2008-02

ALTERNATING NORMAL FORMS FOR BRAIDS AND LOCALLY GARSIDE MONOIDS

PATRICK DEHORNOY

Abstract. We describe new types of normal forms for braid monoids, Artin–Tits monoids, and, more generally, for all monoids in which divisibility has some convenient lattice properties ("locally Garside monoids"). We show that, in the case of braids, one of these normal forms coincides with the normal form introduced by Burckel and deduce that the latter can be computed easily. This approach leads to a new, simple description for the standard order ("Dehornoy order") of B_n in terms of that of B_{n-1}, and to a quadratic upper bound for the complexity of this order.

The first aim of this paper is to improve our understanding of the well-order of positive braids and of the Burckel normal form of [6, 7], which after more than ten years remain mysterious objects. This aim is achieved, at least partially, by giving a new, alternative definition for the Burckel normal form that makes it natural and easily computable. This new description is direct, involving right divisors only, while Burckel's original approach resorts to iterating some tricky reduction procedure. It turns out that the construction we describe below relies on a very general scheme for which many monoids are eligible, and we hope for further applications beyond the case of braids.

After the seminal work of F.A. Garside [23], braid monoids are known to be equipped with a normal form, namely the so-called greedy normal form of [5, 1, 20, 33], which gives for each element of the monoid a distinguished representative word. This normal form, which also exists in spherical Artin–Tits monoids and in Garside monoids that generalize them, is excellent both in theory and in practice as it provides a bi-automatic structure and it is easily computable [21, 10, 14].

In this paper we proceed to construct a new type of normal form for braid monoids and their generalizations. Our construction keeps one of the ingredients of the (right) greedy normal form, namely considering the maximal right divisor that lies in some subset A, but, instead of taking for A the set of so-called simple elements, *i.e.*, the divisors of the Garside element Δ, we choose A to be some standard parabolic submonoid M_I of M, *i.e.*, the monoid generated by some subset I of the standard generating set S. When I is a proper subset of S, the submonoid M_I is a proper subset of M, and the construction stops after one step. However, by considering two parabolic submonoids M_I, M_J which together generate M, we can obtain a well-defined, unique decomposition consisting of alternating factors in M_I and M_J, as in the case of an amalgamated product. By considering convenient families of submonoids, we can iterate the process and obtain a unique normal form for each element of M. When it exists, typically in all Artin–Tits monoids, such a

1991 *Mathematics Subject Classification.* 20F36, 20M05, 06F05.

Key words and phrases. braid group, braid ordering, normal form, Garside monoid, Artin–Tits monoid, locally Garside monoid.

normal form is exactly as easy to compute as the greedy normal form, and, as the greedy form, it solves the word problem in quadratic time.

The above construction is quite general, as it only requires the ground monoid M to be what is now called locally right Garside—or locally left Gaussian in the obsolete terminology of [17]. However, our main interest in the current paper lies in the case of braids and, more specifically, their order. For a convenient choice of the parameters, the alternating normal form turns out to coincide with the Burckel normal form of [7]. As a consequence, we obtain both an easy algebraic description of the latter, and an efficient algorithm for computing it. Mainly, because of the connection between the Burckel normal form and the standard order of braids ("Dehornoy order"), we obtain a new characterization of the latter. The result can be summarized as follows. As usual, B_n^+ denotes the monoid of positive n-strand braids. We denote by Φ_n the involutive flip automorphism of B_n^+ that maps σ_i to σ_{n-i} for each i, and by $<$ the standard braid order.

Theorem A. (i) *Every positive n-strand braid x admits a unique decomposition*

$$x = \Phi_n^{p-1}(x_p) \cdot \ldots \cdot \Phi_n^2(x_3) \cdot \Phi_n(x_2) \cdot x_1$$

with $x_p, \ldots, x_1$ in B_{n-1}^+ such that, for each $r \geqslant 2$, the only generator σ_i that divides $\Phi_n^{p-r}(x_p) \cdot \ldots \cdot \Phi_n(x_{r+1}) \cdot x_r$ on the right is σ_1. Starting from $x^{(0)} = x$, the element x_r is determined by the condition that x_r is the maximal right divisor of $x^{(r)}$ that lies in B_{n-1}^+, and $x^{(r)}$ is $\Phi_n(x^{(r-1)} x_r^{-1})$.

(ii) *Let x, y be positive n-strand braids. Let $(x_p, \ldots, x_1)$ and $(y_q, \ldots, y_1)$ be the sequences associated with x and y as in* (i). *Then $x < y$ holds in B_n^+ if and only if we have either $p < q$, or $p = q$ and, for some $r \leqslant p$, we have $x_{r'} = y_{r'}$ for $r < r' \leqslant p$ and $x_r < y_r$ in B_{n-1}^+.*

In other words, via the above decomposition, the order of B_n^+ is a `ShortLex`-extension of that of B_{n-1}^+, this meaning the variant of lexicographical extension in which the length is given priority. In the above statement, Point (i)—Proposition 4.1 below—is easy, but Point (ii)—Corollary 5.20—is not. Another outcome of the current approach is the following complexity upper bound for the braid order—Corollary 5.22:

Theorem B. *For each n, the standard order of B_n has at most a quadratic complexity: given two n-strand braid words u, v of length ℓ, we can decide whether the braid represented by u is smaller than the braid represented by v in time $O(\ell^2)$.*

We think that the tools developed in this paper might be useful for addressing other types of questions, typically those involving conjugacy in B_n.

The paper is organized as follows. In Section 1, we describe the alternating decompositions obtained when considering two submonoids in a locally Garside monoid. In Section 2, we show how to iterate the construction using a binary tree of nested submonoids. In Section 3, we deduce a normal form result in the case when the base submonoids are generated by atoms. From Section 4 on, we concentrate on the specific case of braids and investigate what we call the Φ-splitting and the Φ-normal form of a braid. In Section 5, we investigate the connection between the Φ-normal form and the Burckel normal form, and deduce the above mentioned applications to the braid order. Finally, we gather in Section 6 some further results and open questions.

Remark. All constructions developed in this paper involve right divisibility and the derived notions. This choice is dictated by the applications to braids of Section 5. We could have used left divisibility instead and obtained symmetric versions in the framework of monoids that are locally Garside on the left.

We use $\mathbb{N}$ for the set of all nonnegative integers.

1. Alternating decompositions

We construct unique decompositions for the elements of monoids in which enough least common left multiples (left lcm's) exist. If M is such a monoid and A is a subset of M that is closed under the left lcm operation, then, under weak additional assumptions, every element x admits a distinguished decomposition $x = x'x_1$, where x_1 is a maximal right divisor of x that lies in A. The element x_1 will be called the A-tail of x. If we assume that every non-trivial (*i.e.*, $\neq 1$) element of M has a non-trivial A-tail, we can consider the A-tail of x', and, iterating the process, obtain a distinguished decomposition of x as a product of elements of A, as done for the standard greedy normal form of Garside monoids. Here, we drop the assumption that every non-trivial element has a non-trivial A-tail, but instead consider two subsets A_1, A_2 of M with the property that, for every non-trivial x, at least one of the A_1- or A_2-tails of x is non-trivial. Then, we obtain a distinguished decomposition of x as an alternating product of elements of A_1 and of A_2.

1.1. Locally Garside monoids.

Divisibility features play a key rôle throughout the paper, and we first fix some notation.

Notation 1.1. For M a monoid and $x, y \in M$, we say that y is a *right divisor* of x, or, equivalently, that x is a *left multiple* of y, denoted $x \succcurlyeq y$, if $x = zy$ holds for some z; we write $x \succ y$ if $x = zy$ holds for some $z \neq 1$. The set of all right divisors of x is denoted by $\mathrm{Div}_R(x)$.

The approach considered below turns out to be relevant for the following monoids.

Definition 1.2. We say that a monoid M is a *locally right Garside* if:
(C_1) The monoid M is right cancellative, *i.e.*, $xz = yz$ implies $x = y$;
(C_2) Any two elements of M that admit a common left multiple admit a left lcm;
(C_3) For every x in M, there is no infinite ascending chain in $(\mathrm{Div}_R(x), \prec)$, *i.e.*, there is no sequence $x_1, x_2, \ldots$ in $\mathrm{Div}_R(x)$ such that $x_{n+1} \succ x_n$ holds for every n.

If M is a locally right Garside monoid, and x, y are elements of M satisfying $x \succcurlyeq y$, the element z satisfying $x = zy$ is unique by right cancellativity, and we denote it by $x\,y^{-1}$.

Example 1.3. According to [5] and [29], all Artin–Tits monoids are locally right (and left) Garside. We recall that an Artin–Tits monoid is a monoid generated by a set S and relations of the form $sts... = tst...$ with $s, t \in S$, both sides of the same length, and at most one such relation for each pair s, t. An important example is Artin's braid monoid B_n^+ [24], which corresponds to $S = \{\sigma_1, \ldots, \sigma_{n-1}\}$ with

$$\sigma_i\sigma_j = \sigma_j\sigma_i \quad \text{for } |i-j| \geqslant 2, \qquad \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \quad \text{for } |i-j| = 1. \tag{1.1}$$

As the name suggests, more general examples of locally Garside monoids are the Garside monoids of [18, 14, 11, 12, 31], which include torus knot monoids [32], dual braid monoids [4], and many more.

If M is locally right Garside, then no non-trivial element of M is invertible: if we had $xy = 1$ with $x \neq 1$, hence $y \neq 1$, the sequence $x, 1, x, 1, ...$ would contradict (C_3). So right divisibility is antisymmetric, and, therefore, it is a partial order on M. As a consequence, the left lcm, when it exists, is unique.

Definition 1.2—which also appears in [19]—is satisfactory in that it exclusively involves the right divisibility relation, and it directly leads to Lemma 1.5 below. Actually, it does not coincide with the definitions of [14] and [18], where (C_3) is replaced with some condition involving left divisibility. However, both definitions are equivalent. For a while, we use $\prec_L$ for the proper left divisibility relation, *i.e.*, $x \prec_L y$ means $y = xz$ with $z \neq 1$. Let us consider the following conditions:

(C_3') There is no infinite descending chain in $(M, \prec_L)$.

(C_3^+) There exists $\lambda : M \to \mathbb{N}$ such that $y \neq 1$ implies $\lambda(xy) \geqslant \lambda(x) + \lambda(y) > \lambda(x)$.

Lemma 1.4. (i) *Condition* (C_3^+) *implies* (C_3).
(ii) *Condition* (C_3) *implies* (C_3').
(iii) *If M is right cancellative,* (C_3) *is equivalent to* (C_3').

Proof. (i) Assume that $\lambda : M \to \mathbb{N}$ satisfies the hypotheses of (C_3^+). Then $z \neq 1$ implies $\lambda(z) \geqslant \lambda(1) + \lambda(z) > \lambda(1)$, hence $\lambda(z) \geqslant 1$. Therefore $y \succ x$ implies $\lambda(y) > \lambda(x)$, since $y = zx$ with $z \neq 1$ implies $\lambda(y) \geqslant \lambda(z) + \lambda(x)$. It follows that every ascending sequence in $\mathrm{Div}_R(x)$ has length at most $\lambda(x)$, and (C_3) is satisfied.

(ii) Assume that (C_3') fails in M. Let $z_0, z_1, ...$ be a descending chain for $\prec_L$. For each n, choose $y_n \neq 1$ satisfying $z_n = z_{n+1} y_n$. Let $x = z_0$, $x_1 = 1$, and, inductively, $x_{n+1} = y_n x_n$. By construction, we have $x_{n+1} \succ x_n$ for each n. Now, we also have $x = z_n x_n$ for each n, so all elements x_n belong to $\mathrm{Div}_R(x)$, and the sequence $x_1, x_2, ...$ witnesses that (C_3) fails.

(iii) Assume that M is right cancellative and (C_3) fails in M. There exists x in M and a sequence $x_1, x_2, ...$ in $\mathrm{Div}_R(x)$ such that $x_{n+1} \succ x_n$ holds for every n. So, for each n, there exists $y_n \neq 1$ satisfying $x_{n+1} = y_n x_n$. On the other hand, as x_n belongs to $\mathrm{Div}_R(x)$, there exist z_n satisfying $x = z_n x_n$. We find

$$x = z_n x_n = z_{n+1} x_{n+1} = z_{n+1} y_n x_n.$$

By cancelling x_n on the right, we deduce $z_n = z_{n+1} y_n$, hence $z_{n+1} \prec_L z_n$ for each n, and the sequence $z_0, z_1, ...$ witnesses that (C_3') fails. □

Condition (C_3^+) holds in particular in every monoid that is presented by homogeneous relations, *i.e.*, relations of the form $u = v$ where u and v are words of the same length: then we can define $\lambda(x)$ to be the length of any word representing x. This is the case for the Artin–Tits monoids of Example 1.3.

Lemma 1.4 implies that locally right Garside monoids coincide with the monoids called locally left Gaussian in [14], in connection with the left Gaussian monoids of [18]. The reason for changing terminology is that the current definition is coherent with [19] and it is more natural: locally right Garside monoids involve right divisibility, and the normal forms we discuss below are connected with what is usually called the right normal form.

Assume that M is a locally right Garside monoid. Condition (C_2) is equivalent to saying that, for every x in M, any two elements of $\mathrm{Div}_R(x)$ admit a left lcm, and it follows that any finite subset of $\mathrm{Div}_R(x)$ admits a global left lcm. By the Noetherianity condition (C_3), the result extends to arbitrary subsets. We say that a set X is *closed under left lcm* if the left lcm of any two elements of X exists and lies in X whenever it exists in M, *i.e.*, by (C_2), whenever these elements admit a common left multiple in M.

Lemma 1.5. *Assume that M is a locally right Garside monoid, and $x \in M$. Then every nonempty subset X of $\mathrm{Div}_R(x)$ admits a global left lcm x_1; if moreover X is closed under left lcm, then x_1 belongs to X.*

Proof. Assume first that X is closed under left lcm. By the axiom of dependent choices, Condition (C_3) implies that $(\mathrm{Div}_R(x), \succ)$ is a well-founded poset, so X admits some $\succ$-minimal, *i.e.*, some $\prec$-maximal, element x_1: so $x'x_1 \in X$ implies $x' = 1$. Then x_1 is a global left lcm for X. Indeed, assume $y_1 \in X$. By hypothesis, x_1 and y_1 lie in $\mathrm{Div}_R(x)$, so, by (C_2), they admit a left lcm z, which can be expressed as $z = y'y_1 = x'x_1$. The hypothesis that X is closed under left lcm implies $z \in X$. The choice of x_1 implies $x' = 1$, hence $x_1 \succcurlyeq y_1$.

If the assumption that X is closed under left lcm is dropped, we can apply the above result to the closure $\widehat{X}$ of X under left lcm. Then the global left lcm x_1 of $\widehat{X}$ is a global left lcm for X, but we cannot be sure that x_1 lies in X—yet it is certainly the left lcm of some finite subset of X. ☐

Although standard, the previous result is crucial. By applying Lemma 1.5 to the subset $\mathrm{Div}_R(x) \cap \mathrm{Div}_R(y)$ of $\mathrm{Div}_R(x)$, we deduce that any two elements x, y of a locally right Garside monoid M admit a right gcd (greatest common divisor), and, therefore, for every x in M, the structure $(\mathrm{Div}_R(x), \succcurlyeq)$ is a lattice, with minimum 1 and maximum x.

1.2. **The A-tail of an element.** If M is a monoid and $x, x_p, \dots, x_1$ belong to M, we say that $(x_p, \dots, x_1)$ is a *decomposition* of x if $x = x_p \dots x_1$ holds. The basic observation is that, for each subset A of the monoid M that contains 1 and is closed under left lcm, and every x in M, Lemma 1.5 leads to a distinguished decomposition (x', x_1) of x with $x_1 \in A$.

Lemma 1.6. *Assume that M is a locally right Garside monoid and A is a subset of M that contains 1 and is closed under left lcm. Then, for each element x of M, there exists a unique right divisor x_1 of x that lies in A and is maximal with respect to right divisibility, namely the left lcm of $\mathrm{Div}_R(x) \cap A$.*

Proof. Apply Lemma 1.5 with $X = \mathrm{Div}_R(x) \cap A$. The latter set is nonempty as it contains at least 1, and it is closed under left lcm as it is the intersection of two sets that are closed under left lcm. ☐

Definition 1.7. Under the hypotheses of Lemma 1.6, the element x_1 is called the *A-tail* of x, and denoted $\mathrm{tail}(x, A)$.

Example 1.8. Let M be an Artin–Tits monoid with standard set of generators S. We assume in addition that M is of spherical type, which means that the Coxeter group obtained by adding the relation $s^2 = 1$ for each s in S is finite. Then, Garside's theory shows that any two elements of M admit a common left multiple, hence a left lcm. We shall consider two types of closed subsets of M. The first, standard choice consists in considering the set Σ of so-called simple elements in M, namely the divisors of the lcm Δ of S. By construction, Σ contains 1 and is closed under left (and right) divisor, and under left (and right) lcm. For each x in M, the Σ-tail of x is the right gcd of x and Δ.

A second choice consists in considering $I \subseteq S$, and taking for A the standard parabolic submonoid M_I of M generated by I. The specific form of the Artin–Tits relations implies that M_I is closed under left (and right) divisor, and under left (and right) lcm, hence it is eligible for our approach. Denote by Δ_I the lcm of I. Then, for every element x of M, the M_I-tail x_1 of x is the right gcd of x and $\Delta_I^{|x|}$, where $|x|$ denotes the common length of all words representing x. Indeed, let x_1' be the latter gcd, and let $\ell = |x|$. By definition, x_1 is a right divisor of x, so we have $|x_1| \leqslant \ell$, and, as for each z in M_I satisfying $|z| \leqslant \ell$ is, we have $\Delta_I^\ell \succcurlyeq x_1'$, hence $x_1' \succcurlyeq x_1$. Conversely, x_1' is an element of $\mathrm{Div}_R(x) \cap M_I$, hence we have $x_1 \succcurlyeq x_1'$, and, finally, $x_1 = x_1'$. Note that the previous approach does not require that M be of spherical type, but only that M_I is. Actually, M_I is a closed submonoid even if it is not of spherical type—but, then, the characterization of the M_I-tail in terms of powers of Δ_I vanishes.

1.3. **Alternating decompositions.** In the second case of Example 1.8, the involved subset is a submonoid of M, *i.e.*, in addition to being closed under left lcm, it is closed under multiplication. From now on, we shall concentrate on this situation. Then, the decomposition of Lemma 1.6 takes a specific form.

Definition 1.9. Assume that M is a locally right Garside monoid. We say that a submonoid M_1 of M is *closed* if it is closed under both left lcm and left divisor, *i.e.*, every left lcm of elements of M_1 belongs to M_1 and every left divisor of an element of M_1 belongs to M_1.

Example 1.10. If M is an Artin–Tits monoid with standard set of generators S, then every standard parabolic submonoid of M is closed. This need not be the case in every locally right Garside monoid, or even in every Garside monoid. For instance, the monoid $\langle a, b \mid aba = b^2\rangle^+$ is Garside, hence locally right Garside—the associated Garside group is the braid group B_3. However, the submonoid generated by b is not closed, as it contains b^2, which is aba, but it contains neither a nor ab, which are left divisors of b^2.

Notation 1.11. For M a monoid, $x \in M$ and $A \subseteq M$, we write $x \perp A$ if no non-trivial element of A is a right divisor of x, *i.e.*, if $\mathrm{Div}_R(x) \cap A$ is either $\emptyset$ or $\{1\}$.

Lemma 1.12. *Assume that M is a locally right Garside monoid, and M_1 is a closed submonoid of M. Then, for each x in M, there exists a unique decomposition (x', x_1) of x satisfying*

$$x' \perp M_1 \quad \textit{and} \quad x_1 \in M_1, \tag{1.2}$$

namely the one given by $x_1 = \mathrm{tail}(x, M_1)$ and $x' = x\, x_1^{-1}$.

Proof. Let $x_1 = \mathrm{tail}(x, M_1)$ and $x' = x\, x_1^{-1}$. We claim that, for each decomposition (y', y_1) of x with $y_1 \in M_1$, we have

$$y' \perp M_1 \quad \Longleftrightarrow \quad y_1 = x_1. \tag{1.3}$$

First, assume $z \in \mathrm{Div}_R(x') \cap M_1$. Then we have $x' = x''z$ for some x'', hence $x = x''zx_1$, and $zx_1 \in \mathrm{Div}_R(x)$. As z and x_1 belong to M_1 and the latter is a submonoid of M, we deduce $zx_1 \in M_1$, hence $z = 1$ by definition of x_1. So $x' \perp M_1$ holds, and the $\Longleftarrow$ implication in (1.3) is true.

