The proof of Birman’s conjecture on singular braid monoids

LUI S PARIS

Institut de Mathématiques de Bourgogne, Université de Bourgogne
UMR 5584 du CNRS, BP 47870, 21078 Dijon cedex, France

Email: lparis@u-bourgogne.fr

URL: http://math.u-bourgogne.fr/topo/paris/index.html

Abstract

Let $B_n$ be the Artin braid group on $n$ strings with standard generators $\sigma_1, \ldots, \sigma_{n-1}$, and let $SB_n$ be the singular braid monoid with generators $\sigma_1^{\pm 1}, \ldots, \sigma_{n-1}^{\pm 1}, \tau_1, \ldots, \tau_{n-1}$. The desingularization map is the multiplicative homomorphism $\eta: SB_n \to \mathbb{Z}[B_n]$ defined by $\eta(\sigma_i^{\pm 1}) = \sigma_i^{\pm 1}$ and $\eta(\tau_i) = \sigma_i - \sigma_i^{-1}$, for $1 \leq i \leq n-1$. The purpose of the present paper is to prove Birman’s conjecture, namely, that the desingularization map $\eta$ is injective.

AMS Classification numbers
Primary: 20F36
Secondary: 57M25. 57M27

Keywords: Singular braids, desingularization, Birman’s conjecture

Proposed: Joan Birman
Received: 6 January 2004
Seconded: Robion Kirby, Cameron Gordon
Revised: 21 September 2004

© Geometry & Topology Publications
1 Introduction

Define an \(n\)-braid to be a collection \(b = (b_1, \ldots, b_n)\) of disjoint smooth paths in \(\mathbb{C} \times [0,1]\), called the strings of \(b\), such that the \(k\)-th string \(b_k\) runs monotonically in \(t \in [0,1]\) from the point \((k,0)\) to some point \((\zeta(k),1)\), where \(\zeta\) is a permutation of \(\{1, 2, \ldots, n\}\). An isotopy in this context is a deformation through braids which fixes the ends. Multiplication of braids is defined by concatenation. The isotopy classes of braids with this multiplication form a group, called braid group on \(n\) strings, and denoted by \(B_n\). This group has a well-known presentation with generators \(\sigma_1, \ldots, \sigma_{n-1}\) and relations

\[
\begin{align*}
\sigma_j \sigma_k &= \sigma_k \sigma_j & \text{if} & \quad |j-k| > 1, \\
\sigma_j \sigma_k \sigma_j &= \sigma_k \sigma_j \sigma_k & \text{if} & \quad |j-k| = 1.
\end{align*}
\]

The group \(B_n\) has other equivalent descriptions as a group of automorphisms of a free group, as the fundamental group of a configuration space, or as the mapping class group of the \(n\)-punctured disk, and plays a prominent rôle in many disciplines. We refer to [4] for a general exposition on the subject.

The Artin braid group \(B_n\) has been extended to the singular braid monoid \(SB_n\) by Birman [5] and Baez [1] in order to study Vassiliev invariants. The strings of a singular braid are allowed to intersect transversely in finitely many double points, called singular points. As with braids, isotopy is a deformation through singular braids which fixes the ends, and multiplication is by concatenation. Note that the isotopy classes of singular braids form a monoid and not a group. It is shown in [5] that \(SB_n\) has a monoid presentation with generators \(\sigma_1^\pm 1, \ldots, \sigma_{n-1}^\pm 1, \tau_1, \ldots, \tau_{n-1}\), and relations

\[
\begin{align*}
\sigma_i \sigma_i^{-1} &= \sigma_i^{-1} \sigma_i = 1, & \sigma_i \tau_i &= \tau_i \sigma_i & \text{if} & \quad 1 \leq i \leq n-1, \\
\sigma_i \sigma_j &= \sigma_j \sigma_i, & \sigma_i \tau_j &= \tau_j \sigma_i, & \tau_i \tau_j &= \tau_j \tau_i, & \text{if} & \quad |i-j| > 1, \\
\sigma_i \sigma_j \sigma_i &= \sigma_j \sigma_i \sigma_j, & \sigma_i \sigma_j \tau_i &= \tau_i \sigma_i \sigma_j, & \sigma_i \tau_i \tau_i &= \tau_i \sigma_i \tau_i, & \text{if} & \quad |i-j| = 1.
\end{align*}
\]

Consider the braid group ring \(\mathbb{Z}[B_n]\). The natural embedding \(B_n \to \mathbb{Z}[B_n]\) can be extended to a multiplicative homomorphism \(\eta: SB_n \to \mathbb{Z}[B_n]\), called desingularization map, and defined by

\[
\eta(\sigma_i^{\pm 1}) = \sigma_i^{\pm 1}, \quad \eta(\tau_i) = \sigma_i - \sigma_i^{-1}, \quad \text{if} \quad 1 \leq i \leq n-1.
\]

This homomorphism is one of the main ingredients of the definition of Vassiliev invariants for braids. It has been also used by Birman [5] to establish a relation between Vassiliev knot invariants and quantum groups.

One of the most popular problems in the subject, known as “Birman’s conjecture”, is to determine whether \(\eta\) is an embedding (see [5]). At the time of this
writing, the only known partial answer to this question is that $\eta$ is injective on singular braids with up to three singularities (see [17]), and on singular braids with up to three strings (see [13]).

The aim of the present paper is to solve this problem, namely, we prove the following.

**Theorem 1.1** The desingularization map $\eta: SB_n \to \mathbb{Z}[B_n]$ is injective.

Let $S_d B_n$ denote the set of isotopy classes of singular braids with $d$ singular points. Recall that a Vassiliev invariant of type $d$ is defined to be a homomorphism $v: \mathbb{Z}[B_n] \to A$ of $\mathbb{Z}$-modules which vanishes on $\eta(S_{d+1} B_n)$. One of the main results on Vassiliev braid invariants is that they separate braids (see [3], [15], [16]). Whether Vassiliev knot invariants separate knots remains an important open question. Now, it has been shown by Zhu [17] that this separating property extends to singular braids if $\eta$ is injective. So, a consequence of Theorem 1.1 is the following.

**Corollary 1.2** Vassiliev braid invariants classify singular braids.

Let $\Gamma$ be a graph (with no loop and no multiple edge), let $X$ be the set of vertices, and let $E = E(\Gamma)$ be the set of edges of $\Gamma$. Define the graph monoid of $\Gamma$ to be the monoid $\mathcal{M}(\Gamma)$ given by the monoid presentation

$$\mathcal{M}(\Gamma) = \langle X \mid xy = yx \text{ if } \{x, y\} \in E(\Gamma)^+ \rangle.$$  

Graph monoids are also known as free partially commutative monoids or as right-angled Artin monoids. They were first introduced by Cartier and Foata [7] to study combinatorial problems on rearrangements of words, and, since then, have been extensively studied by both computer scientists and mathematicians.

The key point of the proof of Theorem 1.1 consists in understanding the structure of the multiplicative submonoid of $\mathbb{Z}[B_n]$ generated by the set $\{\alpha \sigma_i^2 \alpha^{-1} - 1; \alpha \in B_n \text{ and } 1 \leq i \leq n - 1\}$. More precisely, we prove the following.

**Theorem 1.3** Let $\Omega$ be the graph defined as follows.

- $\Sigma = \{\alpha \sigma_i^2 \alpha^{-1}; \alpha \in B_n \text{ and } 1 \leq i \leq n - 1\}$ is the set of vertices of $\Omega$;
- $\{u, v\}$ is an edge of $\Omega$ if and only if we have $uv = vu$ in $B_n$.

