A FAST SOLUTION TO THE CONJUGACY PROBLEM IN THE 4-STRAND BRAID GROUP

MATTHIEU CALVEZ AND BERT WIEST

Abstract. We present an algorithm for solving the conjugacy search problem in the four strand braid group. The computational complexity is cubic with respect to the braid length.

1. Introduction

The *conjugacy problem* is one of the three famous decision problems in groups first formulated by Dehn in the early 20th century. The aim is to decide whether two given elements x and y of a group G are conjugate in G, i.e. whether there exists an element z in G such that $x = z^{-1}yz$ (which we shall denote $x = y^z$). If so, then an additional problem is to actually search for such a conjugating element z. These two problems are called CDP (conjugacy decision problem) and CSP (conjugacy search problem).

We know since Garside [17] that CDP and CSP are solvable for the braid groups B_n, meaning that there exists an algorithm for solving these two problems in B_n, $n \geqslant 1$. In fact, the properties of braid groups discovered in [17] are now known to hold for a large class of groups, called Garside groups [13]; this class of groups contains for instance all Artin-Tits groups of spherical type [7].

A *Garside group* is a group equipped with a Garside structure, that is, roughly speaking, a lattice structure together with a distinguished element Δ satisfying some properties initially discovered by Garside for braids in [17]. A crucial output of this is the left normal form for each element of a Garside group G: this is a unique decomposition of the form $\Delta^p x_1 \dots x_r$ where the factors belong to the set of the so-called *simple elements*. This provides a measure of the length of an element: the *canonical length* $\ell(x)$ of an element $x \in G$ is the integer r in the decomposition above. See Section 2 for more details. In the particular case of the braid groups, two distinct Garside structures are known. The *classical* one, stemming from Garside's original article [17] and the *dual* one, introduced by Birman, Ko and Lee in [5].

Since Garside, several more and more powerful algorithms for solving CDP and CSP have been proposed [15, 18, 19]. We briefly recall that each of the algorithms [15, 18, 19] for solving CDP and CSP in a Garside group G is based on the calculation, for any given $x \in G$, of a finite non-empty subset E_x of the conjugacy class of x, satisfying $E_x = E_y$ if and only if x and y are conjugate. The *Super Summit Sets* (*SSS*) [15], the *Ultra Summit Sets* (*USS*) [18] and the *sets of Sliding*

2010 *Mathematics Subject Classification.* 20F36, 20F10.

Circuits (*SC*) [19] are three examples of such characteristic subsets. Unfortunately, despite the very high speed (in practice) of the most recent algorithms, the existence of a polynomial bound on the algorithmic complexity (with respect to the length of the input) is still an open problem, even in the case of the braid groups.

The main result of the current article is the following:

Theorem 1.1. *There exists an algorithm which solves CDP and CSP in the braid group B_4 and whose algorithmic complexity is cubic with respect to the length of the input braid words.*

We are not able to prove Theorem 1.1 using only the tools of Garside theory. We shall also use a geometric point of view on braids. It is known (see e.g. [1]) that the braid group B_n $(n \geqslant 1)$ can be identified with the mapping class group of the n-times closed punctured disk $\mathbb{D}_n$. In this context, braids can be classified according to their dynamical properties, in the following trichotomy (Nielsen-Thurston classification) [11, 16]: a braid x is

- *periodic*, if there exists an integer m such that $x^m \in ZB_n = \langle \Delta^2 \rangle$,
- *reducible*, if there exists a non-empty family $\mathcal{F}$ (called the *canonical reduction system*) of isotopy classes of nondegenerate disjoint simple closed curves in $\mathbb{D}_n$ (non-degenerate means not null-homotopic, not homotopic into a puncture and not boundary-parallel) such that
    - the x-action leaves $\mathcal{F}$ invariant,
    - no element of $\mathcal{F}$ intersects an other isotopy class of simple closed curve in $\mathbb{D}_n$ which is invariant under some power of x
- *pseudo-Anosov* (pA) otherwise.

We remark that the definition of "reducible" most frequently found in the literature also encompasses certain periodic elements. In this paper we only apply the word "reducible" to the braids which would usually be called "reducible non-periodic".

The paper [2] proposes a program, based both on the above classification and on Garside theory, for solving CDP and CSP in the braid groups *in polynomial time* with respect to both the length of the input braid words and their number of strands. A first step in this program is the construction of a polynomial time algorithm for deciding the dynamical type of any given braid (Open question 1 in [2]).

In [9], the authors answered this question in the case of the group B_4: they produced an algorithm of complexity $O(\ell^2)$ to decide the Nielsen-Thurston type of any given 4-strand braid of length ℓ. Thus in the group B_4, in order to solve CDP and CSP it is sufficient to solve these problems for pairs of elements which are known to be of the same dynamical type (as pairs of braids of different dynamical type are never conjugate).

The algorithm given in [9] also implies a solution to CDP and CSP for *reducible* four-strand braids of length at most ℓ in time $O(\ell^2)$. The main lemma here is that for braids with at most 3 strands and of length at most ℓ, the problems CDP and CSP are solvable in time $O(\ell^2)$, see [9].

The case of *periodic* braids is treated in [4], where an algorithm of complexity $O(\ell^3 n^2 \log n)$ for solving CDP and CSP for periodic braids with n strands of canonical length at most ℓ is presented.

In order to prove Theorem 1.1, we thus have to produce an algorithm of complexity at most $O(\ell^3)$ capable of solving CDP and CSP for *pseudo-Anosov* four-strand braids of length at most ℓ. Technically, our main contribution is the following result, which gives a partial affirmative answer (in the special case of pseudo-Anosov 4-strand braids) to the Open Question 2 in [2]: using the vocabulary of [19], if a 4-strand pseudo-Anosov braid is *rigid* (meaning, roughly speaking, that the normal form is as simple as possible), then its set of Sliding Circuits (and also its Ultra Summit Set) is "small":

Theorem 1.2. *For every braid x in B_4 which is pseudo-Anosov and rigid with respect to the dual Garside structure, the cardinality of $SC(x)$ for the dual structure is bounded above by $O(\ell(x)^2)$.*

This result implies that the algorithm given in [20] for solving CDP and CSP has complexity $O(\ell^3)$ when applied to two 4-strand braids which are of length at most ℓ, pseudo-Anosov and rigid in the dual structure.

The rest of the proof of Theorem 1.1 thus has to consist of a reduction to the rigid case. We shall prove, thanks mostly to Masur-Minsky's conjugacy bound [24]:

Theorem 1.3. *There is an algorithm with the following properties:*

- *as input, it takes two pseudo-Anosov braids $x, y \in B_n$ of canonical length at most ℓ,*
- *as output, it yields an integer s and n-strand braids $\bar{x}$, $\bar{y}$, z_1 and z_2 such that $\bar{x}$ and $\bar{y}$ are rigid and satisfy $\bar{x} = (x^s)^{z_1}$ and $\bar{y} = (y^s)^{z_2}$,*
- *for any fixed n, the complexity is $O(\ell^2)$.*

Then for $n = 4$, the quick solution to CDP/CSP for two rigid pseudo-Anosov braids $\bar{x}$ and $\bar{y}$ results in a quick solution to the same problems for the initial pseudo-Anosov braids x and y, because of the unicity of roots of pseudo-Anosov braids [21]. We are now in position to describe the algorithm promised by Theorem 1.1:

ALGORITHM:
INPUT: x and y two elements of the four-strand braid group.
OUTPUT: whether or not x and y are conjugate, and if they are, an element $z \in B_4$ so that $x = y^z$.

