FAST NIELSEN-THURSTON CLASSIFICATION OF BRAIDS

MATTHIEU CALVEZ

Abstract. We prove the existence of an algorithm which solves the reducibility problem in braid groups and runs in quadratic time with respect to the braid length for any fixed braid index.

1. Introduction

One of the main algorithmic decision problems regarding braids (viewed as mapping classes of a punctured closed disk) is the problem to determine the Nielsen-Thurston type of a given braid: reducible, periodic or pseudo-Anosov [21],[13],[20]. This problem is called the *reducibility* problem because it amounts to determining whether a given non-periodic braid is reducible or not, i.e. whether it is reducible or pseudo-Anosov. Indeed, the case of periodic braids can be easily discarded: a braid x is periodic if and only if its nth power or its $(n-1)$st power is a power of the half-twist Δ (see [7]); and this is easy to decide algorithmically.

To solve the reducibility problem, two kinds of techniques have been used and several algorithms have been written; however none of them works in polynomial time with respect to the braid length for the general braid group B_n.

Firstly, the Bestvina-Handel algorithm [3] uses the theory of train-tracks and it is valid for any mapping class group. Although this algorithm works fast in practice, its theoretical complexity remains unknown.

Secondly, following the ideas introduced by Benardete, Gutierrez and Nitecki [1, 2], connections between the reducibility problem and the Garside structures of braid groups have been used for detecting reducibility [1, 2, 28, 27, 12, 10]. Our work fits in this approach and builds mainly on the last algorithm by González-Meneses and Wiest [27].

However Garside tools are not the only ones needed in the paper: we bring into play a very deep property of Mapping Class Groups: the so-called *linearly bounded conjugator property* [29, 31], see Theorem 16. At this point we already warn the reader that the algorithm given in the paper is not well-defined (although it will be actually described) because it rests on the above linear bound, which is not explicitly known. Therefore our main result is an existence result only.

The latter can be stated as follows. For a braid x, let us denote by $|x|$ the minimal possible length of a word representing x whose letters are positive permutation

2010 *Mathematics Subject Classification.* 20F36, 20F10, 20F65.

The author was partially supported by a grant from Région Bretagne, by MTM2010-19355 and FEDER, and by FONDECYT through postdoctoral grant no. 3130569.

braids and their inverses (in other words, the letters are braids in which any pair of strands crosses at most once and all crossings have the same orientation).

We will prove:

Theorem 1. *Let n be a positive integer. There exists an algorithm which decides the Nielsen-Thurston type of any given braid x with n strands and runs in time $O(|x|^2)$.*

The paper is organized as follows. In Section 2 we recall useful tools from Garside theory and give precise statements relating the latter and the reducibility problem; an actual description of the algorithm whose existence is stated in Theorem 1 is also given. The detailed proofs are deferred to Section 3.

2. The reducibility problem and Garside theory

2.1. **Reminders on Garside theory.** We first recall some basic notions of Garside theory in the specific case of braid groups, with emphasis on the *classical* structure; references are [22, 18, 19]. The reader is referred to [17, 15, 16] for a general account on Garside groups.

The *classical Garside structure* of the braid group consists in the following 2-fold data: B_n^+ is the monoid whose elements are braids which can be expressed as words on the Artin generators σ_i with only positive exponents and Δ is the so-called *Garside element* or half-twist.

The relation $\preccurlyeq$ on B_n defined by $x \preccurlyeq y$ if and only if $x^{-1}y \in B_n^+$ defines a partial order called *prefix order*, which turns out to be a lattice order. We will denote by τ the inner automorphism associated to Δ: this is an involution which for each i, maps σ_i to σ_{n-i}; actually the center of B_n ($n \geqslant 3$) is the cyclic group generated by Δ^2. It can be shown that for any braid x, there exist relative integers r, s such that $\Delta^r \preccurlyeq x \preccurlyeq \Delta^s$. This allows to define the so-called *infimum* and *supremum* of x, respectively:

$$\inf(x) = \max\{r \in \mathbb{Z} | \Delta^r \preccurlyeq x\}, \qquad \sup(x) = \min\{s \in \mathbb{Z} | x \preccurlyeq \Delta^s\}.$$

The *canonical length* of x is defined by $\ell(x) = \sup(x) - \inf(x)$.

