# The rotating normal form of braids is regular

Jean Fromentin

# THE ROTATING NORMAL FORM IS REGULAR

JEAN FROMENTIN

Abstract. Defined on Birman–Ko–Lee monoids, the rotating normal form has strong connections with the Dehornoy's braid ordering. It can be seen as a process for selecting between all the representative words of a Birman–Ko–Lee braid a particular one, called *rotating* word. In this paper we construct, for all $n \geqslant 2$, a finite state automaton which recognizes the rotating words on $n$ strands. As a consequence the language of rotating words on $n$ strands is proved to be regular for any $n \geqslant 2$.

## 1. Introduction

Originally, the group $B_n$ of $n$-strand braids was defined as the group of isotopy classes of $n$-strand geometric braids. An algebraic presentation of $B_n$ was given by E. Artin in [1]

$$\left\langle \sigma_1, \dots, \sigma_{n-1} \;\middle|\; \begin{array}{rcll} \sigma_i\sigma_j &=& \sigma_j\sigma_i & \text{for } |i-j| \geqslant 2 \\ \sigma_i\sigma_j\sigma_i &=& \sigma_j\sigma_i\sigma_j & \text{for } |i-j| = 1 \end{array} \right\rangle. \tag{1}$$

An $n$-strand braid is an equivalence class consisting of (infinitely many) words in the letters $\sigma_i^{\pm 1}$. The standard correspondence between elements of the presented group $B_n$ and geometric braids consists in using $\sigma_i$ as a code for the geometric braid where only the $i$th and the $(i+1)$st strands cross, with the strands originally at position $(i+1)$ in front of the other.

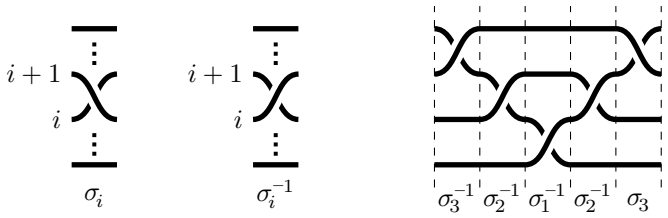



Figure 1. Interpretation of a word in the letters $\sigma_i^{\pm 1}$ as a geometric braid diagram.

2010 *Mathematics Subject Classification.* 20F36, 20M35, 20F10.

*Key words and phrases.* dual braid monoid, rotating normal form, regular language, automata.

In 1998, J.S. Birman, K.H. Ko, and S.J. Lee [3] introduced and investigated for each $n$ a submonoid $B_n^{+*}$ of $B_n$, which is known as the *Birman–Ko–Lee* monoid. The name "*dual braid monoid*" was subsequently proposed because several numerical parameters obtain symmetric values when they are evaluated on the positive braid monoid $B_n^+$ and on $B_n^{+*}$, a correspondence that was extended to the more general context of Artin–Tits groups by D. Bessis [2] in 2003. The dual braid monoid $B_n^{+*}$ is the submonoid of $B_n$ generated by the braids $a_{i,j}$ with $1 \leqslant i < j \leqslant n$, where $a_{i,j}$ is defined by $a_{i,j} = \sigma_i \dots \sigma_{j-1}\ \sigma_j\ \sigma_{j-1}^{-1} \dots \sigma_i^{-1}$. In geometrical terms, the braid $a_{i,j}$ corresponds to a crossing of the $i$th and $j$th strands, both passing behind the (possible) intermediate strands.

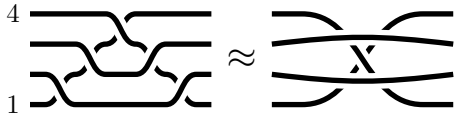



FIGURE 2. In the geometric braid $a_{1,4}$, the strands 1 and 4 cross under the strands 2 and 3.

By definition, $\sigma_i$ equals $a_{i,i+1}$ and, therefore, the positive braid monoid $B_n^+$ is included in the monoid $B_n^{+*}$, a proper inclusion for $n \geqslant 3$ since the braid $a_{1,3}$ does not belong to the monoid $B_3^+$.

We denote by $A_n$ the set $\{a_{p,q} \,|\, 1 \leqslant p < q \leqslant n\}$. The following presentation of the monoid $B_n^{+*}$ is given in [3].

**Proposition 1.1.** *The monoid $B_n^{+*}$ is presented by generators $A_n$ and relations*

$$a_{p,q}a_{r,s} = a_{r,s}a_{p,q} \quad \textit{for } [p,q] \textit{ and } [r,s] \textit{ disjoint or nested}, \tag{2}$$

$$a_{p,q}a_{q,r} = a_{q,r}a_{p,r} = a_{p,r}a_{p,q} \quad \textit{for } 1 \leqslant p < q < r \leqslant n. \tag{3}$$

The integral interval $[p,q]$ is said to be *nested* in $[r,s]$ if the relation $r < p < q < s$ holds.

Since [2] and [3] it is known that the dual braid monoid $B_n^{+*}$ admits a Garside structure whose simple elements are in bijection with the non-crossing partitions of $n$. In particular, there exists a normal form associated with this Garside structure, the so-called greedy normal form.

The rotating normal form is another normal form on $B_n^{+*}$, it was introduced in [8, 9]. Roughly speaking, for every braid $\beta \in B_n^{+*}$ the rotating normal form picks up a unique representative word on the letters $A_n$ among all of these representing $\beta$. It can be see as a map $r_n$ from the dual braid monoid $B_n^{+*}$ to the set of words $A_n^*$. The language of all $n$-rotating words, denoted by $R_n$ is then the image of $B_n^{+*}$ under the map $r_n$.

The aim of this paper is to construct for all $n \geqslant 2$ an explicit finite state automaton which recognizes the language $R_n$. As a consequence we obtain that the language $R_n$ of $n$-rotating words is regular.

The paper is divided as follow. In section 2 we recall briefly the construction of the rotating normal form and its useful already known properties. In third section we describe the left reversing process on dual braid monoids. In section 4 we give a syntactical characterization of $n$-rotating normal words. In fifth section we construct, for each $n \geqslant 2$, a finite state automaton which recognizes the language $R_n$ of $n$-rotating normal words.

## 2. The rotating normal form

The main ingredient to define the rotating normal form is the Garside automorphism $\phi_n$ of $B_n^{+*}$ defined by $\phi_n(\beta) = \delta_n\,\beta\,\delta_n^{-1}$ where $\delta_n = a_{1,2}\,a_{2,3}\,...a_{n-1,n}$ is the Garside braid of $B_n^{+*}$. In terms of Birman–Ko–Lee generators, the map $\phi_n$ can be defined by

$$\phi_n(a_{p,q}) = \begin{cases} a_{p+1,q+1} & \text{for } q \leqslant n-1, \\ a_{1,p+1} & \text{for } q = n. \end{cases} \tag{4}$$

Geometrically, $\phi_n$ should be viewed as a rotation, which makes sense provided braid diagrams are drawn on a cylinder rather than on a plane rectangle.

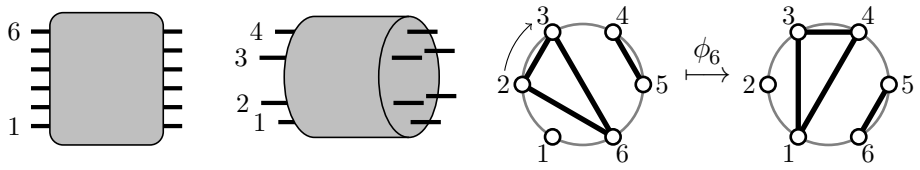



FIGURE 3. Rolling up the usual braid diagram helps us to visualize the symmetries of the braids $a_{p,q}$. On the resulting cylinder, $a_{p,q}$ naturally corresponds to the chord connecting vertices $p$ and $q$. With this representation, $\phi_n$ acts as a clockwise rotation of the marked circles by $2\pi/n$.

For $\beta$ and $\gamma$ in $B_n^{+*}$, we say that $\gamma$ is a *right-divisor* of $\beta$, if there exists a dual braid $\beta'$ of $B_n^{+*}$ satisfying $\beta = \beta'\,\gamma$.

**Definition 2.1.** For $n \geqslant 3$ and $\beta$ a braid of $B_n^{+*}$, the maximal braid $\beta_1$ lying in $B_{n-1}^{+*}$ that right divides the braid $\beta$ is called the $B_{n-1}^{+*}$-*tail* of $\beta$.

Using basic Garside properties of the monoid $B_n^{+*}$ we obtain the following result (Proposition 2.5 of [9]) which allow us to express each braid of $B_n^{+*}$ as a unique finite sequence of braids lying in $B_{n-1}^{+*}$.