(1) Determine the dynamical types of x and y, using [9]. If they are not the same, answer "x and y are not conjugate" and STOP.
(2) If x and y are periodic use [4] and STOP.
(3) If x and y are reducible, use [9] and STOP.
(4) If x and y are pseudo-Anosov, use the algorithm of Theorem 1.3 in order to produce $s, \bar{x}, \bar{y}, z_1, z_2$ with the required properties.
(5) Apply Algorithm 3 of [20] to $\bar{x}$ and $\bar{y}$. If $\bar{x}$ and $\bar{y}$ are conjugate, then this algorithm produces $c \in B_4$ such that $\bar{x} = \bar{y}^c$. In this case answer "x is conjugate to y by $z_2 c z_1^{-1}$." and STOP.
(6) Answer "x and y are not conjugate".

Remark 1.4. Note that the preceding algorithm is completely explicit (in particular, we shall prove Theorem 1.3 by explicitly constructing the required algorithm). However, our cubic bound on the algorithmic complexity in Theorem 1.1

is not explicit, and this is due to the non-explicitness of Masur-Minsky's conjugacy bound [24]. More precisely, there are two things for which we have only existence proofs, not explicit constructions, namely

(1) the quadratic function bounding the size of $SC(x)$ in Theorem 1.2 (see Proposition 5.12),
(2) the linear function bounding the number of cyclic slidings in the proof of Theorem 1.3, and thus the quadratic bound on the complexity of the algorithm in Theorem 1.3.

Remark 1.5. The proposed algorithm itself was probably known to experts in the field. As is explained above, Steps 1 to 3 were known to have polynomial complexity; thus our main contribution is showing the polynomial complexity of Step 5 (Theorem 1.2) and Step 4 (Theorem 1.3, resting on Masur-Minsky's linear bound).

This paper is organized as follows. In Section 2 we recall some definitions and basic facts about Garside groups. Assuming Theorem 1.2, we prove Theorem 1.3 and Theorem 1.1 in Section 3. The two last sections are devoted to the proof of Theorem 1.2.

Acknowledgements. The authors are grateful to Juan González-Meneses for suggesting a simplification in the proof of Theorem 1.2. The first-named author was partially supported by a grant from Région Bretagne, by MTM2010-19355 and FEDER, and by FONDECYT through postdoctoral grant no. 3130569 and the Center of Dynamical Systems and Related Fields (project Anillo 1103).

After this paper was completed, Sang Jin Lee communicated to us that a (degree 4) polynomial solution to the conjugacy problem in the 4-strand braid groups was already present in his unpublished PhD Thesis [23]. He notably showed a (degree 4) polynomial bound as in Theorem 1.2, also in the context of the dual Garside structure.

2. The conjugacy problem in Garside groups

In this section we recall the definition and some general facts concerning Garside groups and the known solutions to the conjugacy problem.

Definition 2.1. [19] *Let G be a group. We say that G is a* Garside group *(of finite type) if it admits a submonoid P satisfying $P \cap P^{-1} = \{1\}$ (the monoid of* positive elements*) and a distinguished element $\Delta \in P$* (Garside element) *such that the following properties hold:*

(1) *The partial order $\preccurlyeq$ on G defined by $x \preccurlyeq y$ if and only if $x^{-1}y \in P$ is a lattice order, meaning that any two elements admit a greatest common divisor and a least common multiple (note that it is invariant under left-multiplication); this is called the* prefix order*,*
(2) *The set $\{x \in G, 1 \preccurlyeq z \preccurlyeq \Delta\}$ is finite and generates G; its elements are called* simple elements*,*
(3) *Conjugation by Δ preserves the submonoid P,*

(4) *For every $x \in P - \{1\}$,*

$$||x|| = \sup\{k \ \exists\ a_1, \dots, a_k \in P - \{1\},\ x = a_1 \cdots a_k\} < \infty.$$

In this context we also say that the triple (G, P, Δ) is a Garside structure *of finite type for G.*

Throughout this section, G denotes a Garside group with Garside structure (G, P, Δ). The greatest common divisor of two elements x, y of G with respect to $\preccurlyeq$ is denoted by $x \wedge y$. We denote by τ the inner automorphism associated to Δ. Because it preserves P and hence $\preccurlyeq$, the automorphism τ induces a permutation of the (finite) set of simple elements, and since these elements generate G, τ is of finite order.

We also recall that every simple element s possesses a *right complement* $\partial(s)$ defined by the formula $\partial(s) = s^{-1}\Delta$. This allows to define the notion of *left-weightedness*: a pair of simple elements s_1, s_2 is said to be *left-weighted* if $\partial(s_1) \wedge s_2 = 1$, or in other words if s_1 is the greatest simple divisor of $s_1 s_2$.

A crucial property of Garside groups is the existence of unique (*left*) *normal forms*:

Proposition 2.2. [13, 15] *Let $x \in G$. There exists a unique decomposition $x = \Delta^p x_1 \dots x_r$, where r is a non-negative integer, the factors x_i are simple elements such that $x_1 \neq \Delta$, $x_r \neq 1$, and (if $r \geqslant 2$) the pair $x_i x_{i+1}$ is left-weighted for $i = 1, \dots, r-1$.*

If the left normal form of x is $\Delta^p x_1 \dots x_r$, the integers p and r are called the *infimum* and the *canonical length* of x, and they are denoted by $\inf(x)$ and $\ell(x)$. They are respectively the maximal integer $p \in \mathbb{Z}$ such that Δ^p is a prefix of x and the minimal number of simple factors needed to express the element $\Delta^{-p}x$. The *supremum* $\sup(x)$ is the quantity $p+r$. For every element x of G, $\sup(x) = \min\{k \in \mathbb{Z}, x \preccurlyeq \Delta^k\}$.

We observe that the elements of canonical length zero are precisely the powers of Δ; these elements are as simple as possible within their conjugacy class. For an element x of positive canonical length and normal form $\Delta^p x_1 \dots x_r$, one can define its *initial* and *final* factor as

$$\iota(x) = \tau^{-p}(x_1), \quad \varphi(x) = x_r.$$

Remark 2.3. The set of simple elements, taken as a generating set of G, induces a length function on G: the length $|x|$ of an element x of G is by definition the smallest possible length of a word representing x whose letters are simple elements or their inverses. We note that always $\ell(x) \leqslant |x|$. We also have the following relations, for any x satisfying $\inf(x) = p$ and $\ell(x) = r$ [13, 12]:

$$|x| = \begin{cases} p + r & \text{if } p \geqslant 0, \\ r & \text{if } p < 0 \text{ and } |p| \leqslant r, \\ |p| & \text{if } p < 0 \text{ and } |p| > r. \end{cases}$$

We recall that G is equipped with different operations which are defined in terms of normal forms, each corresponding to a particular conjugation.

Definition 2.4. [15] *Let $x \in G$ with normal form $x = \Delta^p x_1 \dots x_r$. Suppose $r \geqslant 1$. We define:*

- *the* cycling $\mathbf{c}(x) = x^{\iota(x)} = \Delta^p x_2 \dots x_r \tau^{-p}(x_1)$,
- *the* decycling $\mathbf{d}(x) = x^{\varphi(x)^{-1}} = \Delta^p \tau^p(x_r) x_1 \dots x_{r-1}$.

If $\ell(x) = 0$, we also define $\mathbf{c}(x) = \mathbf{d}(x) = x$.

More recently, Gebhardt and González-Meneses introduced a new type of conjugation which combines cycling and decycling into a single, conceptually simpler, operation:

Definition 2.5. [19] *Let $x \in G$ with normal form $x = \Delta^p x_1 \dots x_r$. Suppose $r \geqslant 1$. We define the* preferred prefix *of x by the formula $\mathfrak{p}(x) = \iota(x) \wedge \partial(\varphi(x))$.* Cyclic sliding *is the operation $\mathfrak{s}$ defined by*

$$\mathfrak{s}(x) = x^{\mathfrak{p}(x)}.$$

If $\ell(x) = 0$ then we also define $\mathfrak{s}(x) = x$.

