

A simple solution to the word problem for virtual braid groups

Paolo Bellingeri, Bruno Aaron Cisneros de La Cruz, Luis Paris

► To cite this version:

Paolo Bellingeri, Bruno Aaron Cisneros de La Cruz, Luis Paris. A simple solution to the word problem for virtual braid groups. 2015. hal-01164543v1

HAL Id: hal-01164543 https://hal.science/hal-01164543v1

Preprint submitted on 17 Jun 2015 (v1), last revised 4 Mar 2016 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers. L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A simple solution to the word problem for virtual braid groups

PAOLO BELLINGERI, BRUNO A. CISNEROS DE LA CRUZ, LUIS PARIS

June 17, 2015

Abstract

We show a simple and easily implementable solution to the word problem for virtual braid groups.

AMS Subject Classification. Primary: 20F36. Secondary: 20F10, 57M25.

1 Introduction

Virtual braid groups were introduced by L. Kauffman in his seminal paper on virtual knots and links [10]. They can be defined in several ways, such as in terms of Gauss diagrams [2, 7], in terms of braids in thickened surfaces [7], and in terms of virtual braid diagrams. The latter will be our starting point of view.

A virtual braid diagram on n strands is a n-tuple $\beta = (b_1, \ldots, b_n)$ of smooth paths in the plane \mathbb{R}^2 satisfying the following conditions.

- (a) $b_i(0) = (i, 0)$ for all $i \in \{1, \dots, n\}$.
- (b) There exists a permutation $g \in \mathfrak{S}_n$ such that $b_i(1) = (g(i), 1)$ for all $i \in \{1, \ldots, n\}$.
- (c) $(p_2 \circ b_i)(t) = t$ for all $i \in \{1, \ldots, n\}$ and all $t \in [0, 1]$, where $p_2 : \mathbb{R}^2 \to \mathbb{R}$ denotes the projection on the second coordinate.
- (d) The b_i 's intersect transversely in a finite number of double points, called the *crossings* of the diagram.

Each crossing is endowed with one of the following attributes: positive, negative, virtual. In the figures they are generally indicated as in Figure 1.1. Let VBD_n be the set of virtual braid diagrams on n strands, and let \sim be the equivalence relation on VBD_n generated by ambient isotopy and the virtual Reidemeister moves depicted in Figure 1.2. The concatenation of diagrams induces a group structure on VBD_n/\sim . The latter is called *virtual braid group* on n strands, and is denoted by VB_n .



positive negative virtual

Figure 1.1. Crossings in a virtual braid diagram.

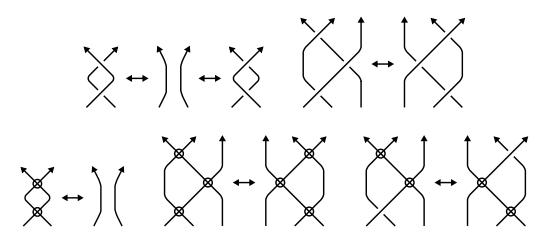


Figure 1.2. Virtual Reidemeister moves.

It was observed in [9, 15] that VB_n has a presentation with generators $\sigma_1, \ldots, \sigma_{n-1}, \tau_1, \ldots, \tau_{n-1}$, and relations

$$\begin{aligned} \tau_i^2 &= 1 & \text{for } 1 \leq i \leq n-1 \\ \sigma_i \sigma_j &= \sigma_j \sigma_i \,, \ \sigma_i \tau_j = \tau_j \sigma_i \,, \text{ and } \tau_i \tau_j = \tau_j \tau_i & \text{for } |i-j| \geq 2 \\ \sigma_i \sigma_j \sigma_i &= \sigma_j \sigma_i \sigma_j \,, \ \sigma_i \tau_j \tau_i = \tau_j \tau_i \sigma_j \,, \text{ and } \tau_i \tau_j \tau_i = \tau_j \tau_i \tau_j & \text{for } |i-j| = 1 \end{aligned}$$

A solution to the word problem for virtual braid groups was shown in [8]. However, this solution is quite theoretical and its understanding requires some heavy technical knowledge on Artin groups. Therefore, it is incomprehensible and useless for most of the potential users, including low dimensional topologists. Moreover, its implementation would be difficult. Our aim here is to show a new solution, which is simpler and easily implementable, and whose understanding does not require any special technical knowledge. This new solution is in the spirit of the one shown in [8], in the sense that one of the main ingredients in its proof is the study of parabolic subgroups in Artin groups.

Acknowledgments. The research of the first author was partially supported by French grant ANR-11-JS01-002-01.

2 The algorithm

Our solution to the word problem for VB_n is divided into four steps. In Step 1 we define a subgroup KB_n of VB_n and a generating set S for KB_n , and we show an algorithm (called Algorithm A) which decides whether an element of VB_n belongs to KB_n and, if yes, determines a word over $S^{\pm 1}$ which represents this element. For $\mathcal{X} \subset S$, we denote by $KB_n(\mathcal{X})$ the subgroup of KB_n generated by \mathcal{X} . The other three steps provide a solution to the word problem for $KB_n(\mathcal{X})$ which depends recursively on the cardinality of \mathcal{X} . Step 2 is the beginning of the induction. More precisely, the algorithm proposed in Step 2 (called Algorithm B) is a solution to the word problem for $KB_n(\mathcal{X})$ when \mathcal{X} is a full subset of S (the notion of "full subset" will be also defined in Step 2; for now, the reader just need to know that singletons are full subsets). In Step 3 we suppose given a solution to the word problem for $KB_n(\mathcal{X})$, and, for a given subset $\mathcal{Y} \subset \mathcal{X}$, we show an algorithm which solves the membership problem for $KB_n(\mathcal{Y})$ in $KB_n(\mathcal{X})$ (Algorithm C). In Step 4 we show an algorithm which solves the word problem for $KB_n(\mathcal{X})$ when \mathcal{X} is not a full subset, under the assumption that the group $KB_n(\mathcal{Y})$ has a solvable word problem for any proper subset \mathcal{Y} of \mathcal{X} (Algorithm D).

