THE ROTATING NORMAL FORM OF BRAIDS 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 rotating words on n strands, proving that the rotating normal form is regular. As a consequence we obtain the regularity of a σ-definite normal form defined on the whole braid group.

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]:

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

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 σ_i as a code for the geometric braid where only the ith and the $(i+1)$st strands cross, with the strand originally at position $(i+1)$ in front of the other.

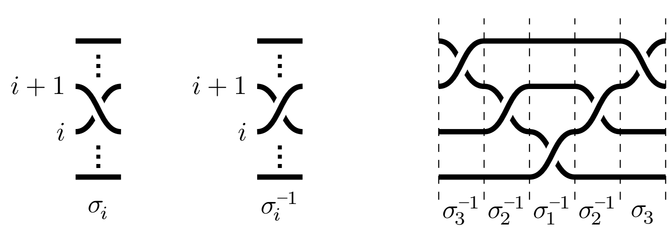


FIGURE 1. Interpretation of a word in the letters $\sigma_i^{\pm 1}$ as a geometric braid diagram.

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 $a_{i,j} = \sigma_i \cdots \sigma_{j-1}\ \sigma_j\ \sigma_{j-1}^{-1} \cdots \sigma_i^{-1}$. In geometrical terms, the braid $a_{i,j}$ corresponds to a crossing of the ith and jth strands, both passing behind the (possible) intermediate strands.

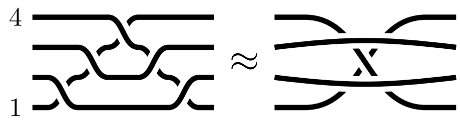


FIGURE 2. In the geometric braid $a_{1,4}$, the strands 1 and 4 cross under the strands 2 and 3.

Remark. In [3], the braid $a_{i,j}$ is defined to be $\sigma_{j-1} \cdots \sigma_{i+1}\,\sigma_i\,\sigma_{i+1}^{-1} \cdots \sigma_{j-1}^{-1}$, corresponding to a crossing of the ith and jth strands, both passing in **front** of the (possible) intermediate strands. The two definitions lead to isomorphic monoids. Our choice is this of [13] and has connections with Dehornoy's braid ordering: B_{n-1}^{+*} is an initial segment of B_n^{+*}.

By definition, σ_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^+.

For $n \geqslant 2$, we denote by A_n the set $\{a_{p,q} \,|\, 1 \leqslant p < q \leqslant n\}$. If p and q are two integers of $\mathbb{N}$ satisfying $p \leqslant q$, we denote by $[p, q]$ the interval $\{p, ..., q\}$ of $\mathbb{N}$. The interval $[p, q]$ is said to be *nested* in the interval $[r, s]$ if the relation $r < p < q < s$ holds. 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:*

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

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

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^{+*}, and was introduced in [12] and [13]. 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 β. It can be seen 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. We recall that the rotating normal form is a dual version of the alternating normal form introduced by P. Dehornoy in [8] and itself building on S. Burckel's normal form defined in [4]

The aim of this paper is to construct for all $n \geqslant 2$ an explicit finite-state automaton which recognizes the language R_n, implying that the language of n-rotating words is regular. Following [13] and [14] we can define, from the rotating normal form, a σ-definite normal form defined on the whole braid group. The corresponding language is then proven to be regular.

The paper is divided as follows. In section 2 we recall briefly the construction of the rotating normal form and its useful already known properties. In the 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 the fifth section we construct, for each $n \geqslant 2$, a finite-state automaton which recognizes the language R_n of n-rotating normal words. Section 5 is devoted to establish the regularity of the σ-definite normal form. In last section we prove that the rotating normal form is not right-automatic.

2. The rotating normal form

The main ingredient used to define the rotating normal form is the Garside automorphism ϕ_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 ϕ_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, ϕ_n should be viewed as a rotation, which makes sense provided braid diagrams are drawn on a cylinder rather than on a plane rectangle.

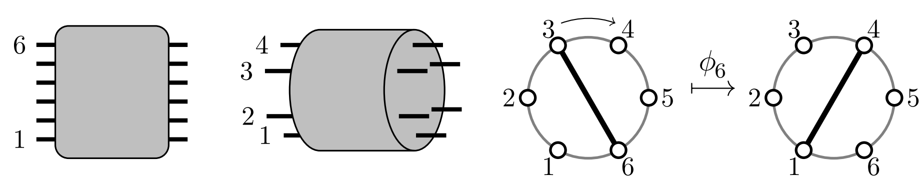


Figure 3. Rolling up the usual braid diagram helps us to visualize the symmetries of the braids $a_{p,q}$. On the resulting cylinder, $a_{p,q}$ naturally corresponds to the chord connecting vertices p and q. With this representation, ϕ_n acts as a clockwise rotation of the marked circles by $2\pi/n$.

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

Definition 2.1. For $n \geqslant 3$ and β a braid of B_n^{+*}, the maximal braid β_1 lying in B_{n-1}^{+*} that right-divides the braid β is called the B_{n-1}^{+*}-*tail* of β.

Using basic Garside properties of the monoid B_n^{+*} we obtain the following result (Proposition 2.5 of [13]) which allows 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 non-trivial braid β of B_n^{+*} there exists a unique sequence $(\beta_b, ..., \beta_1)$ of braids of B_{n-1}^{+*} satisfying $\beta_b \neq 1$ and*

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

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

Under the above hypotheses, the sequence $(\beta_b, ..., \beta_1)$ is called the ϕ_n-*splitting* of the braid β. It is shown in [13] that Condition (6) can be replaced by:

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

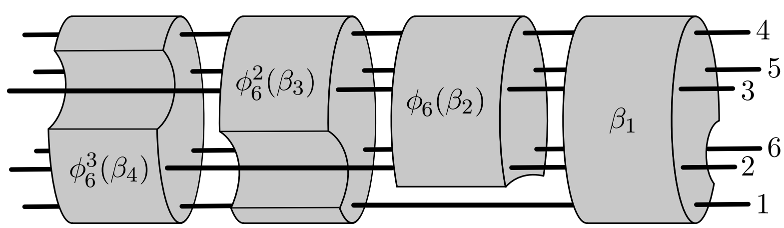


FIGURE 4. The ϕ_6-splitting of a braid of B_6^{+*}. Starting from the right, we extract the maximal right divisor that keeps the sixth strand unbraided, then extract the maximal right divisor that keeps the first strand unbraided, etc.

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 β 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 $\beta_1 = a_{1,2}a_{1,2}$. As the word $a_{1,2}a_{1,3}$ is alone in its equivalence class, the braid $\phi_3(\gamma_1) = a_{1,2}a_{1,3}$ is not right-divisible by $a_{1,2}$ and so its B_2^{+*}-tail is trivial. The braid $\phi_3(\gamma_1)$ is exactly the one of (6) for $n = 3$ and $k = 1$. Considering γ_1 instead of β 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 $\beta_2 = 1$. As the word $a_{1,3}a_{2,3}$ is also alone in its equivalence class, the braid $\phi_3(\gamma_2) = a_{1,3}a_{2,3}$ is not right-divisible by $a_{1,2}$ and so its B_2^{+*}-tail is trivial. The braid $\phi_3(\gamma_2)$ is the one of (6) for $n = 3$ and $k = 2$.