Conversely, assume $x = y'y_1$ with $y_1 \in M_1$. By definition of the M_1-tail, we have $x_1 = zy_1$ for some z. The assumption that M_1 is closed under left divisor implies

$z \in M_1$. Then we find $y'y_1 = x = x'x_1 = x'zy_1$, hence $y' = x'z$ by cancelling y_1, and finally $z \in \mathrm{Div}_R(y') \cap M_1$. Then $\mathrm{Div}_R(y') \cap M_1 = \{1\}$ implies $z = 1$, *i.e.*, $y_1 = x_1$, and, from there, $y' = x'$. So the $\Longrightarrow$ implication in (1.3) is true. $\square$

By definition, the relation $x' \perp M_1$ of (1.3) is equivalent to $\mathrm{tail}(x', M_1) = 1$. This shows that iterating the decomposition of Lemma 1.12 makes no sense: we extracted the maximal right divisor of x that lies in M_1, so, after that, there remains nothing to extract any longer. But assume that M is locally right Garside, and that M_2, M_1 are *two* closed submonoids of M. For each x in M, Lemma 1.12 gives a distinguished decomposition (x', x_1) of x with x_1 in M_1. If x' is not 1, and if $M_2 \cup M_1$ generates M, the M_2-tail of x' is not 1, and we obtain a new decomposition (x'', x_2, x_1) of x with $x_2 \in M_2$ and $x_1 \in M_1$. If x'' is not 1, we repeat the process with M_1, *etc.* finally obtaining a decomposition of x as an alternating sequence of elements of M_2 and M_1.

Definition 1.13. If M is a locally right Garside monoid, we say that (M_2, M_1) is a *covering* of M if M_2 and M_1 are closed submonoids of M and $M_2 \cup M_1$ generates M (as a monoid).

Example 1.14. Let M be an Artin–Tits monoid with standard set of generators S, and let S_2, S_1 be two subsets of S satisfying $S_2 \cup S_1 = S$. For $k = 2, 1$, let M_k be the standard parabolic submonoid of M generated by S_k. Then (M_2, M_1) is a covering of M. Indeed, we already observed that M_1 and M_2 are closed submonoids of M. Moreover, S is included in $M_2 \cup M_1$, so the latter generates M.

Similar results hold for every locally right Garside monoid that is generated by the union of two sets S_2, S_1 provided we define M_k to be the smallest *closed* submonoid of M generated by S_k.

Notation 1.15. For each (nonnegative) integer r, we define $[r]$ to be 1 if r is odd, and 2 if r is even.

Proposition 1.16. *Assume that M is a locally right Garside monoid and (M_2, M_1) is a covering of M. Then, for every non-trivial element x of M, there exists a unique decomposition $(x_p, \dots, x_1)$ of x satisfying $x_p \neq 1$ and, for each $r \geqslant 1$,*

$$x_p \dots x_{r+1} \perp M_{[r]} \quad \text{and} \quad x_r \in M_{[r]}. \tag{1.4}$$

The elements x_r are determined from $x^{(0)} = x$ by

$$x_r = \mathrm{tail}(x^{(r-1)}, M_{[r]}) \quad \text{and} \quad x^{(r)} = x^{(r-1)}\, x_r^{-1}. \tag{1.5}$$

Moreover, we have $x_r \neq 1$ for $r \geqslant 2$.

Proof. Let x belong to M, and let x_r, $x^{(r)}$ be as specified by (1.5). Using induction on $r \geqslant 1$, we first prove the relations

$$x = x^{(r)} x_r \cdots x_1, \tag{1.6}$$

$$x^{(r)} \perp M_{[r]}. \tag{1.7}$$

For $r = 1$, Lemma 1.12 for x and M_1 gives $x = x^{(1)} x_1$, which is (1.6), and $x^{(1)} \perp M_1$, which is (1.7). Assume $r \geqslant 2$. Then (1.5) implies $x^{(r-1)} = x^{(r)} x_r$, and, susbtituting in $x = x^{(r-1)} x_{r-1} \dots x_1$, which holds by induction hypothesis, we obtain (1.6). Moreover, Lemma 1.12 for $x^{(r)}$ and $M_{[r]}$ gives (1.7).

By construction, the sequence x_1, x_2x_1, $x_3x_2x_1$, ... is increasing in $(\mathrm{Div}_R(x), \prec)$. By Condition (C_3), it is eventually constant. By right cancellability, this implies that there exists p such that $x_r = x^{(r)} = 1$ holds for all $r \geqslant p$. Then (1.6) implies $x = x_p ... x_1$, with $x_p \neq 1$ provided p is chosen to be minimal and x is not 1.

So the expected sequence $(x_p, \ldots, x_1)$ exists and satisfies (1.4) and (1.5). We show now $x_r \neq 1$ for $r \geqslant 2$. Indeed, assume $x^{(r-1)} \neq 1$. By hypothesis, $M_2 \cup M_1$ generates M, implying $x^{(r-1)} \not\perp (M_2 \cup M_1)$. By (1.7), we have $x^{(r-1)} \perp M_{[r-1]}$, hence $x^{(r-1)} \not\perp M_{[r]}$. Therefore the $M_{[r]}$-tail of $x^{(r-1)}$, which by definition is x_r, is not 1—the argument fails for $r = 1$ because $x^{(0)} \perp M_{[0]}$ need not hold.

We turn to uniqueness. Consider any decomposition $(y_q, \ldots, y_1)$ of x satisfying $y_q \neq 1$ with $y_r \in M_{[r]}$ and $y_q ... y_{r+1} \perp M_{[r]}$ for each r. We inductively prove $y_r = x_r$ and $y_q ... y_{r+1} = x^{(r)}$ for $r \geqslant 1$. For $r = 1$, the hypotheses $x = (y_q ... y_2)y_1$ with $y_1 \in M_1$ and $y_q ... y_2 \perp M_1$ imply $y_1 = x_1$ and $y_q ... y_2 = x^{(1)}$ by Lemma 1.12. Assume $r \geqslant 2$. By induction hypothesis, we have $y_q ... y_r = x^{(r-1)}$, and the hypotheses about the elements y_j give $x^{(r-1)} = (y_q ... y_{r+1})y_r$ with $y_r \in M_{[r]}$ and $y_q ... y_{r+1} \perp M_{[r]}$. Then Lemma 1.12 implies $y_r = \mathrm{tail}(x^{(r-1)}, M_{[r]}) = x_r$ and $y_q ... y_{r+1} = x^{(r-1)}\, x_r^{-1} = x^{(r)}$. Finally, $q > p$ would imply $x_q = y_q \neq 1$, contradicting the choice of p. □

Definition 1.17. In the framework of Proposition 1.16, the sequence $(x_p, \ldots, x_1)$ is called the (M_2, M_1)-*decomposition* of x.

Example 1.18. Consider the 4-strand braid monoid B_4^+. Let M_1 be the submonoid generated by σ_1 and σ_2, *i.e.*, B_3^+, and M_2 be the submonoid generated by σ_2 and σ_3. Choose $x = \Delta_4^2 = (\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1)^2$. The computation of the (M_2, M_1)-decomposition of x is as follows:

$$\begin{aligned}
&x^{(0)} = x = \Delta_4^2 && x_1 = \mathrm{tail}(x^{(0)}, M_1) = \Delta_3^2,\\
&x^{(1)} = x^{(0)}\, x_1^{-1} = \sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3 && x_2 = \mathrm{tail}(x^{(1)}, M_2) = \sigma_2\sigma_3,\\
&x^{(2)} = x^{(1)}\, x_2^{-1} = \sigma_3\sigma_2\sigma_1^2 && x_3 = \mathrm{tail}(x^{(2)}, M_1) = \sigma_2\sigma_1^2,\\
&x^{(3)} = x^{(2)}\, x_3^{-1} = \sigma_3 && x_4 = \mathrm{tail}(x^{(3)}, M_2) = \sigma_3,\\
&x^{(4)} = x^{(3)}\, x_4^{-1} = 1. &&
\end{aligned}$$

Thus the (M_2, M_1)-decomposition of Δ_4^2 is the sequence $(\sigma_3, \sigma_2\sigma_1^2, \sigma_2\sigma_3, \Delta_3^2)$—see Figure 1 for an illustration in terms of standard braid diagrams. Note that the decomposition depends on the order of the submonoids: the (M_1, M_2)-decomposition of Δ_4^2 is $(\sigma_1, \sigma_2\sigma_3^2, \sigma_2\sigma_1, (\sigma_2\sigma_3\sigma_2)^2)$.

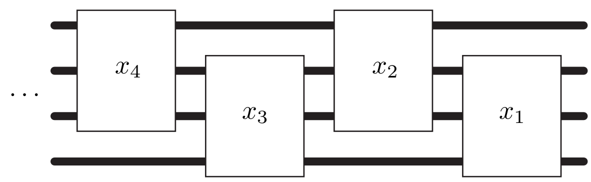


FIGURE 1. Diagram associated with the (M_2, M_1)-decomposition of a 4-braid: starting from the right, we alternatively select the maximal right divisor that does not involve the nth strand and the first strand.

Remark 1.19. In the framework of Proposition 1.16, x_1 is the left lcm of all right divisors of x that lie in M_1. Comparing with the case of the greedy normal form, we might expect that, similarly, x_2x_1 is the left lcm of all right divisors of x of the form y_2y_1 with $y_k \in M_k$, *i.e.*, lying in M_2M_1. This is not the case. Consider Example 1.18 again, and let $x = \sigma_1^e\sigma_2\sigma_1$ with $e \geqslant 1$. Then the (M_2, M_1)-decomposition of x is $(\sigma_1^e, \sigma_2, \sigma_1)$, so x_2x_1 is $\sigma_2\sigma_1$ here. Now, we also have $x = \sigma_2\sigma_1\sigma_2^e$, so σ_2^e, *i.e.*, $\sigma_2^e \cdot 1$, is a right divisor of x that belongs to M_2M_1 and does not divide $\sigma_2\sigma_1$. More generally, we see that the braids σ_i that are right divisors of x cannot be retrieved from the last two elements of the (M_2, M_1)-decomposition of x.

Remark 1.20. Assume that M is a locally right Garside monoid, and (M_2, M_1) is a covering of M. Define an (M_2, M_1)-*sequence* to be any finite sequence $(x_p, \dots, x_1)$ such that x_r belongs to $M_{[r]}$ for each r. Then the (M_2, M_1)-decomposition of x is a certain decomposition of x that is a (M_2, M_1)-sequence. As we take the maximal right divisor at each step, we might expect to obtain a short (M_2, M_1)-sequence, possibly the shortest possible one. We shall see in Section 5 below that this is indeed the case for the covering of Example 1.18. However, this is not the case in general. Indeed, keep the braid monoid B_4^+, but consider the covering (M_2', M_1'), where M_1' (*resp.* M_2') is the submonoid generated by σ_1 and σ_3 (*resp.* by σ_2 and σ_3). Let x be $\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3^2\sigma_2$. The (M_2', M_1')-decomposition of x turns out to be $(\sigma_1, \sigma_2^2, \sigma_3\sigma_1, \sigma_2, \sigma_1)$, a sequence of length 5, but another decomposition of x is the (M_2', M_1')-sequence $(\sigma_3\sigma_2, \sigma_1, \sigma_2\sigma_3^2\sigma_2, 1)$, which has length 4: choosing the maximal right divisor at each step does *not* guarantee that we obtain the shortest sequence.

Finally, it is clear that, instead of considering two closed submonoids M_2, M_1 of M, we could consider any finite family of such submonoids $M_m, \dots, M_1$. Provided the union of all M_j's generates M, we can extend Proposition 1.16 and obtain for every element x of M a distinguished decomposition $(x_p, \dots, x_1)$ such that x_r belongs to $M_{[r]}$ and $x_p...x_{r+1} \perp M_{[r]}$ holds for every r, where $[r]$ now denotes the unique element of $\{1, \dots, m\}$ that equals r mod m. The only difference is that the condition $x_r \neq 1$ for $r \geqslant 2$ has to be relaxed to $x_{r+m-2}...x_r \neq 1$ for $r \geqslant m$, since the conjunction of $x \neq 1$ and $x \perp M_{[r]}$ need not guarantee $x \not\perp M_{[r+1]}$, but only $x \not\perp (M_{[r+m-1]} \cup ... \cup M_{[r+1]})$. Adapting is easy—see [22] for an example.

1.4. **Algorithmic aspects.** Computing the alternating decomposition is easy provided one can efficiently perform right division in the ground monoid. To give a precise statement, we recall from [18] the notion of word norm (or pseudolength) that generalizes the standard notion of word length. In the sequel, for S included in M and w a word on S, we denote by $\overline{w}$ the element of M represented by w.

Definition 1.21. Assume that M is a locally right Garside monoid that satisfies Condition (C_3^+), and S generates M. For w a word on S, we denote by $\|w\|$ the maximal length of a word w' satisfying $\overline{w'} = \overline{w}$.

Condition (C_3^+) is precisely what is needed to guarantee that $\|w\|$ exists for every word w. Indeed, if $\lambda : M \to \mathbb{N}$ witnesses that (C_3^+) is satisfied, then every word w' satisfying $\overline{w'} = \overline{w}$ must satisfy $|w| \leqslant \lambda(\overline{w})$. Conversely, if $\|w\|$ exists for each word w, then the map $w \mapsto \|w\|$ induces a well-defined map of M to $\mathbb{N}$ that witnesses (C_3^+). In the case of Artin–Tits monoids and, more generally, of monoids presented by homogeneous relations, $\|w\|$ coincides with the length $|w|$.

Proposition 1.22. *Assume that M is a locally right Garside monoid, generated by some finite set S, and satisfying Condition (C_3^+) plus:*

($*$) *There exists an algorithm $\mathcal{A}$ that, for w a word on S and s in S, runs in time $O(\|w\|)$, recognizes whether $\overline{w} \succcurlyeq s$ holds and, if so, returns a word representing $\overline{w}\, s^{-1}$.*

Let $S_2, S_1 \subseteq S$ satisfying $S_2 \cup S_1 = S$. Let M_k be the submonoid of M generated by S_k, and suppose that M_2, M_1 are closed. Then there exists a algorithm that, for w a word on S, runs in time $O(\|w\|^2)$ and computes the (M_2, M_1)-decomposition of $\overline{w}$.

Proof. Having listed the elements of S_1 and S_2, and starting with w, we use $\mathcal{A}$ to divide by elements of S_1 until division fails, then we divide by elements of S_2 until division fails, *etc.* We stop when the remainder is 1. If we start with a word w satisfying $\|w\| = \ell$, then the words w_r subsequently occurring represent the elements $x^{(r)}$ of (1.5), which are left divisors of x, and, hence, we have $|w_r| \leqslant \|w_r\| \leqslant \ell$. Moreover, at each step, $\|w_r\|$ decreases by at least 1, so termination occurs after at most $\mathrm{card}(S) \times \ell$ division steps. By hypothesis, the cost of each division step is bounded above by $O(\ell)$, whence a quadratic global upper bound. □

Example 1.23. Let M be an Artin–Tits of spherical type, or, more generally, a Garside monoid, and let S be the set of atoms in M. Then there exist division algorithms running in linear time, *e.g.*, those involving a rational transducer based on the (right) automatic structure [21]. Alternatively, for the specific question of dividing by an atom, the reversing method of [15] is specially convenient.

2. Iterated alternating decompositions

If the submonoids involved in a covering are monogenous, it makes no sense to iterated the alternating decomposition. But, in general, for instance in the case of Example 1.18, the covering submonoids need not be monogenous, and they can in turn be covered by smaller submonoids. In such cases, it is natural to iterate the alternating decomposition using a sequence of nested coverings. This is the idea we develop in this section. The main observation is that the result of the iterated decomposition can be obtained directly, without any iteration.

2.1. **Iterated coverings.** The possibility of iterating the alternating decomposition relies on the following observation:

Lemma 2.1. *Every closed submonoid of a locally right Garside monoid is locally right Garside.*

Proof. Assume that M_1 is a closed submonoid of a locally right Garside monoid M. First, M_1 admits right cancellation as every submonoid of a right cancellative monoid does. Then, if x, y belong to M_1 and admit a common left multiple z in M_1, then z is a common left multiple of x and y in M, so, in M, the left lcm z' of x and y exists. The hypothesis that M_1 is closed under left lcm implies $z' \in M_1$, and, then, z' must be a left lcm for x and y in the sense of M_1. Finally, the right divisibility relation of M_1 is included in the right divisibility relation of M, so a sequence contradicting Condition (C_3) in M_1 would also contradict (C_3) in M. □

Assume that M is a locally right Garside monoid and (M_2, M_1) is a covering of M. By Lemma 2.1, M_2 and M_1 are locally right Garside, and we can repeat the process: assuming that $(M_{k,2}, M_{k,1})$ is a covering of M_k for $k = 2, 1$, every element of M_k admits a $(M_{k,2}, M_{k,1})$-decomposition, and, therefore, every element of M admits a distinguished decomposition in terms of the four monoids M_{22}, M_{21}, M_{12}, and M_{22}—we drop commas in indices.

Example 2.2. As in Example 1.18, consider the 4-strand braid monoid B_4^+, and let M_2, M_1 be the parabolic submonoids respectively generated by σ_3, σ_2, and by σ_2, σ_1. Then let M_{22}, M_{21}, M_{12}, and M_{11} be the submonoids respectively generated by σ_2, σ_3, σ_2, and σ_1. Then (M_{k2}, M_{k1}) is a covering of M_k for $k = 2, 1$.

To make the construction formal, we introduce the notion of an iterated covering.

Definition 2.3. Assume that M is a locally right Garside monoid. By convention, M is a 0-*covering* of itself; for $n \geqslant 1$, an n-*covering* of M is a pair $(\boldsymbol{M}_2, \boldsymbol{M}_1)$ for which there exists a covering (M_2, M_1) of M such that $\boldsymbol{M}_k$ is an $(n-1)$-covering of M_k for $k = 1, 2$.

So a 1-covering of M is just an ordinary covering, and, for instance, a 2-covering of M consists of a covering (M_2, M_1) of M, plus coverings of M_2 and M_1, as in Example 2.2.

An iterated covering of a monoid M has the structure of a binary tree, and we can specify the various submonoids by using finite sequences of twos and ones—or of ones and zeroes, or of letters 'L' and 'R'—to indicate at each forking which direction is to be taken. In the sequel, such a finite sequence of length n is called a *binary n-address*. In this way, an n-covering of a monoid M is a sequence of submonoids M_α indexed by binary addresses of length at most n, such that, for each α of length smaller than n, the pair $(M_{\alpha 2}, M_{\alpha 1})$ is a covering of M_α, and $M_\varnothing$ is M—using $\varnothing$ for the empty address. In the sequel, if $\boldsymbol{M}$ is an iterated covering, we shall always use M_α for the α-entry in $\boldsymbol{M}$.

If the ground monoid M has some distinguished generating set S, we can specify an n-covering by choosing a subset S_α of S for each α in $\{2,1\}^n$, and, for β in $\{2,1\}^n$ with $m \leqslant n$, defining M_β to be the submonoid generated by all S_α's such that β is a prefix of α. We obtain an n-covering provided each submonoid M_β is closed. For such coverings, we can display the inclusions in a binary tree—see Figure 2.

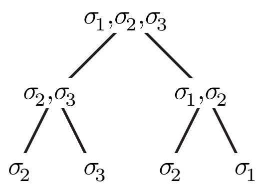


FIGURE 2. Skeleton of the 2-covering of B_4^+ of Example 2.5: a depth 2 binary tree displaying the inclusions between the generating sets of the successive submonoids; this example corresponds to $S_{22} = S_{12} = \{\sigma_2\}$, $S_{21} = \{\sigma_3\}$, and $S_{11} = \{\sigma_1\}$; we find for instance $M_2 = \langle \sigma_2, \sigma_3 \rangle^+$, and $M_{12} = \langle \sigma_2 \rangle^+$.

2.2. **Iterated $\boldsymbol{M}$-decomposition.** As was shown in Section 1, each covering (M_2, M_1) of a monoid M leads to a distinguished decomposition for the elements of M in terms of elements of M_2 and M_1. An iterated covering similarly leads to what can be called an iterated decomposition.