Step 1

Recall that \mathfrak{S}_n denotes the group of permutations of $\{1, \ldots, n\}$. We denote by $\theta: VB_n \to \mathfrak{S}_n$ the epimorphism which sends σ_i to 1 and τ_i to (i, i + 1) for all $1 \leq i \leq n - 1$, and by KB_n the kernel of θ . Note that θ has a section $\iota: \mathfrak{S}_n \to VB_n$ which sends (i, i + 1) to τ_i for all $1 \leq i \leq n - 1$, and therefore VB_n is a semi-direct product $VB_n = KB_n \rtimes \mathfrak{S}_n$. The following proposition is proved in a master thesis [12] which, unfortunately, is not available anywhere. However, its proof can also be found in [3].

Proposition 2.1 (Rabenda [12]). For $1 \le i < j \le n$ we set

$$\delta_{i,j} = \tau_i \tau_{i+1} \cdots \tau_{j-2} \sigma_{j-1} \tau_{j-2} \cdots \tau_{i+1} \tau_i,$$

$$\delta_{j,i} = \tau_i \tau_{i+1} \cdots \tau_{j-2} \tau_{j-1} \sigma_{j-1} \tau_{j-1} \tau_{j-2} \cdots \tau_{i+1} \tau_i$$

Then KB_n has a presentation with generating set

$$\mathcal{S} = \left\{ \delta_{i,j} \mid 1 \le i \ne j \le n \right\},\$$

and relations

$$\delta_{i,j}\delta_{k,\ell} = \delta_{k,\ell}\delta_{i,j} \qquad for \ i,j,k,\ell \ distinct$$

$$\delta_{i,j}\delta_{j,k}\delta_{i,j} = \delta_{j,k}\delta_{i,j}\delta_{j,k} \qquad for \ i,j,k \ distinct$$

The virtual braids $\delta_{i,j}$ and $\delta_{j,i}$ are depicted in Figure 2.1.

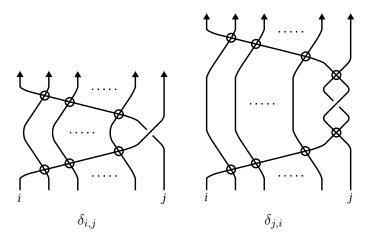


Figure 2.1. Generators for KB_n .

The following is an important tool in the forthcoming Algorithm A.

Lemma 2.2 (Bardakov, Bellingeri [3]). Let u be a word over $\{\tau_1, \ldots, \tau_{n-1}\}$, let \bar{u} be the element of VB_n represented by u, and let $i, j \in \{1, \ldots, n\}, i \neq j$. Then $\bar{u}\delta_{i,j}\bar{u}^{-1} = \delta_{i',j'}$, where $i' = \theta(\bar{u})(i)$ and $j' = \theta(\bar{u})(j)$.

Note that $\tau_i^{-1} = \tau_i$, since $\tau_i^2 = 1$, for all $i \in \{1, \ldots, n-1\}$. Hence, the letters $\tau_1^{-1}, \ldots, \tau_{n-1}^{-1}$ are not needed in the above lemma and below.

Now, we give an algorithm which, given a word u over $\{\sigma_1^{\pm 1}, \ldots, \sigma_{n-1}^{\pm 1}, \tau_1, \ldots, \tau_{n-1}\}$, decides whether the element \bar{u} of VB_n represented by u belongs to KB_n . If yes, it also determines a word u' over $S^{\pm 1} = \{\delta_{i,j}^{\pm} \mid 1 \leq i \neq j \leq n\}$ which represents \bar{u} . The fact that this algorithm is correct follows from Lemma 2.2.

Algorithm A. Let u be a word over $\{\sigma_1^{\pm 1}, \ldots, \sigma_{n-1}^{\pm 1}, \tau_1, \ldots, \tau_{n-1}\}$. We write u in the form

$$u = v_0 \sigma_{i_1}^{\varepsilon_1} v_1 \cdots v_{\ell-1} \sigma_{i_\ell}^{\varepsilon_\ell} v_\ell$$

where v_0, v_1, \ldots, v_ℓ are words over $\{\tau_1, \ldots, \tau_{n-1}\}$, and $\varepsilon_1, \ldots, \varepsilon_\ell \in \{\pm 1\}$. On the other hand, for a word $v = \tau_{j_1} \cdots \tau_{j_k}$ over $\{\tau_1, \ldots, \tau_{n-1}\}$, we set $\theta(v) = (j_1, j_1 + 1) \cdots (j_k, j_k + 1) \in \mathfrak{S}_n$. Note that $\theta(\bar{u}) = \theta(v_0) \theta(v_1) \cdots \theta(v_\ell)$. If $\theta(\bar{u}) \neq 1$, then $\bar{u} \notin KB_n$. If $\theta(\bar{u}) = 1$, then $\bar{u} \in KB_n$, and \bar{u} is represented by

$$u' = \delta_{a_1,b_1}^{\varepsilon_1} \delta_{a_2,b_2}^{\varepsilon_2} \cdots \delta_{a_\ell,b_\ell}^{\varepsilon_\ell},$$

where

$$a_k = \theta(v_0 \cdots v_{k-1})(i_k)$$
 and $b_k = \theta(v_0 \cdots v_{k-1})(i_k+1)$

for all $k \in \{1, \ldots, \ell\}$.

Step 2

Let S be a finite set. A Coxeter matrix over S is a square matrix $M = (m_{s,t})_{s,t\in S}$, indexed by the elements of S, such that $m_{s,s} = 1$ for all $s \in S$, and $m_{s,t} = m_{t,s} \in \{2, 3, 4, ...\} \cup \{\infty\}$ for all $s, t \in S, s \neq t$. We represent this Coxeter matrix with a labelled graph $\Gamma = \Gamma_M$, called Coxeter diagram. The set of vertices of Γ is S. Two vertices $s, t \in S$ are connected by an edge labelled by $m_{s,t}$ if $m_{s,t} \neq \infty$.

If a, b are two letters and m is an integer ≥ 2 , we set $\langle a, b \rangle^m = (ab)^{\frac{m}{2}}$ if m is even, and $\langle a, b \rangle^m = (ab)^{\frac{m-1}{2}}a$ if m id odd. In other words, $\langle a, b \rangle^m$ denotes the word $aba \cdots$ of length m. The Artin group of Γ is the group $A = A(\Gamma)$ defined by the following presentation.

$$A = \langle S \mid \langle s, t \rangle^{m_{s,t}} = \langle t, s \rangle^{m_{s,t}} \text{ for all } s, t \in S, \ s \neq t \text{ and } m_{s,t} \neq \infty \rangle.$$

The Coxeter group of Γ , denoted by $W = W(\Gamma)$, is the quotient of A by the relations $s^2 = 1$, $s \in S$.

