# 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 <br> 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 $\beta=\left(b_{1}, \ldots, b_{n}\right)$ of smooth paths in the plane $\mathbb{R}^{2}$ satisfying the following conditions.
(a) $b_{i}(0)=(i, 0)$ for all $i \in\{1, \ldots, n\}$.
(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) $\left(p_{2} \circ b_{i}\right)(t)=t$ for all $i \in\{1, \ldots, n\}$ and all $t \in[0,1]$, where $p_{2}: \mathbb{R}^{2} \rightarrow \mathbb{R}$ 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 $V B D_{n}$ be the set of virtual braid diagrams on $n$ strands, and let $\sim$ be the equivalence relation on $V B D_{n}$ generated by ambient isotopy and the virtual Reidemeister moves depicted in Figure 1.2. The concatenation of diagrams induces a group structure on $V B D_{n} / \sim$. The latter is called virtual braid group on $n$ strands, and is denoted by $V B_{n}$.

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 $V B_{n}$ has a presentation with generators $\sigma_{1}, \ldots, \sigma_{n-1}, \tau_{1}, \ldots, \tau_{n-1}$, and relations

$$
\begin{array}{cl}
\tau_{i}^{2}=1 & \text { for } 1 \leq i \leq n-1 \\
\sigma_{i} \sigma_{j}=\sigma_{j} \sigma_{i}, \sigma_{i} \tau_{j}=\tau_{j} \sigma_{i}, \text { and } \tau_{i} \tau_{j}=\tau_{j} \tau_{i} & \text { for }|i-j| \geq 2 \\
\sigma_{i} \sigma_{j} \sigma_{i}=\sigma_{j} \sigma_{i} \sigma_{j}, \sigma_{i} \tau_{j} \tau_{i}=\tau_{j} \tau_{i} \sigma_{j}, \text { and } \tau_{i} \tau_{j} \tau_{i}=\tau_{j} \tau_{i} \tau_{j} & \text { for }|i-j|=1
\end{array}
$$

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 $V B_{n}$ is divided into four steps. In Step 1 we define a subgroup $K B_{n}$ of $V B_{n}$ and a generating set $\mathcal{S}$ for $K B_{n}$, and we show an algorithm (called Algorithm A) which decides whether an element of $V B_{n}$ belongs to $K B_{n}$ and, if yes, determines a word over $\mathcal{S}^{ \pm 1}$ which represents this element. For $\mathcal{X} \subset \mathcal{S}$, we denote by $K B_{n}(\mathcal{X})$ the subgroup of $K B_{n}$ generated by $\mathcal{X}$. The other three steps provide a solution to the word problem for $K B_{n}(\mathcal{X})$ 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 $K B_{n}(\mathcal{X})$ when $\mathcal{X}$ is a full subset of $\mathcal{S}$ (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 $K B_{n}(\mathcal{X})$, and, for a given subset $\mathcal{Y} \subset \mathcal{X}$, we show an algorithm which solves the membership problem for $K B_{n}(\mathcal{Y})$ in $K B_{n}(\mathcal{X})$ (Algorithm C). In Step 4 we show an algorithm which solves the word problem for $K B_{n}(\mathcal{X})$ when $\mathcal{X}$ is not a full subset, under the assumption that the group $K B_{n}(\mathcal{Y})$ 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 $\theta: V B_{n} \rightarrow \mathfrak{S}_{n}$ the epimorphism which sends $\sigma_{i}$ to 1 and $\tau_{i}$ to $(i, i+1)$ for all $1 \leq i \leq n-1$, and by $K B_{n}$ the kernel of $\theta$. Note that $\theta$ has a section $\iota: \mathfrak{S}_{n} \rightarrow V B_{n}$ which sends $(i, i+1)$ to $\tau_{i}$ for all $1 \leq i \leq n-1$, and therefore $V B_{n}$ is a semi-direct product $V B_{n}=K B_{n} \rtimes \mathfrak{S}_{n}$. 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 $1 \leq i<j \leq n$ we set

$$
\begin{aligned}
\delta_{i, j} & =\tau_{i} \tau_{i+1} \cdots \tau_{j-2} \sigma_{j-1} \tau_{j-2} \cdots \tau_{i+1} \tau_{i} \\
\delta_{j, i} & =\tau_{i} \tau_{i+1} \cdots \tau_{j-2} \tau_{j-1} \sigma_{j-1} \tau_{j-1} \tau_{j-2} \cdots \tau_{i+1} \tau_{i}
\end{aligned}
$$

