On the cycling operation in braid groups

Juan González-Meneses* Volker Gebhardt

March 19, 2007

Abstract

The cycling operation is a special kind of conjugation that can be applied to elements in Artin's braid groups, in order to reduce their length. It is a key ingredient of the usual solutions to the conjugacy problem in braid groups. In their seminal paper on braid-cryptography, Ko, Lee et al. proposed the *cycling problem* as a hard problem in braid groups that could be interesting for cryptography. In this paper we give a polynomial solution to that problem, mainly by showing that cycling is surjective, and using a result by Maffre which shows that pre-images under cycling can be computed fast. This result also holds in every Artin-Tits group of spherical type.

On the other hand, the conjugacy search problem in braid groups is usually solved by computing some finite sets called (left) *ultra summit sets* (left-USS), using left normal forms of braids. But one can equally use right normal forms and compute right-USS's. Hard instances of the conjugacy search problem correspond to elements having big (left and right) USS's. One may think that even if some element has a big left-USS, it could possibly have a small right-USS. We show that this is not the case in the important particular case of *rigid* braids. More precisely, we show that the left-USS and the right-USS of a given rigid braid determine isomorphic graphs, with the arrows reversed, the isomorphism being defined using iterated cycling. We conjecture that the same is true for every element, not necessarily rigid, in braid groups and Artin-Tits groups of spherical type.

1 Introduction

Braid groups [3] were related to cryptography in two independent seminal papers [2, 17]. In both papers, the security of the proposed cryptosystems relied on the presumed difficulty of some problems in non-commutative groups, namely the conjugacy search problem (CSP) and the multiple simultaneous conjugacy problem (MSCP). They proposed Artin braid groups as good candidates to implement their cryptosystem, and a lot of literature has been produced on this subject since then. The results in this paper refer to braid groups as the main example, but some of them also hold in other instances of the so-called *Garside* groups [9, 10], which is a family of groups sharing some basic algebraic properties with braid groups, and which contain all Artin-Tits groups of spherical type.

It seems clear that the main objection to the above cryptosystems, either in braid groups or in other groups, is the choice of keys. If one just chooses public and secret keys at random in a braid group, with given parameters such as length or number of strands, none of the above cryptosystems can be considered to be secure. It is then crucial to be able to choose hard instances that resist all known attacks.

*Partially supported by MTM2004-07203-C02-01 and FEDER.

There are other presumably hard problems in braid groups that have been proposed as being possibly interesting for cryptography. In [17], the *cycling problem*, among others, was suggested. It can be explained as follows. In braid groups one has a well known *left normal form*, that is, a unique way to write a braid on n strands $x \in B_n$ as a product $x = \Delta^p x_1 \cdots x_r$, where Δ is the Garside element, and each x_i is a simple braid. This normal form will be explicitly defined later. If we define the **initial factor** of x as $\iota(x) = \Delta^p x_1 \Delta^{-p}$ for $r > 0$, and $\iota(x) = 1$ for $r = 0$, then one has $x = \iota(x)\, \Delta^p x_2 \cdots x_r$. The **left cycling** of x is defined to be the conjugate of x by its initial factor. That is, $\mathbf{c}_L(x) = \Delta^p x_2 \cdots x_r\, \iota(x)$. The same definition makes sense in every Garside group.

The **cycling problem** asks for, given a braid y and a positive integer t such that y is in the image of $\mathbf{c}_L^t$, find a braid x such that $\mathbf{c}_L^t(x) = y$.

In this paper we will show that the cycling problem has a polynomial solution. Namely, it was shown in [20] that the cycling problem for $t = 1$ has a very efficient solution. That is, if y is the cycling of some braid, then one can find x such that $\mathbf{c}_L(x) = y$ very fast. In the first part of this paper we will show the following result, which holds in a special kind of Garside groups (for instance, it holds in every braid group, and in every Artin-Tits group of spherical type).

Theorem 1.1. *If G is a Garside group which is atom-friendly (on the left), then $\mathbf{c}_L : G \to G$ is surjective.*

As an immediate corollary, a solution to the cycling problem is just given by applying t times the algorithm in [20]. This clearly gives a polynomial solution to the cycling problem, since it is so for $t = 1$.

The proof of Theorem 1.1 makes use not only of left normal forms, but of *right normal forms* of elements in B_n (or in G). We shall see that, under certain conditions, an inverse of x under cycling, using left normal forms, is precisely the cycling of x using right normal forms. This shows that *left* and *right cyclings*, $\mathbf{c}_L$ and $\mathbf{c}_R$, are closely related.

The cycling operation is mainly used to find simpler conjugates of a braid, and also to compute finite sets which are invariants of conjugacy classes and allow to solve the conjugacy problem in B_n. One of such sets is the ultra summit set of a given braid x, $USS(x)$. One usually defines this set by using left normal forms, but it is equally possible to define it using right normal forms, hence one usually has two finite sets associated to x, that we denote $USS_L(x)$ and $USS_R(x)$.

The algorithmic solution to the conjugacy search problem in braid groups (and in any Garside group) developed in [15] relies on computing ultra summit sets. Hence braids having small ultra summit sets are not hard instances for the conjugacy search problem. This means that if one wants to find a good key for a cryptographic protocol, one needs to choose a braid with a big ultra summit set. But we have seen that there are two kind of ultra summit sets, $USS_L(x)$ and $USS_R(x)$, and the question arises on whether one of them can be big while the other one is small.

On the other hand, there are three geometric kind of braids: periodic, reducible and pseudo-Anosov [8]. The conjugacy search problem for periodic braids is solvable in polynomial time [7]. Reducible braids are those which can be decomposed, in some sense, into braids with fewer strands. There are algorithms to find this decomposition [4], see also [19], although they are not polynomial. Nevertheless, in most cases the decomposition can be found very fast, and the conjugacy problem is split into several conjugacy problems on fewer strands. Hence, it would be desirable to know pseudo-Anosov braids whose ultra summit sets are big.

But one can solve the conjugacy search problem for pseudo-Anosov braids using *rigid* braids (these will be defined later): In [16] it is shown that the conjugacy search problem for two pseudo-Anosov braids x and y is equivalent to the same problem for x^m and y^m, for every nonzero integer m. And in [5] it is shown that every pseudo-Anosov element in its ultra summit set, has a small power which is rigid (we will be more explicit in the next section). Therefore, one just needs to care about rigid braids. So the above question is transformed into the following: if x is a rigid braid, is it possible that $USS_L(x)$ is big and $USS_R(x)$ is small, or vice versa? The answer is negative, and it is given by the following results.

Theorem 1.2. *A braid $x \in B_n$ with $\ell(x) > 1$ is conjugate to a left rigid braid if and only if it is conjugate to a right rigid braid.*

In the above case, we will show that $\#(USS_L(x)) = \#(USS_R(x))$. Therefore, if one is able to find a rigid element x such that $USS_L(x)$ is big, the same will happen with $USS_R(x)$, so the conjugacy search problem will be equally difficult by using either left or right normal forms.

Moreover, we will show that the relation between $USS_L(x)$ and $USS_R(x)$ is deeper than just having the same number of elements. In order to compute $USS_L(x)$ using the algorithm in [15], one actually computes a directed graph, that we will denote $USG_L(x)$ (left ultra summit graph of x). The vertices of $USG_L(x)$ correspond to the elements of $USS_L(x)$, and the arrows are labeled by simple braids, in such a way that there is an arrow labeled by s, going from u to v, if and only if $s^{-1}us = v$. In the same way, one can define $USG_R(x)$, where in this case the vertices correspond to elements in $USS_R(x)$, and there is an arrow labeled by s, going from u to v, if and only if $sus^{-1} = v$. We will denote by $USG_R(x)^{op}$ the graph which is isomorphic to $USG_R(x)$ as a (non-directed) graph, but with the arrows reversed. The result that compares the graphs $USS_L(x)$ and $USS_R(x)$ is the following:

Theorem 1.3. *Let $x \in B_n$ with $\ell(x) > 1$ be conjugate to a left rigid braid. Then $USG_L(x)$ and $USG_R(x)^{op}$ are isomorphic directed graphs.*

Remark 1.4. *We recently learnt from Jean Michel, François Digne et David Bessis, that $USG_L(x)$ (and thus $USG_R(x)$) are Garside categories. In this context, the notation $USG_R(x)^{op}$ makes sense, since it refers to the opposite category. Then Theorem 1.3 says that $USG_L(x)$ and $USG_R(x)^{op}$ are isomorphic Garside categories. Or in other words, there exists a contravariant isomorphism from $USG_L(x)$ to $USG_R(x)$*

This paper is structured as follows: In Section 2 some basic notions of braids and Garside theory are given. Specialists in Garside theory may skip this Section and go directly to Section 3, in which Theorem 1.1 is shown. The proofs of Theorems 1.2 and 1.3 are given in Section 4.

Acknowledgements: This paper was conceived in the framework of a collaboration of the authors with Joan S. Birman. Most arguments in it have been discussed with her, and in particular she participated in finding the right conjectures that became Theorems 1.2 and 1.3. We are deeply grateful to her for these contributions, and also for her advice and support. The first author thanks Thierry Berger and Samuel Maffre for inviting him to Limoges, to the PhD defense of the latter, where he learnt about the results which are a key tool in Section 3.

2 Basic ingredients of Garside theory.

In this section we will explain the notions and results that will be used throughout the rest of the paper. Namely, we will briefly describe the basic ingredients of the Garside structure of braid groups. In general, a Garside group is a group satisfying the structural properties defined in this section, and the main examples are braid groups and Artin-Tits groups of spherical type. For a short introduction to Garside theory, with a precise definition of a Garside group, see [5].

The braid group on n strands, B_n can be defined by its well known group presentation [3]:

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

If we consider the above as a monoid presentation, this defines the monoid of positive braids, B_n^+. Garside [14] showed that B_n^+ embeds into B_n, so the elements of B_n^+, called *positive braids* can be seen as the braids in B_n that can be written as a word in the generators (but not their inverses). There is a special positive element, called *half twist* or **Garside element**, defined by $\Delta = \sigma_1(\sigma_2\sigma_1)\cdots(\sigma_{n-1}\cdots\sigma_1)$. Artin [3] showed that the center of B_n is the cyclic subgroup generated by Δ^2. In general, every Garside group has a distinguished monoid of positive elements, and a special Garside element, Δ, which has a central power Δ^e. Conjugation by Δ is an inner automorphism which preserves the set of simple elements; we denote this automorphism by τ.

In B_n one can define two partial relations, related to left and right divisibility, respectively. Namely, given $a, b \in B_n$ we say that $a \preccurlyeq b$ if $a^{-1}b \in B_n^+$, that is, if $ap = b$ for some positive braid p. We then say that a is a *left-divisor*, or a *prefix* of b. On the other hand, we say that $a \succcurlyeq b$ if $ab^{-1} \in B_n^+$, that is, if $a = pb$ for some positive braid p. In this case we say that b is a *right-divisor*, or a *suffix* of a. Notice that $B_n^+ = \{p \in B_n;\ 1 \preccurlyeq p\} = \{p \in B_n;\ p \succcurlyeq 1\}$.

Each of the above partial orders define a lattice structure on B_n. This means that given two braids $a, b \in B_n$, there exist a unique greatest common divisor $a \wedge_L b$ and a unique least common multiple $a \vee_L b$, naturally defined by the left divisibility relation $\preccurlyeq$, and also unique gcd's and lcm's, $a \wedge_R b$ and $a \vee_R b$, naturally defined by $\succcurlyeq$.