We decompose the braid γ_2 as $\phi_3(\gamma_3) \cdot \beta_3$ with $\gamma_3 = \phi_3^{-1}(a_{2,3}) = a_{1,2}$ and $\beta_3 = a_{1,2}$. As the braid $\phi_3(\gamma_3) = a_{2,3}$ is not right-divisible by $a_{1,2}$, its B_2^{+*}-tail is trivial. The braid $\phi_3(\gamma_3)$ it the one of (6) for $n = 3$ and $k = 3$. Eventually we express γ_3 as $\phi_3(\gamma_4) \cdot \beta_4$ with $\gamma_4 = 1$ and $\beta_4 = a_{1,2}$. The process ends as the remaining braid γ_4 is trivial. We conclude that the ϕ_3-splitting of β is $(\beta_4, \beta_3, \beta_2, \beta_1) = (a_{1,2}, a_{1,2}, 1, a_{1,2}^2)$.

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

Definition 2.4. Assume $n \geqslant 2$. 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 $A_n^{\pm}$-words, 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 ε.

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 ϕ_n-splitting.

Definition 2.5. For $\beta \in B_2^{+*}$, we define $r_2(\beta)$ to be the unique A_2-word $a_{1,2}^k$ representing β. 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 ϕ_n-splitting of β. 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, about the *rotating normal form* of a dual braid.

Example 2.6. We reconsider the braid β of Example 2.3. We know that the ϕ_3-splitting of β 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 [13]. Connections, established in [12] and [13], between the rotating normal form and the braid ordering introduced by P. Dehornoy in [6] are based on these properties.

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

Definition 2.7. For every non-empty word w, the last letter of w is denoted by $w^{\#}$. Assume $n \geqslant 2$. For each non-trivial braid β in B_n^{+*}, we define the *last letter* of β, denoted $\beta^{\#}$, to be the last letter in the rotating normal form of β.

Lemma 2.8 (Lemma 3.2 of [13]). *Assume $n \geqslant 3$ and let $(\beta_b, ..., \beta_1)$ be the ϕ_n-splitting of a braid of B_n^{+*}.*

(i) For $k \geqslant 2$, the letter $\beta_k^\#$ is of type $a_{..,n-1}$ unless $\beta_k = 1$.
(ii) For $k \geqslant 3$ and for $k = b$, we have $\beta_k \neq 1$.

The fact that β_b is not trivial is a direct consequence of the definition of ϕ_n-splitting. As, for $k \geqslant 2$, the braid $\beta' = \phi_n(\beta_{k+1}^\#)\beta_k$ is a right divisor of $\phi_n^{b-k}(\beta_b) \cdot ... \cdot \beta_k$, 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. For $n \geqslant 3$ and p, r, s in $[1, n-1]$, we say that a letter $a_{r,s}$ is an $a_{p,n}$*-barrier* if the relation $r < p < s$ holds.

There exists 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.

The following result guarantees that the rotating normal form of a braid satisfying some properties must contain an $a_{p,n}$-barrier.

Lemma 2.10 (Lemma 3.4 of [13])**.** *Assume $n \geqslant 4$, $p \in [2, n-2]$ and let β be a braid of B_{n-1}^{+*} such that the B_{n-1}^{+*}-tail of $\phi_n(a_{p,n}\beta)$ is trivial. Then the rotating normal form of β is not the empty word and it contains an $a_{p,n}$-barrier.*

It turns out that the above mentioned braid property are easily checked for entries of a ϕ_n-splitting.

Lemma 2.11 (Lemma 3.5 of [13])**.** *Assume $n \geqslant 3$ and let $(\beta_b, ..., \beta_1)$ be the ϕ_n-splitting of some braid of B_n^{+*}. 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 β_k contains a $\phi_n(\beta_{k+1}^\#)$-barrier.*

3. Left reversing for dual braid monoid

The left-reversing process was introduced by P. Dehornoy in [7]. It is a powerful tool for 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:

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

together with $f(x,x) = \varepsilon$ 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

$$\begin{aligned} f(a_{1,2}, a_{2,3}) &= f(a_{1,2}, a_{1,3}) = a_{1,3}, \\ f(a_{2,3}, a_{1,2}) &= f(a_{2,3}, a_{1,3}) = a_{1,2}, \\ f(a_{1,3}, a_{1,2}) &= f(a_{1,3}, a_{2,3}) = a_{2,3}. \end{aligned}$$

However the monoid B_4^{+*} with presentation of Proposition 1.1 is not left-complemented. Indeed there is no relation of type $\ldots a_{1,3} = \ldots a_{2,4}$. It follows that 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 words $f(a_{p,q}, a_{r,s})$ 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.

For 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 $f(a_{1,3}, a_{2,4}) = a_{1,4}a_{2,3}$ 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 $(x,y) \in A_n^2$. □

Assume $n \geqslant 2$. As illustrated above, the characterization of the map f_n from the presentation of B_n^{+*} is not well-defined: many choices are possible. Our map f_n admits the following remarkable property: for every letters $a_{p,q}$ and $a_{r,s}$ of A_n, the last letter of the word $f_n(a_{p,q}, a_{r,s})$ is of the form $a_{t,s}$, with $t \leqslant r$, whenever $q < s$. This property will be use in the sequel, for example in the proof of Lemma 4.6.

Definition 3.3. Assume $n \geqslant 2$. For w and w' two $A_n^{\pm}$-words, we say that w *left-reverses in one step* to w', denoted by $w \curvearrowleft^1 w'$, 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 $w \curvearrowleft w'$, if there exists a sequence $w = w_1, \ldots, w_\ell = w'$ of $A_n^{\pm}$-words satisfying $w_k \curvearrowleft^1 w_{k+1}$ 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 (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 $a_{1,2}a_{2,3}a_{1,2}a_{1,3}^{-1} \curvearrowright a_{2,3}a_{2,3}$.

A consequence of Lemma 1.1 of [7] is the following definition of left denominator and left numerator of an $A_n^{\pm}$-word.

Definition 3.5. Assume $n \geqslant 2$. For w an $A_n^{\pm}$-word, we denote by $D(w)$ and $N(w)$ the A_n-words, if there exist, such that $w \curvearrowright D(w)^{-1}\, N(w)$ holds. If such words exist, then they are unique, hence the notations $D(w)$ and $N(w)$ are unambiguous. 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 its left numerator is $N(u) = a_{2,3}a_{2,3}$.

Assume $n \geqslant 2$. By Example 8 of [10] based on [3], the monoid B_n^{+*} is a Garside monoid and f_n is a *left lcm selector*. A consequence of Lemma 4.3 of [10] is that for every $w \in A_n^{\pm}$, the words $N(w)$ and $D(w)$ exist. We obtain also the following result:

Proposition 3.6. *Assume $n \geqslant 2$. For w an A_n-word and $a_{p,q}$ 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 left denominator of $u = a_{1,2}a_{2,3}a_{1,2}a_{1,3}^{-1}$ 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

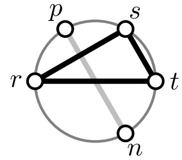
The aim of this section is to give a syntactical characterization of n-rotating words among A_n-words.

Lemma 4.1. *Assume $n \geqslant 3$. For β in B_{n-1}^{+*} there is equivalence between*

(i) an A_n-word representing β contains an $a_{p,n}$-barrier,

(ii) every A_n-word representing β contains an $a_{p,n}$-barrier.

Proof. Clearly (ii) implies (i). For $(i) \Rightarrow (ii)$ it is sufficient to prove that relations of Proposition 1.1 preserve $a_{p,n}$-barriers. For relation (2) this is immediate since it conserves involved letters. If one of the three words $a_{r,s}a_{s,t}$, $a_{s,t}a_{r,s}$ and $a_{r,t}a_{r,s}$ of relations (3) contains an $a_{p,n}$-barrier then the two others also, as illustrated by the following chord diagram.



