ISSN 1364-0380 (on line) 1465-3060 (printed) **1281**

Geometry & Topology
Volume 8 (2004) 1281–1300
Published: 28 September 2004

The proof of Birman's conjecture on singular braid monoids

Luis 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 $\sigma_1, \dots, \sigma_{n-1}$, and let SB_n be the singular braid monoid with generators $\sigma_1^{\pm 1}, \dots, \sigma_{n-1}^{\pm 1}$, $\tau_1, \dots, \tau_{n-1}$. The desingularization map is the multiplicative homomorphism $\eta\colon SB_n \to \mathbb{Z}[B_n]$ defined by $\eta(\sigma_i^{\pm 1}) = \sigma_i^{\pm 1}$ and $\eta(\tau_i) = \sigma_i - \sigma_i^{-1}$, for $1 \le i \le n-1$. The purpose of the present paper is to prove Birman's conjecture, namely, that the desingularization map η is injective.

AMS Classification numbers Primary: 20F36

Secondary: 57M25. 57M27

Keywords: Singular braids, desingularization, Birman's conjecture

Proposed: Joan Birman
Seconded: Robion Kirby, Cameron Gordon

Received: 6 January 2004
Revised: 21 September 2004

1 Introduction

Define an n–*braid* to be a collection $b = (b_1, \dots, b_n)$ 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 ζ is a permutation of $\{1,2,\dots,n\}$. 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 $\sigma_1, \dots, \sigma_{n-1}$ and relations

$$\begin{array}{rcl} \sigma_j\sigma_k = \sigma_k\sigma_j & & \text{if } |j-k|>1\,, \\ \sigma_j\sigma_k\sigma_j = \sigma_k\sigma_j\sigma_k & & \text{if } |j-k|=1\,. \end{array}$$

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 $\sigma_1^{\pm 1}, \dots, \sigma_{n-1}^{\pm 1}$, $\tau_1, \dots, \tau_{n-1}$, and relations

$$\begin{array}{lll} \sigma_i\sigma_i^{-1} = \sigma_i^{-1}\sigma_i = 1\,, \quad \sigma_i\tau_i = \tau_i\sigma_i & & \text{if } 1 \le i \le n-1\,, \\ \sigma_i\sigma_j = \sigma_j\sigma_i\,, \quad \sigma_i\tau_j = \tau_j\sigma_i\,, \quad \tau_i\tau_j = \tau_j\tau_i\,, & & \text{if } |i-j|>1\,, \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j\,, \quad \sigma_i\sigma_j\tau_i = \tau_j\sigma_i\sigma_j\,, & & \text{if } |i-j|=1\,. \end{array}$$

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 $\eta\colon SB_n \to \mathbb{Z}[B_n]$, called *desingularization map*, and defined by

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

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 η is an embedding (see [5]). At the time of this writing, the only known partial answer to this question is that η 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 $\eta\colon SB_n \to \mathbb{Z}[B_n]$ is injective.*

Let S_dB_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 $v\colon \mathbb{Z}[B_n] \to A$ 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 η is injective. So, a consequence of Theorem 1.1 is the following.

Corollary 1.2 *Vassiliev braid invariants classify singular braids.*

Let Γ 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 Γ. Define the *graph monoid* of Γ to be the monoid $\mathcal{M}(\Gamma)$ given by the monoid presentation

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

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 $\{\alpha\sigma_i^2\alpha^{-1} - 1;\ \alpha \in B_n \text{ and } 1 \le i \le n-1\}$. More precisely, we prove the following.

Theorem 1.3 *Let Ω be the graph defined as follows.*

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

Let $\nu\colon \mathcal{M}(\Omega) \to \mathbb{Z}[B_n]$ be the homomorphism defined by $\nu(u) = u - 1$, for all $u \in \Upsilon$. Then ν is injective.

The proof of the implication Theorem 1.3 $\Rightarrow$ 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 $\nu\colon \mathcal{M}(\Omega) \to \mathbb{Z}[B_n]$ is the restriction to $\mathcal{M}(\Omega)$ of the desingularization map. The proof of this implication is the subject of Section 2. Let $A_{i\,j}$, $1 \le i < j \le n$, be the standard generators of the pure braid group PB_n. In Section 3, we show that Υ is the disjoint union of the conjugacy classes of the $A_{i\,j}$'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, $A_{i\,j}$ and $A_{r\,s}$. If $\{i,j\} \cap \{r,s\} \neq \emptyset$, then the subgroup generated by the conjugacy classes of $A_{i\,j}$ and $A_{r\,s}$ 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 $1 \le i \le n-1$. Then SB_n is generated as a monoid by $\sigma_1^{\pm 1}, \dots, \sigma_{n-1}^{\pm 1}, \delta_1, \dots, \delta_{n-1}$, and has a monoid presentation with relations

$$\begin{array}{rl} \sigma_i\sigma_i^{-1} = \sigma_i^{-1}\sigma_i = 1\,, \quad \sigma_i\delta_i = \delta_i\sigma_i\,, & \text{if } \ 1 \le i \le n-1\,, \\ \sigma_i\sigma_j = \sigma_j\sigma_i\,, \quad \sigma_i\delta_j = \delta_j\sigma_i\,, \quad \delta_i\delta_j = \delta_j\delta_i\,, & \text{if } \ |i-j| > 1\,, \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j\,, \quad \sigma_i\sigma_j\delta_i = \delta_j\sigma_i\sigma_j\,, & \text{if } \ |i-j| = 1\,. \end{array}$$

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

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

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

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

(1) $\beta\sigma_i^2 = \sigma_j^2\beta$;

(2) $\beta\delta_i = \delta_j\beta$.