In B_n, the generators $\sigma_1, \cdots, \sigma_{n-1}$ are called **atoms**. In general, in a Garside group, an atom is a positive element that cannot be decomposed as a product of two positive elements. In the particular case of B_n and of Artin-Tits groups of spherical type, the Garside element Δ is the (left and right) least common multiple of all atoms. This is not true in general for other Garside groups, and this is one of the reasons why the proof of Theorem 1.1 above does not generalize to every Garside group.

Several normal forms for elements in B_n have been defined. We will concentrate in the one defined independently by Adjan [1], Deligne [11], Elrifai-Morton [12] and Thurston [13], which is an improvement of the solution to the word problem given by Garside [14]. We say that a braid is **simple** if it is a positive prefix of Δ. It is well known that this happens if and only if it is a positive *suffix* of Δ. The set of simple braids is then $S = \{s \in B_n;\ 1 \preccurlyeq s \preccurlyeq \Delta\} = \{s \in B_n;\ \Delta \succcurlyeq s \succcurlyeq 1\}$.

Definition 2.1. *Given two simple elements s, s', we say that the decomposition ss' is* **left-weighted** *if s is the maximal simple prefix of ss', that is, if $s = (ss') \wedge_L \Delta$. Similarly, we say that ss' is* **right-weighted** *if s' is the maximal simple suffix of ss', that is, if $s' = (ss') \wedge_R \Delta$.*

For a simple element s we call $\partial(s) = s^{-1}\Delta$ the **right complement** *of s. Note that as $s \preccurlyeq \Delta$ and $s\,\partial(s) = \Delta$, the element $\partial(s)$ is simple. Hence, this defines a map $\partial : S \to S$ on the set S of simple elements. As $\partial(\partial(s)) = \Delta^{-1}s\Delta = \tau(s)$ for any simple s, the map ∂ is a bijection on S and $\partial^2 = \tau$. We similarly define the* **left complement** *of s as $\Delta s^{-1} = \Delta\partial(s)\Delta^{-1} = \tau^{-1}(\partial(s)) = \partial^{-1}(s)$.*

Observe that, given two simple elements s and s', the product ss' is left weighted if and only if there is no prefix $t \preccurlyeq s'$ such that st is simple, or in other words, such that $t \preccurlyeq \partial(s)$. Hence ss' is left weighted if and only if $\partial(s) \wedge_L s' = 1$. Similarly, ss' is right weighted if and only if $s \wedge_R \partial^{-1}(s') = 1$.

Definition 2.2. *Given a braid $x \in B_n$, its* **left normal form** *is a decomposition $x = \Delta^p x_1 \cdots x_r$, satisfying the following conditions:*

1. *$p \in \mathbb{Z}$ is the maximal integer such that $\Delta^{-p}x$ is positive.*
2. *$x_i = (x_i \cdots x_r) \wedge_L \Delta \neq 1$ for $i = 1, \ldots, r$.*

In other words, each x_i is a proper simple element (different from 1 and Δ), and it is the biggest simple prefix of $x_i \cdots x_r$. It is well known that normal forms can be recognized 'locally'. This means that $\Delta^p x_1 \cdots x_r$ is in left normal form if and only if each x_i is a proper simple element and $x_i x_{i+1}$ is left-weighted for $i = 1, \ldots, r-1$. The left normal form of a braid exists and it is unique. The integers p and r are then determined by x, so one can define the **infimum**, **supremum** and **canonical length** of x, respectively, by $\inf(x) = p$, $\sup(x) = p+r$ and $\ell(x) = r$. This terminology is explained by noticing that p and $p+r$ are, respectively, the biggest and the smallest integers such that $\Delta^p \preccurlyeq x \preccurlyeq \Delta^{p+r}$, which is usually written $x \in [\Delta^p, \Delta^{p+r}]$, or simply $x \in [p, p+r]$. The canonical length r is just the size of this interval, which corresponds to the number of non-Delta factors in the left normal form of x.

We notice that one has the analogous definitions related to $\succcurlyeq$:

Definition 2.3. *Given a braid $x \in B_n$, its* **right normal form** *is a decomposition $x = y_1 \cdots y_r \Delta^p$, satisfying the following conditions:*

1. *$p \in \mathbb{Z}$ is the maximal integer such that $x\Delta^{-p}$ is positive.*
2. *$y_i = (y_1 \cdots y_i) \wedge_R \Delta \neq 1$ for $i = 1, \ldots, r$.*

The property of being a right normal form is also a local property ($y_i y_{i+1}$ is right-weighted for every i), and this decomposition also exists and is unique for each braid. We remark that the integers p and r in this case are exactly the same as those corresponding to the left normal form. This means that $\inf(x) = p$ and $\sup(x) = p+r$ are, respectively, the maximal and minimal integers such that $\Delta^{p+r} \succcurlyeq x \succcurlyeq \Delta^p$, hence $\inf(x)$, $\sup(x)$ and $\ell(x)$ can be equally defined using right normal forms instead of left normal forms.

Recall that we defined the initial factor of a braid in the introduction. Since we are using two distinct structures in B_n, we will define left and right versions of initial and final factors, as follows. Given $x = \Delta^p x_1 \cdots x_r$ in left normal form, we define its **left initial factor** as $\iota_L(x) = \tau^{-p}(x_1)$, and its **left final factor** by $\varphi_L(x) = x_r$. In the same way, if $x = y_1 \cdots y_r \Delta^p$ is in right normal form, we define its **right initial factor** by $\iota_R(x) = \tau^p(y_r)$, and its **right final factor** by $\varphi_R(x) = y_1$.

There are special maps from the braid group to itself that consist of conjugating each element by the above initial or final factors. These operations, called cyclings and decyclings, are key ingredients in most of the known solutions to the conjugacy problem in braid groups. The precise definition is as follows.

Definition 2.4. *The following maps, from B_n to itself, are defined for each $x \in B_n$ as follows:*

1. **Left cycling:** $\mathbf{c}_L(x) = \iota_L(x)^{-1} \cdot x \cdot \iota_L(x)$.
2. **Left decycling:** $\mathbf{d}_L(x) = \varphi_L(x) \cdot x \cdot \varphi_L(x)^{-1}$.
3. **right cycling:** $\mathbf{c}_R(x) = \iota_R(x) \cdot x \cdot \iota_R(x)^{-1}$.
4. **right decycling:** $\mathbf{d}_R(x) = \varphi_R(x)^{-1} \cdot x \cdot \varphi_R(x)$.

In other words, if $x = \Delta^p x_1 \cdots x_r$ is in left normal form, then

$$\mathbf{c}_L(x) = \Delta^p x_2 \cdots x_r \tau^{-p}(x_1), \qquad \mathbf{d}_L(x) = x_r \Delta^p x_1 \cdots x_{r-1},$$

and if $x = y_1 \cdots y_r \Delta^p$ is in right normal form, then

$$\mathbf{c}_R(x) = \tau^p(y_r) y_1 \cdots y_{r-1} \Delta^p, \qquad \mathbf{d}_R(x) = y_2 \cdots y_r \Delta^p y_1.$$

We notice that there is an involution of the braid group, $rev:\ B_n \to B_n$, which sends every braid $x = \sigma_{i_1}^{e_1} \cdots \sigma_{i_m}^{e_m}$ to its **reverse** $rev(x) = \overleftarrow{x} = \sigma_{i_m}^{e_m} \cdots \sigma_{i_1}^{e_1}$, that is, the same word read backwards.

Observe that the map *rev* is well-defined, as the relations of B_n are invariant under *rev*. The map *rev* is an anti-isomorphism, and one can easily check that the left normal form of x is mapped by *rev* to the right normal form of $\overleftarrow{x}$, and vice versa. Also $\overleftarrow{\iota_R(x)} = \iota_L(\overleftarrow{x})$, $\overleftarrow{\varphi_R(x)} = \varphi_L(\overleftarrow{x})$, and then $\overleftarrow{\mathbf{c}_R(x)} = \mathbf{c}_L(\overleftarrow{x})$ and $\overleftarrow{\mathbf{d}_R(x)} = \mathbf{d}_L(\overleftarrow{x})$. This means that applying $\mathbf{c}_R$ and $\mathbf{d}_R$ to a braid x corresponds to applying the usual cycling and decycling operations, $\mathbf{c}_L$ and $\mathbf{d}_L$, to its reverse $\overleftarrow{x}$. This implies that all results which are usually shown using left normal forms, $\mathbf{c}_L$ and $\mathbf{d}_L$, will also hold using right normal forms, $\mathbf{c}_R$ and $\mathbf{d}_R$, by symmetry.

Cyclings and decyclings have been used to define suitable finite subsets of B_n which allow to solve the conjugacy decision problem and the conjugacy search problem in braid groups. Namely, the **super summit set** of an element x, denoted $SSS(x)$ [12] is defined as follows. If we denote $C(x)$ the conjugacy class of x, then

$$SSS(x) = \{y \in C(x); \quad \ell(y) \text{ is minimal}\}.$$

Notice that this set does not depend on which structure of B_n (left or right) we used to define $\ell(y)$. A subset of $SSS(x)$ is the *ultra summit set* of x [15]. In this case, since $USS(x)$ is defined by using cyclings, one needs to distinguish between the **left ultra summit set** of x,

$$USS_L(x) = \{y \in SSS(x); \quad \exists t \geq 1,\ \mathbf{c}_L^t(y) = y\},$$

and the **right ultra summit set** of x,

$$USS_R(x) = \{y \in SSS(x); \quad \exists t \geq 1,\ \mathbf{c}_R^t(y) = y\}.$$

Both $SSS(x)$, $USS_L(x)$ and $USS_R(x)$ are, by definition, invariants of the conjugacy class of x. Hence one can determine whether two braids $x, y \in B_n$ are conjugate by computing, say, $USS_L(x)$ and $USS_L(y)$ and checking if they are equal. Actually, it suffices to compute $USS_L(x)$, one element $y' \in USS_L(y)$ and to check whether $y' \in USS_L(x)$. In [12] it is shown how to compute $SSS(x)$, and [15] gives an algorithm to compute $USS_L(x)$ (which can also be used to compute $USS_R(x)$). More precisely, the algorithm computes a directed graph whose set of vertices is $USS_L(x)$. We will define such a graph as follows.

Definition 2.5. *Given $x \in B_n$, we define the* **left ultra summit graph** *of x, denoted $USG_L(x)$, as the directed graph whose set of vertices is $USS_L(x)$ and whose arrows are labeled by simple elements, in such a way that there is an arrow labeled s, starting at u and ending at v, if $s^{-1}us = v$.*

In the same way, we define the **right ultra summit graph** *of x, denoted $USG_R(x)$, as the directed graph whose set of vertices is $USS_R(x)$ and whose arrows are labeled by simple elements, in such a way that there is an arrow labeled s, starting at u and ending at v, if $sus^{-1} = v$.*

We remark that in [15], the graph that is computed is not precisely $USG_L(x)$, but one with less arrows:

Definition 2.6. *Given $x \in B_n$, we define the graph $minUSG_L(x)$ to be the subgraph of $USG_L(x)$ with the same set of vertices, but only with* **minimal** *arrows. An arrow labeled by s and starting at u is said to be minimal if it cannot be decomposed as a product of arrows, that is, if there is no directed path in $USG_L(x)$ starting at u, with labels $s_1, \ldots, s_k$, such that $s = s_1 \cdots s_k$.*

In the same way, we define the graph $minUSG_R(x)$ to be the subgraph of $USG_R(x)$ with the same set of vertices, but only with minimal arrows.