A letter $a_{r,s}$ is an $a_{p,n}$-barrier if and only if its chord intersects properly that of the letter $a_{p,n}$. □

As a consequence, containing an $a_{p,n}$-barrier is not a word property but a braid one.

Lemma 4.2. *Assume that $n \geqslant 3$. A non-empty braid $\beta \in B_n^{+*}$ has trivial B_{n-1}^{+*}-tail if and only if there exists a unique letter in A_n that right-divides β, and this letter is of the form $a_{..,n}$.*

Proof. If $a_{p,n}$ is the only letter right-divising β, then the B_{n-1}^{+*}-tail of β is certainly trivial. Conversely, assume that the B_{n-1}^{+*}-tail of β is trivial. Hence, no letter $a_{p,q}$ with $q < n$ right-divides β. Assume, for a contradiction, that two distinct letters $a_{p,n}$ and $a_{q,n}$ with $p < q < n$ right-divide β. The braid β is then right-divisible by their lcm

$$a_{p,n} \vee a_{q,n} = a_{p,q}\, a_{q,n} = a_{q,n}\, a_{p,n} = a_{p,n},\, a_{p,q},$$

hence by $a_{p,q}$, which is impossible since the B_{n-1}^{+*}-tail of β is trivial. □

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

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

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

a strictly increasing sequence $j(0), ..., j(h)$, with $j(0) = p$ and $j(h) = n-1$, and a sequence $i(1), ..., i(h)$ 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,
(iii) the last letter of v_h is $a_{q-1,n-1}$.

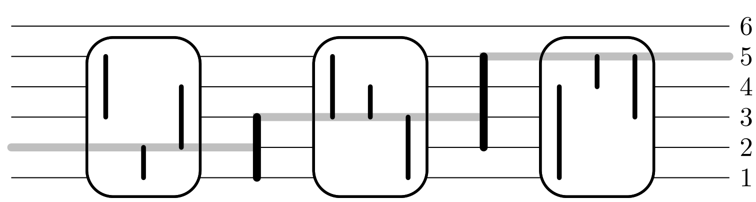


FIGURE 5. An $a_{2,6}$-ladder lent on $a_{3,5}$ (the last letter). The gray line starts at position 1 and goes up to position 5 using the bar of the ladder. The empty spaces between bars in the ladder are represented by a framed box. In such boxes the vertical line representing the letter $a_{i,j}$ does not cross the gray line. The bar of the ladder are represented by black thick vertical lines.

Condition (i) is equivalent to saying that 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 [13] is:

Lemma 4.4. *Assume $n \geqslant 4$, $p \in [2, n-2]$ and let β be a braid of B^{+*}_{n-1} such that the B^{+*}_{n-1}-tail of $\phi_n(\beta)$ is trivial and such that β contains an $a_{p,n}$-barrier. Then the rotating normal form of β is an $a_{p,n}$-ladder lent of $\beta^{\#}$.*

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

Proposition 4.5. *Assume $n \geqslant 4$. For $\beta \in B^{+*}_{n-1}$ and $p \in [2, n-2]$ 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 β contains an $a_{p,n}$-barrier,

Our proof of Proposition 4.5 rests on the following Lemma.

Lemma 4.6. *Assume $n \geqslant 3$. For u an A_{n-1}-word and $p \in [1, n-1]$, the left denominator $D(ua^{-1}_{p,n})$ is not empty. More precisely, their exists $q \in [1, p]$ such that $D(ua^{-1}_{p,n})^{-1}$ begins with $a^{-1}_{q,n}$.*

Proof. Assume that $w_1, ..., w_\ell$ is a reversing sequence from the word $w_1 = ua^{-1}_{p,n}$ to the word $D(w_1)^{-1}N(w_1)$. For $k \in [1, \ell]$ we denote by y_k^{-1} the leftmost negative letter in w_k, if such a negative letter exists in w_k. We will show by induction on $k \in [1, \ell]$ the existence of a non-increasing sequence $r(k)$ such that $y_k = a_{r(k),n}$.

By construction, we have $r(1) = p$ and $y_1 = a_{r(1),n}$. Each reversing step consists in replacing a factor xy^{-1} of w_k by $f_n(x, y)^{-1} f_n(y, x)$. For $k \in [1, \ell - 1]$, if the reversed factor of w_k does not contain the leftmost occurence of y_k^{-1} in w_k then, y_{k+1} equals y_k and so $r(k+1) = r(k)$. Assume now that the reversed factor contains the leftmost negative letter y_k of w_k and that y_k is equal to $a_{r(k),n}$. In particular, their exits a positive letter x such that the reversed factor is of the form $xy_k^{-1} = xa^{-1}_{r(k),n}$. As all letters of w_k on the left of the leftmost negative letter of w_k must belong to A_{n-1}, the letter x is of the form $a_{i,j}$ with $1 \leqslant i < j < n$. Lemma 3.2 implies

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

which gives in particular

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

It follows that y_{k+1} is equal to $a_{r(k+1),n}$ with $r(k+1) \leqslant r(k)$. Eventually we obtain that $ua^{-1}_{p,n}$ left reverses to $a^{-1}_{r(\ell),n} \cdots$ with $r(\ell) \leqslant r(1) = p$ and so the desired property on $D(ua_{p,n})$ holds. $\square$

Proof of Proposition 4.5. Let us first assume (i). As the the B_{n-1}^{+*}-tail of $\phi_n(\beta)$ is a right-divisor of $\phi_n(a_{p,n}\,\beta)$ the first statement of (ii) holds and the second statement of (ii) is Lemma 2.10.

We now prove $(ii) \Rightarrow (i)$. By Lemma 4.2 and Condition (ii), there exists a unique letter in A_n that right-divises $\phi_n(\beta)$ and it is of type $a_{..,n}$. It follows that the last letter $\beta^\#$ of β is of type $a_{..,n-1}$. We denote by w the rotating normal form of β. Let $a_{r,s}$ be an A_n-letter different from $\beta^\#$. It remains to show that $a_{r,s}$ cannot be a right divisor of $a_{p,n}\,\beta$.

Assume first $s \leqslant n-1$. Then the letter $a_{r,s}$ belongs to A_{n-1}. As β lies in B_{n-1}^{+*}, Lemma 4.2 implies that the braid $a_{r,s}$ could not be a right-divisor of β. Hence, by Proposition 3.6 the word $D(w\,a_{r,s}^{-1})$ must be non-empty. As the reversing of an $A_{n-1}^{\pm}$-word is also an $A_{n-1}^{\pm}$-word, there exists a letter $a_{t,t'}$ with $t' < n$ such that:

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

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 β plus Lemma 4.4 imply that w is an $a_{p,n}$-ladder lent on $\beta^\#$. Following Definition 4.3, we write

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

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

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

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

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

By construction w_0 is v_0 while w'_0 is the empty word and $\eta(h)$ is r. For $k \in [0,h]$, Lemma 4.6 with $u = v_k$ and $p = \eta(k)$ imply that the word

$$w_k\,a_{\eta(k),n}^{-1}\,\cdots = w'_k\,v_k\,a_{\eta(k),n}^{-1}\,\cdots$$

left-reverses to $w'_k\,a_{\mu(k),n}^{-1}\cdots$ with $\mu(k) \leqslant \eta(k)$. Then, for $k \neq 0$, Lemma 4.6 (with $u = v_{k-1}$ and $p = \mu(k)$) implies that the word

$$w'_k\,a_{\mu(k),n}^{-1}\,\cdots = w_{k-1}\,x_k\,a_{\mu(k),n}^{-1}\,\cdots$$

left-reverses to $w_{k-1}\,a_{\eta(k-1),n}^{-1}\cdots$ with $\eta(k-1) \leqslant \mu(k)$. Using an inductive argument on $k = h, \ldots, 0$ we then obtain:

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

Following Definition 4.3 we write $x_k = a_{i(k),j(k)}$.