The aim of cycling, decycling and cyclic sliding is to simplify the left normal forms; note that we have $\ell(\mathbf{c}(x)) \leqslant \ell(x)$, $\ell(\mathbf{d}(x)) \leqslant \ell(x)$ and $\ell(\mathfrak{s}(x)) \leqslant \ell(x)$. Also note that all of the three operations commute with the automorphism τ. Finally we make the following computational observation, which will be very useful in the sequel: if x is an element of G given in normal form, then its respective results under the three previously defined special conjugations can be computed in time $O(\ell(x))$.

Proposition 2.6. [15] *Let $x \in G$.*

(i) [15] *The subset of the conjugacy class of x consisiting of all elements with minimal canonical length is finite and non-empty. Its elements have* simultaneously *maximal infimum and minimal supremum. This subset is called the* Super Summit Set *of x, and denoted by $SSS(x)$.*
(ii) [15] *There exist $k_0, l_0 \in \mathbb{N}$ such that for every $k \geqslant k_0$ and $l \geqslant l_0$, $\mathbf{c}^k(\mathbf{d}^l(x)) \in SSS(x)$.*
(iii) [19] *There exists $k_0 \in \mathbb{N}$ such that for every $k \geqslant k_0$, $\mathfrak{s}^k(x) \in SSS(x)$.*

The observation that $\mathfrak{s}$ preserves $SSS(x)$ implies that the set of periodic points of $\mathfrak{s}$ in the conjugacy class of x is a (finite) nonempty subset of $SSS(x)$; this defines another conjugacy invariant:

Definition 2.7. [19] *Let $x \in G$. The* set of Sliding Circuits *of x is the set of all conjugates of x which are periodic points of the cyclic sliding operation. That is, $SC(x) = \{y \in x^G \mid \exists k \in \mathbb{N},\ \mathfrak{s}^k(y) = y\}$.*

An important example of fixed points of $\mathfrak{s}$ are the so-called rigid elements:

Definition 2.8. *Let $x \in G$ with normal form $x = \Delta^p x_1 \dots x_r$. Suppose $r \geqslant 1$. We say x is* rigid *if the pair $\varphi(x)\iota(x)$ is left-weighted.*

In particular, an element of canonical length 0 is not rigid. Let us mention that ([2] Lemma 3.5) an element $x \in G$ is rigid if and only if x^{-1} is.

One very useful quality of the Super Summit Set, which is not known to hold for the set of Sliding Circuits (see Proposition 3.2) is that it can *quickly* be reached by iterated cyclic sliding:

Theorem 2.9. [6, 19] *Let G be a Garside group. Then there exists a constant α, which depends only on the group G and its Garside structure, such that for every $x \in G$, $\mathfrak{s}^{\ell(x)\cdot\alpha}(x) \in SSS(x)$.*

For instance in the case of the classical Garside structure on B_n we have $\alpha = \frac{n(n-1)}{2}$, and $\alpha = n-1$ for the dual structure. This result has a very important algorithmic application: it yields an algorithm of complexity $O(\ell^2)$ for calculating an element $y \in SSS(x)$ for any given $x \in B_n$ in normal form of canonical length $\ell(x) = \ell$. The algorithm can even output an explicit conjugating element between x and y.

For the rest of the paper, we shall mostly be dealing with braids which lie in their own Super Summit Set (because pushing braids into their own SSS only costs $O(\ell^2)$, as we have just seen).

3. Proofs of Theorems 1.3 and 1.1

Throughout the section we shall assume Theorem 1.2 holds. Provided with the precise definitions and vocabulary related to the conjugacy problem in Garside groups, we now proceed to prove Theorems 1.3 and 1.1. The plan is to prove Theorem 1.3 first, and then to prove the validity of the algorithm described in the Introduction and to analyse its complexity.

First we recall one of the main results of [2]:

Theorem 3.1. ([2], Theorem 3.37) *Let $x \in B_n$ be a pseudo-Anosov braid. Then there exists an integer m such that x^m is conjugate to a rigid braid. Moreover, the integer m can be bounded independently of the length of x: $m < (\frac{n(n-1)}{2})^3$ for the classical Garside structure and $m < (n-1)^3$ for the dual structure.*

The second main ingredient in Theorem 1.3 is Masur-Minsky's linear conjugacy bound [24], through the following result from [8] whose proof relies on the latter bound. (Recall that $\mathfrak{s}$ denotes the cyclic sliding operation – see Definition 2.5).

Proposition 3.2. ([8], Theorem 2) *There exists a constant C, depending only on n and on the chosen Garside structure, with the following property: if $x \in B_n$ is a pseudo-Anosov braid lying in its own Super Summit Set, and if x possesses some rigid conjugate, then the conjugate $\mathfrak{s}^{C|x|}(x)$ is rigid.*

This proposition yields a quadratic time algorithm for finding a rigid conjugate y of any given pseudo-Anosov braid x satisfying $x \in SSS(x)$, and also for finding a conjugating element, provided a rigid conjugate exists at all.

We are now ready to prove Theorem 1.3.

Proof of Theorem 1.3. First recall that n is considered fixed. Let us denote $\beta(n)$ the upper bound on m in the statement of Theorem 3.1. Let $x, y \in B_n$ be pseudo-Anosov braids. Our aim is to algorithmically find rigid conjugates of x^s and y^s for some $s \in \mathbb{N}$.

Due to Theorem 3.1, there exist two integers i_x and i_y, both smaller than $\beta(n)$, such that x^{i_x} and y^{i_y} are conjugate to rigid braids. For all $i = 1, \ldots, \beta(n) - 1$

simultaneously, our algorithm iterates the operation $\mathfrak{s}$ starting from x^i, until a rigid braid is found. The corresponding power i_x and a braid z_x such that $(x^{i_x})^{z_x}$ is rigid are memorized. We denote $\tilde{x}$ this rigid conjugate of x^{i_x}. The same procedure, applied to y, yields an integer i_y and braids z_y and $\tilde{y}$ with the corresponding properties.

Note that the algorithm so far is doable in time $O(\ell^2)$, where ℓ is the maximum of the canonical lengths of x and y. In order to prove this, we remark that the canonical length of all the braids x^i and y^i, for $i = 1, \ldots, \beta(n) - 1$, is bounded above by $\beta(n)\ell$. By Theorem 2.9 and Proposition 3.2, the number of iterations needed in order to find $\widetilde{x}$ is linearly bounded with respect to this length $\beta(n)\ell$. Finally, each iteration of the operation $\mathfrak{s}$ on a braid of canonical length ℓ takes time $O(\ell)$(see [20]).

Let $s = lcm(i_x, i_y)$. Since powers of rigid braids are again rigid, x^s and y^s are conjugate to rigid braids. So all our algorithm has to do now is to calculate s, and output $\bar{x} = \tilde{x}^{\frac{s}{i_x}}$, $\bar{y} = \tilde{y}^{\frac{s}{i_y}}$, and $z_1 = z_x$, $z_2 = z_y$. This satisfies the requirements of Theorem 1.3. □

Proof of Theorem 1.1. We have to prove that the algorithm described in the introduction is valid and of complexity $O(\ell(x)^3)$. Steps (1) and (3) are of complexity $O(\ell^2)$, as was shown in [9]. Step (2) is of complexity $O(\ell^3)$ (see Theorem 1 in [4]). Step (4) is of complexity $O(\ell^2)$, by Theorem 1.3. Finally, Theorem 4.11 of [20] ensures us that Algorithm 3 in [20] correctly solves CDP and CSP for rigid braids of length at most ℓ in time $O(\ell \cdot \kappa)$, where κ denotes the cardinality of the sets of Sliding Circuits of the input braids. Our Theorem 1.2 now implies that step (5) of our algorithm has complexity $O(\ell^3)$. Finally, step (5) gives the correct answer, because of [21] (Subsection 4.2). Indeed, it is shown there that for any $m \in \mathbb{N}$, any pseudo-Anosov braid has *at most one* mth root, so that the relation $\bar{x} = \bar{y}^c$ for a braid c (i.e. $(x^s)^{z_1} = ((y^s)^{z_2})^c$) is equivalent to the relation $x^{z_1} = y^{z_2 c}$, which is in turn equivalent to x being conjugate to y by $z_2 c z_1^{-1}$. □

It therefore remains to prove Theorem 1.2; this occupies the rest of the paper.

