. $(C_1, C_2) = (x_1, B_1)$. Suppose that $y \in R(x_1) \cap S(B_1)$. Since $y \in S(B_1)$, we have $y \preccurlyeq B_1 \preccurlyeq P$. Hence $P = yQ$ with $Q \in \mathcal{P}$, $\|Q\| < \|P\|$, and $\ell(Q) \leq \ell(P)$. Since $y \in R(x_1)$, we have $x_1 \in L(y)$. By Lemma 3.1, this implies $x_1 y = y x_2$ for some $x_2 \in x^G \cap \mathcal{A}$. and we obtain $X = P^{-1} x_1^k y Q = P^{-1} y x_2^k Q = Q^{-1} x_2^k Q$. Contradiction.

Case 3. $(C_1, C_2) = (x_1, x_1)$. Follows from the condition that the Garside structure is square free when $k \geq 2$.

Case 4. $(C_1, C_2) = (A_1, x_1)$. Suppose that $R(A_1) \cap S(x_1) \neq \varnothing$. Since $S(x_1) = \{x_1\}$, this means that $x_1 \in R(A_1)$. Hence $A_1 x_1 = x_2 A_1$ for some $x_2 \in x^G \cap \mathcal{A}$ by Lemma 3.1. Thus, denoting $B_2 \ldots B_n$ by Q, we obtain $X = Q^{-1} \delta^{-1} A_1 x_1^k B_1 Q = Q^{-1} \delta^{-1} x_2^k A_1 B_1 Q = Q^{-1} x_3^k Q$ for $x_3 = \tau(x_2) \in x^G \cap \mathcal{A}$. Evidently, $\|Q\| < \|P\|$, and $\ell(Q) < \ell(P)$. Contradiction.

Case 5. $(C_1, C_2) = (A_{i+1}, A_i)$. Follows from the fact that $B_i \cdot B_{i+1}$ is left weighted (see, e. g., [3; Remark 1.8] or [12; proof of Prop. 4.5]). $\square$

The rest of this section is devoted to the proof of Theorem 1(b). So, let us fix $x, y \in \mathcal{A}$ and $k, l \geq 1$. Let

$$\mathcal{Q}_m = \{P^{-1} x_1^k P y_1^l \mid \ell(P) \leq m, x_1 \in x^G, y_1 \in y^G\}, \tag{11}$$

For any $X \in (x^k)^G (y^l)^G$ we set

$$\operatorname{len}_{\mathcal{Q}}(X) = \min\{m \mid \mathcal{Q}_m \cap X^G \neq \varnothing\}, \tag{12}$$

$$\mathcal{Q}_{\min}(X) = \mathcal{Q}_n \cap X^G \text{ where } n = \operatorname{len}_{\mathcal{Q}}(X). \tag{13}$$

If $\operatorname{len}_{\mathcal{Q}}(X) = 0$, then the conclusion of Theorem 2(b) holds by definition of $\operatorname{len}_{\mathcal{Q}}(X)$, so we shall consider the case when $\operatorname{len}_{\mathcal{Q}}(X) > 0$.

From now on $x_1, x_2, \ldots$ and $y_1, y_2, \ldots$ will always denote some atoms which are conjugate to x and y respectively.

Lemma 3.3. *If $X \in \mathcal{Q}_{\min}(X)$ and $\operatorname{len}_{\mathcal{Q}}(X) > 0$, then the left normal form of X is as stated in Theorem 1(b) with $n = \operatorname{len}_{\mathcal{Q}}(X)$.*

Proof. Let $X \in \mathcal{Q}_{\min}(X)$. Then $X = P^{-1} x_1^k P y_1^l$ with $\ell(P) = n = \operatorname{len}_{\mathcal{Q}}(X)$. Without loss of generality we may assume that $\inf P = 0$ (otherwise we replace x_1 by $\tau^{\inf P}(x_1)$) and $\|P\|$ is the minimal possible among all presentations of X in this form. Let $P = B_1 \cdot \ldots \cdot B_n$ be the left normal form of P and let

$A_1, \dots, A_n$ be defined by (2). Then (3) represents X. Let us show that (3) is left weighted. By Lemma 3.2, the part $\delta^{-n} \cdot A_n \cdot \dots \cdot B_n$ of (3) is left weighted, so, it remains to prove that $B_n \cdot y_1$ is left weighted. Suppose that it is not. Then $y_1 \in R(B_n)$ and, by Lemma 3.1, we obtain $B_n y_1^l = y_2^l B_n$. Thus X is conjugate to $B_n \delta^{-n} A_n \dots A_1 x_1^k B_1 \dots B_{n-1} y_2^l = \delta^{-(n-1)} A_{n-1} \dots A_1 x_1^k B_1 \dots B_{n-1} y_2^l$ which contradicts the fact that $n = \mathcal{Q}_{\min}(X)$. $\square$

Lemma 3.4. *If $X \in \mathcal{Q}_{\min}(X)$ and $\operatorname{len}_{\mathcal{Q}}(X) > 0$, then $\mathfrak{s}(X) \in \mathcal{Q}_{\min}(X)$.*

Proof. By Lemma 3.3, we may assume that the left normal form of X is (3) with $n = \operatorname{len}_{\mathcal{Q}}(X)$. Let $A = A_{n-1} \dots A_1$ and $B = B_1 \dots B_{n-1}$. Let $u = \mathfrak{p}(X)$ (see Definition 1.12). Then we have $A_n = \tau^{-n}(u) A'_n$, $A'_n \in \mathcal{P}$, and $y_1 u \preccurlyeq \delta$. In particular, we have $y_1 \in L(u)$, hence Lemma 3.1 implies $y_1^l u = u y_2^l$. By (2) we have also $\tau^{-n}(u) A'_n \delta^{n-1} B_n = \delta^n$ which is equivalent to $\tau^{n-1}(A'_n) B_n u = \delta$. Thus $B_n u$ is a simple element and we obtain $\mathfrak{s}(X) = \delta^{-n} A'_n A x_1^k B B_n y_1^l u = \delta^{-n} A'_n A x_1^k B B_n u y_2^l = P^{-1} x_1^k P y_2^l$ where P is a product of n simple elements: $P = B_1 \cdot \dots \cdot B_{n-1} \cdot B_n u$. Hence $\ell(P) \le n$ and we obtain $\mathfrak{s}(X) \in \mathcal{Q}_n = \mathcal{Q}_{\min}(X)$. $\square$

Corollary 3.5. *If $X \in (x^k)^G (y^l)^G$, $\operatorname{len}_{\mathcal{Q}}(X) > 0$, then $\operatorname{SC}(X) \cap \mathcal{Q}_{\min}(X) \neq \varnothing$.* $\square$

Thus, $\operatorname{SC}(X)$ contains at least one element of the desired form if $\operatorname{len}_{\mathcal{Q}}(X) > 0$.

Lemma 3.6. *Let $X \in \operatorname{SC}(X) \cap \mathcal{Q}_{\min}(X)$, $\operatorname{len}_{\mathcal{Q}}(X) > 0$, and let s be an SC-minimal conjugator for X. Then:*

(a). *If $\varphi(X)s \prec \delta$, i. e., if the arrow $X \xrightarrow{s} X^s$ is grey, then either X^s or $\mathbf{c}(X^s)$ is in $\mathcal{Q}_{\min}(X)$.*

(b). *If $\varphi(X) \cdot s$ is left weighted, i. e., if the arrow $X \xrightarrow{s} X^s$ is black, then $\mathbf{d}(X^s) = X$.*

Proof. Let $X = P^{-1} x_1^k P y_1^l$ with $P \in \mathcal{P}$, $\ell(P) = n = \operatorname{len}_{\mathcal{Q}}(X)$. We have $\ell(X) = k + l + 2n$ by Lemma 3.3.