This lemma shows the following.

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

- $\hat{\Upsilon} = \{\alpha\delta_i\alpha^{-1};\ \alpha \in B_n \text{ and } 1 \le i \le n-1\}$ *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 $\varphi\colon \mathcal{M}(\hat{\Omega}) \to \mathcal{M}(\Omega)$ *which sends* $\alpha\delta_i\alpha^{-1} \in \hat{\Upsilon}$ *to* $\alpha\sigma_i^2\alpha^{-1} \in \Upsilon$ *for all* $\alpha \in B_n$ *and* $1 \le i \le n-1$*.*

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

$$\begin{array}{rccc} & \alpha\sigma_i^2\alpha^{-1} = \beta\sigma_j^2\beta^{-1} & \Leftrightarrow & (\beta^{-1}\alpha)\sigma_i^2 = \sigma_j^2(\beta^{-1}\alpha) \\ \Leftrightarrow & (\beta^{-1}\alpha)\delta_i = \delta_j(\beta^{-1}\alpha) & \Leftrightarrow & \alpha\delta_i\alpha^{-1} = \beta\delta_j\beta^{-1}\,. \end{array}$$

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

$$\begin{array}{rc} & (\alpha\sigma_i^2\alpha^{-1})(\beta\sigma_j^2\beta^{-1}) = (\beta\sigma_j^2\beta^{-1})(\alpha\sigma_i^2\alpha^{-1}) \\ \Leftrightarrow & \sigma_i^2(\alpha^{-1}\beta\sigma_j^2\beta^{-1}\alpha) = (\alpha^{-1}\beta\sigma_j^2\beta^{-1}\alpha)\sigma_i^2 \\ \Leftrightarrow & \delta_i(\alpha^{-1}\beta\sigma_j^2\beta^{-1}\alpha) = (\alpha^{-1}\beta\sigma_j^2\beta^{-1}\alpha)\delta_i \\ \Leftrightarrow & (\beta^{-1}\alpha\delta_i\alpha^{-1}\beta)\sigma_j^2 = \sigma_j^2(\beta^{-1}\alpha\delta_i\alpha^{-1}\beta) \\ \Leftrightarrow & (\beta^{-1}\alpha\delta_i\alpha^{-1}\beta)\delta_j = \delta_j(\beta^{-1}\alpha\delta_i\alpha^{-1}\beta) \\ \Leftrightarrow & (\alpha\delta_i\alpha^{-1})(\beta\delta_j\beta^{-1}) = (\beta\delta_j\beta^{-1})(\alpha\delta_i\alpha^{-1}) \end{array}$$

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

Now, we have the following decomposition for SB_n.

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

Proof Clearly, there exists a homomorphism $f\colon \mathcal{M}(\hat{\Omega}) \rtimes B_n \to SB_n$ which sends β to $\beta \in SB_n$ for all $\beta \in B_n$, and sends $\hat{u}$ to $\hat{u} \in SB_n$ for all $\hat{u} \in \hat{\Upsilon}$. On the other hand, one can easily verify using the presentation of SB_n that there exists a homomorphism $g\colon SB_n \to \mathcal{M}(\hat{\Omega}) \rtimes B_n$ such that $g(\sigma_i^{\pm 1}) = \sigma_i^{\pm 1} \in B_n$ for all $i \in \{1, \dots, n-1\}$, and $g(\delta_i) = \delta_i \in \hat{\Upsilon}$ for all $i \in \{1, \dots, n-1\}$. Obviously, $f \circ g = \mathrm{Id}$ and $g \circ f = \mathrm{Id}$. □

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

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

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

(2) The decomposition $SB_n = \mathcal{M}(\hat{\Omega}) \rtimes B_n$ 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 $\deg\colon B_n \to \mathbb{Z}$ defined by $\deg(\sigma_i) = 1$ for $1 \le i \le n-1$. 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 β. Since $\eta(\gamma) = \eta(\gamma')$, it follows that $\beta = \beta'$.

So, multiplying γ and γ' on the right by β^{-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 ν is injective (Theorem 1.3) and φ 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 Γ be a graph, let X be the set of vertices, and let $E = E(\Gamma)$ be the set of edges of Γ. Let $x_1, \dots, x_l, y_1, \dots, y_l \in X$ and $k \in \{1, 2, \dots, l\}$ such that:*

- $x_1 x_2 \dots x_l = y_1 y_2 \dots y_l$ *(in* $\mathcal{M}(\Gamma)$*);*
- $y_k = x_1$, *and* $y_i \neq x_1$ *for all* $i = 1, \dots, k-1$.

Then $\{y_i, x_1\} \in E(\Gamma)$ *for all* $i = 1, 2, \dots, k-1$.

Proof Let $F^+(X)$ denote the free monoid freely generated by X. Let $\equiv_1$ be the relation on $F^+(X)$ defined as follows. We set $u \equiv_1 v$ if there exist $u_1, u_2 \in F^+(X)$ and $x, y \in X$ such that $u = u_1 x y u_2$, $v = u_1 y x u_2$, and $\{x, y\} \in E(\Gamma)$. For $p \in \mathbb{N}$, we define the relation $\equiv_p$ on $F^+(X)$ by setting $u \equiv_p v$ if there exists a sequence $u_0 = u, u_1, \dots, u_p = v$ in $F^+(X)$ such that $u_{i-1} \equiv_1 u_i$ for all $i = 1, \dots, p$. Consider the elements $u = x_1 x_2 \dots x_l$ and $v = y_1 y_2 \dots y_l$ in $F^+(X)$. Obviously, there is some $p \in \mathbb{N}$ such that $u \equiv_p v$. Now, we prove the result of Lemma 3.1 by induction on p.