Then $K B_{n}$ has a presentation with generating set

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

and relations

$$
\begin{aligned}
\delta_{i, j} \delta_{k, \ell} & =\delta_{k, \ell} \delta_{i, j} & & \text { for } i, j, k, \ell \text { distinct } \\
\delta_{i, j} \delta_{j, k} \delta_{i, j} & =\delta_{j, k} \delta_{i, j} \delta_{j, k} & & \text { for } i, j, k \text { distinct }
\end{aligned}
$$

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

$\delta_{i, j}$


Figure 2.1. Generators for $K B_{n}$.

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

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

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 $\left\{\sigma_{1}^{ \pm 1}, \ldots, \sigma_{n-1}^{ \pm 1}, \tau_{1}, \ldots, \tau_{n-1}\right\}$, decides whether the element $\bar{u}$ of $V B_{n}$ represented by $u$ belongs to $K B_{n}$. If yes, it also determines a word $u^{\prime}$ over $\mathcal{S}^{ \pm 1}=\left\{\delta_{i, j}^{ \pm} \mid 1 \leq i \neq j \leq n\right\}$ which represents $\bar{u}$. The fact that this algorithm is correct follows from Lemma 2.2.

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

$$
u=v_{0} \sigma_{i_{1}}^{\varepsilon_{1}} v_{1} \cdots v_{\ell-1} \sigma_{i_{\ell} \ell}^{\varepsilon_{\ell}} v_{\ell}
$$

where $v_{0}, v_{1}, \ldots, v_{\ell}$ are words over $\left\{\tau_{1}, \ldots, \tau_{n-1}\right\}$, 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 $\left\{\tau_{1}, \ldots, \tau_{n-1}\right\}$, we set $\theta(v)=\left(j_{1}, j_{1}+1\right) \cdots\left(j_{k}, j_{k}+1\right) \in \mathfrak{S}_{n}$. Note that $\theta(\bar{u})=\theta\left(v_{0}\right) \theta\left(v_{1}\right) \cdots \theta\left(v_{\ell}\right)$. If $\theta(\bar{u}) \neq 1$, then $\bar{u} \notin K B_{n}$. If $\theta(\bar{u})=1$, then $\bar{u} \in K B_{n}$, and $\bar{u}$ is represented by

$$
u^{\prime}=\delta_{a_{1}, b_{1}}^{\varepsilon_{1}} \delta_{a_{2}, b_{2}}^{\varepsilon_{2}} \cdots \delta_{a_{\ell}, b_{\ell}}^{\varepsilon_{\ell}},
$$

where

$$
a_{k}=\theta\left(v_{0} \cdots v_{k-1}\right)\left(i_{k}\right) \text { and } b_{k}=\theta\left(v_{0} \cdots v_{k-1}\right)\left(i_{k}+1\right)
$$

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

## Step 2

Let $S$ be a finite set. A Coxeter matrix over $S$ is a square matrix $M=\left(m_{s, t}\right)_{s, t \in S}$, indexed by the elements of $S$, such that $m_{s, s}=1$ for all $s \in S$, and $m_{s, t}=m_{t, s} \in\{2,3,4, \ldots\} \cup\{\infty\}$ 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 $\Gamma$ 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 $\geq 2$, we set $\langle a, b\rangle^{m}=(a b)^{\frac{m}{2}}$ if $m$ is even, and $\langle a, b\rangle^{m}=(a b)^{\frac{m-1}{2}} a$ if $m$ id odd. In other words, $\langle a, b\rangle^{m}$ denotes the word $a b a \cdots$ of length $m$. The Artin group of $\Gamma$ is the group $A=A(\Gamma)$ defined by the following presentation.

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

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

Example. Let $\mathrm{V} \Gamma_{n}$ be the Coxeter diagram defined as follows. The set of vertices of $\mathrm{V} \Gamma_{n}$ is $\mathcal{S}$. If $i, j, k, \ell \in\{1, \ldots, n\}$ are distinct, then $\delta_{i, j}$ and $\delta_{k, \ell}$ are connected by an edge labelled by 2 . If $i, j, k \in\{1, \ldots, n\}$ are distinct, then $\delta_{i, j}$ and $\delta_{j, k}$ are connected by an edge labelled by 3 . There is no other edge in $\mathrm{V} \Gamma_{n}$. Then, by Proposition 2.1, $K B_{n}$ is isomorphic to $A\left(\mathrm{~V} \Gamma_{n}\right)$.