(a). Since $\varphi(X)s = y_1 s \preccurlyeq \delta$, we have $y_1^l s = s y_2^l$ by Lemma 3.1. Hence $X^s = X_0 y_2^l$ where $X_0 = (Ps)^{-1} x_1^k (Ps)$. It follows from Lemma 3.2 that $\ell(X_0) = 2m + k$ and $X^s \in \mathcal{Q}_m$ with $m \le \ell(Ps) \le n + 1$. Since $n = \operatorname{len}_{\mathcal{Q}}(X)$, it follows that $m \ge n$ and if $m = n$, then $X^s \in \mathcal{Q}_{\min}(X)$ and we are done. So, we suppose that $m = n + 1$. Then $X_0 = \delta^{-(n+1)} X_1$ where $X_1 \in \mathcal{P}$ and, by the "right-to-left version" of Lemma 3.2, the right normal form of X_1 is $A_{n+1} \cdot \dots \cdot A_1 \cdot x_2^k \cdot B_1 \cdot \dots \cdot B_{n+1}$ with A_i, B_i satisfying (2) for $i = 1, \dots, n+1$. Since $X^s \in \operatorname{SC}(X)$, we have $\inf X^s = \inf X = n$ which implies that $\delta \prec X_1 y_2^l$. Since $y_2^l = y_2 \cdot \dots \cdot y_2$ is the left normal form of y_2^l, it follows from Lemma 2.4 that $\delta \preccurlyeq B_{n+1} y_2$. Since $\|y_2\| = 1$ and $\|B_{n+1}\| < \|\delta\|$, this yields $B_{n+1} y_2 = \delta$. This fact combined with $A_{n+1} \delta^n B_{n+1} = \delta^{n+1}$ implies $A_{n+1} = \tau^{-(n+1)}(y_2)$, thus

$$\begin{aligned} X^s &= \delta^{-(n+1)} \cdot \tau^{-(n+1)}(y_2) \cdot A_n \cdot \dots \cdot A_1 \cdot x_2^k \cdot B_1 \cdot \dots \cdot B_n \cdot \delta \cdot y_2^{l-1} \\ &= \delta^{-n} \cdot \tau^{-n}(y_2) \cdot \tau\bigl(A_n \cdot \dots \cdot A_1 \cdot x_2^k \cdot B_1 \cdot \dots \cdot B_n\bigr) \cdot y_2^{l-1} \\ &= \delta^{-n} \cdot \tau^{-n}(y_2) \cdot A'_n \cdot \dots \cdot A'_1 \cdot x_3^k \cdot B'_1 \cdot \dots \cdot B'_n \cdot y_2^{l-1} \end{aligned}$$

where $A'_n \cdot \dots \cdot A'_1 \cdot x_3^k \cdot B'_1 \cdot \dots \cdot B'_n$ is the left normal form of $\tau(A_n \dots A_1 x_2^k B_1 \dots B_n)$. The number of simple factors in this decomposition of X^s is equal to $k + l + 2n = \ell(X^s)$. Hence, by Lemma 2.6, we have $\iota(X^s) = y_2 t$ with $t \preccurlyeq \tau^n(A'_n)$. Then we have

$y_2t = ty_3$ by Lemma 3.1. Since $\tau^{-n}(t) \preccurlyeq A'_n$, we have also $A'_n = \tau^{-n}(t)u$ where u is a simple element. Hence, we obtain

$$\begin{aligned}\mathbf{c}(X^s) &= \delta^{-n}uA'_{n-1}\dots A'_1x_3^kB'_1\dots B'_ny_2^lt\\ &= \delta^{-n}\cdot u\cdot A'_{n-1}\cdot\ldots\cdot A'_1\cdot x_3^k\cdot B'_1\cdot\ldots\cdot B'_{n-1}\cdot B'_nt\cdot y_3^l\end{aligned}$$

Since $u\cdot\delta^{n-1}\cdot B'_nt = \delta^n$, we conclude that $\mathbf{c}(X^s)\in\mathcal{Q}_{\min}(X)$.

(b). Let the left normal form of X be as in (3). We have $1 \prec s \preccurlyeq st = \iota(X) = \tau^n(A_n)$. Hence

$$X^s = \delta^{-n}\cdot\tau^{-n}(t)\bigl(A_{n-1}\cdot\ldots\cdot A_1\cdot x_1^k\cdot B_1\cdot\ldots\cdot B_n\cdot y_1^l\cdot s\bigr).$$

Since the tail of this decomposition starting with A_{n-1} is left weighted, we have $\varphi(X^s) = s$ by Corollary 2.7, hence $\mathbf{d}(X^s) = X$. $\square$

Lemma 3.7. (a). *Let $X \in \mathrm{SC}(X)$, $\mathrm{len}_{\mathcal{Q}}(X) > 0$, and let s be an* SC*-minimal conjugator for X. Suppose that the cycling orbit of X contains an element of $\mathcal{Q}_{\min}(X)$. Then the cycling orbit of X^s also contains an element of $\mathcal{Q}_{\min}(X)$.*

(b)*. The same statement for the decycling orbits.*

Proof. (a). Let $Y = \mathbf{c}^m(X)$ be the element of the $\mathbf{c}$-orbit of X which belongs to $\mathcal{Q}_{\min}(X)$. Let $(Y,t) = \mathbf{c}_*^m(X,s)$ (see the end of §2). By Corollary 2.20, t is an SC-minimal conjugator for Y, i. e., $Y \xrightarrow{t} Y^t$ is an arrow of the graph $\mathrm{SCG}(X)$.

By Corollary 2.16, any arrow of $\mathrm{SCG}(X)$ is either grey or black or both grey and black. Hence, by Lemma 3.6 applied to Y and t, one of Y^t, $\mathbf{c}(Y^t)$, or $\mathbf{d}(Y^t)$ is in $\mathcal{Q}_{\min}(X)$. In the former two cases we are done. In the latter case it suffices to note that if $\mathbf{d}(Y^t)\in\mathcal{Q}_{\min}(X)$, then $Z = \mathfrak{s}^{-1}(\mathbf{d}(Y^t))\in\mathcal{Q}_{\min}(X)$ by Lemma 3.4 (as in the end of §2, here $\mathfrak{s}^{-1}$ stands for the inverse of $\mathfrak{s}|_{\mathrm{SC}(X)}$) and $Z = \mathfrak{s}^{-1}(\mathbf{d}(\mathbf{c}^m(X^s))) = \mathbf{c}^{m-1}(X^s)$ by Corollary 2.11, thus Z is an element of the cycling orbit of X^s belonging to $\mathcal{Q}_{\min}(X)$.

(b). The same proof but with $\mathbf{c}$ and $\mathbf{d}$ exchanged. $\square$

Theorem 1(b) follows immediately from Lemma 3.3, Corollary 3.5, and Lemma 3.7 combined with the fact that the graph $\mathrm{SCG}(X)$ is connected (see [17; Cor. 10]).

§4. Artin groups: proof of Theorem 2

Let $(G,\mathcal{P},\Delta)$ be the standard Garside structure on an Artin-Tits group of spherical type. This is the case studied in details in [6, 11]. We recall that $G = \langle\mathcal{A}\mid\mathcal{R}\rangle$ where $\mathcal{A}$ can be considered as the set of vertices of a Coxeter graph (one of A_n, B_n, D_n, E_6, E_7, E_8, F_4, G_2, H_3, H_4, $I_2(p)$) and $\mathcal{R} = \{R_{ab}\mid a,b\in\mathcal{A}\}$ where R_{ab} is the relation $\langle a\,b\rangle^{m_{ab}} = \langle b\,a\rangle^{m_{ab}}$. The notation $\langle a\,b\rangle^m$ means

$$\langle a\,b\rangle^m = \underbrace{abab\ldots}_{m\text{ letters}} = \begin{cases}(ab)^{m/2}, & m\text{ is even,}\\ (ab)^{(m-1)/2}a, & m\text{ is odd.}\end{cases} \tag{14}$$

The matrix (m_{ab}) is encoded by the Coxeter graph in the usual way. The set of atoms of the standard Garside structure is $\mathcal{A}$, and $\mathcal{P}$ is the set of products of atoms.

Lemma 4.1. (Follows from [6; Lemma 3.3]). *$a \vee b = \langle a\, b\rangle^{m_{ab}} = \langle b\, a\rangle^{m_{ab}}$ for $a, b \in \mathcal{A}$.* $\square$

Lemma 4.2. [6; Lemma 5.4]. *Let $X \in \mathcal{P}$. Then X is simple if and only if it is square free.* $\square$

In our notation, Lemma 3.4 from [6] can be reformulated as follows.

Lemma 4.3. *Let W be a simple element of G. Then $S(W) = \mathcal{A} \setminus L(W)$ and $F(W) = \mathcal{A} \setminus R(W)$.* $\square$

Remark. The statement of Lemma 4.3 is wrong for the dual Garside structures on the braid groups.

The proof of Theorem 2(a) is very similar to that of Theorem 1(a). It is an immediate consequence of the following fact.

Lemma 4.4. *Under the hypothesis of Theorem 2, suppose that $X = (x_1^k)^P$ with $x_1 \in x^G \cap \mathcal{A}$, $\inf P = 0$. Let $P = B_1 \cdot \ldots \cdot B_n$, $n \geq 1$, be the left normal form of P and let $A_1, \ldots, A_n$ be defined by* (5)*. Then either* (4) *is the left normal form of X and* (6) *holds, or there exist $x_2 \in x^G \cap \mathcal{A}$ and $Q \in \mathcal{P}$ such that $X = (x_2^k)^Q$, $\|Q\| < \|P\|$, and $\ell(Q) \leq \ell(P)$.*

Proof. Suppose that such x_2 and Q do not exist and let us show that $x_1 B_1$ is a simple element, (6) holds, and (4) is left weighted. Indeed:

Suppose that $x_1 B_1$ is not a simple element, i. e., $x_1 \notin L(B_1)$. By Lemma 2.1 and Lemma 4.3, this implies $x_1 \in S(B_1) = R(A_1)$. Hence $B_1 = x_1 B_1'$ and we obtain $X = (x_1^k)^Q$ with $Q = B_1' B_2 \ldots B_n$, $\|Q\| < \|P\|$, and $\ell(Q) \leq \ell(P)$. Contradiction.