4. Prerequisites for the proof of Theorem 1.2

We advise the reader that none of the results in this section are new; however, we shall introduce some non-standard notation which will be useful in the proof.

4.1. **Sets of Sliding Circuits of rigid elements.** Our aim is to describe the structure of the set of Sliding Circuits of a rigid element of a Garside group. We use the same notations as in Section 2. The following results are proven in [19], for any element rigid or not. First we note that the set $SC(x)$ is stable under conjugation by Δ, cycling and decycling.

Definition 4.1. [19] *Let $x \in G$ and $y \in SC(x)$. A simple, non-trivial element s of G is said to be a* minimal arrow *for y if $y^s \in SC(x)$ and if the only positive prefixes t of s with $y^t \in SC(x)$ are $t = 1$ and $t = s$.*

Proposition 4.2. [19]*(See also* [3]*, Corollary 2.7). Let $x \in G$. For every $y \in SC(x)$, the minimal arrows for y are prefixes of $\iota(y)$ or of $\partial(\varphi(y))$.*

Definition 4.3. [19] *To every element x of G we associate a connected, oriented graph $SCG(x)$ describing the set $SC(x)$ as follows:*

- *the graph has one vertex for every element of $SC(x)$,*
- *for every element y of $SC(x)$ and every minimal arrow s for y, the graph $SCG(x)$ has an oriented edge from the vertex y to the vertex y^s. This edge is labelled s.*

When x has a rigid conjugate, the graph $SCG(x)$ has a particularly elegant structure, which we describe now. Our study is based mainly on the following proposition from [19]:

Proposition 4.4. ([19], Theorem 1) *Let $x \in G$. Suppose that x has a rigid conjugate. Then $SC(x)$ is precisely the set of all rigid conjugates of x.*

Definition 4.5. *Let $x \in G$ be a rigid element, and let $y \in SC(x)$. The* orbit *of y is the set $O_y = \{\tau^k \mathbf{c}^l(y) \mid k, l \in \mathbb{N}\}$.*

Lemma 4.6. *Let $x \in G$ be a rigid element, and let $y \in SC(x)$.*

(i) *The orbit O_y is a subset of $SC(x)$.*
(ii) *The orbit O_y is stable under cycling, decycling, and τ; in particular, for every $z \in O_y$, $z^{\iota(z)}$ and $z^{\partial(\varphi(z))}$ are element of O_y.*
(iii) *Let $y_1, y_2 \in SC(x)$. Then $O_{y_1} \neq O_{y_2}$ if and only if $O_{y_1} \cap O_{y_2} = \emptyset$.*
(iv) *The cardinality of the orbit O_y is bounded above by $f \cdot \ell(y)$, where f is the order of τ).*

Proof. Just observe that cycling and decycling induce cyclic permutations (up to τ) of the non Δ factors of the normal form of a rigid element. □

For the rest of this subsection we shall always suppose that x is rigid. The relation $\sim$, defined by $x \sim y$ if and only if $O_x = O_y$, is an equivalence relation on $SC(x)$, and $SC(x)$ is the disjoint union of the different orbits O_y. We denote by $\widetilde{SC}(x)$ the quotient set $SC(x)/\!\sim$. We now associate a "quotient graph" $\widetilde{SCG}(x)$ to $\widetilde{SC}(x)$ in the same way as $SCG(x)$ is associated to $SC(x)$. In order to do this rigorously, we need the following definition:

Definition 4.7. *Let $y \in SC(x)$ be rigid, and let s be a minimal arrow for y. We say s is a minimal* useful *arrow if $y^s \notin O_y$.*

Remark 4.8. According to Proposition 4.2 and Lemma 4.6 (ii), the minimal useful arrows for y are *strict* prefixes of $\iota(y)$ or of $\partial(\varphi(y))$.

We recall the notion, due to Gebhardt [18], of the *transport under cycling* of an arrow: if $y, s \in G$, we define the transport under cycling of s at y by the formula $s_y^{(1)} = \iota(y)^{-1} s \iota(y^s)$. It is known ([18], Corollary 2.7) that the transport induces a bijection between the set of minimal arrows for $y \in SC(x)$ and the set of minimal arrows for $\mathbf{c}(y)$. Similarly, conjugation by Δ induces a bijection between the minimal arrows for y and the minimal arrows for $\tau(y)$. In particular, if s is a minimal useful arrow between y and y^s, then $s_y^{(1)}$ is a minimal useful arrow between $\mathbf{c}(y)$ and $\mathbf{c}(y^s)$, and $\tau(s)$ is a minimal useful arrow between $\tau(y)$ and $\tau(y^s)$. Thus we can define the desired quotient graph without any ambiguity (i.e. the arbitrary choices made in the following definition do not matter):

Definition 4.9. *To every rigid element x of G we associate a connected, oriented graph $\widetilde{SCG}(x)$ as follows:*

- *The vertices of the graph correspond to elements of $\widetilde{SC}(x)$,*
- *For every element $O_y \in \widetilde{SC}(x)$, we arbitrarily choose a representative y' of O_y. Now, to any minimal useful arrow s for y', from $y' \in O_y$ to $z' \in O_z$, we associate an edge of the graph, oriented from O_y to O_z.*

In order to bound the size of $SC(x)$, it suffices to bound the number of vertices of $\widetilde{SCG}(x)$: if $\widetilde{SCG}(x)$ has k vertices, then the cardinality of $SC(x)$ is at most $k \cdot f \cdot \ell(x)$ (due to Lemma 4.6 (iv)).

4.2. The dual structure of B_4.

A detailed account of the dual Garside structure on braid groups can be found in the original article [5], and an introduction in Chapter VIII of [14]. We restrict ourselves here to a brief description of this structure in the case of the four-strand braid group B_4. We consider the sub-monoid BKL_4^+ of B_4 generated by the braids $a_{p,q}$, $1 \leqslant p < q \leqslant 4$, where

$$a_{p,p+1} = \sigma_p \quad \text{for} \quad p = 1, \ldots, 3,$$

$$a_{1,3} = \sigma_2^{-1}\sigma_1\sigma_2,$$

$$a_{2,4} = \sigma_3^{-1}\sigma_2\sigma_3,$$

$$a_{1,4} = \sigma_3^{-1}\sigma_2^{-1}\sigma_1\sigma_2\sigma_3.$$

The notation BKL is derived from the names of the discoverers of this structure: Birman, Ko and Lee. The monoid BKL_4^+ induces a partial order relation on B_4: $x \preccurlyeq y$ if and only if $x^{-1}y \in BKL_4^+$. Taking as Garside element the braid $\delta = \sigma_1\sigma_2\sigma_3$, these data give rise to a new Garside structure, which we denote BKL_4. For instance, we shall write $x \in BKL_4$ in order to say that x is a four-strand braid seen in the structure BKL_4, and given as a product of the generators $a_{i,j}$.