Example. Let $V\Gamma_n$ be the Coxeter diagram defined as follows. The set of vertices of $V\Gamma_n$ is S. If $i, j, k, \ell \in \{1, ..., n\}$ are distinct, then $\delta_{i,j}$ and $\delta_{k,\ell}$ are connected by an edge labelled by 2. If $i, j, k \in \{1, ..., n\}$ are distinct, then $\delta_{i,j}$ and $\delta_{j,k}$ are connected by an edge labelled by 3. There is no other edge in $V\Gamma_n$. Then, by Proposition 2.1, KB_n is isomorphic to $A(V\Gamma_n)$. Let Γ be a Coxeter diagram. For $X \subset S$, we denote by Γ_X the subdiagram of Γ spanned by X, by A_X the subgroup of $A = A(\Gamma)$ generated by X, and by W_X the subgroup of $W = W(\Gamma)$ generated by X. By [11], A_X is the Artin group of Γ_X , and, by [5], W_X is the Coxeter group of Γ_X .

For $\mathcal{X} \subset \mathcal{S}$, we denote by $KB_n(\mathcal{X})$ the subgroup of KB_n generated by \mathcal{X} . By the above, $KB_n(\mathcal{X})$ has a presentation with generating set \mathcal{X} and relations

- st = ts if s and t are connected in $V\Gamma_n$ by an edge labelled by 2,
- sts = tst if s and t are connected in $V\Gamma_n$ by an edge labelled by 3.

Definition. We say that a subset \mathcal{X} of \mathcal{S} is *full* if any two distinct elements s, t of \mathcal{X} are connected by an edge of $V\Gamma_n$. Recall that the aim of Step 2 is to give a solution to the word problem for $KB_n(\mathcal{X})$ when \mathcal{X} is full.

We denote by $F_n = F(x_1, \ldots, x_n)$ the free group of rank *n* freely generated by x_1, \ldots, x_n . For $i, j \in \{1, \ldots, n\}, i \neq j$, we define $\varphi_{i,j} \in \operatorname{Aut}(F_n)$ by

$$\varphi_{i,j}(x_i) = x_i x_j x_i^{-1}, \ \varphi_{i,j}(x_j) = x_i, \ \text{and} \ \varphi_{i,j}(x_k) = x_k \ \text{for} \ k \notin \{i, j\}.$$

It is easily checked from the presentation in Proposition 2.1 that the map $\mathcal{S} \to \operatorname{Aut}(F_n), \delta_{i,j} \mapsto \varphi_{i,j}$, induces a representation $\varphi: KB_n \to \operatorname{Aut}(F_n)$. For $\mathcal{X} \subset \mathcal{S}$, we denote by $\varphi_{\mathcal{X}}: KB_n(\mathcal{X}) \to \operatorname{Aut}(F_n)$ the restriction of φ to $KB_n(\mathcal{X})$. The following will be proved in Section 3.

Proposition 2.3. If \mathcal{X} is a full subset of \mathcal{S} , then $\varphi_{\mathcal{X}} : KB_n(\mathcal{X}) \to Aut(F_n)$ is faithful.

Remark. The whole representation $\varphi : KB_n \to \operatorname{Aut}(F_n)$ is not faithful. Indeed, we have $\varphi_{1,3}\varphi_{3,2}\varphi_{3,1} = \varphi_{2,3}\varphi_{1,3}\varphi_{3,2}$, whereas $\delta_{1,3}\delta_{3,2}\delta_{3,1} \neq \delta_{2,3}\delta_{1,3}\delta_{3,2}$. In order to show that these two elements of KB_n are different, the reader may use the solution to the word problem given in the present paper. (Actually, Algorithm C of Step 3 suffices.)

Notation. From now on, if u is a word over $S^{\pm 1}$, then \bar{u} will denote the element of KB_n represented by u.

Algorithm B. Let \mathcal{X} be a full subset of \mathcal{S} , and let $u = s_1^{\varepsilon_1} \cdots s_{\ell}^{\varepsilon_{\ell}}$ be a word over $\mathcal{X}^{\pm 1}$. We have $\varphi(\bar{u}) = \varphi(s_1)^{\varepsilon_1} \cdots \varphi(s_{\ell})^{\varepsilon_{\ell}}$. If $\varphi(\bar{u}) = \mathrm{Id}$, then $\bar{u} = 1$. Otherwise, $\bar{u} \neq 1$.

Step 3

Let G be a group, and let H be a subgroup of G. A solution to the membership problem for H in G is an algorithm which, given $g \in G$, decides whether g belongs to H or not. In the present step we will assume that $KB_n(\mathcal{X})$ has a solution to the word problem, and, from this solution, we will give a solution to the membership problem for $KB_n(\mathcal{Y})$ in $KB_n(\mathcal{X})$, for $\mathcal{Y} \subset \mathcal{X}$. Furthermore, if the tested element belongs to $KB_n(\mathcal{Y})$, then this algorithm will determine a word over $\mathcal{Y}^{\pm 1}$ which represents this element.

Let u be a word over S. (Attention: here the alphabet is S, and not $S^{\pm 1}$.)

• Suppose that u is written in the form u_1ssu_2 , where u_1, u_2 are words over S and s is an element of S. Then we say that $u' = u_1u_2$ is obtained from u by an *M*-operation of type I.

- Suppose that u is written in the form $u_1 stu_2$, where u_1, u_2 are words over S and s, t are two elements of S connected by an edge labelled by 2. Then we say that $u' = u_1 t s u_2$ is obtained from u by an *M*-operation of type II⁽²⁾.
- Suppose that u is written in the form $u_1 stsu_2$, where u_1, u_2 are words over S and s, t are two elements of S connected by an edge labelled by 3. Then we say that $u' = u_1 tstu_2$ is obtained from u by an M-operation of type II⁽³⁾.

Let \mathcal{Y} be a subset of \mathcal{S} .

Suppose that u is written in the form tu', where u' is a word over S and t is an element of Y. Then we say that u' is obtained from u by an M-operation of type III_Y.