Let $\nu: \mathcal{M}(\Omega) \to \mathbb{Z}[B_n]$ be the homomorphism defined by $\nu(u) = u - 1$, for all $u \in \Sigma$. Then $\nu$ is injective.
The proof of the implication Theorem 1.3 ⇒ Theorem 1.1 is based on the observation that $SB_n$ is isomorphic to the semi-direct product of $\mathcal{M}(\Omega)$ with the braid group $B_n$, and that $\nu: \mathcal{M}(\Omega) \to \mathbb{Z}[B_n]$ is the restriction to $\mathcal{M}(\Omega)$ of the desingularization map. The proof of this implication is the subject of Section 2. Let $A_{ij}$, $1 \leq i < j \leq n$, be the standard generators of the pure braid group $PB_n$. In Section 3, we show that $Y$ is the disjoint union of the conjugacy classes of the $A_{ij}$’s in $PB_n$. Using homological arguments, we then show that we can restrict the study to the submonoid of $\mathcal{M}(\Omega)$ generated by the conjugacy classes of two given generators, $A_{ij}$ and $A_{rs}$. If $\{i, j\} \cap \{r, s\} \neq \emptyset$, then the subgroup generated by the conjugacy classes of $A_{ij}$ and $A_{rs}$ is a free group, and we prove the injectivity using a sort of Magnus expansion (see Section 4). The case $\{i, j\} \cap \{r, s\} = \emptyset$ is handled using the previous case together with a technical result on automorphisms of free groups (Proposition 5.1).

Acknowledgement  My first proof of Proposition 5.1 was awful, hence I asked some experts whether they know another proof or a reference for the result. The proof given here is a variant of a proof indicated to me by Warren Dicks. So, I would like to thank him for his help.

2 Theorem 1.3 implies Theorem 1.1

We assume throughout this section that the result of Theorem 1.3 holds, and we prove Theorem 1.1.

Let $\delta_i = \sigma_i \tau_i$ for $1 \leq i \leq n - 1$. Then $SB_n$ is generated as a monoid by $\sigma_1^{\pm 1}, \ldots, \sigma_{n-1}^{\pm 1}, \delta_1, \ldots, \delta_{n-1}$, and has a monoid presentation with relations

\[
\begin{align*}
\sigma_i \sigma_i^{-1} &= \sigma_i^{-1} \sigma_i = 1, & & \text{if } 1 \leq i \leq n - 1, \\
\sigma_i \sigma_j &= \sigma_j \sigma_i, & \sigma_i \delta_i &= \delta_i \sigma_i, & & \text{if } |i - j| > 1, \\
\sigma_i \sigma_j \sigma_i &= \sigma_j \sigma_i \sigma_j, & \sigma_i \sigma_j \delta_i &= \delta_j \sigma_i \sigma_j, & & \text{if } |i - j| = 1.
\end{align*}
\]

Moreover, the desingularization map $\eta: SB_n \to \mathbb{Z}[B_n]$ is determined by

\[
\eta(\sigma_i^{\pm 1}) = \sigma_i^{\pm 1}, \quad \eta(\delta_i) = \sigma_i^2 - 1, \quad \text{if } 1 \leq i \leq n - 1.
\]

The following lemma is a particular case of [12], Theorem 7.1.

**Lemma 2.1** Let $i, j \in \{1, \ldots, n - 1\}$, and let $\beta \in SB_n$. Then the following are equivalent:

1. $\beta \sigma_i^2 = \sigma_j^2 \beta$;
2. $\beta \delta_i = \delta_j \beta$.

*Geometry & Topology, Volume 8 (2004)*
This lemma shows the following.

**Lemma 2.2** Let $\hat{\Omega}$ be the graph defined as follows.

- $\hat{\Omega} = \{\alpha\delta_i\alpha^{-1}; \alpha \in B_n$ and $1 \leq i \leq n-1\}$ is the set of vertices of $\hat{\Omega}$;
- $\{\hat{u}, \hat{v}\}$ is an edge of $\hat{\Omega}$ if and only if we have $\hat{u}\hat{v} = \hat{v}\hat{u}$ in $SB_n$.

Then there exists an isomorphism $\varphi: M(\hat{\Omega}) \to M(\Omega)$ which sends $\alpha\delta_i\alpha^{-1} \in \hat{\Omega}$ to $\alpha\sigma_i^2\alpha^{-1} \in \Omega$ for all $\alpha \in B_n$ and $1 \leq i \leq n-1$.

**Proof** Let $\alpha, \beta \in B_n$ and $i, j \in \{1, \ldots, n-1\}$. Then, by Lemma 2.1,

$$\alpha\sigma_i^2\alpha^{-1} = \beta\sigma_j^2\beta^{-1} \iff (\beta^{-1}\alpha)\sigma_i^2 = \sigma_j^2(\beta^{-1}\alpha)$$

$$\iff (\beta^{-1}\alpha)\delta_i = \delta_j(\beta^{-1}\alpha) \iff \alpha\delta_i\alpha^{-1} = \beta\delta_j\beta^{-1}.$$ 

This shows that there exists a bijection $\varphi: \hat{\Omega} \to \Omega$ which sends $\alpha\delta_i\alpha^{-1} \in \hat{\Omega}$ to $\alpha\sigma_i^2\alpha^{-1} \in \Omega$ for all $\alpha \in B_n$ and $1 \leq i \leq n-1$. Let $\alpha, \beta \in B_n$ and $i, j \in \{1, \ldots, n-1\}$. Again, by Lemma 2.1,

$$(\alpha\sigma_i^2\alpha^{-1})(\beta\sigma_j^2\beta^{-1}) = (\beta\sigma_j^2\beta^{-1})(\alpha\sigma_i^2\alpha^{-1})$$

$$\iff \sigma_i^2(\alpha^{-1}\beta\sigma_j^2\beta^{-1}\alpha) = (\alpha^{-1}\beta\sigma_j^2\beta^{-1}\alpha)\sigma_i^2$$

$$\iff \delta_i(\alpha^{-1}\beta\sigma_j^2\beta^{-1}\alpha) = (\alpha^{-1}\beta\sigma_j^2\beta^{-1}\alpha)\delta_i$$

$$\iff (\beta^{-1}\alpha\delta_i\alpha^{-1}\beta)\delta_i = \delta_j(\beta^{-1}\alpha\delta_i\alpha^{-1}\beta)$$

$$\iff (\alpha\delta_i\alpha^{-1})(\beta\delta_j\beta^{-1}) = (\beta\delta_j\beta^{-1})(\alpha\delta_i\alpha^{-1})$$

This shows that the bijection $\varphi: \hat{\Omega} \to \Omega$ extends to an isomorphism $\varphi: M(\hat{\Omega}) \to M(\Omega)$.

Now, we have the following decomposition for $SB_n$.

**Lemma 2.3** $SB_n = M(\hat{\Omega}) \times B_n$.

**Proof** Clearly, there exists a homomorphism $f: M(\hat{\Omega}) \times B_n \to SB_n$ which sends $\beta$ to $\beta \in SB_n$ for all $\beta \in B_n$, and sends $\hat{u}$ to $\hat{u} \in SB_n$ for all $\hat{u} \in \hat{\Omega}$. On the other hand, one can easily verify using the presentation of $SB_n$ that there exists a homomorphism $g: SB_n \to M(\hat{\Omega}) \times B_n$ such that $g(\sigma_i^{\pm1}) = \sigma_i^{\pm1} \in B_n$ for all $i \in \{1, \ldots, n-1\}$, and $g(\delta_i) = \delta_i \in \hat{\Omega}$ for all $i \in \{1, \ldots, n-1\}$. Obviously, $f \circ g = \text{Id}$ and $g \circ f = \text{Id}$.
Remarks  

(1) Let $G(\hat{\Omega})$ be the group given by the presentation

$$G(\hat{\Omega}) = \langle \hat{T} \mid \hat{u}\hat{v} = \hat{v}\hat{u} \text{ if } \{\hat{u}, \hat{v}\} \in E(\hat{\Omega}) \rangle.$$ 

It is well-known that $\mathcal{M}(\hat{\Omega})$ embeds in $G(\hat{\Omega})$ (see [9], [10]), thus $SB_n = \mathcal{M}(\hat{\Omega}) \times B_n$ embeds in $G(\hat{\Omega}) \times B_n$. This furnishes one more proof of the fact that $SB_n$ embeds in a group (see [11], [2], [14]).

(2) The decomposition $SB_n = \mathcal{M}(\hat{\Omega}) \times B_n$ together with Lemma 2.2 can be used to solve the word problem in $SB_n$. The proof of this fact is left to the reader. Another solution to the word problem for $SB_n$ can be found in [8].