A central property of Garside groups is the existence of a distinguished generating set allowing for the definition of normal forms. Consider the set of positive prefixes of Δ; these elements are called *simple elements* or *positive permutation braids* (because they are in one-to-one correspondence with the elements of the symmetric group on n objects). Geometrically, simple elements are positive braids in which every pair of strands crosses at most once. Because it contains all Artin's generators σ_i, the set of simple elements generates B_n.

Definition 2. *A pair (s_1, s_2) of simple elements is said to be* left-weighted *if for any non-trivial positive prefix t of s_2, the product $s_1 t$ is not a simple element.*

This allows to state:

Proposition 3. [18] *Let $x \in B_n$. There exists a unique decomposition $x = \Delta^p x_1 \dots x_r$, where $p = \inf(x)$, the x_i are simple elements with $x_r \neq 1$ and (if*

$r \geqslant 2$) the pair $x_i x_{i+1}$ is left-weighted for $i = 1, \ldots, r-1$. We have $\sup(x) = p + r$ *and* $\ell(x) = r$.

Recall the braid length $|\cdot|$ defined in the introduction. It can be shown [19] that every braid admits a unique decomposition of the form $a^{-1}b$, where a, b are positive braids having no common non-trivial positive prefix. This is called the *mixed canonical form*. Moreover, if $a = a_1 \ldots a_k$ and $b = b_1 \ldots b_l$ are the left normal forms of a and b respectively, it is shown in [14] that the word $a_k^{-1} \ldots a_1^{-1} b_1 \ldots b_l$ is a geodesic in the Cayley graph of B_n with respect to the set of simple elements. Hence the braid length $|\cdot|$ is given by the length of the mixed canonical form. Finally notice that the latter is related to the canonical length in the following way: if $x = \Delta^p x_1 \ldots x_r$ is the left normal form of $x \in B_n$, we have $|x| = \max(|p|, r, p + r)$ and $\ell(x) \leqslant |x|$.

Although we do not need that, it is worth mentionning that the braid group admits another Garside structure, called the *dual Garside structure*, see [8].

The existence of normal forms for braids allows to construct algorithms for solving the conjugacy problem in the braid groups, that is for deciding whether any two given braids are conjugate and finding a conjugator whenever there exists one [22, 18, 23, 24, 25]. We now recall some related notions.

All existing algorithms for solving the conjugacy problem in braid groups rely on the definition of a particular finite computable characteristic subset of each conjugacy class in B_n, consisting of its "simplest" elements (in some sense). A first example of such a characteristic subset is given by the following:

Proposition-Definition 4. [18] *Let $x \in B_n$. The subset of the conjugacy class of x consisting of all elements with minimal canonical length is finite (and non-empty). Its elements have simultaneously maximal infimum and minimal supremum within the conjugacy class of x. This set is called the Super Summit Set of x and is denoted by $SSS(x)$.*

An element in the Super Summit Set of a given braid can be computed using a special kind of conjugation called *cyclic sliding*:

Definition 5. [24] *Let $x = \Delta^p x_1 \ldots x_r$ be the normal form of $x \in B_n$. Suppose that $r > 0$. The* preferred prefix *of x is the maximal positive prefix t of $\tau^{-p}(x_1)$ such that $x_r t$ is a simple element; it is denoted by $\mathfrak{p}(x)$. If $r = 0$, that is if x is a power of Δ, $\mathfrak{p}(x)$ is just defined to be the trivial braid. The result of the conjugation of x by its preferred prefix $\mathfrak{p}(x)$ is called* cyclic sliding *of x and denoted by $\mathfrak{s}(x)$.*

The cyclic sliding operation actually achieves computing elements in Super Summit Sets, in an effective way. Indeed, only a polynomial (with respect to both length and braid index) number of iterations of $\mathfrak{s}$ is required to compute an element in the Super Summit Set:

Theorem 6. [9, 24] *Let $x \in B_n$. The following alternative holds: $\ell(\mathfrak{s}^{\frac{n(n-1)}{2}-1}(x)) < \ell(x)$ or $x \in SSS(x)$.*

Another (smaller) example of conjugacy invariant subset was defined later by Gebhardt and González-Meneses:

Proposition-Definition 7. [24] *Let $x \in B_n$. The subset of the conjugacy class of x consisting of all elements which are periodic points under the cyclic sliding operation is finite and non-empty. It is a subset of the Super Summit Set of x, called set of Sliding Circuits of x and denoted by $SC(x)$.*

Iterative application of the cyclic sliding operation to a braid x eventually reaches an element of $SC(x)$; however by contrast with the case of $SSS(x)$, no general bound on the number of repetitions involved is known (see Conjecture 11).