We say that u is *M*-reduced (resp. $M_{\mathcal{Y}}$ -reduced) if its length cannot be shortened by *M*-operations of type I, II⁽²⁾, II⁽³⁾ (resp. of type I, II⁽²⁾, II⁽³⁾, III_{\mathcal{Y}}). An *M*-reduction (resp. $M_{\mathcal{Y}}$ -reduction) of u is an *M*-reduced word (resp. $M_{\mathcal{Y}}$ -reduced word) obtained from u by *M*-operations (resp. $M_{\mathcal{Y}}$ -operations). We can easily enumerate all the words obtained from u by *M*-operations (resp. $M_{\mathcal{Y}}$ -operations), hence we can effectively determine an *M*-reduction and/or an $M_{\mathcal{Y}}$ -reduction of u.

Let \mathcal{Y} be a subset of \mathcal{S} . From a word $u = s_1^{\varepsilon_1} \cdots s_\ell^{\varepsilon_\ell}$ over $\mathcal{S}^{\pm 1}$, we construct a word $\pi_{\mathcal{Y}}(u)$ over $\mathcal{Y}^{\pm 1}$ as follows.

- For $i \in \{0, 1, \dots, \ell\}$ we set $u_i^+ = s_1 \cdots s_i$ (as ever, u_0^+ is the identity).
- For $i \in \{0, 1, \dots, \ell\}$ we calculate an $M_{\mathcal{Y}}$ -reduction v_i^+ of u_i^+ .
- For a word $v = t_1 \cdots t_k$ over \mathcal{S} , we denote by $\operatorname{op}(v) = t_k \cdots t_1$ the *anacycle* of v. Let $i \in \{1, \ldots, \ell\}$. If $\varepsilon_i = 1$, we set $w_i^+ = v_{i-1}^+ \cdot s_i \cdot \operatorname{op}(v_{i-1}^+)$. If $\varepsilon_i = -1$, we set $w_i^+ = v_i^+ \cdot s_i \cdot \operatorname{op}(v_i^+)$.
- For all $i \in \{1, \ldots, \ell\}$ we calculate an *M*-reduction g_i of w_i^+ .
- If g_i is of length 1 and $g_i = t_i \in \mathcal{Y}$, we set $T_i = g_i^{\varepsilon_i} = t_i^{\varepsilon_i}$. Otherwise we set $T_i = 1$.
- We set $\pi_{\mathcal{Y}}(u) = T_1 T_2 \cdots T_\ell$.

The proof of the following is given in Section 4.

Proposition 2.4. Let \mathcal{Y} be a subset of \mathcal{S} . Let u, v be two words over $\mathcal{S}^{\pm 1}$. If $\bar{u} = \bar{v}$, then $\pi_{\mathcal{Y}}(u) = \pi_{\mathcal{Y}}(v)$. Moreover, we have $\bar{u} \in KB_n(\mathcal{Y})$ if and only if $\bar{u} = \pi_{\mathcal{Y}}(u)$.

Algorithm C. Take two subsets \mathcal{X} and \mathcal{Y} of \mathcal{S} such that $\mathcal{Y} \subset \mathcal{X}$, and assume given a solution to the word problem for $KB_n(\mathcal{X})$. Let u be a word over $\mathcal{X}^{\pm 1}$. We calculate $v = \pi_{\mathcal{Y}}(u)$. If $uv^{-1} \neq 1$, then $\bar{u} \notin KB_n(\mathcal{Y})$. If $uv^{-1} = 1$, then $\bar{u} \in KB_n(\mathcal{Y})$ and v is a word over $\mathcal{Y}^{\pm 1}$ which represents the same element as u.

Step 4

Now, we assume that \mathcal{X} is a non-full subset of \mathcal{S} , and that we have a solution to the word problem for $KB_n(\mathcal{Y})$ for any proper subset \mathcal{Y} of \mathcal{X} (induction hypothesis). We can and do choose two elements $s_1, s_2 \in \mathcal{X}$ that are not connected by an edge in $V\Gamma_n$, and we set $\mathcal{X}_1 = \mathcal{X} \setminus \{s_1\}$, $\mathcal{X}_2 = \mathcal{X} \setminus \{s_2\}$, and $\mathcal{X}_0 = \mathcal{X} \setminus \{s_1, s_2\}$. It follows from the presentations of the $KB_n(\mathcal{X}_i)$'s given in Step 2 that we have the amalgamated product

$$KB_n(\mathcal{X}) = KB_n(\mathcal{X}_1) *_{KB_n(\mathcal{X}_0)} KB_n(\mathcal{X}_2).$$

Our last algorithm is based on the following result. This is well-known and can be found for instance in [13, Chap. 5.2].

Proposition 2.5. Let $A_1 *_B A_2$ be an amalgamated product of groups. Let g_1, \ldots, g_ℓ be a sequence of elements of $A_1 \sqcup A_2$ different from 1 and satisfying the following condition:

if $q_i \in A_1$ (resp. $g_i \in A_2$), then $g_{i+1} \in A_2 \setminus B$ (resp. $g_{i+1} \in A_1 \setminus B$), for all $i \in \{1, \ldots, \ell-1\}$.

Then $g_1g_2 \cdots g_\ell$ is different from 1 in $A_1 *_B A_2$.

Algorithm D. Let u be a word over $\mathcal{X}^{\pm 1}$. We write u in the form $u_1 u_2 \cdots u_\ell$, where

u_i is either a word over X^{±1}₁, or a word over X^{±1}₂,
if u_i is a word over X^{±1}₁ (resp. over X^{±1}₂), then u_{i+1} is a word over X^{±1}₂ (resp. over X^{±1}₁). We decide whether \bar{u} is trivial by induction on ℓ . Suppose that $\ell = 1$ and $u = u_1 \in KB_n(\mathcal{X}_i)$ $(j \in \{1, 2\})$. Then we apply the solution to the word problem for $KB_n(\mathcal{X}_i)$ to decide whether \bar{u} is trivial or not. Suppose that $\ell \geq 2$. For all *i* we set $v_i = \pi_{\mathcal{X}_0}(u_i)$. If $\overline{u_i v_i^{-1}} \neq 1$ for all *i*, then $\bar{u} \neq 1$. Suppose that there exists $i \in \{1, \dots, \ell\}$ such that $\overline{u_i v_i^{-1}} = 1$. Let $u'_i = v_1 u_2$ if i = 1, $u'_{i} = u_{\ell-1}v_{\ell}$ if $i = \ell$, and $u'_{i} = u_{i-1}v_{i}u_{i+1}$ if $2 \le i \le \ell - 1$. Set $v = u_{1}\cdots u_{i-2}u'_{i}u_{i+2}\cdots u_{\ell}$. Then $\bar{u} = \bar{v}$ and, by induction, we can decide whether v represents 1 or not.