Proof of Theorem 1.1  

Consider the homomorphism $\deg : B_n \to \mathbb{Z}$ defined by $\deg(\sigma_i) = 1$ for $1 \leq i \leq n - 1$. For $k \in \mathbb{Z}$, let $B_n^{(k)} = \{\beta \in B_n ; \deg(\beta) = k\}$. We have the decomposition

$$\mathbb{Z}[B_n] = \bigoplus_{k \in \mathbb{Z}} \mathbb{Z}[B_n^{(k)}],$$

where $\mathbb{Z}[B_n^{(k)}]$ denotes the free abelian group freely generated by $B_n^{(k)}$. Let $P \in \mathbb{Z}[B_n]$. We write $P = \sum_{k \in \mathbb{Z}} P_k$, where $P_k \in \mathbb{Z}[B_n^{(k)}]$ for all $k \in \mathbb{Z}$. Then $P_k$ is called the $k$-th component of $P$.

Let $\gamma, \gamma' \in SB_n$ such that $\eta(\gamma) = \eta(\gamma')$. We write $\gamma = \alpha\beta$ and $\gamma' = \alpha'\beta'$ where $\alpha, \alpha' \in \mathcal{M}(\hat{\Omega})$ and $\beta, \beta' \in B_n$ (see Lemma 2.3). Let $d = \deg(\beta)$. We observe that the $d$-th component of $\eta(\gamma)$ is $\pm \beta$, and, for $k < d$, the $k$-th component of $\eta(\gamma)$ is 0. In particular, $\eta(\gamma)$ completely determines $\beta$. Since $\eta(\gamma) = \eta(\gamma')$, it follows that $\beta = \beta'$.

So, multiplying $\gamma$ and $\gamma'$ on the right by $\beta^{-1}$ if necessary, we may assume that $\gamma = \alpha \in \mathcal{M}(\hat{\Omega})$ and $\gamma' = \alpha' \in \mathcal{M}(\hat{\Omega})$. Observe that

$$(\nu \circ \varphi)(\gamma) = \eta(\gamma) = \eta(\gamma') = (\nu \circ \varphi)(\gamma').$$

Since $\nu$ is injective (Theorem 1.3) and $\varphi$ is an isomorphism (Lemma 2.2), we conclude that $\gamma = \gamma'$.

3 Proof of Theorem 1.3

We start this section with the following result on graph monoids.

Lemma 3.1  Let $\Gamma$ be a graph, let $X$ be the set of vertices, and let $E = E(\Gamma)$ be the set of edges of $\Gamma$. Let $x_1, \ldots, x_l, y_1, \ldots, y_l \in X$ and $k \in \{1, 2, \ldots, l\}$ such that:

Now, consider the standard epimorphism \( \theta: B_n \to \text{Sym}_n \) defined by \( \theta (\sigma_i) = (i, i + 1) \) for \( 1 \leq i \leq n - 1 \). The kernel of \( \theta \) is called the pure braid group on \( n \) strings, and is denoted by \( PB_n \). It has a presentation with generators

\[
A_{i,j} = \sigma_{j-1} \ldots \sigma_{i+1} \sigma_i^{-1} \ldots \sigma_{j-1}^{-1}, \quad 1 \leq i < j \leq n,
\]

and relations

\[
A_{r,s}^{-1} A_{i,j} A_{r,s} = A_{i,j} \quad \text{if} \quad r < s < i < j \quad \text{or} \quad i < r < s < j,
\]

\[
A_{r,s}^{-1} A_{i,j} A_{r,s} = A_{r,j} A_{i,j} A_{r,s}^{-1} \quad \text{if} \quad s = i,
\]

\[
A_{r,s}^{-1} A_{i,j} A_{r,s} = A_{i,j} A_{s,j} A_{i,j} A_{s,j}^{-1} A_{i,j}^{-1} \quad \text{if} \quad i = r < s < j,
\]

\[
A_{r,s}^{-1} A_{i,j} A_{r,s} = A_{r,j} A_{s,j} A_{r,j} A_{s,j}^{-1} A_{r,j}^{-1} \quad \text{if} \quad r < i < s < j.
\]

(See [4]). We denote by \( H_1(PB_n) \) the abelianization of \( PB_n \), and, for \( \beta \in PB_n \), we denote by \( [\beta] \) the element of \( H_1(PB_n) \) represented by \( \beta \). A consequence of the above presentation is that \( H_1(PB_n) \) is a free abelian group freely generated.
by \( \{[A_{ij}]; 1 \leq i < j \leq n\} \). This last fact shall be of importance in the remainder of the paper.

For \( 1 \leq i < j \leq n \), we set
\[
\mathcal{Y}_{ij} = \{\beta A_{ij}\beta^{-1} ; \beta \in PB_n\}.
\]

**Lemma 3.2** We have the disjoint union \( \mathcal{Y} = \bigcup_{i<j} \mathcal{Y}_{ij} \).

**Proof** It is easily checked that
\[
\sigma_r A_{ij} \sigma_r^{-1} = \begin{cases} 
A_{ij+1} & \text{if } r = j, \\
A_{j-1}A_{ij}^{-1}A_{j-1} & \text{if } r = j-1 > i, \\
A_{i+1} & \text{if } j-1 > i = r, \\
A_{ij}^{-1}A_{i-1}A_{ij} & \text{if } r = i-1, \\
A_{ij} & \text{otherwise}.
\end{cases}
\]

This implies that the union \( \bigcup_{i<j} \mathcal{Y}_{ij} \) is invariant by the action of \( B_n \) by conjugation. Moreover, \( \sigma^2_r = A_{i+1} \in \mathcal{Y}_{ii+1} \) for all \( i \in \{1, \ldots, n-1\} \), thus \( \mathcal{Y} \subset \bigcup_{i<j} \mathcal{Y}_{ij} \). On the other hand, \( A_{ij} \) is conjugate (by an element of \( B_n \)) to \( A_{ij}^{-1} \), thus \( \mathcal{Y}_{ij} \subset \mathcal{Y} \) for all \( i < j \), therefore \( \bigcup_{i<j} \mathcal{Y}_{ij} \subset \mathcal{Y} \).

Let \( i, j, r, s \in \{1, \ldots, n\} \) such that \( i < j, r < s \), and \( \{i, j\} \neq \{r, s\} \). Let \( u \in \mathcal{Y}_{ij} \) and \( v \in \mathcal{Y}_{rs} \). Then \( [u] = [A_{ij}] \neq [A_{rs}] = [v] \), therefore \( u \neq v \). This shows that \( \mathcal{Y}_{ij} \cap \mathcal{Y}_{rs} = \emptyset \).

The following lemmas 3.3 and 3.5 will be proved in Sections 4 and 5, respectively.

Let \( F(X) \) be a free group freely generated by some set \( X \). Let \( Y = \{g x g^{-1}; g \in F(X) \text{ and } x \in X\} \), and let \( F^+(Y) \) be the free monoid freely generated by \( Y \).

We prove in Section 4 that the homomorphism \( \nu: F^+(Y) \to Z[F(X)] \), defined by \( \nu(y) = y - 1 \) for all \( y \in Y \), is injective (Proposition 4.1). The proof of this result is based on the construction of a sort of Magnus expansion. Proposition 4.1 together with the fact that \( PB_n \) can be decomposed as \( PB_n = F \times PB_{n-1} \), where \( F \) is a free group freely generated by \( \{A_i; 1 \leq i \leq n-1\} \), are the main ingredients of the proof of Lemma 3.3.

Choose some \( x_0 \in X \), consider the decomposition \( F(X) = \langle x_0 \rangle \ast F(X \setminus \{x_0\}) \), and let \( \rho: F(X) \to F(X) \) be an automorphism which fixes \( x_0 \) and which leaves \( F(X \setminus \{x_0\}) \) invariant. Let \( y_1, \ldots, y_l \in \{gxg^{-1}; g \in F(X)\} \). We prove in Section 5 that, if \( \rho(y_1 \ldots y_l) = y_1 \ldots y_l \), then \( \rho(y_i) = y_i \) for all \( i = 1, \ldots, l \) (Proposition 5.1). The proof of Lemma 3.5 is based on this result together with Corollary 3.4 below.
Lemma 3.3 Let $i, j, r, s \in \{1, \ldots, n\}$ such that $i < j$, $r < s$, $\{i, j\} \neq \{r, s\}$, and $\{i, j\} \cap \{r, s\} \neq \emptyset$. Let $\mathcal{M}[i, j, r, s]$ be the free monoid freely generated by $\Upsilon_{ij} \cup \Upsilon_{rs}$, and let $\overline{\nu} : \mathcal{M}[i, j, r, s] \to \mathbb{Z}[B_n]$ be the homomorphism defined by $\overline{\nu}(u) = u - 1$ for all $u \in \Upsilon_{ij} \cup \Upsilon_{rs}$. Then $\overline{\nu}$ is injective.