To conclude this paragraph, we recall the important notion of *rigid* braid:

Definition 8. [24] *A braid x is said to be* rigid *if its preferred prefix is trivial.*

In particular a rigid braid is a fixed point of $\mathfrak{s}$ and is an element of its own set of Sliding Circuits. Moreover, if a conjugacy class contains one rigid braid, then the corresponding set of Sliding Circuits consists only of rigid braids [24].

2.2. **Previous works.** We now turn to the relations between the reducibility problem and the notions above. First of all, we recall some definitions and properties related to reducible braids.

Let $\mathbb{D}_n$ be the closed disk in $\mathbb{C}$ with diameter $[0, n+1]$ and with the points $\{1, \dots, n\}$ removed. As the Mapping Class Group of $\mathbb{D}_n$, the braid group B_n induces a (right)-action on the set of isotopy classes of simple closed curves in $\mathbb{D}_n$. A curve is said to be *non-degenerate* if it is not contractible and surrounds more than one and less than n punctures. By the word "curve" alone we will mean the isotopy class of a non-degenerate simple closed curve.

A braid x is *reducible* if it preserves setwise a family of curves; such a curve is then said to be a *reducing* curve for x. Notice that reducibility is a conjugacy-invariant property. Moreover a reducible braid x is not periodic if the set of its *essential* reducing curves, that is reducing curves which do not intersect any other reducing curve, is not empty. An important matter when we want to detect the reducibility of a braid is to actually detect reducing curves whenever they exist. This leads to formulate:

Definition 9. [2, 27] *A curve $\mathcal{C}$ in $\mathbb{D}_n$ is said to be* round *if it is isotopic to a geometric circle in $\mathbb{D}_n$. A curve $\mathcal{C}$ in $\mathbb{D}_n$ is said to be* almost round *if it has a unique maximum and a unique minimum in the horizontal direction. The latter is equivalent to saying that $\mathcal{C}$ can be transformed into a round curve by the action of a simple element.*

Whenever a reducible braid preserves a family of round curves, the reducibility is easy to detect (there are only $\frac{n(n-1)}{2}$ round curves), see [1]. Moreover the notion of roundness of a curve behaves well with respect to Garside-theoretic operations:

Theorem 10. [2, 26] *Let $x \in B_n$ be a reducible braid preserving a family of round curves. Then so does $\mathfrak{s}(x)$.*

Notice that any family of curves can be transformed into a family of round curves under the action of some braid, in other word a reducible braid always preserves a family of round curves up to conjugacy. It follows from Theorems 6 and 10 that for any reducible braid x, there exists some element of $SSS(x)$ that preserves a family of round curves.

Therefore computing the whole Super Summit Set of a braid gives a manner of testing its reducibility: x is reducible if and only if some element in $SSS(x)$ preserves a family of round curves. We remark that the same approach can be carried out in the framework of the dual Garside structure, replacing round curves by *standard* curves (see [10]). However in either structure, the resulting algorithm is far from polynomial because the Super Summit Sets are exponentially large in general, with respect to both length and braid index [26, 30].

In the special case of the four-strand braid group B_4, it is possible to overcome the latter difficulty, showing that *every* element of the (classical) super summit set of a given reducible 4-braid with a reducing curve surrounding three punctures preserves a round or an almost-round curve. This leads to a polynomial-time algorithm for solving the reducibility problem in B_4, described in [12].

In [28], Lee and Lee replaced the condition about *some* element of the *super* summit set of a reducible braid x by the condition that *every* element of the *ultra* summit set of x (which is another conjugacy invariant subset introduced in [23]) preserves a family of round curves. However this was shown at the cost of a technical hypothesis about the external and internal components of x.

In [27], González-Meneses and Wiest showed that every element of (some refined version of) the set of Sliding Circuits of a reducible braid preserves a family of round or almost-round curves.

