Alternating normal forms for braids and locally Garside monoids

Patrick Dehornoy

2007-03

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, 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 turns out to coincide 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 canonical well-order of B_n^+ in terms of that of B_{n-1}^+.

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 a decade remain mysterious objects [16]. Here this aim is achieved, at least partially, by giving a new, alternative construction of the Burckel normal form that makes the latter hopefully more natural, and, in any case, very easily computable. However, it turns out that the construction we describe below relies on a very general scheme for which many monoids are eligible, and we may hope for further applications beyond the case of braids.

Following the seminal work of F.A. Garside [22], we know that braid monoids and, more generally, Artin–Tits monoids and Garside monoids that generalize them, can be equipped with a normal form, namely the so-called greedy normal form of [5, 1, 20, 33], which constructs for each element of the monoid a distinguished representative word in terms of some standard generators. The latter normal form is excellent both in theory and in practice in that it provides an automatic structure, and it is easily computable [21, 9, 13].

What we do in this paper is 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 of the considered monoid M, but, instead of taking for A the finite 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_0 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_0 is a proper subset of M, and the construction stops after one step. However, by considering two parabolic submonoids M_1, M_0 which together generate M, we can obtain a well-defined, unique decomposition alternatively involving M_1 and M_0, according to a scheme that is usual in the case of an amalgamated product. By considering convenient families of submonoids, we can iterate the process and finally obtain a unique normal form for each element of M. When it exists, typically for all Artin–Tits monoids, such a normal form

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

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

is exactly as easy to compute as the greedy normal form, and it provides a new solution of quadratic complexity for the word problem.

The above construction is quite general, as it only requires that the ground monoid M is what is now called locally Garside on the right—or locally left Gaussian in the obsolete terminology of [17]. However, our main interest in this paper lies in the application to the specific case of the braid monoids B_n^+. The key result is that, for a convenient choice of the parameters, the alternating normal form turns out to coincide with the Burckel normal form alluded to above. As a consequence, we at last obtain both an easy algebraic description of the latter, and an efficient algorithm for computing it. And, mainly, because of the known connection between the Burckel normal form and the standard well-order of positive braids, we obtain a new characterization of the latter. The result can be summarized as follows:

Theorem. *Let B_n^+ denote the monoid of positive n strand braids. For x in B_{n-1}^+, denote by $x^\#$ the image of x under the shift morphism that maps σ_i to σ_{i+1} for each i. Let ϕ_n denote the flip automorphism of B_n^+ that maps σ_i to σ_{n-i} for each i.*

(i) For every x in B_n^+, there exists a unique sequence $(x_p, ..., x_0)$ with $x_0, ..., x_p$ in B_{n-1}^+ satisfying

$$x = \ldots \cdot x_4 \cdot x_3^\# \cdot x_2 \cdot x_1^\# \cdot x_0$$

such that, for $i \geqslant 1$, the only σ dividing $\ldots \cdot x_{2i+1}^\# \cdot x_{2i}$ on the right is σ_1, and the only σ dividing $\ldots \cdot x_{2i} \cdot x_{2i-1}^\#$ on the right is σ_{n-1}.

(ii) Let $x, y \in B_n^+$. Let $(x_p, ..., x_0)$ and $(y_q, ..., y_0)$ be the decompositions of 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 there exists r satisfying $x_i = y_i$ for $p \geqslant i > r$ and, respectively, $x_r < y_r$ in B_{n-1}^+ if r is even, and $\phi_{n-1}(x_r) < \phi_{n-1}(y_r)$ in B_{n-1}^+ if r is odd.

In other words, via the above decomposition, the well-order on B_n^+ is just a sort of lexicographical extension of the well-order on B_{n-1}^+. As an application, one deduces that (arbitrary) braids can be compared with respect to the braid ordering in quadratic time. In the above statement, (i) is easy, but (ii) is not.