Corollary 3.4 Let $i, j \in \{1, \ldots, n\}$ such that $i < j$. Let $\mathcal{M}[i, j]$ be the free monoid freely generated by $\Upsilon_{ij}$, and let $\overline{\nu} : \mathcal{M}[i, j] \to \mathbb{Z}[B_n]$ be the homomorphism defined by $\overline{\nu}(u) = u - 1$ for all $u \in \Upsilon_{ij}$. Then $\overline{\nu}$ is injective.

Lemma 3.5 Let $i, j, r, s \in \{1, \ldots, n\}$ such that $i < j$, $r < s$, and $\{i, j\} \cap \{r, s\} = \emptyset$. (In particular, we have $n \geq 4$.) Let $\Omega[i, j, r, s]$ be the graph defined as follows.

- $\Upsilon_{ij} \cup \Upsilon_{rs}$ is the set of vertices of $\Omega[i, j, r, s]$;
- $\{u, v\}$ is an edge of $\Omega[i, j, r, s]$ if and only if we have $uv = vu$ in $B_n$.

Let $\mathcal{M}[i, j, r, s] = \mathcal{M}(\Omega[i, j, r, s])$, and let $\overline{\nu} : \mathcal{M}[i, j, r, s] \to \mathbb{Z}[B_n]$ be the homomorphism defined by $\overline{\nu}(u) = u - 1$ for all $u \in \Upsilon_{ij} \cup \Upsilon_{rs}$. Then $\overline{\nu}$ is injective.

Proof of Theorem 1.3 Recall the decomposition

$$\mathbb{Z}[B_n] = \bigoplus_{k \in \mathbb{Z}} \mathbb{Z}[B_n^{(k)}]$$

(1)

given in the proof of Theorem 1.1, where $B_n^{(k)} = \{\beta \in B_n; \deg(\beta) = k\}$, and $\mathbb{Z}[B_n^{(k)}]$ is the free abelian group freely generated by $B_n^{(k)}$. Note that $\deg(u) = 2$ for all $u \in \Upsilon$.

Let $\alpha \in \mathcal{M}(\Omega)$. We write $\alpha = u_1 u_2 \ldots u_l$, where $u_i \in \Upsilon$ for all $i = 1, \ldots, l$. Define the length of $\alpha$ to be $|\alpha| = l$. We denote by $\overline{\alpha}$ the element of $B_n$ represented by $\alpha$ (ie, $\overline{\alpha} = u_1 u_2 \ldots u_l$ in $B_n$). Let $[1, l] = \{1, 2, \ldots, l\}$. Define a subindex of $[1, l]$ to be a sequence $I = (i_1, i_2, \ldots, i_q)$ such that $i_1, i_2, \ldots, i_q \in [1, l]$, and $i_1 < i_2 < \cdots < i_q$. The notation $I < [1, l]$ means that $I$ is a subindex of $[1, l]$. The length of $I$ is $|I| = q$. For $I = (i_1, i_2, \ldots, i_q) < [1, l]$, we set $\alpha(I) = u_{i_1} u_{i_2} \ldots u_{i_q} \in \mathcal{M}(\Omega)$ and $\overline{\alpha}(I)$ denotes the corresponding element of $B_n^{(2q)}$.

Observe that the decomposition of $\nu(\alpha)$ with respect to the direct sum (1) is:

$$\nu(\alpha) = \sum_{q=0}^{l} (-1)^{l-q} \sum_{I < [1, l], |I| = q} \overline{\alpha}(I),$$

(2)

and
\[
\sum_{I \prec [1, l], |I| = q} \bar{\alpha}(I) \in \mathbb{Z}[B_n^{(2q)}],
\]
for all \( q = 0, 1, \ldots, l \).

Let \( \alpha' = u'_1 u'_2 \ldots u'_l \in \mathcal{M}(\Omega) \) such that \( \nu(\alpha) = \nu(\alpha') \). The decomposition given in (2) shows that \( k = l \) and
\[
\sum_{I \prec [1, l], |I| = q} \bar{\alpha}(I) = \sum_{I \prec [2, l], |I| = q} \bar{\alpha}'(I),
\]
for all \( q = 0, 1, \ldots, l \).

We prove that \( \alpha = \alpha' \) by induction on \( l \). The cases \( l = 0 \) and \( l = 1 \) being obvious, we assume \( l \geq 2 \).

Suppose first that \( u'_1 = u_1 \). We prove
\[
\sum_{I \prec [2, l], |I| = q} \bar{\alpha}(I) = \sum_{I \prec [2, l], |I| = q} \bar{\alpha}'(I)
\]
by induction on \( q \). The case \( q = 0 \) being obvious, we assume \( q \geq 1 \). Then
\[
\sum_{I \prec [2, l], |I| = q} \bar{\alpha}(I)
= \sum_{I \prec [1, l], |I| = q} \bar{\alpha}(I) - u_1 \cdot \sum_{I \prec [2, l], |I| = q-1} \bar{\alpha}(I)
= \sum_{I \prec [1, l], |I| = q} \bar{\alpha}'(I) - u_1 \cdot \sum_{I \prec [2, l], |I| = q-1} \bar{\alpha}'(I) \quad \text{(by induction and (3))}
= \sum_{I \prec [2, l], |I| = q} \bar{\alpha}'(I).
\]

Let \( \alpha_1 = u_2 \ldots u_l \) and \( \alpha'_1 = u'_2 \ldots u'_l \). By (4), we have
\[
\nu(\alpha_1) = \sum_{q=0}^{l-1} (-1)^{l-1-q} \sum_{I \prec [2, l], |I| = q} \bar{\alpha}(I)
= \sum_{q=0}^{l-1} (-1)^{l-1-q} \sum_{I \prec [2, l], |I| = q} \bar{\alpha}'(I) = \nu(\alpha'_1)
\]
thus, by the inductive hypothesis, \( \alpha_1 = \alpha'_1 \), therefore \( \alpha = u_1 \alpha_1 = u_1 \alpha'_1 = \alpha' \).
Now, we consider the general case. (3) applied to \( q = 1 \) gives
\[
\sum_{i=1}^{l} u_i = \sum_{i=1}^{l} u'_i.
\]
(5)
So, there exists \( k \in \{1, \ldots, l\} \) such that \( u'_k = u_1 \) and \( u'_i \neq u_1 \) for all \( i = 1, \ldots, k - 1 \). We prove that, for \( 1 \leq i \leq k - 1 \), \( u'_i \) and \( u_1 = u'_k \) multiplicatively commute (in \( B_n \) or, equivalently, in \( \mathcal{M}(\Omega) \)). It follows that \( \alpha' = u_1 u'_1 \cdots u'_{k-1} u_{k+1} \cdots u'_l \), and hence, by the case \( u_1 = u'_1 \) considered before, \( \alpha = \alpha' \).

Fix some \( t \in \{1, \ldots, k-1\} \). Let \( i, j, r, s \in \{1, \ldots, n\} \) such that \( i < j, r < s \), \( u_1 = u'_k \in \Upsilon_{ij} \), and \( u'_t \in \Upsilon_{rs} \). There are three possible cases that we handle simultaneously:

1. \( \{i, j\} = \{r, s\} \);
2. \( \{i, j\} \neq \{r, s\} \) and \( \{i, j\} \cap \{r, s\} \neq \emptyset \);
3. \( \{i, j\} \cap \{r, s\} = \emptyset \).

Let \( \Omega[i, j, r, s] \) be the graph defined as follows.

- \( \Upsilon_{ij} \cup \Upsilon_{rs} \) is the set of vertices of \( \Omega[i, j, r, s] \);
- \( \{u, v\} \) is an edge of \( \Omega[i, j, r, s] \) if and only if we have \( uv = vu \) in \( B_n \).