Both approaches from [28] and [27] suffer the same drawback, namely the lack of control on the distance to the first repetition when applying iteratively the cyclic sliding operation. The algorithm in [27] indeed solves the reducibility problem in arbitrary braid groups with polynomial complexity, both in braid length and braid index, provided the following conjecture holds:

Conjecture 11. ([27], Conjecture 3.5) *Let $x \in B_n$, with canonical length r. Let t be the minimal positive integer such that $\mathfrak{s}^k(x) = \mathfrak{s}^t(x)$ for some k with $0 \leqslant k < t$. Then t is bounded by a polynomial in r and n.*

2.3. **Our algorithm.** One of the keys for proving Theorem 1 will be a partial demonstration of Conjecture 11. We shall prove, using Masur-Minsky's linear bound:

Theorem 12. *There exists a constant $C(n)$ (depending only on n) such that for any pseudo-Anosov n-strand braid $x \in SSS(x)$, the following holds: x has a rigid conjugate if and only if $\mathfrak{s}^{C(n)\cdot|x|}(x)$ is rigid.*

Theorem 12 gives a partial solution to Conjecture 11: in the pseudo-Anosov rigid case, starting from a super summit element, Theorem 12 guarantees that a rigid conjugate (or equivalently an element of the set of Sliding Circuits) is found after only $C(n) \cdot |x|$ iterations of cyclic sliding (in other words, if a pseudo-Anosov super summit braid has rigid conjugates, then the cyclic sliding operation converges towards one of them in linear time with respect to braid length). This gives in this particular case (with the notation of Conjecture 11) the bound $t \leqslant C(n)r + 1$.

The importance of the rigid case comes from the following result, which will play a crucial role in our proof of Theorem 1. It is due to Birman, Gebhardt and González-Meneses:

Theorem 13. [5]. *Let $x \in B_n$ be a pseudo-Anosov braid. There exists a positive integer $m < (\frac{n(n-1)}{2})^3$ such that x^m is conjugate to a rigid braid.*

Finally we recall the two following results from [27]:

Theorem 14. ([27], Theorem 5.16). *Let $x \in B_n$ be a non-periodic, reducible braid which is rigid. Then some essential reducing curve of x is round or almost-round. More precisely, there is some positive integer $k \leqslant n$ such that one of the following holds:*

(1) *x^k preserves a round essential curve,*
(2) *$\inf(x^k)$ and $\sup(x^k)$ are even and either $\Delta^{-\inf(x^k)}x^k$ or $x^{-k}\Delta^{\sup(x^k)}$ is a positive braid preserving an almost-round essential reducing curve whose interior strands do not cross.*

Theorem 15. ([27], Theorem 2.9). *There is an algorithm which decides whether a given positive braid x preserves an almost-round curve whose interior strands do not cross. Its complexity is $O(\ell(x)n^4)$.*

We are now ready to describe the algorithm promised in Theorem 1. It takes as input an n-braid x. The output is “periodic”, “reducible” or “pseudo-Anosov”.

1. If x^{n-1} or x^n is a power of Δ, return “periodic” and stop.
2. For $i = 1, \dots, (\frac{n(n-1)}{2})^3 - 1$ compute the normal form of x^i. Iteratively apply cyclic sliding to x^i until the canonical length has not decreased during the $\frac{n(n-1)}{2} - 1$ last iterations. This computes $y_i \in SSS(x^i)$. Then compute $z_i = \mathfrak{s}^{C(n)\cdot|y_i|}(y_i)$. If none of the braids z_i is rigid return “reducible” and stop. Else let j be such that z_j is rigid.
3. For $k = 1, \dots, n$, apply the algorithm in [1] to the braid z_j^k to test whether it preserves a round curve; apply the algorithm in Theorem 15 to both braids $\Delta^{-\inf(z_j^k)}z_j^k$ and $z_j^{-k}\Delta^{\sup(z_j^k)}$. If a round or an almost-round reducing curve is found, then return “reducible” and stop.
4. Return “pseudo-Anosov”.

As mentioned above, we remark that this algorithm, and specifically Step 2, is not well-defined because the constant $C(n)$ is not explicitly known. In the next section, we will prove Theorem 12, show the correctness of the above algorithm and study its complexity.