Let $\Gamma$ be a Coxeter diagram. For $X \subset S$, we denote by $\Gamma_{X}$ the subdiagram of $\Gamma$ 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 $\Gamma_{X}$, and, by [5], $W_{X}$ is the Coxeter group of $\Gamma_{X}$.

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

- $s t=t s$ if $s$ and $t$ are connected in $\mathrm{V}_{n}$ by an edge labelled by 2 ,
- sts $=t$ st if $s$ and $t$ are connected in $\mathrm{V} \Gamma_{n}$ 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 $\mathrm{V} \Gamma_{n}$. Recall that the aim of Step 2 is to give a solution to the word problem for $K B_{n}(\mathcal{X})$ when $\mathcal{X}$ is full.

We denote by $F_{n}=F\left(x_{1}, \ldots, x_{n}\right)$ 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 $\varphi_{i, j} \in \operatorname{Aut}\left(F_{n}\right)$ by

$$
\varphi_{i, j}\left(x_{i}\right)=x_{i} x_{j} x_{i}^{-1}, \varphi_{i, j}\left(x_{j}\right)=x_{i}, \text { and } \varphi_{i, j}\left(x_{k}\right)=x_{k} \text { for } k \notin\{i, j\}
$$

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

Proposition 2.3. If $\mathcal{X}$ is a full subset of $\mathcal{S}$, then $\varphi_{\mathcal{X}}: K B_{n}(\mathcal{X}) \rightarrow \operatorname{Aut}\left(F_{n}\right)$ is faithful.
Remark. The whole representation $\varphi: K B_{n} \rightarrow \operatorname{Aut}\left(F_{n}\right)$ 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 $K B_{n}$ 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 $\mathcal{S}^{ \pm 1}$, then $\bar{u}$ will denote the element of $K B_{n}$ 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 $\varphi(\bar{u})=\varphi\left(s_{1}\right)^{\varepsilon_{1}} \cdots \varphi\left(s_{\ell}\right)^{\varepsilon_{\ell}}$. 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 $K B_{n}(\mathcal{X})$ has a solution to the word problem, and, from this solution, we will give a solution to the membership problem for $K B_{n}(\mathcal{Y})$ in $K B_{n}(\mathcal{X})$, for $\mathcal{Y} \subset \mathcal{X}$. Furthermore, if the tested element belongs to $K B_{n}(\mathcal{Y})$, then this algorithm will determine a word over $\mathcal{Y}^{ \pm 1}$ which represents this element.

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

- Suppose that $u$ is written in the form $u_{1} s s u_{2}$, where $u_{1}, u_{2}$ are words over $\mathcal{S}$ and $s$ is an element of $\mathcal{S}$. Then we say that $u^{\prime}=u_{1} u_{2}$ is obtained from $u$ by an $M$-operation of type I.
- Suppose that $u$ is written in the form $u_{1} s t u_{2}$, where $u_{1}, u_{2}$ are words over $\mathcal{S}$ and $s, t$ are two elements of $\mathcal{S}$ connected by an edge labelled by 2 . Then we say that $u^{\prime}=u_{1} t s u_{2}$ is obtained from $u$ by an $M$-operation of type $\mathrm{II}^{(2)}$.
- Suppose that $u$ is written in the form $u_{1} s t s u_{2}$, where $u_{1}, u_{2}$ are words over $\mathcal{S}$ and $s, t$ are two elements of $\mathcal{S}$ connected by an edge labelled by 3 . Then we say that $u^{\prime}=u_{1} t s t u_{2}$ is obtained from $u$ by an $M$-operation of type $\mathrm{II}^{(3)}$.
Let $\mathcal{Y}$ be a subset of $\mathcal{S}$.
- Suppose that $u$ is written in the form $t u^{\prime}$, where $u^{\prime}$ is a word over $\mathcal{S}$ and $t$ is an element of $\mathcal{Y}$. Then we say that $u^{\prime}$ is obtained from $u$ by an $M$-operation of type $\mathrm{III}_{\mathcal{Y}}$.