It is known that all the above graphs are connected. The arrows in these graphs allow to know how to connect, by a conjugation, x to any element in $USS_L(x)$ and y to any element in $USS_L(y)$. Hence, the above procedure also solves the conjugacy search problem in B_n (and in any Garside group), that is, it finds a conjugating element from x to y provided it exists.

In [5] one can find is a project to find a polynomial solution to the conjugacy search problem in braid groups. One of the crucial open problems in this project concerns *rigid* braids, which are defined as follows. As above, since we are using two different structures of B_n we will define rigid elements on the left and on the right. In this way, we will say that an element $x = \Delta^p x_1 \cdots x_r$ (written here in left normal form, with $r > 0$) is **left rigid**, if $\Delta^p x_1 \cdots x_r \iota_L(x)$ is in left normal form as written. In the same way, we will say that $x = y_1 \cdots y_r \Delta^p$ (written in right normal form, with $r > 0$) is **right rigid** if $\iota_R(x) y_1 \cdots y_r \Delta^p$ is in right normal form as written, or alternatively, if $\overleftarrow{x}$ is left rigid. These are the elements that have the best possible behavior with respect to cyclings and decyclings, since in this case iterated cyclings or decyclings just correspond to cyclic permutation of the factors (for non-rigid elements this is not the case, since one needs to compute the left normal form of $\mathbf{c}_L(x)$ in order to be able to apply $\mathbf{c}_L$ again, and this modifies some of the original factors of x).

There are some interesting results concerning rigid braids.

Theorem 2.7. [5] *If $x \in B_n$ is left [right] rigid then $x \in USS_L(x)$ [$x \in USS_R(x)$]. Moreover, if $\ell(x) > 1$ then $USS_L(x)$ [$USS_R(x)$] is precisely the set of left [right] rigid conjugates of x.*

Theorem 2.8. [5] *If $x \in B_n$ is a pseudo-Anosov braid, and $x \in USS_L(x)$ [$x \in USS_R(x)$], then x^m is left [right] rigid for some $m < (\frac{n(n-1)}{2})^3$.*

Since pseudo-Anosov braids seem to be generic in B_n, and the conjugacy search problem for pseudo-Anosov braids x and y can be solved just by solving it for x^m and y^m for any $m \neq 0$ [16], the rigid case turns out to be probably the most important case to solve the conjugacy search problem in B_n.

As was noticed in [15], if the canonical length of a random braid x is big enough with respect to the number of strands, then $USS_L(x)$ consists exactly of $2\ell(x)$ elements in 100% of the tested cases, meaning that the probability of getting a larger $USS_L(x)$ seems to tend to zero very rapidly as $\ell(x)$ grows. Moreover, in this 'generic' cases the braids in $USS_L(x)$ are pseudo-Anosov and left rigid. We remark that Gebhardt's algorithm is a deterministic algorithm that is 'generically' polynomial, although there is no written proof, to our knowledge, that either pseudo-Anosov braids or braids conjugate to a rigid element are generic in B_n.

There are instances of left rigid elements whose ultra summit set is much bigger than expected. For instance, as is noticed in [5], the braid in B_{12}

$$\begin{aligned} E &= (\sigma_2\sigma_1\sigma_7\sigma_6\sigma_5\sigma_4\sigma_3\sigma_8\sigma_7\sigma_{11}\sigma_{10}) \cdot (\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_4\sigma_3\sigma_{10}) \cdot \\ &\quad (\sigma_1\sigma_3\sigma_4\sigma_{10}) \cdot (\sigma_1\sigma_{10}) \cdot (\sigma_1\sigma_{10}\sigma_9\sigma_8\sigma_7\sigma_{11}) \cdot (\sigma_1\sigma_2\sigma_7\sigma_{11}) \end{aligned}$$

is a pseudo-Anosov, rigid braid with $\ell(E) = 6$, such that $\#(USS_L(E)) = 264 = 44 \cdot 6$, instead of the expected value of $12 = 2 \cdot 6$. Also, the braid in B_{12}

$$\begin{aligned} F &= (\sigma_3\sigma_2\sigma_1\sigma_4\sigma_6\sigma_8\sigma_7\sigma_6\sigma_9\sigma_{10}\sigma_{11}\sigma_{10}) \cdot (\sigma_1\sigma_2\sigma_4\sigma_3\sigma_2\sigma_1\sigma_5\sigma_7\sigma_{10}\sigma_{11}\sigma_{10}) \cdot \\ &\quad (\sigma_3\sigma_5\sigma_7\sigma_{10}\sigma_{11}\sigma_{10}) \cdot (\sigma_3\sigma_5\sigma_7\sigma_6\sigma_8\sigma_{10}\sigma_{11}) \end{aligned}$$

is pseudo-Anosov and rigid, with $\ell(F) = 4$ and $\#(USS_L(F)) = 232 = 58 \cdot 4$, instead of the expected value of $8 = 2 \cdot 4$. The reason why these special examples of rigid braids exist, and how one can compute them, is still a mystery. Solving this problem would be an important step towards finding secure keys for cryptographic protocols with braid groups.

But recall that we are considering two distinct structures in B_n. Hence it could be possible, a priori, that $USS_R(E)$ or $USS_R(F)$ are much smaller that $USS_L(E)$ or $USS_L(F)$, respectively. Theorem 1.2 tells us that this is not the case, since $\#(USS(x)) = \#(USS(x))$ for every rigid braid x of canonical length greater than 1.

3 Cycling is surjective

In this section we will show Theorem 1.1, that is, we will show that $\mathbf{c}_L$ (and thus $\mathbf{c}_R$) is a surjective map.

First we recall the definition of the right complement $\partial(s)$ of a simple element s from Definition 2.1. A product ss' of two simple elements s and s' is left-weighted if and only if $\partial(s) \wedge_L s' = 1$.

It was shown by Maffre [20] that the pre-image of a braid $x \in B_n$ under $\mathbf{c}_L$ can be computed fast, provided that x is in the image of $\mathbf{c}_L$. The procedure depends on whether the infimum of the existing pre-image of x is equal to $\inf(x)$ or not. We will treat the situation from a slightly different point of view, although the pre-images that we will compute are exactly the same as those given by Maffre.

The following result holds for every Garside group G. In the particular case of B_n, recall that the atoms are just the generators $\sigma_1, \ldots, \sigma_{n-1}$. We will see that in some particular cases, we can obtain a pre-image of x by $\mathbf{c}_L$, just by conjugating x by an atom, and then by Δ^{-1}.

Proposition 3.1. *Let G be a Garside group, and let $x = \Delta^p x_1 \cdots x_r \in G$ be written in left normal form. If there is an atom a such that $\tau^p(a) \not\preccurlyeq x_1 \cdots x_r a$, then $\mathbf{c}_L(\tau^{-1}(a^{-1}xa)) = x$.*

Proof. Define $z = a^{-1}xa = \partial(a)\Delta^{p-1}x_1 \cdots x_r a = \Delta^{p-1}\partial^{2p-1}(a)x_1 \cdots x_r a$. Notice that $\partial(\partial^{2p-1}(a)) = \partial^{2p}(a) = \tau^p(a) \not\preccurlyeq x_1 \cdots x_r a$. But τ transforms atoms into atoms, hence $\tau^p(a)$ is an atom. This means that $\tau^p(a) \not\preccurlyeq x_1 \cdots x_r a$ is equivalent to $\tau^p(a) \wedge_L x_1 \cdots x_r a = 1$, since an atom has no nontrivial prefixes.

Notice that $\Delta \not\preccurlyeq x_1 \cdots x_r a$, otherwise $a \preccurlyeq \Delta \preccurlyeq x_1 \cdots x_r a$. Hence $\inf(x_1 \cdots x_r a) = 0$ which implies that $\iota(x_1 \cdots x_r a)$ is precisely the biggest simple prefix of $x_1 \cdots x_r a$. Therefore, since $\tau^p(a) \wedge_L x_1 \cdots x_r a = 1$, we also have $\tau^p(a) \wedge_L \iota(x_1 \cdots x_r a) = 1$. In other words, if $z_2 \cdots z_k$ is the left normal form of $x_1 \cdots x_r a$, then $\tau^p(a) \wedge_L z_2 = 1$, that is $\partial(\partial^{2p-1}(a)) \wedge_L z_2 = 1$, so $\partial^{2p-1}(a)z_2$ is left-weighted. This implies that $\partial^{2p-1}(a)z_2 \cdots z_k$ is the left normal form of $\partial^{2p-1}(a)x_1 \cdots x_r a$. Hence $\iota(z) = \tau^{-p+1}(\partial^{2p-1}(a)) = \partial^{-2p+2}(\partial^{2p-1}(a)) = \partial(a)$.

If we apply left-cycling to z, we then obtain

$$\mathbf{c}_L(z) = z^{\partial(a)} = \Delta^{p-1}x_1 \cdots x_r a\partial(a) = \Delta^{p-1}x_1 \cdots x_r \Delta = \tau(x)$$

It is well known (and can be derived from the definitions and from the fact that τ is a bijection of S) that τ sends left (and right) normal forms to left (and right) normal forms. Hence τ commutes with $\mathbf{c}_L$ (and with $\mathbf{c}_R$). Therefore $\mathbf{c}_L(\tau^{-1}(z)) = \tau^{-1}(\mathbf{c}_L(z)) = \tau^{-1}(\tau(x)) = x$, as we wanted to show. $\square$

We will now see that, in the cases where the hypothesis of Proposition 3.1 are not satisfied, then a preimage by $\mathbf{c}_L$ of x is just $\mathbf{c}_R(x)$. This time our proof does not work for every Garside group, but we need some special property to be satisfied. Given a Garside group G, we will denote by $\mathcal{A}$ the set of atoms. Given a simple element $s \in G$, we will define the **starting set** of s as $\mathcal{S}(s) = \{a \in \mathcal{A};\ a \preccurlyeq s\}$.

Definition 3.2. *Given a Garside group G, we will say that G is* **atom-friendly** *(on the left) if*

1. $\mathrm{lcm}_L(\mathcal{A}) = \Delta$.
2. $\mathcal{S}(\mathrm{lcm}_L(\mathcal{B})) = \mathcal{B}$ *for every* $\mathcal{B} \subset \mathcal{A}$.

We remark that the terminology *atom-friendly* is new. To our knowledge, no common name has been given to those Garside groups satisfying the above two conditions. It is nevertheless well known [21] that braid groups, and more generally Artin-Tits group of spherical type are atom-friendly (on the left and on the right). Hence the following result holds in all Artin-Tits groups of spherical type.