3 **Proof of Proposition 2.3**

Recall that $F_n = F(x_1, \ldots, x_n)$ denotes the free group of rank n freely generated by x_1, \ldots, x_n , and that we have a representation $\varphi: KB_n \to \operatorname{Aut}(F_n)$ which sends $\delta_{i,j}$ to $\varphi_{i,j}$, where

$$\varphi_{i,j}(x_i) = x_i x_j x_i^{-1}, \ \varphi_{i,j}(x_j) = x_i, \text{ and } \varphi_{i,j}(x_k) = x_k \text{ for } k \notin \{i, j\}$$

For $\mathcal{X} \subset \mathcal{S}$, we denote by $\varphi_{\mathcal{X}} : KB_n(\mathcal{X}) \to \operatorname{Aut}(F_n)$ the restriction of φ to $KB_n(\mathcal{X})$. In this section we prove that $\varphi_{\mathcal{X}}$ is faithful if \mathcal{X} is a full subset of \mathcal{S} .

Consider the following groups.

$$B_n = \left\langle \sigma_1, \dots, \sigma_{n-1} \middle| \begin{array}{c} \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j & \text{if } |i-j| = 1 \\ \sigma_i \sigma_j = \sigma_j \sigma_i & \text{if } |i-j| \ge 2 \end{array} \right\rangle,$$
$$\tilde{B}_n = \left\langle \sigma_1, \dots, \sigma_n \middle| \begin{array}{c} \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j & \text{if } i \equiv j \pm 1 \mod n \\ \sigma_i \sigma_j = \sigma_j \sigma_i & \text{if } i \neq j \text{ and } i \neq j \pm 1 \mod n \end{array} \right\rangle, \quad n \ge 3.$$

The group B_n is the classical braid group, and B_n is the affine braid group.

We define representations $\psi_n: B_n \to \operatorname{Aut}(F_n)$ and $\tilde{\psi}_n: \tilde{B}_n \to \operatorname{Aut}(F_n)$ in the same way as φ as follows.

$$\begin{split} \psi_n(\sigma_i)(x_i) &= x_i x_{i+1} x_i^{-1}, \ \psi_n(\sigma_i)(x_{i+1}) = x_i, \ \psi_n(\sigma_i)(x_k) = x_k \text{ if } k \notin \{i, i+1\} \\ \tilde{\psi}_n(\sigma_i)(x_i) &= x_i x_{i+1} x_i^{-1}, \ \tilde{\psi}_n(\sigma_i)(x_{i+1}) = x_i, \ \tilde{\psi}_n(\sigma_i)(x_k) = x_k \text{ if } k \notin \{i, i+1\}, \text{ for } i < n \\ \tilde{\psi}_n(\sigma_n)(x_n) &= x_n x_1 x_n^{-1}, \ \tilde{\psi}_n(\sigma_n)(x_1) = x_n, \ \tilde{\psi}_n(\sigma_n)(x_k) = x_k \text{ if } k \notin \{1, n\} \end{split}$$

The key of the proof of Proposition 2.3 is the following.

Theorem 3.1 (Artin [1], Bellingeri, Bodin [4]). The representations $\psi_n : B_n \to \operatorname{Aut}(F_n)$ and $\tilde{\psi}_n : \tilde{B}_n \to \operatorname{Aut}(F_n)$ are faithful.

The support of a generator $\delta_{i,j}$ is defined to be $\operatorname{supp}(\delta_{i,j}) = \{i, j\}$. The support of a subset \mathcal{X} of \mathcal{S} is $\operatorname{supp}(\mathcal{X}) = \bigcup_{s \in \mathcal{X}} \operatorname{supp}(s)$. We say that two subsets \mathcal{X}_1 and \mathcal{X}_2 of \mathcal{S} are perpendicular¹ if $\operatorname{supp}(\mathcal{X}_1) \cap \operatorname{supp}(\mathcal{X}_2) = \emptyset$. Note that this condition implies that $\mathcal{X}_1 \cap \mathcal{X}_2 = \emptyset$. More generally, we say that a family $\mathcal{X}_1, \ldots, \mathcal{X}_\ell$ of subsets of \mathcal{S} is perpendicular if $\operatorname{supp}(\mathcal{X}_i) \cap \operatorname{supp}(\mathcal{X}_j) = \emptyset$ for all $i \neq j$. In that case we write $\mathcal{X}_1 \cup \cdots \cup \mathcal{X}_\ell = \mathcal{X}_1 \boxplus \cdots \boxplus \mathcal{X}_\ell$. We say that a subset \mathcal{X} of \mathcal{S} is indecomposable if it is not the union of two perpendicular nonempty subsets. The following observations will be of importance in what follows.

Remark. Let \mathcal{X}_1 and \mathcal{X}_2 be two perpendicular subsets of \mathcal{S} , and let $\mathcal{X} = \mathcal{X}_1 \boxplus \mathcal{X}_2$.

- (1) \mathcal{X} is a full subset if and only if \mathcal{X}_1 and \mathcal{X}_2 are both full subsets.
- (2) $KB_n(\mathcal{X}) = KB_n(\mathcal{X}_1) \times KB_n(\mathcal{X}_2).$

Indeed, if $\delta_{i,j} \in \mathcal{X}_1$ and $\delta_{k,\ell} \in \mathcal{X}_2$, then i, j, k, ℓ are distinct, and therefore $\delta_{i,j}$ and $\delta_{k,\ell}$ are connected by and edge labelled by 2, and $\delta_{i,j}\delta_{k,\ell} = \delta_{k,\ell}\delta_{i,j}$.

Lemma 3.2. Let \mathcal{X}_1 and \mathcal{X}_2 be two perpendicular subsets of \mathcal{S} , and let $\mathcal{X} = \mathcal{X}_1 \boxplus \mathcal{X}_2$. Then $\varphi_{\mathcal{X}} : KB_n(\mathcal{X}) \to \operatorname{Aut}(F_n)$ is faithful if and only if $\varphi_{\mathcal{X}_1} : KB_n(\mathcal{X}_1) \to \operatorname{Aut}(F_n)$ and $\varphi_{\mathcal{X}_2} : KB_n(\mathcal{X}_2) \to \operatorname{Aut}(F_n)$ are both faithful.

