ISSN 1472-2739 (on-line) 1472-2747 (printed)

Algebraic & Geometric Topology
Volume 3 (2003) 1103–1118
Published: 1 November 2003

ATG

The nth root of a braid is unique up to conjugacy

Juan González-Meneses

Abstract We prove a conjecture due to Makanin: if α and β are elements of the Artin braid group B_n such that $\alpha^k = \beta^k$ for some nonzero integer k, then α and β are conjugate. The proof involves the Nielsen-Thurston classification of braids.

AMS Classification 20F36; 20F65.

Keywords Braid, root, conjugacy, Nielsen-Thurston theory.

1 Introduction

The Artin braid group on n strands, B_n, is the group of automorphism of the n-punctured disc that fix the boundary pointwise, up to isotopies relative to the boundary. One can also consider the elements of B_n (*braids*) as isotopy classes of loops in the space of configurations of n points in a disc D. That is, a braid is represented by the disjoint movements of n points in the disc, starting and ending with the same configuration, maybe permuting their positions. Braids can also be represented in a three dimensional picture: if we consider the cylinder $D \times [0,1]$, and fix n base points $P_1, \ldots, P_n$ in D, the movement of the point P_i is represented by a path, called ith *strand*, going from $P_i \times \{0\}$ to some $P_j \times \{1\}$. The n strands of a braid are always disjoint, and isotopies correspond to deformations of the strands, keeping the endpoints fixed.

The braid group B_n is of interest in several fields of mathematics, with important applications to low dimensional topology, knot theory, algebraic geometry or cryptography. Among the basic results concerning braid groups, one can find the presentation, in terms of generators and relations, given by Artin [1]

$$B_n = \left\langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & (|i-j| \geq 2) \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} & (1 \leq i \leq n-2) \end{array} \right\rangle ;$$

and the solutions to the word problem [11, 20, 3] and the conjugacy problem [7, 3, 9]. Closely related to the latter is the problem of determining the centralizer of a given braid [15, 10, 12]. It is in the context of these two problems (conjugacy problem and computation of centralizers) that extraction of roots in braid groups becomes interesting (see Corollary 1.2 in this paper, and the last section of [12]).

Remark We read the product of two braids $\alpha\beta$ from left to right, as is usually done in braid theory. That is, if we consider α and β as automorphisms of the disc D, then $\alpha\beta(D) = \beta(\alpha(D))$.

Given a braid $\beta \in B_n$ and an integer k, the problem to determine if there exists $\alpha \in B_n$ such that $\alpha^k = \beta$ has been solved in [18] (see also [17]). But it is known that such an α is not necessarily unique. For instance $(\sigma_1\sigma_2)^3 = (\sigma_2\sigma_1)^3$ but $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$. G. S. Makanin (see [16], problem B11) conjectured that any two solutions of the above equation are conjugate, and in this paper we will show that it is true. In other words, we show the following:

Theorem 1.1 *If $\alpha, \beta \in B_n$ are such that $\alpha^k = \beta^k$ for some $k \neq 0$, then α and β are conjugate.*

Our proof involves the Nielsen-Thurston classification of braids into periodic, reducible or pseudo-Anosov. We will see, for instance, that the kth root of a pseudo-Anosov braid is unique, if it exists, while a periodic or reducible braid may have several roots.

One easy consequence of Theorem 1.1 is the following, which could be useful for testing conjugacy in braid groups.

Corollary 1.2 *Let $\alpha, \beta \in B_n$ and let k be a nonzero integer. Then α is conjugate to β if and only if α^k is conjugate to β^k.*

Proof If α is conjugate to β then $\gamma^{-1}\alpha\gamma = \beta$ for some braid γ. Then $\gamma^{-1}\alpha^k\gamma = (\gamma^{-1}\alpha\gamma)^k = \beta^k$, hence α^k and β^k are conjugate.

Conversely, suppose that α^k and β^k are conjugate. Then $\gamma^{-1}\alpha^k\gamma = \beta^k$ for some γ. This means that $(\gamma^{-1}\alpha\gamma)^k = \beta^k$, and by Theorem 1.1 this implies that β is conjugate to $\gamma^{-1}\alpha\gamma$, thus β is conjugate to α. □

Hence, if we want to test whether two braids are conjugate, and we know a kth root or the kth power of each one, we just need to test if these roots or powers are conjugate.

This paper is structured as follows. In Section 2 we give the basic notions and results from Nielsen-Thurston theory applied to braids. In Section 3 we study in more detail a particular case of reducible braids, called *reducible braids in regular form*, that we introduce to simplify the proof of Theorem 1.1. This proof is given in Section 4.

2 Nielsen-Thurston theory

In the same way as isotopy classes of homeomorphisms of surfaces can be classified into periodic, reducible or pseudo-Anosov [19, 8], one has an analogous classification for braids [4, 12].

A braid β is said to be *periodic* if it is a root of a power of Δ^2, where $\Delta = \sigma_1(\sigma_2\sigma_1)(\sigma_3\sigma_2\sigma_1)\cdots(\sigma_{n-1}\cdots\sigma_1)$ is Garside's half twist. That is, β is periodic if $\beta^k = \Delta^{2m}$ for some nonzero integers k and m.

A braid β is said to be *reducible* if it preserves (up to isotopy) a family of disjoint nontrivial simple closed curves on the n-punctured disc. Here 'nontrivial' means not isotopic to the boundary but enclosing at least two punctures. Such an invariant family of curves is called a *reduction system*. There exists a *canonical reduction system* CRS(β) (see [4, 13]), which is the union of all nontrivial curves C satisfying the following two conditions:

(1) C is preserved by some power of β.