We say that $u$ is $M$-reduced (resp. $M_{\mathcal{Y}}$-reduced) if its length cannot be shortened by $M$ operations of type $\mathrm{I}, \mathrm{II}^{(2)}, \mathrm{II}^{(3)}$ (resp. of type $\mathrm{I}, \mathrm{II}^{(2)}, \mathrm{II}^{(3)}, \mathrm{III} \mathcal{Y}$ ). An $M$-reduction (resp. Myreduction) 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 $i \in\{0,1, \ldots, \ell\}$ we set $u_{i}^{+}=s_{1} \cdots s_{i}$ (as ever, $u_{0}^{+}$is the identity).
- For $i \in\{0,1, \ldots, \ell\}$ we calculate an $M_{y}$-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 $w_{i}^{+}=v_{i-1}^{+} \cdot s_{i} \cdot \mathrm{op}\left(v_{i-1}^{+}\right)$. If $\varepsilon_{i}=-1$, we set $w_{i}^{+}=v_{i}^{+} \cdot s_{i} \cdot \operatorname{op}\left(v_{i}^{+}\right)$.
- 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 $\overline{\pi_{\mathcal{Y}}(u)}=\overline{\pi_{\mathcal{Y}}(v)}$. Moreover, we have $\bar{u} \in K B_{n}(\mathcal{Y})$ if and only if $\bar{u}=\overline{\pi_{\mathcal{Y}}(u)}$.

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 $K B_{n}(\mathcal{X})$. Let $u$ be a word over $\mathcal{X}^{ \pm 1}$. We calculate $v=\pi_{\mathcal{Y}}(u)$. If $\overline{u v^{-1}} \neq 1$, then $\bar{u} \notin K B_{n}(\mathcal{Y})$. If $\overline{u v^{-1}}=1$, then $\bar{u} \in K B_{n}(\mathcal{Y})$ 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 $K B_{n}(\mathcal{Y})$ 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 $\mathcal{X}_{1}=\mathcal{X} \backslash\left\{s_{1}\right\}$, $\mathcal{X}_{2}=\mathcal{X} \backslash\left\{s_{2}\right\}$, and $\mathcal{X}_{0}=\mathcal{X} \backslash\left\{s_{1}, s_{2}\right\}$. It follows from the presentations of the $K B_{n}\left(\mathcal{X}_{i}\right)$ 's given in Step 2 that we have the amalgamated product

$$
K B_{n}(\mathcal{X})=K B_{n}\left(\mathcal{X}_{1}\right) *_{K B_{n}}\left(\mathcal{X}_{0}\right) K B_{n}\left(\mathcal{X}_{2}\right) .
$$

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 $g_{1}, \ldots, g_{\ell}$ be a sequence of elements of $A_{1} \sqcup A_{2}$ different from 1 and satisfying the following condition:

$$
\text { if } g_{i} \in A_{1} \text { (resp. } g_{i} \in A_{2} \text { ), then } g_{i+1} \in A_{2} \backslash B\left(\text { resp. } g_{i+1} \in A_{1} \backslash B\right) \text {, for all } i \in\{1, \ldots, \ell-1\}
$$