Proposition 3.3. *Let G be a Garside group which is atom-friendly (on the left). Let $x = \Delta^p x_1 \cdots x_r \in G$ be written in left normal form. If for every atom a one has $\tau^p(a) \preccurlyeq x_1 \cdots x_r a$, then $\mathbf{c}_L(\mathbf{c}_R(x))) = x$.*

Proof. Let us define $\mathcal{D}$ to be the set of atoms a such that $\tau^p(a) \not\preccurlyeq x_1$. That is $\mathcal{D} = \mathcal{A} \backslash \mathcal{S}(\tau^{-p}(x_1)) = \mathcal{A} \backslash \mathcal{S}(\iota(x))$. Define also the simple element $D = \mathrm{lcm}_L(\mathcal{D})$. Let us show that $\Delta \preccurlyeq x_1 \cdots x_r D$. Indeed, for every atom $a \notin \mathcal{D}$ one has $\tau^p(a) \preccurlyeq x_1 \preccurlyeq x_1 \cdots x_r D$, and for every atom $a \in \mathcal{D}$ one has $a \preccurlyeq D$, so using the hypothesis it follows that $\tau^p(a) \preccurlyeq x_1 \cdots x_r a \preccurlyeq x_1 \cdots x_r D$. Therefore $\tau^p(a) \preccurlyeq x_1 \cdots x_r D$ for every atom a. Since τ^p induces a permutation on the set of atoms, this means that $a \preccurlyeq x_1 \cdots x_r D$ for every atom a. But since G is atom-friendly, $\Delta = \mathrm{lcm}(\mathcal{A})$, hence we finally obtain that $\Delta \preccurlyeq x_1 \cdots x_r D$.

Now denote $z_1 \cdots z_r$ the right normal form of $x_1 \cdots x_r$. We just showed that $\Delta \preccurlyeq z_1 \cdots z_r D$, but this is equivalent to say that $z_1 \cdots z_r D \succcurlyeq \Delta$. Since $z_1 \cdots z_r$ is in right normal form, this implies that $z_r D \succcurlyeq \Delta$, which is equivalent to $\Delta \preccurlyeq z_r D$ or, in other words, $\partial(z_r) \preccurlyeq D$.

Now we use again that G is atom-friendly, so $\mathcal{S}(D) = \mathcal{D}$. But since $\mathcal{D} = \mathcal{A} \backslash \mathcal{S}(\iota(x)))$, one has that $\mathcal{S}(D) \cap \mathcal{S}(\iota(x)) = \emptyset$. This means that $D \wedge_L \iota(x) = D \wedge_L \tau^{-p}(x_1) = 1$, which is equivalent to $\tau^p(D) \wedge_L x_1 = 1$.

Finally, consider $y = \mathbf{c}_R(x) = x^{z_r^{-1}} = \Delta^p \tau^p(z_r) z_1 \cdots z_{r-1}$. We will show that $\mathbf{c}_L(y) = x$. Recall that $\partial(z_r) \preccurlyeq D$, hence $\partial(\tau^p(z_r)) \preccurlyeq \tau^p(D)$. On the other hand, $z_1 \cdots z_{r-1} \preccurlyeq z_1 \cdots z_r = x_1 \cdots x_r$. Hence, if we denote by $\alpha = \iota(z_1 \cdots z_{r-1})$, we have $\alpha \preccurlyeq \iota(z_1 \cdots z_r) = \iota(x_1 \cdots x_r) = x_1$. But since $\tau^p(D) \wedge_L x_1 = 1$, and we are considering left divisors $\partial(\tau^p(z_r)) \preccurlyeq \tau^p(D)$ and $\alpha \preccurlyeq x_1$, it follows that $\partial(\tau^p(z_r)) \wedge_L \alpha = 1$. In other words, $\tau^p(z_r)\alpha$ is left weighted as written. This is equivalent to say that $\tau^p(z_r)$ is the first factor in the left normal form of $\tau^p(z_r) z_1 \cdots z_{r-1}$. Therefore $\mathbf{c}_L(y) = y^{z_r} = x$, as we wanted to show. $\square$

We have thus shown Theorem 1.1, since Propositions 3.1 and 3.3 run over all possibilities.

We end this section by recalling a result by Maffre [20] showing when each of the above two cases hold.

Theorem 3.4. [20] *Let G be a Garside groups, and let $x = \Delta^p x_1 \cdots x_r \in G$ be written in left normal form. Then*

1. *$\mathbf{c}_L(y) = x$ for some $y \in G$ with $\inf(y) = p-1$, if and only if $\mathbf{c}_L(\tau^{-1}(x^a)) = x$ for some atom a.*
2. *$\mathbf{c}_L(y) = x$ for some $y \in G$ with $\inf(y) = p$, if and only if $\mathbf{c}_L(\mathbf{c}_R(x)) = x$.*

What we showed in Theorem 1.1 is that at least one of the above cases must happen.

4 Rigid ultra summit sets

4.1 Left rigid and right rigid elements

In this section we will show Theorem 1.2. Let $x \in B_n$, and recall the definition of $USS_L(x)$ and $USS_R(x)$ given in Section 2. Since the statement of Theorem 1.2 refers to the conjugacy class of x, and not to x itself, we can assume that $x \in SSS(x)$, that is, x has minimal canonical length in its conjugacy class. We will see how one can determine if x is conjugate to a rigid braid by looking at its powers. First we will see that if x is conjugate to a rigid element, then the infimum and supremum of its powers behave as one should expect.

Definition 4.1. [18] *Given an element x in a Garside group G, we say that x is* **periodically geodesic** *if $\inf(x^m) = m\inf(x)$ and $\sup(x^m) = m\sup(x)$ for every $m \geq 1$.*

Lemma 4.2. *If $x \in SSS(x)$ in a Garside group G, and x is conjugate to a (left or right) rigid element, then x is periodically geodesic.*

Proof. Let $y = \Delta^p y_1 \cdots y_r$ be a left rigid element conjugate to x. Then every power of y is left rigid and y is periodically geodesic. Notice also that the left normal form of x is $x = \Delta^p x_1 \cdots x_r$, where p and r are the same as above, since $x \in SSS(x)$. Hence $\inf(x^m) \geq pm$ and $\sup(x^m) \leq (p+r)m$. Now y^m is rigid, thus $y^m \in USS(y^m) \subset SSS(y^m)$, hence $\inf(y^m) = pm$ is maximal in its conjugacy class, and $\sup(y^m) = (p+r)m$ is minimal in its conjugacy class. Since x^m is conjugate to y^m, this implies that $\inf(x^m) = pm = m\inf(x)$ and $\sup(x^m) = (p+r)m = m\sup(x)$, so x is periodically geodesic. □

The above result is not the only one relating periodically geodesic and rigid elements.

Lemma 4.3. *Let x be an element in a Garside group G. If x is periodically geodesic and x^m is left (resp. right) rigid for some $m \geq 1$, then x is left (resp. right) rigid.*

Proof. Let $\Delta^p x_1 \cdots x_r$ be the left normal form of x. Since x is periodically geodesic, the left normal form of x^m is $\Delta^{mp} z_1 \cdots z_{rm}$, where

$$z_1 \cdots z_{rm} = \tau^{(m-1)p}(x_1 \cdots x_r)\tau^{(m-2)p}(x_1 \cdots x_r) \cdots \tau^p(x_1 \cdots x_r)(x_1 \cdots x_r).$$

This means that $\tau^{(m-1)p}(x_1) \preccurlyeq z_1 \cdots z_{rm}$, hence $\tau^{(m-1)p}(x_1) \preccurlyeq z_1$, since $z_1 \cdots z_{rm}$ is in left normal form. But then $\iota(x) = \tau^{-p}(x_1) \preccurlyeq \tau^{-mp}(z_1) = \iota(x^m)$.

In the same way, since the last simple factor in the above decomposition of $z_1 \cdots z_{rm}$ is x_r, and the number of factors is precisely rm, it follows that $x_r \succcurlyeq z_{rm}$. In other words, $\varphi(x) \succcurlyeq \varphi(x^m)$.

Finally, recall that x^m is rigid, which means that $\varphi(x^m)\iota(x^m)$ is left weighted as written, that is, $\partial(\varphi(x^m)) \wedge_L \iota(x^m) = 1$. Since $\varphi(x) \succcurlyeq \varphi(x^m)$ is equivalent to $\partial(\varphi(x)) \preccurlyeq \partial(\varphi(x^m))$, we have $\partial(\varphi(x)) \wedge_L \iota(x) \preccurlyeq \partial(\varphi(x^m)) \wedge_L \iota(x^m) = 1$. That is, $\varphi(x)\iota(x)$ is left weighted, whence x is rigid. □

Corollary 4.4. *Let x be an element of a Garside group G. If x has a left rigid power and x is conjugate to a right rigid element, then x if left rigid. Also, if x has a right rigid power and x is conjugate to a left rigid element, then x is right rigid.*

Proof. This is a direct consequence of Lemmas 4.2 and 4.3. □

After this result, in order to show that every left rigid element is conjugate to a right rigid element, and vice versa, we must show that every left rigid element has a conjugate which has a right rigid power. In braid groups, this holds for pseudo-Anosov braids, since one has the following result.

Theorem 4.5. [5, Theorem 3.23] *Let $x \in B_n$ be a pseudo-Anosov braid. If $x \in USS_L(x)$ and $\ell(x) > 1$, then x has a left rigid power. In the same way, if $x \in USS_R(x)$ and $\ell(x) > 1$, then x has a right rigid power.*

Corollary 4.6. *If $x \in B_n$ is a left (resp. right) rigid, pseudo-Anosov braid, and $\ell(x) > 1$, then x is conjugate to a right (resp. left) rigid braid.*

Proof. Suppose that x is left rigid, and consider $y \in USS_R(x)$. By Theorem 4.5, the braid y has a right rigid power, hence y itself must be right rigid by Corollary 4.4. If x is right rigid, the proof follows the same reasoning. □

But there are two more kind of braids, namely periodic and reducible ones. Does the above result hold for these ones? The answer is positive, as we shall see. We recall that a braid $x \in B_n$ is called **periodic** if $x^m = \Delta^t$ for some nonzero integers m and t. The above result holds trivially for periodic braids, due to the following lemma.

Lemma 4.7. *A left or right rigid braid can never be periodic.*

Proof. By definition, if $x \in B_n$ is rigid then $\ell(x) > 0$. Also, by Lemma 4.2, x is periodically geodesic. Hence $\ell(x^m) = |m|\ell(x) > 0$ for every nonzero integer m. Therefore no power of x can be a power of Δ, since $\ell(\Delta^t) = 0$ for every t. □

It just remains to show the case of reducible braids. A braid $x \in B_n$ is said to be **reducible** if, regarding x as a homeomorphism of the n-times punctured disc, it preserves a family of disjoint, closed, essential curves, up to isotopy [8]. This can be expressed in other terms: A braid $x \in B_n$ is said to admit a **coherent tape structure** [4] if it can be obtained from a braid $\widehat{x} \in B_m$, with $m < n$, by replacing, for each $i = 1, \ldots, m$, the i-th strand of $\widehat{x}$ by a braid $x_{[i]} \in B_{k_i}$, with $k_i \geq 1$. One can think that the i-th strand of $\widehat{x}$ becomes a tube, and that $x_{[i]}$ lies inside that tube. One further requirement is that the m-tuple $(k_1, \ldots, k_m)$ is coherent with the permutation induced by $\widehat{x}$, that is, if the i-th strand of $\widehat{x}$ ends at position j, then $k_i = k_j$. The braid $\widehat{x}$ is called the **tubular**, or **external** braid of this decomposition of x, while each $x_{[i]}$ is called the i-th **internal** braid. A braid is then **periodic** if one of its conjugates admits a coherent tape structure.