(2) Any curve C' having nontrivial geometric intersection with C is not preserved by any power of β.

It is known that, if β is reducible, then CRS(β) $= \emptyset$ if and only if β is periodic. Hence every reducible, non-periodic braid has a nontrivial canonical reduction system.

Finally, a braid β is *pseudo-Anosov* if it is neither periodic nor reducible. In this case [19] there exist two projective measured foliations of the disc, F^u and F^s, which are preserved by β. Moreover, the action of β on F^u (the unstable foliation) scales its measure by a real factor $\lambda > 1$, while the action on F^s (the stable foliation) scales its measure by λ^{-1}. These two foliations and the scaling factor λ (called the *stretch factor*), are uniquely determined by β.

Conversely, suppose that a braid β preserves two measured foliations, scaling their measures by λ and λ^{-1}. One has the following: If $\lambda > 1$ then β is pseudo-Anosov, and if $\lambda = 1$ then β is periodic (see [13]).

In order to prove Theorem 1.1, we need to show the following results. Although they are all well-known, we include some short proofs.

Lemma 2.1 *If* $\in B_n$ *is periodic, then* ^{k} *is periodic, for every* $k \neq 0$.

Proof There is some $t \neq 0$ such that ^{t} is a power of ^{2}. Hence $(^k)^t = (^t)^k$ is also a power of ^{2}, thus ^{k} is periodic. □

Lemma 2.2 *If* $\in B_n$ *is reducible and not periodic, then* ^{k} *is also reducible and not periodic, for every* $k \neq 0$. *Moreover,* $CRS( ) = CRS(^k)$.

Proof A curve is preserved by a power of if and only if it is preserved by a power of ^{k}. Hence, from the definition of the canonical reduction system of a braid, one has CRS( ) = CRS(^{k}). Since this family of curves is nonempty, it also follows that ^{k} is reducible and not periodic. □

Lemma 2.3 *If* $\in B_n$ *is pseudo-Anosov, with projective foliations* F^u *and* F^s, *and stretch factor* , *then for every* $k \neq 0$, ^{k} *is also pseudo-Anosov, with projective foliations* F^u *and* F^s, *and stretch factor* $^{|k|}$.

Proof This is a straightforward consequence of the definitions. □

Corollary 2.4 *If* $; \in B_n$ *are such that* $^k = {}^k$, *then and are of the same Nielsen-Thurston type.*

Proof By the above lemmas, the Nielsen-Thurston type of (resp.) is the same as the type of ^{k} (resp ^{k}). Since $^k = {}^k$, their types coincide. □

3 Reducible braids in regular form

The most difficult case in the proof of Theorem 1.1 occurs when and are reducible. Hence, we will study this kind of braid in more detail in this section. More precisely, we will define a special type of reducible braids, called reducible braids in *regular form*, which are easier to handle if we care about conjugacy. They were defined in [12] to study centralizers of braid. It is also shown in [12] that every reducible, non-periodic braid can be conjugated to another one in regular form. We will repeat that construction here since we need it for our purposes. Later we will give necessary and sufficient conditions for two braids in regular form to be conjugate. This will allow us to simplify the proof of Theorem 1.1.

First we will fix a reducible, non-periodic braid . We know that CRS( ) is nonempty, but the curves forming CRS( ) may be rather complicated. If we conjugate by some element , the canonical reduction system of $^{-1}$ will be (CRS( )) (here is considered as an automorphism of the punctured disc). We can then choose a braid which sends CRS( ) to the simplest possible family of closed curves: a family of circles, centered at the real axis (each circle will enclose more than one and less than n punctures). In other words, up to conjugacy we can suppose that CRS( ) is a family of circles (see Figure 1).

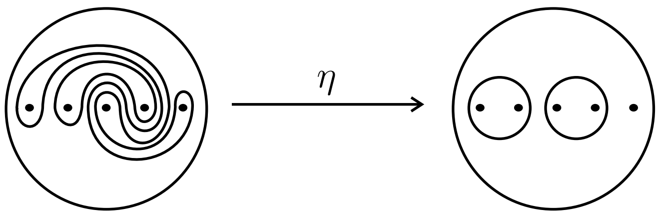

Figure 1: Canonical reduction systems can be simplified

Now we can decompose the punctured disc D in the following way (taken from [12]): Let $\mathcal{C}$ be the set of outermost circles of CRS( ). This set is preserved by , and we can distinguish the different orbits of circles under . We denote these orbits by $\mathcal{C}_1, \ldots, \mathcal{C}_t$, and the circles forming $\mathcal{C}_i$ by $C_{i,1}, C_{i,2}, \ldots, C_{i,r_i}$. That is, $\mathcal{C} = \bigcup_{i=1}^{t}(\bigcup_{u=1}^{r_i} C_{i,u})$ and sends $C_{i,u}$ to $C_{i,u+1}$, where $C_{i,r_i+1} = C_{i,1}$. In Figure 3 we can see an example showing the notation of these circles. In the examples we will usually number the orbits, and the circles inside each orbit, from left to right, but this does not need to be true in general: the only necessary condition is that sends $C_{i,u}$ to $C_{i,u+1}$. If at some time we need to stress that these circles, or orbits, belong to CRS( ), we will write $C_{i,u}( )$ or $\mathcal{C}_i( )$.