**Proposition 2.2.** *Assume $n \geqslant 3$. For each nontrivial braid $\beta$ of $B_n^{+*}$ there exists a unique sequence $(\beta_b, \dots, \beta_1)$ of braids of $B_{n-1}^{+*}$ satisfying $\beta_b \neq 1$ and*

$$\beta = \phi_n^{b-1}(\beta_b) \cdot \ldots \cdot \phi_n(\beta_2) \cdot \beta_1, \tag{5}$$

*for each $k \geqslant 1$, the $B_{n-1}^{+*}$-tail of $\phi_n^{b-k}(\beta_b) \cdot \ldots \cdot \phi_n(\beta_{k+1})$ is trivial.* (6)

Under the above hypotheses, the sequence $(\beta_b, \dots, \beta_1)$ is called the $\phi_n$-*splitting* of the braid $\beta$. It is shown in [9] that Condition (6) can be replaced by

$$\text{for each } k \leqslant 1,\ \beta_k \text{ is the } B_{n-1}^{+*}\text{-tail of } \phi_n^{b-k}(\beta_b) \cdot \dots \cdot \phi_n(\beta_{k-1}) \cdot \beta_k. \qquad (7)$$

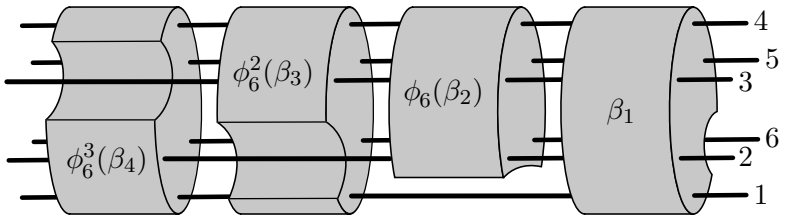



FIGURE 4. The $\phi_6$-splitting of a braid of $B_6^{+*}$. Starting from the right, we extract the maximal right-divisor that keeps the sixth strand unbraided, then extract the maximal right-divisor that keeps the first strand unbraided, etc.

**Example 2.3.** Consider the braid $\beta = a_{1,2}a_{2,3}a_{1,2}a_{2,3}$ of $B_3^{+*}$. Using relations (3) on the underlined factors we obtain

$$\beta = a_{1,2}a_{2,3}\underline{a_{1,2}a_{2,3}} = a_{1,2}\underline{a_{2,3}a_{1,3}}a_{1,2} = a_{1,2}a_{1,3}a_{1,2}a_{1,2}$$

We decompose $\beta$ as $\phi_3(\gamma_1) \cdot \beta_1$ with $\gamma_1 = \phi_3^{-1}(a_{1,2}a_{1,3}) = a_{1,3}a_{2,3}$ and $\beta_1 = a_{1,2}a_{1,2}$. The braid $\phi_3(\gamma_1) = a_{1,2}a_{2,3}$ is exactly the one of (6) for $n = 3$ and $k = 1$. As the word $a_{1,3}a_{2,3}$ is alone in its equivalence class the braid $\phi_3(\gamma_1)$ is not right divisible by $a_{1,2}$ and so its $B_2^{+*}$-tail is trivial. Considering $\gamma_1$ instead of $\beta$ we obtain $\gamma_1 = \phi_3(\gamma_2) \cdot \beta_2$ with $\gamma_2 = \phi_3^{-1}(a_{1,3}a_{2,3}) = a_{2,3}a_{1,2}$ and $\beta_2 = 1$. The braid $\phi_3(\gamma_2) = a_{1,3}a_{2,3}$ is the braid of (6) for $n = 3$ and $k = 2$ and it is always alone in its equivalence class, implying that its $B_2^{+*}$-tail is trivial. We express $\gamma_2$ as $\phi_3(\gamma_3) \cdot \beta_3$ with $\gamma_3 = \phi_3^{-1}(a_{2,3}) = a_{1,2}$ and $\beta_3 = a_{1,2}$. Since $\gamma_3$ equals $a_{1,2}$ we obtain $\gamma_4 = 1$ and $\beta_4 = a_{1,2}$. We conclude that the $\phi_3$-splitting of $\beta$ is $(a_{1,2}, a_{1,2}, 1, a_{1,2}^2)$.

Before giving the definition of the rotating normal we fix some definitions about words.

**Definition 2.4.** A word on the alphabet $A_n$ is an $A_n$-*word*. A word on the alphabet $A_n^{\pm} = A_n \sqcup A_n^{-1}$ is an $A_n^{\pm}$-*word*. The braid represented by the $A_n^{\pm}$-word $w$ is denoted by $\overline{w}$. For $w$, $w'$ two $A_n^{\pm}$-word, we say that $w$ is equivalent to $w'$, denoted by $w \equiv w'$ if $\overline{w} = \overline{w'}$ holds. The empty word is denoted by $\varepsilon$.

The $n$-*rotating normal form* is an injective map $r_n$ from $B_n^{+*}$ to the set of $A_n$-words defined inductively using the $\phi_n$-splitting.

**Definition 2.5.** For $\beta \in B_2^{+*}$, we define $r_2(\beta)$ to be the unique word $a_{1,2}^k$ representing $\beta$. The rotating normal form of a braid $\beta \in B_n^{+*}$ with $n \geqslant 3$ is

$$r_n(\beta) = \phi_n^{b-1}(r_{n-1}(\beta_b)) \cdot \ldots \cdot \phi_n(r_{n-1}(\beta_2)) \cdot r_{n-1}(\beta_1),$$

where $(\beta_b, \ldots, \beta_1)$ is the $\phi_n$-splitting of $\beta$. A word $w$ is said to be *$n$-rotating* if it is the $n$-rotating normal form of a braid of $B_n^{+*}$.

As the $n$-rotating normal form of a braid of $B_{n-1}^{+*}$ is equal to its $(n-1)$-rotating normal form we can talk without ambiguities of the *rotating normal form* about a dual braid.

**Example 2.6.** We reconsider the braid $\beta$ of Example 2.3. We know that the $\phi_3$-splitting of $\beta$ is $(a_{1,2}, a_{1,2}, 1, a_{1,2}^2)$. Since $r_2(1) = \varepsilon$, $r_2(a_{1,2}) = a_{1,2}$ and $r_2(a_{1,2}^2) = a_{1,2}^2$ we obtain

$$r_3(\beta) = \phi_3^3(a_{1,2}) \cdot \phi_3^2(a_{1,2}) \cdot \phi_3(\varepsilon) \cdot a_{1,2}^2 = a_{1,2}a_{1,3}a_{1,2}a_{1,2}.$$

Some properties of the rotating normal form have been established in [9]. Connections, established in [8] and [9], between the rotating normal form and the braid's ordering introduced by P. Dehornoy are based on these properties.

We finish this section with some already known or immediate properties about $\phi_n$-splittings and $n$-rotating words.

**Definition 2.7.** For every nonempty word $w$, the last letter of $w$ is denoted by $w^\#$. For each nontrivial braid $\beta$ in $B_n^{+*}$, we define the *last letter* of $\beta$, denoted $\beta^\#$, to be the last letter in the rotating normal form of $\beta$.

**Lemma 2.8** (Lemma 3.2 of [9])**.** *Assume $n \geqslant 3$ and let $(\beta_b, \ldots, \beta_1)$ be a $\phi_n$-splitting*

*(i) For $k \geqslant 2$, the letter $\beta_k^\#$ is of type $a_{\cdot\cdot,n-1}$ unless $\beta_k = 1$.*

*(ii) For $k \geqslant 3$ and $k = b$, we have $\beta_k \neq 1$.*

The fact that $\beta_b$ is not trivial is a direct consequence of the definition of $\phi_n$-splitting. As, for $k \geqslant 2$, the braid $\beta' = \phi_n(\beta_{k+1}^\#)\beta_k$ is a right-divisor of $\phi_n^{b-k}(\beta_b) \cdot \ldots \cdot \beta_k$, it must satisfy some properties. In particular, if $\beta_{k+1}^\# = a_{p-1,n-1}$ holds then the $B_{n-1}^{+*}$-tail of $\phi_n(a_{p,n}\beta_k)$ is trivial by (6).

**Definition 2.9.** We say that a letter $a_{r,s}$ is an *$a_{p,n}$-barrier* if $1 \leqslant r < p < s \leqslant n-1$ holds.

There exist no $a_{p,n}$-barrier with $n \leqslant 3$ and the only $a_{p,4}$-barrier is $a_{1,3}$, which is an $a_{2,4}$-barrier. By definition, if the letter $x$ is an $a_{p,n}$-barrier, then in the presentation of $B_n^{+*}$ there exists no relation of the form $a_{p,n} \cdot x = y \cdot a_{p,n}$ allowing one to push the letter $a_{p,n}$ to the right through the letter $x$: so, in some sense, $x$ acts as a barrier.

**Lemma 2.10** (Lemma 3.4 of [9])**.** *Assume that $n \geqslant 3$, $\beta$ is a braid of $B_{n-1}^{+*}$ and the $B_{n-1}^{+*}$-tail of $\phi_n(a_{p,n}\beta)$ is trivial for $2 \leqslant p \leqslant n-2$. Then the rotating normal form of $\beta$ is not the empty word and it contains an $a_{p,n}$-barrier.*

**Lemma 2.11** (Lemma 3.5 of [9]). *Let $(\beta_b, ..., \beta_1)$ be a $\phi_n$-splitting of some braid of $B_n^{+*}$ with $n \geqslant 3$. Then for each $k \in [2, b-1]$ such that $\beta_{k+1}^{\#}$ is not $a_{n-2,n-1}$ (if any), the rotating normal form of $\beta_k$ contains an $\phi_n(\beta_{k+1}^{\#})$-barrier.*

## 3. Left reversing for dual braid monoid

Left reversing process was introduced by P. Dehornoy in [5]. It is a powerfull tool tfor the investigation of division properties in some monoids as stated by Proposition 3.6.

**Definition 3.1.** A monoid $M$ defined by a presentation $\langle S \,|\, R\rangle^+$ is *left complemented* if there exists a map $f : S \times S \to S^*$ satisfying

$$R = \left\{ f(x,y)x = f(y,x)y \,|\, (x,y) \in S^2 \right\}$$

and if $f(x,x) = \varepsilon$ holds for all $x \in S$.