3. Proofs of our results

In order to prove Theorem 12, we combine two important results. The first one is the already mentionned linearly bounded conjugator property for Mapping Class Groups [29]. Although the range of surfaces considered by Masur and Minsky is much broader, only the $(n+1)$-times punctured sphere $\mathbb{S}_{n+1}$ ($n \geqslant 3$) is relevant for our purposes, so we state their result in this special case:

Theorem 16. ([29], Theorem 7.2). *Let $\mathcal{G}$ be any generating set of the Maping Class Group $\mathcal{MCG}(\mathbb{S}_{n+1})$. There exists a constant $\gamma(\mathcal{G})$, depending only on $\mathcal{G}$, such that any pair of conjugate pseudo-Anosov mapping classes can be related by a conjugating element w satisfying*

$$|w|_{\mathcal{G}} \leqslant \gamma(\mathcal{G})(|x|_{\mathcal{G}} + |y|_{\mathcal{G}}),$$

(where $|\cdot|_{\mathcal{G}}$ denotes the word length with respect to the chosen generating set $\mathcal{G}$).

We aim at an analogous result for braids, namely we want to show:

Proposition 17. *There exists a constant $c(n)$, depending only on n, such that any pair of conjugate pseudo-Anosov n-braids can be related by a conjugating element w satisfying*

$$|w| \leqslant c(n)(|x| + |y|).$$

Before proving Proposition 17, we recall that the quotient $B_n/\left\langle\Delta^2\right\rangle$ can be seen as the Mapping Class Group of an n-times punctured closed disk (with boundary fixed setwise). For a braid x in B_n, denote by $\hat{x}$ its image in the quotient $B_n/\left\langle\Delta^2\right\rangle$. Simple elements are sent bijectively to a generating set of the quotient (whose elements we still call simple); this defines a length $||\cdot||$ on $B_n/\left\langle\Delta^2\right\rangle$ (notice that for any braid x, $||\hat{x}|| \leqslant |x|$). Collapsing the boundary of the n-times punctured closed disk to a puncture in the sphere $\mathbb{S}_{n+1}$ (where the punctures are uniformly placed along the horizontal great circle), we can view $B_n/\left\langle\Delta^2\right\rangle$ as the finite index subgroup of $\mathcal{MCG}(\mathbb{S}_{n+1})$ consisting of the mapping classes which fix the $(n+1)$st puncture. The group $\mathcal{MCG}(\mathbb{S}_{n+1})$ is equipped with the generating set consisting of the simple elements in the quotient $B_n/\left\langle\Delta^2\right\rangle$ together with a clockwise rotation by an angle of $\frac{2\pi}{n+1}$, which we denote by ρ. Notice that for any $u \in B_n/\left\langle\Delta^2\right\rangle$, we have $|u|_{\mathcal{G}_n} \leqslant ||u||$. Conversely, we will see in a simple computational way that the length $||u||$ is linearly bounded in terms of $|u|_{\mathcal{G}_n}$:

Lemma 18. *For any $u \in B_n/\left\langle\Delta^2\right\rangle$, we have $||u|| \leqslant \frac{n(n-1)}{2}|u|_{\mathcal{G}_n}$.*

Proof. Let $u \in B_n/\left\langle\Delta^2\right\rangle$. We will construct a word representative W of u using only the letters $\hat{\sigma}_1^{\pm 1}, \ldots, \hat{\sigma}_{n-1}^{\pm 1}$ such that $||W|| \leqslant \frac{n(n-1)}{2}|u|_{\mathcal{G}_n}$. This is achieved thanks to the following relations in $\mathcal{MCG}(\mathbb{S}_{n+1})$ (which can be easily deduced from the presentation in [4] Theorem 4.5). For $1 \leqslant i \leqslant n-1$, $0 \leqslant j \leqslant n$:

$$\hat{\sigma}_i\rho^j = \rho^j\hat{\sigma}_{i-j \pmod{n+1}}, \quad i-j \neq 0, n \pmod{n+1} \tag{1}$$

$$\hat{\sigma}_i\rho^i = \rho^{i+1}(\hat{\sigma}_1 \ldots \hat{\sigma}_{n-1})^{-1}, \tag{2}$$

$$\hat{\sigma}_i\rho^{i+1} = \rho^i(\hat{\sigma}_{n-1} \ldots \hat{\sigma}_1)^{-1}. \tag{3}$$