The organization of the paper is as follows. In Section 1, we describe what will be called the alternating decomposition obtained when considering two submonoids of a convenient monoid. In Section 2, we iterate the construction so as to obtain unique normal forms. In Section 3, we concentrate on the specific case of braids and investigate what will be called the flip decomposition and the derived flip normal form. Finally, in Section 4, we show that the flip normal form of braids coincides with the Burckel normal form, and deduce the above mentioned applications to the braid order.

Remark. All constructions developed in this paper involve right divisibility and the derived notions. This choice is dictated by the braid applications of Section 4. Of course, we could use left divisibility instead and obtain symmetric versions for all results, 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 show how to obtain unique decompositions for the elements of monoids in which least common left multiples (left lcm's) exist. The general idea is that, 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 $x = x'x_0$, where x_0 is a maximal right divisor of x lying in A that will be called the A-tail of x. If we assume that every nontrivial (*i.e.*, $\neq 1$) element of M has a nontrivial A-tail, then we can consider the A-tail x_1 of x', and, iterating the process, obtain a decomposition of x as a product of elements of A. This is the situation exploited in the standard greedy normal form for Garside monoids. Here, we shall skip the above additional assumption on A, but instead consider two subsets A_1, A_0 of M with the property that, for every nontrivial element x of M, at least one of the A_1- or A_0-tails of x is nontrivial. In this way, we obtain a distinguished decomposition of x as an alternating product of elements of A_0 and of A_1.

1.1. **Locally Garside monoids.** Divisibility features play the 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 $x \succcurlyeq y$ (or $y \preccurlyeq x$), 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 Garside on the right*, or *right locally 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 $(\mathrm{Div}_R(x), \prec)$.

If M is a right locally 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.

Example 1.3. According to [5] and [29], all Artin–Tits monoids are locally Garside (on both sides). We recall that Artin–Tits monoids are the monoids generated by the elements of a set S subject to relations of the form $sts... = tst...$, both sides of the same length, and with at most one such relation for each pair of generators $\{s, t\}$. An important example is Artin's braid monoid B_n^+ [23], which corresponds to choosing $S = \{\sigma_1, .., \sigma_{n-1}\}$ with the relations,

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

As the name suggests, more general examples of locally Garside monoids are the now standard Garside monoids of [18, 13, 10, 11, 28], which include the torus knot monoids [32], the dual braid monoids [4], and many more.

If M is locally Garside on the right, then no nontrivial element of M is invertible: if we had $xy = 1$ with $x \neq 1$, hence $y \neq 1$, the periodic sequence $x, 1, x, 1, ...$ would contradict (C_3). It follows that the right divisibility relation is antisymmetric, and, therefore, it is a partial ordering on M. As a consequence, the left lcm of two elements, 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 [13] 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.*, $x \prec_L y$ holds if we have $y = xz$ with $z \neq 1$.

Lemma 1.4. (*i*) *If M is right cancellative, Condition (C_3) is equivalent to*
(C_3') *There is no infinite descending chain in $(M, \prec_L)$.*
(*ii*) *In any case, Conditions (C_3) and (C_3') follow from*
(C_3^*) *There exists $\lambda : M \to \mathbb{N}$ such that $x \neq 1$ implies $\lambda(x) \geqslant 1$ and $z = xy$ implies $\lambda(z) \geqslant \lambda(x) + \lambda(y)$.*

Proof. (*i*) Assume that M is right cancellative and (C_3) fails in M. Thus there exists x in M and a sequence $x_0, x_1, ...$ 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 $x = z_n x_n$. Then 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.

Conversely, assume that (C_3') fails in M. Let $z_0, z_1, ...$ is a descending chain for $\prec_L$. For each n, choose $y_n \neq 1$ satisfying $z_n = z_{n+1} y_n$. Let $x = z_0$, $x_0 = 1$, and, inductively, $x_{n+1} = y_n x_n$. Then, 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 x_n's belong to $\mathrm{Div}_R(x)$. Thus the sequence $x_0, x_1, ...$ witnesses that (C_3) fails.

Point (*ii*) should be clear. □

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 for, in this case, we can define $\lambda(x)$ to be the length of any word representing x. This is the case with the Artin–Tits monoids of Example 1.3.