Denote by $D_{i,u} = D_{i,u}( )$ the punctured disc enclosed by the circle $C_{i,u}$, and let $\widehat{D} = D \setminus (\bigcup_{i,u} D_{i,u})$. Notice that $\widehat{D}$ can also be considered as a punctured disc, if we collapse each hole to a puncture (see Figure 2). Hence we have decomposed D into several punctured discs: $D = \widehat{D} \cup (\bigcup_{i,u} D_{i,u})$.

Now denote by $B_{\mathcal{C}}$ the subgroup of B_n formed by those braids that preserve $\mathcal{C}$ setwise (maybe permuting the curves that enclose the same number of punctures). Every braid in $B_{\mathcal{C}}$, considered as an automorphism of D, induces automorphisms (braids) on $\widehat{D}$ and on every $D_{i,u}( )$. More precisely, let m be the

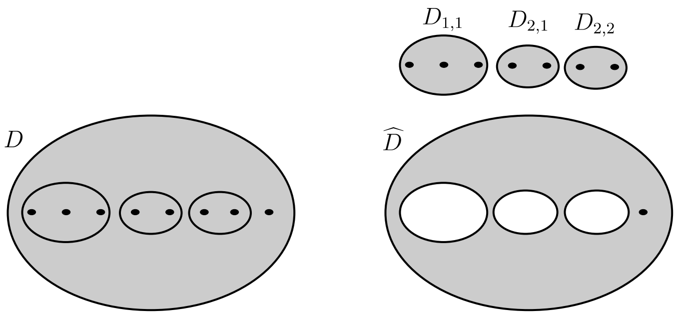

Figure 2: Decomposition of the disc along a canonical reduction system

number of punctures in $\widehat{D}$. We can define the map $p : B_C \to B_m$ that sends any $\in B_C$ to b, the braid corresponding to the automorphism induced by on $\widehat{D}$. It is easy to show that p is a homomorphism. The braid $p(\ ) =$ b is called the *tubular* braid associated to .

In the same way, given $\in B_C$, we can define for $i = 1, \dots, t$ and $u = 1, \dots, r_i$ the braid $_{i,u} = \ _{i,u;}$ induced by on the disc $D_{i,u}(\ )$. That is, $_{i,u}$ is the homeomorphism $_{i,u} : D_{i,u} \to D_{i,u+1}$ induced by . These braids are called the *interior* braids of . Hence every braid in B_C can be decomposed into one tubular braid and several interior braids (one for each circle in C).

One can also see this decomposition in a three dimensional picture. If we look at a braid $\in B_C$ in the cylinder $D \ [0,1]$, where the movements of the punctures are represented as strands, then the movements of the circles $C_{i,u}$ correspond to 'tubes'. If we forget the strands inside the tubes, we obtain the tubular braid b, where the solid tubes can be regarded as fat strands. On the other hand, the strands inside the tube that starts at $C_{i,u}$ and ends at $C_{i,u+1}$, correspond to the interior braid $_{i,u}$. See an example in Figure 3.

Notice that every $\in B_C$ is completely determined by the braids b and $_{i,u}$. We can now define a particulary simple kind of braid. The definition is taken from [12]:

Definition 3.1 Let be a reducible, non-periodic braid, whose canonical reduction system is a family of circles. With the above notations, we say that is in *regular form* if it satisfies the following conditions:

(1) For $i = 1, \dots, t$, the interior braids $_{i,u}$ are all trivial, except possibly $_{i,r_i}$, which is denoted $_{[i]}$.

(2) For $i, j \in \{1, \dots, t\}$, the interior braids $_{[i]}$ and $_{[j]}$ are either equal or non-conjugate.

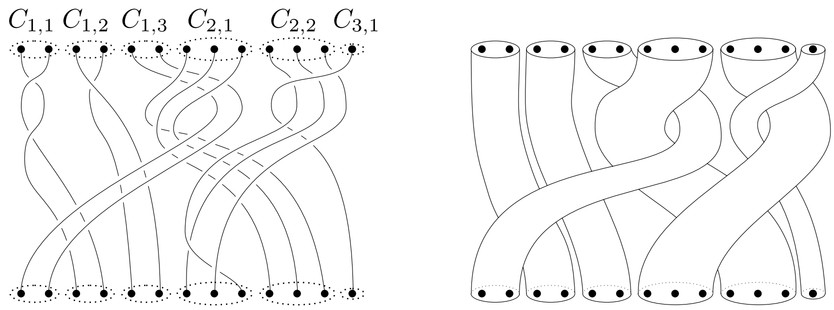

Figure 3: Example of a reducible braid α, and its corresponding tubular braid $\hat{\alpha}$. Notice the indices of the circles of C.

It is shown in [12] that every reducible, non-periodic braid α is conjugate to another one in regular form (although regular forms are not unique, that is, there could be more than one braid in regular form conjugate to α, as we shall see). The precise conjugation shown in [12] is the following. We define $\mu(\alpha) \in B_C$ as the braid whose tubular braid $\widehat{\mu(\alpha)}$ is trivial (vertical tubes), and whose interior braids are the following: $\mu(\alpha)_{i;u} = \alpha_{i,u}\alpha_{i,u+1}\cdots\alpha_{i,r_i}$, for $i = 1,\ldots,t$ and $u = 1,\ldots,r_i$. It is an easy exercise to show that $\alpha' = \mu(\alpha)^{-1}\alpha\mu(\alpha)$ has the same tubular braid as α, and its interior braids are all trivial, except possibly $\alpha'_{i,r_i} = \alpha'_{[i]} = \alpha_{i,1}\alpha_{i,2}\cdots\alpha_{i,r_i}$. In other words, conjugating by $\mu(\alpha)$ we 'transfuse' all interior braids of α in every C_i to its last tube (see Figure 4). Hence α' satisfies the first condition of Definition 3.1.