As the relation $x = x$ is always true for $x \in S$ we say that $M$ is left complemented even if $x = x$ does not occur in $R$ for $x \in S$.

The monoid $B_3^{+*}$ with presentation of Proposition 1.1 is left complemented with respect to the map $f$ given by

$$f(a_{1,2}, a_{2,3}) = f(a_{1,2}, a_{1,3}) = a_{1,3}$$
$$f(a_{2,3}, a_{1,2}) = f(a_{2,3}, a_{1,3}) = a_{1,2}$$
$$f(a_{1,3}, a_{1,2}) = f(a_{1,3}, a_{2,3}) = a_{2,3}$$

However the monoid $B_4^{+*}$ with presentation of Proposition 1.1 is not left complemented. Indeed there is no relation of the form $... a_{1,3} = ... a_{2,4}$. Hence the words $f(a_{1,3}, a_{2,4})$ and $f(a_{2,4}, a_{1,3})$ are not well defined.

In general for $1 \leqslant p < r < q < s \leqslant n$, the word $f(a_{p,q}, a_{r,s})$ and $f(a_{r,s}, a_{p,q})$ are not defined for the presentation of $B_n^{+*}$ given in Proposition 1.1. In order to obtain a left complemented presentation of $B_n^{+*}$ we must exhibit some extra relations from these given in Proposition 1.1.

By example, the relation $a_{2,3}a_{1,4}\, a_{1,3} \equiv a_{3,4}a_{1,2}\, a_{2,4}$ holds and so we can consider $f(a_{1,3}, a_{2,4})$ to be $a_{2,3}a_{1,4}$. However the relation $a_{1,4}a_{2,3}\, a_{1,3} \equiv a_{3,4}a_{1,2}\, a_{2,4}$ is also satisfied and so $f(a_{1,3}, a_{2,4}) = a_{2,3}a_{1,4}$ is an other valid choice.

**Lemma 3.2.** *For $n \geqslant 2$, the map $f_n : A_n \times A_n \to A_n^*$ defined by*

$$f_n(a_{p,q}, a_{r,s}) = \begin{cases} \varepsilon & \text{for } a_{p,q} = a_{r,s}, \\ a_{p,s} & \text{for } q = r, \\ a_{s,q} & \text{for } p = r \text{ and } q > s, \\ a_{r,p} & \text{for } q = s \text{ and } p > r, \\ a_{r,q}a_{p,s} & \text{for } p < r < q < s, \\ a_{s,q}a_{r,p} & \text{for } r < p < s < q, \\ a_{r,s} & \text{otherwise.} \end{cases}$$

*provides a structure of left complemented monoid to* $B_n^{+*}$.

*Proof.* Direct computations using Proposition 1.1 establish $f_n(x,y)\cdot x \equiv f_n(y,x)\cdot y$ for all $(x,y)\in A_n^2$. □

Our choice for $f_n(a_{p,q},a_{r,s})$ with $p<r<q<s$ is well suited for the sequel and some proof would be invalid if we made an other one.

**Definition 3.3.** For $w$ and $w'$ two $A_n^{\pm}$-words, we say that $w$ *left reverses in one step* to $w'$, denoted $w \curvearrowright^1 w'$, if we can obtain $w'$ from $w$ substituting a factor $xy^{-1}$ (with $x,y\in A_n$) by $f_n(x,y)^{-1}f_n(y,x)$. We say that $w$ *left reverses* to $w'$, denoted by $w\curvearrowright w'$, if there exists a sequence $w=w_1,...,w'_\ell=w'$ of $A_n^{\pm}$-words such that $w_k\curvearrowright^1 w_{k+1}$ for $k\in[1,\ell-1]$.

**Example 3.4.** The word $u=a_{1,2}a_{2,3}a_{1,2}a_{1,3}^{-1}$ left reverses to $a_{2,3}a_{2,3}$ as the following left reversing sequence shows (left reversed factor are underlined)

$$a_{1,2}a_{2,3}\underline{a_{1,2}a_{1,3}^{-1}} \curvearrowright^1 a_{1,2}\underline{a_{2,3}a_{1,3}^{-1}}a_{2,3} \curvearrowright^1 \underline{a_{1,2}a_{1,2}^{-1}}a_{2,3}a_{2,3} \curvearrowright^1 a_{2,3}a_{2,3},$$

which is denoted by $a_{1,2}a_{2,3}a_{1,2}a_{1,3}^{-1}\curvearrowright a_{2,3}a_{1,2}$.

**Definition 3.5.** For $w$ an $A_n^{\pm}$-word, we denote by $D(w)$ and $N(w)$ the unique $A_n$-word, if there exist, such that $w\curvearrowright D(w)^{-1}N(w)$. The word $N(w)$ is the *left numerator* of $w$ while the word $D(w)$ is its *left denominator*.

Reconsidering Example 3.4, we obtain that the left denominator of $u$ is $D(u)=\varepsilon$ and that is left numerator its $N(u)=a_{2,3}a_{2,3}$.

A consequence of Example 8 and Proposition 3.5 of [6] based on [5] and [3] is that $N(w)$ and $D(w)$ exists for any $A_n^{\pm}$-word $w$. We obtain also the following result:

**Proposition 3.6.** *Let $w$ be an $A_n$-word and $a_{p,q}$ be in $A_n$. The braid $\overline{w}$ is right divisible by $a_{p,q}$ if and only if $D(w\cdot a_{p,q}^{-1})$ is empty.*

Since the denominator of $a_{1,2}a_{2,3}a_{1,2}a_{1,3}^{-1}$ is empty, the braid $a_{1,3}$ right divides the braid $a_{1,2}a_{2,3}a_{1,2}$.

## 4. Characterization of rotating normal words

The aim of this section is to give a syntactical characterization of $n$-rotating words among $A_n$-words.

**Definition 4.1.** We say that a braid $\beta$ in $B_n^{+*}$ contains an $a_{p,n}$-barrier if its rotating normal form does.

**Lemma 4.2.** *Assume that $n\geqslant 3$, $\beta$ belongs to $B_{n-1}^{+*}$ and that the $B_{n-1}^{+*}$-tail of $\phi_n(\beta)$ is trivial. Then every $A_{n-1}$-word representing $\beta$ ends with $\beta^{\#}$.*

*Proof.* Let $u$ be an $A_{n-1}$-word representing $\beta$. As the $B_{n-1}^{+*}$-tail of $\phi_n(\beta)$ is trivial, the last letter $u^{\#}$ of $u$ not belongs to $A_{n-2}$ and so $u^{\#}$ is $a_{p,n-1}$ for some integer $p<n-1$. Assume now $v$ is an other $A_{n-1}$-word representing $\beta$. For the same reason as $u$, we have $v^{\#}=a_{q,n-1}$ for some $q<n-1$. Since the two

braids $a_{p,n-1}$ and $a_{q,n-1}$ are right divisors of $\beta$, their left lcm is also a right divisor of $\beta$. Assume for a contradiction that $p$ and $q$ are different. The braid $\beta$ is then right divisible by $a_{p,q}a_{q,n-1}$, which is the left lcm of $a_{p,n-1}$ and $a_{q,n-1}$. Since $a_{p,q}a_{q,n-1}$ is equivalent to $a_{p,n-1}a_{p,q}$, the braid $a_{p,q}$ is also a right divisor of $\beta$. In particular $a_{p+1,q+1}$, with $q+1<n$, is a right divisor of $\phi_n(\beta)$, which is impossible since the $B^{+*}_{n-1}$-tail of $\phi_n(\beta)$ is supposed to be trivial. Therefore, every $A_{n-1}$-word representing $\beta$ ends with the same letter, namely $\beta^{\#}$. □

We conclude that, under some hypotheses, the last letter of a word is a braid invariant.

**Definition 4.3.** For $n \geqslant 3$ and $2 \leqslant p \leqslant n-1$, we say that an $n$-rotating word $w$ is an $a_{p,n}$-*ladder* is there exist a decomposition

$$w = v_0\, x_1\, v_1\, \ldots\, v_{h-1}\, x_h\, v_h,$$

a sequence $p = j(0) < j(1) < ... < j(h) = n-1$ and a sequence $i$ such that
($i$) for each $k \leqslant h$, the letter $x_k$ is $a_{i(k),j(k)}$ with $i(k) < j(k-1) < j(k)$,
($ii$) for each $k < h$, the word $v_k$ contains no $a_{j(k),n}$-barrier,

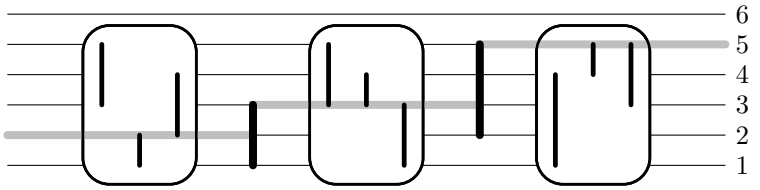



FIGURE 5. An $a_{2,6}$-ladder. The gray line starts at position 1 and goes up to position 5 using the bar of the ladder. The empty spaces between bars in the ladder are represented by a framed box. In such boxes the vertical line representing the letter $a_{i,j}$ does not cross the gray line. The bar of the ladder are represented by black thick vertical lines.

Condition ($ii$) is equivalent to: for each $k \leqslant h$, the letter $x_k$ is an $a_{j(k-1),n}$-barrier of type $a_{..,j(k)}$.