Then $g_{1} g_{2} \cdots g_{\ell}$ 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 $\mathcal{X}_{1}^{ \pm 1}$, or a word over $\mathcal{X}_{2}^{ \pm 1}$,
- if $u_{i}$ is a word over $\mathcal{X}_{1}^{ \pm 1}\left(\right.$ resp. over $\left.\mathcal{X}_{2}^{ \pm 1}\right)$, then $u_{i+1}$ is a word over $\mathcal{X}_{2}^{ \pm 1}$ (resp. over $\left.\mathcal{X}_{1}^{ \pm 1}\right)$. We decide whether $\bar{u}$ is trivial by induction on $\ell$. Suppose that $\ell=1$ and $u=u_{1} \in K B_{n}\left(\mathcal{X}_{j}\right)$ $(j \in\{1,2\})$. Then we apply the solution to the word problem for $K B_{n}\left(\mathcal{X}_{j}\right)$ to decide whether $\bar{u}$ is trivial or not. Suppose that $\ell \geq 2$. For all $i$ we set $v_{i}=\pi_{\mathcal{X}_{0}}\left(u_{i}\right)$. If $\overline{u_{i} v_{i}^{-1}} \neq 1$ for all $i$, then $\bar{u} \neq 1$. Suppose that there exists $i \in\{1, \ldots, \ell\}$ such that $\overline{u_{i} v_{i}^{-1}}=1$. Let $u_{i}^{\prime}=v_{1} u_{2}$ if $i=1$, $u_{i}^{\prime}=u_{\ell-1} v_{\ell}$ if $i=\ell$, and $u_{i}^{\prime}=u_{i-1} v_{i} u_{i+1}$ if $2 \leq i \leq \ell-1$. Set $v=u_{1} \cdots u_{i-2} u_{i}^{\prime} u_{i+2} \cdots u_{\ell}$. 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 $F_{n}=F\left(x_{1}, \ldots, x_{n}\right)$ denotes the free group of rank $n$ freely generated by $x_{1}, \ldots, x_{n}$, and that we have a representation $\varphi: K B_{n} \rightarrow \operatorname{Aut}\left(F_{n}\right)$ which sends $\delta_{i, j}$ to $\varphi_{i, j}$, where

$$
\varphi_{i, j}\left(x_{i}\right)=x_{i} x_{j} x_{i}^{-1}, \varphi_{i, j}\left(x_{j}\right)=x_{i}, \text { and } \varphi_{i, j}\left(x_{k}\right)=x_{k} \text { for } k \notin\{i, j\}
$$

For $\mathcal{X} \subset \mathcal{S}$, we denote by $\varphi_{\mathcal{X}}: K B_{n}(\mathcal{X}) \rightarrow \operatorname{Aut}\left(F_{n}\right)$ the restriction of $\varphi$ to $K B_{n}(\mathcal{X})$. 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.

$$
\begin{gathered}
B_{n}=\left\langle\sigma_{1}, \ldots, \sigma_{n-1} \left\lvert\, \begin{array}{cl}
\sigma_{i} \sigma_{j} \sigma_{i}=\sigma_{j} \sigma_{i} \sigma_{j} & \text { if }|i-j|=1 \\
\sigma_{i} \sigma_{j}=\sigma_{j} \sigma_{i} & \text { if }|i-j| \geq 2
\end{array}\right.\right\rangle \\
\tilde{B}_{n}=\left\langle\sigma_{1}, \ldots, \sigma_{n} \left\lvert\, \begin{array}{cl}
\sigma_{i} \sigma_{j} \sigma_{i}=\sigma_{j} \sigma_{i} \sigma_{j} & \text { if } i \equiv j \pm 1 \quad \bmod n \\
\sigma_{i} \sigma_{j}=\sigma_{j} \sigma_{i} & \text { if } i \neq j \text { and } i \not \equiv j \pm 1 \quad \bmod n
\end{array}\right.\right\rangle, \quad n \geq 3 .
\end{gathered}
$$

The group $B_{n}$ is the classical braid group, and $\tilde{B}_{n}$ is the affine braid group.
We define representations $\psi_{n}: B_{n} \rightarrow \operatorname{Aut}\left(F_{n}\right)$ and $\tilde{\psi}_{n}: \tilde{B}_{n} \rightarrow \operatorname{Aut}\left(F_{n}\right)$ in the same way as $\varphi$ as follows.

$$
\begin{gathered}
\psi_{n}\left(\sigma_{i}\right)\left(x_{i}\right)=x_{i} x_{i+1} x_{i}^{-1}, \psi_{n}\left(\sigma_{i}\right)\left(x_{i+1}\right)=x_{i}, \psi_{n}\left(\sigma_{i}\right)\left(x_{k}\right)=x_{k} \text { if } k \notin\{i, i+1\} \\
\tilde{\psi}_{n}\left(\sigma_{i}\right)\left(x_{i}\right)=x_{i} x_{i+1} x_{i}^{-1}, \tilde{\psi}_{n}\left(\sigma_{i}\right)\left(x_{i+1}\right)=x_{i}, \tilde{\psi}_{n}\left(\sigma_{i}\right)\left(x_{k}\right)=x_{k} \text { if } k \notin\{i, i+1\}, \text { for } i<n \\
\tilde{\psi}_{n}\left(\sigma_{n}\right)\left(x_{n}\right)=x_{n} x_{1} x_{n}^{-1}, \tilde{\psi}_{n}\left(\sigma_{n}\right)\left(x_{1}\right)=x_{n}, \tilde{\psi}_{n}\left(\sigma_{n}\right)\left(x_{k}\right)=x_{k} \text { if } k \notin\{1, n\}
\end{gathered}
$$