Let \( \mathcal{M}[i, j, r, s] = \mathcal{M}(\Omega[i, j, r, s]) \), and let \( \bar{\nu} : \mathcal{M}[i, j, r, s] \rightarrow \mathbb{Z}[B_n] \) be the homomorphism defined by \( \bar{\nu}(u) = u-1 \) for all \( u \in \Upsilon_{ij} \cup \Upsilon_{rs} \). Note that, by Corollary 3.4 and Lemma 3.3, \( \Omega[i, j, r, s] \) has no edge and \( \mathcal{M}[i, j, r, s] \) is a free monoid in Cases 1 and 2. Moreover, the homomorphism \( \bar{\nu} \) is injective by Lemmas 3.3 and 3.5 and by Corollary 3.4.

Let \( a_1 = 1, a_2, \ldots, a_p \in \{1, l\} \), \( a_1 < a_2 < \cdots < a_p \), be the indices such that \( u_{a_\xi} \in \Upsilon_{ij} \cup \Upsilon_{rs} \) for all \( \xi = 1, 2, \ldots, p \). Let \( I_0 = (a_1, a_2, \ldots, a_p) \), and let \( \alpha(I_0) = u_{a_1} u_{a_2} \cdots u_{a_p} \in \mathcal{M}[i, j, r, s] \). (It is true that \( \mathcal{M}[i, j, r, s] \) is a submonoid of \( \mathcal{M}(\Omega) \), but this fact is not needed for our purpose. So, we should consider \( \alpha(I_0) \) as an element of \( \mathcal{M}[i, j, r, s] \), and not as an element of \( \mathcal{M}(\Omega) \).) Recall that, for \( \beta \in PB_n \), we denote by \([\beta] \) the element of \( H_1(PB_n) \) represented by \( \beta \). Recall also that \( H_1(PB_n) \) is a free abelian group freely generated by \( \{[A_{ij}]; 1 \leq i < j \leq n\} \). Observe that
\[
\bar{\nu}(\alpha(I_0)) = \sum_{q=0}^{p} \sum_{I \subset \{1, l\}, |I| = q, \alpha(I) \in \mathbb{Z}[A_{ij}] + \mathbb{Z}[A_{rs}]} (-1)^{p-q} \bar{\nu}(I).
\]
(6)
Let $b_1, \ldots, b_p \in [1, l]$, $b_1 < b_2 < \cdots < b_p$, be the indices such that $u'_{b_1} \in T_{i,j} \cup T_{i,s}$ for all $\xi = 1, 2, \ldots, p$. (Clearly, (5) implies that we have as many $a_\xi$’s as $b_\xi$’s.) Note that $t, k \in \{b_1, \ldots, b_p\}$. Let $I'_0 = (b_1, b_2, \ldots, b_p)$, and let $\alpha'(I'_0) = u'_{b_1} u'_{b_2} \ldots u'_{b_p} \in \mathcal{M}[i,j,r,s]$. By (3) we have

$$\sum_{I \in [1,l], |I| = q, |\bar{\alpha}(I)| \in \mathbb{Z}[A_{ij}]+\mathbb{Z}[A_{rs}]} \bar{\alpha}(I) = \sum_{I' \in [1,l], |I'| = q, |\bar{\alpha}'(I')| \in \mathbb{Z}[A_{ij}]+\mathbb{Z}[A_{rs}]} \bar{\alpha}'(I'),$$

for all $q \in \mathbb{N}$, thus, by (6), $\bar{\nu}(\alpha(I_0)) = \bar{\nu}(\alpha'(I'_0))$. Since $\bar{\nu}$ is injective, it follows that $\alpha(I_0) = \alpha'(I'_0)$, and we conclude by Lemma 3.1 that $u'_t$ and $u'_k$ commute. \hfill $\square$

## 4 Proof of Lemma 3.3

As pointed out in the previous section, the key point of the proof of Lemma 3.3 is the following result.

**Proposition 4.1** Let $F(X)$ be a free group freely generated by some set $X$, let $Y = \{g x g^{-1}; \ g \in F(X) \text{ and } x \in X\}$, let $F^+(Y)$ be the free monoid freely generated by $Y$, and let $\nu: F^+(Y) \to \mathbb{Z}[F(X)]$ be the homomorphism defined by $\nu(y) = y - 1$ for all $y \in Y$. Then $\nu$ is injective.

First, we shall prove Lemmas 4.2, 4.3, and 4.4 that are preliminary results to the proof of Proposition 4.1.

Let $\deg: F(X) \to \mathbb{Z}$ be the homomorphism defined by $\deg(x) = 1$ for all $x \in X$. Write $\mathcal{A} = \mathbb{Z}[F(X)]$. For $k \in \mathbb{Z}$, let $F_k(X) = \{g \in F(X); \deg(g) \geq k\}$, and let $\mathcal{A}_k = \mathbb{Z}[F_k(X)]$ be the free $\mathbb{Z}$–module freely generated by $F_k(X)$. The family $\{\mathcal{A}_k\}_{k \in \mathbb{Z}}$ is a filtration of $\mathcal{A}$ compatible with the multiplication, that is:

- $\mathcal{A}_k \subset \mathcal{A}_l$ if $k \geq l$;
- $\mathcal{A}_p \cdot \mathcal{A}_q \subset \mathcal{A}_{p+q}$ for all $p, q \in \mathbb{Z}$;
- $1 \in \mathcal{A}_0$.

Moreover, this filtration is a separating filtration, that is:

- $\cap_{k \in \mathbb{Z}} \mathcal{A}_k = \{0\}$.

Let $\hat{\mathcal{A}}$ denote the completion of $\mathcal{A}$ with respect to this filtration. For $k \in \mathbb{Z}$, we write $F^{(k)}(X) = \{g \in F(X); \deg(g) = k\}$, and we denote by $\mathcal{A}^{(k)} = \mathbb{Z}[F^{(k)}(X)]$ the free $\mathbb{Z}$–module freely generated by $F^{(k)}(X)$. Then any element of $\hat{\mathcal{A}}$ can be

The proof of Birman's conjecture on singular braid monoids

uniquely represented by a formal series \( \sum_{k=d}^{+\infty} P_k \), where \( d \in \mathbb{Z} \) and \( P_k \in \mathcal{A}^{(k)} \) for all \( k \geq d \).

We take a copy \( G_x \) of \( \mathbb{Z} \times \mathbb{Z} \) generated by \( \{ x, x \hat{x} \} \), for all \( x \in X \), and we set \( \hat{G} = \ast_{x \in X} G_x \). Let \( \mathcal{U}(\hat{A}) \) denote the group of units of \( \hat{A} \). Then there is a homomorphism \( \hat{\eta}: \hat{G} \to \mathcal{U}(\hat{A}) \) defined by
\[
\hat{\eta}(x) = x, \quad \hat{\eta}(\hat{x}) = x - 1, \quad \text{for } x \in X.
\]

Note that
\[
\hat{\eta}(x^{-1}) = -\sum_{k=0}^{+\infty} x^k, \quad \text{for } x \in X.
\]

The homomorphism \( \hat{\eta} \) defined above is a sort of Magnus expansion and the proof of the following lemma is strongly inspired by the proof of [6], Ch. II, § 5, Thm. 1.

**Lemma 4.2** The homomorphism \( \hat{\eta}: \hat{G} \to \mathcal{U}(\hat{A}) \) is injective.

**Proof** Let \( g \in \hat{G} \). Define the normal form of \( g \) to be the finite sequence \((g_1, g_2, \ldots, g_l)\) such that:

- for all \( i \in \{1, \ldots, l\} \), there exists \( x_i \in X \) such that \( g_i \in G_{x_i} \setminus \{1\} \);
- \( x_i \neq x_{i+1} \) for all \( i = 1, \ldots, l-1 \);
- \( g = g_1 g_2 \cdots g_l \).

Clearly, such an expression for \( g \) always exists and is unique. The length of \( g \) is defined to be \( \text{lg}(g) = l \).

Let \( (p, q) \in \mathbb{Z} \times \mathbb{Z} \), \( (p, q) \neq (0, 0) \). Write
\[
(t - 1)^{pt^n} = \sum_{k=d}^{+\infty} c_{kpq} t^k,
\]
where \( d \in \mathbb{Z} \) and \( c_{kpq} \in \mathbb{Z} \) for all \( k \geq d \). We show that there exists \( a \geq d \) such that \( a \neq 0 \) and \( c_{apq} \neq 0 \). If \( q \neq 0 \), then \( a = q \neq 0 \) and \( c_{qpq} = \pm 1 \neq 0 \). If \( q = 0 \), then \( a = 1 \neq 0 \) and \( c_{1p0} = \pm p \neq 0 \).