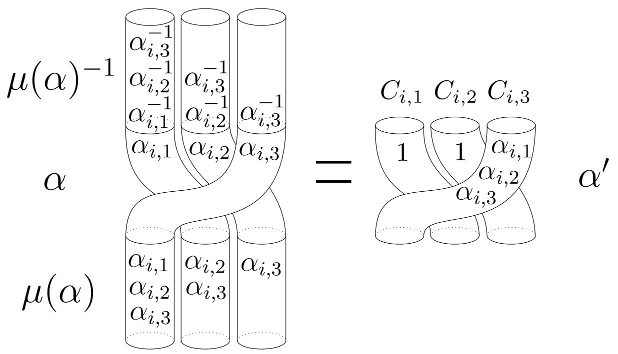

Figure 4: The conjugation of α by $\mu(\alpha)$ simplifies interior braids.

Now consider the interior braids $\alpha'_{[1]},\ldots,\alpha'_{[t]}$. For every $i = 1,\ldots,t$, choose one representative $_i$ of the conjugacy class of $\alpha'_{[i]}$, in such a way that if $\alpha'_{[i]}$ is conjugate to $\alpha'_{[j]}$, then $_i = {}_j$. For $i = 1,\ldots,t$, choose a braid $_i$ that conjugates $'_{[i]}$ to $_i$. Then we de ne ( ) $2\ B_C$ as the braid whose tubular braid ( ) is trivial, and whose interior braids are the following: $(\ )_{i;u;} = \ _i$ for $i = 1; : : : ; t$ and $u = 1; : : : ; r_i$. If we now conjugate $'$ by ( ), then every $'_{[i]}$ is replaced by $_i$ (see Figure 5), that is, $'' = (\ )^{-1}\ '\ (\ )$ satis es the two conditions of De nition 3.1, thus $''$ is in regular form.

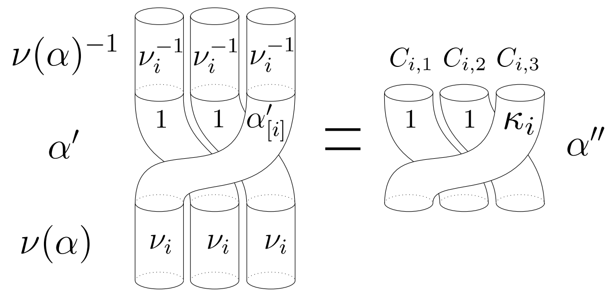

Figure 5: The conjugation by ( ) replaces $'_{[i]}$ by $_i$.

Therefore every reducible, non-periodic braid can be conjugated to a braid in regular form, and one possible conjugating braid is ( ) ( ). Notice that ( ) depends on our choice of the last tube of each C_i, and ( ) depends on our choice of a representative for the conjugacy class of each $'_{[i]}$. Hence, in general, the element $''$ in regular form conjugate to is not unique, though the interior braid $''_{[i]} = \ _i$ is conjugate to $_{i;1}\ \ _{i;r_i}$ in any case.

Next we need a result to test whether two reducible, non-periodic braids in regular form, having the same canonical reduction system, are conjugate. An obvious necessary condition is that their tubular braids be conjugate. A necessary and su cient condition is given by:

Proposition 3.2 *Let and be two reducible, non-periodic braids in regular form, such that CRS( ) = CRS( ) is a family of circles. Then and are conjugate if and only if there exists a braid that conjugates* b *to* b *such that, if sends the orbit C_i of* b *to the orbit C_j of* b*, then $_{[i]}$ is conjugate to $_{[j]}$.*

Proof Suppose that and are conjugate, and let be a conjugating braid, that is, $^{-1} \ =$. It is not di cult to show (and it is shown in [13]), that in this case (CRS( )) = CRS( ). But CRS( ) = CRS( ), hence preserves CRS( ), thus $2\ B_C$, where C is the set of outermost circles of CRS( ) = CRS( ). We can then apply p to all factors of the above equality, and we obtain b^{-1}bb = b, hence b and b are conjugate by b.

Now focus on the permutations induced by b and b on their base points $Q_1; : : : ; Q_m$. Consider one cycle $(Q_{i_1}; : : : ; Q_{i_r})$ of the permutation induced by b. Conjugation by b sends it to (b$(Q_{i_1}); : : : ;$ b(Q_{i_r})), which is a cycle of the permutation induced by (this is a general property in symmetric groups). Since these cycles correspond to the orbits of circles of and , then must send any orbit $C_i($ $)$ to an orbit $C_j($ $)$.