The key of the proof of Proposition 2.3 is the following.
$\underset{\sim}{\text { Theorem }} 3.1$ (Artin [1], Bellingeri, Bodin [4]). The representations $\psi_{n}: B_{n} \rightarrow \operatorname{Aut}\left(F_{n}\right)$ and $\tilde{\psi}_{n}: \tilde{B}_{n} \rightarrow \operatorname{Aut}\left(F_{n}\right)$ are faithful.

The support of a generator $\delta_{i, j}$ is defined to be $\operatorname{supp}\left(\delta_{i, j}\right)=\{i, j\}$. The support of a subset $\mathcal{X}$ of $\mathcal{S}$ is $\operatorname{supp}(\mathcal{X})=\cup_{s \in \mathcal{X}} \operatorname{supp}(s)$. We say that two subsets $\mathcal{X}_{1}$ and $\mathcal{X}_{2}$ of $\mathcal{S}$ are perpendicular ${ }^{1}$ if $\operatorname{supp}\left(\mathcal{X}_{1}\right) \cap \operatorname{supp}\left(\mathcal{X}_{2}\right)=\emptyset$. 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 $\operatorname{supp}\left(\mathcal{X}_{i}\right) \cap \operatorname{supp}\left(\mathcal{X}_{j}\right)=\emptyset$ 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) $K B_{n}(\mathcal{X})=K B_{n}\left(\mathcal{X}_{1}\right) \times K B_{n}\left(\mathcal{X}_{2}\right)$.

Indeed, if $\delta_{i, j} \in \mathcal{X}_{1}$ and $\delta_{k, \ell} \in \mathcal{X}_{2}$, then $i, j, k, \ell$ 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 $\varphi_{\mathcal{X}}: K B_{n}(\mathcal{X}) \rightarrow \operatorname{Aut}\left(F_{n}\right)$ is faithful if and only if $\varphi_{\mathcal{X}_{1}}: K B_{n}\left(\mathcal{X}_{1}\right) \rightarrow \operatorname{Aut}\left(F_{n}\right)$ and $\varphi_{\mathcal{X}_{2}}:$ $K B_{n}\left(\mathcal{X}_{2}\right) \rightarrow \operatorname{Aut}\left(F_{n}\right)$ are both faithful.

Proof. For $X \subset\left\{x_{1}, \ldots, x_{n}\right\}$, we denote by $F(X)$ the subgroup of $F_{n}$ generated by $X$. There is a natural embedding $\iota_{X}: \operatorname{Aut}(F(X)) \hookrightarrow \operatorname{Aut}\left(F_{n}\right)$ defined by

$$
\iota_{X}(\alpha)\left(x_{i}\right)= \begin{cases}\alpha\left(x_{i}\right) & \text { if } x_{i} \in X \\ x_{i} & \text { otherwise }\end{cases}
$$

Moreover, if $X_{1}$ and $X_{2}$ are disjoint subsets of $\left\{x_{1}, \ldots, x_{n}\right\}$, then the homomorphism

$$
\begin{array}{ccc}
\left(\iota_{X_{1}} \times \iota_{X_{2}}\right): \operatorname{Aut}\left(F\left(X_{1}\right)\right) \times \operatorname{Aut}\left(F\left(X_{2}\right)\right) & \rightarrow & \operatorname{Aut}\left(F_{n}\right) \\
\left(\alpha_{1}, \alpha_{2}\right) & \mapsto \iota_{X_{1}}\left(\alpha_{1}\right) \iota_{X_{2}}\left(\alpha_{2}\right)
\end{array}
$$

is well-defined and injective. From now on, we will assume $\operatorname{Aut}(F(X))$ to be embedded in $\operatorname{Aut}\left(F_{n}\right)$ via $\iota_{X}$, for all $X \subset\left\{x_{1}, \ldots, x_{n}\right\}$.