Let \( g \in \hat{G} \), \( g \neq 1 \). Let \((x_1^{p_1} x_2^{p_2} \cdots, x_l^{p_l} x_l^{p_l})\) be the normal form of \( g \). We have
\[
\hat{\eta}(g) = (x_1 - 1)^{p_1} x_1^{p_1} (x_2 - 1)^{p_2} x_2^{p_2} \cdots (x_l - 1)^{p_l} x_l^{p_l}
= \sum_{k_1 \geq d_1, \ldots, k_l \geq d_t, \quad k < d_1} c_{k_1, p_1, q_1} c_{k_1, p_2, q_2} \cdots c_{k_1, p_l, q_l} \cdot x_1^{k_1} x_2^{k_2} \cdots x_l^{k_l}.
\]
By the above observation, there exist \( a_1, a_2, \ldots, a_l \in \mathbb{Z} \setminus \{0\} \) such that \( c_{a_i, p_i, q_i} \neq 0 \) for all \( i = 1, \ldots, l \). Now, we show that \( x_1^{k_1} \cdots x_i^{k_i} \neq x_1^{a_1} \cdots x_i^{a_i} \) if \( (k_1, \ldots, k_l) \neq (a_1, \ldots, a_l) \). This implies that the coefficient of \( x_1^{a_1} \cdots x_i^{a_i} \) in \( \tilde{\eta}(g) \) is \( c_{a_1, p_1, q_1} \cdots c_{a_l, p_l, q_l} \neq 0 \), thus \( \tilde{\eta}(g) \neq 1 \).

Since \( (x_1^{p_1} x_1^{q_1}, \ldots, x_1^{p_l} x_1^{q_l}) \) is the normal form of \( g \), we have \( x_i \neq x_{i+1} \) for all \( i = 1, \ldots, l - 1 \), thus \( (x_1^{a_1}, \ldots, x_1^{a_l}) \) is the normal form of \( x_1^{a_1} \cdots x_i^{a_i} \cdots x_1^{a_l} \). Suppose \( k_i \neq 0 \) for all \( i = 1, \ldots, l \). Then \( (x_1^{k_1}, \ldots, x_1^{k_l}) \) is the normal form of \( x_1^{k_1} \cdots x_i^{k_i} \cdots x_1^{k_l} \), therefore \( x_1^{k_1} \cdots x_i^{k_i} \neq x_1^{a_1} \cdots x_i^{a_i} \) if \( (k_1, \ldots, k_l) \neq (a_1, \ldots, a_l) \). Suppose there exists \( i \in \{1, \ldots, l\} \) such that \( k_i = 0 \). Then

\[
\log(x_1^{k_1} \cdots x_i^{k_i}) < l = \log(x_1^{a_1} \cdots x_i^{a_i})
\]

thus \( x_1^{k_1} \cdots x_i^{k_i} \neq x_1^{a_1} \cdots x_i^{a_i} \).

For each \( x \in X \), we take a copy \( SG_x \) of \( \mathbb{Z} \times \mathbb{N} \) generated as a monoid by \( \{x, x^{-1}, \hat{x}\} \), and we set \( SG = \ast_{x \in X} SG_x \). Then there is a homomorphism \( \eta: SG \to \mathbb{Z}[F(X)] \) defined by

\[
\eta(x^{\pm 1}) = x^{\pm 1}, \quad \eta(\hat{x}) = x - 1, \quad \text{for } x \in X.
\]

**Lemma 4.3** The homomorphism \( \eta: SG \to \mathbb{Z}[F(X)] \) is injective.

**Proof** We have \( SG \subset \tilde{G} \), and, since \( \{A_k\}_{k \in \mathbb{Z}} \) is a separating filtration, \( A = \mathbb{Z}[F(X)] \) is a subalgebra of \( \tilde{A} \). Now, observe that \( \eta: SG \to \mathbb{Z}[F(X)] \) is the restriction of \( \tilde{\eta} \) to \( SG \), thus, by Lemma 4.2, \( \eta \) is injective.

Let \( \hat{Y} = \{g \hat{x} g^{-1}: g \in F(X) \text{ and } x \in X\} \subset SG \), and let \( F^+(\hat{Y}) \) be the free monoid freely generated by \( \hat{Y} \). The proof of the following lemma is left to the reader. A more general statement can be found in [9].

**Lemma 4.4** We have \( SG = F^+(\hat{Y}) \rtimes F(X) \).

Now, we can prove Proposition 4.1, and, consequently, Lemma 3.3.

**Proof of Proposition 4.1** Let \( \tilde{\nu} : F^+(\hat{Y}) \to \mathbb{Z}[F(X)] \) be the restriction of \( \eta: SG = F^+(Y) \rtimes F(X) \to \mathbb{Z}[F(X)] \) to \( F^+(\hat{Y}) \), and let \( \varphi : F^+(\hat{Y}) \to F^+(Y) \) be the epimorphism defined by \( \varphi(g \hat{x} g^{-1}) = g x g^{-1} \) for all \( g \in F(X) \) and \( x \in X \).

(1) The proof that \( \varphi \) is well-defined is left to the reader. The homomorphism \( \tilde{\nu} \) is injective (Lemma 4.3), \( \varphi \) is a surjection, and \( \tilde{\nu} = \nu \circ \varphi \), thus \( \varphi \) is an isomorphism and \( \nu \) is injective.

*Geometry \\& Topology, Volume 8 (2004)*
Proof of Lemma 3.3 Take $\zeta \in \text{Sym}_n$ such that $\zeta(\{i,j\}) = \{1, n\}$ and $\zeta(\{r,s\}) = \{2, n\}$. Choose $\beta \in B_n$ such that $\theta(\beta) = \zeta$. Then $\beta \iota_{ij} \beta^{-1} = \iota_{1n}$ and $\beta \iota_{rs} \beta^{-1} = \iota_{2n}$. So, up to conjugation by $\beta$ if necessary, we may assume that $\{i,j\} = \{1, n\}$ and $\{r,s\} = \{2, n\}$.

Let $F$ be the subgroup of $PB_n$ generated by $\{A_i; 1 \leq i \leq n-1\}$. We have:

1. $F$ is a free group freely generated by $\{A_i; 1 \leq i \leq n-1\}$;
2. $PB_n = F \times PB_{n-1}$;
3. $\iota_{in} = \{gA_{1n}g^{-1}; g \in F\}$ for all $i = 1, \ldots, n-1$.

(1) and (2) are well-known and are direct consequences of the presentation of $PB_n$ given in Section 3, and (3) follows from the fact that the conjugacy class of $A_n$ in $F$ is invariant by the action of $PB_{n-1}$.

Let $\Upsilon' = \bigcup_{i=1}^{n-1} \iota_{in}$, and let $F^+(\Upsilon')$ be the free monoid freely generated by $\Upsilon'$. By Proposition 4.1, the homomorphism $\nu ': F^+(\Upsilon') \to \mathbb{Z}[F]$, defined by $\nu '(u) = u - 1$ for all $u \in \Upsilon'$, is injective. Recall that $M[1, n, 2, n]$ denotes the free monoid freely generated by $\iota_{1n} \cup \iota_{2n}$. Then $M[1, n, 2, n] \subset F^+(\Upsilon')$, $\mathbb{Z}[F] \subset \mathbb{Z}[B_n]$, and $\nu : M[1, n, 2, n] \to \mathbb{Z}[B_n]$ is the restriction of $\nu '$ to $M[1, n, 2, n]$, thus $\nu$ is injective.

5 Proof of Lemma 3.5

We assume throughout this section that $n \geq 4$. As pointed out in Section 3, one of the main ingredients of the proof of Lemma 3.5 is the following result.

Proposition 5.1 Let $F(X)$ be a free group freely generated by some set $X$, let $x_0 \in X$, and let $\rho : F(X) \to F(X)$ be an automorphism which fixes $x_0$ and leaves $F(X \setminus \{x_0\})$ invariant (where $F(X \setminus \{x_0\})$ denotes the subgroup of $F(X)$ (freely) generated by $X \setminus \{x_0\}$). Let $y_1, \ldots, y_l \in \{gx_0g^{-1}; g \in F(X)\}$. If $\rho(y_1y_2 \ldots y_l) = y_1y_2 \ldots y_l$, then $\rho(y_i) = y_i$ for all $i = 1, \ldots, l$.