We will now prove 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 the case where $\mu(k+1) \leqslant i(k+1)$ 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 $r = \mu(k+1)$ (satisfying the relation $i < r \leqslant j$) we obtain

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

for 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

$$\mu(h) \leqslant \eta(h) = r \leqslant n-1$$

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 $wa^{-1}_{r,n} \curvearrowright a^{-1}_{\mu(0),n} \cdots$. As $a_{\mu(0),n}$ cannot be a right divisor of $a_{p,n}$ it follows that the left denominator of $a_{p,n}\, w\, a^{-1}_{r,n}$ 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. This case is treated by the following result.

Proposition 4.7. *Assume $n \geqslant 3$. For β 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 B^{+*}_{n-1}-tail of $\phi_n(\beta)$ is trivial.

Proof. As a right divisor of $\phi_n(\beta)$ is also a right of $\phi_n(a_{n-1,n}\,\beta)$, the implication $(i) \Rightarrow (ii)$ is clear. Let us now prove $(ii) \Rightarrow (i)$. For $x \in A_{n-1}$ and y, z in A_n, the only relations in B^{+*}_n of the form $a_{n-1,n}\, x = y\, z$ with $(y, z) \neq (a_{n-1,n}, x)$ are commutations relations, for which x is of type $a_{p,q}$ with $p < q < n-1$. Hence, if w is a representative of β, the relations in the dual braid monoid B^{+*}_{n-1} allow only transforming the word $a_{n-1,n}\, w$ into words of the form $u\, a_{n-1,n}\, v$. The A_{n-2}-word u represents a dual braid that commute with $a_{n-1,n}$ and $u\, v$ represents β. By Lemma 4.2 the only letter in A_n that right-divides $\phi_n(\beta)$ is of type $a_{..,n}$, hence any representative word of β must end with a letter of type $a_{..,n-1}$. In particular v is not an A_{n-2}-word and so v is not empty and it admits only $\beta^{\#}$ as last letter. We have then established that every representative word of $a_{n-1,n}\,\beta$ ends with the letter $\beta^{\#}$ which is of type $a_{..,n-1}$. Therefore, the B^{+*}_{n-1}-tail of $\phi_n(a_{n-1,n}\,\beta)$ is trivial. □

Theorem 4.8. *Assume $n \geqslant 3$. A finite sequence $(\beta_b, ..., \beta_1)$ of braids in B^{+*}_{n-1} is the ϕ_n-splitting of a braid of B^{+*}_n if and only if:*
(i) for $k \geqslant 3$ and $k = b$, the braid β_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 β_{k-1} contains an $\phi_n(\beta_k^{\#})$-barrier.

Proof. Let $(\beta_b, ..., \beta_1)$ be the ϕ_n-splitting of some braid of B_n^{+*}. Condition (i) is 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 ϕ_n-splitting of some braid of B_n^{+*}. Condition (i) implies that β_b is not trivial. For $k \geqslant 2$ we denote by γ_k the braid

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

For $k \geqslant 3$, and for $k \geqslant 2$ 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 β_b is $\beta_b^{\#}$. Since any right divisors of a braid of B_{n-1}^{+*} lies 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 $a_{p-1,n-1}$. Conditions (ii) and (iii) imply that the B_{n-1}^{+*}-tail of $\phi_n(\beta_{k-1})$ is trivial and that β_{k-1} contains an $a_{p,n}$-barrier whenever $p < n-1$ holds. Hence, by Proposition 4.5 (for $p < n-1$) and Proposition 4.7 (for $p = n-1$), the B_{n-1}^{+*}-tail of the braid $\phi_n(a_{p,n}\beta_{k-1})$ is trivial. Using Lemma 4.2, we obtain that $\phi_n(a_{p,n}\beta_{k-1})$ is right-divisible by a unique A_n-letter. It follows that the unique A_n-letter right-divising $a_{p,n}\,\beta_{k-1}$ is $\beta_{k-1}^{\#}$.

We denote by $ua_{p-1,n-1}$ and v two A_n-words representing γ_k and β_{k-1} respectively. The braid γ_{k-1} is then represented by $\phi_n(u)a_{p,n}v$. Let y be an A_n-letter different from $\beta_{k-1}^{\#}$. As y is not a right divisor of $a_{p,n}\,\beta_{k-1}$, Proposition 3.6 implies the existence of an A_n-letter x different from $a_{p,n}$ satisfying

$$\phi_n(u)a_{p,n}vy^{-1} \curvearrowright \phi_n(u)a_{p,n}x^{-1} \cdots .$$

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 γ_{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-dividing $\phi_n(\gamma_k)$ is of type $a_{..,n}$ and so, by Lemma 4.2 the B_{n-1}^{+*}-tail of the braid γ_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 β_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 γ_3. Since $\gamma_2 = \phi_n(\gamma_3)$ holds, the letter $\phi_n^2(a_{n-2,n-1}) = a_{1,n}$ is the only letter right-dividing $\phi_n(\gamma_2)$. In particular the B_{n-1}^{+*}-tail of $\phi_n(\gamma_2)$ is trivial. $\square$

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. *Assume $n \geqslant 3$ and let $(w_b, ..., w_1)$ be a finite sequence of A_{n-1}-words. The A_n-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 with $a_{p-1,n-1}$ for some p,

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

(iv) if, for $k \geqslant 3$, the word w_k ends with $a_{p-1,n-1}$ 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 in (12) is rotating.

We denote by β_i (resp. β) 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 ϕ_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 now prove Condition (ii) of Theorem 4.8. Let k be in $[2, b]$. 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 β_k lies in B_{n-1}^{+*}, we must have $p \neq 1$ and therefore β_k is right-divisible by $a_{p-1,q-1}$ with $q-1 \leqslant n-2$. The B_{n-1}^{+*}-tail of w_k is then not trivial. Since the word w_k is $(n-1)$-rotating, its last letter must come from its B_{n-1}^{+*}-tail. Hence w_k must end with a letter $a_{i,j}$ satisfying $j \leqslant n-2$, which is in contradiction with Conditions (ii) and (iii).