Since $x_1 \in L(B_1)$, Lemma 2.1 implies that $x_1 \in F(A)$, thus (6) holds.

Let us show that (4) is left weighted. We should check that if C_1 and C_2 are two successive factors in (4) (not including Δ^{-n}), then $R(C_1) \cap S(C_2) = \varnothing$. We consider all possible cases for (C_1, C_2).

Case 1. $(C_1, C_2) = (B_i, B_{i+1})$, $i \geq 2$. Follows from the fact that $B_1 \cdot \ldots \cdot B_n$ is the left normal form of P.

Case 2. $(C_1, C_2) = (x_1 B_1, B_2)$. Follows from the fact that $B_1 \cdot B_2$ is left weighted.

Case 3. $(C_1, C_2) = (\varphi(A_1 \cdot x_1^{k-1}), x_1 B_1)$. By (6) combined with Lemma 4.2, we have $x_1 \notin R(C_1)$. So, it is enough to show that $S(x_1 B_1) = \{x_1\}$. Suppose that there exists $x_2 \in S(x_1 B_1) \setminus \{x_1\}$. Then we have $x_1 \preccurlyeq x_1 B_1$ and $x_2 \preccurlyeq x_1 B_1$, hence $x_1 \vee x_2 \preccurlyeq x_1 B_1$. Let $x_1 B_1 = (x_1 \vee x_2) B$.

It follows from Lemma 4.1 that $x_1 (x_1 \vee x_2) = (x_1 \vee x_2) x_i$, $i \in \{1, 2\}$. So, by (6), we have $A_1 x_1^k B_1 = A_1' x_1^{k+1} B_1 = A_1' x_1^k (x_1 \vee x_2) B = A_1' (x_1 \vee x_2) x_i^k B = A x_i^k B$ where $A = A_1'(x_1 \vee x_2)$. Since $AB = A_1'(x_1 \vee x_2) B = A_1' x_1 B_1 = A_1 B_1 = \Delta$, we obtain a contradiction with the minimality of $\|P\|$.

Case 4. $(C_1, C_2) = (x_1, x_1)$. (when $k \geq 3$). See Lemma 4.2.

Case 5. $(C_1, C_2) = (A_1, x_1)$ (when $k \geq 2$). Combine (6) and Lemma 4.2.

Case 6. $(C_1, C_2) = (A_{i+1}, A_i)$. See Case 5 of the proof of Theorem 1(a). $\square$

In our proof of Theorem 2(b) we use one more particular property of Artin groups which is not a property of any Garside group.

Lemma 4.5. *Let $a, b \in \mathcal{A}$ and $A \in [1, \Delta]$. If $a \preccurlyeq Ab$ and $a \not\preccurlyeq A$, then $Ab = aA$.*

Proof. Combine Lemmas 4.7(b), 4.8, and 4.9. □

Remark 4.6. (1). Let us denote the Artin group corresponding to a Coxeter graph Γ by $\mathrm{Br}(\Gamma)$. In the case when G is the braid group (i. e., $G = \mathrm{Br}(A_n)$), Lemma 4.5 immediately follows from the interpretation of simple elements as permutation braids given in [12]. Due to the embedding $\mathrm{Br}(B_n) \to \mathrm{Br}(A_{2n})$ (see [8; Prop. 5.1]), the same arguments work also in the case $G = \mathrm{Br}(B_n)$.

(2). Lemma 4.5 can be reformulated as follows: *if $A \in [1, \Delta]$, $y \in \mathcal{A}$, and $\|y \vee A\| \le \|A\| + 1$, then $y \vee A \succcurlyeq A$.* This statement is no longer true if one omits the condition $\|y \vee A\| \le \|A\| + 1$, Indeed, let $G = \mathrm{Br}_4$, $A = \sigma_2\sigma_1\sigma_3$, and $y = \sigma_1$. Then we have $y \vee A = \sigma_2\sigma_1\sigma_3\sigma_2\sigma_3 \not\succcurlyeq A$.

In Lemmas 4.7 – 4.9 below, we use the divisibility theory for Artin groups developed by Brieskorn and Saito in [6; §3]. Let us recall some notions and facts from [6]. Let $\mathcal{A}^*$ be the free monoid freely generated by $\mathcal{A}$ (the set of all words in the alphabet $\mathcal{A}$). Let $a, b \in \mathcal{A}$. We say that a word $C \in \mathcal{A}^*$ is an *elementary or primitive chain from a to b* and we write $a \xrightarrow{C} b$ if there exist $c \in \mathcal{A} \setminus \{a\}$ and j, $0 < j < m_{ac}$, such that $C = \langle c\,a\rangle^j$, and b is the last letter of $\langle c\,a\rangle^{j+1}$, thus $aCb = \langle a\,c\rangle^{j+2}$ (the notation $\langle \dots \rangle^j$ is introduced by (14)). The chain C is called *primitive* when $m_{ac} = 2$ and it is called *elementary* when $m_{ac} > 2$. We say that C is *saturated* if $j = m_{ac} - 1$.

A word $W \in \mathcal{A}^*$ is called a *chain from a to b* if there exists a sequence of elementary or primitive chains

$$a = a_0 \xrightarrow{C_1} a_1 \xrightarrow{C_2} \dots \xrightarrow{C_n} a_n = b. \tag{15}$$

such that $W = C_1 \dots C_n$. It is *saturated* if each of $C_1, \dots, C_n$ is a saturated.

Lemma 4.7. (a). *Let $a \in \mathcal{A}$ and $X \in \mathcal{P}$. Then one and only one of the following possibilities holds:*

(i) *$a \preccurlyeq X$.*
(ii) *X can be represented by a chain from a to c for some atom c.*

(b). *Let $a, b \in \mathcal{A}$ and $X \in \mathcal{P}$. Suppose that $a \preccurlyeq Xb$ and $a \not\preccurlyeq X$. Then X can be represented by a chain from a to b.*

Proof. (a). Follows from [6; Lemma 3.2 and Lemma 3.3].

(b). Since $a \not\preccurlyeq X$, it follows from (a) that X can be represented by a chain $a \to c$ for some atom c. Suppose that $c \ne b$. Then the chain can be extended up to $a \to c \xrightarrow{b} c$ which represents Xb. By (a), this contradicts the condition $a \preccurlyeq Xb$. □

Lemma 4.8. *Let $a, b \in \mathcal{A}$ and $X \in \mathcal{P}$. Suppose that X is represented by a saturated chain from a to b. Then $aX = Xb$.*

Proof. Suppose that X is represented by an elementary or primitive saturated chain. Then $X = \langle ca\rangle^{m-1}$, $m = m_{ac}$, hence $aX = a\langle ca\rangle^{m-1} = \langle ac\rangle^m = \langle ca\rangle^m = \langle ca\rangle^{m-1}b = Xb$. In the general case, if $X = C_1 \dots C_n$ is as in (15), then

$$a_0C_1 \dots C_n = C_1a_1C_2 \dots C_n = C_1C_2a_2C_3 \dots C_n = \dots = C_1 \dots C_na_n. \quad \square$$

Lemma 4.9. *Let A be a simple element of G represented by a chain W from a to b. If $a \preccurlyeq Ab$, then the chain W is saturated.*

Proof. Let W be as in (15). Let i be the minimal index such that the chain

$$a_i \xrightarrow{C_{i+1}} a_{i+1} \xrightarrow{C_{i+2}} \dots \xrightarrow{C_n} a_n = b$$

is saturated. If $i = 0$, then we are done. Suppose that $i \geq 1$. Then, for some $c \in \mathcal{A} \setminus \{a_i\}$ and $j \leq m_{a_i c} - 2$, we have $C_i = \dots c a_i c$ (j letters), hence $C_i a_i = \dots c a_i c a_i$ ($j + 1$ letters), i. e., $C_i a_i$ is an elementary chain from a_{i-1} to c.

Case 1. $c \preccurlyeq C_{i+1} \dots C_n$. Since $C_i = (\dots c a_i c) \succcurlyeq c$, it follows that $A = C_1 \dots C_n$ is not square free. Since A is simple, this fact contradicts Lemma 4.2.