Proof. For $X \subset \{x_1, \ldots, x_n\}$, we denote by F(X) the subgroup of F_n generated by X. There is a natural embedding $\iota_X : \operatorname{Aut}(F(X)) \hookrightarrow \operatorname{Aut}(F_n)$ defined by

$$\iota_X(\alpha)(x_i) = \begin{cases} \alpha(x_i) & \text{if } x_i \in X \\ x_i & \text{otherwise} \end{cases}$$

Moreover, if X_1 and X_2 are disjoint subsets of $\{x_1, \ldots, x_n\}$, then the homomorphism

$$\begin{aligned} (\iota_{X_1} \times \iota_{X_2}) : & \operatorname{Aut}(F(X_1)) \times \operatorname{Aut}(F(X_2)) & \to & \operatorname{Aut}(F_n) \\ (\alpha_1, \alpha_2) & \mapsto & \iota_{X_1}(\alpha_1) \iota_{X_2}(\alpha_2) \end{aligned}$$

is well-defined and injective. From now on, we will assume $\operatorname{Aut}(F(X))$ to be embedded in $\operatorname{Aut}(F_n)$ via ι_X , for all $X \subset \{x_1, \ldots, x_n\}$.

By abuse of notation, for $\mathcal{X} \subset \mathcal{S}$, we will also denote by $\operatorname{supp}(\mathcal{X})$ the set $\{x_i \mid i \in \operatorname{supp}(\mathcal{X})\}$. Set $X_1 = \operatorname{supp}(\mathcal{X}_1)$ and $X_2 = \operatorname{supp}(\mathcal{X}_2)$. We have $\operatorname{Im}(\varphi_{\mathcal{X}_i}) \subset \operatorname{Aut}(F(X_i))$ for $i = 1, 2, X_1 \cap X_2 = \emptyset$, and $KB_n(\mathcal{X}) = KB_n(\mathcal{X}_1) \times KB_n(\mathcal{X}_2)$. Hence, Lemma 3.2 follows from the following claim whose proof is left to the reader.

Claim. Let $f_1 : G_1 \to H_1$ and $f_2 : G_2 \to H_2$ be two group homomorphisms. Let $(f_1 \times f_2) : (G_1 \times G_2) \to (H_1 \times H_2)$ be the homomorphism defined by $(f_1 \times f_2)(u_1, u_2) = (f_1(u_1), f_2(u_2))$. Then $(f_1 \times f_2)$ is injective if and only if f_1 and f_2 are both injective.

¹This terminology is derived from the theory of Coxeter groups.

For $2 \leq m \leq n$ we set

$$\mathcal{Z}_m = \{\delta_{1,2}, \dots, \delta_{m-1,m}\}, \ \tilde{\mathcal{Z}}_m = \{\delta_{1,2}, \dots, \delta_{m-1,m}, \delta_{m,1}\}.$$

Note that the map $\{\sigma_1, \ldots, \sigma_{m-1}\} \to \mathbb{Z}_m, \sigma_i \mapsto \delta_{i,i+1}$, induces an isomorphism $f_m : B_m \to KB_n(\mathbb{Z}_m)$. This follows from the presentation of $KB_n(\mathbb{Z}_m)$ given in Step 2 of Section 2. Similarly, for $m \geq 3$, the map $\{\sigma_1, \ldots, \sigma_m\} \to \tilde{\mathbb{Z}}_m, \sigma_i \mapsto \delta_{i,i+1}$ for $1 \leq i \leq m-1, \sigma_m \mapsto \delta_{m,1}$, induces an isomorphism $\tilde{f}_m : \tilde{B}_m \to KB_n(\tilde{\mathbb{Z}}_m)$.

Recall that the symmetric group \mathfrak{S}_n acts on \mathcal{S} by $g \, \delta_{i,j} = \delta_{g(i),g(j)}$, and that this action induces an action of \mathfrak{S}_n on KB_n . On the other hand, there is a natural embedding $\mathfrak{S}_n \hookrightarrow \operatorname{Aut}(F_n)$, where $g \in \mathfrak{S}_n$ sends x_i to $x_{g(i)}$ for all $i \in \{1, \ldots, n\}$, and this embedding induces by conjugation an action of \mathfrak{S}_n on $\operatorname{Aut}(F_n)$. It is easily seen that the homomorphism $\varphi : KB_n \to \operatorname{Aut}(F_n)$ is equivariant under these actions of \mathfrak{S}_n .

Lemma 3.3. If \mathcal{X} is a full and indecomposable nonempty subset of \mathcal{S} , then there exist $g \in \mathfrak{S}_n$ and $m \in \{1, \ldots, n\}$ such that either $\mathcal{X} = g \mathcal{Z}_m$, or $\mathcal{X} = g \tilde{\mathcal{Z}}_m$ and $m \geq 3$.

Proof. An oriented graph Υ is the data of two sets, $V(\Upsilon)$, called set of vertices, and $E(\Upsilon)$, called set of arrows, together with two maps sou, tar : $E(\Upsilon) \to V(\Upsilon)$. We associate an oriented graph $\Upsilon_{\mathcal{X}}$ to any subset \mathcal{X} of \mathcal{S} as follows. The set of vertices is $V(\Upsilon_{\mathcal{X}}) = \operatorname{supp}(\mathcal{X})$, the set of arrows is $E(\Upsilon_{\mathcal{X}}) = \mathcal{X}$, and, for $\delta_{i,j} \in \mathcal{X}$, we set $\operatorname{sou}(\delta_{i,j}) = i$ and $\operatorname{tar}(\delta_{i,j}) = j$. Assume that \mathcal{X} is a full and indecomposable nonempty subset of \mathcal{S} . Since \mathcal{X} is indecomposable, $\Upsilon_{\mathcal{X}}$ must be connected. Since \mathcal{X} is full, if $s, t \in \mathcal{X}$ are two different arrows of $\Upsilon_{\mathcal{X}}$ with a common vertex, then there exist $i, j, k \in \{1, \ldots, n\}$ distinct such that either $s = \delta_{j,i}$ and $t = \delta_{i,k}$, or $s = \delta_{i,j}$ and $t = \delta_{k,i}$. This implies that $\Upsilon_{\mathcal{X}}$ is either an oriented segment, or an oriented cycle with at least 3 vertices (see Figure 3.1). If $\Upsilon_{\mathcal{X}}$ is an oriented segment, then there exist $g \in \mathfrak{S}_n$ and $m \in \{1, \ldots, n\}$ such that $\mathcal{X} = g \mathbb{Z}_m$. If $\Upsilon_{\mathcal{X}}$ is an oriented cycle, then there exist $g \in \mathfrak{S}_n$ and $m \in \{1, \ldots, n\}, m \geq 3$, such that $\mathcal{X} = g \tilde{\mathbb{Z}}_m$.