We can now extend the result of Corollary 4.6 to the whole B_n, so we can show the following result, which is equivalent to Theorem 1.2.

Theorem 4.8. *If $x \in B_n$ is a left (resp. right) rigid braid, and $\ell(x) > 1$, then x is conjugate to a right (resp. left) rigid braid.*

Proof. Suppose that x is left rigid. We will show the result by induction on n. If $n = 1$, x is trivial and there is nothing to show. If $n = 2$, x is either trivial or periodic and by Lemma 4.7, it cannot be rigid. We then suppose that $n > 2$ and that the result holds for braids with less than n strands.

If x is pseudo-Anosov, the result is given by Corollary 4.6. On the other hand, x cannot be periodic by Lemma 4.7. Hence we can assume that x is reducible.

In [4] it was shown that if a braid α admits a coherent tape structure, so do $\mathbf{c}_L(\alpha)$ and $\mathbf{d}_L(\alpha)$. By symmetry, the same property holds for $\mathbf{c}_R(\alpha)$ and $\mathbf{d}_R(\alpha)$. This implies that for every reducible braid, there is some element in its (left or right) ultra summit set that admits a coherent tape structure. Since we are assuming that x is left rigid and $\ell(x) > 1$, $USS_L(x)$ is the set of left rigid conjugates of x, hence there is a conjugate of x which is left rigid, and admits a coherent tape structure. We can then assume that x itself admits a coherent tape structure.

Let $y \in USS_R(x)$, obtained from y by a finite number of applications of $\mathbf{c}_R$ and $\mathbf{d}_R$. After [4], y admits a coherent tape structure. By Corollary 4.4, we just need to show that y has a right rigid power.

We will denote $\widehat{y} \in B_m$ and $y_{[1]}, \ldots, y_{[m]}$, respectively, the external and internal braids associated to y, where $y_{[i]} \in B_{k_i}$ for $i = 1, \ldots, m$, and $k_1 + \cdots + k_m = n$. Notice that if y admits a coherent tape structure, so does every power of y. In order to simplify the notation, we will replace y by a power y^m such that the permutation induced by $\widehat{y^m}$ is trivial ($\widehat{y^m}$ is a pure braid). Notice that x^m is left-rigid, y^m admits a coherent tape structure, and if we show that y^m has a right rigid power, this will also be true for y. Hence can assume that $\widehat{y}$ is a pure braid.

Let $p = \inf(x)$ and $p + r = \sup(x) > 1$. Notice that, since x is left rigid, $\varphi(x)\iota(x)$ is left weighted. One can see the tape structure of x in this pair of simple elements, in the following way. One has $\inf(x) = \min\{\inf(\widehat{x}), \inf(x_{[1]}), \ldots, \inf(x_{[m]})\}$ and $\sup(x) = \max\{\sup(\widehat{x}), \sup(x_{[1]}), \ldots, \sup(x_{[m]})\}$. The part of $\widehat{x}$ (resp. $x_{[i]}$) that one can see in $\varphi(x)$ will be $\varphi(\widehat{x})$ (resp. $\varphi(x_{[i]})$) if $\sup(\widehat{x}) = p + r$ (resp. $\sup(x_{[i]}) = p + r$), and will be trivial otherwise. Analogously, the part of $\widehat{x}$ (resp. $x_{[i]}$) that one can see in $\iota(x)$ will be $\iota(\widehat{x})$ (resp. $\iota(x_{[i]})$) if $\inf(\widehat{x}) = p$ (resp. $\inf(x_{[i]}) = p$), and will be equal to $\Delta \in B_m$ (resp. $\Delta \in B_{k_i}$) otherwise. If we had a trivial component in $\varphi(x)$, then $\varphi(x)\iota(x)$ could not be left weighted, unless the corresponding component of $\iota(x)$ would be trivial. In the same way, If we had a Δ component in $\iota(x)$, then $\varphi(x)\iota(x)$ could not be left weighted, unless the corresponding component of $\iota(x)$ would be also Δ. Therefore, each external or internal component of x must be as follows: either it is trivial, or it is Δ^{p+r} (with the corresponding number of strands), or it is left rigid with infimum p and supremum $p + r$. This has an important consequence: applying (left or right) cyclings and decyclings to x induces (left or right) cyclings and decyclings to $\widehat{x}$, $x_{[1]}, \ldots, x_{[m]}$. Therefore, $y \in USS_R(x)$ implies that $\widehat{y} \in USS_R(\widehat{x})$ and $y_{[i]} \in USS_R(x_{[i]})$ for $i = 1, \ldots, m$.

Finally, each of the components of y (having less than n strands) which is neither trivial nor Δ^{p+r} is conjugate to a left rigid braid with canonical length greater than 1. The induction hypothesis tells us that each of these components is then right rigid, and it has infimum p and supremum $p + r$. Therefore, y itself must be right rigid, as we wanted to show. $\square$

4.2 Left and right ultra summit graphs are isomorphic

We will now show that given a left rigid braid $x \in USS_L(x)$ with $\ell(x) > 1$, then the directed graphs $USG_L(x)$ and $USG_R(x)$ are isomorphic, with the arrows reversed. That is, we will show Theorem 1.3. We need to define an isomorphism of directed graphs (in other words, an invertible functor from the category $USG_L(x)$ to the category $USG_R(x)^{op}$). The isomorphism is very easy to define at the level of vertices (objects), that is, the elements of the ultra summit sets.

Definition 4.9. *Let $x \in B_n$ be a left rigid braid, with $\ell(x) = r > 1$. We define $\Phi(x) = \mathbf{c}_R^{2rt}(x)$, where t is any non-negative integer such that $\mathbf{c}_R^{2rt}(x)$ is right rigid.*

Notice that Φ is well defined: Since x is left rigid, $x \in SSS(x)$, so one can go from x to $USS_R(x)$ by iterated right cycling. Since $\ell(x) > 1$, Theorem 4.8 tells us that x is conjugate to a right rigid element, hence $USS_R(x)$ consists of right rigid elements, and one obtains a right rigid element by applying iterated right cycling to x. Also, for every right rigid element z with $\ell(z) = r$, one has $\mathbf{c}_R^{2r}(z) = z$. Hence, if t is an integer such that $\mathbf{c}_R^{2rt}(x)$ is right rigid, then $\mathbf{c}_R^{2rt}(x) = \mathbf{c}^{2r}(\mathbf{c}_R^{2rt}(x)) = \mathbf{c}_R^{2r(t+1)}(x)$. This implies that if $\mathbf{c}_R^{2rt}(x)$ and $\mathbf{c}_R^{2rt'}(x)$ are both right rigid, they are equal. Hence Φ is well defined.

We will show below that Φ is a bijective map from $USS_L(x)$ to $USS_R(x)$. But we also want to show that $USG_L(x)$ is isomorphic to $USG_R(x)^{op}$. We already know a map Φ that sends vertices (objects) of $USG_L(x)$ to vertices (objects) of $USG_R(x)^{op}$. Let us see how Φ is defined on the arrows (morphisms) of $USG_L(x)$. In order to do this, we recall the definition of the transport map. This map is defined in [15] using left normal forms, but it can be equally defined, by symmetry, using right normal forms.

Definition 4.10. [15] *Given $x \in SSS(x)$ in a Garside group, and given a positive element u such that $u^{-1}xu = y \in SSS(x)$, one defines the* **left transport** *of u as:*

$$u_L^{(1)} = \iota_L(x)^{-1} \cdot u \cdot \iota_L(y).$$

The **iterated left transports** *of u are defined recursively, for every $i \geq 1$, by*

$$u_L^{(i)} = \left(u_L^{(i-1)}\right)_L^{(1)}.$$

Notice that, since $u^{-1}xu = y$, one has $\left(u_L^{(i)}\right)^{-1} \mathbf{c}_L^i(x)\ u_L^{(i)} = \mathbf{c}_L^i(y)$. In other words, since u conjugates (on the right) x to y , the i-th left transport of u conjugates (on the right) the i-th left cycling of x to the i-th left cycling of y.

Definition 4.11. [15] *Given $x \in SSS(x)$ in a Garside group, and given a positive element v such that $vxv^{-1} = z \in SSS(x)$, one defines the* **right transport** *of v as:*

$$v_R^{(1)} = \iota_R(z) \cdot v \cdot \iota_R(x)^{-1}.$$

The **iterated right transports** *of v are defined recursively, for every $i \geq 1$, by*

$$v_R^{(i)} = \left(v_R^{(i-1)}\right)_R^{(1)}.$$

In this case, since $vxv^{-1} = z$, one has $v_R^{(i)}\ \mathbf{c}_R^i(x) \left(v_R^{(i)}\right)^{-1} = \mathbf{c}_R^i(z)$. In other words, since v conjugates (on the left) x to z, the i-th right transport of v conjugates (on the left) the i-th right cycling of x to the i-th right cycling of z.

Theorem 4.12. [15] *With the above conditions, one has the following properties, for every $i \geq 1$:*

1. *If $u_1 \preccurlyeq u_2$ then $(u_1)_L^{(i)} \preccurlyeq (u_2)_L^{(i)}$.*   *If $v_1 \succcurlyeq v_2$ then $(v_1)_R^{(i)} \succcurlyeq (v_2)_R^{(i)}$.*
2. $(u_1 \wedge_L u_2)_L^{(i)} = (u_1)_L^{(i)} \wedge_L (u_2)_L^{(i)}$. $(v_1 \wedge_R v_2)_R^{(i)} = (v_1)_R^{(i)} \wedge_R (v_2)_R^{(i)}$.
3. $\Delta_L^{(i)} = \Delta, \qquad 1_L^{(i)} = 1.$ $\Delta_R^{(i)} = \Delta, \qquad 1_R^{(i)} = 1.$
4. *If u is simple, $u_L^{(i)}$ is simple.*   *If v is simple, $v_R^{(i)}$ is simple.*

Let us then define Φ on the arrows of $USS_L(x)$.

Definition 4.13. *Let $x, y \in USS_L(x) \subset B_n$ be left rigid braids with $\ell(x) > 1$, and let t be a nonnegative integer such that $\Phi(x) = \mathbf{c}_R^{2rt}(x)$ and $\Phi(y) = \mathbf{c}_R^{2rt}(y)$. Given $u \in B_n$ such that $u^{-1}xu = y$, so that $uyu^{-1} = x$, we define $\Phi(u) = u_R^{(2rt)}$.*

Proposition 4.14. *Φ is a well defined map of directed graphs (a well defined functor) from $USG_L(x)$ to $USG_R(x)^{op}$.*

Proof. We already know that $\Phi(y) \in USS_R(x)$ for every $y \in USS_L(x)$, hence Φ sends vertices of $USG_L(x)$ to vertices of $USG_R(x)^{op}$. Now consider an arrow s going from x to y in $USG_L(x)$. Since $s^{-1}xs = y$, one has $sys^{-1} = x$. Hence, if we denote $s_0 = s_R^{(2rt)}$ for an integer t such that $\Phi(x) = \mathbf{c}_R^{2rt}(x)$ and $\Phi(y) = \mathbf{c}_R^{2rt}(y)$, we have $s_0\ \mathbf{c}_R^{2rt}(y)\ s_0^{-1} = \mathbf{c}_R^{2rt}(x)$, that is, $s_0\ \Phi(y)\ s_0^{-1} = \Phi(x)$, where $\Phi(y)$ and $\Phi(x)$ are right rigid.