Case 2. $c \not\preccurlyeq C_{i+1} \dots C_n$. Then, by Lemma 4.7(a), we have $C_{i+1} \dots C_n = C'_1 \dots C'_p$ where $c \xrightarrow{C'_1} \dots \xrightarrow{C'_p} d$ is a chain from c to some atom d. By Lemma 4.8, we have $C_{i+1} \dots C_n b = a_i C_{i+1} \dots C_n$, thus $Ab = C_1 \dots C_i a_i C'_1 \dots C'_p$ which means that

$$a = a_0 \xrightarrow{C_1} \dots \xrightarrow{C_{i-1}} a_{i-1} \xrightarrow{C_i a_i} c \xrightarrow{C'_1} \dots \xrightarrow{C'_p} d$$

is a chain from a to d which represents Ab. Hence $a \not\preccurlyeq Ab$ by Lemma 4.7(a). $\square$

The rest of this section is devoted to the proof of Theorem 2(b). So, we fix $x, y \in \mathcal{A}$ and $k, l \geq 1$ and we define $\mathcal{Q}_m$, $\operatorname{len}_{\mathcal{Q}}(X)$, and $\mathcal{Q}_{\min}(X)$ by (11)–(13), see §3. We set also

$$\mathcal{Q}^0_m = \{X \in \mathcal{Q}_m \mid \ell(X) \leq 2m + k + l - 2\}$$

and $\mathcal{Q}^0_{\min}(X) = \mathcal{Q}^0_n \cap X^G$ for $n = \operatorname{len}_{\mathcal{Q}}(X)$. If $\operatorname{len}_{\mathcal{Q}}(X) = 0$, then the conclusion of Theorem 2(b) holds by definition of $\operatorname{len}_{\mathcal{Q}}(X)$, so we shall consider the case when $\operatorname{len}_{\mathcal{Q}}(X) > 0$.

From now on, $x_1, x_2, \dots$ and $y_1, y_2, \dots$ will always denote some atoms which are conjugate to x and y respectively.

Lemma 4.10. (a). *If $X \in \mathcal{Q}_m$ and $m > 0$, then $\ell(X) \leq 2m + k + l - 1$.*

(b). *If $\mathcal{Q}_m \cap X^G \neq \varnothing$ and $m > 0$, then $\mathcal{Q}^0_m \cap X^G \neq \varnothing$. In particular, $\mathcal{Q}^0_{\min}(X) \neq \varnothing$ when $\operatorname{len}_{\mathcal{Q}}(X) > 0$.*

Proof. (a). Let $X = P^{-1} x_1^k P y_1^l$, $\ell(P) = m$. We have $\ell(y_1^l) = l$ and, by Lemma 4.4, we have $\ell(P^{-1} x_1^k P) \leq 2m + k - 1$. Thus the result follows from Lemma 2.2.

(b). Let $X_0 = P^{-1} x_1^k P$ and $X = X_0 y_1^l$ with $\inf P = 0$, $\ell(P) \leq m$. We have to show that $\mathcal{Q}^0_m \cap X^G \neq \varnothing$. By Lemma 4.4, we may assume that the left normal form of X_0 is as stated in Theorem 2(a) with $n \leq m$. If $n < m$, then the result follows from (a). So, we suppose that $n = m$. Without loss of generality we may assume that $P = B_1 \dots B_n$. If $y_1 \notin F(\varphi(X_0))$, then $\varphi(X_0) y_1$ is a simple element by Lemma 4.3, hence $\ell(X) \leq \ell(X_0) + \ell(y_1^l) - 1$ and we are done. So, we suppose that $y_1 \in F(\varphi(X_0))$.

Case 1. $m \geq 2$. We have $\varphi(X_0) = B_n = B'_n y_1$, $B'_n \in \mathcal{P}$. Since B_n is square free, we have $B'_n \not\succcurlyeq y_1$. Let $P' = B_1 \dots B_{n-1} B'_n$, $X'_0 = (P')^{-1} x_1 P'$, $X' = X'_0 y_1^l$. Then we have $\ell(P') \leq m$, hence $X' \in \mathcal{Q}_m$. The condition (5) for $i = n$ can be rewritten as $\Delta = B_n \tau^n(A_n) = B'_n y_1 \tau^n(A_n)$, thus $A'_n = \tau^{-n}(y_1) A_n$ is a simple element such that $A'_n \Delta^{n-1} B'_n = \Delta^n$. Hence $X'_0 = \Delta^{-n} \cdot A'_n \cdot A_{n-1} \cdot \ldots \cdot A_1 \cdot x_1^{k-1} \cdot x_1 B_1 \cdot B_2 \cdot \ldots \cdot B_{n-1} \cdot B'_n$

and we obtain $X' = \Delta^{-n}\cdot A'_n\cdot A_{n-1}\cdot\ldots\cdot A_1\cdot x_1^{k-1}\cdot x_1B_1\cdot B_2\cdot\ldots\cdot B_{n-1}\cdot B'_n y_1\cdot y^{l-1}$. The number of simple factors in this decomposition is $2m+k+l-2$. Thus $X'\in\mathcal{Q}^0_m$. It remains to note that $X' = y_1Xy_1^{-1}\in X^G$.

Case 2. $m=1$. We have $\varphi(X_0) = x_1B_1 \succcurlyeq y_1$. If $B_1\succcurlyeq y_1$, then we repeat the same arguments as in Case 1. If $B_1\not\succcurlyeq y_1$, then the "right-to-left version" of Lemma 4.5 implies $B_1y_1 = y_2B_1$, hence $X = B_1^{-1}x_1^kB_1y_1^l = B_1^{-1}x_1^ky_2^lB_1\in\mathcal{Q}_0^G$ which contradicts the condition $\mathrm{len}_{\mathcal{Q}}(X)=1$. $\square$

Lemma 4.11. *If $X\in\mathcal{Q}^0_{\min}(X)$ and $\mathrm{len}_{\mathcal{Q}}(X)>0$, then the left normal form of X is as stated in Theorem* 2(b) *with $n=\mathrm{len}_{\mathcal{Q}}(X)$.*

Proof. Let $X\in\mathcal{Q}^0_{\min}(X)$. Then $X = P^{-1}x_1^kPy_1^l$ with $\ell(P)=n=\mathrm{len}_{\mathcal{Q}}(X)$. Without loss of generality we may assume that $\inf P = 0$ and $\|P\|$ is the minimal possible among all presentations of X in this form. Let $P = B_1\cdot\ldots\cdot B_n$ be the left normal form of P and let $A_1,\ldots,A_n$ be defined by (5). Then (7) represents X.

Case 1. $n\ge 2$. Let us show that (7) is left weighted and (6), (8) hold. By Lemma 4.4, the part $\Delta^{-n}\cdot A_n\cdot\ldots\cdot B_n$ of (7) is left weighted and (6) holds (here we use the minimality of $\|P\|$). So, it remains to prove that: (i) B_ny_1 is a simple element; (ii) (8) holds; (iii) $B_ny_1\cdot y_1$ is left weighted; (iv) $B_{n-1}\cdot B_ny_1$ is left weighted. Indeed:

(i). Otherwise $A_n\cdot\ldots\cdot B_n\cdot y_1^l$ is left weighted, hence $\ell(X)=2n+k+l-1$ which contradicts the fact that $X\in\mathcal{Q}^0_{\min}(X)$.

(ii). Combine (i), Lemma 2.1, and the fact that $B_n\tau^n(A_n)=\Delta$.

(iii). Follows from Lemma 4.2.

(iv). Suppose that there exists $z\in R(B_{n-1})\cap S(B_ny_1)$. Since $B_{n-1}\cdot B_n$ is left weighted, we have $z\notin S(B_n)$. Hence, by Lemma 4.5, we have $B_ny_1^l = z^lB_n$. Thus $z\sim y_1$ and $B_nXB_n{}^{-1} = Q^{-1}x_1^kQz^l$ where $Q = B_1\ldots B_{n-1}$. Since $\ell(Q)=n-1$, this contradicts the fact that $n=\mathrm{len}_{\mathcal{Q}}(X)$.

Case 2. $n=1$. In this case (7) takes the form $\Delta^{-1}\cdot A_1\cdot x_1^{k-1}\cdot x_1B_1y_1\cdot y_1^{l-1}$. We have to show that this product is left weighted and (9) holds, that is: (i) $x_1B_1y_1$ is a simple element; (ii) (9) holds; (iii) $x_1B_1y_1\cdot y_1$ is left weighted; (iv) $\varphi(A_1x_1^{k-1})\cdot x_1B_1y_1$ is left weighted; (v) $A_1\cdot x_1$ is left weighted. Indeed:

(i). Otherwise $A_1\cdot x_1^{k-1}\cdot x_1B_1\cdot y^l$ is left weighted (because $A_1\cdot x_1^{k-1}\cdot x_1B_1$ is so by Lemma 4.4), hence $\ell(X)=k+l+1$ which contradicts the fact that $X\in\mathcal{Q}^0_{\min}(X)$.

(ii). Let $\tilde y_1 = \delta^{-1}(y_1)$ (as in (9)). By (i) we have $y_1\in R(B_1)=S(\tau(A_1))$ and $x_1\in L(B_1)=F(A_1)$. So, $\tilde y_1\preccurlyeq A_1 = A'_1x_1$ with $A'_1\in\mathcal{P}$. We have to show that $\tilde y_1\preccurlyeq A'_1$. Suppose that $\tilde y_1\not\preccurlyeq A'_1$. Then it follows from Lemma 4.5 that $\tilde y_1A'_1 = A'_1x_1$. Hence $y_1\sim x_1$ and $\tilde y_1A_1 = \tilde y_1A'_1x_1 = A'_1x_1^2 = A_1x_1$. Thus $X = \Delta^{-1}A_1x^kB_1y_1^l = \Delta^{-1}\tilde y_1^kA_1B_1y_l = y_1^{k+l}\in\mathcal{Q}_0$ which contradicts the fact that $X\in\mathcal{Q}^0_{\min}(X)$.