We now introduce some notation concerning the BKL_4-structure which we shall be using for the rest of the article. We recall that B_4 can be seen as the mapping class group of the four times punctured disk $\mathbb{D}_4$. In the context of the BKL_4-structure it is practical to parametrize $\mathbb{D}_4$ as the unit disk in $\mathbb{C}$ with punctures $P_j = \frac{1}{2}e^{-\frac{i(2j-1)\pi}{4}}$, for $j = 1, \ldots, 4$. The braid $a_{p,q}$ then corresponds to the counterclockwise half Dehn-twist along the arc (P_p, P_q). Pictorially, we will represent the braid $a_{p,q}$ by the segment (P_p, P_q); for instance, $a_{2,4}$ is denoted (), $a_{1,4}$ is written (), and so on. Similarly, the braid which cyclically exchanges P_3, P_2 and P_1 by a counterclockwise movement is denoted (). With this notation, the generators $a_{p,q}$ are subject to the following relations:

$$()() = ()() = (), \;\; ()() = ()() = (),$$

$$()() = ()() = ()() = (), \;\; ()() = ()() = ()() = (),$$

$$()() = ()() = ()() = (), \;\; ()() = ()() = ()() = ().$$

The Garside element is $\delta = ()$. Conjugation by δ corresponds to a one-quarter counterclockwise turn, and τ is an automorphism of order 4 of B_4. Therefore, Lemma 4.6(iv), applied to the BKL_4-structure, states that the orbit of a rigid braid x contains at most $4 \cdot \ell(x)$ elements.

Our proof of Theorem 1.2 is based on the simplicity of the lattice of simple elements of BKL_4. It has only 14 elements:

$$1, (), (), (), (), (), (), (), (), (), (), (), (), \delta.$$

The relations listed above are length-preserving (the word length on the letters $a_{p,q}$). This allows us to define a morphism $\lambda\colon\ B_4 \longrightarrow \mathbb{Z}$ by sending every braid $a_{p,q}$ to 1. For any braid x, we call $\lambda(x)$ the *weight* of x. We have $\lambda(\delta) = 3$ and for any other simple nontrivial element s we have $\lambda(s) = 1$ or 2. This observation (as already noted in [6]) yields a new quantity, in addition to canonical length, supremum and infimum, which is constant inside the Super Summit Set:

Lemma 4.10. *Let $x \in BKL_4$, and let $y \in SSS(x)$. For every $z \in SSS(x)$, the normal form of z contains as many factors of weight 2 and as many factors of weight 1 as the normal form of y.*

Proof. For every braid $x \in BKL_4$, if k_1 is the number of factors of weight 1 and k_2 the number of factors of weight 2 in the normal form of x, then $\ell(x) = k_1 + k_2$ and $\lambda(x) = 3\inf(x) + 2k_2 + k_1$. Thus k_1 and k_2 are constant in the Super Summit Set, since canonical length, weight, and infimum are constant there. □

Again concerning the weight of the factors of a normal form, we make the following simple observation which will be needed later.

Remark 4.11. Recall that if x has normal form $\delta^p x_1 \dots x_r$, then its inverse x^{-1} has normal form $\delta^{-p-r} x'_r \dots x'_1$, where $x'_i = \tau^{-p-i}(\partial(x_i))$ ([2], Theorem 1.5 for any Garside group). In particular , we have for the BKL_4 case $\lambda(x'_i) = 3 - \lambda(x_i)$.

The following very simple remark will turn out to be very useful:

Remark 4.12. Let a and b be two simple elements for BKL_4. If a is of weight 2 and δ does not divide the product ab, then the pair $a \cdot b$ is left-weighted.

We finally claim that in the BKL_4 structure, the existence of a minimal useful arrow s from $y' \in O_y$ to $z' \in O_z$ is equivalent to the existence of a minimal useful arrow from $z' \in O_z$ to some element of O_y. (In other words, every edge in $\widetilde{SCG}(x)$, for $G = BKL_4$, is oriented both ways.) Let us prove this claim. According to Remark 4.8, such a minimal arrow s is a *strict* prefix either of $\iota(y')$ or of $\partial(\varphi(y'))$. In particular, $\lambda(s) = 1$. Now there is an arrow, which is of weight 1 and thus minimal, given in the first case by $s^{-1}\iota(y')$ from z' to $\mathbf{c}(y')$, and in the second case by $s^{-1}\partial(\varphi(y'))$, from z' to $\tau\mathbf{d}(y')$.

5. Proof of Theorem 1.2

Throughout this section, we use the dual Garside structure on B_4. Our aim is to prove Theorem 1.2, so we consider a rigid pseudo-Anosov braid x, and we try to bound the size of $SC(x)$. The hypothesis that x is pseudo-Anosov implies that the canonical length of x is strictly larger than 1 (this can be proven by analysing all braids with canonical length 1).

We shall see that it suffices to prove Theorem 1.2 separately in three special cases, which are defined in terms of the simple factors occurring in x (see Subsection 4.2). We will consider successively the following three cases:

- The normal form of x contains at least one factor of weight 1 and one factor of weight 2 – this case is solved in Proposition 5.1. (Notice that all other elements of $SC(x)$ will have the same property, by Lemma 4.10).
- There exists an element y of $SC(x)$ such that all the factors other than δ occurring in the normal form of y belong to $\{(),(),(),()\}$ – this case is solved in Proposition 5.3.
- For every element y of $SC(x)$, all the factors other than δ occurring in the normal form of y are of weight 1, and at least one of them is () or () – this case is solved in Proposition 5.12.

In the first two cases, the hypothesis that x should be pseudo-Anosov is in fact unnecessary. In these cases, we even construct a *linear* bound on $\#SC(x)$. The third case requires much more sophisticated techniques, and gives rise to an example showing that the quadratic bound is optimal.

5.1. **A simple special case.**

We now describe a simple special case where Theorem 1.2 can be proved by elementary arguments.

Proposition 5.1. *Let $x \in BKL_4$ be a rigid braid whose normal form contains at least one factor of weight 1 and at least one factor of weight 2. Then the set $SC(x)$ consists only of O_x and in particular $\#SC(x) \leqslant 4 \cdot \ell(x)$.*

Proof. We shall see that no strict prefix of $\iota(x)$ (nor of $\partial(\varphi(x))$) can conjugate x to a rigid braid and in particular x has *no* minimal useful arrow. Suppose on the contrary that $t \prec \iota(x)$ and that x^t is rigid. Then using the fact that the transport under cycling (already alluded to above in the paragraph before Definition 4.9) preserves the order $\preccurlyeq$ ([18], Corollary 2.2 (b)), we see that the transport $t^{(1)}$ of t satisfies $1 \prec t^{(1)} \prec \iota(\mathbf{c}(x))$ (and conjugates $\mathbf{c}(x)$ to the rigid braid $\mathbf{c}(x^t)$). Iterating this argument we see that *all* factors of x must have weight 2, contradicting our hypothesis. On the other hand, if t were a strict prefix of $\partial(\varphi(x))$, the same line of argument applied to x^{-1} would finally establish that *all* factors of x have weight 1 (Remark 4.11). The latter part of the claim in Proposition 5.1 follows immediately from the former together with Lemma 4.6(iv). □

Now, in order to prove Theorem 1.2, we have to find a quadratic bound on the size of $SC(x)$ for any rigid pseudo-Anosov braid $x \in BKL_4$. By Proposition 5.1, we can restrict our attention to braids whose normal form has all its factors (other than δ) of the same weight (1 or 2). Up to considering inverses, we can restrict ourselves to the case of weight 1 (see [3], Subsection 3.1 where it is shown that when x is rigid (and so is x^{-1}), the graphs $SCG(x)$ and $SCG(x^{-1})$ are isomorphic).

So for the rest of the proof of Theorem 1.2, we can suppose that x is a rigid pseudo-Anosov braid whose normal form has only factors of weight 1 (i.e. (), (), (), (),

(), ()), and $\delta^{\pm 1}$. By Lemma 4.10, all elements of $SSS(x)$ have the same property. Moreover, using Remark 4.8, we see that for every $y \in SC(x)$, all possible minimal useful arrows for y are strict prefixes of $\partial(\varphi(y))$ (there is no strict non-trivial prefix of $\iota(y)$ because $\lambda(\iota(y)) = 1$). In particular, all vertices of $\widetilde{SCG}(x)$ have degree at most 3.