An immediate adaptation of Proposition 3.9 of [9] is :

**Lemma 4.4.** *Assume that $n \geqslant 3$, $\beta$ belongs to $B^{+*}_{n-1}$, the $B^{+*}_{n-1}$-tail of $\phi_n(\beta)$ is trivial and $\beta$ contains an $a_{p,n}$-barrier for some $2 \leqslant p \leqslant n-2$. Then the normal form of $\beta$ is an $a_{p,n}$-ladder.*

In order to obtain a syntactical characterization of $n$-rotating words we want a local version of condition (6) characterizing a $\phi_n$-splitting. The following result is the first one in this way.

**Proposition 4.5.** *For $\beta \in B^{+*}_{n-1}$ and $p$ an integer satisfying $2 \leqslant p \leqslant n-2$ there is equivalence between*

(*i*) *the* $B^{+*}_{n-1}$*-tail of* $\phi_n(a_{p,n}\beta)$ *is trivial,*
(*ii*) *the* $B^{+*}_{n-1}$*-tail of* $\phi_n(\beta)$ *is trivial and* $\beta$ *contains an* $a_{p,n}$*-barrier,*
(*iii*) *the only* $A_n$*-letter that right divides* $a_{p,n}\beta$ *is* $\beta^{\#}$*, which is of type* $a_{..,n-1}$.

Our proof of Proposition 4.5 rests on the following Lemma.

**Lemma 4.6.** *For* $n \geqslant 3$*,* $u$ *an* $A_{n-1}$*-word and* $p \in [1, n-1]$*, the left denominator* $D(ua_{p,n}^{-1})$ *is not empty. More precisely,* $D(ua_{p,n}^{-1})^{-1}$ *begins with* $a_{q,n}^{-1}$ *satisfying* $q \leqslant p$*.*

*Proof.* Assume that $w_1, ..., w_\ell$ is a reversing sequence from the word $w_1 = ua_{p,n}^{-1}$ to the word $D(w_1)^{-1}N(w_1)$. For $k \in [1, \ell]$ we denote by $y_k$ the leftmost negative letter in $w_k$. Each reversing step consists in replacing a factor $xy^{-1}$ of $w_k$ by $f_n(x, y)^{-1}f_n(y, x)$. If for $k \in [1, \ell]$ the reversed factor of $w_k$ does not contains $y_k^{-1}$ then $y_{k+1}$ equals $y_k$. Assume now that the reversed factor is $xy_k^{-1}$ with $y_k = a_{r,n}$. Lemma 3.2 implies

$$f_n(x, y_k) = f_n(a_{i,j}, a_{r,n}) = \begin{cases} a_{i,n} & \text{for } j = r, \\ a_{r,j}a_{i,n} & \text{for } i < r < j, \\ a_{r,n} & \text{otherwise,} \end{cases}$$

which gives in particular

$$xy_k^{-1} = a_{i,j}a_{r,n}^{-1} \curvearrowright \begin{cases} a_{i,n}^{-1}... & \text{for } i < r \leqslant j, \\ a_{r,n}^{-1}... & \text{otherwise.} \end{cases} \tag{8}$$

It follows that $y_{k+1}$ is equal to $a_{s,n}$ for some $s \leqslant r$. Eventually we obtain that $ua_{p,n}^{-1}$ left reverses to $a_{q,n}^{-1}...$ with the relation $q \leqslant p$ and so the desired property on $D(ua_{p,n})$ holds. □

*Proof of Proposition 4.5.* Assume (*i*). As the the $B^{+*}_{n-1}$-tail of $\phi_n(\beta)$ is also a right divisor of $\phi_n(a_{p,n}\,\beta)$ the first statement of (*ii*) holds. The second statement is Lemma 2.10. Let us prove that (*iii*) implies (*i*). By hypothesis the last letter of $\beta$ is $a_{q-1,n-1}$ for some $q$. As the only $A_n$-letter that right divides $\phi_n(a_{p,n}\beta)$ is $\phi_n(a_{q-1,n-1}) = a_{q,n}$, the $B^{+*}_{n-1}$-tail of $\phi_n(a_{p,n}\,\beta)$ must be trivial.

We now prove (*ii*) ⇒ (*iii*). Since the $B^{+*}_{n-1}$-tail of $\phi_n(\beta)$ is trivial, the letter $\beta^{\#}$ must be of type $a_{..,n-1}$. We denote by $w$ the rotating normal from of $\beta$. Let $a_{r,s}$ be an $A_n$-letter different from $\beta^{\#}$. We will show that $a_{r,s}$ cannot be a right divisor of $a_{p,n}\,\beta$. Assume first $s \leqslant n-1$. By Lemma 4.2, $a_{r,s}$ is not a right divisor of $\beta$. Proposition 3.6 implies that the word $D(w\,a_{r,s}^{-1})$ must be non empty. As the reversing of an $A^{\pm}_{n-1}$-word is also an $A^{\pm}_{n-1}$-word, there exists a letter $a_{t,t'}$ with $t' < n$ such that

$$a_{p,n}\,w\,a_{r,s}^{-1} \curvearrowright a_{p,n}\,a_{t,t'}^{-1}...,$$

holds. Clearly, the braid $a_{t,t'}$ is not a right divisor of $a_{p,n}$ (since we have $t' < n$). Therefore, by Proposition 3.6, the left denominator of $a_{p,n}\,w\,a_{r,s}^{-1}$ is not empty, and we conclude that $a_{r,s}$ is not a right divisor of $a_{p,n}\beta$.

Assume now $s = n$. Hypotheses on $\beta$ plus Lemma 4.4 imply that $w$ is an $a_{p,n}$-ladder. Following Definition 4.3, we write

$$w = v_0\, x_1\, v_1 \,...\, v_{h-1}\, x_h\, v_h.$$

By Lemma 4.6, there exist two maps $\eta$ and $\mu$ from $\mathbb{N}$ to itself such that

$$wa_{r,n}^{-1} = w_h a_{\eta(h),n}^{-1} \curvearrowright w'_h a_{\mu(h),n}^{-1} \cdots \curvearrowright \,...\, \curvearrowright w_0 a_{\eta(0),n}^{-1} \cdots \curvearrowright w'_0 a_{\mu(0),n}^{-1},$$

where for all $k \in [0, h]$,

$$w_k = v_0\, x_1\, v_1 \,...\, v_{k-1}\, x_k\, v_k,$$
$$w'_k = v_0\, x_1\, v_1 \,...\, v_{k-1}\, x_k.$$

By construction $w_0$ is $v_0$ while $w'_0$ is the empty word. Lemma 4.6 implies

$$\mu(0) \leqslant \eta(0) \leqslant \mu(1) \leqslant \,...\, \leqslant \mu(h) \leqslant \eta(h) = r. \tag{9}$$

Following Definition 4.3 we write $x_k = a_{i(k),j(k)}$. We will now prove by induction

$$\text{for all } k \in [0, h-1],\ \mu(k+1) \leqslant j(k+1) \Rightarrow \eta(k) < j(k) \tag{10}$$

Let $k \in [0, h-1]$ and assume $\mu(k+1) \leqslant j(k+1)$. Definition 4.3 $(i)$ guarantees the relation $i(k+1) < j(k) < j(k+1)$. For $\mu(k+1) \leqslant i(k+1)$ we have

$$\eta(k) \leqslant \mu(k+1) \leqslant i(k+1) < j(k),$$

and we are done in this case. The remaining case is $\mu(k+1) > i(k+1)$. By relation (8), with $i = i(k+1)$, $j = j(k+1)$ and $r = \eta(k+1)$ we obtain

$$x_{k+1}\, a_{\mu(k+1),n}^{-1} = a_{i(k+1),j(k+1)}\, a_{\mu(k+1),n}^{-1} \curvearrowright a_{i(k+1),n}^{-1} v$$

with some $A_n^{\pm}$-word $v$. In particular, we have $\eta(k) = i(k+1) < j(k)$ and (10) is established. For $k = h-1$ the left hand member of (10) is satisfied since $j(h)$ is equal to $n-1$ and $r \leqslant n-1$ holds by definition of $r$. Properties (9) and (10) imply $\mu(k) < j(k)$ for all $k \in [0, h-2]$. In particular we have $\mu(0) < j(0) = p$ together with $wa_{r,n}^{-1} \curvearrowright a_{\mu(0),n}^{-1} \cdots$. As $a_{\mu(0),n}$ can not be a right divisor of $a_{p,n}$ it follows that the left denominator of $a_{p,n}\, w\, a_{r,n}^{-1}$ is also non empty and so that $a_{r,n}$ is not a right divisor of $a_{p,n}\beta$. □

As the reader can see, the case $p = n-1$ is excluded from Proposition 4.5. It is the aim of the following result.