Lemma 1.4 implies that right locally Garside monoids coincide with the monoids called locally left Gaussian in [13], in connection with the left Gaussian monoids of [18]. The reason for changing terminology and left/right orientation is that the current notation is coherent with [19] and, mostly, that it is more natural: right locally 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 right locally Garside monoid. The key point in the sequel is the existence of left lcm's in M. Condition (C_2) in Definition 1.2 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 right locally Garside, and $x \in M$. Then every nonempty subset X of $\mathrm{Div}_R(x)$ admits a global left lcm x_0; if moreover X is closed under left lcm, then x_0 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 has to admit some $\succ$-minimal, *i.e.*, some $\prec$-maximal, element x_0: so $x' x_0 \in X$ implies $x' = 1$. We claim that x_0 is a global left lcm for X. Indeed, let y_0 be any

element of X. By hypothesis, x_0 and y_0 lie in $\mathrm{Div}_R(x)$, so, by (C_2), they admit a left lcm z_0, which can be expressed as $y'y_0 = x'x_0$. The hypothesis that X is closed under left lcm implies $z_0 \in X$. The choice of x_0 implies $x' = 1$, and we conclude that x_0 is a left multiple of y_0.

If we drop the assumption that X is closed under left lcm, we can apply the above result to the closure $\widehat{X}$ of X under left lcm, *i.e.*, to the smallest subset of $\mathrm{Div}_R(x)$ that includes X and is closed under left lcm. Then the global left lcm x_0 of $\widehat{X}$ is a global left lcm for X, but we cannot be sure that x_0 lies in X—yet it is certainly the left lcm of some finite subset of X. □

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

1.2. **The A-tail of an element.** The basic observation is that, for any fixed subset A of the considered monoid M that is closed under left lcm, Lemma 1.5 leads to a distinguished decomposition for every element of M.

Lemma 1.6. *Assume that M is a right locally Garside monoid and A is a subset of M that is closed under left lcm. Then, for each element x of M, there exists a unique right divisor x_0 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 closed under left lcm as it is the intersection of two sets that are closed under left lcm. □

For M, A and x as above, Lemma 1.6 gives a distinguished decomposition

$$x = x'x_0 \tag{1.2}$$

with $x_0 \in A$.

Definition 1.7. For M, A, x, x_0 as in (1.2), the element x_0 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 to the presentation 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. A first, standard choice consists in considering the set Σ of all so-called simple elements in M, namely the divisors of the lcm Δ of S. By construction, Σ is closed under left (and right) divisor, and under left (and right) lcm, and, for every element x of M, the Σ-tail of x is the right gcd of x and Δ.

A second choice consists in considering a subset I of S, and taking for A the so-called standard parabolic submonoid M_I of M generated by I. Then 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, and therefore it is eligible for our approach. In this case, denote by Δ_I the lcm of I. Then, for every element x of M, the M_I-tail x_0 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_0' be the latter gcd, and let $\ell = |x|$. By

definition, x_0 is a right divisor of x, so we have $|x_0| \leqslant \ell$, and, as for every element z of M_I satisfying $|z| \leqslant \ell$ is, we have $\Delta_I^\ell \succcurlyeq x_0'$, hence $x_0' \succcurlyeq x_0$. Conversely, x_0' is an element of $\mathrm{Div}_R(x) \cap M_I$, hence we have $x_0 \succcurlyeq x_0'$, and, finally, $x_0 = x_0'$. Observe 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 the powers of Δ_I vanishes.

1.3. **Alternating decompositions.** In the second case considered in Example 1.8, the involved closed subset is a submonoid of M, *i.e.*, in addition to being closed under left lcm, it is closed under multiplication and contains 1. This is the case on which we shall concentrate now. Then, the decomposition of Lemma 1.6 takes a more specific form.

Definition 1.9. Assume that M is a right locally Garside. We say that a submonoid M_0 of M is *closed* if it is closed under both left lcm and left divisor, *i.e.*, every left lcm of elements of M_0 belongs to M_0 and every left divisor of an element of M_0 belongs to M_0.