Consider an orbit $C_i($ $)$, which is sent to $C_j($ $)$ by conjugation by . The number of circles in each of these two orbits must coincide, so we call it r. Now, since $^{-1}$ = , one has $^{-1}$ ^{r} = ^{r}. But ^{r} is a braid that preserves each circle $C_{i;u}($ $)$, and the interior braid corresponding to any of these circles is $_{[i]}$ (recall that is in regular form). In the same way, ^{r} preserves each circle $C_{j;u}($ $)$, and the interior braid corresponding to any of these circles is $_{[j]}$. Choose then some $C_{i;u}($ $)$; it will be sent by to some $C_{j;v}($ $)$. Then one has:

$$_{[j]} = (\ ^r)_{j;v;} = \ ^{-1}_{i;u;} \ (\ ^r)_{i;u;} \ _{i;u;} = \ ^{-1}_{i;u;} \ _{[i]} \ _{i;u;} :$$

Hence $_{[i]}$ and $_{[j]}$ are conjugate. Therefore, the stated condition is satis ed by taking = b.

Conversely, suppose that there exists satisfying the above condition: For every $i = 1; : : : ; t$, the braid sends the orbit C_i of b to an orbit C_j of b, and $_{[i]}$ is conjugate to $_{[j]}$. This implies that $_{[i]}$ and $_{[j]}$ have the same number of strands, that is, all circles in $C_i($ $)$, and in $C_j($ $)$, enclose the same number of punctures. This condition allows us to de ne a braid $2 \ B_C$ such that b = : it su ces to consider the only braid in B_C whose tubular braid is and whose interior braids are all trivial (with the suitable number of strands).

If we conjugate by , we obtain a braid $^0 \ 2 \ B_C$, whose orbits of circles coincide with those of . Moreover, if conjugation by sends $C_i($ $)$ to $C_j($ $)$, then in $C_j($ $)$ there is just one nontrivial interior braid of ^{0}, which is precisely $_{[i]}$. But this nontrivial interior braid does not lie, in general, in the last tube of $C_j($ $)$. Anyway, we know how to conjugate ^{0} to a braid in regular form, with the same labelling of circles as : First, we de ne the braid $(\ ^0)$, such that $(\ ^0)^{-1} \ ^0 \ (\ ^0)$ has its nontrivial interior braids (which are still equal to $_{[i]}$) in the same tubes as . Then, if we take $_{[i]}$ as the representative for the conjugacy class of $_{[i]}$, this determines a braid $(\ ^0)$. Conjugating ^{0} by $(\ ^0) \ (\ ^0)$, we obtain a braid whose tubular braid is b, and whose interior braids coincide with those of , hence we obtain . We have then shown that is conjugate to , and the result follows. □

4 Proof of Theorem 1.1

Suppose that $\alpha, \beta \in B_n$ are such that $\alpha^k = \beta^k$ for some $k \neq 0$. By Corollary 2.4, we can distinguish three cases, depending whether α and β are periodic, reducible or pseudo-Anosov.

4.1 α and β are periodic

In this case we shall use a well known result that characterises periodic braids. Consider the following braids in B_n: $\delta = \sigma_1\sigma_2\cdots\sigma_{n-1}$ and $\gamma = \sigma_1^2\sigma_2\cdots\sigma_{n-1}$. They are drawn in Figure 6. It is easy to see that $\delta^n = \gamma^{n-1} = \Delta^2$, hence they are both periodic. The classification result is the following.

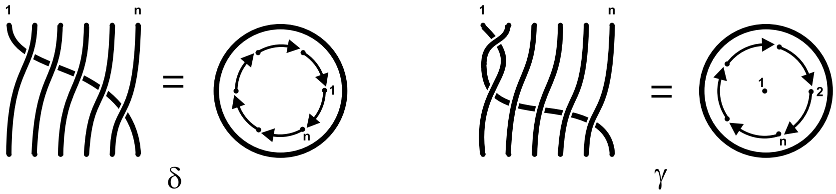

Figure 6: The periodic braids δ and γ.

Theorem 4.1 (de Kerekjarto [14, 5], Eilenberg [6]) *Every periodic braid is conjugate either to a power of δ or to a power of γ.*

Now we will show that α and β are conjugate to the same power of δ or γ, so they are conjugate to each other.

If we write every braid in terms of Artin generators, and we notice that the defining relations in the Artin presentation are homogeneous, it follows that the exponent sum $s(\alpha)$ of a braid α is an invariant of its conjugacy class. Notice that $s(\delta) = n-1$, while $s(\gamma) = n$. Hence, every conjugate of δ^t has exponent sum $(n-1)t$, and every conjugate of γ^t has exponent sum nt. The converse is also true:

Proposition 4.2 *Let α be a periodic braid. If $s(\alpha) = (n-1)t$ for some t, then α is conjugate to δ^t. If $s(\alpha) = nt$ for some t, then α is conjugate to γ^t.*

Proof If $s(\alpha) = (n-1)t$ and t is not a multiple of n, then δ^t is the only power of δ or γ with the same exponent sum as α, hence by Theorem 4.1, α is conjugate to δ^t. The same happens if $s(\alpha) = nt$, and t is not a multiple of

$n-1$: in this case is conjugate to γ^t. It remains to show what happens when $s(\ ) = n(n-1)q$, for some q. In this case could be conjugate either to ^{nq} or to $\gamma^{(n-1)q}$. But $^{nq} = \gamma^{(n-1)q} = \ ^{2q}$, hence both statements are true. □

Coming back to our problem, notice that $s(\ )k = s(\ ^k) = s(\ ^k) = s(\ )k$, so $s(\ ) = s(\ )$, since $k \neq 0$. Hence, by the above proposition, and are conjugate to the same power of or γ, as we wanted to show. The result is thus true if and are periodic.