By abuse of notation, for $\mathcal{X} \subset \mathcal{S}$, we will also denote by $\operatorname{supp}(\mathcal{X})$ the $\operatorname{set}\left\{x_{i} \mid i \in \operatorname{supp}(\mathcal{X})\right\}$. Set $X_{1}=\operatorname{supp}\left(\mathcal{X}_{1}\right)$ and $X_{2}=\operatorname{supp}\left(\mathcal{X}_{2}\right)$. We have $\operatorname{Im}\left(\varphi \mathcal{X}_{i}\right) \subset \operatorname{Aut}\left(F\left(X_{i}\right)\right)$ for $i=1,2, X_{1} \cap X_{2}=\emptyset$, and $K B_{n}(\mathcal{X})=K B_{n}\left(\mathcal{X}_{1}\right) \times K B_{n}\left(\mathcal{X}_{2}\right)$. Hence, Lemma 3.2 follows from the following claim whose proof is left to the reader.

Claim. Let $f_{1}: G_{1} \rightarrow H_{1}$ and $f_{2}: G_{2} \rightarrow H_{2}$ be two group homomorphisms. Let $\left(f_{1} \times f_{2}\right)$ : $\left(G_{1} \times G_{2}\right) \rightarrow\left(H_{1} \times H_{2}\right)$ be the homomorphism defined by $\left(f_{1} \times f_{2}\right)\left(u_{1}, u_{2}\right)=\left(f_{1}\left(u_{1}\right), f_{2}\left(u_{2}\right)\right)$. Then $\left(f_{1} \times f_{2}\right)$ is injective if and only if $f_{1}$ and $f_{2}$ are both injective.

[^0]For $2 \leq m \leq n$ we set

$$
\mathcal{Z}_{m}=\left\{\delta_{1,2}, \ldots, \delta_{m-1, m}\right\}, \tilde{\mathcal{Z}}_{m}=\left\{\delta_{1,2}, \ldots, \delta_{m-1, m}, \delta_{m, 1}\right\}
$$

Note that the map $\left\{\sigma_{1}, \ldots, \sigma_{m-1}\right\} \rightarrow \mathcal{Z}_{m}, \sigma_{i} \mapsto \delta_{i, i+1}$, induces an isomorphism $f_{m}: B_{m} \rightarrow$ $K B_{n}\left(\mathcal{Z}_{m}\right)$. This follows from the presentation of $K B_{n}\left(\mathcal{Z}_{m}\right)$ given in Step 2 of Section 2. Similarly, for $m \geq 3$, the $\operatorname{map}_{\tilde{\sim}}\left\{\sigma_{1}, \ldots, \sigma_{m}\right\} \rightarrow \tilde{\mathcal{Z}}_{m}, \sigma_{i} \mapsto \delta_{i, i+1}$ for $1 \leq i \leq m-1, \sigma_{m} \mapsto \delta_{m, 1}$, induces an isomorphism $\tilde{f}_{m}: \tilde{B}_{m} \rightarrow K B_{n}\left(\tilde{\mathcal{Z}}_{m}\right)$.

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 $K B_{n}$. On the other hand, there is a natural embedding $\mathfrak{S}_{n} \hookrightarrow \operatorname{Aut}\left(F_{n}\right)$, 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 $\operatorname{Aut}\left(F_{n}\right)$. It is easily seen that the homomorphism $\varphi: K B_{n} \rightarrow \operatorname{Aut}\left(F_{n}\right)$ 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 $\Upsilon$ 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 : $E(\Upsilon) \rightarrow V(\Upsilon)$. We associate an oriented graph $\Upsilon_{\mathcal{X}}$ to any subset $\mathcal{X}$ of $\mathcal{S}$ as follows. The set of vertices is $V\left(\Upsilon_{\mathcal{X}}\right)=\operatorname{supp}(\mathcal{X})$, the set of arrows is $E\left(\Upsilon_{\mathcal{X}}\right)=\mathcal{X}$, and, for $\delta_{i, j} \in \mathcal{X}$, we set $\operatorname{sou}\left(\delta_{i, j}\right)=i$ and $\operatorname{tar}\left(\delta_{i, j}\right)=j$. 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 $\mathcal{X}=g \mathcal{Z}_{m}$. 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 $\mathcal{X}=g \tilde{\mathcal{Z}}_{m}$.