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 under left lcm and left divisor. This need not be the case in a general right locally Garside monoid, or even in a Garside monoid. For instance, the monoid $\langle a, b \ ; \ aba = b^2 \rangle^+$ is Garside, hence locally Garside on the right—and 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 nontrivial 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 right locally Garside monoid and M_0 is a closed submonoid of M. Then every element x of M admits a unique decomposition $x = x'x_0$ satisfying*

$$x_0 \in M_0 \quad \text{and} \quad x' \perp M_0; \tag{1.3}$$

The elements x_0 and x' are determined by $x_0 = \mathrm{tail}(x, M_0)$ and $x' = x/x_0$.

Proof. Let $x_0 = \mathrm{tail}(x, M_0)$ and $x' = x/x_0$. We claim that, for each decomposition $x = y'y_0$ with $y_0 \in M_0$, we have

$$y_0 = x_0 \iff y' \perp M_0. \tag{1.4}$$

First, assume $z \in \mathrm{Div}_R(x') \cap M_0$. Then we have $x' = x''z$ for some x'', hence $x = x''zx_0$, and $zx_0 \in \mathrm{Div}_R(x)$. As z and x_0 belong to M_0 and the latter is a submonoid of M, we deduce $zx_0 \in M_0$, hence $z = 1$ by definition of x_0. So $x' \perp M_0$ holds, and the direct implication in (1.4) is true.

Conversely, assume $x = y'y_0$ with $y_0 \in M_0$. By definition of the M_0-tail, y_0 is a right divisor of x_0, *i.e.*, we have $x_0 = zy_0$ for some z. As z is a left divisor of x_0, the assumption that M_0 is closed under left divisor implies $z \in M_0$. Then we find $y'y_0 = x = x'x_0 = x'zy_0$, hence $y' = x'z$ by cancelling y_0 on the right, and finally $z \in \mathrm{Div}_R(y') \cap M_0$. Then $\mathrm{Div}_R(y') \cap M_0 = \{1\}$ implies $z = 1$, *i.e.*, $y_0 = x_0$, and, from there, $y' = x'$. So the converse implication in (1.4) is true. □

Assume now that M is locally Garside on the right, that M_0, M_1 are two closed submonoids of M, and x belongs to M. By Lemma 1.12, we have a distinguished

decomposition $x = x'x_0$ involving the maximal right divisor of x that lies in M_0. If x' is not 1, and if M_1 is sufficiently distinct from M_0, in some sense to be made precise, it might be that the M_1-tail of x' is not 1, and we obtain a new decomposition $x = x''x_1x_0$ with $x_1 \in M_1$ and $x_0 \in M_0$. If x'' is not 1, we can iterate the process, and, in this way, obtain, in good cases, a decomposition of x as an alternating product of elements of M_0 and M_1.

Definition 1.13. Assume that M is a right locally Garside. We say that (M_1, M_0) is a *covering* of M if M_1, M_0 are closed submonoids of M and, moreover, $M_1 \cup M_0$ generates M (as a monoid).

Example 1.14. Let M be an Artin–Tits monoid with standard set of generators S, and let S_0, S_1 be two subsets of S satisfying $S_1 \cup S_0 = S$. For $i = 1, 0$, let M_i be the standard parabolic submonoid of M generated by S_i. Then (M_1, M_0) is a covering of M. Indeed, we already mentioned that M_0 and M_1 are closed submonoids of M. Moreover, S is included in $M_1 \cup M_0$, so the latter certainly generates M.

Similar results hold for any a right locally Garside generated by a set S when we consider subsets S_1, S_0 of S satisfying $S_1 \cup S_0 = S$ and we define M_i to be the smallest *closed* submonoid of M generated by S_i.

Notation 1.15. For each (nonnegative) integer, we denote by $[i]$ the unique element of $\{1, 0\}$ that is equal to i mod 2.

Then we can easily establish the existence of an alternating decomposition of the expected type.