This allows to gather (at the beginning) all powers of ρ appearing in a shortest representative for u on the alphabet $\mathcal{G}_n$; this results in a power of ρ^{n+1} (because $u \in B_n/\left\langle\Delta^2\right\rangle$) followed by a word W in $\hat{\sigma}_1^{\pm 1}, \ldots, \hat{\sigma}_{n-1}^{\pm 1}$. The word W represents u and as a word on the simple elements and their inverses, its length is bounded by $\frac{n(n-1)}{2}|u|_{\mathcal{G}_n}$ (because each simple element can be written with at most $\frac{n(n-1)}{2}$ letters $\hat{\sigma}_i$ so that the above relations are used at most $\frac{n(n-1)}{2}|u|_{\mathcal{G}_n}$ times; and because both $\hat{\sigma}_1 \ldots \hat{\sigma}_{n-1}$ and $\hat{\sigma}_{n-1} \ldots \hat{\sigma}_1$ are simple). $\square$

Proof of Proposition 17. Given a pair of conjugate pseudo-Anosov n-braids x and y, we know a conjugating element between $\hat{x}$ and $\hat{y}$, say υ in the quotient $B_n/\langle\Delta^2\rangle$. In their proof of Theorem 16, Masur and Minsky construct a "short" conjugating element υ' between $\hat{x}$ and $\hat{y}$; this element υ' is expressed as a product $\hat{x}^m\upsilon$, for some integer m and therefore it belongs to the subgroup $B_n/\langle\Delta^2\rangle$ of $\mathcal{MCG}(\mathbb{S}_{n+1})$. Moreover,

$$|\upsilon'|_{\mathcal{G}_n} \leqslant \gamma(\mathcal{G}_n)(|\hat{x}|_{\mathcal{G}_n} + |\hat{y}|_{\mathcal{G}_n}) \leqslant \gamma(\mathcal{G}_n)(||\hat{x}|| + ||\hat{y}||)$$

and we get from Lemma 18

$$||\upsilon'|| \leqslant \frac{n(n-1)}{2}\gamma(\mathcal{G}_n)(||\hat{x}|| + ||\hat{y}||).$$

Finally, as $\langle\Delta^2\rangle$ is the center of B_n, and because a braid x conjugate to y cannot be conjugate to $\Delta^{2k}y$ for $k \neq 0$, any lifting of υ' in B_n conjugates x to y and we can choose one, say w, so that $|w| = ||\upsilon'||$. Therefore, taking $c(n) = \frac{n(n-1)}{2}\gamma(\mathcal{G}_n)$ achieves the proof of Proposition 17. □

The second step towards Theorem 12 is a general fact about Garside groups. It explains that if a super summit element has a rigid conjugate, then iterated cyclic sliding is the shortest way of obtaining such a rigid conjugate.

Theorem 19. [24]. *Let $x \in B_n$ and assume that x is conjugate to a rigid braid.*

(1) *There exists a unique positive braid $f(x)$ such that $f(x)^{-1}xf(x)$ is rigid and $f(x) \preccurlyeq g$ for any positive braid g such that $g^{-1}xg$ is rigid.*
(2) *If $y \in SSS(x)$, then (unless y is already rigid) there exists some positive integer k such that $f(y) = \prod_{i=1}^{k} \mathfrak{p}(\mathfrak{s}^{i-1}(y))$. That is, $f(y)$ is the product of the k conjugating simple elements involved when applying k iterations of cyclic sliding to y.*

Now, the proof of Theorem 12 is just a combination of both of the previous results.

Proof of Theorem 12. Let x be a pseudo-Anosov n-strand braid such that $x \in SSS(x)$. Let us assume that x has a rigid conjugate z. By Proposition 17, there exists $w \in B_n$ such that $z = w^{-1}xw$ and $|w| \leqslant c(n)(|x| + |z|)$. Since $x, z \in SSS(x)$, we have $|x| = |z|$. Let r be the number of negative factors in the mixed canonical form of w. If r is even, then $w' = \Delta^r w$ is a positive braid conjugating x to z (recall that Δ^2 is central). Otherwise r is odd and $w' = \Delta^{r+1}w$ does the same job. In either case, we get a positive braid w' conjugating x to z with $|w'| \leqslant |w|+1 \leqslant (2c(n)+1)|x|$ (we may assume that $|x| \geqslant 1$).