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 $\varphi$ 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 $Z_{m}=\left\{x_{1}, \ldots, x_{m}\right\}=\operatorname{supp}\left(\mathcal{Z}_{m}\right)=$ $\operatorname{supp}\left(\tilde{\mathcal{Z}}_{m}\right)$, and identify $F_{m}$ with $F\left(Z_{m}\right)$. 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.

## 4 Proof of Proposition 2.4

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 $M=\left(m_{s, t}\right)_{s, t \in S}$, indexed by the elements of $S$, such that $m_{s, s}=1$ for all $s \in S$, and $m_{s, t}=m_{t, s} \in\{2,3,4, \ldots\} \cup\{\infty\}$ 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 $\Gamma$ 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 $\geq 2$, we set $\langle a, b\rangle^{m}=(a b)^{\frac{m}{2}}$ if $m$ is even, and $\langle a, b\rangle^{m}=(a b)^{\frac{m-1}{2}} a$ if $m$ id odd. The Artin group of $\Gamma$ is the group $A=A(\Gamma)$ defined by the following presentation.

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

The Coxeter group of $\Gamma$, 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 $\Gamma_{Y}$ the subdiagram of $\Gamma$ 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 $\Gamma_{Y}$, and, by [5], $W_{Y}$ is the Coxeter group of $\Gamma_{Y}$.

Let $u$ be a word over $S$.

- Suppose that $u$ is written in the form $u_{1} s s u_{2}$, where $u_{1}, u_{2}$ are words over $S$ and $s$ is an element of $S$. Then we say that $u^{\prime}=u_{1} u_{2}$ 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

$$
u^{\prime}=u_{1}\langle t, s\rangle^{m_{s, t}} u_{2},
$$

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 $t u^{\prime}$, where $u^{\prime}$ is a word over $S$ and $t$ is an element of $Y$. Then we say that $u^{\prime}$ is obtained from $u$ by an $M$-operation of type $\mathrm{III}_{Y}$.

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, $\mathrm{II}, \mathrm{III}_{Y}$ ). 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 $i \in\{0,1, \ldots, \ell\}$ we set $u_{i}^{+}=s_{1} \cdots s_{i}$.
- For all $i \in\{0, \ldots, \ell\}$ we calculate an $M_{Y}$-reduction $v_{i}^{+}$of $u_{i}^{+}$.
- Let $i \in\{1, \ldots, \ell\}$. If $\varepsilon_{i}=1$, we set $w_{i}^{+}=v_{i-1}^{+} \cdot s_{i} \cdot \operatorname{op}\left(v_{i-1}^{+}\right)$. If $\varepsilon_{i}=-1$, we set $w_{i}^{+}=v_{i}^{+} \cdot s_{i} \cdot \operatorname{op}\left(v_{i}^{+}\right)$.
- 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 $\overline{\pi_{Y}(u)}=\overline{\pi_{Y}(v)}$. Moreover, we have $\bar{u} \in A_{Y}$ if and only if $\bar{u}=\overline{\pi_{Y}(u)}$.

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) $\lg _{S}(s g)>\lg _{S}(g)$ for all $s \in Y$,
(c) $\lg _{S}(h g)=\lg _{S}(h)+\lg _{S}(g)$ for all $h \in W_{Y}$.

A "nice" set-retraction $\rho_{Y}: A \rightarrow A_{Y}$ to the inclusion $\iota_{Y}: A_{Y} \rightarrow A$ is constructed in [8, 6]. This is defined as follows (we refer to [6] for its correctness). Let $\alpha$ be an element of $A$. Let $\widehat{\alpha}=s_{1}{ }^{\varepsilon_{1}} \cdots s_{\ell}{ }^{\varepsilon_{\ell}}$ be a word over $S^{ \pm 1}$ which represents $\alpha$. 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

$$
\begin{gathered}
\tau_{i}= \begin{cases}x_{i}{ }^{\varepsilon_{i}} & \text { if } x_{i} \in Y \\
1 & \text { otherwise }\end{cases} \\
\widehat{\tau}=\tau_{1} \tau_{2} \cdots \tau_{\ell} .
\end{gathered}
$$

Then $\rho_{Y}(\alpha)$ is the element of $A_{Y}$ represented by $\widehat{\tau}$.
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 $w^{\prime}$ 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.

## 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, $S L_{2}$. 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


[^0]:    ${ }^{1}$ This terminology is derived from the theory of Coxeter groups.