Proposition 1.16. *Assume that M is a right locally Garside monoid and (M_1, M_0) is a covering of M. Then, for every nontrivial element x of M, there exists a unique finite sequence $(x_p, ..., x_0)$ satisfying $x = x_p...x_0$ with $x_p \neq 1$ and, for each i,*

$$x_i \in M_{[i]} \quad \text{and} \quad x_p...x_{i+1} \perp M_{[i]}. \tag{1.5}$$

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

$$x_i := \mathrm{tail}(x^{(i)}, M_{[i]}) \quad \text{and} \quad x^{(i+1)} := x^{(i)}/x_i. \tag{1.6}$$

Moreover, we have $x_i \neq 1$ for $p \geqslant i \geqslant 1$,

Proof. Let x belong to M, and let x_i, $x^{(i)}$ be the elements specified by (1.6). We first prove the relations

$$x = x^{(i+1)}x_i \cdots x_0, \tag{1.7}$$

$$x^{(i+1)} \perp M_{[i]} \tag{1.8}$$

for every $i \geqslant 0$ using induction on i. For $i = 0$, Lemma 1.12 for x and M_0 gives $x = x^{(1)}x_0$, which is (1.7), and $x^{(1)} \perp M_0$, which is (1.8). Assume $i \geqslant 1$. By definition, we have $x_i = \mathrm{tail}(x^{(i)}, M_{[i]})$ and $x^{(i+1)} = x^{(i)}/x_i$, hence $x^{(i)} = x^{(i+1)}x_i$ by construction. Susbtituting in $x = x^{(i)}x_{i-1}...x_0$, which holds by induction hypothesis, we obtain (1.7). Moreover, Lemma 1.12 for $x^{(i)}$ and $M_{[i]}$ gives (1.8).

By construction, the sequence x_0, x_1x_0, $x_2x_1x_0$, ... is increasing in $(\mathrm{Div}_R(x), \prec)$. By Condition (C_3), it must be eventually constant. By right cancellability, this implies that there exists p such that $x_i = x^{(i)} = 1$ holds for all $i \geqslant p$. Then (1.7) implies $x = x_p...x_0$, with $x_p \neq 1$ provided p is chosen to be minimal and x is not 1.

At this point, we proved that the expected sequence $(x_p, ..., x_0)$ exists and satisfies (1.5) and (1.6). We show now that $x_i \neq 1$ holds for all i with $p \geqslant i \geqslant 1$. Indeed, assume $x^{(i+1)} \neq 1$. By hypothesis, $M_1 \cup M_0$ generates M, hence we must have $x^{(i+1)} \not\perp (M_1 \cup M_0)$. By (1.8), we have $x^{(i+1)} \perp M_{[i]}$, hence $x^{(i+1)} \not\perp M_{[i+1]}$. Therefore the $M_{[i+1]}$-tail of $x^{(i+1)}$, which by definition is x_{i+1}, is not 1. (Observe that $x_0 = 1$ does not imply $x = x^{(0)} = 1$ because $x^{(0)} \perp M_1$ need not hold).

We turn to uniqueness. Consider any decomposition $x = y_q...y_0$ satisfying $y_q \neq 1$ with $y_i \in M_{[i]}$ and $y_q...y_{i+1} \perp M_{[i]}$ for each i. We inductively prove that $y_i = x_i$ and $y_q...y_{i+1} = x^{(i+1)}$ hold for $i \geqslant 0$. For $i = 0$, by hypothesis, we have $x = (y_q...y_1)y_0$ with $y_0 \in M_0$ and $y_q...y_1 \perp M_0$, so Lemma 1.12 implies $y_0 = x_0$ and $y_q...y_1 = x^{(1)}$. Assume $i \geqslant 1$. By induction hypothesis, we have $y_q...y_i = x^{(i)}$, and the hypotheses about the y_j's give $x^{(i)} = (y_q...y_{i+1})y_i$ with $y_i \in M_{[i]}$ and $y_q...y_{i+1} \perp M_{[i]}$. Then Lemma 1.12 again implies $y_i = \mathrm{tail}(x^{(i)}, M_{[i]}) = x_i$ and $y_q...y_{i+1} = x^{(i)}/x_i = x^{(i+1)}$. This completes the proof, as $q > p$ 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 $(x_p, ..., x_0)$ is called the (alternating) (M_1, M_0)-*decomposition* of x.