Figure 3.1. Oriented segment and oriented cycle.

Proof of Proposition 2.3. Let \mathcal{X} be a full nonempty subset of \mathcal{S} . Write $\mathcal{X} = \mathcal{X}_1 \boxplus \cdots \boxplus \mathcal{X}_\ell$, where \mathcal{X}_j is an indecomposable nonempty subset. As observed above, each \mathcal{X}_j is also a full subset. Moreover, by Lemma 3.2, in order to show that $\varphi_{\mathcal{X}}$ is faithful, it suffices to show that $\varphi_{\mathcal{X}_j}$ is faithful for all $j \in \{1, \ldots, \ell\}$. So, we can assume that \mathcal{X} is a full and indecomposable nonempty subset of \mathcal{S} . By Lemma 3.3, there exist $g \in \mathfrak{S}_n$ and $m \in \{1, \ldots, n\}$ such that either $\mathcal{X} = g \mathcal{Z}_m$, or $\mathcal{X} = g \tilde{\mathcal{Z}}_m$ and $m \geq 3$. Since φ is equivariant under the actions of \mathfrak{S}_n , upon conjugating by g^{-1} , we can assume that either $\mathcal{X} = \mathcal{Z}_m$, or $\mathcal{X} = \tilde{\mathcal{Z}}_m$. Set $Z_m = \{x_1, \ldots, x_m\} = \operatorname{supp}(\mathcal{Z}_m) =$ $\operatorname{supp}(\tilde{\mathcal{Z}}_m)$, and identify F_m with $F(Z_m)$. Then $\varphi_{\mathcal{Z}_m} = \psi_m \circ f_m^{-1}$ and $\varphi_{\tilde{\mathcal{Z}}_m} = \tilde{\psi}_m \circ \tilde{f}_m^{-1}$, hence $\varphi_{\mathcal{X}}$ is faithful by Theorem 3.1.

Proof of Proposition 2.4 4

Proposition 2.4 will be proved in the general setting of Artin groups. Let S be a finite set. Recall that a Coxeter matrix over S is a square matrix $M = (m_{s,t})_{s,t \in S}$, indexed by the elements of S, such that $m_{s,s} = 1$ for all $s \in S$, and $m_{s,t} = m_{t,s} \in \{2,3,4,\dots\} \cup \{\infty\}$ for all $s, t \in S, s \neq t$. We represent this Coxeter matrix with a labelled graph $\Gamma = \Gamma_M$, called *Coxeter diagram*. The set of vertices of Γ is S. Two vertices $s, t \in S$ are connected by an edge labelled by $m_{s,t}$ if $m_{s,t} \neq \infty$.

If a, b are two letters and m is an integer ≥ 2 , we set $\langle a, b \rangle^m = (ab)^{\frac{m}{2}}$ if m is even, and $\langle a,b\rangle^m = (ab)^{\frac{m-1}{2}}a$ if m id odd. The Artin group of Γ is the group $A = A(\Gamma)$ defined by the following presentation.

$$A = \langle S \mid \langle s, t \rangle^{m_{s,t}} = \langle t, s \rangle^{m_{s,t}} \text{ for all } s, t \in S, \ s \neq t \text{ and } m_{s,t} \neq \infty \rangle.$$

The Coxeter group of Γ , denoted by $W = W(\Gamma)$, is the quotient of A by the relations $s^2 = 1$, $s \in S$.

For $Y \subset S$, we denote by Γ_Y the subdiagram of Γ spanned by Y, by A_Y the subgroup of $A = A(\Gamma)$ generated by Y, and by W_Y the subgroup of $W = W(\Gamma)$ generated by Y. By [11], A_Y is the Artin group of Γ_Y , and, by [5], W_Y is the Coxeter group of Γ_Y .

Let u be a word over S.

- Suppose that u is written in the form u_1ssu_2 , where u_1, u_2 are words over S and s is an element of S. Then we say that $u' = u_1 u_2$ is obtained from u by an M-operation of type I.
- Suppose that *u* is written in the form

$$u = u_1 \langle s, t \rangle^{m_{s,t}} u_2 \,,$$

where u_1, u_2 are words over S and s, t are two elements of S connected by an edge labelled by $m_{s,t}$. Then we say that

$$u' = u_1 \langle t, s \rangle^{m_{s,t}} u_2 \,,$$

is obtained from u by an M-operation of type II. Let Y be a subset of S.

• Suppose that u is written in the form tu', where u' is a word over S and t is an element of Y. Then we say that u' is obtained from u by an M-operation of type III_Y.

We say that a word u is *M*-reduced (resp. M_Y -reduced) if its length cannot be shortened by *M*-operations of type I, II (resp. of type I, II, III_Y). An *M*-reduction (resp. M_Y -reduction) of a word u is an M-reduced word (resp. M_Y -reduced word) obtained from u by M-operations (resp. M_Y -operations).

Let Y be a subset of S. From a word $u = s_1^{\varepsilon_1} \cdots s_{\ell}^{\varepsilon_{\ell}}$ over $S^{\pm 1}$, we construct a word $\pi_Y(u)$ over $Y^{\pm 1}$ as follows.

- For $i \in \{0, 1, ..., \ell\}$ we set $u_i^+ = s_1 \cdots s_i$.
- For all $i \in \{0, \dots, \ell\}$ we calculate an M_Y -reduction v_i^+ of u_i^+ . Let $i \in \{1, \dots, \ell\}$. If $\varepsilon_i = 1$, we set $w_i^+ = v_{i-1}^+ \cdot s_i \cdot \operatorname{op}(v_{i-1}^+)$. If $\varepsilon_i = -1$, we set $w_i^+ = v_i^+ \cdot s_i \cdot \operatorname{op}(v_i^+)$.