The case $p = 0$ being obvious, we may assume $p \geq 1$. There exists a sequence $u_0 = u, u_1, \dots, u_{p-1}, u_p = v$ in $F^+(X)$ such that $u_{i-1} \equiv_1 u_i$ for all $i = 1, \dots, p$. By definition of $\equiv_1$, there exists $j \in \{1, 2, \dots, l-1\}$ such that $\{y_j, y_{j+1}\} \in E(\Gamma)$ and $u_{p-1} = y_1 \dots y_{j-1} y_{j+1} y_j y_{j+2} \dots y_l$. If either $j < k-1$ or $j > k$, then, by the inductive hypothesis, we have $\{x_1, y_i\} \in E(\Gamma)$ for all $i = 1, \dots, k-1$. If $j = k-1$, then, by the inductive hypothesis, we have $\{x_1, y_i\} \in E(\Gamma)$ for all $i = 1, \dots, k-2$. Moreover, in this case, $\{y_j, y_{j+1}\} = \{y_{k-1}, y_k\} = \{y_{k-1}, x_1\} \in E(\Gamma)$. If $j = k$, then, by the inductive hypothesis, we have $\{y_i, x_1\} \in E(\Gamma)$ for all $i = 1, \dots, k-1$ and $i = k+1$. $\square$

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

$$A_{i\,j} = \sigma_{j-1} \dots \sigma_{i+1} \sigma_i^2 \sigma_{i+1}^{-1} \dots \sigma_{j-1}^{-1}, \quad 1 \leq i < j \leq n,$$

and relations

$$\begin{gathered} A_{r\,s}^{-1} A_{i\,j} A_{r\,s} = A_{i\,j} \quad \text{if} \;\; r < s < i < j \text{ or } i < r < s < j, \\ A_{r\,s}^{-1} A_{i\,j} A_{r\,s} = A_{r\,j} A_{i\,j} A_{r\,j}^{-1} \quad \text{if} \;\; s = i, \\ A_{r\,s}^{-1} A_{i\,j} A_{r\,s} = A_{i\,j} A_{s\,j} A_{i\,j} A_{s\,j}^{-1} A_{i\,j}^{-1} \quad \text{if} \;\; i = r < s < j, \\ A_{r\,s}^{-1} A_{i\,j} A_{r\,s} = A_{r\,j} A_{s\,j} A_{r\,j}^{-1} A_{s\,j}^{-1} A_{i\,j} A_{s\,j} A_{r\,j} A_{s\,j}^{-1} A_{r\,j}^{-1} \quad \text{if} \;\; r < i < s < j. \end{gathered}$$

(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 β. A consequence of the above presentation is that $H_1(PB_n)$ is a free abelian group freely generated by $\{[A_{i\,j}];\ 1 \le i < j \le n\}$. This last fact shall be of importance in the remainder of the paper.

For $1 \le i < j \le n$, we set

$$\Upsilon_{i\,j} = \{\beta A_{i\,j} \beta^{-1}\ ;\ \beta \in PB_n\}\,.$$

Lemma 3.2 *We have the disjoint union $\Upsilon = \bigsqcup_{i<j} \Upsilon_{i\,j}$.*

Proof It is esily checked that

$$\sigma_r A_{i\,j} \sigma_r^{-1} = \begin{cases} A_{i\,j+1} & \text{if } r = j\,, \\ A_{j-1\,j} A_{i\,j-1} A_{j-1\,j}^{-1} & \text{if } r = j-1 > i\,, \\ A_{i+1\,j} & \text{if } j-1 > i = r\,, \\ A_{i\,j}^{-1} A_{i-1\,j} A_{i\,j} & \text{if } r = i-1\,, \\ A_{i\,j} & \text{otherwise}\,. \end{cases}$$

This implies that the union $\bigcup_{i<j} \Upsilon_{i\,j}$ is invariant by the action of B_n by conjugation. Moreover, $\sigma_i^2 = A_{i\,i+1} \in \Upsilon_{i\,i+1}$ for all $i \in \{1,\dots,n-1\}$, thus $\Upsilon \subset \bigcup_{i<j} \Upsilon_{i\,j}$. On the other hand, $A_{i\,j}$ is conjugate (by an element of B_n) to σ_i^2, thus $\Upsilon_{i\,j} \subset \Upsilon$ for all $i<j$, therefore $\bigcup_{i<j} \Upsilon_{i\,j} \subset \Upsilon$.

Let $i,j,r,s \in \{1,\dots,n\}$ such that $i<j$, $r<s$, and $\{i,j\} \neq \{r,s\}$. Let $u \in \Upsilon_{i\,j}$ and $v \in \Upsilon_{r\,s}$. Then $[u] = [A_{i\,j}] \neq [A_{r\,s}] = [v]$, therefore $u \neq v$. This shows that $\Upsilon_{i\,j} \cap \Upsilon_{r\,s} = \emptyset$. □

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 $Y = \{gxg^{-1};\ g \in F(X) \text{ and } x \in X\}$, and let $F^+(Y)$ be the free monoid freely generated by Y. We prove in Section 4 that the homomorphism $\nu\colon F^+(Y) \to \mathbb{Z}[F(X)]$, 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 $PB_n = F \rtimes PB_{n-1}$, where F is a free group freely generated by $\{A_{i\,n};\ 1 \le i \le n-1\}$, are the main ingredients of the proof of Lemma 3.3.