Definition 2.4. Assume that M is a locally right Garside monoid, and $\boldsymbol{M}$ is an n-covering of M. For x in M, we define the $\boldsymbol{M}$-*decomposition* $D_{\boldsymbol{M}}(x)$ of x by

$D_{\boldsymbol{M}}(x) = x$ for $n = 0$, and, for $n \geqslant 1$ and $\boldsymbol{M} = (\boldsymbol{M}_2, \boldsymbol{M}_1)$, by

$$D_{\boldsymbol{M}}(x) = (D_{\boldsymbol{M}_{[p]}}(x_p)\,,\, \dots\,,\, D_{\boldsymbol{M}_1}(x_1)), \tag{2.1}$$

where $(x_p, \dots, x_1)$ is the (M_2, M_1)-decomposition of x.

Example 2.5. Consider the braid Δ_4^2 of B_4^+ and the covering $\boldsymbol{M}$ of Example 2.2. We saw in Example 1.18 that the (M_2, M_1)-decomposition of Δ_4^2 is

$$(\sigma_3, \sigma_2\sigma_1^2, \sigma_2\sigma_3, \Delta_3^2).$$

Now, the (M_{12}, M_{11})-decomposition of Δ_3^2 turns out to be $(\sigma_2, \sigma_1^2, \sigma_2, \sigma_1^2)$. Similarly, the (M_{22}, M_{21})-decomposition of $\sigma_2\sigma_3$ is (σ_2, σ_3). Continuing in this way, we obtain

$$D_{\boldsymbol{M}}(\Delta_4^2) = ((\sigma_3), (\sigma_2, \sigma_1^2), (\sigma_2, \sigma_3), (\sigma_2, \sigma_1^2, \sigma_2, \sigma_1^2)), \tag{2.2}$$

corresponding to the factorization $\Delta_4^2 = (\sigma_3) \cdot (\sigma_2 \cdot \sigma_1^2) \cdot (\sigma_2 \cdot \sigma_3) \cdot (\sigma_2 \cdot \sigma_1^2 \cdot \sigma_2 \cdot \sigma_1^2)$.

For $n \geqslant 2$, the $\boldsymbol{M}$-decomposition of an element is a sequence of sequences. More precisely, it is an *n-sequence*, defined to be a single element for $n = 0$, and to be a sequence of $(n-1)$-sequences for $n \geqslant 1$. Such iterated sequences can naturally be viewed as trees, on the model of Figure 3 (left).

Entries in an ordinary sequence of length p are usually specified using numbers from 1 to p—or rather p to 1 in the context of this paper where we start from the right. Entries in an iterated sequence are then specified using finite sequence of numbers, as done in Section 2.1 with binary addresses. In the sequel, a length n sequence of positive numbers is called an *n-address*: for instance, 32 is a typical 2-address—in examples, we drop brackets and separating commas. If $\boldsymbol{s}$ is an n-sequence, and θ is an m-address with $m \leqslant n$, we denote by $\boldsymbol{s}_\theta$ the θ-subsequence of $\boldsymbol{s}$, *i.e.*, the $(n-m)$-sequence made by those entries in $\boldsymbol{s}$ whose address begins with θ—when it exists, *i.e.*, when the considered sequences are long enough—see Figure 3 (right).

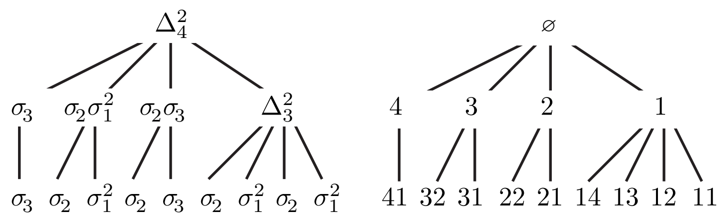


FIGURE 3. The tree associated with the 2-sequence of (2.2): on the left, the braid entries, on the right, the addresses; the entry list specifies the name of the leaves, while the address list specifies the shape of the tree; for each address θ, the θ-subsequence $\boldsymbol{s}_\theta$ corresponds to what lies below θ in $\boldsymbol{s}$; here, the 31-subsequence is σ_1^2, while the 2-subsequence is (σ_2, σ_3). The 23-subsequence does not exist.

Note that addresses are just a way of specifying brackets in an iterated sequence: an n-sequence is determined by its unbracketing—that is, the (ordinary) sequence obtained by removing all inner brackets—and its address list. For instance, in the 2-sequence of (2.2), the unbracketing and the address list are

$$(\sigma_3, \sigma_2, \sigma_1^2, \sigma_2, \sigma_3, \sigma_2, \sigma_1^2, \sigma_2, \sigma_1^2) \quad \text{and} \quad (41, 32, 31, 22, 21, 14, 13, 12, 11). \tag{2.3}$$

Assume that $\boldsymbol{s}$ is the $\boldsymbol{M}$-decomposition of an element x. For each θ that is the address of a node of $\boldsymbol{s}$ (viewed as a tree), write x_θ for the product of the subsequence $\boldsymbol{s}_\theta$. Then, by definition, if θ is the address of an inner node and $\theta p, \dots, \theta 1$ are the addresses of the nodes that lie immediately below θ in $\boldsymbol{s}$, the sequence $(x_{\theta p}, \dots, x_{\theta 1})$ is the $(M_{[\theta]2}, M_{[\theta]1})$-decomposition of x_θ, where $[\theta]$ denotes the binary address obtained by replacing each r ocurring in θ with $[r]$—which is coherent with Notation 1.15. Applying Proposition 1.16 immediately gives the following characterization.

Proposition 2.6. *Assume that M is a locally right Garside monoid, $\boldsymbol{M}$ is an n-covering of M, and $\boldsymbol{s} = D_{\boldsymbol{M}}(x)$. For each address θ in $\boldsymbol{s}$, let x_θ denote the product of $\boldsymbol{s}_\theta$. Assume that θ is the address of an inner node and $\theta p, \dots, \theta 1$ are the addresses of the nodes that lie immediately below θ in $\boldsymbol{s}$. Then, the elements $x_{\theta r}$ are determined from $x_\theta^{(0)} = x_\theta$ by*

$$x_{\theta r} = \mathrm{tail}(x_\theta^{(r-1)}, M_{[\theta r]}) \quad \text{and} \quad x_\theta^{(r)} = x_\theta^{(r-1)}\, x_{\theta r}^{-1}. \tag{2.4}$$

Example 2.7. In the context of Example 2.5 and Figure 3, (2.4) gives

$$x_1 = \sigma_2\sigma_1^2\sigma_2\sigma_1^2 = \mathrm{tail}(x, B_3^+), \quad x_2 = \sigma_2\sigma_3 = \mathrm{tail}(\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3, \langle\sigma_2,\sigma_3\rangle^+), \textit{etc.}$$

which involve the whole of x, but also, at the next level, we have

$$x_{11} = \sigma_1^2 = \mathrm{tail}(\sigma_2\sigma_1^2\sigma_2\sigma_1^2, B_2^+), \quad x_{12} = \sigma_2 = \mathrm{tail}(\sigma_2\sigma_1^2\sigma_2, \langle\sigma_2\rangle^+), \textit{etc.}$$

which only involve the element x_1, namely $\sigma_2\sigma_1^2\sigma_2\sigma_1^2$, and not the whole of x.

2.3. **A transitivity lemma.** Proposition 2.6 looks intricate, and it is not satisfactory in that it does not give a global characterization of the $\boldsymbol{M}$-decomposition and a way to obtain it directly. This is what we shall do now. The point is that, according to the following result, there is no need to consider local remainders when computing iterated tails.

Lemma 2.8. *Assume that M is a locally right Garside monoid, that M_1 is a closed submonoid of M, and that M_{11} is a closed submonoid of M_1. Then, for every z in M and every left divisor y of $\mathrm{tail}(z, M_1)$, we have*

$$\mathrm{tail}((z\,\mathrm{tail}(z, M_1)^{-1})y, M_{11}). = \mathrm{tail}(y, M_{11}). \tag{2.5}$$

Proof. Put $z_1 = \mathrm{tail}(z, M_1)$ and $z' = z\,z_1^{-1}$. By definition, $\mathrm{tail}(y, M_{11})$ is a right divisor of $\mathrm{tail}(z'y, M_{11})$, hence the point is to prove that every right divisor of $z'y$ lying in M_{11} is a right divisor of y. So assume $z'y = x'x$ with $x \in M_{11}$. By hypothesis, we have $z_1 = yz_1'$ for some z_1', necessarily lying in M_1. Then, we have $z = z'z_1 = z'yz_1' = x'xz_1'$. Now $x \in M_{11}$ implies $x \in M_1$, hence $xz_1' \in M_1$, and xz_1' has to be a right divisor of $\mathrm{tail}(z, M_1)$, *i.e.*, of z_1, which is also yz_1'. It follows that x is a right divisor of y, as expected. □

In particular, when we choose y to be z_1 itself, (2.5) gives

$$\mathrm{tail}(z, M_{11}) = \mathrm{tail}(\mathrm{tail}(z, M_1), M_{11}), \tag{2.6}$$

which is vaguely reminiscent of the equality $\mathrm{tail}(zy, \Sigma) = \mathrm{tail}(\mathrm{tail}(z, \Sigma)y, \Sigma)$ that is crucial in the construction of the right greedy normal form in a Garside monoid.

2.4. **Global characterization of the iterated decomposition.** We shall now give a direct description of the $\boldsymbol{M}$-decomposition not involving the intermediate values x_θ. Consider Examples 2.5 and 2.7 again. The problem is as follows: in the case of the 1-covering of B_3^+, only two submonoids are involved, and the final decomposition consists of alternating blocks belonging to each of them; in the case of the 2-covering of B_4^+, the decomposition consists of blocks of σ_1's, σ_2's, and σ_3's, but the order in which these blocks appear is not so simple. Indeed, on the left of a block of σ_2's, there may be either a block of σ_1's or a block of σ_3's, depending on the current address, *i.e.*, on the position in (the skeleton of) the covering, typically on which of the two occurrences of σ_2 in the tree of Figure 2 the considered block of σ_2's is to be associated: on the left of a block of σ_2's associated with the rightmost σ_2 in Figure 2, σ_1 is expected, while σ_3 is expected in the other case. This is what Proposition 2.11 below says, namely that the $\boldsymbol{M}$-decomposition can be obtained directly provided we keep track of some position specified by a binary address.

To make the description precise, we introduce the notion of successors of an address. It comes in two versions, one for general addresses, one for binary addresses.

Definition 2.9. For θ an n-address and $0 \leqslant m \leqslant n$, the *$m$-successor* $\theta^{(m)}$ of θ is the n-address obtained by keeping the first m digits of θ, adding 1 to the next one, and completing with 1's, *i.e.*, for $\theta = d_1...d_n$, the m-successor is $d'_1...d'_n$ with $d'_r = d_r$ for $r \leqslant m$, and, if $m < n$ holds, $d'_{m+1} = d_{m+1} + 1$ and $d'_r = 1$ for $r > m+1$. For α a binary n-address, the *binary m-successor* $\alpha^{[m]}$ of α is defined to be $[\alpha^{(m)}]$.

Example 2.10. Let $\theta = 3612$. The successors of θ are

$$\theta^{(0)} = 4111, \quad \theta^{(1)} = 3711, \quad \theta^{(2)} = 3621, \quad \theta^{(3)} = 3613, \quad \theta^{(4)} = 3612.$$

Similarly, the binary successors of $\alpha = 1212$ are

$$\alpha^{[0]} = 2111, \quad \alpha^{[1]} = 1111, \quad \alpha^{[2]} = 1221, \quad \alpha^{[3]} = 1211, \quad \alpha^{[4]} = 1212.$$

Note that $\theta^{(n)} = \theta$ holds for every n-address θ. We recall that specifying an iterated sequence amounts to specifying both its unbracketing and its address list.

Proposition 2.11. *Assume that M is a locally right Garside monoid, and $\boldsymbol{M}$ is an n-covering of M. Then, for x in M, the unbracketing $(x_p, \ldots, x_1)$ and the address list $(\theta_p, \ldots, \theta_1)$ of $D_{\boldsymbol{M}}(x)$ are inductively determined from $x^{(0)} = x$ and $\theta_1 = 1^n$ by*

$$x_r = \mathrm{tail}(x^{(r-1)}, M_{[\theta_r]}) \ , \quad x^{(r)} = x^{(r-1)}\, x_r^{-1} \ , \quad \text{and} \quad \theta_{r+1} = \theta_r^{(m)}, \tag{2.7}$$

where m is the length of the longest prefix θ of θ_r that satisfies $x^{(r)} \not\perp M_{[\theta]}$.

Proof. As can be expected, we use an induction on n. The argument relies on the transivity relation of Lemma 2.8.

For $n = 0$, everything is trivial, and, for $n = 1$, the result is a restatement of Proposition 1.16: in this case, the 1-address θ_r is r, the longest prefix of θ_r satisfying $x^{(r)} \not\perp M_{[\theta]}$ is $\varnothing$, and the induction rule reduces to $\theta_{r+1} = r + 1$.

Assume $n \geqslant 2$. Let $(y_q, \ldots, y_1)$ be the (M_2, M_1)-decomposition of x. By definition, we have

$$D_{\boldsymbol{M}}(x) = (D_{\boldsymbol{M}_{[q]}}(y_q) \ldots, D_{\boldsymbol{M}_1}(y_1)). \tag{2.8}$$

For $q \geqslant j \geqslant 1$, let $(y_{j,p_j}, \ldots, y_{j,1})$ and $(\theta_{j,p_j}, \ldots, \theta_{j,1})$ be the unbracketing and the address list in $D_{\boldsymbol{M}_{[j]}}(y_j)$. Then, by (2.8), we have

$$(x_p, \ldots, x_1) = (y_{q,p_q}, \ldots, y_{q,1})^\frown \ldots ^\frown (y_{1,p_1}, \ldots, y_{1,1}), \tag{2.9}$$

where $\frown$ denotes concatenation, and, similarly,

$$(\theta_p, \dots, \theta_1) = (q\theta_{q,p_q}, \dots, q\theta_{q,1}) \frown \dots \frown (1\theta_{1,p_1}, \dots, 1\theta_{1,1}). \tag{2.10}$$

By induction hypothesis, the sequences of y_j's and $\theta_{j,k}$'s satisfy the counterpart of (2.7), and we wish to deduce (2.7), *i.e.*, dropping the elements $x^{(r)}$, to prove

$$x_r = \mathrm{tail}(x_p...x_r, M_{\theta_r}) \quad \text{and} \quad \theta_{r+1} = \theta_r^{(m)}$$

where m is the length of the maximal prefix θ of θ_r satisfying $x_p...x_{r+1} \not\perp M_{[\theta]}$. We use induction on $r \geqslant 1$.

Assume that x_r corresponds to some entry $y_{j,k}$ in (2.9). By construction, we have $\theta_r = j\theta_{j,k}$. Let $y = y_{j,p_j}...y_{j,k}$. The induction hypothesis gives

$$x_r = y_{j,k} = \mathrm{tail}(y, M_{[j\theta_{j,k}]}) = \mathrm{tail}(y, M_{[\theta_r]}). \tag{2.11}$$

On the other hand, by construction, y is a left divisor of $y_{j,p_j}...y_{j,1}$, *i.e.*, of y_j, and y_j is the $M_{[j]}$-tail of $y_q...y_j$, *i.e.*, putting $z = y_q...y_j$, we have

$$y_j = \mathrm{tail}(z, M_{[j]}). \tag{2.12}$$

Applying Lemma 2.8 to the monoids $M_{[\theta_r]} \subseteq M_{[j]} \subseteq M$, we deduce from (2.11) and (2.12) the relation $x_r = \mathrm{tail}((z\, y_j^{-1})y, M_{[\theta_r]})$, which is $x_r = \mathrm{tail}(x_p...x_r, M_{[\theta_r]})$, as, by construction, we have $(z\, y_j^{-1})y = x_p...x_r$.

Consider now θ_{r+1}. Two cases are possible, according to whether x_r corresponds to an initial or a non-initial entry in some sequence of y's, *i.e.*, with the above notation, according to whether $k = p_j$ holds or not. Assume first $k < p_j$. Then $\theta_{j,k+1}$ exists, and the induction hypothesis implies that $\theta_{j,k+1}$ is the m-successor of $\theta_{j,k}$, where m is the length of the maximal prefix θ of $\theta_{j,k}$ for which $y_{j,p_j}...y_{j,k+1} \not\perp M_{[j\theta]}$ holds. The latter relation is equivalent to $x_p...x_{r+1} \not\perp M_{[j\theta]}$: indeed, $x \not\perp A$ is equivalent to $\mathrm{tail}(x, A) \neq 1$, and, as above, Lemma 2.8 implies $\mathrm{tail}(x_p...x_{r+1}, M_{[j\theta]}) = \mathrm{tail}(y_{j,p_j}...y_{j,k+1}, M_{[j\theta]})$. Therefore, θ_{r+1}, which is $j\theta_{j,k+1}$, is the $m+1$-successor of $j\theta_{j,k}$, *i.e.*, of θ_r, where m is the length of the maximal prefix θ of $\theta_{j,k}$ for which $x_p...x_{r+1} \not\perp M_{[j\theta]}$ holds, hence $m+1$ is the length of the maximal prefix θ' of θ_r (namely $j\theta$) for which $x_p...x_{r+1} \not\perp M_{[\theta']}$ holds.

Finally, assume $k = p_j$, *i.e.*, $\theta_{j,k}$ is the leftmost address in the $\boldsymbol{M}_{[j]}$-decomposition of y_j. In this case, by hypothesis, we have $\theta_{r+1} = (j+1)1^{n-1}$. Now, the hypothesis implies $y_q...y_{j+1} \perp M_{[j]}$, *i.e.*, $x_p...x_{r+1} \perp M_{[j]}$. So, in this case, the only prefix θ of θ_r, *i.e.*, of $j\theta_{j,p_j}$, for which $x_p...x_{r+1} \not\perp M_{[\theta]}$ may hold is the empty address $\varnothing$, which is the expected relation with $m = 0$. ☐

Example 2.12. Consider the case of B_4^+ and Δ_4^2 again. Proposition 2.11 directly gives the $\boldsymbol{M}$-decomposition of Δ_4^2 as follows. We start with $x = \Delta_4^2$ and $\theta_1 = 11$. Then we compute M_{11}-tail, *i.e.*, here the $\langle\sigma_1\rangle^+$-tail, of $x^{(0)}$, which turns out to be σ_1^2, and call the quotient $x^{(1)}$. Then the address θ_2 is obtained by looking at the maximal prefix θ of θ_1, *i.e.*, of 11, for which $M_{[\theta]} \not\perp x^{(1)}$ holds. In the current case, we have $x^{(1)} \perp M_{11}$ and $x^{(1)} \not\perp M_1$, hence $\theta = 1$, so θ_2 is obtained from 11 by incrementing the second digit, leading to $\theta_2 = 12$, which corresponds to $M_{[\theta_2]} = \langle\sigma_2\rangle^+$. We take the $\langle\sigma_2\rangle^+$-tail of $x^{(1)}$, call the remainder $x^{(2)}$, and iterate. The successive values are displayed in Table 1.

r	$x^{(r)}$	θ_r	$[\theta_r]$	$M_{[\theta_r]}$	x_r
0	$\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$				
1	$\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_1\sigma_2$	11	11	$\langle\sigma_1\rangle^+$	σ_1^2
2	$\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_1$	12	12	$\langle\sigma_2\rangle^+$	σ_2
3	$\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3$	13	11	$\langle\sigma_1\rangle^+$	σ_1^2
4	$\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3$	14	12	$\langle\sigma_2\rangle^+$	σ_2
5	$\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2$	21	21	$\langle\sigma_3\rangle^+$	σ_3
6	$\sigma_3\sigma_2\sigma_1\sigma_1$	22	22	$\langle\sigma_2\rangle^+$	σ_2
7	$\sigma_3\sigma_2$	31	11	$\langle\sigma_1\rangle^+$	σ_1^2
8	σ_3	32	12	$\langle\sigma_2\rangle^+$	σ_2
9	1	41	21	$\langle\sigma_3\rangle^+$	σ_3

TABLE 1. Direct determination of the iterated decomposition of Δ_4^2: at step r, we extract the maximal right divisor x_r of the current remainder $x^{(r-1)}$ that lies in the monoid $M_{[\theta_r]}$, we update the remainder into $x^{(r)}$, and we define the next address θ_{r+1} to be the maximal successor θ of θ_r for which $x^{(r)}$ is not orthogonal to $M_{[\theta]}$; we stop when only 1 is left.