(iii). Follows from Lemma 4.2.

(iv). Suppose that there exists $z\in R(\varphi(A_1x_1^{k-1}))\cap S(x_1B_1y_1)$. Since $\varphi(A_1x_1^{k-1})\cdot x_1B_1$ is left weighted by Lemma 4.4, we have $z\preccurlyeq x_1B_1y_1$ and $z\not\preccurlyeq x_1B_1$. By Lemma 4.5, it follows that $zx_1B_1 = x_1B_1y_1$. Hence, $z\sim y_1$ and $X = B^{-1}x_1^{k-1}(x_1B_1)y_1^l = B_1^{-1}x_1^{k-1}z^l(x_1B_1)\sim x_1^kz^l\in\mathcal{Q}_0$ which contradicts the fact that $X\in\mathcal{Q}^0_{\min}(X)$.

(v). Combine (9) and Lemma 4.2. $\square$

Lemma 4.12. *If $X \in \mathcal{Q}^0_{\min}(X)$ and $\operatorname{len}_{\mathcal{Q}}(X) > 0$, then $\mathfrak{s}(X) \in \mathcal{Q}^0_{\min}(X)$.*

Proof. By Lemma 4.11, we may assume that the left normal form of X is as stated in Theorem 2(b) with $n = \operatorname{len}_{\mathcal{Q}}(X)$.

Case 1. $n \ge 2$ or $l \ge 2$. Let $\tilde{A}_n = \iota(X) = \tau^n(A_n)$ and $Y = \tilde{A}_n^{-1} y_1^l \tilde{A}_n = \Delta^{-1} B_n y_1^l \tilde{A}_n$. By Lemma 4.4, the left normal form of Y is $\Delta^{-1} \cdot B'_n \cdot y_2^{l-1} \cdot y_2 \tilde{A}'_n$ where B'_n and $\tilde{A}'_n$ are simple elements such that $B'_n \tilde{A}'_n = \Delta$ and $B'_n = B''_n y_2$, $B''_n \in \mathcal{P}$. We can rewrite the left normal form of Y also as $\Delta^{-1} \cdot B''_n y_2 \cdot y_2^{l-1} \cdot \tilde{A}''_n$ where $\tilde{A}''_n = y_2 \tilde{A}'_n$. Let $A''_n = \tau^{-n}(\tilde{A}''_n)$. Then, by Corollary 2.9(a) (if $n > 1$) or by Corollary 2.9(b) (if $n = 1$ and $l > 1$), we have

$$\mathfrak{s}(X) = \Delta^{-n} \cdot A''_n \cdot A_{n-1} \cdot \ldots \cdot A_1 \cdot x_1^k \cdot B_1 \cdot B_2 \cdot \ldots \cdot B_{n-1} \cdot B''_n \cdot y_2^l.$$

Hence $\mathfrak{s}(X) \in \mathcal{Q}_n$. Since, $\ell(\mathfrak{s}(X)) \le \ell(X)$ (see [17; Lemma 1]), we conclude that $\mathfrak{s}(X) \in \mathcal{Q}^0_{\min}(X)$.

Case 2. $n = l = 1$. Combining (7) and (9) and denoting A''_1 by A and B_1 by B, we may rewrite the left normal form of X a more symmetric way as $\Delta^{-1} \cdot \tilde{y}_1 A x_1 \cdot x_1^{k-1} \cdot x_1 B y_1$ where $\tilde{y}_1 A x_1 B = A x_1 B y_1 = \Delta$ (and hence $\tau(\tilde{y}_1) = y_1$). Then we have $\mathbf{d}(X) = \tilde{x}_1 \tilde{B} \tilde{y}_1 \cdot \tilde{y}_1 A x_1 \cdot x_1^{k-1}$ where $\tau(\tilde{x}_1) = x_1$ and $\tau(\tilde{B}) = B$.

Let us define $\bar{\mathcal{Q}}_m$, $\bar{\mathcal{Q}}^0_m$, etc. in the same way as $\mathcal{Q}_m$, $\mathcal{Q}^0_m$, etc. but with x^k and y^l exchanged. Then we have $\mathbf{d}(X) \in \bar{\mathcal{Q}}^0_1$. It is clear that $\mathcal{Q}_m \cap X^G \ne \varnothing$ if and only if $\bar{\mathcal{Q}}_m \cap X^G \ne \varnothing$. Since, moreover, $\ell(\mathbf{d}(X)) \le \ell(X)$, we conclude that $\mathbf{d}(X) \in \bar{\mathcal{Q}}^0_{\min}(X) = \bar{\mathcal{Q}}^0_1 \cap X^G$. Then, by Lemma 4.11 applied to $\bar{\mathcal{Q}}^0_{\min}(X)$, the left normal form of $\mathbf{d}(X)$ is $\Delta^{-1} \cdot \tilde{x}_2 \tilde{B}' \tilde{y}_2 \cdot \tilde{y}_2 A' x_2 \cdot x_2^{k-1}$ where $\tilde{x}_2 \tilde{B}' \tilde{y}_2 A' = \tilde{B}' \tilde{y}_2 A' x_2 = \Delta$. Hence $\mathbf{c}(\mathbf{d}(X)) = \Delta^{-1} \cdot \tilde{y}_2 A' x_2 \cdot x_2^{k-1} \cdot x_2 B' y_2 \in \mathcal{Q}^0_{\min}(X)$. where $B' = \tau(\tilde{B}')$ and $y_2 = \tau(\tilde{y}_2)$. It remains to note that $\mathbf{c}(\mathbf{d}(X)) = \mathfrak{s}(X)$ by Lemma 2.10. $\square$

Theorem 1(b) follows immediately from Lemma 4.10(b), Lemma 4.11, and Lemma 4.12 combined with the fact that $\mathfrak{s}^m(X) \in \mathrm{SC}(X)$ for m sufficiently large.

5. An example

It is shown in [22] that if a braid X with three strings is quasipositive, then any positive word W in the standard generators σ_1, σ_2 of Br_3 such that $X = \Delta^p W$ with $p \le 0$, satisfies the following property. There exists a word W' obtained by removing $e(X)$ letters from W such that $\Delta^p W' = 1$. The same result is true for the dual Garside structure on Br_3.

Theorems 1 and 2 of the present paper show that if X is a quasipositive braid with any number of strings but with $e(X) \le 2$, then $\mathrm{SC}(X)$ contains an element which can be presented in the form $\Delta^p W$ where W is a positive word which satisfies the above property.

The following example shows that this is no longer true in the dual Garside structure on Br_4 for braids of algebraic length 3. Namely, let σ_1, σ_2, σ_3 still denote the standard Artin generators of Br_4. Let $\delta = \sigma_3\sigma_2\sigma_1$, $\sigma_0 = \sigma_3^\delta$, $\alpha = \sigma_1^{\sigma_2}$, $\beta = \sigma_2^{\sigma_3}$. Then $\sigma_0, \ldots, \sigma_3, \alpha, \beta$ are the atoms and δ is the Garside element of the Birman-Ko-Lee Garside structure [4] on Br_4. Let

$$X = \delta^{-1} \cdot \beta \cdot \alpha \cdot \sigma_1 \cdot \sigma_2 \cdot \alpha \cdot \beta \tag{16}$$

This braid is quasipositive, indeed, if we remove the second α, then we obtain

$$\delta^{-1} \cdot \beta \cdot \alpha \cdot \sigma_1 \cdot \sigma_2 \beta = \delta^{-1} \cdot \beta \cdot \alpha \cdot \sigma_1 \cdot \sigma_3 \sigma_2 = \delta^{-1} \cdot \beta \cdot \alpha \cdot \sigma_1 \sigma_3 \cdot \sigma_2$$

which is of the form (3) with $n = 1$, $x_1 = \alpha$, $y_1 = \sigma_2$, $A_1 = \beta$, $B_1 = \sigma_1\sigma_3$. The braid X is rigid and (16) is its left (and also right) normal form, so, $\mathbf{c}^6(X) = \tau(X)$. The cycling orbit of X contains 24 elements and it can be easily checked that it coincides with the summit set $\mathrm{SS}(X)$ (and hence with $\mathrm{SSS}(X)$, $\mathrm{USS}(X)$, and $\mathrm{SC}(X)$). Thus, for any presentation of any element of $\mathrm{SS}(X)$ in the form $\delta^{-1}W$ with a positive word W, it is impossible to remove three letters from W to obtain the trivial braid.