Choose some $x_0 \in X$, consider the decomposition $F(X) = \langle x_0 \rangle * F(X \setminus \{x_0\})$, and let $\rho\colon F(X) \to F(X)$ be an automorphism which fixes x_0 and which leaves $F(X \setminus \{x_0\})$ invariant. Let $y_1,\dots,y_l \in \{gx_0g^{-1};\ g \in F(X)\}$. We prove in Section 5 that, if $\rho(y_1 \dots y_l) = y_1 \dots y_l$, then $\rho(y_i) = y_i$ for all $i = 1,\dots,l$ (Proposition 5.1). The proof of Lemma 3.5 is based on this result together with Corollary 3.4 below.

Lemma 3.3 *Let $i,j,r,s \in \{1,\dots,n\}$ 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 $\bar\nu\colon \mathcal{M}[i,j,r,s] \to \mathbb{Z}[B_n]$ be the homomorphism defined by $\bar\nu(u) = u-1$ for all $u \in \Upsilon_{ij} \cup \Upsilon_{rs}$. Then $\bar\nu$ is injective.*

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

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

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

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

Proof of Theorem 1.3 Recall the decomposition

$$\mathbb{Z}[B_n] = \bigoplus_{k\in\mathbb{Z}} \mathbb{Z}[B_n^{(k)}] \tag{1}$$

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 $\alpha = u_1u_2\dots u_l$, where $u_i \in \Upsilon$ for all $i=1,\dots,l$. Define the *length* of α to be $|\alpha| = l$. We denote by $\bar\alpha$ the element of B_n represented by α (ie, $\bar\alpha = u_1u_2\dots u_l$ in B_n). Let $[1,l] = \{1,2,\dots,l\}$. Define a *subindex* of $[1,l]$ to be a sequence $I = (i_1,i_2,\dots,i_q)$ such that $i_1,i_2,\dots,i_q \in [1,l]$, and $i_1 < i_2 < \dots < i_q$. The notation $I \prec [1,l]$ means that I is a subindex of $[1,l]$. The *length* of I is $|I| = q$. For $I = (i_1,i_2,\dots,i_q) \prec [1,l]$, we set $\alpha(I) = u_{i_1}u_{i_2}\dots u_{i_q} \in \mathcal{M}(\Omega)$ and $\bar\alpha(I)$ denotes the corresponding element of $B_n^{(2q)}$.

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

$$\nu(\alpha) = \sum_{q=0}^{l} (-1)^{l-q} \sum_{I\prec[1,l],\ |I|=q} \bar\alpha(I)\,, \tag{2}$$

and

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

for all $q = 0, 1, \dots, l$.

Let $\alpha' = u'_1 u'_2 \dots u'_k \in \mathcal{M}(\Omega)$ such that $\nu(\alpha) = \nu(\alpha')$. The decomposition given in (2) shows that $k = l$ and

$$\sum_{I \prec [1,l],\ |I|=q} \bar{\alpha}(I) = \sum_{I \prec [1,l],\ |I|=q} \bar{\alpha}'(I)\,, \tag{3}$$

for all $q = 0, 1, \dots, l$.

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

$$\sum_{I \prec [2,l],\ |I|=q} \bar{\alpha}(I) = \sum_{I \prec [2,l],\ |I|=q} \bar{\alpha}'(I) \tag{4}$$

by induction on q. The case $q = 0$ being obvious, we assume $q \geq 1$. Then

$$\begin{aligned}
&\sum_{I \prec [2,l],\ |I|=q} \bar{\alpha}(I) \\
= &\sum_{I \prec [1,l],\ |I|=q} \bar{\alpha}(I) - u_1 \cdot \sum_{I \prec [2,l],\ |I|=q-1} \bar{\alpha}(I) \\
= &\sum_{I \prec [1,l],\ |I|=q} \bar{\alpha}'(I) - u_1 \cdot \sum_{I \prec [2,l],\ |I|=q-1} \bar{\alpha}'(I) \quad \text{(by induction and (3))} \\
= &\sum_{I \prec [2,l],\ |I|=q} \bar{\alpha}'(I)\,.
\end{aligned}$$

Let $\alpha_1 = u_2 \dots u_l$ and $\alpha'_1 = u'_2 \dots u'_l$. By (4), we have

$$\begin{aligned}
\nu(\alpha_1) &= \sum_{q=0}^{l-1} (-1)^{l-1-q} \sum_{I \prec [2,l],\ |I|=q} \bar{\alpha}(I) \\
&= \sum_{q=0}^{l-1} (-1)^{l-1-q} \sum_{I \prec [2,l],\ |I|=q} \bar{\alpha}'(I) = \nu(\alpha'_1)
\end{aligned}$$

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

$$\sum_{i=1}^{l} u_i = \sum_{i=1}^{l} u'_i\,. \tag{5}$$

So, there exists $k \in \{1,\dots,l\}$ such that $u'_k = u_1$ and $u'_i \neq u_1$ for all $i = 1,\dots,k-1$. We prove that, for $1 \le i \le k-1$, u'_i and $u_1 = u'_k$ multiplicatively commute (in B_n or, equivalently, in $\mathcal{M}(\Omega)$). It follows that $\alpha' = u_1 u'_1 \dots u'_{k-1} u'_{k+1} \dots u'_l$, and hence, by the case $u_1 = u'_1$ considered before, $\alpha = \alpha'$.