3. The alternating normal form

We shall now deduce normal form results in (good) locally Garside monoids. The initial remark is that, if M is a locally Garside monoid generated by an element g, then M must be torsion-free by Condition (C_3) of Definition 1.2, hence it is a free monoid, and every element of M admits a unique expression as g^e with $e \in \mathbb{N}$. Now, if M is an arbitrary locally right Garside monoid and if $\boldsymbol{M}$ is an (iterated) covering of M, then each element of x has been given a distinguished decomposition in terms of the factor monoids M_α of $\boldsymbol{M}$. If, moreover, each of the monoids M_α happens to be generated by a single element g_α, the $\boldsymbol{M}$-decomposition gives a unique distinguished expression in terms of the elements g_α. This situation occurs for instance in the case of the 2-covering of Example 2.2.

3.1. **Atomic coverings.** From now on, we consider locally right Garside monoids that satisfy Condition (C_3^+) of Section 1.1. It is easily seen that such monoids are generated by atoms, *i.e.*, elements g such that $g = xy$ implies $x = 1$ or $y = 1$—see for instance [18]. In view of the above remarks, it is natural to concentrate on coverings that involve submonoids generated by atoms.

Definition 3.1. Assume that M is a locally right Garside monoid, and $\boldsymbol{g}$ is an n-sequence of atoms of M. We say that an n-covering of M is *atomic* based on the sequence $\boldsymbol{g}$ if, for each n-address α, the monoid M_α is the submonoid of M generated by the atom g_α.

For instance, the 2-covering of Example 2.2 is atomic, based on $((\sigma_2, \sigma_3), (\sigma_2, \sigma_1))$. Note that a base sequence must contain all atoms of M, as, by definition, it generates M. An arbitrary sequence of atoms need not always define a covering, as a submonoid generated by a family of atoms is not necessarily closed in the sense of Definition 1.9. This however is true in braid monoids—and in all Artin–Tits monoids.

Before going on and defining the $\boldsymbol{M}$-normal form, we discuss one more general point, namely whether $\boldsymbol{M}$-decompositions may have gaps, this meaning that a trivial factor 1 may appear between two non-trivial factors.

Example 3.2. Let M be the 5-strand braid monoid B_5^+, and $\boldsymbol{M}$ be the 2-covering based on $((\sigma_4, \sigma_3), (\sigma_2, \sigma_1))$. One easily checks that the $\boldsymbol{M}$-decomposition of x is $((\sigma_4, 1), (\sigma_1))$, which has a trivial entry lying between two non-trivial entries.

It is easy to state conditions that exclude such gaps.

Definition 3.3. We say that an n-covering $\boldsymbol{M}$ is *dense* if, for each binary address β of length m with $0 \leqslant m < n$,

(3.1) $\qquad M_\beta$ is generated by $M_{\beta 1}$ and $M_{\beta 21^{n-m-1}}$, and by $M_{\beta 2}$ and $M_{\beta 1^{n-m}}$.

Lemma 3.4. *Decompositions associated with a dense covering have no gap.*

Proof. Owing to Proposition 2.11, the point is to prove that, if, for some binary n-address α and some m, writing β (*resp.* β') for the length m (*resp.* $m+1$) prefix of α, we have both $x \not\perp M_\beta$ and $x \perp M_{\beta'}$, then necessarily the $M_{\alpha^{[m]}}$-tail of x is not trivial. Write $\beta' = \beta r$. For $r = 1$, a sufficient condition for the previous implication is that M_β is generated by $M_{\beta 1}$ and $M_{\beta 21^{n-m-1}}$: then, a non-trivial right divisor of x lying in M_β cannot be right divisible by any factor in $M_{\beta 1}$ and, therefore, it must be right divisible by some factor in $M_{\beta 21^{n-m-1}}$, and, by definition, we have $\beta 21^{n-m-1} = \alpha^{[m]}$. For $r = 2$, the argument is similar, replacing $\beta 1$ with β, and $\beta 21^{n-m-1}$ with $\beta 1^{n-m}$. So, the conditions in (3.1) are sufficient. ☐

In the case of an atomic covering, the density condition of Definition 3.3 requires that the base sequence be highly redundant. Such conditions are important in practice because they strongly limit the patterns that can be used in the construction of dense atomic coverings.

Proposition 3.5. *Assume that $\boldsymbol{M}$ is a dense atomic n-covering of M based on $\boldsymbol{g}$. Then, for each n-address α, the set $\{g_{\alpha^{[m]}} \mid 0 \leqslant m \leqslant n\}$ is the atom set of M, and the latter contains at most $n+1$ elements.*

Proof. Use induction on $n \geqslant 0$. The case $n = 0$ is obvious. Assume $n \geqslant 1$. Write $\alpha = d\beta$ with $d = 1$ or 2. Assume first $d = 1$. By (3.1), M is generated by $g_{21^{n-1}}$, which is the 0-successor of α, and M_1. By induction hypothesis, the latter is generated by the family of all $g_{1\beta^{[m]}}$'s, so M is generated by the successors of α. The argument is symmetric for $d = 2$, using the second part of (3.1). By construction, every n-address admits $n+1$ successors, hence there are at most $n+1$ atoms in M. ☐

We shall see in Section 4 that dense atomic n-coverings involving $n+1$ atoms exist for each n. For $n = 2$, the only possible pattern is (up to renaming) that of Figure 2. For $n \geqslant 3$, several non-isomorphic patterns exist—see Figure 4.

3.2. **The $\boldsymbol{M}$-normal form.** We are now ready to convert the results of Sections 2 into the construction of a normal form. We recall that, for S generating M and w a word on S, we denote by $\overline{w}$ the element of M represented by w. We write $w(k)$ for the kth letter in w *from the right.*

Definition 3.6. Assume that M is a locally right Garside monoid with atom set S, and that $\boldsymbol{M}$ is a dense atomic n-covering of M based on $\boldsymbol{g}$. A length ℓ word w on S is said to be $\boldsymbol{M}$-*normal* if

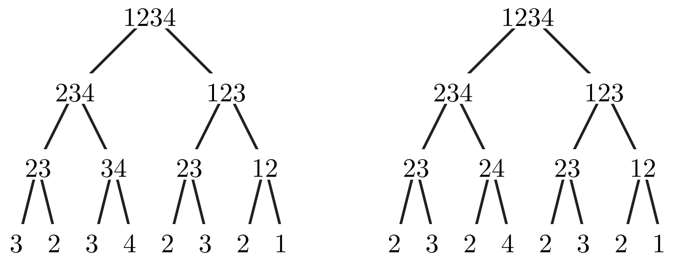


FIGURE 4. The two possible patterns for a dense 3-covering involving four atoms.

> There exist n-addresses $\alpha_\ell, \dots, \alpha_0$ with $\alpha_0 = 1^n$ such that, for each k, $w(k) = g_{\alpha_k}$ holds, where α_k is the maximal successor of α_{k-1}—*i.e.*, is $\alpha_{k-1}^{[m]}$ with maximal m—for which g_{α_k} is a right divisor of $\overline{w(\ell)...w(k)}$.

The above definition may look convoluted, but handling a few examples should make it easily understandable. Table 3 shows that our favourite example, namely $\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$, is $\boldsymbol{M}$-normal with respect to the 2-covering of Example 2.2.

The expected existence and uniqueness of the $\boldsymbol{M}$-normal form is the following easy result.

Proposition 3.7. *Assume that M is a locally right Garside monoid with atom set S, and $\boldsymbol{M}$ is a dense atomic n-covering of M based on $\boldsymbol{g}$. Then each element x of M admits a unique $\boldsymbol{M}$-normal representative, namely $g_{\alpha_\ell} ... g_{\alpha_1}$, where $\alpha_\ell, \dots, \alpha_1$ are inductively determined from $x^{(0)} = x$ and $\alpha_0 = 1^n$ by*

$$\alpha_k = \alpha_{k-1}^{[m]} \quad \textit{and} \quad x^{(k)} = x^{(k-1)}\, g_{\alpha_k}^{-1}, \tag{3.2}$$

where m is maximal such that $g_{\alpha_{k-1}^{[m]}}$ is a right divisor of $x^{(k)}$. Moreover, $g_{\alpha_\ell} ... g_{\alpha_1}$ is the word obtained from the $\boldsymbol{M}$-decomposition of x by concatenating the entries and possibly deleting the final 1.

Proof. The existence follows from the assumption that $\boldsymbol{M}$ is dense, which guarantees that, as long as the remainder $x^{(k)}$ is not trivial, there must exist a successor $\alpha_{k-1}^{[m]}$ of the address α_{k-1} such that $g_{\alpha_{k-1}^{[m]}}$ is a right divisor of $x^{(k)}$. Uniqueness follows from the choice of that successor.

The inductive construction of (3.2) is essentially the construction of the $\boldsymbol{M}$-decomposition as given in Proposition 2.11. The only difference is that, here, we do not extract the whole tail of the current remainder, but only one letter at each step. For instance, if, at some point, the generator to be looked for is g and the current remainder $x^{(k-1)}$ is divisible by g^2, then $x^{(k)}$ is $x^{(k-1)}\, g^{-1}$, and, at the next step, α_k is the n-successor of α_{k-1}, *i.e.*, it is α_{k-1} again, and the next letter of the normal form is g again. In such a case, we have $m = n$. By contrast, in Proposition 2.11, the parameter m is never n. $\square$

Under the hypotheses of Proposition 3.7, the word w is called the *$\boldsymbol{M}$-normal form* of x. The construction described in Proposition 3.7 is an algorithm, displayed in Table 2. A typical example is given in Table 3.

Input: A word w on S;

Procedure:

$w' :=$ `emptyword`;
$\alpha := 1^n$;
`while` $w \neq$ `emptyword do`
  $m := n$;
  `while quotient`$(w, g_{\alpha^{[m]}})$ `= error do`
    $m := m - 1$;
  `od`;
  $\alpha := \alpha^{[m]}$;
  $w :=$ `quotient`(w, g_α);
  $w' :=$ `concat`(g_α, w');
`od`.

Output: The unique $\boldsymbol{M}$-normal word w' that is equivalent to w.

TABLE 2. Algorithm for the $\boldsymbol{M}$-normal form; we assume that S is the atom set of M, and $\boldsymbol{M}$ is a dense atomic n-covering of M based on $\boldsymbol{g}$; moreover, we assume that `quotient`(w, g) is a subroutine that, for w a word on S and g in S, returns `error` if g is not a right divisor of $\overline{w}$, and returns a word representing $\overline{w}\, g^{-1}$ otherwise.

As for complexity, computing the $\boldsymbol{M}$-normal form is as easy as computing the $\boldsymbol{M}$-decomposition. In our current atomic context, the existence of the norm (Definition 1.21) is guaranteed [18].

Proposition 3.8. *Assume that M is a locally right Garside monoid with atom set S, that $\boldsymbol{M}$ is a dense atomic n-covering of M based on $\boldsymbol{g}$, and that Condition* $(*)$ *of Proposition 1.22 is satisfied. Then, for each word w on S, the algorithm of Table 2 runs in time $O(\|w\|^2)$.*

Proof. The only change with respect to Proposition 1.22 is that we have to keep track of binary addresses of fixed length n so as to know in which order the divisions have to be tried. Getting a new letter of the normal word under construction requires at most $n+1$ divisions, but the rest is similar. ☐

3.3. **The exponent sequence.** We conclude this section with an easy remark about $\boldsymbol{M}$-decompositions in the context of atomic coverings, namely that an element of the monoid is non-ambiguously determined by the iterated sequence of exponents in its $\boldsymbol{M}$-decomposition, *i.e.*, we can forget about names of atoms and only keep track of exponents without losing information.

Definition 3.9. For $M, \boldsymbol{M}$ as in Definition 3.6, and for $\boldsymbol{s}$ an iterated sequence whose entries are of the form $g_\alpha^{e_\alpha}$, we define the *exponent sequence* $\boldsymbol{s}^*$ of $\boldsymbol{s}$ to be the iterated sequence obtained by replacing $g_\alpha^{e_\alpha}$ with e_α everywhere in $\boldsymbol{s}$.

For instance, in the context of Example 2.5, the $\boldsymbol{M}$-decomposition of Δ_4^2 is the 2-sequence $((\sigma_3), (\sigma_2, \sigma_1^2), (\sigma_2, \sigma_3), (\sigma_2, \sigma_1^2, \sigma_2, \sigma_1^2))$, so the exponent sequence is the 2-sequence of natural numbers

$$((1), (1, 2), (1, 1), (1, 2, 1, 2)).$$

k	w_k	w'_k	α_{k-1}	m	$\alpha_{k-1}^{[m]}$	$g_{\alpha_{k-1}^{[m]}}$	$\overline{w_k} \succcurlyeq g_{\alpha_{k-1}^{[m]}}$?
0	$\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$	-	11	2	11	σ_1	yes
1	$\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2$	σ_1	11	2	11	σ_1	yes
2	$\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_1\sigma_2$	$\sigma_1\sigma_1$	11	2	11	σ_1	no
				1	12	σ_2	yes
3	$\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_1$	$\sigma_2\sigma_1\sigma_1$	12	2	12	σ_2	no
				1	11	σ_1	yes
4	$\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3$	$\sigma_1\sigma_2\sigma_1\sigma_1$	11	2	11	σ_1	yes
5	$\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3$	$\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	11	2	11	σ_1	no
				1	12	σ_2	yes
6	$\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3$	$\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	12	2	12	σ_2	no
				1	11	σ_1	no
				0	21	σ_3	yes
7	$\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2$	$\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	21	2	21	σ_3	no
				1	22	σ_2	yes
8	$\sigma_3\sigma_2\sigma_1\sigma_1$	$\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	22	2	22	σ_2	no
				1	21	σ_3	no
				0	11	σ_1	yes
9	$\sigma_3\sigma_2\sigma_1$	$\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	11	2	11	σ_1	yes
10	$\sigma_3\sigma_2$	$\sigma_1\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	11	2	11	σ_1	no
				1	12	σ_2	yes
11	σ_3	$\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	12	2	12	σ_2	no
				1	11	σ_1	no
				0	21	σ_3	yes
12	-	$\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	21	-	-	-	

TABLE 3. Computation of the $\boldsymbol{M}$-normal form of Δ_4^2, for $\boldsymbol{M}$ the 2-covering of Example 2.5, starting from the word $(\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1)^2$: at each step, we try to divide the current word w_k by some generator σ_r and, when succesful, we add this σ_r on the left of w'_k, until no letter is left in w_k; the point is to know in which order the generators are tried, and this is specified by the address α_k: we try the successors of α_{k-1} starting with the last one, *i.e.*, with α_{k-1}, and then consider shorter and shorter prefixes of α_{k-1}; density guarantees that we cannot get stuck until w_k is empty.

As in the case of every iterated sequence, specifying the exponent sequence of $D_{\boldsymbol{M}}(x)$ amounts to giving two ordinary sequences, namely its unbracketing—in the above example $(1, 1, 2, 1, 1, 1, 2, 1, 2)$—and its address list—$(41, 32, 31, 22, 21, 14, 13, 12, 11)$ above. Easy examples show that, taken separately, neither of the above sequences is sufficient to recover x. But, when we take them simultaneously, we can recover x.

Proposition 3.10. *If $\boldsymbol{M}$ is an atomic n-covering of M, then, for every x in M, the exponent sequence of $D_{\boldsymbol{M}}(x)$ determines x.*

Proof. Let $\boldsymbol{g}$ be the base sequence of $\boldsymbol{M}$, and let $(e_p, \dots, e_1)$ and $(\theta_p, \dots, \theta_1)$ be the unbracketing and the address list in the exponent sequence of $D_{\boldsymbol{M}}(x)$. Then we recover $D_{\boldsymbol{M}}(x)$ itself, and therefore x, by replacing for each r the entry e_r

corresponding to an address θ_r with $g_{[\theta_r]}^{e_r}$. The formal proof is an easy induction on the degree of the covering $\boldsymbol{M}$—see Figure 5 for an example. □

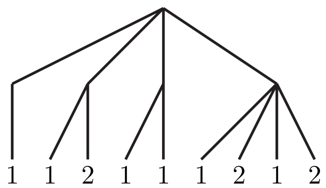


FIGURE 5. Tree representation of the exponent sequence of $D_{\boldsymbol{M}}(\Delta_4^2)$, *i.e.*, of $((1),(1,2),(1,1),(1,2,1,2))$; Proposition 3.10 states that the geometry of the tree determines the missing names: for instance, the leftmost 2 has address 31 in the tree, so it corresponds to the generator $g_{[31]}$, which is σ_1; hence, this entry 2 must correspond to a factor σ_1^2 in $D_{\boldsymbol{M}}(\Delta_4^2)$.

4. The Φ-normal form of braids

From now on, we concentrate on the specific case of braids. In order to apply the previous results, we fix for each n a covering of B_n^+ by two copies of B_{n-1}^+, namely B_{n-1}^+ and its image under the flip automorphism Φ_n. We study the decomposition associated with this covering, as well as an iterated version and the derived normal form, called the Φ-normal form. This naturally leads to introducing a certain linear order of B_n^+, which will be subsequently proved to be connected with the standard braid order.

4.1. **The Φ-splitting of a braid.** In the sequel, we always consider B_{n-1}^+ as a submonoid of B_n^+: an $(n-1)$-strand braid is a special n-strand braid. We denote by Φ_n the flip automorphism of B_n^+ that exchanges σ_i and σ_{n-i} for each i. It is well-known—see for instance [16, Chapter 1]—that Φ_n is the conjugation by the Garside element Δ_n. We also use Φ_n for n-strand braid words, thus denoting by $\Phi_n(w)$ the image of a braid word w under Φ_n letter by letter.

The initial, obvious observation is that, for each $n \geqslant 3$, the monoids B_{n-1}^+ and $\Phi_n(B_{n-1}^+)$ are closed submonoids of B_n^+, and that the pair $(\Phi_n(B_{n-1}^+), B_{n-1}^+)$ is a covering of B_n^+ in the sense of Definition 1.13. Thus Proposition 1.16 gives for every n-strand braid a distinguished decomposition as an alternating product of elements of B_{n-1}^+ and $\Phi_n(B_{n-1}^+)$, according to the scheme of Figure 1. We now restate the general result so as to emphasize the rôle of the flip automorphism.

Proposition 4.1. *Every braid x in B_n^+ admits a unique decomposition*

$$x = \Phi_n^{p-1}(x_p) \cdot \ldots \cdot \Phi_n(x_2) \cdot x_1 \tag{4.1}$$

with $x_1, \ldots, x_p$ in B_{n-1}^+ such that, for each $r \geqslant 2$, the only σ_i that is a right divisor of $\Phi_n^{p-r}(x_p) \cdot \ldots \cdot \Phi_n(x_{r+1}) \cdot x_r$ is σ_1. The braids x_r are determined from $x^{(0)} = x$ by

$$x_r = \mathrm{tail}(x^{(r-1)}, B_{n-1}^+), \quad x^{(r)} = \Phi_n(x^{(r-1)}\, x_r^{-1}). \tag{4.2}$$

Proof. As Φ_n is an automorphism of B_n^+, the relation $y_1 = \mathrm{tail}(y, \Phi_n(B_{n-1}^+))$ is equivalent to $\Phi_n(y_1) = \mathrm{tail}(\Phi_n(y), B_{n-1}^+)$. Moreover Φ_n is an automorphism for the quotient operation as well. Then (4.1) and the divisibility constraints just express that the sequence $(\Phi_n^{p-1}(x_p), \dots, \Phi_n(x_2), x_1)$ is the $(\Phi_n(B_{n-1}^+), B_{n-1}^+)$-decomposition of x. $\square$

Definition 4.2. The sequence $(x_p, \dots, x_1)$ involved in (4.1) is called the *n-splitting* of x; the parameter p is called the *n-breadth of x*.