Proof Let $Z = \{hx_0h^{-1}; h \in F(X \setminus \{x_0\})\}$, and let $F(Z)$ be the subgroup of $F(X)$ generated by $Z$. Observe that $Z$ freely generates $F(Z)$, $\rho$ permutes the elements of $Z$, and $\{gx_0g^{-1}; g \in F(X)\} = \{\beta x_0 \beta^{-1}; \beta \in F(Z)\}$ and $z \in Z$.

For $f \in F(Z)$, we denote by $\text{lg}(f)$ the word length of $f$ with respect to $Z$. For $f, g \in F(Z)$, we write $fg = f * g$ if $\text{lg}(fg) = \text{lg}(f) + \text{lg}(g)$. Note that, if $fg = f * g$, then $\rho(fg) = \rho(f) * \rho(g)$. Moreover, if $fg = f * g$ and $\rho(fg) = fg$, then $\rho(f) = f$ and $\rho(g) = g$.
Let $g_0 = y_1 y_2 \ldots y_l$. Recall that we are under the assumption that $\rho(g_0) = g_0$. For $i = 1, \ldots, l$, let $\beta_i \in F(Z)$ and $z_i \in Z$ such that $y_i = \beta_i * z_i * \beta_i^{-1}$. Now, we prove that $\rho(y_i) = y_i$ for all $i = 1, \ldots, l$ by induction on $\sum_{i=1}^l \lg(y_i) = l + 2 \sum_{i=1}^l \lg(\beta_i)$.

We have three cases to study.

**Case 1** There exists $t \in \{1, \ldots, l - 1\}$ such that $\beta_{t+1} = \beta_t * z_t^{-1} * \gamma_t$, where $\gamma_t \in F(Z)$.

Let $y'_{t+1} = \beta_t \gamma_t z_t^{-1} \gamma_t^{-1} \beta_t^{-1} = y_t y_{t+1}^{-1}$. Observe that $g_0 = y_1 \ldots y_{t-1} y_t y_{t+1} \ldots y_l$.

We have $\lg(\beta_t \gamma_t) < \lg(\beta_{t+1})$, thus, by the inductive hypothesis, $\rho(y_i) = y_i$ for all $i = 1, \ldots, t-1, t, t+2, \ldots, l$, and $\rho(y'_{t+1}) = y'_{t+1}$. Moreover, since $y_{t+1} = y_{t+1}^{-1} y'_{t+1} y_{t+1}$, we also have $\rho(y_{t+1}) = y_{t+1}$.

**Case 2** There exists $t \in \{2, \ldots, l\}$ such that $\beta_{t-1} = \beta_t * z_t * \gamma_t$, where $\gamma_t \in F(Z)$.

Then we prove that $\rho(y_i) = y_i$ for all $i = 1, \ldots, l$ as in the previous case.

**Case 3** For all $t \in \{1, \ldots, l\}$ and for all $\gamma_t \in F(Z)$ we have $\beta_{t+1} \neq \beta_t * z_t^{-1} * \gamma_t$ and $\beta_{t-1} \neq \beta_t * z_t * \gamma_t$.

We observe that

$$g_0 = \beta_1 * z_1 * \beta_1^{-1} \beta_2 * z_2 * \cdots * \beta_{t-1}^{-1} \beta_t * z_t * \beta_t^{-1}.$$

Since $\rho(g_0) = g_0$, it follows that $\rho(\beta_1) = \beta_1$, $\rho(z_1) = z_1$, $\rho(\beta_1^{-1} \beta_2) = \beta_1^{-1} \beta_2$, $\rho(z_2) = z_2$, ..., $\rho(\beta_{t-2}^{-1} \beta_{t-1}) = \beta_{t-2}^{-1} \beta_{t-1}$, $\rho(z_{t-1}) = z_{t-1}$, and $\rho(\beta_{t-1}^{-1}) = \beta_{t-1}^{-1}$. This clearly implies that $\rho(y_i) = y_i$ for all $i = 1, \ldots, l$.

**Corollary 5.2** Let $u \in \Upsilon_{12}$ and $v_1, \ldots, v_l \in \Upsilon_{n-1,n}$. If $u$ commutes with $v_1 v_2 \ldots v_l$ (in $B_n$), then $u$ commutes with $v_i$ for all $i = 1, \ldots, l$.

**Proof** Let $\alpha_0 \in PB_n$ such that $u = \alpha_0 A_1^{-1} A_0^{-1}$. Up to conjugation of $v_1, \ldots, v_l$ by $\alpha_0^{-1}$ if necessary, we can suppose that $\alpha_0 = 1$ and $u = A_{12}$.

Recall that $F$ denotes the subgroup of $PB_n$ generated by $\{A_{i,n}; 1 \leq i \leq n-1\}$. Recall also that:

- $F$ is a free group freely generated by $\{A_{i,n}; 1 \leq i \leq n-1\}$
- $PB_n = F \rtimes PB_{n-1}$

*Geometry \\& Topology, Volume 8 (2004)*
The proof of Birman’s conjecture on singular braid monoids

Let \( \rho: F \to F \) be the action of \( A_{12} \) by conjugation on \( F \) (namely, \( \rho(g) = A_{12}gA_{12}^{-1} \)). Observe that \( \rho(A_{n-1,n}) = A_{n-1,n} \) and the subgroup of \( F \) generated by \( \{A_i: 1 \leq i \leq n-2\} \) is invariant by \( \rho \). Then, Proposition 5.1 shows that \( \rho(v_i) = v_i \) for all \( i = 1, \ldots, l \) if \( \rho(v_1v_2 \ldots v_l) = v_1v_2 \ldots v_l \).

Now, we can prove Lemma 3.5.

**Proof of Lemma 3.5** Take \( \zeta \in \text{Sym}_n \) such that \( \zeta(\{i,j\}) = \{1,2\} \) and \( \zeta(\{r,s\}) = \{n-1,n\} \). Choose \( \beta \in B_n \) such that \( \theta(\beta) = \zeta \). Then \( \beta \tau_{ij}^{-1} = \tau_{12} \) and \( \beta \tau_{rs}^{-1} = \tau_{n-1,n} \). So, up to conjugation by \( \beta \) if necessary, we may assume that \( \{i,j\} = \{1,2\} \) and \( \{r,s\} = \{n-1,n\} \).

We use the same notations as in the proof of Theorem 1.3. Let \( \alpha \in \mathcal{M}[1,2,n-1,n] \). We write \( \alpha = u_1u_2 \ldots u_l \), where \( u_i \in \mathcal{T}_{12} \cup \mathcal{T}_{n-1,n} \) for all \( i = 1, \ldots, l \). Define the length of \( \alpha \) to be \( |\alpha| = l \). We denote by \( \hat{\alpha} \) the element of \( B_n \) represented by \( \alpha \). Let \( [1,l] = \{1,2,\ldots,l\} \). Define a subindex of \( [1,l] \) to be a sequence \( I = (i_1,i_2,\ldots,i_q) \) such that \( i_1,i_2,\ldots,i_q \in [1,l] \) and \( i_1 < i_2 < \cdots < i_q \). The notation \( I \prec [1,l] \) means that \( I \) is a subindex of \( [1,l] \). The length of \( I \) is \( |I| = q \). For \( I = (i_1,i_2,\ldots,i_q) \prec [1,l] \), we set \( \alpha(I) = u_{i_1}u_{i_2} \ldots u_{i_q} \in \mathcal{M}[1,2,n-1,n] \).

Observe that

\[
\tilde{\nu}(\alpha) = \sum_{q=0}^{l} (-1)^{l-q} \sum_{I \prec [1,l], |I| = q} \hat{\alpha}(I),
\]

and

\[
\sum_{I \prec [1,l], |I| = q} \hat{\alpha}(I) \in \mathbb{Z}[B_n(2q)],
\]

for all \( q = 0,1,\ldots,l \).

Let \( \alpha' = u'_1u'_2 \ldots u'_k \in \mathcal{M}[1,2,n-1,n] \) such that \( \tilde{\nu}(\alpha) = \tilde{\nu}(\alpha') \). As in the proof of Theorem 1.3, the decomposition given in \( (7) \) shows that \( k = l \) and

\[
\sum_{I \prec [1,l], |I| = q} \hat{\alpha}(I) = \sum_{I \prec [1,l], |I| = q} \hat{\alpha'}(I),
\]

for all \( q = 0,1,\ldots,l \).