We conclude applying Theorem 4.8. $\square$

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 $n \geqslant 3$ and every n-rotating word w, there exists a unique sequence $(w_b, ..., w_1)$ of $(n-1)$-rotating words such that w decomposes 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 loss of generality, we may assume that w'_k is a proper suffix of w_k, *i.e.*, $w_k = u \cdot w'_k$. Let x be the last letter of w'_{k+1} or the last letter of w'_{k+2} if w_{k+1} is empty. By Conditions (ii) and (iii) of Corollary 4.9, 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 $w'_2 = \varepsilon$. In this case w'_2 is empty and so Condition (iv) of Corollary 4.9 implies that 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 w_k is an A_{n-1}-word. $\square$

A direct consequence of Corollary 4.9 and Proposition 4.10 is

Theorem 4.11. *For $n \geqslant 3$, 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

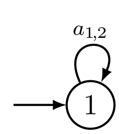
In this section we will show that the language of n-rotating words, denoted by R_n, is regular, *i.e.*, there exists a finite-state automaton recognizing the language of n-rotating words. As the rotating normal form is defined using right division it is more natural for an automaton to read words from the right. For $w = x_0 \cdot ... \cdot x_k$ an A_n-word we will denote by $\Pi(w)$ the mirror word $x_k \cdot ... \cdot x_0$. By Theorem 1.2.8 of [11] 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 6-tuple $(S \cup \{\otimes\}, A, \mu, Y, i, \otimes)$ where $S \cup \{\otimes\}$ is the finite set of *states*, A is a finite *alphabet*,

$$\mu : (S \cup \{\otimes\}) \times A \to S \cup \{\otimes\}$$

is the *transition function*, $Y \subseteq S$ is the set of *accepting states* and i is the *initial state*. In this paper each automaton is equipped with an undrawn dead state $\otimes$ and each state except the dead one is accepting, *i.e.*, $Y = S$ always hold.

To characterize $\mathcal{A}$ it is enough to describe μ on $(s, x) \in S \times A$ instead of $(S \cup \{\otimes\}) \times A$. For example an automaton recognizing the language $R_2 = \Pi(R_2)$ is $\mathcal{A}_2 = (\{1, \otimes\}, \{a_{1,2}\}, \mu_2, \{1\}, 1, \otimes)$ with $\mu_2(1, a_{1,2}) = 1$. The corresponding automaton diagram is:



The horizontal arrow points to the initial state.

We will now construct an automaton $\mathcal{A}_3$ recognizing the language $\Pi(R_3)$.

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*

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

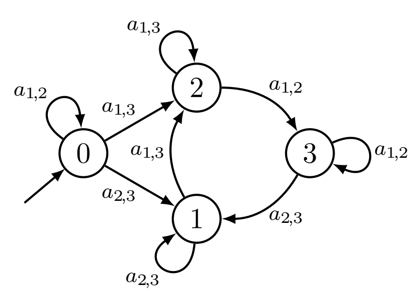
is rotating if and only if $e_k \neq 0$ for all $k \geqslant 3$.

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 each non-empty word w_k ends with $a_{1,2}$, Condition (*iv*) of Corollary 4.9 is vacuously true. Hence the word w is rotating if and only if it satisfies Conditions (*ii*) and (*iii*) of Corollary 4.9, *i.e.*, e_k is not 0 for $k \geqslant 3$. □

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



We now explain the principle of our construction of an automaton $\mathcal{A}_n$ recognizing the language $\Pi\,(R_n)$ for $n \geqslant 4$. Following the Condition (*i*) of Corollary 4.9, the construction will be done by induction on $n \geqslant 3$. Quite natural it will be more complicated for $n \geqslant 4$ than for $n = 2$ and $n = 3$ since Condition (*iv*) of Corollary 4.9 is not empty for $n \geqslant 4$ and must be checked. As suggested by Condition (*ii*) the language R_n^* (see Definition 5.2) of n-rotating words ending with a letter $a_{..,n}$ is in the core of the process. Hence, instead of directly construct the automaton $\mathcal{A}_n$ we will construct an automaton $\mathcal{A}_n^*$ recognizing the language $\Pi(R_n^*)$. As the language $\Pi(R_n)$ is the concatenation of $\Pi(R_{n-1})$ and $\Pi(R_n^*)$, the automaton $\mathcal{A}_n$ is naturally obtained from $\mathcal{A}_{n-1}$ and $\mathcal{A}_n^*$.

Assume that the automaton $\mathcal{A}_{n-1}^*$ recognizing $\Pi(R_{n-1}^*)$ is given. In order to check Condition (*iv*) of Corollary 4.9, we must modify $\mathcal{A}_{n-1}^*$ to store information about the existence of $a_{..,n}$-barriers in the involved word. A duplication of states contained in $\mathcal{A}_{n-1}^*$ together with some standard modifications on the transition function allow us to store one bit of information. Since there is exactly $n-3$ types of $a_{..,n}$-barriers we must multiply the number of states of $\mathcal{A}_{n-1}^*$ by at most 2^{n-3} in order to obtain an automaton $\mathcal{B}_{n-1}^0$ recognizing $\Pi(R_{n-1}^*)$ and detecting barriers.

Then, for $k \in [1, n-1]$ we construct an automaton $\mathcal{B}^k_{n-1}$ recognizing the language $\Pi(\phi^k_n(R^*_{n-1}))$ by applying ϕ^k_n to $\mathcal{B}^0_{n-1}$. Eventually we obtain $\mathcal{A}^*_n$ by plugging cyclically automata $\mathcal{B}^0_{n-1}, ..., \mathcal{B}^{n-1}_{n-1}$. Transitions between automata $\mathcal{B}^k_{n-1}$ and $\mathcal{B}^{k+1}_{n-1}$ will be done in respect with Condition (iv) of Corollary 4.9 thanks to informations about encountered barriers stored in $\mathcal{B}^k_{n-1}$.

Definition 5.2. For $n \geqslant 2$, we denote by R^*_n the language of n-rotating words that are empty or end with a letter of type $a_{p,n}$ for some p.

As explained above, we will first 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 6-tuple $P = (S \cup \{\otimes\}, A, \mu, S, I, \otimes)$ where S, A and μ are defined as for an automaton and $I : A \to S \cup \{\otimes\}$ is the *initial* map. The closure of a partial automaton P is the automaton

$$\mathcal{A}(P) = (S \cup \{\circ, \otimes\}, A, \mu^c, S \cup \{\circ\}, \circ, \otimes)$$

whose transition function is given by

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

In the sequel, we will plug partial automata using their initial maps. A partial automaton is represented as an automaton excepted for the initial map I: for each $x \in A$ we draw an arrow attached to the state $I(x)$ and labelled x. We say that a partial automaton recognizes a given language if its closure does.

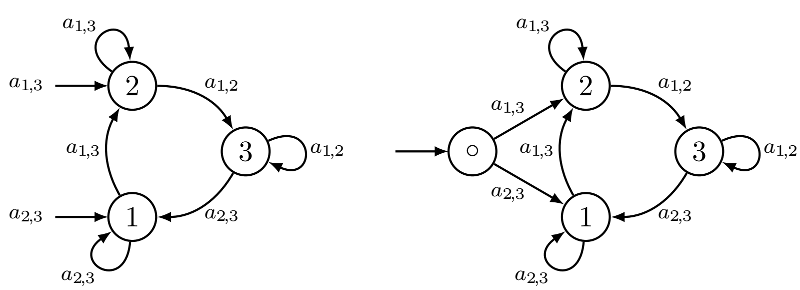


FIGURE 6. The partial automaton P_3 and the corresponding closure, which recognizes the language $\Pi(R^*_3)$.

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 that $n \geqslant 4$ and that

$$P^*_{n-1} = (S^*_{n-1} \cup \{\otimes\}, A_{n-1}, \mu^*_{n-1}, S^*_{n-1}, I^*_{n-1}, \otimes)$$

is a given partial automaton which recognizes the language $\Pi(R^*_{n-1})$.

We construct a partial automaton P_n^0 that recognize $\Pi(R_{n-1}^*)$ and store informations about the encountered barriers. We define S_n^0 to be the set

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

A state in S_n^0 is then written $(0, s, m)$. The integer 0 is used to identify this particular partial automaton among those that will eventually constitute P_n^*. The set m stores informations on encountered barriers.