We make one more simple, but very useful general observation:

Lemma 5.2. *Suppose that the normal form of the rigid braid $y \in SC(x)$ has only factors of weight 1 (and $\delta^{\pm 1}$), with at least one factor equal to () or to (). Then the vertex O_y of $\widetilde{SCG}(x)$ is of degree at most 2.*

Proof. Up to replacing y by $y' \in O_y$, we can suppose that $\varphi(y) = ()$. But $\partial(()) = ()$, and this simple element has only two strict positive prefixes. □

We split the rest of our argument into two parts. In Subsection 5.2, we study the case where $SC(x)$ contains an element that does not satisfy the hypotheses of Lemma 5.2, i.e. an element whose normal form contains, apart from $\delta^{\pm 1}$, only the letters from $\{(), (), (), ()\}$; we shall denote the latter set $\mathcal{E}$. By contrast, Subsection 5.3 deals with the case where all elements of $SC(x)$ satisfy the hypotheses of Lemma 5.2.

5.2. **Some element of $SC(x)$ has all its factors in $\mathcal{E}$.** We recall the notation $\mathcal{E} = \{(), (), (), ()\}$. Our aim in this subsection is to prove the following result, whose proof is elementary but involves a lot of careful case-checking:

Proposition 5.3. *Let $x \in BKL_4$ be a rigid braid. Let us suppose that $SC(x)$ contains some element y whose normal form has all of its factors (apart from $\delta^{\pm 1}$) belonging to $\mathcal{E}$. Then the graph $\widetilde{SCG}(x)$ has at most six vertices. Moreover, $\#SC(x) \leqslant 24 \cdot \ell(x)$.*

The last sentence of Proposition 5.3 follows immediately from the preceding one, together with Lemma 4.6 (iv).

First we note that in order to prove Proposition 5.3, it suffices to prove that for some non-zero integer $m \in \mathbb{N}$ the graph $\widetilde{SCG}(x^m)$ has at most 6 vertices. Indeed, since all braids in $SC(x)$ are rigid, there is an injection from $\widetilde{SC}(x)$ to $\widetilde{SC}(x^m)$, sending an orbit O_y to an orbit O_{y^m}.

So possibly after replacing x by x^4, we can suppose that $\inf(x)$ is a multiple of 4. In fact, since for any integer m, multiplication by δ^{4m} induces an isomorphism between $SC(x)$ and $SC(\delta^{4m}x)$, we can even suppose that $\inf(x) = 0$ (and thus that the infimum of any element of $SSS(x)$ is zero).

So for the rest of the proof of Proposition 5.3, we shall assume that for y (and hence for all elements of O_y) the normal form has all letters belonging to $\mathcal{E}$.

Remark 5.4. Conjugation by δ induces a permutation of $\mathcal{E}$. Moreover, for all $s, t \in \mathcal{E}$, the product st is in normal form if and only if $t \in \{s, \tau(s)\}$.

Remark 5.4 allows us to give a precise description of the normal form of y:

Lemma 5.5. *Let $y \in BKL_4$ be a rigid braid with $\inf(y) = 0$, all of whose factors belong to $\mathcal{E}$. Then, possibly after replacing y by another element of O_y, the normal form of y is of the form*

$$y = \prod_{j=1}^{r} \tau^{-r+j}\left(()^{k_j} \right),$$

where the k_j, $j = 1, \ldots, r$ are strictly positive integers, and $r = 1$ or $r \equiv 0 \pmod 4$.

Proof. Up to conjugating y by a power of δ, we can suppose that $\varphi(y) = ()$. By Remark 5.4 and our hypothesis on y, the normal form of y is indeed a product of the form

$$y = \tau^{-(r-1)}\left(()^{k_1} \right) \ldots ()^{k_r}$$

for integers r and $k_1, \ldots, k_r$ all strictly positive. Then, due to rigidity and Remark 5.4, we have $\iota(y) = \varphi(y)$ or $\iota(y) = \tau\left(\varphi(y)\right)$. Let us suppose that $r > 1$. Up to cycling, we can suppose $\iota(y) = \tau\left(\varphi(y)\right)$, which means that $\tau^{-r+1}\left(()\right) = \tau\left(()\right)$. This implies that $r \equiv 0 \pmod 4$. □

Lemma 5.6. *If $r = 1$ in Lemma 5.5, then $\#SC(x) = 6$.*

Proof. If $r = 1$ then $SC(x) = \{()^{k_1}, ()^{k_1}, ()^{k_1}, ()^{k_1}, ()^{k_1}, ()^{k_1}\}$. □

Lemma 5.7. *Suppose that $r > 1$ in Lemma 5.5. Then there exists a minimal arrow for y if and only if $r \equiv 0 \pmod 3$. If this is the case, then y admits in fact three minimal (but not necessarily useful) arrows. If not, then the graph $\widetilde{SCG}(x)$ has a single vertex.*

Proof. According to Lemma 5.5, we have $r \equiv 0 \pmod 4$, and we can rewrite

$$y = \prod_{j=1}^{m}\left(()^{k_{j,1}} ()^{k_{j,2}} ()^{k_{j,3}} ()^{k_{j,4}} \right) =: \prod_{j=1}^{m} \alpha_j,$$

with $m := \frac{r}{4}$ and $k_{j,i} > 0$ for all j, i with $1 \leqslant j \leqslant m$ and $1 \leqslant i \leqslant 4$. The minimal useful arrows for y, if they exist, are all strict prefixes of $\partial(())$, so they are $()$, $()$ or $()$.

The proof of the lemma essentially comes down to the following calculations, where the right hand sides of the equations (except for their first factor) are always in normal form; in other words, A_j, B_j and C_j are normal forms, independently of the powers occurring in the formulae (this calculation uses the notation α_j defined in the previous paragraph):

$$\alpha_j () = () \left(()()^{k_{j,1}-1} ()^{k_{j,2}} ()()^{k_{j,3}} ()^{k_{j,4}-1} \right) =: ()A_j,$$

$$\alpha_j () = () \left(()()^{k_{j,1}} ()^{k_{j,2}-1} ()^{k_{j,3}} ()()^{k_{j,4}-1} \right) =: ()B_j,$$

$$\alpha_j () = () \left(()^{k_{j,1}} ()()^{k_{j,2}} ()^{k_{j,3}-1} ()^{k_{j,4}} \right) =: ()C_j.$$

We remark that, independently of j and of the powers occurring, the "pairs" $A \cdot C$, $B \cdot A$ and $C \cdot B$ are in normal form. On the one hand, if $r \equiv 1$ or $r \equiv 2 \pmod 3$, then this shows that for every u with $u \prec \partial(())$ we have $u \not\preccurlyeq yu$, and in particular

$y^u \notin SSS(x)$. On the other hand, if $m \equiv 0 \pmod 3$, then this shows that the three braids

$$y^{()} = \left(\prod_{j=1}^{\frac{m}{3}} \alpha_{3j-2}\alpha_{3j-1}\alpha_{3j}\right)^{()} = \prod_{j=1}^{\frac{m}{3}} C_{3j-2}B_{3j-1}A_{3j},$$

$$y^{()} = \prod_{j=1}^{\frac{m}{3}} B_{3j-2}A_{3j-1}C_{3j} \quad \text{and} \quad y^{()} = \prod_{j=1}^{\frac{m}{3}} A_{3j-2}C_{3j-1}B_{3j}$$

are rigid. □

We suppose from now on that $r \equiv 0 \pmod 3$ (this is always satisfied up to replacing x by x^3). Let u be a minimal useful arrow for y (so implicitly we suppose that $SC(x)$ is not reduced to the single orbit O_y). It follows in particular from our proof of Lemma 5.7 that we can always find, up to cyclic permutation of the factors, an element z of O_{y^u} of the form

$$z = \prod_{j=1}^{\frac{m}{3}} C_{3j-2}B_{3j-1}A_{3j},$$

by making an appropriate choice of indices and powers inside the factors.