- For all $i \in \{1, \ldots, \ell\}$ we calculate an *M*-reduction g_i of w_i^+ .
- If g_i is of length 1 and $g_i = t_i \in Y$, we set $T_i = g_i^{\varepsilon_i} = t_i^{\varepsilon_i}$. Otherwise we set $T_i = 1$.
- We set $\pi_Y(u) = T_1 T_2 \cdots T_\ell$.

Now, Proposition 2.4 is a straightforward consequence of the following.

Proposition 4.1. Let Y be a subset of S. Let u, v be two words over $S^{\pm 1}$. If $\bar{u} = \bar{v}$, then $\pi_Y(u) = \pi_Y(v)$. Moreover, we have $\bar{u} \in A_Y$ if and only if $\bar{u} = \pi_Y(u)$.

The rest of the section is dedicated to the proof of Proposition 4.1.

Since we have $s^2 = 1$ in W for all $s \in S$, every element g in W can be represented by a word over S. Such a word is called an *expression* of g. The minimal length of an expression of g is called the *length* of g and is denoted by $\lg_S(g)$. An expression of g of length $\lg_S(g)$ is a *reduced expression* of g. Let Y be a subset of S, and let $g \in W$. We say that g is Y-minimal if it is of minimal length among the elements of the coset $W_Y g$.

Proposition 4.2. (Bourbaki [5]). Let $Y \subset S$, and let $g \in W$. There exists a unique Y-minimal element in the coset $W_Y g$. Moreover, the following conditions are equivalent.

(a) g is Y-minimal,

- (b) $\lg_S(sg) > \lg_S(g)$ for all $s \in Y$,
- (c) $\lg_S(hg) = \lg_S(h) + \lg_S(g)$ for all $h \in W_Y$.

A "nice" set-retraction $\rho_Y : A \to A_Y$ to the inclusion $\iota_Y : A_Y \to A$ is constructed in [8, 6]. This is defined as follows (we refer to [6] for its correctness). Let α be an element of A. Let $\hat{\alpha} = s_1^{\varepsilon_1} \cdots s_\ell^{\varepsilon_\ell}$ be a word over $S^{\pm 1}$ which represents α . Let $i \in \{1, \ldots, \ell\}$. Set $g_i = s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_i^{\varepsilon_i} = s_1 s_2 \cdots s_i \in W$. Write g_i in the form $g_i = h_i k_i$, where $h_i \in W_Y$ and k_i is Y-minimal. If $\varepsilon_i = 1$, set $x_i = k_{i-1} s_i k_{i-1}^{-1}$. If $\varepsilon_i = -1$, set $x_i = k_i s_i k_i^{-1}$. Set

$$\tau_i = \begin{cases} x_i^{\varepsilon_i} & \text{if } x_i \in Y \\ 1 & \text{otherwise} \end{cases}$$
$$\widehat{\tau} = \tau_1 \tau_2 \cdots \tau_\ell.$$

Then $\rho_Y(\alpha)$ is the element of A_Y represented by $\hat{\tau}$.

So, in order to prove Proposition 4.1, it suffices to prove the following.

Proposition 4.3. Let $g \in W$.

- (1) An expression w of g is a reduced expression if and only if w is M-reduced.
- (2) Any two reduced expressions w and w' of g are connected by a finite sequence of M-operations of type II.
- (3) Let w be an reduced expression of g. Then g is Y-minimal if and only if w is M_Y -reduced.

Proof. (1) and (2) are the celebrate Tits solution to the word problem for Coxeter groups (see [14]). (3) easily follows from (1), (2), and Proposition 4.2. \Box

References

- [1] E. Artin. Theory of braids. Ann. of Math. (2) 48 (1947), 101–126.
- [2] D. Bar Natan, Z. Dancso. Finite Type Invariants of w-Knotted Objects I: w-Knots and the Alexander Polynomial. arXiv:1405.1956.
- [3] V. G. Bardakov, P. Bellingeri. Combinatorial properties of virtual braids. Topology Appl. 156 (2009), no. 6, 1071–1082.
- [4] P. Bellingeri, A. Bodin. The braid group of a necklace. Preprint. arXiv:1404.2511.
- [5] N. Bourbaki. Eléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: Systèmes de racines. Actualités Scientifiques et Industrielles, No. 1337, Hermann, Paris, 1968.
- [6] R. Charney, L. Paris. Convexity of parabolic subgroups in Artin groups. Bull. Lond. Math. Soc. 46 (2014), no. 6, 1248–1255.
- [7] Bruno A. Cisneros De La Cruz. Virtual braids from a topological viewpoint. arXiv:1402.0300, to appear in J. Knot Theory Ramifications.
- [8] E. Godelle, L. Paris. $K(\pi, 1)$ and word problems for infinite type Artin-Tits groups, and applications to virtual braid groups. Math. Z. **272** (2012), no. 3-4, 1339–1364.
- [9] S. Kamada. Braid presentation of virtual knots and welded knots. Osaka J. Math. 44 (2007), no. 2, 441–458.
- [10] L.H. Kauffman. Virtual knot theory. European J. Combin. 20 (1999), no. 7, 663–690.
- [11] H. van der Lek. The homotopy type of complex hyperplane complements. Ph. D. Thesis, Nijmegen, 1983.
- [12] L. Rabenda. Mémoire de DEA (Master thesis), Université de Bourgogne, 2003.
- [13] J.-P. Serre. Arbres, amalgames, SL₂. Astérisque, No. 46. Société Mathématique de France, Paris, 1977.
- [14] J. Tits. Le problème des mots dans les groupes de Coxeter. Symposia Mathematica (INDAM, Rome, 1967/68), Vol. 1, pp. 175–185, Academic Press, London, 1969.
- [15] V. V. Vershinin. On homology of virtual braids and Burau representation. J. Knot Theory Ramifications 10 (2001), no. 5, 795–812.

Paolo Bellingeri,

LMNO UMR6139, CNRS, Université de Caen, F-14000 Caen, France. E-mail: paolo.bellingeri@unicaen.fr

Bruno A. Cisneros de la Cruz,

IMB UMR5584, CNRS, Univ. Bourgogne Franche-Comté, F-21000 Dijon, France. E-mail: bruno.cisneros-de-la-cruz@u-bourgogne.fr

Luis Paris,

IMB UMR5584, CNRS, Univ. Bourgogne Franche-Comté, F-21000 Dijon, France. E-mail: lparis@u-bourgogne.fr