For $a_{i,j} \in A_{n-1}$ we denote by $\mathrm{bar}(a_{i,j})$ the set of letters $a_{p,n}$ such that $a_{i,j}$ is an $a_{p,n}$-barrier, *i.e.*,

$$\mathrm{bar}(a_{i,j}) = \{a_{p,n} \,|\, i < p < j\}.$$

Definition 5.4. We define $P_n^0 = (S_n^0 \cup \{\otimes\}, A_{n-1}, \mu_n^0, S_n^0, I_n^0, \otimes)$ to be the partial automaton defined by: 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 $\Pi\left(R_{n-1}^*\right)$. Moreover an accepted A_n-word $\Pi(w)$ contains an $a_{p,n}$-barrier if and only if P_n^0 has state $(0, s, m)$ with $a_{p,n} \in m$ after reading $\Pi(w)$.*

Proof. We denote by $\mathcal{A}$ and $\mathcal{A}'$ the closure of P_{n-1}^* and P_n^0 respectively. Assume $w = w_1 \cdot \ldots \cdot w_\ell$ is an A_n-word of length ℓ. For all $k \in [1, \ell]$, we denote by s_k (resp. s'_k) the state of the automaton $\mathcal{A}$ (resp. $\mathcal{A}'$) after reading the k-th letter of $\Pi(w)$, *i.e.*, the letter $w_{\ell-k+1}$. By construction of μ_n^0, for all $k \in [1, \ell]$, we have

$$s'_k = \begin{cases} \otimes & \text{if } s_k = \otimes, \\ (0, s_k, m_k) & \text{otherwise (for a certain set } m_k). \end{cases}$$

In particular $s'_\ell \neq \otimes$ if and only if $s_\ell \neq \otimes$. Hence both automata accept the word $\Pi(w)$ or not and so P_n^0 recognizes $\Pi(R_{n-1}^*)$ since P_{n-1}^* does.

Let us prove the result on m_ℓ whence $\Pi(w)$ is accepted. By an immediate induction of $k \in [1, \ell]$, the set m_k contains $\mathrm{bar}(w_\ell) \cup \ldots \cup \mathrm{bar}(w_{\ell-k+1})$. The set m_ℓ is then $\mathrm{bar}(w_1) \cup ... \cup \mathrm{bar}(w_\ell)$. We conclude by definition of bar(), that w contains an $a_{p,n}$-barrier if and only if $a_{p,n}$ belongs to m_ℓ. □

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 7.

We now construct $n-1$ twisted copies of P_n^0 using the word homomorphism ϕ_n. For $t = (0, s, m) \in S_n^0$ and $k \in [1, n-1]$, we define $\Phi_n^k(t)$ to be

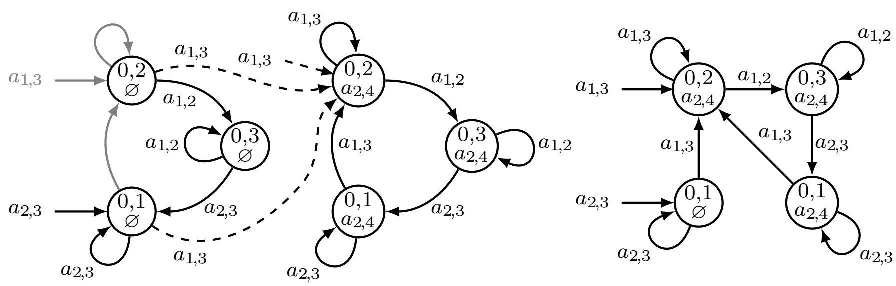


FIGURE 7. The partial automaton P_4^0. Obsolete transitions from P_3^* are in gray. New added transitions are dashed. The right partial automaton is P_4^0 without inaccessible states.

the state (k, s, m). We also define S_n^k to be $\Phi_n^k\left(S_n^0\right)$ and

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

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 the state $(0, s, m)$ by (k, s, m). By Proposition 5.5, we obtain immediately that P_n^k recognizes the language $\phi_n^k\left(\Pi(R_n^*)\right)$ and store informations about encountered barriers.

We can now construct the partial automaton P_n^* by plugging cyclically n partial automata P_n^k for $k \in [0, n-1]$. Transition between two adjacent partial automata is done using initial maps accordingly to Condition (iv) of Corollary 4.9.

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

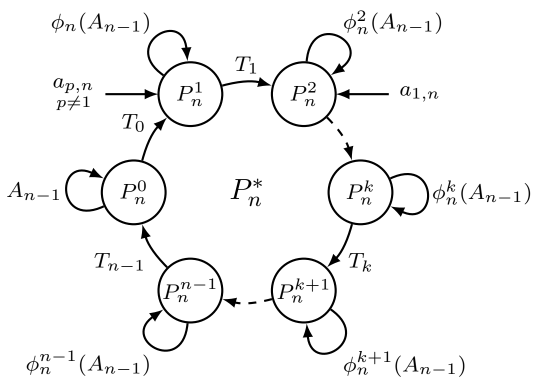
$$I_n^*(x) = \begin{cases} I_n^1(x) & \text{if } x = a_{p,n} \text{ with } p \neq 1, \\ I_n^2(x) & \text{if } x = a_{1,n}, \\ \otimes & \text{otherwise,} \end{cases}$$

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

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

and for all i, the word $\phi_n^i(w_i)$ is the maximal suffix of $\phi_n^{b-1}(w_b)\cdot...\cdot\phi_n^i(w_i)$ belonging to $\phi_n^i\left(A_{n-1}^*\right)$. By definition of I_n^*, the word $\Pi(w)$ is accepted by P_n^* only if w ends with 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 $p=1$. In both cases, after reading the first letter of $\Pi(w)$, the automaton $\mathcal{A}^*$ is in state $s\in S_n^j$. The automaton reaches a state outside of S_n^j if it goes to the state $\otimes$ or if it reads a letter outside of $\phi_n^{j-1}(A_{n-1})$, *i.e.*, a letter of $\phi_n^j(\Pi(w_{j+1}))$. This is a general principle: after reading a letter of $\phi_n^{i-1}(\Pi(w_i))$ the automaton $\mathcal{A}$ is in state (t,s,m) with $t=i$ mod n. By construction of P_n^t, the word $\phi_n^{i-1}(\Pi(w_i))$ provides an accepted state if and only if w_i is a word of 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 $t=i$ mod n after reading the word

$$\Pi(\phi_n^{i-1}(w_i)\cdot...\cdot\phi_n(w_2)\cdot w_1).$$

We denote by x the letter $w_{i+1}^\#$. By construction of w_{i+1}, the letter x does not belong to $\phi_n^{i-1}(A_{n-1})$ and so $x=\phi_n^i(a_{p,n})$ for some p. By definition of μ_n^* we have $\mu_n^*((t,s,m),\phi_n^i(a_{p,n}))\neq\otimes$ if and only if $p=n-1$ or if $p\in[2,n-2]$ together with $a_{p,n}\in m$. As, by construction of P_n^t, we have $a_{p,n}\in m$ if and only if w_i contains an $a_{p,n}$-barrier, Condition (iv) of Corollary 4.9 is satisfied.