4.2 and are pseudo-Anosov

Let F^u and F^s be the projective foliations corresponding to , and let be its stretch factor. By Lemma 2.3, the foliations and stretch factor corresponding to $^k = \ ^k$ are F^u, F^s and $^{|k|}$. Therefore, those corresponding to are F^u, F^s and .

We will show that, in this case, and commute: their commutator, $=$ $^{-1} \ ^{-1}$ preserves F^u and F^s, and its stretch factor is 1. Therefore, is periodic, thus conjugate to a power of or γ. Since the exponent sum $s(\ ) = 0$ then $= 1$, so and commute.

Now since $^k = \ ^k$ one has $^k \ ^{-k} = 1$. But since and commute, $^k \ ^{-k} =$ $(\ ^{-1})^k = 1$. This implies that $^{-1}$ is a torsion element of B_n, but since B_n is torsion free, it follows that $^{-1} = 1$ hence $=$. Therefore, if and are pseudo-Anosov, then not only is conjugate to : they coincide.

4.3 and are reducible, not periodic

We will show this case by induction on the number of strands. Since the case $n = 2$ has already been studied (all braids on two strands are periodic), we can suppose that $n > 2$, and that our result is true for every pair of braids with less than n strands.

Since and are reducible and not periodic, we know that their canonical reduction systems are non-empty and, by Lemma 2.2, they must coincide since they are both equal to CRS(^{k}) = CRS(^{k}).

We will now conjugate and by some braid , in order to simplify their canonical reduction system. This can be done due to the following fact: since $^k = \ ^k$, we have that $(\ ^{-1} \ )^k = \ ^{-1} \ ^k \ = \ ^{-1} \ ^k \ = (\ ^{-1} \ )^k$. If we then show that $^{-1}$ and $^{-1}$ are conjugate, then and will also be conjugate. Therefore, it su ces to show the result for suitable conjugates of and , hence we can suppose that CRS( ) = CRS( ) is a family of circles.

As usual, we denote by C the set of outermost circles of CRS( ) = CRS( ). Since $;\ \ 2\ B_C$, we can study their tubular and interior braids. First, since $^k = {}^k$ one has $\mathrm{b}^k = \mathrm{b}^k$. Moreover, since C is formed by the outermost circles of CRS( ) = CRS( ), this implies that CRS(b) = CRS(b) = $;$. That is, b and b are either pseudo-Anosov or periodic. We will treat these two cases separately.

b and b are pseudo-Anosov In this case, since $\mathrm{b}^k = \mathrm{b}^k$, we have already shown that b = b. Hence we can label the circles of C in the same way for both braids: $C = \bigcup_{i=1}^{t}(C_i) = \bigcup_{i=1}^{t}(\bigcup_{u=1}^{r_i}(C_{i;u}))$. We will show that and are conjugate by conjugating them to the same braid in regular form.

Recall that if we conjugate by ( ) ( ), we obtain a braid ^{00}, in regular form, such that $^{00}_{[i]}$ (the interior braid starting at $C_{i;r_i}$) is conjugate to ($_{i;1}$ $_{i;2}$ $_{i;r_i}$) for $i = 1;:::;t$. In the same way, if we conjugate by ( ) ( ), we obtain a braid ^{00}, in regular form, such that $^{00}_{[i]}$ is conjugate to ($_{i;1}$ $_{i;2}$ $_{i;r_i}$) for $i = 1;:::;t$. Therefore, ^{00} and ^{00} are two braids in regular form, whose tubular braids coincide (c^{00} = b = b = c^{00}), and whose nontrivial interior braids are placed into the same tubes. It just remains to show that we can take $^{00}_{[i]} = {}^{00}_{[i]}$. But $^{00}_{[i]}$ and $^{00}_{[i]}$ are just representatives of their conjugacy classes, hence it su ces to show that ($_{i;1}$ $_{i;2}$ $_{i;r_i}$) is conjugate to ($_{i;1}$ $_{i;2}$ $_{i;r_i}$) for $i = 1;:::;t$. In order to prove this, we can forget about ^{00} and ^{00}, and look at and , and their tubular and interior braids, as follows.

We know that $\mathrm{b}^k = \mathrm{b}^k$. Up to raising this braid to a suitable power, we can suppose that b^k is a pure braid (its corresponding permutation is trivial). Hence, for $i = 1;:::;t$, the length r_i of the orbit C_i must be a divisor of k, say $r_i p_i = k$. We will now look at the interior braids of ^{k} and ^{k}. If we raise to the power r_i, then the interior braid $(\ ^{r_i})_{i;1;} = {}_{i;1}\ \ {}_{i;r_i}$. Hence, if we further raise it to the power p_i, we obtain $(\ ^k)_{i;1;} = (\ _{i;1}\ \ _{i;r_i})^{p_i}$. In the same way, one has $(\ ^k)_{i;1;} = (\ _{i;1}\ \ _{i;r_i})^{p_i}$. Since $^k = {}^k$, and $C_{i;1}(\ ) = C_{i;1}(\ )$, it follows that $(\ _{i;1}\ \ _{i;r_i})^{p_i} = (\ _{i;1}\ \ _{i;r_i})^{p_i}$, which yields, by the induction hypothesis, that ($_{i;1}$ $_{i;r_i}$) is conjugate to ($_{i;1}$ $_{i;r_i}$), as we wanted to show.

b and b are periodic This time $\mathrm{b}^k = \mathrm{b}^k$ implies that b and b are conjugate (we have shown this for periodic braids), but not necessarily equal. Since they are periodic and conjugate, then they are both conjugate to the same power of or γ. We can also assume – as above – that $b^k = \hat{b}^k$ is a pure braid, that is, a power of ^{2} (with m strands).