6. Quasipositivity problem for 3-braids

The result of [22] cited in §5 leads to an evident algorithm to decide if a given 3-braid X is quasipositive or not: it is enough to try to remove $e(X)$ letters from W in all possible ways. Here we give a minor improvement of this algorithm in the 'branch and bound' style. The new algorithm is still of exponential time with respect to the algebraic length $e(X)$ but the base of the exponent is smaller. The improvements are based on the simple observations summarized in Proposition 6.5 below.

Given $\vec{a} = (a_1, \dots, a_n)$, $a_i > 0$, and $p \in \mathbb{Z}$, we set $\operatorname{len}(\vec{a}) = n$ and

$$X(p, \vec{a}) = X(p; a_1, \dots, a_n) = \Delta^p \underbrace{\sigma_1^{a_1}\sigma_2^{a_2}\sigma_1^{a_3}\sigma_2^{a_4}\dots}_{n \text{ alternating factors}} \in \mathrm{Br}_3 \tag{17}$$

We say that $(p', \vec{a}')$, is obtained from $(p, \vec{a})$ by an *elementary reduction* in the following cases:

(R1) $n \ge 2$, $n \not\equiv p \mod 2$, $p' = p$, $\vec{a}' = (a_1 + a_n, a_2, \dots, a_{n-1})$;
(R2) $n \ge 3$, $a_2 = 1$, $a_1, a_3 \ge 2$, $p' = p + 1$, $\vec{a}' = (a_1 - 1, a_3 - 1, a_4, \dots, a_n)$;
(R3) p is even, $\vec{a} = (1, a_2)$, $a_2 \ge 3$, $p' = p + 1$, $\vec{a}' = (a_2 - 2)$
(R4) p is even, $\vec{a} = (1, 2)$, $p' = p + 1$, $\vec{a}' = (\,)$;
(R5) $n \ge 4$, $a_2 = a_3 = 1$, $p' = p + 1$, $\vec{a}' = (a_1 + a_4 - 1, a_5, \dots, a_n)$;
(R6) p is odd, $\vec{a} = (1, 1, a_3)$, $a_3 \ge 2$, $p' = p + 1$, $\vec{a}'_1 = (a_3 - 1)$;
(R7) p is odd, $\vec{a} = (1, 1, 1)$, $p' = p + 1$, $\vec{a}' = (\,)$;
(R8) $p \equiv n \mod 2$ and $(p', \vec{a}')$ is obtained from $(p, \vec{a})$ by a cyclic permutation of $\vec{a}$ followed by one of (R2)–(R7).

A pair $(p, \vec{a})$, $n = \operatorname{len}(\vec{a})$, is called *reduced* if no elementary reduction can be applied to it. This is equivalent to the fact that either

$$\text{(i) } n \le 1, \quad \text{or (ii) } \vec{a} = (1, 1),\ p \equiv 0(2), \quad \text{or (iii) } n \equiv p(2) \text{ and all } a_i \ge 2. \tag{18}$$

It is clear that if $(p', \vec{a}')$ is an elementary reduction of $(p, \vec{a})$, then $X(p', \vec{a}')$ is conjugate to $X(p, \vec{a})$. It follows easily from the Garside theory that if a pair $(p, \vec{a})$ is reduced, then $\inf_s X(p, \vec{a}) = p$ and $(p, \vec{a})$ is determined by the conjugacy class of $X(p, \vec{a})$ up to cyclic permutation of $\vec{a}$.

Lemma 6.1. *Suppose that $(p', \vec{a}')$ is obtained from $(p, \vec{a})$ by an elementary reduction. Let $n = \operatorname{len}(\vec{a})$, $n' = \operatorname{len}(\vec{a}')$. Then $p' + n' \le p + n$.* □

For a braid X, we denote the signature and the nullity of its closure by $\mathrm{Sign}(X)$ and $\mathrm{Null}(X)$ respectively (we follow the convention that the nullity of a link is the nullity of the symmetrized Seifert form corresponding to a connected Seifert surface). If a braid X is quasipositive, then Murasugi-Tristram inequality implies

$$1 + \mathrm{Null}(X) \ge |\,\mathrm{Sign}(X)| + m - e(X) \tag{19}$$

where m is the number of strings (see details in [21; §3.1]). The following fact can be easily derived from [23; Prop. 8.2] or from [14; Th. 4.2] (also it was conjectured and partially proved in [18; §§9–11]).

Lemma 6.2. *Let $X = X(p,\vec a)$ with $(p,\vec a)$ reduced, $n = \operatorname{len}(\vec a) \ge 2$, and $\vec a \ne (1,1)$. Then* $\operatorname{Sign}(X) + \operatorname{Null}(X) = p + n - e(X)$ *and*

$$\operatorname{Null}(X) = \begin{cases} 1, & \text{if } \vec a = (2,2,\dots,2) \text{ and } p+n \equiv 0 \mod 4,\\ 0, & \text{otherwise.} \end{cases} \quad \square$$

Let us denote a sequence $(2,2,\dots,2)$ (n times) by 2_n.

Lemma 6.3. (a). *If q is even and $n \ge 0$, then $\Delta^q\sigma_1^{-n} \sim X(q-n;2_n)$. If q is odd, then $\Delta^q\sigma_1^{-1} \sim X(q-1;1,1)$, $\Delta^q\sigma_1^{-2} \sim X(q-1;1)$, and $\Delta^q\sigma_1^{-k} \sim X(q-k+1;3,2_{k-3})$ for $k \ge 3$.*

(b). *A braid $X = \Delta^q\sigma_1^{-n}$ is quasipositive if and only if either $(q,n) = (0,0)$, or $q \ge 0$ and $2n < 5q$.*

Proof. (a). Evident.

(b). Let q be even and $n \ge 2$. Then X is quasipositive if and only if $X' = \Delta^{q-1}\sigma_1^{-(n-2)}$ is quasipositive. Indeed, by (a), we have $X \sim X(q-n;2_n)$, hence, by Proposition 6.5(e), X is quasipositive if and only if one of $X_i = X(q-n, f_i(2_n))$ is. For any i we have $X_i \sim X(q-n;2_2,1,2_{n-3}) \overset{(\mathrm{R2})}{\sim} X(q-n+1;2,1,1,2_{n-4}) \overset{(\mathrm{R5})}{\sim} X(q-n+2;3,2_{n-5}) \sim X'$ (we suppose here that $n \ge 5$ and we leave to the reader to check that $X_i \sim X'$ for $n = 2,3,4$). Since q is even, we have $2n < 5q \Leftrightarrow 2n < 5q-1 \Leftrightarrow 2(n-2) < 5(q-1)$, thus it is enough to prove the statement only for odd q. From now on we suppose that q is odd.

Suppose that $0 < 2n < 5q$. Let us prove by induction that X is quasipositive. If $q = 1$, then $n \le 2$ and $X = \Delta\sigma_1^{-2} = \sigma_1\sigma_2\sigma_1^{-1}$ is quasipositive. If $q \ge 3$, then we have $\Delta^q\sigma_1^{-2}\sigma_2^{-1}\sigma_1^{2-n} = \Delta^q\sigma_1^{-1}\Delta^{-1}\sigma_1^{3-n} = \Delta^{q-1}\sigma_2^{-1}\sigma_1^{3-n} = \sigma_1\Delta^{q-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{3-n} = \sigma_1(\Delta^{q-2}\sigma_1^{5-n})\sigma_1^{-1}$, hence

$$\Delta^q\sigma_1^{-n} = (\sigma_2^{-2}\sigma_1\sigma_2^2)\cdot\Delta^q\sigma_1^{-2}\sigma_2^{-1}\sigma_1^{2-n} = (\sigma_2^{-2}\sigma_1\sigma_2^2)\cdot\sigma_1(\Delta^{q-2}\sigma_1^{5-n})\sigma_1^{-1}.$$

So, if $\Delta^{q-2}\sigma_1^{5-n}$ is quasipositive by the induction hypothesis, then X is also.

Suppose that X is quasipositive. Then (19) combined with (a) and with Lemma 6.2 yields $2n \le 5q-1$. $\square$

Remark 6.4. In [25], the question of the quasipositivity of $X = \Delta^q\sigma_1^{-n} \in \mathrm{Br}_k$ is studied for any k. In particular, it is shown that this is so for $n \le qk^2/3 + O(qk)$. However, for $k = 3$, the construction from [25] gives the quasipositivity of X only when $n \le 2q$ which is weaker than Lemma 6.3(b).

Given $\vec a = (a_1,\dots,a_n)$ and $i \in \{1,\dots,n\}$, we set $f_i(\vec a) = (a'_1,\dots,a'_n)$ where $a'_i = 1$ and $a'_j = a_j$ for $j \ne i$.