**Proposition 4.7.** *For $\beta$ a non-trivial braid of $B_{n-1}^{+*}$ there is equivalence between*

*$(i)$ the $B_{n-1}^{+*}$-tail of $\phi_n(a_{n-1,n}\beta)$ is trivial,*

*$(ii)$ the only $A_n$-letter right divising $a_{n-1,n}\beta$ is $\beta^{\#}$ which is of type $a_{..,n-1}$.*

*Proof.* $(ii) \Rightarrow (i)$ is similar as $(iii) \Rightarrow (i)$ of Proposition 4.7. We now show that $(i)$ implies $(ii)$. Condition $(i)$ implies in particular that the $B_{n-1}^{+*}$-tail of $\phi_n(\beta)$ is trivial. It follows that the last letter of $\beta$ is of type $a_{..,n-1}$. Let $w$ be the rotating normal form of $\beta$ and $a_{r,s}$ be an $A_n$-letter different from $\beta^{\#}$. For $s \leqslant n-1$ we follow proof of Proposition 4.7 to obtain that

$a_{r,s}$ is not a right divisor or the braid $a_{n-1,n}$. Assume now $s = n$. By Lemma 4.6 there exists $q \leqslant r$ such that $wa_{r,n}^{-1} \curvearrowright a_{q,n}^{-1} \cdots$ holds and so we obtain $a_{n-1,n}wa_{r,n}^{-1} \curvearrowright a_{n-1,n}a_{q,n}^{-1} \cdots$. As, for $q \neq n-1$ the braid $a_{q,n-1}$ is not a right divisor of $a_{n-1,n}$ it is sufficient to show $q \neq n-1$ for concluding that $a_{r,n}$ not right divides $a_{n-1,n}\beta$. For $r \leqslant n-2$ it is obvious since $q \leqslant r$ holds. Assume finally $r = n-1$. We denote by $a_{p,n-1}$ the last letter of $\beta$. By (8) we have $a_{p,n-1}a_{n-1,n}^{-1} \curvearrowright a_{p,n}^{-1} \cdots$ and then Lemma 4.6 implies $q \leqslant p < n-1$, as expected. □

**Theorem 4.8.** *A finite sequence $(\beta_b, ..., \beta_1)$ of braids in $B_{n-1}^{+*}$ is the $\phi_n$-splitting of a braid of $B_n^{+*}$ if and only if*

*(i) for $k \geqslant 3$ and $k = b$, the braid $\beta_k$ is not trivial,*

*(ii) for $k \geqslant 2$, the $B_{n-1}^{+*}$-tail of $\phi_n(\beta_k)$ is trivial,*

*(iii) if, for $k \geqslant 3$, we have $\beta_k^{\#} \neq a_{n-2,n-1}$ then $\beta_{k-1}$ contains an $\phi_n(\beta_k^{\#})$-barrier.*

*Proof.* Let $(\beta_b, ..., \beta_1)$ be the $\phi_n$-splitting of some braid of $B_{n-1}^{+*}$. Condition $(i)$ is a consequence of Lemma 2.8.$(ii)$. Condition (6) implies that the $B_{n-1}^{+*}$-tail of

$$\phi_n^{b-k}(\beta_b) \cdot ... \cdot \phi_n(\beta_{k+1})$$

is trivial for $k \geqslant 1$. In particular the $B_{n-1}^{+*}$-tail of $\phi_n(\beta_{k+1})$ must be trivial for $k \geqslant 1$, which implies $(ii)$. Condition $(iii)$ is Lemma 2.11.

Conversely, let us prove that a sequence $(\beta_b, ..., \beta_1)$ of braids of $B_{n-1}^{+*}$ satisfying $(i), (ii)$ and $(iii)$ is the $\phi_n$-splitting of some braid of $B_n^{+*}$. Condition $(i)$ implies that $\beta_b$ is not trivial. For $k \geqslant 2$ we denote by $\gamma_k$ the braid $\phi_n^{b-k}(\beta_b) \cdot ... \cdot \phi_n(\beta_{k+1}) \cdot \beta_k$. For $k \geqslant 3$ and $k \geqslant 2$ whenever $\beta_2 \neq 1$, we first prove

$$\beta_k^{\#} \text{ is the only } A_n\text{-letter that right divides } \gamma_k. \tag{11}$$

We note that Condition $(i)$ guarantees the existence of $\beta_k^{\#}$ for $k \geqslant 3$. For $k = b$, Condition $(ii)$ implies that the $B_{n-1}^{+*}$-tail of $\phi_n(\beta_b)$ is trivial. Hence, by Lemma 4.2 the only $A_{n-1}$-letter that right divides $\beta_b$ is $\beta_b^{\#}$. Since any right divisors of a braid of $B_{n-1}^{+*}$ lie in $B_{n-1}^{+*}$, we have established (11) for $k = b$. Assume (11) holds for $k \geqslant 4$ or $k \geqslant 3$ whenever $\beta_2 \neq 1$ and let us prove it for $k-1$. By Condition $(ii)$ there exists $p$ such that $\beta_k^{\#}$ is $a_{p-1,n-1}$. We denote by $ua_{p-1,n-1}$ and $v$ two $A_n$-words representing $\gamma_k$ and $\beta_{k-1}$ respectively. The braid $\gamma_{k-1}$ is then represented by $\phi_n(u)a_{p,n}v$. Let $y$ be an $A_n$-letter different from $\beta_{k-1}^{\#}$. Proposition 4.5 with Condition $(iii)$ and Proposition 4.7 imply that $y$ is not a right divisor of $a_{p,n}\,\beta_{k-1}$. Therefore, by Proposition 3.6 there exists an $A_n$-letter $x$ different from $a_{p,n}$ such that $\phi_n(u)a_{p,n}vy^{-1} \curvearrowright \phi_n(u)a_{p,n}x^{-1} \cdots$. The word $\phi_n(u)a_{p,n}$ represents $\phi_n(\gamma_k)$. By induction hypothesis $x$ is not a right divisor of $\phi_n(\gamma_k)$. Then Proposition 3.6 implies that $D(\phi_n(u)a_{p,n}x^{-1})$ is not empty. It follows $D(\phi_n(u)a_{p,n}vy^{-1}) \neq \varepsilon$ and so always by Proposition 3.6, the letter $y$ is not a right divisor of $\gamma_{k-1}$. Eventually we have established (11) for $k \geqslant 3$.

A direct consequence of (11) and Condition $(ii)$ is that the only $A_n$-letter right divising $\phi_n(\gamma_k)$ is of type $a_{..,n}$ and so the $B^{+*}_{n-1}$-tail of he braid $\gamma_k$ is trivial for $k \geqslant 3$ and for $k = 2$ whenever $\beta_k \neq 1$. It remains to establish that the $B^{+*}_{n-1}$ tail of $\phi_n(\gamma_2)$ is also trivial whenever $\beta_2$ is trivial. Assume $\beta_2 = 1$. Condition $(iii)$ implies $\beta_3^{\#} = a_{n-2,n-1}$. By (11), $a_{n-2,n-1}$ is the only $A_n$-letter that right divides the braid $\gamma_3$. Since $\gamma_2 = \phi_n(\gamma_3)$, the letter $\phi_n^2(a_{n-2,n-1}) = a_{1,n}$ is the only letter right divising $\phi_n(\gamma_2)$. In particular the $B^{+*}_{n-1}$-tail of $\phi_n(\gamma_2)$ is trivial. □

Conditions $(i)$, $(ii)$ and $(iii)$ are easy to check if the braids $\beta_1, ..., \beta_b$ are given by their rotating normal forms.

**Corollary 4.9.** *Let $(w_b, ..., w_1)$ be a finite sequence of $A_{n-1}$-words, then the word*

$$\phi_n^{b-1}(w_b) \cdot ... \cdot \phi_n(w_2) \cdot w_1, \tag{12}$$

*is $n$-rotating if the following conditions are satisfied*

*$(i)$ for $k \geqslant 1$, the word $w_k$ is $(n-1)$-rotating,*

*$(ii)$ for $k \geqslant 3$, the word $w_k$ ends by $a_{p-1,n-1}$ for some $p$,*

*$(iii)$ the word $w_2$ is either empty (except for $b = 2$) or ends by $a_{p-1,n-1}$ for some $p$,*

*$(iv)$ if, for $k \geqslant 3$, the word $w_k$ ends by $a_{p-1,n-1}$ with $p \neq n-1$ then the word $w_{k-1}$ contains an $a_{p,n}$-barrier.*

*Proof.* Assume that $(w_b, ..., w_1)$ satisfies Conditions $(i)$-$(iv)$ and let us prove that the word $w$ defined at (12) is rotating.

We denote by $\beta_i$ (resp. $\beta$) the braid represented by $w_i$ (resp. $w$). By Condition $(i)$ and Definition 2.5, the word $w$ is rotating if and only if $(\beta_b, ..., \beta_1)$ is a $\phi_n$-splitting. Conditions $(ii)$ and $(iii)$ imply Condition $(i)$ of Theorem 4.8. Theorem 4.8.$(iii)$ is a consequence of $(ii)$ and $(iv)$. We remark that the $B^{+*}_{n-1}$-tail of a braid $\gamma$ is represented by a suffix of the rotating word of $\gamma$. If the $B^{+*}_{n-1}$-tail of $\phi_n(\beta_k)$ is not trivial, then there exists $a_{p,q}$ with $1 \leqslant p < q < n$ that right divides $\phi_n(\beta_k)$. As $\beta_k$ lies in $B^{+*}_{n-1}$, we have $p \neq 1$ and therefore $\beta_k$ is right divisible by $a_{p-1,q-1}$ with $q - 1 \leqslant n - 2$. Assume the $B^{+*}_{n-1}$-tail of $w_k$ is not trivial for $k \geqslant 2$. The previous remark implies that $w_k$ must end with a letter $a_{i,j}$ satisfying $j \leqslant n-2$, which is in contradiction with Conditions $(ii)$ and $(iii)$. □

It is not true that any decomposition of an $n$-rotating word as in (12) satisfies Conditions $(i) - (iv)$ of Corollary 12. However we have the following result.