Let k and $f(x) = \prod_{i=1}^{k} \mathfrak{p}(\mathfrak{s}^{i-1}(x))$ be as in Theorem 19. Then $f(x) \preccurlyeq w'$. It follows that $|f(x)| \leqslant |w'|$. As the braid $f(x)$ is a product of k simple elements, we have $k \leqslant \frac{n(n-1)}{2}|f(x)|$ (because a simple element can be written with at most $\frac{n(n-1)}{2}$ letters σ_i) so that finally $k \leqslant \frac{n(n-1)}{2}\cdot(2c(n)+1)|x|$. Thus taking $C(n) = \frac{n(n-1)}{2}\cdot(2c(n)+1)$ (which depends only on n), we have shown the following: x has a rigid conjugate if and only if $\mathfrak{s}^{C(n)\cdot|x|}(x)$ is a rigid braid (notice that $\mathfrak{s}^m(z) = z$ for any rigid braid z and any integer $m \in \mathbb{N}$). □

We notice that Theorem 12 can be shown as well in the dual setting but we will not need this. We now turn to the proof of Theorem 1, showing the correctness of the algorithm in Section 2 and studying the complexity of each step.

Proof of Theorem 1. The correctness of Step 1 is shown in [7]. This step just consists in a computation of left normal form; therefore it takes time $O(\ell(x)^2)$ for any fixed n, according to [19].

Let us prove that Step 2 is correct. First, by Theorem 6, the braid y_i is an element of $SSS(x^i)$ for each i. Then if x is a pseudo-Anosov braid, by Theorem 13, at least one of the braids x^i (and therefore y_i) is pseudo-Anosov with a rigid conjugate and by Theorem 12 at least one of the braids z_i is rigid.

Let us calculate the complexity of Step 2. The computations of normal forms are known to be quadratic with respect to the length [19]. We then recall that each instance of cyclic sliding (when applied to a braid already in normal form) has linear complexity with respect to the braid length for any given braid index (see [25], Theorem 4.4). Therefore for any $i = 1, \dots, (\frac{n(n-1)}{2})^3 - 1$, the complexity of computing y_i (which requires at most $(\ell(x^i) - 1) \cdot (\frac{n(n-1)}{2} - 1)$ iterations of cyclic sliding) is quadratic with respect to the braid length whenever n is fixed. The same is true for the computation of z_i from y_i which requires $C(n)|y_i| \leqslant C(n)i|x|$ iterations of cyclic sliding.

The validity of Step 3 follows from Theorem 14. This step consists in applying the algorithm in [1] to at most n braids of length at most $nj|x|$ and the algorithm of Theorem 15 to at most $2n$ braids of length at most $nj|x|$. Both of these algorithms work in linear time with respect to the length so that Step 3 is linear with respect to $|x|$. □

We notice that the present algorithm does not always yield the knowledge of reducing curves for reducible elements (actually this failure happens when reducibility is detected at Step 2). Thus, in view of the program in [5], [6], [7], writing an algorithm for solving the conjugacy problem in braid groups in polynomial time still requires the following:

(i) find explicitly the constant $C(n)$ to make the algorithm in Theorem 1 explicit. This amounts to bounding explicitly the required number of cyclic slidings to obtain (if it exists) a rigid conjugate from a pseudo-Anosov super summit element (see Theorem 12); alternatively this rests on the knowledge of an explicit value for Masur-Minsky's constant $c(n)$ (see Proposition 17),

(ii) find reducing curves of a braid, in polynomial time, whenever the braid is known to be reducible,

(iii) find a polynomial bound on the number of rigid braids in a given pseudo-Anosov conjugacy class.

We finish with a discussion of the special case of the four-strand braid group B_4. If we want to decide the Nielsen-Thurston type of a given 4-braid, the algorithm in [12] should rather be used instead of the present one because it is implementable and it finds explicitly the reducing curves whenever they exist (in polynomial time). Using the Birman-Ko-Lee structure of B_4, the author together with Bert Wiest show in [11] the existence of a bound as in (iii) (which depends on Masur-Minsky's constant $c(4)$, see Proposition 17). Unfortunately, they do not know yet how to make explicit the constant $c(4)$ (nor $C(4)$), so that the cardinality of the ultra summit set of a pseudo-Anosov rigid 4-braid is not explicitly known. Nevertheless [11] presents a polynomial-time algorithm for solving the conjugacy problem in B_4.

Acknowledgements. The author thanks Jin Tao for her help with Proposition 17 and Juan González-Meneses for useful comments on an earlier version of that work. His gratefulness also goes to Bert Wiest for many inspiring discussions and careful readings of the manuscript.