Notice that, since $\Phi(y)$ is right rigid and has canonical length r, then $\mathbf{c}_R^{2r}(\Phi(y)) = \Phi(y)$, since the product of the $2r$ conjugating elements for right cycling is precisely $\Phi(y)^2\Delta^{-2}$. In the same way, the product of the $2r$ conjugating elements that perform iterated right cycling of $\Phi(x)$ is precisely $\Phi(x)^2\Delta^{-2}$. Hence, the $2r$-th iterated right transport of s_0 is $s_0^{(2r)} = \Phi(x)^2\Delta^{-2}s_0\Delta^2\Phi(y)^{-2} = \Phi(x)^2 s_0 \Phi(y)^{-2} = \Phi(x)s_0\Phi(y)^{-1} = s_0$. This means that $s^{(2rt')} = s^{(2rt)}$ for every $t' \geq t$. Hence $\Phi(s)$ is a well defined simple element which is, by the above argument, an arrow in $USG_R(x)$ going from $\Phi(y)$ to $\Phi(x)$, hence an arrow in $USG_R(x)^{op}$ going from $\Phi(x)$ to $\Phi(y)$. $\square$

It remains to show that Φ is invertible. In order to do this, we start by recalling a result from [5] that relies cyclings and powers. Given x in a Garside group G, denote $C_i = \iota(\mathbf{c}_L^{i-1}(x))$ for every $i \geq 1$. That is, C_i is the conjugating element from $\mathbf{c}_L^{i-1}(x)$ to $\mathbf{c}_L^{i}(x)$, and $x^{C_1\cdots C_i} = \mathbf{c}_L^i(x)$. Then one has:

Lemma 4.15. [5, Lemma 2.4] *Let G be a Garside group and let $x \in SSS(x) \subset G$, with $\inf(x) = p$ and $\ell(x) > 1$. Then, for every $m \geq 1$,*

$$x^m\Delta^{-mp} = C_1 \cdots C_m \mathbf{R}_m,$$

where

1. $\sup(C_1 \cdots C_m) = m$ *and* $\varphi_L(C_1 \cdots C_m) \succcurlyeq \varphi_L(\mathbf{c}_L^m(x))$.
2. $\inf(\mathbf{R}_m) = 0$ *and* $\iota_L(\mathbf{R}_m) \preccurlyeq C_{m+1} = \iota_L(\mathbf{c}_L^m(x))$.

This result can be improved if x is conjugate to a rigid element.

Lemma 4.16. *Let G be a Garside group and let $x \in SSS(x) \subset G$, with $\inf(x) = p$ and $\ell(x) > 1$. Suppose that x is conjugate to a left rigid element, and let m be such that $y = \mathbf{c}_L^m(x)$ is rigid. Then*

$$C_1 \cdots C_m = (x^m\Delta^{-mp}) \wedge_L \Delta^m,$$

where $\inf(C_1 \cdots C_m) = 0$ *and* $\sup(C_1 \cdots C_m) = m$.

Proof. By the above lemma, $C_1 \cdots C_m \preccurlyeq x^m\Delta^{-mp}$. But since m is conjugate to a rigid element, Lemma 4.2 implies that $\inf(x^m) = mp$, so $\inf(x^m\Delta^{-mp}) = 0$. This means that $\inf(C_1 \cdots C_m) = 0$.

Recall also that $x^m\Delta^{-pm} = C_1 \cdots C_m\mathbf{R}_m$, where $\varphi_L(C_1 \cdots C_m) \succcurlyeq \varphi_L(\mathbf{c}^m(x)) = \varphi_L(y)$ and $\iota_L(\mathbf{R}_m) \preccurlyeq \iota_L(\mathbf{c}^m(x)) = \iota_L(y)$. Since y is left rigid, the decomposition $\varphi_L(y)\iota_L(y)$ is left weighted. Hence, if $z_1 \cdots z_m$ is the left normal form of $C_1 \cdots C_m$, this means that $z_1 \cdots z_m\iota_L(\mathbf{R}_m)$ is in left normal form as written. In other words, the first m factors of the left normal form of $x^m\Delta^{-mp}$ are precisely $z_1 \cdots z_m = C_1 \cdots C_m$. That is, $C_1 \cdots C_m = (x^m\Delta^{-mp}) \wedge_L \Delta^m$, as we wanted to show. $\square$

This allows us to determine very precisely the left normal form of x^m, for m big enough, when x is conjugate to a left rigid element. In order to avoid confusing notation produced by the powers of Δ in the normal forms, we will introduce the following notion:

Definition 4.17. *Let G be a Garside group. Given an element $z \in G$, whose left normal form is $\Delta^p z_1 \cdots z_r$ and whose right normal form is $z'_1 \cdots z'_r\Delta^p$, we define the* **left interior** *of z as*

$$z_L^\circ \quad = \quad z\Delta^{-p} \quad = \quad \tau^{-p}(z_1)\cdots\tau^{-p}(z_r) \quad = \quad z'_1 \cdots z'_r,$$

and the **right interior** *of z as*

$$z_R^\circ \quad = \quad \Delta^{-p}z \quad = \quad z_1 \cdots z_r \quad = \quad \tau^p(z'_1)\cdots\tau^p(z'_r).$$

Notice that the above factorizations are, respectively, the left and right normal forms of z_L° and of z_R°. Notice also that if $y = \Delta^p y_1 \cdots y_r$ is left rigid, then

$$(y^m)_L^\circ = y^m \Delta^{-pm} = \left(\tau^{-p}(y_1) \cdots \tau^{-p}(y_r)\right) \left(\tau^{-2p}(y_1) \cdots \tau^{-2p}(y_r)\right) \cdots \left(\tau^{-mp}(y_1) \cdots \tau^{-mp}(y_r)\right),$$

and it is in left normal form as written. Moreover, in this case $(y^m)_L^\circ$ is precisely the conjugating element that takes y to $\mathbf{c}_L^{rm}(y)$.

Lemma 4.18. *Let G be a Garside group and let $x \in SSS(x) \subset G$, with $\inf(x) = p$ and $\ell(x) = r > 1$. Suppose that x is conjugate to a left rigid element. Let N be such that $y = \mathbf{c}_L^N(x)$ is left rigid. Then:*

1. *There exists an integer M such that $\left(y^M\right)_R^\circ \succcurlyeq C_1 \cdots C_N$.*
2. *Let M be an integer satisfying the above condition. If $z_1 \cdots z_N$ is the left normal form of $C_1 \cdots C_N$, and $z_1' \cdots z_s'$ is the left normal form of $\left(y^M\right)_R^\circ (C_1 \cdots C_N)^{-1}$, then for every $m \geq M$, the left normal form of $(x^m)_L^\circ$ is*

$$(x^m)_L^\circ = (z_1 \cdots z_N) \cdot \left(y^{m-M}\right)_L^\circ \cdot \left(\tau^{-pm}(z_1') \cdots \tau^{-pm}(z_s')\right),$$

where the central factor is assumed to be written in left normal form. Moreover, $N+s = Mr$.

Proof. Recall that $x^{C_1 \cdots C_N} = \mathbf{c}_L^N(x) = y$, so $\left(x^N\right)^{C_1 \cdots C_N} = y^N$. Recall also by Lemma 4.16 that $C_1 \cdots C_N \preccurlyeq \left(x^N\right)_L^\circ = x^N \Delta^{-pN}$. This means that $\alpha = (C_1 \cdots C_N)^{-1} \left(x^N\right)_L^\circ$ is a positive braid. Hence $y^N = (C_1 \cdots C_N)^{-1} x^N (C_1 \cdots C_N) = \alpha \Delta^{pN} C_1 \cdots C_N = \Delta^{pN} \tau^{pN}(\alpha) C_1 \cdots C_n$, so $\left(y^N\right)_R^\circ = \Delta^{-pN} y^N = \tau^{pN}(\alpha) C_1 \cdots C_n \succcurlyeq C_1 \cdots C_N$. Hence the first property is satisfied for $M = N$.

Now let M, m, $z_1 \cdots z_N$ and $z_1' \cdots z_s'$ be defined as in Condition 2. Notice that since $m \geq M$, one has $(y^m)_R^\circ = \Delta^{-pm} y^m \succcurlyeq \Delta^{-pM} y^M \succcurlyeq C_1 \cdots C_N$. That is, there exists a positive braid β such that $y^m = \Delta^{mp} \beta C_1 \cdots C_N$. Since y is a left rigid element, by Lemma 4.15, $\varphi_L(C_1 \cdots C_N) \succcurlyeq \varphi_L(\mathbf{c}_L^N(x)) = \varphi_L(y)$. Also, $\iota(\tau^{-mp}(\beta)) \preccurlyeq \iota(y^m) = \iota(y)$. This implies, as $\varphi(y)\iota(y)$ is left weighted, that $z_N \iota(\tau^{-mp}(\beta))$ is also left weighted.

If we now conjugate y^m by $(C_1 \cdots C_N)^{-1}$, we obtain $x^m = C_1 \cdots C_N \Delta^{mp} \beta = C_1 \cdots C_N \tau^{-mp}(\beta) \Delta^{mp}$, hence $(x^m)^\circ = C_1 \cdots C_N \tau^{-mp}(\beta) = z_1 \cdots z_N \tau^{-mp}(\beta)$. Since $z_N \iota(\tau^{-mp}(\beta))$ is left weighted, it follows that the first N factors in the left normal form of $(x^m)_L^\circ$ are precisely $z_1 \cdots z_N$.

Now recall that $z_1' \cdots z_s'$ is the left normal form of $\Delta^{-pM} y^M (C_1 \cdots C_N)^{-1}$. Hence

$$\begin{aligned} y^m = y^{m-M} y^M = y^{m-M} \Delta^{pM} z_1' \cdots z_s' C_1 \cdots C_N &= \left(y^{m-M}\right)_L^\circ \Delta^{p(m-M)} \Delta^{pM} z_1' \cdots z_s' C_1 \cdots C_N \\ = \left(y^{m-M}\right)_L^\circ \Delta^{pm} z_1' \cdots z_s' C_1 \cdots C_N &= \left(y^{m-M}\right)_L^\circ \left(\tau^{-pm}(z_1') \cdots \tau^{-pm}(z_s')\right) \Delta^{pm} C_1 \cdots C_N. \end{aligned}$$

Conjugating by $(C_1 \cdots C_N)^{-1}$, one obtains

$$x^m = (C_1 \cdots C_N) \left(y^{m-M}\right)_L^\circ \left(\tau^{-pm}(z_1') \cdots \tau^{-pm}(z_s')\right) \Delta^{pm},$$

hence

$$(x^m)_L^\circ = (z_1 \cdots z_N) \cdot \left(y^{m-M}\right)_L^\circ \cdot \left(\tau^{-pm}(z_1') \cdots \tau^{-pm}(z_s')\right).$$

This is written in left normal form since $\varphi\left(\left(y^{m-M}\right)_L^\circ\right) \tau^{-pm}(z_1')$ is left weighted, as can be seen by noticing that $\varphi\left(\left(y^{m-M}\right)_L^\circ\right) = \varphi\left(\tau^{-p(m-M)}(y)\right)$, and also that $z_1' = \iota\left(\Delta^{-pM} y^M (C_1 \cdots C_N)^{-1}\right) \preccurlyeq \iota\left(\tau^{pM}(y)\right)$, so $\tau^{-pm}(z_1') \preccurlyeq \iota\left(\tau^{-p(m-M)}(y)\right)$.