**Proposition 4.10.** *For every $n$-rotating word $w$ with $n \geqslant 3$ there exists a unique sequence $(w_b, ..., w_1)$ of $(n-1)$-rotating words such that $w$ decompose as in (12) and Conditions $(ii) - (iv)$ of 4.9 hold.*

*Proof.* By definition of a rotating normal word and by Lemma 2.8 such a sequence exists. Let us prove now the unicity. Assume $w$ is a $n$-rotating normal word and that $(w_b, ..., w_1)$ and $(w'_c, ..., w'_1)$ are two different sequences of

$(n-1)$-rotating normal words satisfying Conditions $(ii)$ and $(iii)$ of Corollary 4.9. Let $k$ be the minimal integer satisfying $w_k \neq w'_k$. Since the sum of the word lengths of the two sequences are the same, we have $k \leqslant \min\{b, c\}$. Without lost of generality, we may assume that $w'_k$ is a proper suffix of $w_k$, *i.e.*, $w_k = u \cdot w'_k$. By Conditions $(ii)$ and $(iii)$ of Corollary 4.9, the last letter $x$ of $u$ comes from the last letter of $w'_{k+1}$ or $w'_{k+2}$. Hence the letter $x$ is equal to $a_{p-1,n-1}$ for some $p$ and $w_k$ admits either $\phi_n(a_{p-1,n-1})w'_k = a_{p,n}w'_k$ or $\phi_n^2(a_{p-1,n-1})w'_k = a_{1,p+1}w'_k$ as suffix. The first case is impossible since $w_k$ is an $A_{n-1}$-word. The second case may occur only for $k = 1$ and $w'_2 = \varepsilon$. As $w'_2$ is empty, the last letter of $w'_3$, which is $x$, is equal to $a_{n-2,n-1}$. This implies that $w_k$ admits $a_{1,n}u$ as suffix which is also impossible since it is an $A_{n-1}$-word. □

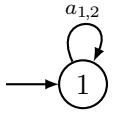
A direct consequence of Corollary 4.9 and Proposition 4.10 is

**Theorem 4.11.** *An $A_n$-word $w$ is rotating if and only if it can be expressed as in* (12) *subject to Conditions $(i) - (iv)$ of Corollary 4.9.*

## 5. Regularity

In this section we will show that the language of $n$-rotating words, denoted by $R_n$ is regular, *i.e.*, there exists a finite state automaton recognizing the $n$-rotating words. As the rotating normal form is defined using right division it is more natural for an automaton to read word from the right. For $w = x_0 \cdot \ldots \cdot x_k$ an $A_n$-word we will denote by $\Pi(w)$ the word $x_k \cdot \ldots \cdot x_0$. By Theorem 1.2.8 of [7] the language $R_n$ is regular if and only if the language $\Pi(R_n)$ is. In this section we will construct an automaton recognizing $\Pi(R_n)$.

For us a *finite state automaton* is a quintuplet $(S \cup \{\otimes\}, A, \mu, Y, i)$ where $S$ is the finite set of *states*, $A$ is a finite *alphabet*, $\mu : S \times A \to S$ is the *transition function*, $Y \subseteq S$ is *acceptating states* and $i$ is the *initial state*. In this paper each automaton is equipped with an undraw dead state $\otimes$ and all states except the dead one is accepting, *i.e.*, $Y = S$ always holds. Therefore an automaton will be briefly denoted by $\mathcal{A} = (S, A, \mu, i)$. To describe $\mathcal{A}$ it is enough to describe $\mu$ on $(s, x) \in S \times A$ where $\mu(s, x) \neq \otimes$ and $s \neq \otimes$. By example an automaton recognizing the language $R_2$ is $\mathcal{A}_2 = (\{1\}, \{a_{1,2}\}, \mu_2, 1)$ with $\mu_2(1, a_{1,2}) = 1$. The corresponding automaton diagram is :




The horizontal arrow points to the initial state.

**Proposition 5.1.** *An $A_3$-word $x_b^{e_b} \cdot \ldots \cdot a_{1,3}^{e_3} a_{2,3}^{e_2} a_{1,2}^{e_1}$ where*

$$x_b = \begin{cases} a_{1,2} & \text{if } b \equiv 1 \bmod 3, \\ a_{2,3} & \text{if } b \equiv 2 \bmod 3, \\ a_{1,3} & \text{if } b \equiv 3 \bmod 3. \end{cases}$$

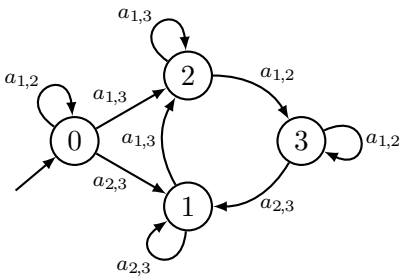
*is rotating if and only if $e_k \neq 0$ for all $k \geqslant 3$.*

*Proof.* The 2-rotating words are powers of $a_{1,2}$. Let $w$ be the word of the statement. Defining $w_k$ to be $a_{1,2}^{e_k}$, we obtain

$$w = \phi_n^{b-1}(w_b) \cdot \ldots \cdot \phi_n(w_2) \cdot w_1.$$

As there is no barrier in $B_3^{+*}$, the word $w$ is rotating if and only if it satisfies Conditions $(ii)$ and $(iii)$ of Corollary 4.9, *i.e.*, the exponent $e_k$ is not 0 for $k \geqslant 3$. □

As a consequence the following automaton recognizes the language $\Pi(R_3)$:




Unfortunately, for $n \geqslant 4$ there is no so simple characterization of $n$-rotating words. We will describe an inductive construction for an automaton recognizing language $\Pi(R_n)$. The process will be illustrated on $n = 4$. The first step is to focus on $n$-rotating words ending with a letter of type $a_{..,n}$.

**Definition 5.2.** We denote by $R_n^*$ the language of $n$-rotating words which are empty or ends with a letter of type $a_{p,n}$ for some $p$.

Before constructing an automaton $\mathcal{A}_n$ recognizing the language $\Pi(R_n)$, we construct by induction on $n \geqslant 3$ an automaton $\mathcal{A}_n^*$ for the language $\Pi(R_n^*)$.

**Definition 5.3.** A *partial automaton* is a quadruplet $P = (S, A, \mu, I)$ where $S$, $A$ and $\mu$ are defined as for an automaton and $I : A \to S$ is a map. The closure of a partial automaton $P$ is the automaton $\mathcal{A}(P) = (S \cup \{\circ\}, A, \mu^c, \circ)$ given by

$$\mu^c(s, x) = \begin{cases} I(x) & \text{if } s = \circ, \\ \mu(s, x) & \text{otherwise.} \end{cases}$$

A partial automaton is represented as an automaton excepted for the function $I$. For each $x \in A$ we draw an arrow attached to state $I(x)$ and

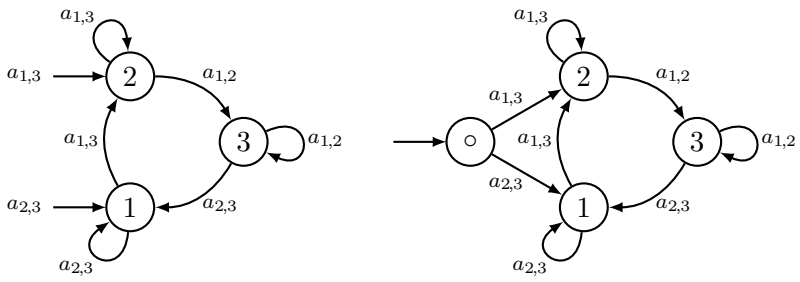



FIGURE 6. The partial automaton $P_3$ and the corresponding closure which recognizes the language $\Pi(R_3^*)$.

labelled $x$. We say that a partial automaton recognizes a given language if its closure does.

We will now show how to construct by induction a partial automaton $P_n$ recognizing $\Pi(R_n^*)$ for $n \geqslant 3$. For $n = 3$ this is already done by Figure 6. For the sequel we assume $n \geqslant 4$ and that $P_{n-1} = (S_{n-1}, A_{n-1}, \mu_{n-1}, I_{n-1})$ is a given partial automaton which recognizes the language $\Pi(R_{n-1})$.

We define $S_n^0$ to be the set

$$S_n^0 = \{0\} \times (S_{n-1} \setminus \{\otimes\}) \times \mathcal{P}(\{a_{2,n}, ..., a_{n-2,n}\}).$$

A state in $S_n^0$ is then written $(0, s, m)$. For $x = a_{i,j} \in A_{n-1}$ we denote by $\mathrm{bar}(x)$ the set $\{a_{p,n} \,|\, i < p < j\}$.