The only difference between the $(\Phi_n(B_{n-1}^+), B_{n-1}^+)$-decomposition and the n-splitting is that the flip Φ_n is applied to each other entry. The benefit is that all entries in the n-splitting of a braid of B_n^+ are braids of B_{n-1}^+, and not elements of B_{n-1}^+ and $\Phi_n(B_{n-1}^+)$, alternately. Note that the n-splitting of x is obtained by repeating a single operation, namely finding the B_{n-1}^+-tail of x—hence the right gcd of x and Δ_{n-1}^∞ as was seen in Example 1.8—and flipping the quotient.

Example 4.3. Let x be the 4-strand braid Δ_4^2. The B_3^+-tail of x is Δ_3^2, with associated quotient $\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3$, hence, after a flip, $x^{(1)} = \sigma_1\sigma_2\sigma_3^2\sigma_2\sigma_1$. The B_3^+-tail of $x^{(1)}$ is $\sigma_2\sigma_1$, with quotient $\sigma_1\sigma_2\sigma_3^2$, hence, after a flip, $x^{(2)} = \sigma_3\sigma_2\sigma_1^2$. The B_3^+-tail of $x^{(2)}$ is $\sigma_2\sigma_1^2$, with quotient σ_3, hence, after a flip, $x^{(3)} = \sigma_1$, which belongs to B_3^+. Thus Δ_4^2 has 4-breadth 4, and its 4-splitting is $(\sigma_1, \sigma_2\sigma_1^2, \sigma_2\sigma_1, \Delta_3^2)$—compare with the $(\Phi_4(B_3^+), B_3^+)$-decomposition of Δ_4^2 as computed in Example 1.18.

Note that, as in the case of the $(\Phi_n(B_{n-1}^+), B_{n-1}^+)$-decomposition, the non-final entries in an n-splitting are never 1, but the final (rightmost) entry may: the 3-splitting of σ_2 is $(\sigma_1, 1)$, as σ_2 is not divisible by σ_1.

4.2. **The flip covering of B_n^+.** The n-splitting operation associates with every braid of B_n^+ a sequence of braids of B_{n-1}^+. We can now iterate the construction, so as to associate with every braid of B_n^+ an iterated sequence of braids of B_2^+. According to the general framework of Section 2, this entails introducing an iterated $(n-2)$-covering of the monoid B_n^+.

Definition 4.4. For $n \geqslant 2$, we denote $\boldsymbol{B}_n^+$ the $(n-2)$-covering of B_n^+ defined by

$$\boldsymbol{B}_2^+ = B_2^+, \quad \boldsymbol{B}_n^+ = (\Phi_n(\boldsymbol{B}_{n-1}^+), \boldsymbol{B}_{n-1}^+). \tag{4.3}$$

Applying the recursive definition, we find

$$\boldsymbol{B}_3^+ = (\Phi_3(B_2^+), B_2^+) = (\langle\sigma_2\rangle^+, \langle\sigma_1\rangle^+),$$
$$\boldsymbol{B}_4^+ = (\Phi_4(\boldsymbol{B}_3^+), \boldsymbol{B}_3^+) = ((\langle\sigma_2\rangle^+, \langle\sigma_3\rangle^+), (\langle\sigma_2\rangle^+, \langle\sigma_1\rangle^+)),$$

which is the 2-covering of Example 2.2. More generally, writing $B_{n,\alpha}^+$ for the α-entry in $\boldsymbol{B}_n^+$, we deduce from (4.3) the rules

$$B_{2,\varnothing}^+ = B_2^+, \quad B_{n,1\alpha}^+ = B_{n-1,\alpha}^+, \quad \text{and} \quad B_{n,2\alpha}^+ = \Phi_n(B_{n-1,\alpha}^+). \tag{4.4}$$

The above values show that $\boldsymbol{B}_3^+$ and $\boldsymbol{B}_4^+$ are dense atomic coverings. This result extends to all values of n, with the following description of the base sequence.

Proposition 4.5. *For $n \geqslant 2$, define the $(n-2)$-sequence $\boldsymbol{g}_n$ by*

$$\boldsymbol{g}_2 = \sigma_1, \quad \boldsymbol{g}_n = (\Phi_n(\boldsymbol{g}_{n-1}), \boldsymbol{g}_{n-1}). \tag{4.5}$$

Then, for each binary address α of length $n-2$, we have $g_\alpha = \sigma_i$ with

$$i = -m_1 + m_2 - ... + (-1)^r m_r + \begin{cases} 1 & \text{if } r \text{ is even,} \\ n & \text{if } r \text{ is odd,} \end{cases} \tag{4.6}$$

if $\alpha = d_1...d_{n-2}$ and $m_1 < ... < m_r$ are the m's for which d_m is even. Moreover, $\boldsymbol{B}_n^+$ is a dense atomic covering based on $\boldsymbol{g}_n$.

Proof. Firstly, we prove (4.6) using induction on $n \geqslant 2$. For $n = 2$, (4.6) reduces to $g_\varnothing = \sigma_1$, which is true. Assume $n \geqslant 3$, and let $\alpha' = d_2...d_{n-2}$. Putting $g_{\alpha'} = \sigma_{i'}$, we aim at proving $i = i'$ if d_1 is odd, and $i = n - i'$ if d_1 is even. Write S for $-m_1 + m_2 - ... + (-1)^r m_r$, and r', m'_1, m'_2, ..., S', n' for the similar parameters associated with α'. Assume first that d_1 is odd. Then we have $r = r'$, and $m_j = m'_j + 1$ for each j, hence $S = S'$ if r is odd, and $S = S' - 1$ if r is even. The induction hypothesis gives $i' = S' + 1$ if r is odd, $S' + n'$ if r is even. We deduce $i = S + 1 = S' + 1 = i'$ if r is even, and $i = S + n = S' - 1 + n' + 1 = i'$ if r is odd.

Assume now that d_1 is even. Then we have $r = r' + 1$, $m_1 = 1$, and $m_{j+1} = m'_j + 1$ for each $j \geqslant 1$, hence $S = -S'$ if r is odd, and $S = -S' - 1$ if r is even. The induction hypothesis gives $i' = S' + n'$ if r is odd, $S' + 1$ if r is even. We deduce $i = S + 1 = -S' + 1 = n - i'$ if r is odd, and $i = S + n = -S' - 1 + n = n - i'$ if r is even.

Nex, the braids σ_i are the atoms of B_n^+, and every parabolic submonoid of B_n^+ is closed, so every surjective sequence of atoms defines a covering. An obvious induction on n shows that, for $n \geqslant 2$, each of $\sigma_1, ..., \sigma_{n-1}$ occurs in the sequence $\boldsymbol{g}_n$. Moreover, comparing (4.3) and (4.5) makes it straightforward that $\boldsymbol{B}_n^+$ is precisely the covering based on $\boldsymbol{g}_n$.

As for density, the point is to show that B_n^+ is generated by B_{n-1}^+ and $B_{n,21^{n-3}}^+$. Now (4.6) gives $g_{21^{n-3}} = \sigma_{n-1}$, precisely the atom of B_n^+ missing in B_{n-1}^+. ☐

It is easy to see that, for each n, the unbracketing of $\boldsymbol{g}_n$ is the length 2^{n-2} suffix of some left infinite sequence $\boldsymbol{g}_\infty$ where indices are

$$..., 6, 3, 4, 3, 2, 4, 3, 4, 5, 3, 2, 3, 4, 2, 3, 2, 1.$$

An example of application for the rule of (4.6) is as follows: in the length 7 address 1221212, there are even digits at positions $2, 3, 5, 7$ (from the left), so (4.6) gives $i = (-2 + 3 - 5 + 7) + 1 = 4$, hence $g_{1221212} = \sigma_4$.

As $\boldsymbol{B}_n^+$ is a dense atomic covering of B_n^+, it is eligible for the results of Section 2. We fix some specific, simplified notation.

Notation 4.6. For x in B_n^+, the $\boldsymbol{B}_n^+$-decomposition of x is denoted by $D_n(x)$, and its exponent sequence is denoted by $D_n^*(x)$.

The recursive definition of $\boldsymbol{B}_n^+$ implies the following connection between the splitting and the $\boldsymbol{B}_n^+$-decomposition.

Lemma 4.7. *For $n \geqslant 3$ and x in B_n^+, we have*

$$D_n(x) = (\Phi_n^{p-1}(D_{n-1}(x_p)), ..., \Phi_n(D_{n-1}(x_2)), D_{n-1}(x_1)). \tag{4.7}$$

where $(x_p, ..., x_1)$ is the n-splitting of x.

Proof. By definition, the $(\Phi_n(B_{n-1}^+), B_{n-1}^+)$-decomposition of x is the sequence

$$(\Phi_n^{p-1}(x_p), ..., \Phi_n(x_2), x_1),$$

and, therefore, by definition again, we have

$$D_n(x) = (D_{\Phi_n^{p-1}(\boldsymbol{B}_{n-1}^+)}(\Phi_n^{p-1}(x_p)), \dots, D_{\Phi_n(\boldsymbol{B}_{n-1}^+)}(\Phi_n(x_2)), D_{\boldsymbol{B}_{n-1}^+}(x_1)).$$

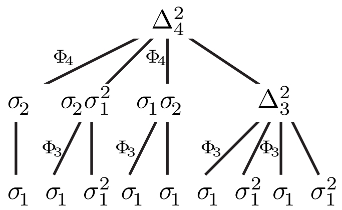
Now, as Φ_n is an automorphism of B_n^+, we have $D_{\Phi_n(\boldsymbol{B}_{n-1}^+)}(\Phi_n(y)) = \Phi_n(D_{\boldsymbol{B}_{n-1}^+}(y))$ for each y in B_{n-1}^+, *i.e.*, $D_{\Phi_n(\boldsymbol{B}_{n-1}^+)}(\Phi_n(y)) = \Phi_n(D_{n-1}(y))$, and (4.7) follows. $\square$

Example 4.8. (See Figure 6) We saw in Example 4.3 that the 4-splitting of Δ_4^2 is $(\sigma_1, \sigma_2\sigma_1^2, \sigma_2\sigma_1, \Delta_3^2)$. Now, the 3-splitting of Δ_3^2 turns out to be $(\sigma_1, \sigma_1^2, \sigma_1, \sigma_1^2)$, that of $\sigma_2\sigma_1$ is (σ_1, σ_1), etc. Gathering the results, and applying the needed flips, we find

$$D_4(\Delta_4^2) = ((\sigma_3), (\sigma_2, \sigma_1^2), (\sigma_2, \sigma_3), (\sigma_2, \sigma_1^2, \sigma_2, \sigma_1^2)), \tag{4.8}$$

as already seen in Example 2.5. The associated exponent sequence is

$$D_4^*(\Delta_4^2) = ((1), (1, 2), (1, 1), (1, 2, 1, 2)), \tag{4.9}$$



i.e., after reintroducing the flips,

$$\sigma_3 \;\; \sigma_2 \;\; \sigma_1^2 \;\; \sigma_2 \;\; \sigma_3 \;\; \sigma_2 \;\; \sigma_1^2 \;\; \sigma_2 \;\; \sigma_1^2$$

FIGURE 6. The $\boldsymbol{B}_4^+$-decomposition of Δ_4^2 viewed as an iterated splitting: we split the initial braid of B_4^+ into a sequence of braids in B_3^+, then we split each of them into a sequence of braids in B_2^+, *i.e.*, of powers of σ_1; the sequence $D_4(\Delta_4^2)$ is obtained by iteratively flipping each other entry.

4.3. **The Φ-normal form.** The iterated covering $\boldsymbol{B}_n^+$ is atomic and, therefore, it gives raise to a unique normal form on B_n^+. According to Proposition 3.7, the $\boldsymbol{B}_n^+$-normal form of a braid x of B_n^+ is the word obtained by concatenating the (unique) expressions of the successive entries in its $\boldsymbol{B}_n^+$-decomposition as powers of atom. For instance, from the $\boldsymbol{B}_4^+$-decomposition of Δ_4^2 given in (4.8), we deduce the $\boldsymbol{B}_4^+$-normal form $\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_1^2$.

If x belongs to B_{n-1}^+, then the n-splitting of x is the length one sequence (x). Therefore, we have $D_n(x) = (D_{n-1}(x))$, and the normal form of x as an element of B_{n-1}^+ coincides with its normal form as an element of B_n^+. Owing to this remark, we shall forget about subscripts, and put the following without ambiguity.

Definition 4.9. For x in B_n^+, the $\boldsymbol{B}_n^+$-normal form of x is called the Φ-*normal form* of x.

Lemma 4.7 implies that the Φ-normal form has the following simple connection with the splitting operation—which could be taken as an alternative definition:

Proposition 4.10. *For $n \geqslant 3$ and x in B_n^+, the Φ-normal form of x is the word*

$$\Phi_n^{p-1}(w_p) \cdot \ldots \cdot \Phi_n(w_2) \cdot w_1, \tag{4.10}$$

where $(x_p, \dots, x_1)$ *is the* n*-splitting of* x*, and, for each* r*, the word* w_r *is the* Φ*-normal form of* x_r*.*

The results of Section 3.2 imply that, in addition to the above recursive definitions, the Φ-normal form also admits direct characterizations. We shall now state such characterizations. Several equivalent statements are possible—and can be used in practical implementations. The principle is always:

> An n-strand braid word w is Φ-normal if, for each k, the kth letter of w starting from the right is the smallest σ_i that is a right divisor of the braid represented by the prefix of w finishing at that letter, smallest referring to some local ordering of the σ_i's that is updated at each step and corresponds to a position in the skeleton of the covering $\boldsymbol{B}_n^+$.

The formal definition includes a description of the local ordering of the σ_i's. The latter can be encoded in several equivalent ways, involving addresses, or numbers, or permutations. If the local order were the fixed order $\sigma_1 < \dots < \sigma_{n-1}$, then being normal would simply mean being lexicographically minimal.

We recall that, for α a binary address, $a^{[m]}$ denotes the binary m-successor of α (Definition 2.9), and that, for w a braid word, $\overline{w}$ denotes the braid represented by w.

Proposition 4.11. *A length* ℓ *positive* n*-strand braid word* w *is* Φ*-normal if and only if any one of the following equivalent conditions holds:*

(i) *There exist binary addresses* $\alpha_\ell, \dots, \alpha_0$ *with* $\alpha_0 = 1^{n-2}$ *such that, for each* k*,* $w(k) = g_{\alpha_k}$ *holds, and* α_k *is the maximal binary successor of* α_{k-1} *such that* g_{α_k} *is a right divisor of* $\overline{w(\ell)...w(k)}$*.*

(ii) *There exist numbers* $m_\ell, \dots, m_1$ *in* $\{0, \dots, n\}$ *such that, putting* $\alpha_0 = 1^{n-2}$ *and inductively defining* $\alpha_k = \alpha_{k-1}^{[m_k]}$*, then, for each* k*, we have* $w(k) = g_{\alpha_k}$ *and* $\overline{w(\ell)...w(k)} \not\succcurlyeq g_\alpha$ *for every* m*-successor* α *of* α_{k-1} *with* $m > m_k$*.*

(iii) *There exist permutations* $\pi_\ell, \dots, \pi_0$ *of* $\{1, \dots, n-1\}$ *such that* π_0 *is the identity, and, for each* k*, we have* $w(k) = \sigma_{\pi_k(1)}$ *and* π_k *is obtained from* π_{k-1} *as follows: let* p *be minimal satisfying* $\overline{w(\ell)...w(k)} \succcurlyeq \sigma_{\pi_{k-1}(p)}$*; then we have* $\pi_k(1) = \pi_{k-1}(p)$*,* $\pi_k(q) = \pi_{k-1}(q)$ *for* $q > p$*, and* $(\pi_k(2), \dots, \pi_k(p))$ *is the increasing (*resp. *decreasing) enumeration of* $\{\pi_{k-1}(1), \dots, \pi_{k-1}(p-1)\}$ *if the latter are larger (*resp. *smaller) than* $\pi_k(1)$ *in the usual ordering of integers.*

Proof. Point (i) is Definition 3.6 and (ii) is a direct reformulation. As for (iii), π_k is the enumeration of the names of the successors of α_k, starting from the bottom, *i.e.*, for each m, we have $g_{\alpha_k^{[m]}} = \sigma_i$ with $i = \pi_k(n-m-1)$. At each step, we select the maximal successor satisfying the divisibility requirement, hence, here, the first entry in the permutation π_{k-1}; the updating rules come from the specific definition of the covering $\boldsymbol{B}_n^+$. □

As for complexity, a direct application of Proposition 3.8 gives:

Proposition 4.12. *Running on a positive* n*-strand braid word of length* ℓ*, the algorithm of Table 2 returns the* Φ*-normal word that is equivalent to* w *in* $O(\ell^2 n \log n)$ *steps; in the meanwhile, it also determines the address list of* $D_n(\overline{w})$*.*

Proof. As for (ii), we recall from [21, Chapter 9] that there exists a division algorithm running in time $O(\ell n \log n)$. □

We refer to Table 2 for the algorithm determining the Φ-normal form, and to Table 3 for the details of the computation for Δ_4^2. Note that, apart from the fact that letters come gathered in blocks in the former, the only difference between the unbracketing of the $\boldsymbol{B}_n^+$-decomposition and the Φ-normal form viewed as a sequence of letters is that the $\boldsymbol{B}_n^+$-decomposition always finishes with a power of σ_1, possibly σ_1^0, *i.e.*, 1: for instance, the Φ-normal form of σ_2 is σ_2, *i.e.*, the length one sequence (σ_2), while its $\boldsymbol{B}_3^+$-decomposition is the length two sequence $(\sigma_2, 1)$.

4.4. **A linear order on B_n^+.** As the monoid B_2^+ is isomorphic to $\mathbb{N}$, it is equipped with a natural linear order. Now, as the n-splitting associates with every braid of B_n^+ a distinguished finite sequence of braids, of B_{n-1}^+, we can recursively order B_n^+.

Definition 4.13. For $n \geqslant 2$, we define the relation $<_n^+$ on B_n^+ as follows:

(i) For x, y in B_2^+, we say that $x <_2^+ y$ holds for $x = \sigma_1^p$ and $y = \sigma_1^q$ with $p < q$;

(ii) For x, y in B_n^+ with $n \geqslant 3$, we say that $x <_n^+ y$ holds if, letting $(x_p, \dots, x_1)$ and $(y_q, \dots, y_1)$ be the n-splittings of x and y, we have either $p < q$, or $p = q$ and for some $r \leqslant p$ we have $x_{r'} = y_{r'}$ for $p \geqslant r' > r$ and $x_r <_{n-1}^+ y_r$.

Thus, $<_n^+$ is a sort of lexicographic extension of the natural order on B_2^+, *i.e.*, on $\mathbb{N}$, via splittings. The extension is not exactly lexicographic: before comparing componentwise, we first compare the lengths of the sequences, *i.e.*, the n-breadths of the considered braids, a comparison method called `ShortLex` in [21].

Proposition 4.14. (i) *For $n \geqslant 2$, the relation $<_n^+$ is a linear ordering of B_n^+, which is a well-ordering. For each braid x, the immediate $<_n^+$-successor of x is $x\sigma_1$.*

(ii) *For $n \geqslant 3$, the order $<_n^+$ extends the order $<_{n-1}^+$, and B_{n-1}^+ is the initial segment of B_n^+ determined by σ_{n-1},* i.e., *we have $B_{n-1}^+ = \{x \in B_n^+ \mid x <_n^+ \sigma_{n-1}\}$.*

Proof. (i) The relation $<_2^+$ is a linear ordering of B_2^+. Then, $<_n^+$ being a linear ordering of B_n^+ follows from $<_{n-1}^+$ being a linear ordering of B_{n-1}^+ and the n-splitting being unique. That $<_n^+$ is a well-order results from a similar induction, owing to the standard result that the `ShortLex`-extension of a well-ordering is a well-ordering. Finally, if the n-splitting of x is $(x_p, \dots, x_1)$, the n-splitting of $x\sigma_1$ is $(x_p, \dots, x_1\sigma_1)$, making it clear that $x\sigma_1$ is the immediate successor of x.

(ii) For x, y in B_{n-1}^+, the n-splittings of x and y are the length one sequences (x) and (y), so, by definition, $x <_n^+ y$ is equivalent to $x <_{n-1}^+ y$. On the other hand, the n-splitting of σ_{n-1} is $(\sigma_1, 1)$, so $x <_n^+ \sigma_{n-1}$ holds for each x in B_{n-1}^+. Conversely, assume $x \in B_n^+$ and $x <_n^+ \sigma_{n-1}$. By construction, if (x_2, x_1) is a n-splitting, x_2 is not 1, hence, by (i), we have $x_2 \geqslant_n^+ \sigma_1$. So, if $x <_n^+ \sigma_{n-1}$ holds, the only possibility is that the n-breadth of x is 1, *i.e.*, that x belongs to B_{n-1}^+. ☐

Owing to Proposition 4.14(ii), we shall skip the index n and write $<^+$ for $<_n^+$.