Fix some $t \in \{1,\dots,k-1\}$. Let $i,j,r,s \in \{1,\dots,n\}$ 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 $\bar\Omega[i,j,r,s]$ be the graph defined as follows.

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

Let $\mathcal{M}[i,j,r,s] = \mathcal{M}(\bar\Omega[i,j,r,s])$, and let $\bar\nu\colon \mathcal{M}[i,j,r,s] \to \mathbb{Z}[B_n]$ 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, $\bar\Omega[i,j,r,s]$ 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 $a_1 = 1, a_2, \dots, a_p \in [1,l]$, $a_1 < a_2 < \dots < a_p$, be the indices such that $u_{a_\xi} \in \Upsilon_{ij} \cup \Upsilon_{rs}$ for all $\xi = 1,2,\dots,p$. Let $I_0 = (a_1, a_2, \dots, a_p)$, and let $\alpha(I_0) = u_{a_1} u_{a_2} \dots u_{a_p} \in \mathcal{M}[i,j,r,s]$. (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 β. Recall also that $H_1(PB_n)$ is a free abelian group freely generated by $\{[A_{ij}];\ 1 \le i < j \le n\}$. Observe that

$$\bar\nu(\alpha(I_0)) = \sum_{q=0}^{p} (-1)^{p-q} \sum_{\substack{I \prec [1,l],\ |I|=q, \\ [\bar\alpha(I)] \in \mathbb{Z}[A_{ij}] + \mathbb{Z}[A_{rs}]}} \bar\alpha(I)\,. \tag{6}$$

Let $b_1, \dots, b_p \in [1, l]$, $b_1 < b_2 < \cdots < b_p$, be the indices such that $u'_{b_\xi} \in \Upsilon_{ij} \cup \Upsilon_{rs}$ for all $\xi = 1, 2, \dots, p$. (Clearly, (5) implies that we have as many a_ξ's as b_ξ's.) Note that $t, k \in \{b_1, \dots, b_p\}$. Let $I'_0 = (b_1, b_2, \dots, b_p)$, and let $\alpha'(I'_0) = u'_{b_1} u'_{b_2} \dots u'_{b_p} \in \mathcal{M}[i, j, r, s]$. By (3) we have

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

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 $u'_k = u_1$ commute. □

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 $Y = \{gxg^{-1};\ g \in F(X) \text{ and } x \in X\}$, let $F^+(Y)$ be the free monoid freely generated by Y, and let $\nu\colon F^+(Y) \to \mathbb{Z}[F(X)]$ be the homomorphism defined by $\nu(y) = y - 1$ for all $y \in Y$. Then ν 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 $\deg\colon F(X) \to \mathbb{Z}$ 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 $\tilde{\mathcal{A}}$ 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 $\tilde{\mathcal{A}}$ can be 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 $k \ge d$.

We take a copy G_x of $\mathbb{Z} \times \mathbb{Z}$ generated by $\{x, \hat{x}\}$, for all $x \in X$, and we set $\hat{G} = *_{x \in X} G_x$. Let $\mathcal{U}(\tilde{\mathcal{A}})$ denote the group of units of $\tilde{\mathcal{A}}$. Then there is a homomorphism $\hat{\eta}\colon \hat{G} \to \mathcal{U}(\tilde{\mathcal{A}})$ defined by

$$\hat{\eta}(x) = x\,, \quad \hat{\eta}(\hat{x}) = x - 1\,, \quad \text{for } x \in X\,.$$

Note that

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

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 $\hat{\eta}\colon \hat{G} \to \mathcal{U}(\tilde{\mathcal{A}})$ is injective.*

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

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

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

Let $(p,q) \in \mathbb{Z} \times \mathbb{Z}$, $(p,q) \neq (0,0)$. Write

$$(t-1)^p t^q = \sum_{k=d}^{+\infty} c_{k\,p\,q} t^k\,,$$

where $d \in \mathbb{Z}$ and $c_{k\,p\,q} \in \mathbb{Z}$ for all $k \ge d$. We show that there exists $a \ge d$ such that $a \neq 0$ and $c_{a\,p\,q} \neq 0$. If $q \neq 0$, then $a = q \neq 0$ and $c_{q\,p\,q} = \pm 1 \neq 0$. If $q = 0$, then $a = 1 \neq 0$ and $c_{1\,p\,0} = \pm p \neq 0$.

Let $g \in \hat{G}$, $g \neq 1$. Let $(\hat{x}_1^{p_1} x_1^{q_1}, \dots, \hat{x}_l^{p_l} x_l^{q_l})$ be the normal form of g. We have

$$\begin{aligned}\hat{\eta}(g) &= (x_1 - 1)^{p_1} x_1^{q_1} (x_2 - 1)^{p_2} x_2^{q_2} \dots (x_l - 1)^{p_l} x_l^{q_l} \\ &= \sum_{k_1 \ge d_1, \dots, k_l \ge d_l} c_{k_1\,p_1\,q_1} c_{k_2\,p_2\,q_2} \dots c_{k_l\,p_l\,q_l} \cdot x_1^{k_1} x_2^{k_2} \dots x_l^{k_l}\,.\end{aligned}$$

By the above observation, there exist $a_1, a_2, \dots, a_l \in \mathbb{Z} \setminus \{0\}$ such that $c_{a_i\,p_i\,q_i} \neq 0$ for all $i = 1, \dots, l$. Now, we show that $x_1^{k_1} \dots x_l^{k_l} \neq x_1^{a_1} \dots x_l^{a_l}$ if $(k_1, \dots, k_l) \neq (a_1, \dots, a_l)$. This implies that the coefficient of $x_1^{a_1} \dots x_l^{a_l}$ in $\hat\eta(g)$ is $c_{a_1\,p_1\,q_1} \dots c_{a_l\,p_l\,q_l} \neq 0$, thus $\hat\eta(g) \neq 1$.