Proposition 6.5. *Let $(p,\vec a)$, $n = \operatorname{len}(\vec a)$, satisfy* (18). *Let $X = X(p,\vec a)$. Then:*

(a). *If $p \ge 0$, then X is quasipositive.*

(b). *If $p < 0$ and X is quasipositive, then*

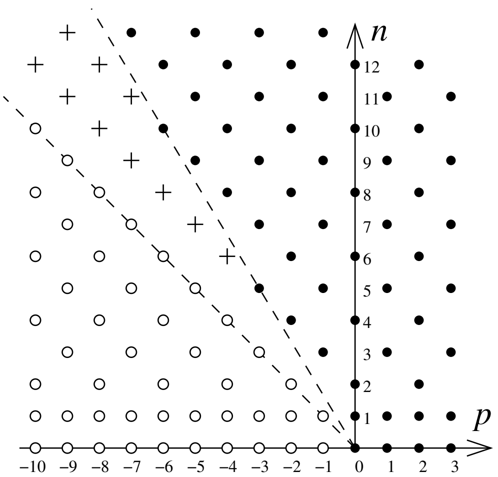
$$0 < p + n < 2e(X). \tag{20}$$

(c). *If $3n + 5p > 0$, then X is quasipositive* (*see Figure 1*).

(d). *If $3n+5p=0$ and $\vec a \ne (2_n)$, then X is quasipositive. Note that* (20) *implies $\vec a \ne (2_n)$ when $3n+5p=0$,*

(e). *X is quasipositive if and only if there exists i such that the braid $X(p, f_i(\vec a))$ is quasipositive.*

(f). *Suppose that $X(p, f_i(\vec a))$ is not quasipositive and $(p', \vec a')$ is obtained from $(p, \vec a)$ by an elementary reduction. If a_i is not involved in the reduction and $a'_{i'}$ is the entry of $\vec a'$ which corresponds to a_i, then $X(p', f_{i'}(\vec a'))$ is not quasipositive.*



$\bullet$ means that $X(p,\vec a)$ with given p and $n = \mathrm{len}(\vec a)$ is quasipositive if $(p,\vec a)$ is reduced; when $3n+5p=0$, we assume also that $\vec a \ne (2_n)$

$\circ$ means that any $X(p,\vec a)$ with given p and $n = \mathrm{len}(\vec a)$ is not quasipositive if $(p,\vec a)$ is reduced

$+$ $X(p,\vec a)$ may or may not be quasipositive

FIGURE 1 . When $X(p,\vec a)$ is *a priori* (non-)quasipositive

Proof. (a) and (f). Evident.

(e) Suppose that X is quasipositive. If $p>0$, then the statement is obvious. Suppose that $p \le 0$. Then, by [22; Prop. 3.1], one can remove some letters from the positive part of the right hand side of (17) so that the resulting braid becomes trivial. This means that there exists $\vec a' = (a'_1, \dots, a'_n)$ such that $a'_i \le a_i$ for each i and $X(p, \vec a') = 1$. It remains to note that if $a'_i \ge 2$ for all i, then $X(p,\vec a') \ne 1$.

(b). Suppose that $p<0$ and X is quasipositive. Then $n \ge 2$ by (e). Thus, when $\vec a \ne (2_n)$, the result follows from (19) combined with Lemma 6.2. If $\vec a = (2_n)$, then the result follows from Lemma 6.3. Note that the left inequality $0 < p+n$ can be proven also by induction using (e) and Lemma 6.1.

(c). It is clear that if $\vec a' = (a'_1, \dots, a'_n)$ is such that $a'_i \le a_i$ for any i, then the quasipositivity of $X(p,\vec a')$ implies that of $X(p,\vec a)$. Thus, the result follows from Lemma 6.3 if we set $\vec a' = (2_n)$.

(d). The same proof but with $\vec a' = (3, 2_{n-1})$. $\square$

Thus we obtain the following recursive algorithm. The input is the pair $(p,\vec a)$ together with the information about the indices i for which it is known already that $X(p, f_i(\vec a))$ is not quasipositive, see Proposition 6.5(f). The pair $(p,\vec a)$ is assumed to be *almost reduced*, i. e., $p \equiv n = \mathrm{len}(\vec a) \mod 2$ when $n \ge 2$, $a_0 \ge 1$, and $a_i \ge 2$ for $i > 0$ (since the algorithm is implemented below in `C` programming language, we assume here that the entries of $\vec a$ are numbered from 0 to $n-1$). First we reduce $(p,\vec a)$ and check if the conclusion can be done using Proposition 6.5(a–d). Then we check recursively if any of $X(p, f_i(\vec a))$ is quasipositive (see Proposition 6.5(e)) taking into account the information that some of them are already known not to be.

Below we present an implementation of this algorithm in the form of a C function **qp3()**. We assume that the input braid is given in the form (17) with $(p,\vec{a})$ almost reduced (the arguments **p** and **a**). The argument **n** should be equal to $\mathrm{len}(\vec{a})$ and the argument **e** should be equal to $e(X(p,\vec{a})) = 3p + \sum a_i$. We assume that the pointer **a** points to a preallocated array of at least `2*e*n` integers. The first n entries of this array contain the vector $\vec{a}$ and the others are used for the intermediate data. The initial values of the array will be lost after the computation.

During the computations, we assume that the vector $\vec{a}$ is represented by the absolute values of the entries of the array **a** whereas the negative sign of **a[i]** is used to encode the information that the braid $X(p, f_i(\vec{a}))$ is not quasipositive, see Proposition 6.5(f). Instead of computing $f_i(\vec{a})$ for $i \ge 1$, we compute f_0 of cyclic permutations of $\vec{a}$ (this ensures that the input is always almost reduced). The function **qp3()** returns 1 if $X(p,\vec{a})$ is quasipositive and 0 otherwise.

```
int qp3( int p, int *a, int n, int e ){
  while( n>1 ){     // reduce (p,a) assuming abs(a[i])>1 for i>0
    if( a[0]==1 && a[n-1]==1 ){
      if( n==2 )break; else p++;
      if( n==3 ){ a[0]=abs(a[1])-1; n=1; break; }
      a[1]=abs(a[1])+abs(a[n-2])-1; a[0]=a[n-=3]; break; }
    if( a[0]==1 )a++; else{ if( a[n-1]!=1 )break; }
    p++;n--;a[0]=abs(a[0])-1;a[n-1]=abs(a[n-1])-1;}   // reduced
  if( p >= 0 )return 1;                         // see Prop. 6.5(a)
  if( !(0 < p+n && p+n < 2*e) )return 0;    // see Prop. 6.5(b)
  if( 3*n + 5*p >= 0 )return 1;             // see Prop. 6.5(c,d)
  { int count=n,e1,*a1,i;
    while( count-- ){ // repeat n times
      if( a[0] > 0 ){ // a[0]<0 means that X(p,f_0(a)) is not qp
        if( (e1=e-a[0]+1) >= 0 ){
          for( a1=a+n,i=1; i<n; i++ )a1[i]=a[i];
          a1[0]=1; if( qp3(p,a1,n,e1) )return 1; } // recursion
        a[0]=-a[0]; }
      a[n] = (*a++); }     // cyclic permutation of the array a
    return 0; }}
```

7. Blocking property of the dual Garside structures on Artin groups

In this section we prove a property (we call it the *blocking property*) of square free symmetric homogeneous Garside structures, in particular, the dual Garside structures on Artin groups and the Garside structure [2] on $G(e,e,r)$. This property is not used in this paper but we hope it to be useful for the quasipositivity problem in the general case.

Proposition 7.1. *Let $(G,\mathcal{P},\delta)$ be a square free symmetric homogeneous Garside structure. Let $k\ge 1$, $A\in\,]1,\Delta[$, $B=\partial A$ (i. e., $AB=\delta$) and let x be an atom such that $X = A\cdot x^k\cdot B$ is in left normal form. Let $Y\in G$, $\inf Y = 0$. Then either $\delta \preccurlyeq XY$, or $\iota(XY) = A$.*

Corollary 7.2. *Let $(G,\mathcal{P},\delta)$ be a square free symmetric homogeneous Garside structure and let X be as in Theorem 1(a), thus the left normal form of X is given by* (1) *and* (2). *Let $Y \in G$, $\inf Y = 0$. Then either $\inf(XY) > \inf X$, or the left normal form of XY begins with $\delta^{-n} \cdot A_n \cdot \ldots \cdot A_1$.*

Lemma 7.3. (Compare with [4; Cor. 3.7]). *Let $(G,\mathcal{P},\delta)$ be a square free and symmetric Garside structure. Let A be a simple element of G and let $S(A) = \{x_1,\ldots,x_m\}$. Then $A = x_1 \vee \cdots \vee x_m$.*

Proof. Let $B = x_1 \vee \cdots \vee x_m$. Then $B \preccurlyeq A$, i. e., $A = BC$ for $C \in [1,\Delta]$. We have to prove that $C = 1$. Suppose that $C \neq 1$. Let $y \in S(C)$. Since $A \succcurlyeq C$ and the Garside structure is symmetric, we have $C \preccurlyeq A$, hence $y \preccurlyeq C \preccurlyeq A$, i. e., $y \in S(A)$. Hence $y \preccurlyeq B$ by the definition of B. Since the Garside structure is symmetric, it follows that $B \succcurlyeq y$. Thus we have $y \in F(B)$ and $y \in S(C)$ which contradicts the fact that $A = BC$ is square free. □