**Definition 5.4.** We define $P_n^0 = (S_n^0 \cup \{\otimes\}, A_{n-1}, \mu_n^0, I_n^0)$ to be the partial automaton where for all $x \in A_{n-1}$,

$$I_n^0(x) = \begin{cases} (0, I_{n-1}(x), \mathrm{bar}(x)) & \text{if } I_{n-1}(x) \neq \otimes, \\ \otimes & \text{if } I_{n-1}(x) = \otimes. \end{cases}$$

and for all $(0, s, m) \in S_n^0$ and for all $x \in A_{n-1}$,

$$\mu_n^0((0, s, m), x) = \begin{cases} (0, \mu_{n-1}(s, x), m \cup \mathrm{bar}(x)) & \text{if } \mu_{n-1}(s, x) \neq \otimes, \\ \otimes & \text{if } \mu_{n-1}(s, x) = \otimes. \end{cases}$$

**Proposition 5.5.** *The partial automaton $P_n^0$ recognizes the language $\Pi(R_{n-1}^*)$. Moreover an accepted $A_n$-word $\Pi(w)$ contains an $a_{p,n}$-barrier if and only if $P_{n,0}$ has state $(s, m)$ with $a_{p,n} \in m$ after reading $\Pi(w)$.*

*Proof.* Let $w$ be an $A_n$-word of length $\ell$, $\mathcal{A}$ and $\mathcal{A}'$ be the closure of $P_{n-1}$ and $P_n^0$ respectively. We denote by $s_k$ (resp. $(s'_k, m_k)$) the state of automaton $\mathcal{A}$ (resp. $\mathcal{A}'$) after reading the $k$-th letter of $\Pi(w)$. If $w$ does not contains an $a_{p,n}$-barrier then $(s'_k, m_k)$ is equal to $(s_k, \varnothing)$ for all $k \in [1, \ell]$. Hence $\Pi(w)$ is accepted or not by the two automata and in particular $m_\ell$ is the empty set. Assume now $w$ contains an $a_{p,n}$-barrier. Let $\ell'$ be the first occurrence on such a barrier in $\Pi(w)$. By construction of $\mu_n$ we have $(s'_k, m_k)$ with $a_{p,n} \in m_k$ for $k \geqslant \ell'$ except if $s_k = \otimes$. As $\mathcal{A}$ (resp. $\mathcal{A}'$) recognizes the word

$\Pi(w)$ if and only if $s_\ell$ (resp. $s'_\ell$) is different from $\otimes$, the word $w$ is recognized or not by both automata. Moreover, in this case $m_\ell$ contains $a_{p,n}$. □

As the only $a_{p,4}$-barrier in $A_4$ is $a_{1,3}$, the partial automaton $P_4^0$ is obtained from $P_3$ by connecting edges labelled $a_{1,3}$ to a copy of $P_3$, as illustrated on figure 5

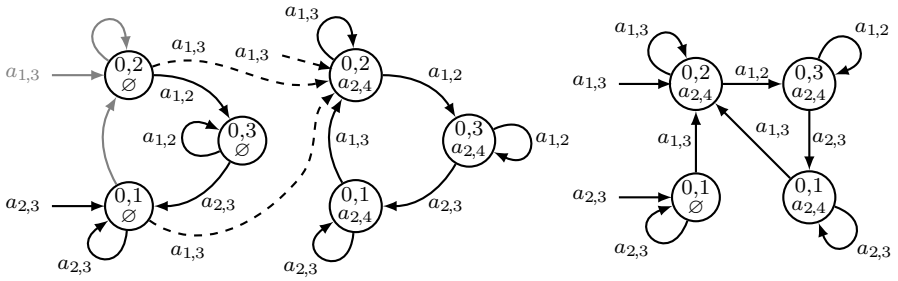



FIGURE 7. The partial automaton $P_4^0$. Obsolete transitions from $P_3$ are in gray. New added transitions are dashed. The right partial automaton is $P_4^0$ without inaccessible states.

For $t = (0, s, m) \in S_n^0$ we define $\phi_n^k(t)$ to be $(k, s, m)$. We also define $S_n^k$ to be $\phi_n^k\left(S_n^0\right)$ and

$$P_n^k = \left(S_n^k, \phi_n^k\left(A_{n-1}\right), \mu_n^k, I_n^k\right)$$

to be the partial automaton given by $I_n^k(\phi_n^k(x)) = \phi_n^k\left(I_n^0(x)\right)$ and

$$\mu_n^k((k, s, m), \phi_n^k(x)) = \phi_n^k\left(\mu_n^0((0, s, m), x)\right)$$

with the convention $\phi_n^k(\otimes) = \otimes$. In other words, $P_n^k$ is obtained from $P_n^0$ by replacing the letter $x$ by $\phi_n^k(x)$ and state $(0, s, m)$ by $(k, s, m)$. We obtain immediately that $P_n^k$ recognizes the word $\phi_n^k\left(\Pi(w)\right)$ if and only if $P_n^0$ recognizes $\Pi(w)$.

We can now construct the partial automaton $P_n$ by plugging together $n$ partial automaton $P_n^k$ for $k \in [0, n-1]$ together.

**Definition 5.6.** We define $P_n = (S_n^* \cup \{\otimes\}, A_n, \mu_n^*, I_n)$, with $S_n^* = S_n^0 \sqcup \ldots \sqcup S_n^k$ to be the partial automaton given by

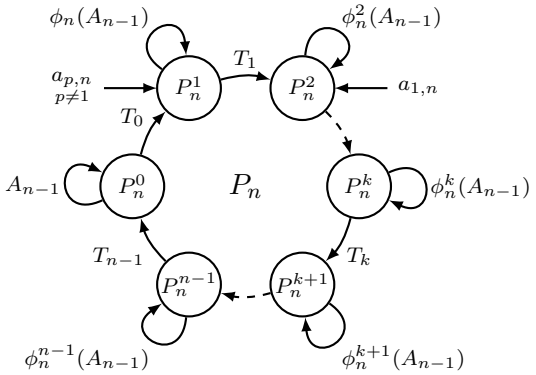
$$I_n(x) = \begin{cases} I_n^1(a_{p-1,n-1}) & \text{if } x = a_{p,n} \text{ with } p \neq 1, \\ I_n^2(a_{n-2,n-1}) & \text{if } x = a_{1,n}, \\ \otimes & \text{otherwise.} \end{cases}$$

and with transition function

$$\mu_n^*((k,s,m),\phi_n^k(x)) = \begin{cases} \mu_n^k((k,s,m),\phi_n^k(x)) & \text{if } x \in A_{n-1}, \\ I_n^{k+1}(\phi_n^k(x)) & \text{if } x = a_{n-1,n} \\ I_n^{k+1}(\phi_n^k(x)) & \text{if } x = a_{p,n} \text{ with } 2 \leqslant p \leqslant n-2 \\ & \text{and } a_{p,n} \in m, \\ \otimes & \text{otherwise} \end{cases}$$

with the convention $I_n^n = I_n^0$.

We summarize the construction of the partial automaton $P_n$ on the following diagram.




An arrow labelled $T_k$ represents the set of transitions $\mu_n^*((k,s,m,\phi_n^k(a_{p,n}))$.

**Lemma 5.7.** *The partial automaton $P_n$ recognizes the language $\Pi(R_n^*)$.*

*Proof.* Let $\mathcal{A}$ be the closure of $P_n$ and $w$ be a non empty $A_n$-word. There exists a unique sequence $(w_b, ..., w_1)$ of $A_{n-1}$-words such that $w_b \neq \varepsilon$, $w$ is equal to

$$\phi_n^{b-1}(w_k) \cdot ... \cdot \phi_n(w_2) \cdot w_1$$

and for all $i$, the word $\phi_n^i(w_i)$ is the maximal suffix of $\phi_n^{k-1}(w_k) \cdot ... \cdot \phi_n^i(w_i)$ belonging to $\phi_n^i(A_{n-1})$. By definition of $I_n$, the word $\Pi(w)$ is accepted by $P_n$ only if $w$ ends by a letter $a_{p,n}$ for some $p$. We assume now that $w$ is such a word. Thus the first integer $j$ such that $w_j$ is non empty is 2 or 3. More precisely, we have $j = 2$ if $p > 1$ and $j = 3$ if $p = 1$ holds. In both cases, the reading of $\Pi(w)$ starts by a state coming form $P_n^j$. The automaton reaches a state different from one of $P_n^j$ if it goes to the state $\otimes$ or if it reads a letter outside of $\phi_n^{j-1}(A_n)$, *i.e.*, a letter of $\phi_n^j(w_{j+1})$. This is a general principle : after reading a letter of $\phi_n^{i-1}(w_i)$ the automaton $\mathcal{A}$ is in state $(t,s,m)$ with $t = i \bmod n$. By construction of $P_n^t$, the word $\phi_n^{i-1}(w_i)$ provides an accepted state if and only if $w_i$ is a word of $\Pi(R_{n-1})$. At this point we have shown that $\Pi(w)$ is accepted by $\mathcal{A}$ only if $w$ is empty or if $w$ satisfies $w'^{\#} = a_{p,n}$ together with Conditions $(i)$, $(ii)$ and $(iii)$ of Corollary 4.9. Let $i$ be in $[j, k-1]$, and assume that $\mathcal{A}$ is in an acceptable state $(t,s,m)$ with $t = i \bmod n$ after

reading the word $\Pi(\phi_n^{i-1}(w_i)\cdot\ldots\cdot\phi_n(w_2)\cdot w_1)$. We denote by $x$ the letter $w_{i+1}^{\#}$. By construction of $w_{i+1}$ we have $x \notin \phi_n^{i-1}(A_{n-1})$ and so $x = \phi_n^i(a_{p,n})$ for some $p$. By definition of $\mu_n^*$ we have $\mu_n^*((t,s,m),\phi_n^i(a_{p,n})) \neq \otimes$ if and only if $p = n-1$ of $p \in [2, n-2]$ and $a_{p,n} \in m$. By construction of $P_n^t$, we have $a_{p,n} \in m$ if and only if $w_i$ contains an $a_{p,n}$, which corresponds to Condition $(iv)$ of Corollary 4.9. Eventually, by Corollary 4.9, the word $\Pi(w)$ is accepted by $\mathcal{A}$ if and only if $w \in R_n^*$. □