We can then rewrite y in the form

$$y = \prod_{\nu=1}^{\frac{m}{3}} ()^{a_\nu}()^{b_\nu}()^{c_\nu}()^{d_\nu}()^{e_\nu}()^{f_\nu}()^{g_\nu}()^{h_\nu}()^{i_\nu}()^{j_\nu}()^{k_\nu}()^{l_\nu},$$

with strictly positive integers $a_\nu, b_\nu, \ldots, l_\nu$ for all $\nu = 1, \ldots, \frac{m}{3}$, and then z becomes

$$z = \prod_{\nu=1}^{\frac{m}{3}} \Big[()^{a_\nu}()()^{b_\nu}()^{c_\nu-1}()^{d_\nu}()()^{e_\nu}()^{f_\nu-1}()^{g_\nu}()()^{h_\nu}()^{i_\nu-1}$$
$$()^{j_\nu}()()^{k_\nu}()^{l_\nu-1}\Big].$$

Lemma 5.8. *If the normal form of z contains a factor $()$ or $()$, then z admits a unique minimal useful arrow, i.e. the vertex O_z of the graph $\widetilde{SCG}(x)$ is a leaf.*

Proof. Up to cycling or conjugating by δ we can suppose that the last factor of z is $()$, and that $l_{\frac{m}{3}} > 1$. There are at most two minimal arrows for z, namely $()$ and $()$. A calculation of the normal form of $z()$ shows that $() \not\preccurlyeq z()$, which implies that $z^{()} \notin SSS(x)$, and hence the lemma.

In order to perform this calculation, we make three observations. Firstly,

$$()^{l_\nu-1}() = ()()()^{l_\nu-2}.$$

Secondly, for arbitrary integers $a, b > 0$,

$$\left(()^a()()^b\right)() = ()\left(()^a()()()^{b-1}\right)$$

and the first factor on the right hand side is independent of the powers a and b. Thirdly, the pair $()()$ is in normal form. Now the previous calculation can be pushed towards the left along the normal form of z, getting twisted by a conjugation by Δ at each step, until it hits, possibly, a factor () or (), where it gets stuck.

This shows that the multiplication of z by () on the right can only modify the beginning of the normal form of z if $()^{l\frac{m}{3}-1}$ is the only occurrence of () or () in z. Moreover, if this is the case, then the initial factor of $z()$ is () and () is not a prefix of the latter. On the other hand, by our hypothesis that O_z is distinct from O_y, there is a minimal arrow from z to some element of O_y. This completes the proof. □

Lemma 5.9. *Suppose that the normal form of z does not contain any factor () or (). Then*

(i) *the three strict prefixes of $\partial(\varphi(z))$ are minimal arrows for z,*
(ii) *if v is a minimal useful arrow for z conjugating z to another rigid braid whose normal form contains no factor () or (), then $z^v \in O_y$ and $v = ()$.*

Proof. According to our hypothesis, we can further rewrite the formulae from the proof of Lemma 5.7:

$$y = \prod_{\nu=1}^{\frac{m}{3}} ()^{a_\nu}()^{b_\nu}()()^{d_\nu}()^{e_\nu}()()^{g_\nu}()^{h_\nu}()()^{j_\nu}()^{k_\nu}()$$

and

$$z = \prod_{\nu=1}^{\frac{m}{3}} ()^{a_\nu}()()^{b_\nu}()^{d_\nu}()()^{e_\nu}()^{g_\nu}()()^{h_\nu}()^{j_\nu}()()^{k_\nu}.$$

(i) According to Lemma 5.7, z admits three minimal (not necessarily useful) arrows.

(ii) Let v be a minimal useful arrow for z such that z^v contains no factor () or (). First at least one such an arrow exists, because of our hypothesis that $O_y \neq O_z$. We know that $v \in \{(), (), ()\}$. Thus it is sufficient to prove that $v \neq ()$ and $v \neq ()$. We are going to apply the formulae from the proof of Lemma 5.7, now with z playing the rôle previously played by y.

If $v = ()$, then the formulae from the proof of Lemma 5.7, together with the restriction that z^v contains neither () nor (), imply the equalities $b_\nu = e_\nu = h_\nu = k_\nu = 1$. But then $z = z^{()}$, contradicting the usefulness of v. Thus $v \neq ()$.

Analogously, if $v = ()$, then due to the formulae from the proof of Lemma 5.7 we obtain $a_\nu = d_\nu = g_\nu = j_\nu = 1$. But then

$$z = \prod_{\nu=1}^{\frac{m}{3}} ()()()^{b_\nu}()()()^{e_\nu}()()()^{h_\nu}()()()^{k_\nu}$$

and

$$z^{()} = \prod_{\nu=1}^{\frac{m}{3}} ()()()()^{b_\nu}()()()^{e_\nu}()()()^{h_\nu}()()()^{k_{nu}-1}.$$

We obtain $\mathbf{c}(z^{()}) = \tau(z)$, contradicting the usefulness of v. Thus $v \neq ()$. □

Lemma 5.9 shows that the graph $\widetilde{SCG}(x)$ cannot contain a chain of 3 vertices whose elements contain no factor () or (). By Lemma 5.8 any vertex which does contain at least one factor () or (), but which is adjacent to a vertex which doesn't, is a leaf.

Since the graph $\widetilde{SCG}(x)$ is connected and all vertices have degree at most 3, this implies that it has at most 6 vertices. This completes the proof of Proposition 5.3.

5.3. **All elements of $SC(x)$ have at least one factor not belonging to $\mathcal{E}$.** In this subsection we suppose that all elements of $SC(x)$ have at least one factor in their normal form equal to $()$ ou $()$. According to Lemma 5.2, the graph $\widetilde{SCG}(x)$ is then a (possibly closed) line. In order to prove Theorem 1.2, we need to bound the length of this line. This task seems much more difficult than in the previous subsections and we have currently no elementary proof of Theorem 1.2 under the above hypotheses. In order to illustrate the difficulty, we show first that the quadratic bound of Theorem 1.2 is optimal. The following example was obtained with the help of the program GAP [25]:

Example 5.10. For all $k \in \mathbb{N}$, the braid $\beta_k = ()()()()()()^{3k}()^{-3k}$, whose normal form is

$$\beta_k = ()()()()()\,[()()()]^k$$

is rigid and pseudo-Anosov with $\ell(\beta_k) = 3k+5$. Moreover, the graph $\widetilde{SCG}(\beta_k)$ is a line with $3k+2$ vertices. (Explicitly, in order to obtain braids representing all vertices of $\widetilde{SCG}(\beta_k)$, it suffices to conjugate β_k by $()^j$, for $j = 0, \ldots, 3k+1$.) Thus $\#SC(\beta_k) = 4 \cdot (3k+2) \cdot (3k+5)$.

Our proof of Theorem 1.2 under the hypotheses of this subsection resorts to Masur-Minsky's linear bound on the length of an element conjugating two pseudo-Anosov elements of a mapping class group ([24], Theorem 7.2).

We consider the length function $|.|$ on B_4 induced by taking as generators of B_4 the set of divisors of δ, i.e. the set of BKL-simple braids (see Remark 2.3). The result of Masur and Minsky, applied to the case of 4-strand braids, then reads:

Theorem 5.11 ([8], Proposition 7)**.** *There exists a constant c such that for every pair (z_1, z_2) of conjugate pseudo-Anosov 4-strand braids, there exists a conjugating element w (i.e. $z_1^w = z_2$) such that $|w| \leqslant c \cdot (|z_1| + |z_2|)$.*

We remark that the length function used in the statement of ([8], Proposition 7) is the length associated to the alphabet of divisors of Δ, i.e. the set of simple braids in the *classical* Garside structure. However, the length functions associated to different finite generating sets in a group are in bi-Lipschitz correspondence. More explicitely, our two length functions on B_4 are related, with the obvious notations, by the formula:

$$|x|_{BKL_4} \leqslant 2 \cdot |x|_{\text{classical}} \leqslant 6 \cdot |x|_{BKL_4}.$$

In order to complete the proof of Theorem 1.2, it is now sufficient to prove the following result (where the constant c is the one promised by Theorem 5.11).