Example 4.15. The 3-splittings of σ_1 and σ_2 respectively are (σ_1) and $(\sigma_1, 1)$, *i.e.*, their respective 3-breadths are 1 and 2. Hence we have $\sigma_1 <^+ \sigma_2$.

Similarly, the 3-splittings of Δ_3 and $\sigma_1^2\sigma_2^2$ are $(\sigma_1, \sigma_1, \sigma_1)$ and $(\sigma_1^2, \sigma_1^2, 1)$. The 3-breadth is 3 in both cases, and we compare lexicographically. The first entries are σ_1 and σ_1^2. The former is smaller, hence $\Delta_3 <^+ \sigma_1^2\sigma_2^2$ holds.

The order $<^+$ has been introduced above by means of the splitting. It can be introduced equivalently by appealing to the exponent sequence of the $\boldsymbol{B}_n^+$-decomposition and to the following ordering of iterated sequences of integers.

Definition 4.16. If $\boldsymbol{s}, \boldsymbol{t}$ are n-sequences of natural numbers, we say that $\boldsymbol{s}$ is ShortLex-smaller than $\boldsymbol{t}$, denoted $\boldsymbol{s} <^{\text{ShortLex}} \boldsymbol{t}$, if we have $n = 0$ and $\boldsymbol{s}$ is smaller than $\boldsymbol{t}$ with respect to the standard order on $\mathbb{N}$, or $n \geqslant 1$ and either $\boldsymbol{s}$—viewed as a sequence of $(n-1)$-sequences—is shorter than $\boldsymbol{t}$, or they have equal length and $\boldsymbol{s}$ is lexicographically smaller than $\boldsymbol{t}$, *i.e.*, writing $\boldsymbol{s} = (\boldsymbol{s}_p, \dots, \boldsymbol{s}_1)$ and $\boldsymbol{t} = (\boldsymbol{t}_p, \dots, \boldsymbol{t}_1)$, there exists $r \leqslant p$ such that we have $\boldsymbol{s}_{r'} = \boldsymbol{t}_{r'}$ for $p \geqslant r' > r$ and $\boldsymbol{s}_r <^{\text{ShortLex}} \boldsymbol{t}_r$.

Lemma 4.17. *For x, y in B_n^+, we have*

$$x <^+ y \iff D_n^*(x) <^{\text{ShortLex}} D_n^*(y). \tag{4.11}$$

Proof. As the relations involved in both sides of (4.11) are linear orders, it is enough to prove one implication. We shall prove using induction on $n \geqslant 2$ that $x <^+ y$ implies $D_n^*(x) <^{\text{ShortLex}} D_n^*(y)$. The result is obvious for $n = 2$. Assume $n \geqslant 3$ and $x <^+ y$ in B_n^+. Let $(x_p, \dots, x_1)$ and $(y_q, \dots, y_1)$ be the n-splittings of x and y. By (4.7), we have

$$D_n^*(x) = (D_{n-1}^*(x_p), \dots, D_{n-1}^*(x_1)), \quad D_n^*(y) = (D_{n-1}^*(y_q), \dots, D_{n-1}^*(y_1)) \tag{4.12}$$

—as the names of the generators are forgotten, the flips do not appear in exponent sequences. According to the definition of $<^+$, two cases are possible. If $p < q$ holds, then the left sequence in (4.12) is shorter than the right sequence, so $D_n^*(x) <^{\text{ShortLex}} D_n^*(y)$ holds. Otherwise, for some $r \leqslant p$, we must have $x_{r'} = y_{r'}$ for $p \geqslant r' > r$ and $x_r <^+ y_r$. We deduce $D_{n-1}^*(x_{r'}) = D_{n-1}^*(y_{r'})$ for $p \geqslant r' > r$ and, using the induction hypothesis, $D_{n-1}^*(x_r) <^{\text{ShortLex}} D_{n-1}^*(y_r)$. Here again, we find $D_n^*(x) <^{\text{ShortLex}} D_n^*(y)$. ☐

For instance, we saw in Example 4.15 that $\Delta_3 <^+ \sigma_1^2\sigma_2^2$ holds. Another way to see it is to compare $D_3^*(D_3)$ and $D_3^*(\sigma_1^2\sigma_2^2)$ with respect to $<^{\text{ShortLex}}$. The respective values are $(1,1,1)$ and $(2,2,0)$: the former is $<^{\text{ShortLex}}$-smaller.

4.5. **The braids $\widehat{\Delta}_{n,p}$.** At this point, whether $x <^+ y$ implies $zx <^+ zy$ is unclear because we do not know much about the n-splittings of zx and zy as compared with those of x and y. We shall come back on the question in Section 5. For the moment, we conclude this section with a technical result about $<^+$, namely we determine the least upper bound of the braids of B_n^+ whose n-breadth is at most p.

Notation 4.18. (See Figure 7) For $n \geqslant 2$ and $d \geqslant 1$, we set

$$\delta_n = \sigma_{n-1} \dots \sigma_1 \text{ and } \widehat{\Delta}_{n,d} = \Phi_n^{d+1}(\delta_n) \cdot \dots \cdot \Phi_n^2(\delta_n) \cdot \Phi_n(\delta_n). \tag{4.13}$$

In other words, $\widehat{\Delta}_{n,d}$ is the length $d(n-1)$ zigzag $\dots\sigma_{n-1}\dots\sigma_1\sigma_1\dots\sigma_{n-1}$ with $d-1$ alternations, finishing with σ_{n-1}. For instance, $\widehat{\Delta}_{4,2}$ is the braid $\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3$.

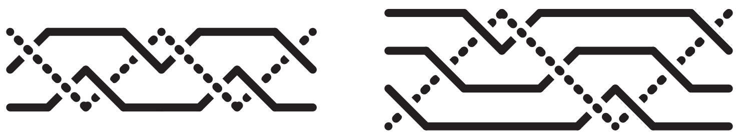


FIGURE 7. The braids $\widehat{\Delta}_{3,4}$ (left) and $\widehat{\Delta}_{4,3}$ (right): starting from the right, the upper strand of $\widehat{\Delta}_{n,d}$ forms d half-twists around all other strands.

Lemma 4.19. (i) *For $n \geqslant 2$ and $d \geqslant 1$, we have*

$$\Delta_n^d = \widehat{\Delta}_{n,d}\, \Delta_{n-1}^d. \tag{4.14}$$

(ii) *For $n \geqslant 2$, $d \geqslant 1$, and $x \in B_{n-1}^+$, the n-splitting of $\widehat{\Delta}_{n,d}\, x$ is*

$$(\sigma_1\ ,\ \underbrace{\delta_{n-1}\sigma_1\ ,\ \dots\ ,\ \delta_{n-1}\sigma_1}_{d-1 \text{ times}}\ ,\ \delta_{n-1}\ ,\ x). \tag{4.15}$$

This holds in particular for $\widehat{\Delta}_{n,d}$ with $x = 1$, and for Δ_n^d with $x = \Delta_{n-1}^d$.

Proof. (i) Among the many equivalent inductive definitions of Δ_n, we choose the recursive definition $\Delta_1 = 1$ and $\Delta_n = \sigma_1 ... \sigma_{n-1} \Delta_{n-1}$, *i.e.*, $\Delta_n = \widehat{\Delta}_{n,1}\Delta_{n-1}$, for $n \geqslant 2$. Then (4.14) holds for $d = 1$. For $d \geqslant 2$, we use induction:

$$\begin{aligned}\Delta_n^d = \Delta_n\Delta_n^{d-1} = \Delta_n\widehat{\Delta}_{n,d-1}\Delta_{n-1}^{d-1} &= \Phi_n(\widehat{\Delta}_{n,d-1})\Delta_n\Delta_{n-1}^{d-1}\\ &= \Phi_n(\widehat{\Delta}_{n,d-1})\widehat{\Delta}_{n,1}\Delta_{n-1}\Delta_{n-1}^{d-1} = \widehat{\Delta}_{n,d}\Delta_{n-1}^d.\end{aligned}$$

(ii) When we evaluate the sequence of (4.15) by flipping each other entry, we obtain $\widehat{\Delta}_{n,d}\, x$. On the other hand, each entry in (4.15) except possibly the last one is right divisible by σ_1, and by no other σ_i. Hence, by Proposition 4.1, the considered sequence is the n-splitting of the braid it represents. □

In particular, the 3-splitting of Δ_3^d is $(\sigma_1, \sigma_1^2, \dots, \sigma_1^2, \sigma_1, \sigma_1^d)$, $d-1$ times σ_1^2, which is $(\sigma_1, \sigma_1, \sigma_1)$ for $d = 1$, corresponding to $\Delta_3 = \sigma_1\sigma_2\sigma_1$, and $(\sigma_1, \sigma_1^2, \sigma_1, \sigma_1^2)$ for $d = 2$, corresponding to $\Delta_3^2 = \sigma_2\sigma_1^2\sigma_2\sigma_1^2$.

We shall see that $\widehat{\Delta}_{n,p-1}$ is the least upper bound for the braids of B_n^+ whose n-breadth at most p. To prove this, we shall show that the n-splitting of $\widehat{\Delta}_{n,p-1}$ is minimal among all n-splittings of length $p + 1$. Therefore, we first investigate the constraints satisfied by n-splittings.

Lemma 4.20. *For $n \geqslant 2$, the braids in B_n^+ that satisfy $x <^+ \delta_n$ are of those of the form $\sigma_{n-1} ... \sigma_m y$ with $n \geqslant m \geqslant 2$ and $y \in B_{m-1}^+$.*

Proof. We use induction on $n \geqslant 2$. For $n = 2$, we have $\delta_n = \sigma_1$, and the result is true, as $x <^+ \sigma_1$ implies $x = 1$, and 1 is the only element of B_1^+. Assume $n \geqslant 3$, and $x <^+ \delta_n$. The n-splitting of δ_n is (σ_1, δ_{n-1}). By definition, two cases are possible: either the n-breadth of x is 1, which means that x lies in B_{n-1}^+, or the n-breadth of x is 2 and, letting (x_2, x_1) be its n-splitting, we have either $x_2 <^+ \sigma_1$, which is impossible, or $x_2 = \sigma_1$ and $x_1 <^+ \delta_{n-1}$. In the latter case, by induction hypothesis, there exist m with $n - 1 \geqslant m \geqslant 2$ and y in B_{m-1}^+ such that $x_1 = \sigma_{n-2} ... \sigma_m y$ holds, and, then, we find $x = \sigma_{n-1}\sigma_{n-2} ... \sigma_m y$. □

Proposition 4.21. *Assume that $(x_p, \dots, x_1)$ is the n-splitting of some braid in B_n^+. Then the following constraints are satisfied:*

$$x_p \geqslant^+ \sigma_1, \quad x_r \geqslant^+ \delta_{n-1}\sigma_1 \text{ for } p > r \geqslant 3, \quad x_2 \geqslant^+ \delta_{n-1} \text{ if } p \geqslant 3 \text{ holds.} \tag{4.16}$$

Proof. First, we have $x_p \neq 1$ by hypothesis, hence $x_p \geqslant^+ \sigma_1$ by Proposition 4.14(i).

Then, x_r is right divisible by σ_1 for $r \geqslant 2$. Indeed, by Proposition 1.16, we have $x_r \neq 1$, hence $x_r \succcurlyeq \sigma_i$ for some i. Now $x_r \succcurlyeq \sigma_i$ implies $\Phi_n^{p-r}(x_p) \cdot \dots \cdot x_r \succcurlyeq \sigma_i$, and $i \geqslant 2$ would contradict the n-splitting condition of Proposition 4.1 at position r.

Assume $p > r \geqslant 3$, and $x_r <^+ \delta_{n-1}\sigma_1$. Write $x_r = y_r\sigma_1$. By Proposition 4.14(i), x_r is the immediate successor of y_r, so $x_r <^+ \delta_{n-1}\sigma_1$ implies $y_r <^+ \delta_{n-1}$. By

Lemma 4.20, we have $y_r = \sigma_{n-2}...\sigma_m y$ with y in B_{m-1}^+ and $n-1 \geqslant m \geqslant 2$. The condition $x_{r+1} \neq 1$ implies $\Phi_n(x_{r+1}) \succcurlyeq \sigma_{n-1}$, hence $\Phi_n(x_{r+1}) \cdot x_r \succcurlyeq \sigma_{n-1} ... \sigma_m y \sigma_1$. Assume first $n > m \geqslant 3$. Then σ_m commutes with y_r and with σ_1, and we obtain $\Phi_n(x_{r+1}) \cdot x_r \succcurlyeq \sigma_m$, which contradicts the n-splitting condition at position r. Assume now $m = 2$, hence $y = 1$. Then we have $\Phi_n(x_{r+1}) \cdot x_r \succcurlyeq \sigma_{n-1} ... \sigma_1$, hence

$$x_{r+1} \cdot \Phi_n(x_r) \cdot x_{r-1} \succcurlyeq \sigma_1 ... \sigma_{n-1} x_{r-1}.$$

Now, for $i \leqslant n-2$, we have $\sigma_1 ... \sigma_{n-1} \sigma_i = \sigma_{i+1} \sigma_1 ... \sigma_{n-1}$, so there exists x' for which $\sigma_1 ... \sigma_{n-1} x_{r-1} = x' \sigma_1 ... \sigma_{n-1}$ holds. We deduce $x_{r+1} \cdot \Phi_n(x_r) \cdot x_{r-1} \succcurlyeq \sigma_{n-1}$, contradicting the n-splitting condition at position $r-1$.

Assume finally $x_2 <^+ \delta_{n-1}$. By Lemma 4.20, we can write $x_2 = \sigma_{n-2} ... \sigma_m x$ with x in B_{m-1}^+ and $n-1 \geqslant m \geqslant 2$. As above, we deduce $\Phi_n(x_3) \cdot x_2 \succcurlyeq \sigma_{n-1} ... \sigma_m x$. If $n > m \geqslant 3$ holds, σ_m commutes with x, and we obtain $\Phi_n(x_3) \cdot x_2 \succcurlyeq \sigma_m$, which contradicts the n-splitting condition at position 2. For $m = 2$, hence $x = 1$, we obtain $\Phi_n(x_3) \cdot x_2 \succcurlyeq \sigma_2$ directly, and the same contradiction. ☐

Proposition 4.22. *For $p \geqslant 1$, the braid $\widehat{\Delta}_{n,p-1}$ is the $<^+$-least upper bound of the elements of B_n^+ whose n-breadth is at most p.*

Proof. By Lemma 4.19(ii), $\widehat{\Delta}_{n,p-1}$ has n-breadth $p+1$, hence $x <^+ \widehat{\Delta}_{n,p-1}$ holds for x with n-breadth at most p. Conversely, assume that the n-breadth of x is at least $p+1$. If it is $p+2$ or more, then $x >^+ \widehat{\Delta}_{n,p-1}$ holds by definition of $<^+$. Otherwise, let $(x_{p+1}, ..., x_1)$ be the n-splitting of x. Proposition 4.21 says that the sequence $(x_{p+1}, ..., x_1)$ is at least $(\sigma_1, \delta_{n-1}\sigma_1, ..., \delta_{n-1}\sigma_1, \delta_{n-1}, 1)$, which is the n-splitting of $\widehat{\Delta}_{n,p-1}$. Hence we have $x \geqslant^+ \widehat{\Delta}_{n,p-1}$. ☐

5. Connection with the braid order

Defining a unique normal representative is of little interest, unless the normal form has some specific additional properties that make it useful. At the moment, the most interesting property of the Φ-normal form of braids seems to be its connection with the so-called Dehornoy order.

5.1. **The braid order.** We shall establish a simple connection between the $<^+$-ordering of B_n^+, *i.e.*, the ordering deduced from the n-splitting, and the standard linear order of braids of [16]. We recall the definition of the latter. Considering B_{n-1}^+ as a submonoid of B_n^+, we denote by B_∞^+ the union of all B_n^+'s, and by B_∞ the group of fractions of B_∞^+, *i.e.*, the braid group on unboundedly many strands.

Definition 5.1. For x, y in B_∞, we say that $x < y$ holds if the braid $x^{-1}y$ admits at least one word representative in which the generator σ_i with maximal index occurs positively only, *i.e.*, σ_i occurs but σ_i^{-1} does not.

Theorem 5.2. (i) [13] *The relation $<$ is a linear ordering of B_∞ that is compatible with multiplication on the left.*

(ii) [25] *The restriction of $<$ to B_∞^+ is a well-ordering.*

(iii) [7] *For each $n \geqslant 2$, the restriction of $<$ to B_n^+, which is the interval $(1, \sigma_n)$ of $(B_\infty^+, <)$, is a well-ordering of type $\omega^{\omega^{n-2}}$.*

In the framework of [16], the orderi of Definition 5.1 is called the upper version of the braid order. In some sources, in particular the early ones, the lower variant is considered, namely the relation $\widetilde{<}$ referring to the letter σ_i with *minimal* index, instead of maximal as above. Both relations are similar as $x < y$ is equivalent to $\Phi_n(x) \mathrel{\widetilde{<}} \Phi_n(y)$ for all x, y in B_n. However, as first noted by S. Burckel in [6], the statements involving the well-order property are more natural with $<$.

5.2. **Adding brackets in a braid word.** In order to connect the braid orders $<^+$ and $<$, we shall compare the Φ-normal form of Section 4 with some other normal form introduced by S. Burckel in his remarkable work, and we first need to introduce some notions from [7]. The original description of [7] is formulated in terms of trees. However, the latter are equivalent to the iterated sequences of Section 2, and we can easily describe the fragment of Burckel's construction needed here in terms of iterated sequences. Here , we give a new description that is more directly connected to our approach. In terms of trees, this amounts to starting from the top and the right, while Burckel's approach starts from the bottom and the left. The equivalence of both descriptions is established in Proposition 5.11 below.

Our basic observation here is that a free monoid is locally right Garside: this is a trivial result, as the right divisibility relation of a free monoid is simply the relation of being a suffix. Then, applying the decomposition process of Sections 1 and 2 to a word w in a free monoid amounts to grouping the letters of w into blocks, *i.e.*, in adding brackets in w. We shall consider the iterated covering of the free braid word monoids that mimicks the covering $\boldsymbol{B}_n^+$ of Section 4.

Notation 5.3. We denote by $\underline{B}_n^+$ the free monoid consisting of all positive n-strand braid words, and by $\underline{\boldsymbol{B}}_n^+$ the atomic iterated covering of $\underline{B}_n^+$ based on the sequence $\boldsymbol{g}_n$—the same as in the case of $\boldsymbol{B}_n^+$.

We shall now use the $\underline{\boldsymbol{B}}_n^+$-decomposition of a word in $\underline{B}_n^+$. As in Section 4, it is convenient to take advantage of the recursive definition of the covering $\underline{\boldsymbol{B}}_n^+$, and to introduce the counterpart of the n-splitting.

Definition 5.4. For $n \geqslant 3$ and w in $\underline{B}_n^+$, the *n-splitting* of w is defined to be the unique sequence $(w_p, \dots, w_1)$ of words in $\underline{B}_{n-1}^+$ such that $(\Phi_n^{p-1}(w_p), \dots, \Phi_n(w_2), w_1)$ is the $(\Phi_n(\underline{B}_{n-1}^+), \underline{B}_{n-1}^+)$-decomposition of w.

As being a right divisor in a free monoid is equivalent to being a suffix, Proposition 1.16 implies that $(w_p, \dots, w_1)$ is the n-splitting of w if and only if, for each r, the word w_r is the longest suffix of $\Phi_n^{p-r}(w_p) \cdot \dots \cdot w_p$ that lies in $\underline{B}_{n-1}^+$.