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

$$\lg(x_1^{k_1} \dots x_l^{k_l}) < l = \lg(x_1^{a_1} \dots x_l^{a_l}),$$

thus $x_1^{k_1} \dots x_l^{k_l} \neq x_1^{a_1} \dots x_l^{a_l}$. □

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 $SG = *_{x \in X} SG_x$. Then there is a homomorphism $\eta\colon SG \to \mathbb{Z}[F(X)]$ 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 $\eta\colon SG \to \mathbb{Z}[F(X)]$ is injective.*

Proof We have $SG \subset \hat G$, and, since $\{\mathcal{A}_k\}_{k \in \mathbb{Z}}$ is a separating filtration, $\mathcal{A} = \mathbb{Z}[F(X)]$ is a subalgebra of $\tilde{\mathcal{A}}$. Now, observe that $\eta\colon SG \to \mathbb{Z}[F(X)]$ is the restriction of $\hat\eta$ to SG, thus, by Lemma 4.2, η 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 $\hat\nu\colon F^+(\hat Y) \to \mathbb{Z}[F(X)]$ be the restriction of $\eta\colon SG = F^+(\hat Y) \rtimes F(X) \to \mathbb{Z}[F(X)]$ to $F^+(\hat Y)$, and let $\varphi\colon F^+(\hat Y) \to F^+(Y)$ be the epimorphism defined by $\varphi(g \hat x g^{-1}) = g x g^{-1}$ for all $g \in F(X)$ and $x \in X$. (The proof that φ is well-defined is left to the reader.) The homomorphism $\hat\nu$ is injective (Lemma 4.3), φ is a surjection, and $\hat\nu = \nu \circ \varphi$, thus φ is an isomorphism and ν is injective. □

Proof of Lemma 3.3 Take $\zeta \in \mathrm{Sym}_n$ such that $\zeta(\{i,j\}) = \{1,n\}$ and $\zeta(\{r,s\}) = \{2,n\}$. Choose $\beta \in B_n$ such that $\theta(\beta) = \zeta$. Then $\beta \Upsilon_{i\,j} \beta^{-1} = \Upsilon_{1\,n}$ and $\beta \Upsilon_{r\,s} \beta^{-1} = \Upsilon_{2\,n}$. So, up to conjugation by β 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 $\{A_{i\,n};\ 1 \le i \le n-1\}$. We have:

(1) F is a free group freely generated by $\{A_{i\,n};\ 1 \le i \le n-1\}$;

(2) $PB_n = F \rtimes PB_{n-1}$;

(3) $\Upsilon_{i\,n} = \{g A_{i\,n} g^{-1};\ g \in F\}$ for all $i = 1, \dots, n-1$.

(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 $A_{i\,n}$ in F is invariant by the action of PB_{n-1}.

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

5 Proof of Lemma 3.5

We assume throughout this section that $n \ge 4$. 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 $\rho\colon F(X) \to F(X)$ 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 $y_1, \dots, y_l \in \{g x_0 g^{-1};\ g \in F(X)\}$. If $\rho(y_1 y_2 \dots y_l) = y_1 y_2 \dots y_l$, then $\rho(y_i) = y_i$ for all $i = 1, \dots, l$.*

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

For $f \in F(Z)$, we denote by $\lg(f)$ the word length of f with respect to Z. For $f, g \in F(Z)$, we write $fg = f * g$ if $\lg(fg) = \lg(f) + \lg(g)$. 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 $g_0 = y_1 y_2 \dots y_l$. Recall that we are under the assumption that $\rho(g_0) = g_0$. For $i = 1, \dots, l$, 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 $i = 1, \dots, l$ 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 $t \in \{1, \dots, l-1\}$ such that $\beta_{t+1} = \beta_t * z_t^{-1} * \gamma_t$, where $\gamma_t \in F(Z)$.

Let $y'_{t+1} = \beta_t \gamma_t z_{t+1} \gamma_t^{-1} \beta_t^{-1} = y_t y_{t+1} y_t^{-1}$. Observe that

$$g_0 = y_1 \cdots y_{t-1} y'_{t+1} y_t y_{t+2} \cdots y_l \,.$$

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

Case 2 There exists $t \in \{2, \dots, l\}$ 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 $i = 1, \dots, l$ as in the previous case.