Suppose that b and $\hat{b}$ are conjugate to some power of . In this case, all the orbits of outermost circles of and (i.e. orbits of points of b and $\hat{b}$) have the same length, say r. And k is a multiple of r, say $k = pr$. But the orbits of and (resp. b and $\hat{b}$) do not necessarily coincide.

We will first conjugate to a braid in regular form. Let us choose, from now on, a representative for each conjugacy class of braids. Then, for $i = 1, \ldots, t$, let $_i$ be the representative of the conjugacy class of ($_{i,1}$ $_{i,r}$). Notice that, by construction, if $_i$ and $_j$ are conjugate, then $_i =$ $_j$. Recall that there exists a braid ( ) ( ) which conjugates to ^{00}, in regular form, whose nontrivial interior braids are $_1, \ldots,$ $_t$.

We will now see that the list $_1, \ldots,$ $_t$ is completely determined by the interior braids of ^{k}. Indeed, take some circle $C_{i,u}($ $)$. Since the orbit $C_i($ $)$ has length r, and $k = pr$, it follows that $(^k)_{i,u;} = (_{i,u}$ $_{i,r}$ $_{i,1}$ $_{i,u-1})^p$. Conjugating this braid by $_{i,u}$ $_{i,r}$, we obtain $(_{i,1}$ $_{i,r})^p$, which is conjugate to ^p_i. That is, $(^k)_{i,u;}$ is conjugate to ^p_i. Hence, the interior braids of ^{k} inside the circles $C_{i,1}($ $), \ldots, C_{i,r}($ $)$ are all conjugate to ^p_i. Suppose that they were also conjugate to ^p_j, for $j \neq i$. Then ^p_i would be conjugate to ^p_j. But these braids have less than n strands, so by Corollary 1.2 (that we are allowed to use by the induction hypothesis), $_i$ would be conjugate to $_j$, and then $_i =$ $_j$.

In other words, the list of representatives $_1, \ldots,$ $_t$, counting repetitions, is completely determined by the interior braids of ^{k}, as follows. First we define a partition of C by the following property: two circles belong to the same coset if and only if the corresponding interior braids of ^{k} are conjugate. Then the number of circles in every coset is always a multiple of r, and the p-th roots of these interior braids determine the representatives $_1, \ldots,$ $_t$. An element $_i$ appears repeated q times in the list if and only if its corresponding coset has qr circles.

Now we can repeat the whole construction with . We will conjugate to ^{00}, in regular form, whose list of nontrivial interior braids is completely determined by ^{k}. But $^k =$ ^{k}, hence the list of nontrivial interior braids of ^{00} is exactly $_1, \ldots,$ $_t$.

We then have two braids ^{00} and ^{00} in regular form, whose lists of nontrivial interior braids coincide, and whose tubular braids, $\widehat{\ }^{00} = b$ and $\widehat{\ }^{00} = \hat{b}$, are both conjugate to the same power of . We must show that, in this case, ^{00}

and $''$ are conjugate. Up to conjugating $''$ and $''$ by elements in B_C with trivial interior braids, we can suppose that $^{\prime\prime} = ^{\prime\prime} = {}^s$, for some s. Hence, the orbits of $''$ and $''$ coincide, although the corresponding interior braids could lie in different tubes (even in different orbits).

We can now apply Proposition 3.2. $''$ and $''$ will be conjugate if it exists a braid that conjugates $''$ to $''$ (that is, a braid that commutes with ^{s}) such that, if $(C_i) = C_j$, then ${}_i = {}_j$. In other words, we need an element of the centralizer of ^{s} which permutes the orbits of ^{s} in the appropriate way. Fortunately, such an element always exists.

The centralizer of a power of has been described in [2] (see also [12]): consider the braid ${}^s = ({}_1 \cdots {}_{m-1})^s$ on m strands. We will now denote by C_i the orbit (of points) induced by ^{s} that starts at the point P_i. That is, $C_i = \{P_i, P_{s+i}, P_{2s+i}, \ldots, P_{(r-1)s+i}\}$, where the indices are taken modulo m. Then, for $i = 1, \ldots, t-1$, consider the braid $S_i = ({}_i\, {}^s)^r$. This braid commutes with ^{s} and permutes the orbits C_i and C_{i+1}. Therefore, taking products of the elements S_i, we can obtain any desired permutation of the orbits. Hence the braid required by Proposition 3.2 exists, so $''$ is conjugate to $''$. Therefore, if $\widehat{\ }$ and $\widehat{\ }$ are conjugate to a power of , then is conjugate to , as we wanted to show.

It remains the case when $\widehat{\ }$ and $\widehat{\ }$ are conjugate to γ^s, for some s. Recall that $\widehat{\ }$ and $\widehat{\ }$ have m strands. We can suppose that s is not a multiple of $m-1$, since in that case γ^s is a power of ^{2}, thus a power of , and this case has already been studied. Therefore, the orbits of $\widehat{\ }$ and $\widehat{\ }$ are as follows: there is one orbit C_1 of length one, and all the other orbits $C_2, \ldots, C_t$ have the same length, say r, where $r > 1$.