Example 5.5. Let w be the 4-strand braid word $\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_1^2$. The longest suffix of w that lies in $\underline{B}_3^+$ is $\sigma_2\sigma_1^2\sigma_2\sigma_1^2$, and the remaining prefix is $\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3$, *i.e.*, $\Phi_4(w^{(1)})$ with $w^{(1)} = \sigma_1\sigma_2\sigma_3^2\sigma_2\sigma_1$. The longest suffix of $w^{(1)}$ that does not contain σ_3 is $\sigma_2\sigma_1$, with remaining prefix $\sigma_1\sigma_2\sigma_3^2$, *i.e.*, $\Phi_4(w^{(2)})$ with $w^{(2)} = \sigma_3\sigma_2\sigma_1^2$. The longest suffix of $w^{(2)}$ that does not contain σ_3 is $\sigma_2\sigma_1^2$, with remaining prefix σ_3. So, by definition, the 4-splitting of the word w is the sequence of 3-strand braid words $(\sigma_1,\ \sigma_2\sigma_1^2,\ \sigma_2\sigma_1,\ \sigma_2\sigma_1^2\sigma_2\sigma_1^2)$.

Imitating for braid words the notation used for braids in Section 4, we put:

Notation 5.6. For w in $\underline{B}_n^+$, we denote the $\underline{\boldsymbol{B}}_n^+$-decomposition of w by $\underline{D}_n(w)$, and its exponent sequence by $\underline{D}_n^*(w)$.

By construction, the iterated sequence $\underline{D}_n(w)$ is a certain bracketing of w. Before giving an example, we note the following connection between the $\underline{\boldsymbol{B}}_n^+$-decomposition and the splitting.

Lemma 5.7. *For $n \geqslant 3$ and w in $\underline{B}_n^+$, we have*

$$\underline{D}_n(w) = (\Phi_n^{p-1}(\underline{D}_{n-1}(w_p)), \dots, \Phi_n(\underline{D}_{n-1}(w_2)), \underline{D}_{n-1}(w_1)). \tag{5.1}$$

where $(w_p, \dots, w_1)$ is the n-splitting of w.

The proof is exactly similar to that of Lemma 4.7.

Example 5.8. Let again w be the 4-strand braid word $\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_1^2$. We saw in Example 5.5 that the 4-splitting of w is $(\sigma_1, \sigma_2\sigma_1^2, \sigma_2\sigma_1, \sigma_2\sigma_1^2\sigma_2\sigma_1^2)$. Then, we can easily see that the 3-splitting of the word $\sigma_2\sigma_1^2\sigma_2\sigma_1^2$ is $(\sigma_2, \sigma_1^2, \sigma_2, \sigma_1^2)$, etc. Using (5.1), we conclude that the $\underline{\boldsymbol{B}}_4^+$-decomposition of w is the 2-sequence

$$\underline{D}_4(w) = ((\sigma_3), (\sigma_2, \sigma_1^2), (\sigma_2, \sigma_3), (\sigma_2, \sigma_1^2, \sigma_2, \sigma_1^2)). \tag{5.2}$$

The braid word w considered in Example 5.8 is the Φ-normal form of Δ_4^2. By comparing (4.8) and (5.2), we see that, up to identifying the word σ_i^e with the braid it represents, the $\underline{\boldsymbol{B}}_4^+$-decomposition of the word w is the $\boldsymbol{B}_4^+$-decomposition of Δ_4^2. This phenomenon is general.

Lemma 5.9. *If w is a Φ-normal n-strand braid word, we have $\underline{D}_n(w) = D_n(\overline{w})$.*

Proof. We use induction on n. For $n = 2$, the result is obvious. Otherwise, let $(x_p, \dots, x_1)$ be the n-splitting of $\overline{w}$, and, for each r, let w_r be the Φ-normal form of x_r. By construction, each word w_r with $r \geqslant 2$ finishes with σ_1, so $(w_p, \dots, w_1)$ is the n-splitting of w. The induction hypothesis implies $\underline{D}_{n-1}(w_r) = D_{n-1}(x_r)$ for each r. Applying (5.1), we deduce

$$\begin{aligned}\underline{D}_n(w) &= (\Phi_n^{p-1}(\underline{D}_{n-1}(w_p)), \dots, \Phi_n(\underline{D}_{n-1}(w_2)), \underline{D}_{n-1}(w_1))\\ &= (\Phi_n^{p-1}(D_{n-1}(x_p)), \dots, \Phi_n(D_{n-1}(x_2)), D_{n-1}(x_1)).\end{aligned}$$

By (4.7), the latter sequence is $D_n(\overline{w})$. ☐

At this point, we can easily establish the connection between our current notion of $\underline{\boldsymbol{B}}_n^+$-decomposition and Burckel's notion of "the tree of a braid word".

Lemma 5.10. *Assume $n \geqslant 3$ and $w \in \underline{B}_n^+$ with $\underline{D}_n(w) = (\boldsymbol{s}_p, \dots, \boldsymbol{s}_1)$. Then, for $1 \leqslant i \leqslant n-1$, and assuming $\boldsymbol{s}_p = \underline{D}_{n-1}(w_p)$, we have*

$$\underline{D}_n(\sigma_i w) = \begin{cases}((\dots(\sigma_i)\dots), \boldsymbol{s}_p, \dots, \boldsymbol{s}_1) & \text{for } p \text{ even and } i = 1,\\ & \quad\text{and for } p \text{ odd and } i = n-1,\\ (\underline{D}_{n-1}(\Phi_n^{p-1}(\sigma_i)w_p), \boldsymbol{s}_{p-1}, \dots, \boldsymbol{s}_1) & \text{otherwise.}\end{cases}$$

Proof. Let $(w_p, \dots, w_1)$ be the n-splitting of w. Then the n-splitting of $\sigma_i w$ is $(\sigma_1, w_p, \dots, w_1)$ for p even and $i = 1$, and for p odd and $i = n-1$, and it is $(\Phi_n^{p-1}(\sigma_i)\, w_p, w_{p-1}, \dots, w_1)$ otherwise. Indeed, the point is whether the additional letter σ_i can be incorporated in the same entry as w_p. Taking the flips into account, this depends on whether $\Phi_n^{p-1}(\sigma_i)$ is σ_{n-1} or not. The value of $\underline{D}_n(\sigma_i w)$ directly follows. ☐

As the rule of Lemma 5.10 directly mimicks the inductive construction of the tree associated with w in the sense of [7], we deduce:

Proposition 5.11. *For each positive n-strand braid word w, the tree associated with $\underline{D}_n(w)$ coincides with the tree of w as defined in [7].*

Before going to Burckel's results, let us observe that the braid ordering $<^+$ of Definition 4.13 admits a simple characterization in terms of Φ-normal words.

Proposition 5.12. *For all x, y in B_n^+, we have*

$$x <^+ y \quad \Longleftrightarrow \quad \underline{D}_n^*(u) <^{\text{ShortLex}} \underline{D}_n^*(v), \tag{5.3}$$

where u and v are the Φ-normal representatives of x and y.

Proof. By Lemma 5.9, we have $D_n(x) = \underline{D}_n(u)$ and $D_n(y) = \underline{D}_n(v)$, so $x <^+ y$, which is equivalent to $D_n^*(x) <^{\text{ShortLex}} D_n^*(y)$ by Lemma 4.17, is also equivalent to $\underline{D}_n^*(u) <^{\text{ShortLex}} \underline{D}_n^*(v)$. □

Remark 5.13. For w in $\underline{B}_n^+$, define a $\underline{\boldsymbol{B}}_n^+$-bracketing of w to be any $(n-2)$-sequence $\boldsymbol{s}$ such that the unbracketing of $\boldsymbol{s}$ is w and, for each address θ of length n–2, the entry $\boldsymbol{s}_\theta$ belongs to $\underline{B}_{[\theta]}^+$ when it exists. So a $\underline{\boldsymbol{B}}_n^+$-bracketing of w is any way of adding brackets in w so that the resulting iterated sequence has its entries correctly dispatched with respect to the skeleton of the iterated covering $\underline{\boldsymbol{B}}_n^+$. By construction, $\underline{D}_n(w)$ is always a $\underline{\boldsymbol{B}}_n^+$-bracketing of w, but it is not the only one. For instance, both (σ_2^2, σ_1) and $(\sigma_2, \varepsilon, \sigma_2, \varepsilon, \varepsilon, \sigma_1)$ are $\underline{\boldsymbol{B}}_3^+$-bracketings of the word $\sigma_2^2\sigma_1$. Then it is easy to check that $\underline{D}_n(w)$ is, among all $\underline{\boldsymbol{B}}_n^+$-bracketings of w, the one that has the $<^{\text{ShortLex}}$-smallest exponent sequence.

5.3. **The Burckel normal form.** We now appeal to Burckel's results in [7] to state a connection between the braid order $<$ and the $<^{\text{ShortLex}}$-ordering of the exponent sequences.

Definition 5.14. A positive n-strand braid word w is said to be *Burckel normal* if the exponent sequence $\underline{D}_n^*(w)$ is $<^{\text{ShortLex}}$-minimal among all $\underline{D}_n^*(w')$ with $w' \equiv w$.

Example 5.15. Let us consider the two positive 3-strand braid words that represent Δ_3, namely $\sigma_1\sigma_2\sigma_1$ and $\sigma_2\sigma_1\sigma_2$. Then we find $\underline{D}_3(\sigma_1\sigma_2\sigma_1) = (\sigma_1, \sigma_2, \sigma_1)$, and $\underline{D}_3(\sigma_2\sigma_1\sigma_1) = (\sigma_2, \sigma_1, \sigma_2, \varepsilon)$—here we use the empty word ε to emphasize that we consider words. So we have $\underline{D}_3^*(\sigma_1\sigma_2\sigma_1) = (1,1,1)$, and $\underline{D}_3^*(\sigma_2\sigma_1\sigma_2) = (1,1,1,0)$. As $(1,1,1)$ is shorter, hence $<^{\text{ShortLex}}$-smaller, than $(1,1,1,0)$, we conclude that $\sigma_1\sigma_2\sigma_1$ is Burckel normal, while $\sigma_2\sigma_1\sigma_2$ is not.

Burckel normal words are called *irreducible* in [7]. As the ShortLex-ordering of n-sequences on $\mathbb{N}$ is a well-ordering, each nonempty set of n-sequences in $\mathbb{N}$ contains a $<^{\text{ShortLex}}$-least element. Therefore, each positive braid admits a unique Burckel normal representative.

Theorem 5.16 (Burckel, [7])**.** *For x, y in B_n^+, we have*

$$x < y \quad \Longleftrightarrow \quad \underline{D}_n^*(u) <^{\text{ShortLex}} \underline{D}_n^*(v), \tag{5.4}$$

where u and v are the Burckel normal representatives of x and y.

Burckel's proof of Theorem 5.16 is quite subtle for $n \geqslant 4$ and requires a transfinite induction. The point is to define a combinatorial operation called reduction so that, if a braid word w is not Burckel normal, then its reduct w' is equivalent to w and satisfies $\underline{D}_n^*(w') <^{\text{ShortLex}} \underline{D}_n^*(w)$.

In the sequel, we shall only use the following consequence of Theorem 5.16.

Corollary 5.17. *If u and v are the Burckel normal representatives of x and $x\sigma_i$, then $\underline{D}_n^*(u) <^{\text{ShortLex}} \underline{D}_n^*(v)$ holds.*

Proof. By definition, we have $x < x\sigma_i$, as the quotient $x^{-1}x\sigma_i$ has an expression, namely σ_i, in which the generator with highest index appears positively only. $\square$

5.4. **Connecting the normal forms.** At this point, two distinguished word representatives have been introduced for each positive braid, namely its Φ-normal form, and its Burckel normal form. We shall now prove that these *a priori* unrelated normal representatives actually coincide.

Proposition 5.18. *The Burckel normal form coincides with the Φ-normal form.*

Proof. As each braid admits a unique Burckel normal representative and a unique Φ-normal representative, proving one implication is sufficient. Here we prove using induction on $n \geqslant 2$ that an n-strand braid word that is not Φ-normal is not either Burckel normal. For $n = 2$, every word, namely every power of σ_1, is normal in both senses. Assume $n \geqslant 3$, and assume that w is a word in $\underline{B}_n^+$ that is not Φ-normal. We aim at proving that w is not Burckel normal. Owing to the definition of a Burckel normal word, it is enough to exhibit a word w' that represents the same braid as w and is such that $\underline{D}_n^*(w')$ is `ShortLex`-smaller than $\underline{D}_n^*(w)$.

Let $(w_p, \dots, w_1)$ be the n-splitting of w. By Lemma 5.7, the value of $\underline{D}_n^*(w)$ is

$$(\underline{D}_{n-1}^*(w_p), \dots, \underline{D}_{n-1}^*(w_2), \underline{D}_{n-1}^*(w_1)) \tag{5.5}$$

—as we consider exponent sequences, we can forget about flips. The hypothesis that w is not Φ-normal may have two causes, namely that one of the words w_r is not Φ-normal, or that all words w_r are Φ-normal but $(\overline{w_p}, \dots, \overline{w_1})$ is not the n-splitting of the braid $\overline{w}$.

Assume first that some word w_r is not Φ-normal. By induction hypothesis, w_r is not Burckel normal either. Hence there exists a word w_r' equivalent to w_r satisfying

$$\underline{D}_{n-1}^*(w_r') <^{\text{ShortLex}} \underline{D}_{n-1}^*(w_r).$$

Let w' be the word obtained from w by replacing the subword $\Phi_n^{r-1}(w_r)$ with $\Phi_n^{r-1}(w_r')$. Then w' is equivalent to w, and, by construction, one has

$$\underline{D}_n^*(w') <^{\text{ShortLex}} \underline{D}_n^*(w),$$

hence w cannot be Burckel normal.

Assume now that each word w_r is Φ-normal and $(\overline{w_p}, \dots, \overline{w_1})$ is not the n-splitting of $\overline{w}$. Then there exists r such that the braid represented by

$$v = \Phi_n^{p-r}(w_p) \cdot \dots \cdot \Phi_n(w_{r+1}) \cdot w_r$$

is right divisible by some σ_i with $i \geqslant 2$. We shall show that the factor σ_i can be removed from w_r and incorporated in the next factor w_{r-1}, so as to give rise to a new word w' equivalent to w and satisfying $\underline{D}_n^*(w') <^{\text{ShortLex}} \underline{D}_n^*(w)$—see Figure 8.

Indeed, let v' be the Burckel normal form of $\overline{v}\,\sigma_i^{-1}$, and let w' be the word $\Phi_n^{r-1}(v') \cdot \Phi_n^{r-2}(\sigma_{n-i}w_{r-1}) \cdot \dots \cdot \Phi_n(w_2) \cdot w_1$. By construction, w' is equivalent to w. The n-splitting of v is $(w_p, \dots, w_r)$. Let $(w_{p'}', \dots, w_r')$ be that of v'. Then the n-splitting of w' is $(w_{p'}', \dots, w_r', \sigma_{n-i}w_{r-1}, w_{r-2}, \dots, w_1)$, and so, by Lemma 5.7, the value of $\underline{D}_n^*(w')$ is

$$(\underline{D}_{n-1}^*(w_{p'}'), \dots, \underline{D}_{n-1}^*(w_r'), \underline{D}_{n-1}^*(\sigma_{n-i}w_{r-1}), \underline{D}_{n-1}^*(w_{r-2}), \dots, \underline{D}_{n-1}^*(w_1)). \tag{5.6}$$

Now—this is the point—Corollary 5.17 implies $\underline{D}_n^*(v') <^{\text{ShortLex}} \underline{D}_n^*(v)$, *i.e.*, always by Lemma 5.7,

$$(\underline{D}_{n-1}^*(w_{p'}'), \dots, \underline{D}_{n-1}^*(w_r')) <^{\text{ShortLex}} (\underline{D}_{n-1}^*(w_p), \dots, \underline{D}_{n-1}^*(w_r))$$

—hence in particular $p' \leqslant p$. Adding $r-1$ entries on the right of the above sequences does not change their order, and we deduce that the sequence of (5.6) is ShortLex-smaller than that of (5.5), *i.e.*, $\underline{D}_n^*(w')$ is ShortLex-smaller than $\underline{D}_n^*(w)$. This shows that w is not Burckel normal. $\square$

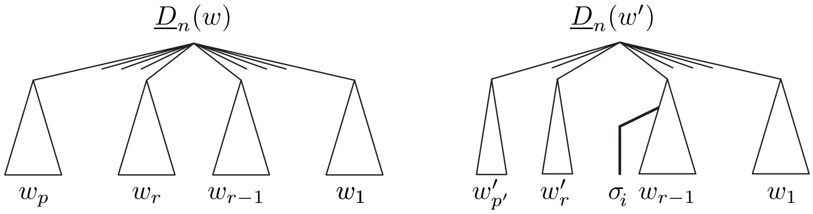


FIGURE 8. Proof of Proposition 5.18: if w is not Φ-normal because some σ_i with $i \geqslant 2$ right divides the braid associated with the $p-r+1$ left factors, then that σ_i can be removed from the left part and incorporated in the next factor; Corollary 5.17 guarantees that the new left part is smaller than the old one, so the new word w' is equivalent to w but its exponent sequence is smaller than that of w.

Remark. It is natural to wonder whether Proposition 5.18 extends to every dense atomic covering $\boldsymbol{M}$ of a locally right monoid M, *i.e.*, whether the $\boldsymbol{M}$-normal form of an element x of M is always the representative whose $\underline{\boldsymbol{M}}$-decomposition—defined in the obvious way from the considered atoms—has the $<^{\mathrm{ShortLex}}$-minimal exponent sequence. This is *not* the case. Indeed, as in Remark 1.20, consider the 2-covering $\boldsymbol{M}$ of B_4^+ based on $((\sigma_3, \sigma_2), (\sigma_3, \sigma_1))$. Then, the $\boldsymbol{M}$-normal form of $\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3^2\sigma_2$ turns out to be the word $\sigma_1\sigma_2^2\sigma_1\sigma_3\sigma_2\sigma_1$. Now the $\underline{\boldsymbol{M}}$-decompositions of the words $\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3^2\sigma_2$ and $\sigma_1\sigma_2^2\sigma_1\sigma_3\sigma_2\sigma_1$ respectively are

$$((\sigma_3, \sigma_2), (\sigma_1), (\sigma_2, \sigma_3^2, \sigma_2), (\varepsilon)) \quad \text{and} \quad ((\sigma_1), (\sigma_2^2), (\sigma_1), (\sigma_3, \sigma_2), g(\sigma_1)),$$

with lengths 4 and 5—this is the same example as in Remark 1.20. The latter has a $<^{\mathrm{ShortLex}}$-larger exponent sequence, so the $\boldsymbol{M}$-normal form does not correspond to the smallest exponent sequence. Technically, the point is that the counterpart to Corollary 5.17 fails: the breadth may decrease under right multiplication. For instance, for $y = \sigma_1\sigma_2^2\sigma_1\sigma_3\sigma_2\sigma_1^2$, the $\boldsymbol{M}$-decomposition of y is $(\sigma_1, \sigma_2^2, \sigma_1\sigma_3, \sigma_2, \sigma_1^2)$, which has length 5, while that of $y\sigma_2$ is $(\sigma_3\sigma_2^2, \sigma_1, \sigma_2\sigma_3^2\sigma_2, \sigma_1)$, which has length 4. This shows that the covering $\boldsymbol{B}_n^+$ is quite specific.

5.5. **Applications.** Once we know that the Φ-normal form and the Burckel normal form coincide, each one inherits the properties of the other, and we easily deduce several consequences, in particular in terms of braid orderings.

Proposition 5.19. *For $x, y \in B_\infty^+$, the relations $x < y$ and $x <^+ y$ are equivalent.*

Proof. Let u and v be the Φ-normal representatives of x and y. By Proposition 5.18, u and v also are the Burckel normal representatives of x and y. The equivalences

$$x < y \iff \underline{D}_n^*(u) <^{\mathrm{ShortLex}} \underline{D}_n^*(v) \iff x <^+ y$$

then follow from Proposition 5.12 and Theorem 5.16. $\square$

We deduce that the standard braid order $<$ inherits the recursive definition of the order $<^+$, which is Theorem A(ii) in the introduction:

Corollary 5.20. *Let x, y be positive n-strand braids. Let $(x_p, \dots, x_1)$ and $(y_q, \dots, y_1)$ be the n-splittings of x and y. Then $x < y$ holds in B_n^+ if and only if we have either $p < q$, or $p = q$ and there exists $r \leqslant p$ such that we have $x_{r'} = y_{r'}$ for $p \geqslant r' > r$ and $x_r < y_r$ in B_{n-1}^+.*

In the other direction, we deduce that the order $<^+$ satisfies the known properties of the order $<$:

Corollary 5.21. *The order $<^+$ is compatible with multiplication on the left, and $x <^+ x\sigma_i$ holds for all x and i.*

Further consequences involve the algorithmic complexity. The following result deals with the braid order $<$, and it is Theorem B in the introduction.