Eventually, by Corollary 4.9, the word $\Pi(w)$ is accepted by $\mathcal{A}$ if and only if w belongs to R_n^*. $\square$

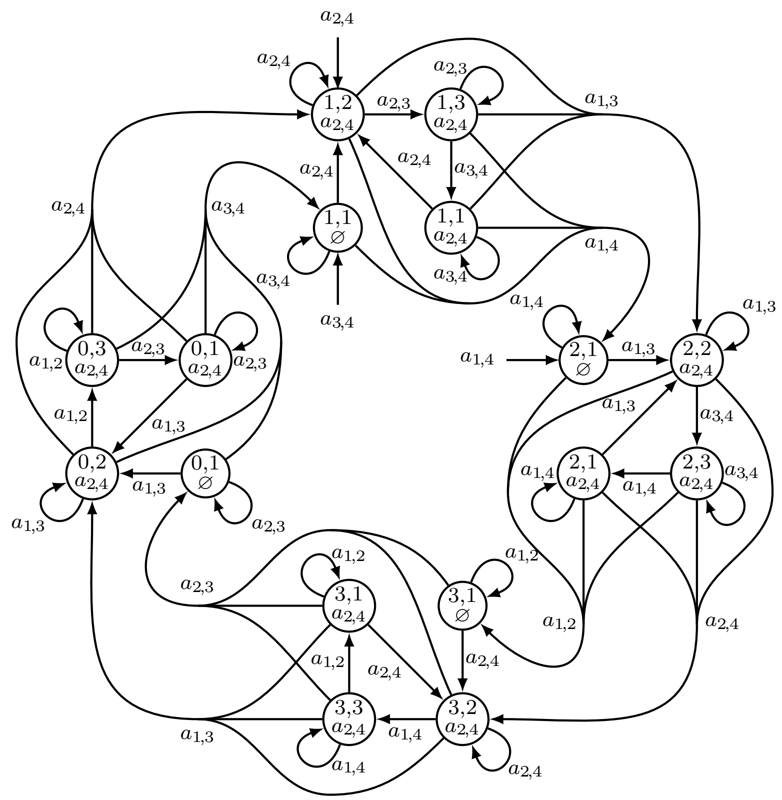


FIGURE 8. Partial automaton recognizing the language $\Pi\left(R_4^*\right)$.

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

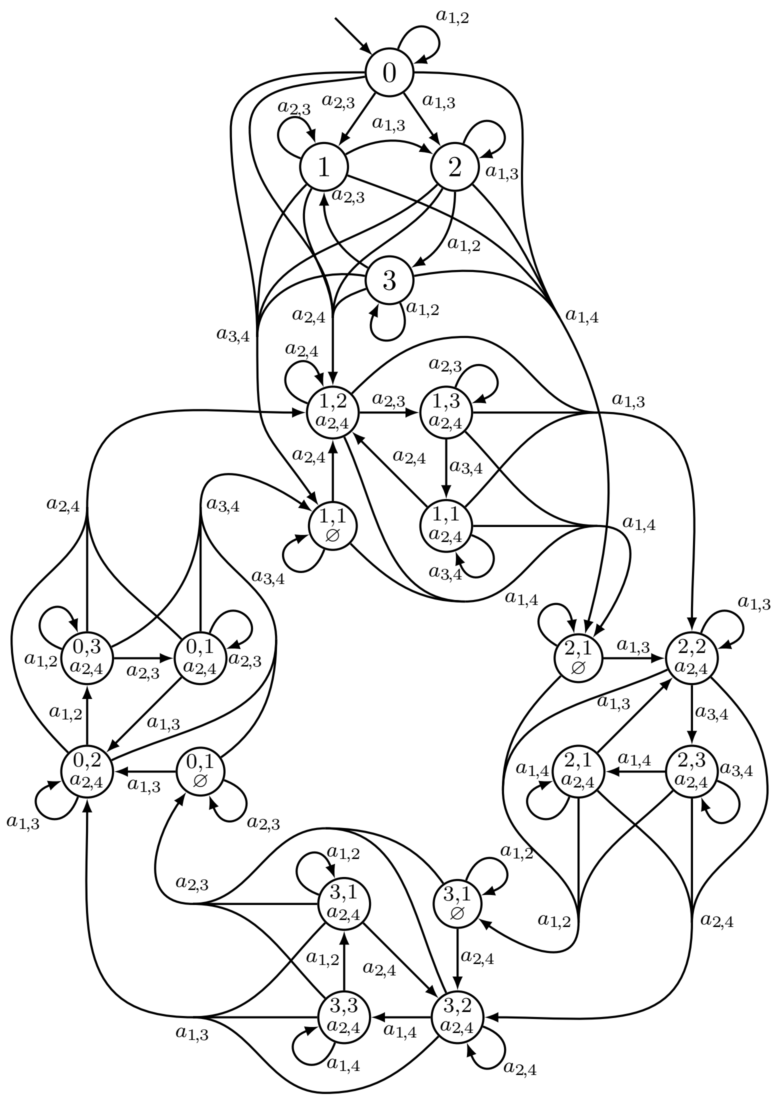


FIGURE 9. Automaton $\mathcal{A}_4$ for the language $\Pi(R_4)$.

the case. By Lemma 5.7 the automaton $\mathcal{A}_n$ is 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. $\square$

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.*

6. Application to σ-definite representative

It it well known since [6] that Artin's braid groups are orderable, by an ordering that enjoys many remarkable properties [9]. The existence of this ordering rests on the property that every non-trivial braid admits a σ-definite representative, *i.e.*, a braid word w in standard Artin generator $\sigma_1, \sigma_2, ...$ in which the generator σ_i with highest index i occurs only positively (no σ_i^{-1}), in which case w is called σ_i-positive, or only negatively (no σ_i), in which case w is called σ_i-negative. Thanks to the word homomorphism defined by $a_{p,q} \mapsto \sigma_p \ldots \sigma_{q-1}\, \sigma_q\, \sigma_{q-1}^{-1} \ldots \sigma_p^{-1}$, the notions of σ-definite, σ_i-positive and σ_i-negative words extend naturally to $A_n^{\pm}$-words. In [13] a particular σ-definite representative is obtained for every non-trivial braid from its rotating normal form.

We say that a braid has *index* $k \geqslant 2$ if it belongs to B_k and not to B_{k-1} with the convention $B_1 = \{1\}$. Each representative, in standard Artin generator, of a braid of index $k \geqslant 2$ must contain a letter σ_{k-1} or a letter σ_{k-1}^{-1}. Hence such a braid is either σ_{k-1}-positive or σ_{k-1}-negative.

First we recall how uniquely express a braid as a quotient.

Proposition 6.1 (Proposition 6.1 of [13])**.** *Assume $n \geqslant 3$. Each braid β of B_n admits a unique expression $\delta_n^{-t}\, w$ where t is a non-negative integer, w is an n-rotating normal word, and the braid $\overline{w}$ is not left-divisible by δ_n unless t is zero.*

A direct adaptation to dual braid context of Proposition 4.4 of [14] gives:

Proposition 6.2. *Assume $n \geqslant 3$ and β is a braid of B_n^{+*}. Let t be a positive integer and $(w_b, ..., w_1)$ the ϕ_n-splitting of β. If $t \geqslant b-1$ holds then the quotient $\delta_n^{-t}\, \beta$ is represented by the σ_{n-1}-negative $A_n^{\pm}$-word*

$$\delta_n^{-t+b+1}\, w_b\, \delta_n^{-1}\, w_{b-1}\, \delta_n^{-1} \ldots w_2\, \delta_n^{-1}\, w_1, \tag{13}$$

where δ_n is written as the word $a_{1,2}\, a_{2,3} \ldots a_{n-1,n}$. Moreover if $t < b-1$ then the quotient $\delta_n^{-t}\, \beta$ is not σ_{n-1}-negative.

Proposition 6.2 gives specific σ-definite representative to each σ_{n-1}-negative braid of B_n. Unfortunately this representative word is not unique.