Proposition 5.12. *Let $x \in BKL_4$ be a rigid pseudo-Anosov braid. Suppose that all elements of $SC(x)$ have at least one factor of their normal form equal to $()$ or $()$. Then the graph $\widetilde{SCG}(x)$ has at most $16 \cdot c \cdot \ell(x)$ vertices. Thus, $\#SC(x) \leqslant 64 \cdot c \cdot \ell(x)^2$.*

Proof. First we can suppose that $|x| \leqslant 2 \cdot \ell(x)$. In order to see this, we notice that multiplying x by any power m of the central element δ^4 induces an isomorphism between the graphs $\widetilde{SCG}(x)$ and $\widetilde{SCG}(\delta^{4m}x)$. In this way, we can suppose that $\inf(x) \in \{-3,-2,-1,0\}$. Then from Remark 2.3 we obtain $|x| \leqslant 2 \cdot \ell(x)$ (recalling that $\ell(x) \geqslant 2$, since x is pseudo-Anosov).

According to Lemma 5.2, every vertex of the graph $\widetilde{SCG}(x)$ has degree at most 2, so topologically the graph is either a compact line segment or a circle. We claim that any two distinct vertices O_a, O_b in the graph $\widetilde{SCG}(x)$ can be connected in the graph by a path of length at most $8 \cdot c \cdot \ell(x)$. Before proving this claim, we observe that the claim, together with Lemma 4.6 (iv), implies Proposition 5.12 (the factor 2 comes from the possibility that the graph might form a circle).

So let O_a and O_b be two distinct vertices of $\widetilde{SCG}(x)$, and let z_a and z_b be representatives of these two orbits. Due to Theorem 5.11, there exists a braid w satisfying $z_a^w = b_b$, and such that $|w| \leqslant 2 \cdot c \cdot |x| \leqslant 4 \cdot c \cdot \ell(x)$. Up to changing the representative z_a we can suppose that $\inf(w) = 0$. Then $\lambda(w) \leqslant 2 \cdot |w|$, as every factor of the normal form of w contributes at most 2 to the weight of w. Thus w is the product of at most $2 \cdot |w|$ minimal arrows, which yields a path of length at most $2 \cdot |w|$ between O_a and O_b in the graph $\widetilde{SCG}(x)$. □

Question 5.13. Open question 2 in [2] concerns the existence of a polynomial bound in n and ℓ on the size of the set of Sliding Circuits of a rigid (pseudo-Anosov) braid with n strands and of canonical length at most ℓ. Prasolov gave a negative answer, by exhibiting a family of rigid pseudo-Anosov braids for which the size of the sets of Sliding Circuits grows exponentially as a function of n (for both structures, dual and classical). On the other hand, if we fix n then no such counter-example is known, and indeed in the special case $n = 4$ our Theorem 1.2 gives an affirmative answer. So we formulate the following question: for any fixed integer n, does there exist a polynomial P_n such that the cardinality of the (classical or dual) set of Sliding Circuits of a rigid pseudo-Anosov braid with n strands is bounded above by $P_n(\ell(x))$?

Question 5.14. Is the size of the (classical or dual) Super Summit Set of a rigid pseudo-Anosov 4-braid x bounded above by $P(\ell(x))$, for some polynomial P? We know from [10] that for braids with five or more strands, the size of the classical Super Summit Set can increase exponentially with the length of the braid.

References

[1] J. Birman, *Braids, Links and Mapping Class Groups*, Annals of Math. Studies 82, (1974).

[2] J. Birman,V. Gebhardt, J. González-Meneses, *Conjugacy in Garside Groups I: Cycling, Powers and Rigidity*, Groups Geom. Dyn. 1 (2007), no. 3, 221-279.

[3] J. Birman,V. Gebhardt, J. González-Meneses, *Conjugacy in Garside Groups II: Structure of the ultra summit set*, Groups Geom. Dyn. 2 (1), (2008), 16-31.

[4] J. Birman, V. Gebhardt, J. González-Meneses, *Conjugacy in Garside groups III: Periodic braids*, J. Algebra 316 (2), (2007), 746-776.

[5] J. Birman, K.-H. Ko, S.-J. Lee, *A new approach to the word and conjugacy problems in the braid groups*, Adv. Math. 139 (2) (1998), 322-353.

[6] 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.

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

[8] M. Calvez, *Fast Nielsen-Thurston classification of braids*, preprint arXiv:1112.0165v1, to appear in Algebraic and Geometric Topology.

[9] M. Calvez, B. Wiest, *Fast algorithmic Nielsen-Thurston classification of four-strand braids*, J. Knot Theory Ramifications, 21 (5), (2012).

[10] S. Caruso, *A family of pseudo-Anosov braids whose Super Summit Sets grow exponentially*, J. Knot Theory Ramifications, 22 (9), (2013).

[11] A. Casson, S. Bleiler, *Automorphisms of surfaces after Nielsen and Thurston*, LMS Student Texts, 9. Cambridge University Press, Cambridge, 1988.

[12] R. Charney, J. Meier, *The language of geodesics for Garside groups*, Math. Z. 248, no. 3 (2004), 495–509.

[13] P. Dehornoy, *Groupes de Garside*, Ann. Sci. École Norm. Sup. (4) 35 (2002), no. 2, 267-306.

[14] P. Dehornoy, I. Dynnikov, D. Rolfsen, B. Wiest, *Ordering Braids*, Providence, R.I.: American Mathematical Society, (2008).

[15] E. ElRifai, H. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford. Ser. (2) 45 (1994), no. 180, 479-497.

[16] A. Fathi, F. Laudenbach, V. Poenaru, *Travaux de Thurston sur les surfaces*, Astérisque 66-67, SMF 1991/1979.

[17] F. Garside, *The braid groups and other groups*, Quart. J. Math. Oxford Ser. (2) 20 (1969), 235-254.

[18] V. Gebhardt, *A new approach to the conjugacy problem in Garside groups*, J. Algebra 292 (2005), no. 1, 282-302.

[19] V. Gebhardt, J. González-Meneses, *The cyclic sliding operation in Garside groups*, Math. Z. 265 (1), (2010), 85-114.

[20] V. Gebhardt, J. González-Meneses, *Solving the conjugacy problem in Garside groups by cyclic sliding*, Journal of Symbolic Computation 45 (6) (2010), 629-656.

[21] J. González-Meneses, *The nth root of a braid is unique up to conjugacy*, Algebraic and Geometric Topology 3 (2003), 1103-1118.

[22] J. González-Meneses, B. Wiest, *Reducible braids and Garside theory*, Algebraic and Geometric Topology 11 (2011), 2971-3010.

[23] S. J. Lee, *Algorithmic solutions to decision problems in the braid groups*, PhD Thesis, Korea Advanced Institute of Science and Technology, 1999.

[24] H. Masur, Y. Minsky, *Geometry of the complex of curves. II. Hierarchical structure*, Geom. Funct. Anal. 10 (2000), no. 4, 902-974.

[25] M. Schönert et. al. GAP – Groups, Algorithms, and Programming – version 3 release 4 patchlevel 4. Lehrstuhl D für Mathematik, Rheinische Westfälische Technische Hochschule, Aachen, Germany, 1997, package CHEVIE.

Matthieu Calvez, Departamento de Matemática y Ciencia de la Computación, Facultad de Ciencias, Universidad de Santiago de Chile, Avenida Libertador Bernardo O'Higgins 3363, Santiago, Chile

Bert Wiest, IRMAR (UMR 6625 du CNRS), Université de Rennes 1, Campus de Beaulieu, 35042 Rennes Cedex, France

E-mail address: calvez.matthieu@gmail.com, bertold.wiest@univ-rennes1.fr