We prove that \( \alpha = \alpha' \) by induction on \( l \). The cases \( l = 0 \) and \( l = 1 \) being obvious, we assume \( l \geq 2 \).


*Geometry & Topology, Volume 8 (2004)*
Assume first that \( u'_1 = u_1 \). Then, by the same argument as in the proof of Theorem 1.3, \( \alpha = \alpha' \).

Now, we consider the general case. (8) applied to \( q = 1 \) gives

\[
\sum_{i=1}^{l} u_i = \sum_{i=1}^{l} u'_i. \tag{9}
\]

It follows that there exists a permutation \( \zeta \in \text{Sym}_l \) such that \( u_i = u'_i(i) \) for all \( i = 1, \ldots, l \). (Note that the permutation \( \zeta \in \text{Sym}_l \) is not necessarily unique. Actually, \( \zeta \) is unique if and only if \( u_i \neq u_j \) for all \( i \neq j \).

Let \( a_1, a_2, \ldots, a_p \in [1, l] \), \( a_1 < a_2 < \cdots < a_p \), be the indices such that \( u_{a_1} \in T_{12} \) for all \( \xi = 1, \ldots, p \). Let \( I_0 = (a_1, a_2, \ldots, a_p) \). Recall that, for \( \beta \in PB_n \), we denote by \([\beta]\) the element of \( H_1(PB_n) \) represented by \( \beta \). Recall also that \( H_1(PB_n) \) is a free abelian group freely generated by \( \{[A_i]; 1 \leq i < j \leq n\} \).

Observe that \( \alpha(I_0) \in M[1, 2] \) and

\[
\bar{\nu}(\alpha(I_0)) = \sum_{k=0}^{p} (-1)^{p-k} \sum_{I \subseteq [1, l], |I|=k, \bar{\alpha}(I) \in \mathbb{Z}[A_{12}]} \bar{\alpha}(I). \tag{10}
\]

Let \( a'_1, a'_2, \ldots, a'_p \in [1, l] \), \( a'_1 < a'_2 < \cdots < a'_p \), be the indices such that \( u'_{a'_1} \in T_{12} \) for all \( \xi = 1, \ldots, p \). Note that \( \{\zeta(a'_1), \zeta(a'_2), \ldots, \zeta(a'_p)\} = \{a_1, a_2, \ldots, a_p\} \).

Let \( I'_0 = (a'_1, a'_2, \ldots, a'_p) \). By (8), we have

\[
\sum_{I \subseteq [1, l], |I|=k, \bar{\alpha}(I) \in \mathbb{Z}[A_{12}]} \bar{\alpha}(I) = \sum_{I \subseteq [1, l], |I|=k, \bar{\alpha}'(I') \in \mathbb{Z}[A_{12}]} \bar{\alpha}'(I'), \tag{11}
\]

for all \( k \in \mathbb{N} \), thus, by (10), \( \bar{\nu}(\alpha(I_0)) = \bar{\nu}(\alpha'(I'_0)) \). By Corollary 3.4, it follows that \( \alpha(I_0) = \alpha'(I'_0) \). So, \( u'_{a'_i} = u_{a_i} \) for all \( i = 1, \ldots, p \), and the permutation \( \zeta \in \text{Sym}_l \) can be chosen so that \( \zeta(a'_i) = a_i \) for all \( i = 1, \ldots, p \).

Let \( b_1, b_2, \ldots, b_q \in [1, l] \), \( b_1 < b_2 < \cdots < b_q \), be the indices such that \( u_{b_i} \in T_{n-1, n} \) for all \( \xi = 1, \ldots, q \). Note that \( [1, l] = \{a_1, \ldots, a_p, b_1, \ldots, b_q\} \). Let \( J_0 = (b_1, b_2, \ldots, b_q) \). Let \( b'_1, b'_2, \ldots, b'_q \in [1, l] \), \( b'_1 < b'_2 < \cdots < b'_q \), be the indices such that \( u'_{b'_i} \in T_{n-1, n} \) for all \( \xi = 1, \ldots, q \), and let \( J'_0 = (b'_1, b'_2, \ldots, b'_q) \). We also have \( \alpha(J_0) = \alpha'(J'_0) \in M[n-1, n] \), \( u_{b_i} = u'_{b'_i} \) for all \( i = 1, \ldots, q \), and \( \zeta \) can be chosen so that \( \zeta(b'_i) = b_i \) for all \( i = 1, \ldots, q \).

Without loss of generality, we can assume that \( u_1 \in \mathcal{T}_{12} \) (namely, \( a_1 = 1 \)). Let \( i \in \{1, \ldots, p\} \). We set:

\[
S(i) = \begin{cases} 
0 & \text{if } a_i < b_i, \\
 j & \text{if } b_j < a_i < b_{j+1}, \\
 q & \text{if } b_q < a_i.
\end{cases}
\]

\[
T(i) = \begin{cases} 
0 & \text{if } a'_i < b'_i, \\
 j & \text{if } b'_j < a'_i < b'_{j+1}, \\
 q & \text{if } b'_q < a'_i.
\end{cases}
\]

Note that \( \alpha' = u'_1 \ldots u'_{T(1)} u'_1 \ldots u_{b_{T(1)}} u_{a_1} \ldots \). Now, we show that \( u_1 = u_{a_1} \) commutes with \( u_{b_i} \) for all \( i = 1, \ldots, T(1) \). It follows that \( \alpha' = u_1 u_{b_1} \ldots u_{b_{T(1)}} \ldots \), and hence, by the case \( u'_1 = u_1 \) considered before, \( \alpha = \alpha' \).

Let

\[
v_i = u_{b_{S(i)}} u_{a_i} u_{b_{S(i)}}^{-1} \ldots u_{b_1} \in \mathcal{T}_{12},
\]

\[
v'_i = u_{b_{S(i)}} u_{a_i} u_{b_{S(i)}}^{-1} \ldots u_{b_1} \in \mathcal{T}_{12},
\]

for all \( i = 1, \ldots, p \), and let

\[
\gamma = v_1 v_2 \ldots v_p \in \mathcal{M}[1, 2], \quad \gamma' = v'_1 v'_2 \ldots v'_p \in \mathcal{M}[1, 2].
\]

Observe that

\[
\bar{\nu}(\gamma) = \left( \sum_{k=0}^{p} (-1)^{p-k} \sum_{I \prec [1, \ell], \ell = k+q, \lfloor \bar{a}(I) \rfloor = k|A_2| + q|A_{n-1}|} \bar{\alpha}(I) \bar{\alpha}(J_0)^{-1} \right),
\]

\[
\bar{\nu}(\gamma') = \left( \sum_{k=0}^{p} (-1)^{p-k} \sum_{I \prec [1, \ell], \ell = k+q, \lfloor \bar{a}'(I) \rfloor = k|A_2| + q|A_{n-1}|} \bar{\alpha}'(I) \bar{\alpha}'(J'_0)^{-1} \right).
\]

We know that \( \alpha(J_0) = \alpha'(J'_0) \), and, by (8),

\[
\sum_{I \prec [1, \ell], \ell = k+q, \lfloor \bar{a}(I) \rfloor = k|A_2| + q|A_{n-1}|} \bar{\alpha}(I) = \sum_{I \prec [1, \ell], \ell = k+q, \lfloor \bar{a}'(I) \rfloor = k|A_2| + q|A_{n-1}|} \bar{\alpha}'(I),
\]

for all \( k = 0, 1, \ldots, p \), thus \( \bar{\nu}(\gamma) = \bar{\nu}(\gamma') \). By Corollary 3.4, it follows that \( \gamma = \gamma' \), namely, \( v_i = v'_i \) for all \( i = 1, \ldots, p \). So,

\[
u_1 = v_1 = v'_1 = u_{b_1} \ldots u_{b_{T(1)}} u_{a_1} u_{b_{T(1)}}^{-1} \ldots u_{b_1}^{-1},
\]

thus \( u_1 \) and \( u_{b_i} \ldots u_{b_{T(1)}} \) commute (in \( B_n \)). We conclude by Corollary 5.2 that \( u_1 \) and \( u_{b_i} \) commute for all \( i = 1, \ldots, T(1) \).
References