Case 3 For all $t \in \{1, \dots, l\}$ 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

$$g_0 = \beta_1 * z_1 * \beta_1^{-1}\beta_2 * z_2 * \cdots * \beta_{l-1}^{-1}\beta_l * z_l * \beta_l^{-1} \,.$$

Since $\rho(g_0) = g_0$, it follows that $\rho(\beta_1) = \beta_1$, $\rho(z_1) = z_1$, $\rho(\beta_1^{-1}\beta_2) = \beta_1^{-1}\beta_2$, $\rho(z_2) = z_2$, …, $\rho(\beta_{l-1}^{-1}\beta_l) = \beta_{l-1}^{-1}\beta_l$, $\rho(z_l) = z_l$, and $\rho(\beta_l^{-1}) = \beta_l^{-1}$. This clearly implies that $\rho(y_i) = y_i$ for all $i = 1, \dots, l$. □

Corollary 5.2 *Let $u \in \Upsilon_{1\,2}$ and $v_1, \dots, v_l \in \Upsilon_{n-1\,n}$. If u commutes with $v_1 v_2 \dots v_l$ (in B_n), then u commutes with v_i for all $i = 1, \dots, l$.*

Proof Let $\alpha_0 \in PB_n$ such that $u = \alpha_0 A_{1\,2} \alpha_0^{-1}$. Up to conjugation of $v_1, \dots, v_l$ by α_0^{-1} if necessary, we can suppose that $\alpha_0 = 1$ and $u = A_{1\,2}$.

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

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

- $\Upsilon_{i\,n} = \{gA_{i\,n}g^{-1};\ g \in F\}$ for all $i = 1, \dots, n-1$.

Let $\rho\colon F \to F$ be the action of $A_{1\,2}$ by conjugation on F (namely, $\rho(g) = A_{1\,2}gA_{1\,2}^{-1}$). Observe that $\rho(A_{n-1\,n}) = A_{n-1\,n}$ and the subgroup of F generated by $\{A_{i\,n};\ 1 \le i \le n-2\}$ is invariant by ρ. Then, Proposition 5.1 shows that $\rho(v_i) = v_i$ for all $i = 1, \dots, l$ if $\rho(v_1 v_2 \dots v_l) = v_1 v_2 \dots v_l$. $\square$

Now, we can prove Lemma 3.5.

Proof of Lemma 3.5 Take $\zeta \in \mathrm{Sym}_n$ 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 $\beta\Upsilon_{i\,j}\beta^{-1} = \Upsilon_{1\,2}$ and $\beta\Upsilon_{r\,s}\beta^{-1} = \Upsilon_{n-1\,n}$. So, up to conjugation by β 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 $\alpha = u_1 u_2 \dots u_l$, where $u_i \in \Upsilon_{1\,2} \cup \Upsilon_{n-1\,n}$ for all $i = 1, \dots, l$. Define the *length* of α to be $|\alpha| = l$. We denote by $\bar{\alpha}$ the element of B_n represented by α. Let $[1,l] = \{1,2,\dots,l\}$. Define a *subindex* of $[1,l]$ to be a sequence $I = (i_1, i_2, \dots, i_q)$ such that $i_1, i_2, \dots, i_q \in [1,l]$ and $i_1 < i_2 < \dots < i_q$. The notation $I \prec [1,l]$ means that I is a subindex of $[1,l]$. The *length* of I is $|I| = q$. For $I = (i_1, i_2, \dots, i_q) \prec [1,l]$, we set $\alpha(I) = u_{i_1} u_{i_2} \dots u_{i_q} \in \mathcal{M}[1,2,n-1,n]$.

Observe that

$$\bar{\nu}(\alpha) = \sum_{q=0}^{l} (-1)^{l-q} \sum_{I \prec [1,l],\ |I|=q} \bar{\alpha}(I)\,, \tag{7}$$

and

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

for all $q = 0, 1, \dots, l$.

Let $\alpha' = u'_1 u'_2 \dots u'_k \in \mathcal{M}[1,2,n-1,n]$ such that $\bar{\nu}(\alpha) = \bar{\nu}(\alpha')$. As in the proof of Theorem 1.3, the decomposition given in (7) shows that $k = l$ and

$$\sum_{I \prec [1,l],\ |I|=q} \bar{\alpha}(I) = \sum_{I \prec [1,l],\ |I|=q} \bar{\alpha}'(I)\,, \tag{8}$$

for all $q = 0, 1, \dots, l$.

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

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 $\zeta \in \mathrm{Sym}_l$ such that $u_i = u'_{\zeta(i)}$ for all $i = 1, \dots, l$. (Note that the permutation $\zeta \in \mathrm{Sym}_l$ is not necessarily unique. Actually, ζ is unique if and only if $u_i \neq u_j$ for all $i \neq j$.)

Let $a_1, a_2, \dots, a_p \in [1,l]$, $a_1 < a_2 < \dots < a_p$, be the indices such that $u_{a_\xi} \in \Upsilon_{12}$ for all $\xi = 1, \dots, p$. Let $I_0 = (a_1, a_2, \dots, a_p)$. Recall that, for $\beta \in PB_n$, we denote by $[\beta]$ the element of $H_1(PB_n)$ represented by β. Recall also that $H_1(PB_n)$ is a free abelian group freely generated by $\{[A_{ij}];\ 1 \le i < j \le n\}$. Observe that $\alpha(I_0) \in \mathcal{M}[1,2]$ and

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

Let $a'_1, a'_2, \dots, a'_p \in [1,l]$, $a'_1 < a'_2 < \dots < a'_p$, be the indices such that $u'_{a'_\xi} \in \Upsilon_{12}$ for all $\xi = 1, \dots, p$. Note that $\{\zeta(a'_1), \zeta(a'_2), \dots, \zeta(a'_p)\} = \{a_1, a_2, \dots, a_p\}$. Let $I'_0 = (a'_1, a'_2, \dots, a'_p)$. By (8), we have

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

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 $i = 1, \dots, p$, and the permutation $\zeta \in \mathrm{Sym}_l$ can be chosen so that $\zeta(a'_i) = a_i$ for all $i = 1, \dots, p$.