Corollary 5.22. *For each n, the braid order $<$ on B_n can be decided in quadratic time: if w is a (not necessarily positive) n-strand braid word of length ℓ, then whether $\overline{w} > 1$ holds can be decided in time $O(\ell^2 n^3 \log n)$.*

Proof. We first observe that, if u, v are positive n-strand braid words of length at most ℓ, then $\overline{u} < \overline{v}$ can be decided in time $O(\ell^2 n \log n)$. Indeed, by Proposition 4.12(ii), we can compute the decompositions $D_n(\overline{u})$ and $D_n(\overline{v})$ within the indicated amount of time; the extra cost of subsequently comparing the corresponding exponent sequences with respect to the `ShortLex`-ordering is linear in ℓn.

If w is an arbitrary n strand braid word of length ℓ, according to [21, Chapter 9], we can find two positive braid words u, v of length in $O(\ell n^2)$ such that w is equivalent to $u^{-1}v$ in time $O(\ell^2 n \log n)$. Then $\overline{w} > 1$ is equivalent to $\overline{u} < \overline{v}$, which, by the above observation, can be decided in time $O(\ell^2 n^5 \log n)$. Actually, we can lower the exponent of n to 3 because an upper bound for the computation of the Φ-normal form is $O(\ell \ell_c n \log n)$, where ℓ_c is the canonical length, *i.e.*, the number of divisors of Δ_n involved in the right greedy normal form. When we go from w to $u^{-1}v$, the canonical lengths of u and v are bounded above by that of w, leading to $O(\ell \ell_c n^3 \log n)$ for the whole comparison. ☐

Finally, another application is that, for each n, the Burckel normal form of a positive n-strand braid word can be computed in quadratic time w.r.t. the length of the initial word, which is clear from Proposition 4.12 and the fact that the Burckel normal form coincides the Φ-normal form. In the approach of [7], the Burckel normal form comes as the final result of an iterated reduction process whose convergence is guaranteed by the fact that an ordinal decreases, and no complexity analysis has been published so far.

6. Open questions and further work

6.1. **The Φ-normal form.** We have seen in Proposition 4.21 that an arbitrary sequence of braids in B_{n-1}^+ need not be the n-splitting of a braid in B_n^+. An obvious question is whether the constraints of Proposition 4.21 are sufficient conditions.

Question 6.1. *Assume that $x_p, \dots, x_1$ are braids of B_{n-1}^+ that satisfy*

$$x_p \geqslant \sigma_1, \quad x_r \geqslant \delta_{n-1}\sigma_1 \text{ for } p > r \geqslant 3, \quad x_2 \geqslant \delta_{n-1} \text{ if } p \geqslant 3 \text{ holds.} \tag{6.1}$$

Does there exist a braid in B_n^+ whose n-splitting is $(x_p, \dots, x_1)$?

The only case where a (positive) answer is known is $n = 3$.

Proposition 6.2. *A sequence* $(\sigma_1^{e_p}, \dots, \sigma_1^{e_1})$ *is the* 3*-splitting of a braid of* B_3^+ *if and only if the numbers* e_r *satisfy the inequalities:*

$$e_p \geqslant 1, \quad e_r \geqslant 2 \text{ for } p > r \geqslant 3, \quad e_2 \geqslant 1 \text{ if } p \geqslant 3 \text{ holds.} \tag{6.2}$$

Proof. What remains to be shown is that, if at least one of the above conditions fails, then $(\sigma_1^{e_p}, \dots, \sigma_1^{e_1})$ is not a 3-splitting. Now, by Lemma 3.4, no gap may exist in a 3-splitting, so $e_r = 0$ is impossible for $p > r \geqslant 2$.

On the other hand, assume $e_r = 1$ with $p > r \geqslant 3$. As we have $\sigma_1^{e_{p+1}}\sigma_2\sigma_1^{e_{p-1}} = \sigma_1^{e_{p+1}-1}\sigma_2^{e_{p-1}}\sigma_1\sigma_2$, the braid $\Phi_3^{p-1-r}(\sigma_1^{e_r}) \cdot \dots \cdot \sigma_1^{e_{p-1}}$ is right divisible by σ_2, contradicting the characteristic property of a 3-splitting. □

The result can be restated as

Corollary 6.3. *Set* $e_1^{\min} = 0$, $e_2^{\min} = 1$, *and* $e_r^{\min} = 2$ *for* $r \geqslant 3$. *Then a positive* 3*-strand braid word* $\sigma_{[p]}^{e_p} \dots \sigma_2^{e_2}\, \sigma_1^{e_1}$ *with* $e_p \geqslant 1$ *is* Φ*-normal if and only if the inequality* $e_r \geqslant e_r^{\min}$ *is satisfied for all indices* r *except possibly* p.

Remark 6.4. A priori, the Φ-normal form of a positive braid is completely different from its right greedy normal form of [21, Chapter 9]. However, it was observed by J. Mairesse (private communication) that, in the case of 3-strands, there is a rather simple connection: starting from the right greedy normal form of a positive 3-strand braid, we can obtain its Φ-normal form by replacing the final factor Δ_3^e with its Φ-normal form, and, depending on the parity of e and on the final letter in the next factor, possibly push some factors σ_i^d through Δ_3^e—see [9] for details.

6.2. **Braid ordering.** The proof of Proposition 5.18 heavily relies on Burckel's Theorem 5.16, a highly non-trivial combinatorial result in the general case.

Question 6.5. *Is there a direct proof for the following results?*
(i) *The orders* $<^+$ *and* $<$ *coincide.*
(ii) *The order* $<^+$ *is compatible with multiplication on the left.*
(iii) *The relation* $x <^+ x\sigma_i$ *always holds.*

So far we have no general answer. We mention below partial results toward a positive answer to Question 6.5(i), namely proving that, for all braids x, y, the relation $x <^+ y$ implies $x < y$—as we are dealing with linear orders, one implication is enough. Here we consider special values for y. By Proposition 4.14(ii), we already know that $x <^+ \sigma_{n-1}$ is equivalent to $x < \sigma_{n-1}$, as both are equivalent to $x \in B_{n-1}^+$. Here is another result of this kind.

Proposition 6.6. *For every* x *in* B_n^+, *the relation* $x <^+ \widehat{\Delta}_{n,d}$ *implies* $x < \widehat{\Delta}_{n,d}$.

Proof. Assume $x <^+ \widehat{\Delta}_{n,d}$. By Proposition 4.22, the n-breadth of x is at most $d+1$, and we can write $x = \Phi_n^d(x_{d+1}) \cdot \dots \cdot \Phi_n(x_2) \cdot x_1$ for some $x_{d+1}, \dots, x_1$ in B_{n-1}^+. An easy computation using (4.14) and the equalities $\Phi_n(x_r^{-1}) = \Delta_n x_r^{-1} \Delta_n^{-1}$ gives

$$x^{-1}\, \widehat{\Delta}_{n,d} = x_1^{-1} \cdot \Delta_n x_2^{-1} \cdot \Delta_n x_3^{-1} \dots \cdot \Delta_n x_{d+1}^{-1} \cdot \Delta_{n-1}^{-d}. \tag{6.3}$$

This leads to an expression of the quotient $x^{-1}\widehat{\Delta}_{n,d}$ in which the letter σ_{n-1} occurs d times, while neither σ_{n-1}^{-1} nor any letter $\sigma_j^{\pm 1}$ with $j \geqslant n$ does. Indeed, each factor Δ_n admits a positive expression in which σ_{n-1} occurs once, namely the one arising from the decomposition $\Delta_n = \widehat{\Delta}_{n,1}\Delta_{n-1}$, while the negative factors x_r^{-1} and Δ_{n-1}^{-d} belong to B_{n-1} and therefore can be expressed using neither σ_{n-1} nor σ_{n-1}^{-1}. Therefore $x < \widehat{\Delta}_{n,d}$ holds. □

It is not hard to deduce that, for every x in B_n^+, the relation $x <^+ \Delta_n^d$ implies $x < \Delta_n^d$, as well as various similar compatibility results between $<^+$ and $<$. But, so far, we have no complete answer to Question 6.5(i) in the general case.

It is however easy to provide such an answer in the case $n = 3$. Indeed, in this special case, the exact form of Φ-normal words is known, and a direct computation similar to that of Proposition 6.6 shows that, for x, y in B_3^+, the relation $x <^+ y$ implies that the braid $x^{-1}y$ are an expression where σ_2 occurs but σ_2^{-1} does not, or an expression where σ_1 occurs but none of $\sigma_1^{-1}, \sigma_2, \sigma_2^{-1}$ does, *i.e.*, that $x < y$ holds.

By [25] and [7], we know that $(B_3^+, <)$ is a well-ordering of order type ω^ω. Hence the position of every braid of B_3^+ is unambiguously specified by an ordinal number, called the *rank* of x, namely the order type of the initial segment of $(B_3^+, <)$ determined by x. Using the formula for the Φ-normal form given in Corollary 6.3, we deduce the following explicit value for the rank of a 3-strand braid.

Proposition 6.7. *The rank of the braid with Φ-normal form $\sigma_{[p]}^{e_p} \dots \sigma_2^{e_2}\, \sigma_1^{e_1}$ in the well-ordering $(B_3^+, <)$ is the ordinal number*

$$\omega^{p-1} \cdot e_p + \sum_{r=p-1}^{r=1} \omega^{r-1} \cdot (e_r - e_r^{\min}), \tag{6.4}$$

where the (absolute) numbers $e_r^{\min}$ are those of Corollary 6.3.

Proof. The point is to determine which Φ-normal words correspond to braids smaller than the considered one. By Corollary 6.3, Φ-normal words are characterized by the inequalities $e_r \geqslant e_r^{\min}$ for $r < p$, and (6.4) follows. ☐

For instance, we saw in Lemma 4.19 that the 3-splitting of Δ_3^d is the length $d+2$ sequence $(\sigma_1, \sigma_1^2, \dots, \sigma_1^2, \sigma_1, \sigma_1^d)$. Proposition 6.7 shows that, for each d, the rank of Δ_3^d in $(B_3^+, <)$ is the ordinal $\omega^{d+1} + d$: only the initial 1 and the final d contribute here, as all intermediate exponents have the minimal legal value $e_r^{\min}$.

Question 6.8. *Does there exist a similar explicit formula for the rank of an arbitrary positive braid in the well-ordering $(B_\infty^+, <)$?*

We refer to [8] for partial results about Question 6.8, and to [9] for further applications, consisting of unprovability statements involving braids.

6.3. **Artin–Tits monoids and other Garside monoids.** We proved in Section 2 that $\boldsymbol{M}$-decompositions exist in every locally right Garside monoid M in which enough closed submonoids exist. This is in particular the case for every Artin–Tits monoid with respect to the standard set of generators S, as every subset of S generates a closed submonoid that is closed. Thus, dense atomic coverings exist for every Artin–Tits monoid M, and each of them leads to $\boldsymbol{M}$-decompositions similar to those of Section 4. Then, we can adapt Section 4.4 and define a linear ordering $<_{\boldsymbol{M}}$ of M using the `ShortLex`-ordering on $\boldsymbol{M}$-decompositions.

Question 6.9. *Let M be an Artin–Tits monoid. Is any of the linear orders $<_{\boldsymbol{M}}$ invariant under left multiplication?*

In type A_n, *i.e.*, if M is a braid monoid, Corollary 5.21 provides a positive answer. But the proof depends on the connection between the orders $<^+$ and $<$ and it is quite specific. More general positive results would presumably entail a direct proof in the case of braids, *i.e.*, an answer to Question 6.5(ii).

Another possible extension of the current approach consists in addressing braids again, but in connection with other monoids. Laver's proof of Theorem 5.2(ii) implies that the restriction of $<$ to any finitely generated submonoid of B_∞ generated by conjugates of the σ_i's is a well-ordering. In particular, the restriction of $<$ to the dual braid monoids of [4] is a well-ordering. The latter are Garside monoids, and they are directly relevant for our approach. Natural analogs to the Φ-normal forms exist, and investigating their connection with the braid order is an obvious task, recently achieved by J. Fromentin in [22]. It turns out that the dual framework is more suitable than the standard one, in that a positive answer to the counterpart of Question 6.5 can be given, with a direct proof that requires no transfinite induction.

6.4. **Geometric and dynamic properties.** As every braid admits a canonical decomposition as a fraction xy^{-1} with x, y in B_∞^+ with no common right divisor, we can extend the Φ-normal form of B_∞^+ into a unique normal form on B_∞. Experiments suggest that the behaviour of this normal form is rather different from that of the greedy normal form, and many questions arise about the geometry it induces on the Cayley graph of B_n. In particular, it is natural to ask for a possible associated automatic structure. The answer seems to be negative.

Proposition 6.10. (i) *For each n, the set of all (positive) Φ-normal n-strand braid words is rational,* i.e.*, recognized by a finite state automaton.*

(ii) *For $n \geqslant 3$, Φ-normal words do not satisfy the Fellow Traveler Property with respect to multiplication on the right.*

Proof (sketch). (i) By Proposition 4.11, a positive n-strand braid word w is Φ-normal if and only if each letter occurring in w is the smallest σ_i that right divides the braid represented by the prefix finishing at that letter, with respect to an ordering of $\{\sigma_1, \dots, \sigma_{n-1}\}$ that depends on the suffix starting at that letter (actually at the next one). It is easy to construct an automaton that, when reading a braid word, returns the set of all σ_i that right divide the braid represented by that word. Similarly, it is easy to construct a reversed automaton that, reading a braid word from the right, returns the local ordering of $\{\sigma_1, \dots, \sigma_{n-1}\}$ that is involved in the above construction. Standard techniques from the theory of automata enable one to mix both constructions, and to build an automaton that recognizes the family of all Φ-normal n-strand braid words.

(ii) For odd (*resp.* even) $d \geqslant 0$, the Φ-normal form of Δ_3^d is $u_d = \widehat{\Delta}_{3,d}\sigma_1^d$, while that of $\Delta_3^d\sigma_2$ is $v_d = \sigma_1 u_d$ (*resp.* $\sigma_2 u_d$)—as $\widehat{\Delta}_{n,d}$ is a braid that admits a unique positive word representative, there is no danger here in using the same notation for the word and the braid. For $\ell = 1, \dots, 3d+1$, the successive distances between the length ℓ prefixes of u_d and v_d turn out to be

$0, 2, 4, 4, 6, 6, \dots, 2(d-1), 2(d-1), 2d, 2d, 2d, 2(d-1), \dots, 6, 4, 2, 1.$

There is no uniform upper bound for the above distances, hence the k-Fellow Traveler Property of [21] fails for every k. $\square$

Investigating the dynamical properties of the Φ-normal form along the lines of [3, 30, 27, 26, 28] is also a natural task. The generic problem is to study growth and stabilization in random walks through B_n or B_n^+: one compares the successive normal forms, typically looking at whether the first factors become eventually constant. Each new normal form gives rise to a new problem. Let $b(x)$ denote the n-breadth of x, and $c_r(x)$ denote the rth entry, starting from the right, in the n-splitting of x.

Question 6.11. *Let X be the random walk through B_n^+ defined by $X_{k+1} = \sigma_i X_k$ with i equidistributed in $\{1, \dots, n-1\}$. What are the distributions of $\frac{1}{k}b(X_k)$ and $\frac{1}{k}|c_r(X_k)|$ for each fixed r?*

Experiments suggest that the length of $c_0(X_k)$ might grow like $k/(n+2)$, while $c_r(X_k)$ with $r \geqslant 1$ tends to stabilize to $\delta_{n-1}\sigma_1$, of constant length, and $b(X_k)$ might be connected with $\sqrt{k}$.

References

[1] S.I. Adyan, *Fragments of the word Delta in a braid group*, Mat. Zam. Acad. Sci. SSSR **36-1** (1984) 25–34; translated Math. Notes of the Acad. Sci. USSR; 36-1 (1984) 505–510.

[2] E. Artin, *Theory of Braids*, Ann. of Math. **48** (1947) 101–126.

[3] R. Bikbov, S. Nechaev & A. Vershik, *Statistical properties of locally free groups with applications to braid groups and growth of random heaps*, Comm. Math. Phys. **212-2** (2000) 469–501.

[4] J. Birman, K.H. Ko & S.J. Lee, *A new approach to the word problem in the braid groups*, Advances in Math. **139-2** (1998) 322-353.

[5] E. Brieskorn & K. Saito, *Artin-Gruppen und Coxeter-Gruppen*, Invent. Math. **17** (1972) 245–271.

[6] S. Burckel, *Le bon ordre sur les tresses positives*, PhD Thesis, Université de Caen (1994).

[7] S. Burckel, *The wellordering on positive braids*, J. Pure Appl. Algebra **120-1** (1997) 1–17.

[8] S. Burckel, *Computation of the ordinal of braids*, Order **16** (1999) 291–304.

[9] L. Carlucci, P. Dehornoy, A. Weiermann, *Unprovability statements involving braids*, Preprint; arXiv: math.LO/0711.3785.

[10] R. Charney, *Artin groups of finite type are biautomatic*, Math. Ann. **292-4** (1992) 671–683.

[11] R. Charney, J. Meier & K. Whittlesey, *Bestvina's normal form complex and the homology of Garside groups*, Geom. Dedicata **105** (2004) 171-188.

[12] R. Charney & J. Meier, *The language of geodesics for Garside groups*, Math. Zeitschr **248** (2004) 495–509.

[13] P. Dehornoy, *Braid groups and left distributive operations*, Trans. Amer. Math. Soc. **345-1** (1994) 115–151.

[14] P. Dehornoy, *Groupes de Garside*, Ann. Scient. Ec. Norm. Sup. **35** (2002) 267–306.

[15] P. Dehornoy, *Complete positive group presentations*, J. of Algebra **268** (2003) 156–197.

[16] P. Dehornoy, with I. Dynnikov, D. Rolfsen, B. Wiest, *Ordering Braids*, Mathematical Surveys and Monographs, Amer. Math. Soc., to appear.

[17] P. Dehornoy & Y. Lafont, *Homology of Gaussian groups*, Ann. Inst. Fourier **53-2** (2003) 1001–1052.

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

[19] F. Digne & J. Michel, *Garside and locally Garside categories*, Preprint; arXiv: math.GR/0612652.

[20] E. A. Elrifai & H.R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford **45-2** (1994) 479–497.

[21] D. Epstein, J. Cannon, D. Holt, S. Levy, M. Paterson & W. Thurston, *Word Processing in Groups*, Jones & Bartlett Publ. (1992).

[22] J. Fromentin, *The cycling normal form on dual braid monoids*, Preprint; arXiv: math.GR/0712.3836.

[23] F. A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20-78** (1969) 235–254.

[24] C. Kassel & V. Turaev, *Braid groups*, Grad. Texts in Math., Springer (2008).

[25] R. Laver, *Braid group actions on left distributive structures and well-orderings in the braid group*, J. Pure Appl. Algebra **108-1** (1996) 81–98.

[26] J. Mairesse, *Random walks on groups and monoids with a Markovian harmonic measure*, Electron. J. Probab. **10** (2005) 1417–1441.

[27] J. Mairesse & F. Mathéus, *Random walks on free products of cyclic groups*, J. London Math. Soc. **75-1** (2007) 47–66.

[28] J. Mairesse & F. Mathéus, *Randomly growing braid on three strands and the manta ray*, Ann. Appl. Probab. **17-2** (2007) 502–536.

[29] J. Michel, *A note on words in braid monoids*, J. Algebra **215** (1999) 366–377.
[30] S. Nechaev & R. Voituriez, *Random walks on 3-strand braids and on related hyperbolic groups*, J. Phys. A **36-1** (2003) 43–66.
[31] M. Picantin, *The center of thin Gaussian groups*, J. of Algebra **245-1** (2001) 92–122.
[32] M. Picantin, *Automatic structures of torus knot groups*, J. Knot Th. and its Ramif. **12-6** (2003) 833-866.
[33] W. Thurston, *Finite state algorithms for the braid group*, Circulated notes (1988).

Laboratoire de Mathématiques Nicolas Oresme, Université de Caen, 14032 Caen, France
E-mail address: dehornoy@math.unicaen.fr
URL: //www.math.unicaen.fr/∼dehornoy