Example 1.18. Let M be the 4 strand braid monoid B_4^+. Let M_0 be the submonoid generated by σ_1 and σ_2, *i.e.*, B_3^+, and M_1 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_1, M_0)-decomposition of x is as follows:

$$\begin{aligned}
x &= \Delta_4^2 & x_0 &= \mathrm{tail}(x, M_0) = \Delta_3^2,\\
x^{(1)} &= x/x_0 = \sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3 & x_1 &= \mathrm{tail}(x^{(1)}, M_1) = \sigma_2\sigma_3,\\
x^{(2)} &= x^{(1)}/x_1 = \sigma_3\sigma_2\sigma_1^2 & x_2 &= \mathrm{tail}(x^{(2)}, M_0) = \sigma_2\sigma_1^2,\\
x^{(3)} &= x^{(2)}/x_2 = \sigma_3 & x_3 &= \mathrm{tail}(x^{(3)}, M_1) = \sigma_3,\\
x^{(4)} &= x^{(3)}/x_3 = 1,
\end{aligned}$$

and the computation stops. Thus the (M_1, M_0)-decomposition of Δ_4^2 is the sequence

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

Note that the decomposition changes when the submonoids are switched. For instance, the (M_0, M_1)-decomposition of Δ_4^2 is $(\sigma_1, \sigma_2\sigma_3^2, \sigma_2\sigma_1, (\sigma_2\sigma_3\sigma_2)^2)$.

Remark. Instead of considering two closed submonoids (M_1, M_0) of M, we could also consider any finite family of such submonoids $(M_{m-1}, ..., M_0)$. Provided the union of these submonoids generates M, we can extend Proposition 1.16 and obtain for every element x of M a distinguished decomposition $x = x_p...x_0$ such that x_i belongs to $M_{[i]}$ and $x_p...x_{i+1} \perp M_{[i]}$ holds for every i, where $[i]$ now denotes the unique element of $\{0, ..., m-1\}$ that is equal to i mod m. The only difference is that the condition $x_i \neq 1$ for $i \geqslant 1$ has to be relaxed to $x_{i+m-2}...x_i \neq 1$, because the conjunction of $x \neq 1$ and $x \perp M_{[i]}$ need not guarantee $x \not\perp M_{[i+1]}$, but only $x \not\perp (M_{[i+m-2]} \cup ... \cup M_{[i+1]})$. Adapting is easy.

1.4. **Algorithmic aspects.** Computing the alternating decomposition is algorithmically easy provided one can efficiently perform right division in the reference 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, if S generates a monoid M, we denote by S^* the set of all words on S, and, for w in S^*, we denote by $\overline{w}$ the element of M represented by w.

Definition 1.19. Assume that M is a right locally Garside monoid satisfying Condition (C_3^*), and S generates M. For w a word on S, we define the *norm* $\|w\|$ of w to be 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. In the case of Artin–Tits monoids and, more generally, of monoids presented by homogeneous relations, $\|w\|$ coincides with the length $|w|$.

Proposition 1.20. *Assume that M is a right locally Garside monoid generated by some finite set S, satisfying Condition (C_3^*) and the following condition:*

> $(*)$ *There exists an algorithm A that, for each word w in S^* and each letter s in S, runs in time $O(\|w\|)$, recognizing if $\overline{w} \succcurlyeq s$ holds and, if so, returning a word representing $\overline{w}s^{-1}$.*

Let $S_1, S_0 \subseteq S$ satisfying $S_1 \cup S_0 = S$. Let M_i be the submonoid of M generated by S_i, and suppose that M_1, M_0 are closed. Then there exists a algorithm that, for w in S^*, runs in time $O(\|w\|^2)$ and computes the (M_1, M_0)-decomposition of $\overline{w}$.