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

Without loss of generality, we can assume that $u_1 \in \Upsilon_{1\,2}$ (namely, $a_1 = 1$). Let $i \in \{1, \dots, p\}$. We set:

$$S(i) = \begin{cases} 0 & \text{if } a_i < b_1\,, \\ j & \text{if } b_j < a_i < b_{j+1}\,, \\ q & \text{if } b_q < a_i\,. \end{cases}$$

$$T(i) = \begin{cases} 0 & \text{if } a'_i < b'_1\,, \\ j & \text{if } b'_j < a'_i < b'_{j+1}\,, \\ q & \text{if } b'_q < a'_i\,. \end{cases}$$

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

$$\begin{aligned} v_i &= u_{b_1} \dots u_{b_{S(i)}} u_{a_i} u_{b_{S(i)}}^{-1} \dots u_{b_1}^{-1} \in \Upsilon_{1\,2}\,, \\ v'_i &= u_{b_1} \dots u_{b_{T(i)}} u_{a_i} u_{b_{T(i)}}^{-1} \dots u_{b_1}^{-1} \in \Upsilon_{1\,2}\,, \end{aligned}$$

for all $i = 1, \dots, p$, and let

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

Observe that

$$\bar\nu(\gamma) = \left(\sum_{k=0}^{p} (-1)^{p-k} \sum_{\substack{I \prec [1,l],\ |I| = k+q,\\ [\bar\alpha(I)] = k[A_{1\,2}] + q[A_{n-1\,n}]}} \bar\alpha(I) \right) \bar\alpha(J_0)^{-1}\,,$$

$$\bar\nu(\gamma') = \left(\sum_{k=0}^{p} (-1)^{p-k} \sum_{\substack{I \prec [1,l],\ |I| = k+q,\\ [\bar\alpha'(I)] = k[A_{1\,2}] + q[A_{n-1\,n}]}} \bar\alpha'(I) \right) \bar\alpha'(J'_0)^{-1}\,.$$

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

$$\sum_{\substack{I \prec [1,l],\ |I| = k+q,\\ [\bar\alpha(I)] = k[A_{1\,2}] + q[A_{n-1\,n}]}} \bar\alpha(I) = \sum_{\substack{I \prec [1,l],\ |I| = k+q,\\ [\bar\alpha'(I)] = k[A_{1\,2}] + q[A_{n-1\,n}]}} \bar\alpha'(I)\,,$$

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

$$u_1 = v_1 = v'_1 = u_{b_1} \dots u_{b_{T(1)}} u_1 u_{b_{T(1)}}^{-1} \dots u_{b_1}^{-1}\,,$$

thus u_1 and $u_{b_1} \dots u_{b_{T(1)}}$ commute (in B_n). We conclude by Corollary 5.2 that u_1 and u_{b_i} commute for all $i = 1, \dots, T(1)$. ◻

References

[1] **J C Baez**, *Link invariants of finite type and perturbation theory*, Lett. Math. Phys. 26 (1992) 43–51

[2] **G Basset**, *Quasi-commuting extensions of groups*, Comm. Algebra 28 (2000) 5443–5454

[3] **D Bar-Natan**, *Vassiliev homotopy string link invariants*, J. Knot Theory Ramifications 4 (1995) 13–32

[4] **J S Birman**, *Braids, links, and mapping class groups*, Annals of Mathematics Studies 82, Princeton University Press, Princeton, N.J. (1974)

[5] **J S Birman**, *New points of view in knot theory*, Bull. Amer. Math. Soc. 28 (1993) 253–287

[6] **N. Bourbaki**, *Groupes et algèbres de Lie, Chapitres 2 et 3*, Hermann, Paris (1972)

[7] **P Cartier**, **D Foata**, *Problèmes combinatoires de commutation et de réarrangements*, Lecture Notes in Mathematics, No. 85, Springer–Verlag, Berlin, New York (1969)

[8] **R Corran**, *A normal form for a class of monoids including the singular braid monoid*, J. Algebra 223 (2000) 256–282

[9] **G Duchamp**, **D Krob**, *Free partially commutative structures*, J. Algebra 156 (1993) 318–361

[10] **C Duboc**, *Commutations dans les monoïdes libres: un cadre théorique pour l'étude du parallélisme*, PhD Thesis, Université de Rouen (1986)

[11] **R Fenn**, **E Keyman**, **C Rourke**, *The singular braid monoid embeds in a group*, J. Knot Theory Ramifications 7 (1998) 881–892

[12] **R Fenn**, **D Rolfsen**, **J Zhu**, *Centralisers in the braid group and singular braid monoid*, Enseign. Math. 42 (1996) 75–96

[13] **A Járai Jr**, *On the monoid of singular braids*, Topology Appl. 96 (1999) 109–119

[14] **E Keyman**, *A class of monoids embeddable in a group*, Turkish J. Math. 25 (2001) 299–305

[15] **T Kohno**, *Vassiliev invariants and de Rham complex on the space of knots*, from: "Symplectic geometry and quantization (Sanda and Yokohama, 1993)" , Contemp. Math. 179, Amer. Math. Soc. Providence, R.I. (1994) 123–138

[16] **S Papadima**, *The universal finite-type invariant for braids, with integer coefficients*, from: "Arrangements in Boston: a Conference on Hyperplane Arrangements (1999)", Topology Appl. 118 (2002) 169–185

[17] **J Zhu**, *On singular braids*, J. Knot Theory Ramifications 6 (1997) 427–440