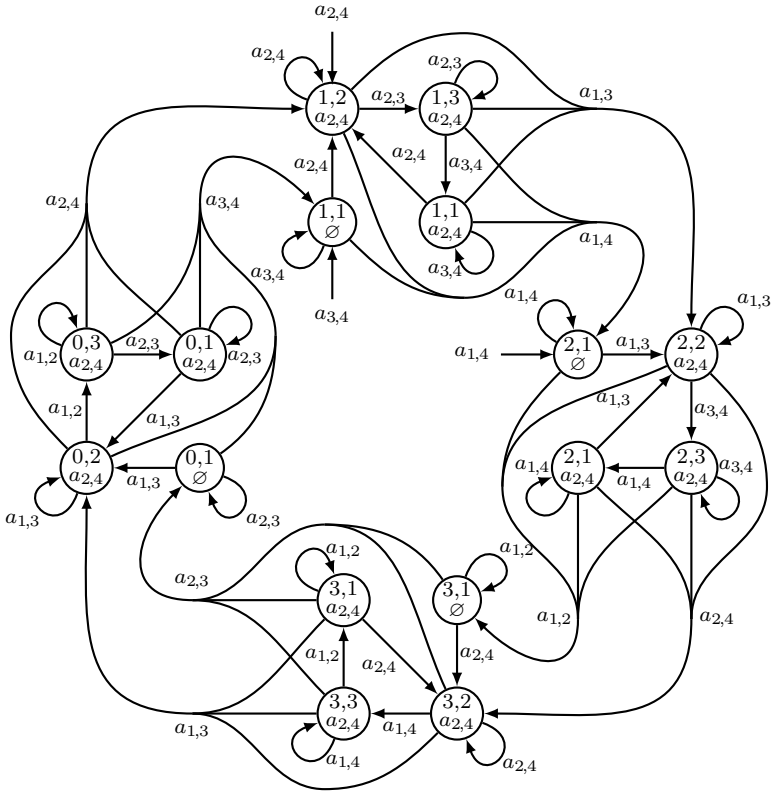



FIGURE 8. Partial automaton recognizing the language $\Pi(R_4^*)$.

Assume that an automaton $\mathcal{A}_{n-1} = (S_{n-1} \cup \{\otimes\}, A_{n-1}, \mu_{n-1}, i)$ recognizing the language $\Pi(R_{n-1})$ for $n \geqslant 4$ is given. Using the partial automaton $P_n = (S_n^* \cup \{\otimes\}, A_n, \mu_n^*, I_n)$ we construct the automaton $\mathcal{A}_n = (S_n \cup \{\otimes\}, A_n, \mu_n, i)$ defined by $S_n = S_{n-1} \sqcup S_n^*$ and

$$\mu_n(s,x) = \begin{cases} \mu_{n-1}(s,x) & \text{if } s \in S_{n-1} \text{ and } x \in A_{n-1}, \\ I_n(x) & \text{if } s \in S_{n-1} \text{ and } x \in A_n \setminus A_{n-1}, \\ \mu_n^*(s,x) & \text{if } s \in S_n^*. \end{cases}$$

**Proposition 5.8.** *If $\mathcal{A}_{n-1}$ recognizes $\Pi(R_{n-1})$, the automaton $\mathcal{A}_n$ recognizes the language $\Pi(R_n)$.*

*Proof.* Let $w$ be an $A_n$-word, $w_1$ be the maximal suffix of $w$ which is an $A_{n-1}$-word and $w'$ be the corresponding prefix. By Corollary 4.9, the word $w$ is rotating if and only if $w_1$ and $w'$ are. By construction of $\mathcal{A}_n$, the automaton is in acceptable state after reading $\Pi(w_1)$ if and only if $w_1$ is an $(n-1)$-rotating word. Hence $w$ is accepted only if $w_1$ is rotating. Assume that it is the case. By Lemma 5.7 the automaton $\mathcal{A}_n$ is always in an acceptable state after reading $\Pi(w')$ if and only if the word $w'$ is rotating. Eventually the word $\Pi(w)$ is accepted by $\mathcal{A}$ if and only if $w_1$ and $w'$ are both rotating, which is equivalent to $w$ is rotating. □

By Proposition 5.8, the language $\Pi(R_n)$ is regular and so we obtain:

**Theorem 5.9.** *The language of $n$-rotating words $R_n$ is regular.*

## Further work

Using syntactical characterization of rotating words we have proved that the language of $n$-rotating words is regular. For $W$ a finite state automaton, we denote by $L(W)$ the language recognized by $W$. Following [4] and [7] we have the following definition:

**Definition 5.10.** Let $M$ be a monoid. A *right automatic structure*, resp. *left automatic structure*, on $M$ consists of a set $A$ of generators of $M$, a finite state automaon $W$ over $A$, and finite state automata $M_x$ over $(A, A)$, for $x \in A \cup \{\varepsilon\}$, satisfying the following conditions:

$(i)$ the map $\pi : L(W) \to M$ is surjective.

$(ii)$ for $x \in A \cup \{\varepsilon\}$, we have $(u, v) \in L(M_x)$ if and only if $\overline{ux} = \overline{y}$, resp. $\overline{xu} = \overline{y}$, and both $u$ and $v$ are elements of $L(W)$.

Naturally we can ask if the rotating normal form provides an left or right automatic structure for the dual braid monoid $B_n^{+*}$. Such a result may needs to obtain some syntactical properties on the word $x\,w$ or $w\,x$ where $w$ is an $n$-rotating word and $x$ is an $A_n$-generator. At this time no result have been obtained in this direction.

## References


[1] E. Artin, *Theorie der Zöpfe*, Abh. Math. Sem. Univ. Hanburg **4** (1925), 47–72.

[2] D. Bessis, *The dual braid monoid*, Ann. Sci. École Norm. Sup. (4) **36** (2003), no. 5, 647–683.

[3] J. S. Birman, K. H. Ko, and S. J. Lee, *A new approach to the word and conjugacy problems in the braid groups*, Adv. Math. **139** (1998), no. 2, 322–353.

[4] C. M. Campbell, E. F. Robertson, N. Ruškuc, and R. M. Thomas, *Automatic semigroups*, Theoretical Computer Science **250** (2001), no. 1-2, 365–391.

[5] P. Dehornoy, *Groups with a complemented presentation*, J. Pure Appl. Algebra **116** (1997), 115–137, Special volume on the occasion of the 60th birthday of Professor Peter J. Freyd.

[6] P. Dehornoy and L. Paris, *Gaussian groups and Garside groups, two generalisations of Artin groups*, Proc. London Math. Soc. (3) **79** (1999), no. 3, 569–604.

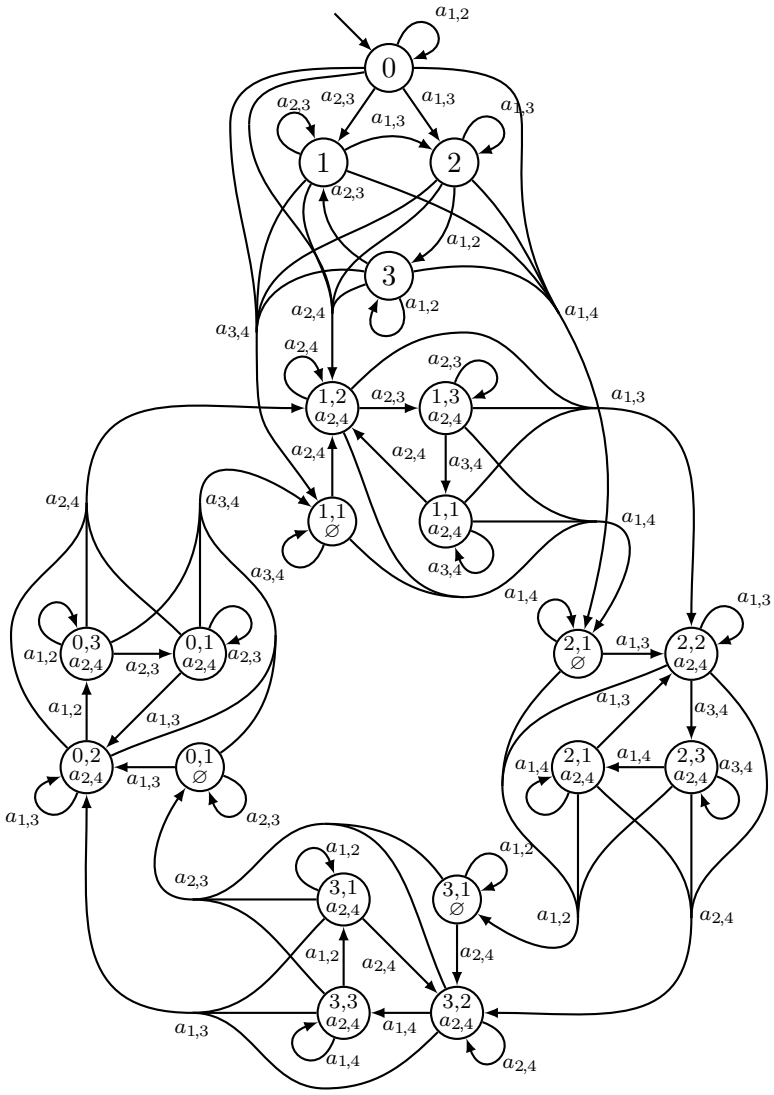



FIGURE 9. Automaton $\mathcal{A}_4$ for the language $\Pi(R_4)$.

[7] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, and W. P. Thurston, *Word processing in groups*, Jones and Bartlett Publishers, Boston, MA, 1992.

[8] J. Fromentin, *A well-ordering of dual braid monoids*, C. R. Math. Acad. Sci. Paris **346** (2008), 729–734.

[9] ———, *Every braid admits a short sigma-definite expression*, Journal of the European Mathematical Society (JEMS) **13** (2011), no. 6, 1591–1631.