Definition 6.3. We denote by $\mathrm{R}_n^{\sigma^{-1}}$ the words of the form (13) such that the braid $\phi_n^{b-1}(w_b) \cdot ... \cdot \phi_n(w_2) \cdot w_1$ is not left-divisible by δ_n.

Assume $(w_b, ..., w_1)$ is a sequence of A_{n-1}-words satisfying Conditions (i)–(iv) of Corollary 4.9. In section 5 we have explicitly constructed by induction a finite-state automaton recognizing the mirror of the word $\phi_n^{b-1}(w_b) \cdots w_1$. This construction rests on verification of conditions of Corollary 4.9 and on the detection of transition between words $\phi_n^{i-1}(w_i)$ and $\phi_n^{i}(w_{i+1})$. Thus, if we add a letter $\$$ to the alphabet A_n we can construct a finite-state automaton recognizing the mirrors of words $w_b\$w_{b-1}\$...\$w_2\$w_1$.

Since A_n contains no negative letters, the word δ_n^{-1} can play the role of the letter $\$$. Hence their exists a finite-state automaton recognizing the reverse of the word

$$w_b\, \delta_n^{-1}\, w_{b-1}\, \delta_n^{-1} \dots w_2\, \delta_n^{-1}\, w_1.$$

We then obtain that mirror of words of (13) constitute a regular language.

Proposition 6.4. *For $n \geqslant 2$, the language $R_n^{\sigma^{-1}}$ is regular.*

Proof. The result is immediate for $n = 2$. Assume $n \geqslant 3$. We denote by W_n the set of words as in (13). As explained previously the language W_n is regular. Let $\mathcal{B}_n$ be a finite-state automaton recognizing W_n and let w be a word as in (13). Following Section 9.2 of [11] we can modify $\mathcal{B}_n$ such that it memorize the maximal simple element $\mathrm{head}(w)$ of B_n^{+*} that left-divides the dual braid $\phi_n^{b-1}(w_b)\cdot \ldots \cdot \phi_n(w_2)\cdot w_1$. Accepting only words such that $\mathrm{head}(w)$ is different from δ_n we obtain an finite-sate automaton which recognize the language $\mathrm{R}_n^{\sigma^{-1}}$. $\square$

Since the inverse of σ_{n-1}-positive braid is a σ_{n-1}-negative braid, each braid of index n admits a representative either in $\mathrm{R}_n^{\sigma^{-1}}$ or in its inverse $\mathrm{R}_n^{\sigma^{+}} = \{w^{-1} \mid w \in \mathrm{R}_n^{\sigma^{-1}}\}$. As $\mathrm{R}_n^{\sigma^{-1}}$ is regular the language $\mathrm{R}_n^{\sigma^{+}}$ is also regular. Defining two regular languages $\mathrm{R}_2^{\sigma^{-1}} = \{a_{1,2}^k \mid k < 0\}$ and $\mathrm{R}_2^{\sigma^{+}} = \{a_{1,2}^k \mid k > 0\}$ we immediately obtain:

Proposition 6.5. *Assume $n \geqslant 2$. Then each braid of B_n admits a unique σ-definite representative lying in*

$$S_n = \{\varepsilon\} \sqcup \bigsqcup_{k=2}^{n} \left(R_k^{\sigma^{-1}} \sqcup R_k^{\sigma^{+}}\right). \tag{14}$$

Since the union of regular languages is also regular, we obtain:

Theorem 6.6. *For $n \geqslant 2$ the language S_n of σ-definite representative of braids of B_n is regular.*

7. Automaticity

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.

From [5] and [11] we introduce the following definition:

Definition 7.1. 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 automaton 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 $L(W)$.

A consequence of Theorem 2.3.5 of [11] is that automaticity for groups is equivalent to *fellow traveller property*. As pointed in [5] the situation is more complicated for monoids. But with Definition 3.11 of [5] for fellow traveller property on monoids we have, Proposition 3.12 of [5], that right (resp. left) automaticity of monoids implies right (resp. left) fellow traveller property of monoids.

As pointed by the anonymous referee the rotating normal form is not right automatic (or even asynchronously right automatic) for $n \geqslant 4$. For all integers $k \geqslant 0$, we define two words

$$w = (a_{2,3}a_{1,2}a_{1,3})^k\, a_{1,2}^{3k}, \quad \text{and} \quad w' = (a_{1,3}a_{2,3}a_{1,2})^k a_{1,4} a_{2,3}^{3k}.$$

The ϕ_4-splitting of w is (w) and w is 3-rotating by Proposition 5.1 and so 4-rotating. The ϕ_4-splitting of w' is $(\underbrace{a_{2,3}, ..., a_{2,3}}_{3k+1}, 1, a_{2,3}^{3k})$. Using Corollary 4.9 we have that w' is 4-rotating.

We observe that $a_{2,3}a_{1,2}a_{1,3}a_{1,2}^3 \equiv a_{1,3}a_{2,3}a_{1,2}a_{2,3}^3 = \delta_3^3$. Since by [3] the braid δ_3^3 is in the center of B_3^{+*} we have $w \equiv \delta_3^{3k}$ and

$$w' \equiv (a_{1,3}a_{2,3}a_{1,2})^k a_{2,3}^k a_{1,4} \equiv \delta_3^{3k} a_{1,4} \equiv w a_{1,4}.$$

Finally, w and w' end with $3k$ copies of two different letters of A_4, hence the (asynchronous) fellow traveller property is falsified. As a consequence we obtain that the n-rotating normal form is not automatic for $n = 4$ (and for $n > 4$ as well).

At this time we don't know if the rotating normal form is left automatic. We think that contrary to the previous example, if w is an n-rotating word and x is an A_n-letter then the existence of barrier in x prevents migration to far on the right of x during the computation of rotating normal form of the braid represented by xw.

Acknowledgments. The author wishes to thank the anonymous referee for his/her very sharp and constructive comments.

References

[1] E. Artin. Theorie der Zöpfe. *Abh. Math. Sem. Univ. Hanburg*, 4:47–72, 1925.
[2] D. Bessis. The dual braid monoid. *Ann. Sci. École Norm. Sup. (4)*, 36(5):647–683, 2003.
[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(2):322–353, 1998.
[4] S. Burckel. The wellordering on positive braids. *J. Pure Appl. Algebra*, 120(1):1–17, 1997.
[5] C. M. Campbell, E. F. Robertson, N. Ruškuc, and R. M. Thomas. Automatic semigroups. *Theoretical Computer Science*, 250(1-2):365–391, 2001.
[6] P. Dehornoy. Braid groups and left distributive operations. *Trans. Amer. Math. Soc.*, 345(1):115–150, 1994.

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

[8] P. Dehornoy. Alternating normal forms for braids and locally Garside monoids. *J. Pure Appl. Algebra*, 212(11):2413–2439, 2008.

[9] P. Dehornoy, I. Dynnikov, D. Rolfsen, and B. Wiest. *Ordering braids*, volume 148 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2008.

[10] P. Dehornoy and L. Paris. Gaussian groups and Garside groups, two generalisations of Artin groups. *Proc. London Math. Soc. (3)*, 79(3):569–604, 1999.

[11] 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.

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

[13] J. Fromentin. Every braid admits a short sigma-definite expression. *Journal of the European Mathematical Society (JEMS)*, 13(6):1591–1631, 2011.

[14] J. Fromentin and L. Paris. A simple algorithm for finding short sigma-definite representatives. *J. Algebra*, 350:405–415, 2012.