References

[1] D. Benardete, M. Gutierrez, Z. Nitecki, *A combinatorial approach to reducibility of mapping classes*, Mapping Class Groups and moduli spaces of Riemann surfaces (Göttingen, 1991/Seattle, WA, 1991), 1-31, Contemp. Math., 150, Amer. Math. Soc., Providence, RI, 1993.
[2] D. Benardete, M. Gutierrez, Z. Nitecki, *Braids and the Nielsen-Thurston classification*, J. Knot Theory Ramifications, 4 (1995), 549-618.
[3] M. Bestvina, M. Handel, *Train-tracks for surface homeomorphisms*, Topology 34 (1995), no. 1, 109-140.
[4] J. Birman, *Braids, Links and Mapping Class Groups*, Annals of Math. Studies 82, (1974).
[5] 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.
[6] 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.
[7] J. Birman, V. Gebhardt, J. González-Meneses, *Conjugacy in Garside groups III: Periodic braids*, J. Algebra 316 (2), (2007), 746-776.
[8] 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.
[9] 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.
[10] M. Calvez, *Dual Garside structure and reducibility of braids*, J. Algebra 356 (1), (2012), 355-373.
[11] M. Calvez, B. Wiest, *The conjugacy problem in the four-strand braid group*, arXiv:1204.6507.
[12] M. Calvez, B. Wiest, *Fast algorithmic Nielsen-Thurston classification of four-strand braids*, J. Knot Theory Ramifications, 21 (5), (2012).
[13] A. Casson, S. Bleiler, *Automorphisms of surfaces after Nielsen and Thurston*, LMS Student Texts, 9. Cambridge University Press, Cambridge, 1988.
[14] R. Charney, *Geodesic automation and growth functions for Artin groups of finite type*, Math. Ann. 301 no.2, (1995), 307-324.
[15] P. Dehornoy, *Groupes de Garside*, Ann. Sci. École Norm. Sup. (4) 35 (2002), no. 2, 267-306.
[16] P. Dehornoy, F. Digne, E. Godelle, D. Krammer, J. Michel, *Foundations of Garside Theory*, in progress.
[17] P.Dehornoy, L. Paris, *Gaussian groups and Garside groups, two generalizations of Artin groups*, Proc. London Math. Soc. 79 (3), (1999), 569-604.
[18] E. ElRifai, H. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford. Ser. (2) 45 (1994), no. 180, 479-497.
[19] D. B. A. Epstein, J. Cannon, D. Holt, S. Levy, M. Paterson, W. Thurston, *Word processing in groups*, Jones and Bartlett Publishers, Boston, MA, 1992.
[20] B. Farb, D. Margalit, *A primer on Mapping Class Groups*, Princeton Mathematical Series, 2011.
[21] A. Fathi, F. Laudenbach, V. Poenaru, *Travaux de Thurston sur les surfaces*, Astérisque 66-67, SMF 1991/1979.
[22] F. Garside, *The braid groups and other groups*, Quart. J. Math. Oxford Ser. (2) 20 (1969), 235-254.
[23] V. Gebhardt, *A new approach to the conjugacy problem in Garside groups*, J. Algebra 292 (1), (2005), 282-302.
[24] V. Gebhardt, J. González-Meneses, *The cyclic sliding operation in Garside groups*, Math. Z. 265 (1), (2010), 85-114.
[25] V. Gebhardt, J. González-Meneses, *Solving the conjugacy problem in Garside groups by cyclic sliding*, Journal of Symbolic Computation 45 (6) (2010), 629-656.
[26] J. González-Meneses, *On reduction curves and Garside properties of braids*, Contemp. Math. 538 (2011), 227-244.

[27] J. González-Meneses, B. Wiest, *Reducible braids and Garside theory*, Algebraic and Geometric Topology 11 (2011), 2971-3010.
[28] E.-K. Lee, S.-J. Lee, *A Garside-theoretic approach to the reducibility problem in braid groups*, J. Algebra 320 (2008), no. 2, 783-820.
[29] H. Masur, Y. Minsky, *Geometry of the complex of curves. II. Hierarchical structure*, Geom. Funct. Anal. 10 (2000), no. 4, 902-974.
[30] M.V. Prasolov, *Small braids with large ultra summit set*, Mat. Zametki 89 (4) (2011), 577-588.
[31] J. Tao, *Linearly Bounded Conjugator Property for Mapping Class Groups*, Geom. Funct. Anal. 23 (2013), no. 1, 415-466.

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

E-mail address: calvez.matthieu@gmail.com