Lemma 7.4. *Let $(G,\mathcal{P},\delta)$ be a symmetric homogeneous Garside structure. Let x and y be atoms such that $xy \not\preccurlyeq \delta$. Let $D = x^{-1}(x \vee y)$, Then $y \vee D = x \vee y$.*

Proof. We have $x \vee y = xD$. Since the Garside structure is symmetric, it follows that $D \preccurlyeq x \vee y$, hence $y \vee D \preccurlyeq x \vee y$. Since the Garside structure is homogeneous, it follows that $\|x \vee y\| = \|xD\| = \|D\| + 1$ and we obtain

$$D \preccurlyeq y \vee D \preccurlyeq x \vee y \quad \text{and} \quad \|x \vee y\| = \|D\| + 1.$$

Thus, it is enough to show that $D \neq y \vee D$. Suppose that $D = y \vee D$. Then we have $y \preccurlyeq D$, hence $xy \preccurlyeq xD = x \vee y \preccurlyeq \delta$. Contradiction. □

Lemma 7.5. *Let $(G,\mathcal{P},\delta)$ be a symmetric square free Garside structure. Let $A \in [1,\Delta]$ and $P \in \mathcal{P}$. Then $\iota(A^2P) = \iota(AP)$. In particular, $S(A^2P) = S(AP)$.*

Proof. Let $B = \iota(AP)$. By Lemma 2.3, we have $\iota(A^2P) = \iota(AB)$. We have $B = AC$ for a simple element C. Since B is simple and the Garside structure is symmetric, we have $B = AC = CA'$ with $A' \in \mathcal{P}$. Hence $AB = ACA' = BA'$. We have $F(A') = S(A')$ (because the Garside structure is symmetric) and $R(A') \subset \mathcal{A} \setminus F(A')$ (because the Garside structure is square free; $\mathcal{A}$ stands for the set of atoms). Hence $R(B) = R(CA') \subset R(A') \subset \mathcal{A} \setminus F(A') = \mathcal{A} \setminus S(A')$ which means that the decomposition $AB = B \cdot A'$ is left weighted. Thus $\iota(A^2P) = \iota(AB) = \iota(B \cdot A') = B = \iota(AP)$ □

Proof of Proposition 7.1. Suppose that $A \neq \iota(Ax^kBY)$. Then $R(A) \cap S(x^kBY) \neq \varnothing$. Let $y \in R(A) \cap S(x^kBY)$. By Lemma 2.1 we have $R(A) = S(B)$, hence

$$y \in S(B). \tag{21}$$

Let $D = x^{-1}(x \vee y)$. Since $y \in S(x^kBY)$, we have $x \vee y \preccurlyeq x^kBY$, i. e., $xD \preccurlyeq x^kBY$. By Lemma 7.5, this implies $xD \preccurlyeq xBY$. By canceling x, we obtain $D \preccurlyeq BY$. Combining this fact with (21), we obtain

$$y \vee D \preccurlyeq BY. \tag{22}$$

Combining (21) with the fact that $A \cdot x^k \cdot B$ is left weighted, we obtain $xy \not\preccurlyeq \delta$. Hence, by Lemma 7.4, we have $y \vee D = x \vee y$. Hence, by (22), we obtain

$$x \preccurlyeq x \vee y = y \vee D \preccurlyeq BY. \tag{23}$$

Let us prove that $B \preccurlyeq x^k BY$. By Lemma 7.3, it is enough to show that $S(B) \subset S(x^k BY)$. Let $z \in S(B)$ and let $E = x^{-1}(x \vee z)$. Combining (23) with $z \preccurlyeq B \preccurlyeq BY$, we obtain $x \vee z \preccurlyeq BY$, i. e., $xE = x \vee z \preccurlyeq BY$. Since the Garside structure is symmetric and $xE \preccurlyeq \delta$, it follows that $E \preccurlyeq xE \preccurlyeq BY$, hence, $xE \preccurlyeq xBY$ and we conclude that $z \preccurlyeq x \vee z = xE \preccurlyeq xBY$. Thus we have proven that $S(B) \subset S(xBY)$. By Lemma 7.5, it follows that $S(xBY) = S(x^k BY)$, hence $S(B) \subset S(x^k BY)$. By Lemma 7.3, this implies $B \preccurlyeq x^k BY$. Multiplying this inequality by A, we obtain $\delta = AB \preccurlyeq Ax^k BY = XY$. □

References

1. D. Bessis, *The dual braid monoid*, Ann. Sci. École Norm. Sup. **36** (2003), no. 5, 647–683.
2. D. Bessis, R. Corran, *Non-crossing partitions of type* (e, e, r), Adv. Math. **202** (2006), 1–49.
3. J. S. Birman, V. Gebhardt, J. González-Meneses, *Conjugacy in Garside groups II: structure of the ultra summit set*, Groups, Geom. and Dynamics **1** (2008), 13–61.
4. J. Birman, K.-H. Ko, S.-J. Lee, *A new approach to the word and conjugacy problems in the braid groups*, Adv. Math. **139** (1998), 322–353.
5. J. Birman, K.-H. Ko, S.-J. Lee, *The infimum, supremum, and geodesic length of a braid conjugacy class*, Adv. Math. **164** (2001), 41–56.
6. E. Brieskorn, K. Saito, *Artin-Gruppen und Coxeter-Gruppen*, Invent. Math. **17** (1972), 245–271.
7. R. Charney, *Artin groups of finite type are biautomatic*, Math. Ann. **292** (1992), 671–683.
8. J. Crisp, *Injective maps between Artin groups*, Geometric Group Theory Down Under, Proceedings of a Special Year in Geometric Group Theory (J. Cossey et al, ed.), W. de Gruyter, 1999, pp. 119–137.
9. P. Dehornoy, *Groupes de Garside*, Ann. Sci. École Norm. Sup. **35** (2002), 267–306.
10. P. Dehornoy, L. Paris, *Gaussian groups and Garside groups, two generalizations of Artin Groups*, Proc. London Math. Soc. (3) **79** (1999), 569–604.
11. P. Deligne, *Les immeubles des groupes de tresses généralisés*, Invent. Math. **17** (1972), 273–302.
12. E. ElRifai, H. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford Ser. (2) **45** (1994), 479–497.
13. D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, W. P. Thurston, *Word Processing in Groups*, Jones & Bartlett, Boston, MA, 1992, pp. Chapter 9..
14. J.-M. Gambaudo, E. Ghys, *Braids and signatures*, Bull. Soc. Math. France **133** (2005), 541–579.
15. F. A. Garside, *The braid group and other groups*, Quart. J. Math. **20** (1969), 235–254.
16. V. Gebhardt, *A new approach to the conjugacy problem in Garside groups*, J. of Algebra **292** (2005), 282–302.
17. V. Gebhardt, J. González-Meneses, *The cyclic sliding operation in Garside groups*, Math. Z. **265** (2010), 85–114.
18. K. Murasugi, *On closed 3-braids*, Memoirs of the AMS, 151, Amer. Math. Soc., Providence, RA, 1974.
19. S. Yu. Orevkov, *Link theory and oval arrangements of real algebraic curves*, Topology **38** (1999), 779–810.
20. S. Yu. Orevkov, *Quasipositivity test via unitary representations of braid groups and its applications to real algebraic curves*, J. Knot Theory and Ramifications **10** (2001), 1005–1023.
21. S. Yu. Orevkov, *Classification of flexible M-curves of degree* 8 *up to isotopy*, GAFA - Geom. and Funct. Anal. **12** (2002), 723–755.
22. S. Yu. Orevkov, *Quasipositivity problem for 3-braids*, Turkish J. Math. **28** (2004), 89–93.
23. S. Yu. Orevkov, *Plane real algebraic curves of odd degree with a deep nest*, J. Knot Theory and Ramifications **14** (2005), 497–522.
24. S. Yu. Orevkov, *Arrangements of an M-quintic with respect to a conic which maximally intersects its odd branch*, Algebra i Analiz **19:4** (2007), 174–242 (Russian); English transl. St. Petersburg Math. J. **19** (2008), 625–674.

25. S. Yu. Orevkov, *Some examples of real algebraic and real pseudoholomorphic curves*, in: Perspectives in Analysis, Geometry and Topology, Progr. in Math. 296, Birkhäuser/Springer, N. Y., 2012, pp. 355-387.
26. M. V. Prasolov, *Small braids with large ultra summit set*, Mat. Zametki **89** (2011), 577–588 (Russian); English transl., Math. Notes **89:4** (2011), 545–554.
27. L. Rudolph, *Algebraic functions and closed braids*, Topology **22** (1983), 191–202.

IMT, Université Toulouse-3, France

Steklov Math. Institute, Moscow, Russia