Finally, since y is left rigid, x is periodically geodesic. Hence $\ell(x^m) = \ell\left((x^m)_L^\circ\right) = mr$. But we just computed the left normal form of $(x^m)_L^\circ$, which has $N + (m-M)r + s$ factors. Therefore $N + (m-M)r + s = mr$, so $N + s = Mr$, as we wanted to show. $\square$

By symmetry, one has the analogous result for conjugates of right rigid braids, but we will perform a slight modification:

Lemma 4.19. *Let G be a Garside group and let $x \in SSS(x) \subset G$, with $\inf(x) = p$ and $\ell(x) = r > 1$. Suppose that x is conjugate to a right rigid element. Let N be such that $y = \mathbf{c}_R^N(x)$ is right rigid, and let $C'_1, \cdots, C'_N$ the conjugating elements for the N right cyclings, that is, $(C'_N \cdots C'_1)\, x\, (C'_N \cdots C'_1)^{-1} = y$. Then:*

1. *There exists an integer M such that $C'_N \cdots C'_1 \preccurlyeq \left(y^M\right)^\circ_L$.*
2. *Let M be an* **even** *integer satisfying the above condition. If $z'_N \cdots z'_1$ is the right normal form of $C'_N \cdots C'_1$, and $z_s \cdots z_1$ is the right normal form of $(C'_N \cdots C'_1)^{-1} \left(y^M\right)^\circ_L$, then for every $m \geq M$, the right normal form of $(x^m)^\circ_L$ is*

$$(x^m)^\circ_L = (z_s \cdots z_1) \cdot \left(y^{m-M}\right)^\circ_L \cdot \left(\tau^{-pm}(z'_N) \cdots \tau^{-pm}(z'_1)\right),$$

where the central factor is assumed to be written in right normal form. Moreover, $N + s = Mr$.

Proof. If one follows the argument of Lemma 4.18 for right normal forms, one obtains that the right normal form of $(x^m)^\circ_R$ is

$$(x^m)^\circ_R = (\tau^{pm}(z_s) \cdots \tau^{pm}(z_1)) \cdot \left(y^{m-M}\right)^\circ_R \cdot (z'_N \cdots z'_1),$$

and now one just needs to notice that $(x^m)^\circ_L = \tau^{-mp}\left((x^m)^\circ_R\right)$ and that, since M is even, $\tau^{-pm}\left(\left(y^{m-M}\right)^\circ_R\right) = \tau^{-p(m-M)}\left(\left(y^{m-M}\right)^\circ_R\right) = \left(y^{m-M}\right)^\circ_L$. $\square$

We can now show that Φ is a bijective map on the vertices.

Proposition 4.20. *Let $x \in B_n$ be a left rigid braid with $\ell(x) > 1$. The map $\Phi : USS_L(x) \to USS_R(x)$ defined above is bijective.*

Proof. Let us define the map $\Psi : USS_R(x) \to USS_L(x)$, which is defined just as Φ, by symmetry. That is, $\Psi(z) = \overleftarrow{\Phi(\overleftarrow{z})}$. We will show that Ψ is the inverse of Φ.

Let $\Delta^p x_1 \cdots x_r$ be the left normal form of x. Recall that $\Phi(x) = \mathbf{c}_R^{2rt}(x)$ for some t, and then $\Phi(x) = \mathbf{c}_R^{2rt'}(x)$ for every $t' \geq t$. We also have $\Psi(\Phi(x)) = \mathbf{c}_L^{2rs}(\Phi(x))$ for some s, and then $\Psi(\Phi(x)) = \mathbf{c}_L^{2rs'}(\Phi(x))$ for every $s' \geq s$. Hence, if we denote $N = 2r\max(t, s)$, we have $\Phi(x) = \mathbf{c}_R^N(x)$ and $\Psi(\Phi(x)) = \mathbf{c}_L^N(\Phi(x)) = \mathbf{c}_L^N(\mathbf{c}_R^N(x))$. We must then show that $\mathbf{c}_L^N(\mathbf{c}_R^N(x)) = x$.

In order to do it, we will study some decompositions of x^m, for m big enough. For simplicity, we will consider m to be even. First, since x is left rigid, the left normal form of $(x^m)^\circ_L$ for every even m is precisely:

$$\begin{aligned}(x^m)^\circ_L &= \left(\tau^{-p}(x_1) \cdots \tau^{-p}(x_r)\right)\left(\tau^{-2p}(x_1) \cdots \tau^{-2p}(x_r)\right) \cdots \left(\tau^{-mp}(x_1) \cdots \tau^{-mp}(x_r)\right)\\ &= \left(\tau^{-p}(x_1) \cdots \tau^{-p}(x_r)\, x_1 \cdots x_r\right)^{m/2}\\ &= \left(\left(x^2\right)^\circ_L\right)^{m/2}.\end{aligned}$$

Notice that if p is even, the above expression is just $(x_1 \cdots x_r)^m$, but if p is odd this does not happen in general.

Now x is conjugate to a right rigid braid, $y = \Phi(x)$. We can then apply Lemma 4.19 to x. We fix M as in Lemma 4.19, where we can assume that M is even (otherwise, take $M+1$). We take m

big enough, so that $m > 2M$ and m is even. We then obtain that the right normal form of $(x^m)^\circ_L$ is:

$$\begin{aligned}(x^m)^\circ_L &= (z_s \cdots z_1) \cdot \left(y^{m-M}\right)^\circ_L \cdot \left(\tau^{-pm}(z'_N) \cdots \tau^{-pm}(z'_1)\right) \\ &= (z_s \cdots z_1) \cdot \left(y^{m-M}\right)^\circ_L \cdot (z'_N \cdots z'_1)\end{aligned}$$

Notice that, by definition, $(z'_N \cdots z'_1)(z_s \cdots z_1) = (y^M)^\circ_L = y^M \Delta^{-pM}$. Also, by definition $z'_N, \ldots, z'_1$ are the conjugate elements of the iterated right cyclings from x to y, that is, $(z'_N \cdots z'_1)x(z'_N \cdots z'_1)^{-1} = y$. Hence $\left(x^M\right)^\circ_L = x^M \Delta^{-pM} = (z'_N \cdots z'_1)^{-1} y^M \Delta^{-pM} (z'_N \cdots z'_1) = (z_s \cdots z_1)(z'_N \cdots z'_1)$. Notice that we used that M is even, so Δ^{pM} is central.

We then obtain the following decomposition:

$$(x^m)^\circ_L = (z_s \cdots z_1)\,(z'_N \cdots z'_1) \cdot \left(x^{m-2M}\right)^\circ_L \cdot (z_s \cdots z_1)\,(z'_N \cdots z'_1)\,.$$

Hence

$$\left(y^{m-M}\right)^\circ_L = (z'_N \cdots z'_1) \cdot \left(x^{m-2M}\right)^\circ_L \cdot (z_s \cdots z_1)\,.$$

Let us write the above factors in left normal form. Let $w_1 \cdots w_N$ the left normal form of $z'_N \cdots z'_1$, and let $w'_1 \cdots w'_s$ be the left normal form of $z_s \cdots z_1$. Then

$$\left(y^{m-M}\right)^\circ_L = (w_1 \cdots w_N) \cdot \left(x^{m-2M}\right)^\circ_L \cdot (w'_1 \cdots w'_s)\,.$$

We will now show that this decomposition is precisely the left normal form of $\left(y^{m-M}\right)^\circ_L$. Indeed, since $\left(x^M\right)^\circ_L = (z_s \cdots z_1)(z'_N \cdots z'_1) = (w'_1 \cdots w'_s)\,(w_1 \cdots w_N)$ and $s + N = Mr$ by Lemma 4.19, it follows that the final factor of the left normal form of $\left(x^M\right)^\circ_L$ is a suffix of w_N. That is, $w_N \succcurlyeq x_r$. Since x is left rigid, this implies that $w_N \cdot \tau^{-p}(x_1)$ is left weighted, where the second factor in this expression is the initial factor in the left normal form of $\left(x^{m-2M}\right)^\circ_L$. But also w'_1 must be a prefix of the initial factor of $\left(x^M\right)^\circ_L$, that is, $w'_1 \preccurlyeq \tau^{-p}(x_1)$. This implies that $x_r \cdot w'_1$ is left weighted, where x_r is the final factor in the left normal form of $\left(x^{m-2M}\right)^\circ_L$. Hence, the above expression is the left normal form of $\left(y^{m-M}\right)^\circ_L$, for m big enough.

But recall from Lemma 4.16 that the product of the first $m - M$ factors in the left normal form of $\left(y^{m-M}\right)^\circ_L$ is precisely the product of the $m - M$ conjugating elements for iterated left cycling of y. If we take m big enough so that $m - M \geq N$ and $m - M$ (as well as N) is a multiple of $2r$, the first $m - M$ factors in the left normal form of $\left(y^{m-M}\right)^\circ_L$ are precisely $w_1 \cdots w_N \left(x^{2k}\right)^\circ_L$, where $\left(x^{2k}\right)^\circ_L$ commutes with x. Since $(w_1 \cdots w_N)^{-1} y (w_1 \cdots w_N) = x$, it then follows that $\mathbf{c}_{m-M}(y) = x$. Since x is left rigid, and $m - M$ is a multiple of $2r$, we finally obtain $\Psi(y) = x$, that is, $\Psi(\Phi(x)) = x$, as we wanted to show. $\square$

In order to finish the proof of Theorem 1.3, it just remains to show that the map Ψ can be extended to the arrows of $USG_R(x)$, so that $\Psi \circ \Phi = \mathrm{id}_{USG_L(x)}$. We will use the following result:

Lemma 4.21. *Let $x \in B_n$ be a left rigid braid with $\ell(x) = r > 1$. Let $T = 2rt$ be such that $\Phi(x) = \mathbf{c}_R^T(x)$ and $\Psi(\Phi(x)) = \mathbf{c}_L^T(\Phi(x))$. Let $C'_T, \ldots, C'_1$ be the conjugating elements for the iterated right cyclings of x, and let $C_1, \ldots, C_T$ be the conjugating elements for the iterated left cyclings of $\Phi(x)$. That is,*

$$\Phi(x) = (C'_1 \cdots C'_T)\, x\, (C'_1 \cdots C'_T)^{-1}$$

and

$$\Psi(\Phi(x)) = (C_1 \cdots C_T)^{-1}\, \Phi(x)\, (C_1 \cdots C_T).$$

Then $C_1 \cdots C_T = C'_1 \cdots C'_T$.