Now we can apply the same methods as before. First, we can suppose that $\widehat{\ }^k = \widehat{\ }^k$ is a pure braid, and we denote $p = k/r$. Then the interior braids of ^{k} are as follows: one of them equals $({}_{1,1})^k$, and the others are conjugate to $({}_{i,1} \cdots {}_{i,r})^p$ for some i. We then choose a representative ${}_1$ for the conjugacy class of ${}_{1,1}$, and a representative ${}_i$ for the conjugacy class of $({}_{i,1}, \ldots, {}_{i,r})$, for $i > 1$. This time, the list ${}_1, \ldots, {}_t$ is determined by ^{k} as follows. First we define a partition of C by the following property: two circles of C belong to the same coset if and only if the interior braids of ^{k} in their corresponding tubes are conjugate. Then there is just one coset whose size is not a multiple of r, but congruent to 1 modulo r. Take any interior braid of ^{k} in that coset. Its kth root is conjugate to ${}_1$. The pth roots of the remaining interior braids of ^{k} yield the elements ${}_2, \ldots, {}_t$, as in the previous case.

Now we conjugate to $''$, in regular form, whose nontrivial interior braids are $_1, \ldots, _t$. Then we conjugate to $''$, in regular form, whose nontrivial interior braids are also $_1, \ldots, _t$, since they are determined by $^k = {}^k$. Notice that, in both cases, $_1$ is the interior braid of the only orbit of length one. We can now conjugate $''$ and $''$ by suitable braids in B_C, with trivial interior braids, thus we can suppose that $C'' = C'' = \gamma^s$. This time, the interior braid $_1$ is already in the same position (the rst tube of γ^s) for both braids, but the remaining interior braids could be in di erent positions. Applying Proposition 3.2 again, we need a braid that commutes with γ^s, permuting the orbits $C_2, \ldots, C_t$ as desired. This is always possible, as we are about to see.

The centralizer of $\gamma^s = ({}_1^2 \; {}_2 \quad {}_{m-1})^s$ has also been studied in [2]. For every $i = 2, \ldots, t-1$, the braid $T_i = ({}_i \gamma^s)^r$ commutes with γ^s and permutes the orbits C_i and C_{i+1}. Therefore we can always de ne as a product of the T_i's, hence $''$ and $''$ are conjugate. It follows that and are conjugate, and the theorem is proved.

Acknowledgements I am very grateful to Bert Wiest for useful conversations, and for his comments and suggestions on an early version of this paper. I also want to thank Tara Brendle, who pointed out some inconsistent notation, and helped to clarify some obscure parts of the proofs.

The author is partially supported by MCYT, BFM2001-3207 and FEDER.

References

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

[2] D. Bessis, F. Digne, J. Michel, Springer theory in braid groups and the Birman-Ko-Lee monoid, Paci c J. Math. 205 (2002), no. 2, 287{309.

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

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

[5] A. Constantin, B. Kolev, The theorem of Kerekjarto on periodic homeomorphisms of the disc and the sphere, Enseign. Math (2) 40 (1994) No 3-4, 193-204.

[6] S. Eilenberg, Sur les transformations periodiques de la surface de sphere, Fund. Math. 22 (1934), 28{41.

[7] E. A. El-Rifai, H. R. Morton, Algorithms for positive braids, Quart. J. Math. Oxford Ser. (2) 45 (1994), no. 180, 479{497.

[8] A. Fathi, F. Laudenbach, V. Poenaru, Travaux de Thurston sur les surfaces - seminaire Orsay, Asterisque 66{67, Societe Math. de France, 1991.

[9] N. Franco, J. Gonzalez-Meneses, Conjugacy problem for braid groups and Garside groups. J. of Algebra 266, no. 1 (2003), 112{132.

[10] N. Franco, J. Gonzalez-Meneses, Computation of centralizers in braid groups and Garside groups. Rev. Mat. Iberoamericana 19, no. 2 (2003), 367{384.

[11] F. A. Garside, The braid group and other groups, Quart. J. Math. Oxford 20 (1969), 235{254.

[12] J. Gonzalez-Meneses and B. Wiest, On the structure of the centralizer of a braid. Preprint. arXiv:math.GT/0305156

[13] N. V. Ivanov, Subgroups of Teichmüller modular groups, Translations of mathematical monographs vol. 115, AMS.

[14] B. de Kerekjarto, Über die periodischen Transformationen der Kreisscheibe und der Kugelfläche, Math. Annalen 80 (1919), 3{7.

[15] G. S. Makanin, On normalizers in the braid group, Mat.Sb. 86 (128), 1971, 171{179.

[16] G. Baumslag, A. G. Myasnikov, V. Shpilrain, Open problems in Combinatorial Group Theory, Second Edition. Comntemporary Mathematics 296 (2002), 1{38. See also http://grouptheory.info

[17] H. Sibert, Extraction of roots in Garside groups, Comm. Algebra 30 (2002), no. 6, 2915{2927.

[18] V. B. Styshnev, Taking the root in the braid group. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 42 (1978), no. 5, 1120{1131.

[19] W. P. Thurston, On the geometry and dynamics of di eomorphisms of surfaces, Bull. Amer. Math. Soc. (N.S.) 19 (1988), 417{431.

[20] W. P. Thurston, Braid Groups, Chapter 9 of \Word processing in groups", D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson and W. P. Thurston, Jones and Bartlett Publishers, Boston, MA, 1992.

Universidad de Sevilla. Dep. Matematica Aplicada I
ETS Arquitectura, Av. Reina Mercedes 2, 41012-Sevilla, Spain

Email: meneses@us.es

URL: www.personal.us.es/meneses

Received: 29 June 2003 Revised: 16 October 2003