Proof. Using the notation in the proof of Proposition 4.20, we notice that the right normal form of $C'_1 \cdots C'_T$ is $(y^{2k})^{\circ}_L(z'_N \cdots z'_1)$ for some k, and the left normal form of $C_1 \cdots C_T$ is $(w_1 \cdots w_N)(x^{2k})^{\circ}_L$, where k is the same as above since the supremum of both elements is precisely T. But notice that $(y^{2k})^{\circ}_L(z'_N \cdots z'_1) = (z'_N \cdots z'_1)(x^{2k})^{\circ}_L = (w_1 \cdots w_N)(x^{2k})^{\circ}_L$, hence the result follows. □

Proof of Theorem 1.3. We define $\Psi : USG_R(x)^{op} \to USG_L(x)$ in the natural way. For every element $u \in USS_R(x)$, we define $\Psi(u)$ as above, in the same way as Φ but using right normal forms, that is, $\Psi(u) = \overleftarrow{\Phi(\overleftarrow{u})}$. In the case of the arrows of $USG_R(x)^{op}$, we proceed exactly the same way. If s is a simple element such that $sus^{-1} = v$ with $u, v \in USS_R(x)$, that is, if s is an arrow in $USG_R(x)^{op}$ going from v to u, we define $\Psi(s) = \overleftarrow{\Phi(\overleftarrow{s})}$, where $\overleftarrow{s}$ corresponds to an arrow in $USS_L(\overleftarrow{x})$ going from $\overleftarrow{u}$ to $\overleftarrow{v}$.

Let us show that, if s is an arrow in $USG_L(x)$ going from x to y, then $\Psi(\Phi(s)) = s$. First, by construction $\Psi(\Phi(s))$ is a simple element conjugating $\Psi(\Phi(x)) = x$ to $\Psi(\Phi(y)) = y$, hence $\Psi(\Phi(s))$ is an arrow in $USG_L(x)$ going from x to y. We just need to show that s and $\Psi(\Phi(s))$ are the same as simple elements.

Let $N = 2rt$ be big enough, so that $\Phi(x) = \mathbf{c}_R^N(x)$, $\Phi(y) = \mathbf{c}_R^N(y)$, $\Psi(\Phi(x)) = \mathbf{c}_L^N(\Phi(x))$ and $\Psi(\Phi(y)) = \mathbf{c}_L^N(\Phi(y))$. By Lemma 4.21, the product of conjugating elements (on the left) to go from x to $\Phi(x)$ is the same as the product of conjugating elements (on the right) to go from $\Phi(x)$ to $\Psi(\Phi(x)) = x$. Denote this product by α. The same happens with y and $\Phi(y)$, and we denote the corresponding product by β. Hence, $\Psi(\Phi(s)) = \Psi(s_R^{(N)}) = \Psi(\alpha s \beta^{-1}) = \alpha^{-1}(\alpha s \beta^{-1})\beta = s$, so the result follows. □

We remark that, since the left transport preserves left gcd's, Φ sends minimal arrows of $USG_L(x)$ to minimal arrows of $USG_R(x)$. By symmetry, Ψ sends minimal arrows in $USG_R(x)$ to minimal arrows of $USG_L(x)$. Therefore, we have:

Corollary 4.22. *Let $x \in B_n$ be a left rigid braid with $\ell(x) > 1$. The restriction of Φ to $minUSG_L(x)$ is an isomorphism of directed graphs: $\Phi : minUSG_L(x) \to minUSG_R(x)^{op}$.*

4.2.1 Φ respects the structure of ultra summit graphs

It was shown in [6] that the arrows of $minUSG_L(x)$, and similarly those of $minUSG_R(x)^{op}$, can be partitioned naturally into two categories, namely *partial cycling* and *partial twisted decycling* components. In this subsection we show that the isomorphism Φ is natural in the sense that it preserves this decomposition of ultra summit graphs.

Proposition 4.23. [6] *Let $x \in B_n$ with $\ell(x) > 0$ and let s be an arrow in $minUSG_L(x)$ going from x to x^s. Then at least one of the following conditions holds:*

1. $s \preccurlyeq \iota_L(x)$
2. $s \preccurlyeq \iota_L(x^{-1})$

Notice that $\iota_L(x^{-1}) = \partial(\varphi_L(x))$.

Definition 4.24. [6] *Let $x \in B_n$ with $\ell(x) > 0$ and let s be an arrow in $USG_L(x)$ going from x to x^s. We call s a* **partial left cycling** *of x and say that the arrow s is* **black** *if $s \preccurlyeq \iota_L(x)$. We call s a* **partial twisted left decycling** *of x and say that the arrow s is* **grey** *if $s \preccurlyeq \iota_L(x^{-1}) = \partial(\varphi_L(x))$.*

By symmetry we have

Proposition 4.25. [6] *Let $x \in B_n$ with $\ell(x) > 0$ and let s be an arrow in $minUSG_R(x)$ going from x to x^s. Then at least one of the following conditions holds:*

1. $\iota_R(x) \succcurlyeq s$
2. $\iota_R(x^{-1}) \succcurlyeq s$

Notice that $\iota_R(x^{-1}) = \partial^{-1}(\varphi_R(x))$.

Definition 4.26. [6] *Let $x \in B_n$ with $\ell(x) > 0$ and let s be an arrow in $USG_R(x)$ going from x to x^s. We call s a* **partial right cycling** *of x and say that the arrow s is* **black** *if $\iota_R(x) \succcurlyeq s$. We call s a* **partial twisted right decycling** *of x and say that the arrow s is* **grey** *if $\partial^{-1}(\varphi_R(x)) = \iota_R(x^{-1}) \succcurlyeq s$.*

Note that the intuitive meaning of "cycling" (respectively "decycling") is to move the first simple factor to the end (respectively, the last simple factor to the front) with respect to the normal form under consideration. Note also that $\tau \circ \mathbf{d}_L(x) = \tau(x^{\varphi_L(x)^{-1}}) = \tau(x^{\iota_L(x^{-1})\Delta^{-1}}) = x^{\iota_L(x^{-1})}$ and that $\tau^{-1} \circ \mathbf{d}_R(x) = \tau^{-1}(x^{\varphi_R(x)}) = \tau^{-1}(x^{\iota_R(x^{-1})^{-1}\Delta}) = x^{\iota_R(x^{-1})^{-1}}$ Hence, the definitions of "partial cycling" and "partial twisted decycling" are natural: a partial cycling or decycling corresponds to moving a prefix or suffix of the first or last simple factor; "twisting" refers to composition with τ.

Partial cyclings and partial twisted decyclings are preserved by the graph isomorphism Φ according to the following results.

Proposition 4.27. *Let $x \in B_n$ be a rigid braid with $\ell(x) > 1$, and let s be an arrow from x to y in $USG_L(x)$ such that $s \preccurlyeq \iota_L(x)$. Then, $\Phi(s)$ is an arrow from $\Phi(y)$ to $\Phi(x)$ in $USG_R(x)$ such that $\iota_R(\Phi(y)) \succcurlyeq \Phi(s)$.*

Proof. Recall that $\Phi(s)$ is defined via iterated transport. As transport is monotonic, we obtain $\Phi(s) \preccurlyeq \iota_L(\Phi(x))$. Moreover, $\Phi(s)$ is simple. If $\Phi(x) = \Delta^p x_1 \cdots x_r$ is in left normal form, we have $\tau^p(\Phi(s)) \preccurlyeq x_1$, whence $\Phi(y) = \Phi(s)^{-1}\Phi(x)\Phi(s) = \Delta^p(\tau^p(\Phi(s))^{-1}x_1)x_2 \cdots x_r\Phi(s)$. The latter implies $\iota_R(\Phi(y)) \succcurlyeq \Phi(s)$ as claimed, since $\inf(\Phi(y)) = \inf(\Phi(x)) = p$. □

Corollary 4.28. *Φ and Ψ are isomorphisms of directed graphs preserving the colours of arrows.*

Proof. We know that Φ and Ψ are isomorphisms of directed graphs by Theorem 1.3; it remains to be shown that they preserve the colours of arrows.

By Proposition 4.27, the image of a black arrow under Φ is a black arrow. Applying Proposition 4.27 to x^{-1}, which is also a rigid element with $\ell(x^{-1}) > 1$, it follows that the image of a grey arrow under Φ is a grey arrow. The analogous result holds for Ψ by symmetry. □

References

[1] S. I. Adyan, *Fragments of the word Δ in the braid group*, (Russian) Mat. Zametki **36**, no. 1 (1984), 25-34.

[2] I. Anshel, M. Anshel and D. Goldfeld, *An algebraic method for public key crypography*, Math Research Letters **6**, No. 3-4 (1999), 287-291.

[3] E. Artin, Theory of braids, *Annals of Math.* **48** (1946), 101-126.

[4] D. Benardete, M. Guitierrez and Z. Nitecki, *Braids and the Nielsen-Thurston classification*, J. Knot Theory and its Ramifications **4** (1995), 549-618.

[5] J. Birman, V. Gebhardt and J. González-Meneses, *Conjugacy in Garside groups I: Cycling, Powers and Rigidity*, preprint arXiv math.GT/0605230.

[6] J. Birman, V. Gebhardt and J. González-Meneses, *Conjugacy in Garside groups II: Structure of the Ultra Summit Set*, preprint arXiv math.GT/0606652. To appear in Groups, Geometry, and Dynamics.

[7] J. Birman, V. Gebhardt and J. González-Meneses, *Conjugacy in Garside groups III: Periodic braids*, preprint arXiv math.GT/0609616. To appear in Journal of Algebra.

[8] J. Birman, A. Lubotzky and J. McCarthy, *Abelian and solvable subgroups of the mapping class groups*, Duke Math **50** (1983), 1107-1120.

[9] P. Dehornoy and L. Paris, *Gaussian groups and Garside groups, two generalizations of Artin groups*, Proc. London Math. Soc. **79** (1999), No. 3, 569-604.

[10] P. Dehornoy, *Groupes de Garside*, Ann. Scient. Ec. Norm. Sup. **35** (2002), 267-306.

[11] P. Deligne, *Les immeubles des groupes de tresses generalises*, Invent. Math. **17** (1972), 273-302.

[12] E. ElRifai and H. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford Ser (2), **45** (180) (1994), 479-497.

[13] D. Epstein, J. Cannon, F. Holt, S. Levy, M. Patterson and W. Thurston, *Word Processing in Groups*, Jones and Bartlett, Boston, MA 1992.

[14] F. Garside, *The braid group and other groups*, Quart. J. Math Oxford **20** (1969), 235-254.

[15] V. Gebhardt, *A new approach to the conjugacy problem in Garside groups*, Journal of Algebra **292**, No. 1 (2005), 282-302.

[16] J. González-Meneses, *The n^{th} root of a braid is unique up to conjugacy*, Algebraic and Geometric Topology **3** (2003), 1103-1118.

[17] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang and C. Park, *New publlic key cryptosystems using braid groups*, in Lecture Notes in Computer Science **1880**, Springer, Berlin 2000.

[18] E.K. Lee and S.J. Lee, *Translation numbers in a Garside group are rational with uniformly bounded denominators*, arXiv math.GT/0604061.

[19] E.-K. Lee and S. J. Lee, *A Garside-theoretic approach to the reducibility problem in braid groups,* arXiv math.GT/0506188.

[20] S. Maffre, PhD thesis. Université de Limoges, 2005. Available at `www.unilim.fr/theses/2005/sciences/2005limo0028/maffre_s.pdf`

[21] M. Picantin, PhD thesis. Université de Caen, 2000. Available at `www.liafa.jussieu.fr/~picantin/publi.html`

Juan González-Meneses:
Dept. Álgebra. Facultad de Matemáticas
Universidad de Sevilla.
Apdo. 1160.
41080 Sevilla (SPAIN)
E-mail: meneses@us.es
URL: www.personal.us.es/meneses

Volker Gebhardt:
School of Computing and Mathematics
University of Western Sydney
Locked Bag 1797
Penrith South DC NSW 1797, Australia
E-mail: v.gebhardt@uws.edu.au