Proof. Having listed the elements of S_0 and S_1, and starting with w, we use A to divide by elements of S_0 until division fails, then we divide by elements of S_1 until division fails, *etc.* We stop when the remainder is 1. As for complexity, the point is that, if we start with a word w of norm ℓ, then the words subsequently occurring represent the elements $x^{(i)}$ of (1.6), which are left divisors of x, and, hence, their norm, and therefore their length in the letters of S, is bounded above by ℓ. At each step, the norm 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 1.21. 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, namely those involving a rational transducer based on the (right) automatic structure [21]. For the specific question of dividing by an atom, the reversing method of [14] is specially convenient for a practical implemention.

2. Iterated alternating decompositions

At this point, we obtained distinguished decompositions for every element in a right locally Garside M, but, in general, these decompositions do not yet provide unique normal forms, unless some unique normal form is known in each of the component submonoids M_1, M_0. One case when such a normal form certainly exists is when the considered submonoids M_i are monogenerated: the hypothesis that M has no nontrivial invertible element and is right cancellative implies that M is torsion free, so, in the case above, there exists a (unique) element s_i such that each element of M_i is uniquely expressed as s_i^e for some exponent $e \geqslant 0$. Such a situation occurs when M is the 3 strand braid monoid B_3^+, and M_1, M_0 are the submonoids respectively generated by σ_2 and σ_1. Then the (M_1, M_0)-decomposition yields a unique distinguished word in the letters σ_1, σ_2 for each braid in B_3^+. For instance,

the normal form of Δ_3^2 happens to be the word $\sigma_2\sigma_1^2\sigma_2\sigma_1^2$, an example suggesting that the normal form we are now addressing is rather different from the classical greedy normal form, here $\Delta_3 \cdot \Delta_3$.

The obvious idea we develop below is to iterate the alternating decomposition of Section 1 so as to always reach the above situation of monogenerated submonoids, and, in this way, obtain unique representative for every element of the considered initial monoid.

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

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

Proof. Assume M_0 is a closed submonoid of some right locally Garside monoid M. First, M_0 admits right cancellation as every submonoid of a right cancellative monoid does. Then, if x, y belong to M_0 and they admit a common left multiple z in M_0, 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_0 is closed under left lcm implies that z' belongs to M_0, and, then, z' must be a left lcm for x and y in the sense of M_0. Finally, the right divisibility relation of M_0 is included in the right divisibility relation of M, so a sequence contradicting Condition (C_3) in M_0 would also contradict (C_3) in M. □

Now, assume that M is a right locally Garside and (M_1, M_0) is a covering of M. By Lemma 2.1, M_1 and M_0 are locally Garside on the right, and we can repeat the process: assuming that $(M_{i,1}, M_{i,0})$ is a covering of M_i for $i = 1, 0$, every element of M_i admits a $(M_{i,1}, M_{i,0})$-decomposition, and, therefore, every element of M admits a distinguished decomposition in terms of elements of the four monoids M_{11}, M_{10}, M_{01}, and M_{00}—we drop commas in indices.

Example 2.2. As in Example 1.18, let M be the 4 strand braid monoid B_4^+, and let M_1, M_0 be the parabolic submonoids of M respectively generated by σ_3, σ_2, and by σ_2, σ_1. Then let M_{11}, M_{10}, M_{01}, and M_{00} be the submonoids respectively generated by σ_2, σ_3, σ_2, and σ_1. Then (M_{i1}, M_{i0}) is a covering of M_i for $i = 1, 0$, and the iterated alternating decomposition of Δ_4^2 with respect to the above coverings turns out to be the sequence of sequences

$$((\sigma_3)\,,\,(\sigma_2, \sigma_1^2)\,,\,(\sigma_2, \sigma_3)\,,\,(\sigma_2, \sigma_1^2, \sigma_2, \sigma_1^2)), \tag{2.1}$$

which corresponds to the iterated factorization

$$\Delta_4^2 = (\sigma_3) \cdot (\sigma_2 \cdot \sigma_1^2) \cdot (\sigma_2 \cdot \sigma_3) \cdot (\sigma_2 \cdot \sigma_1^2 \cdot \sigma_2 \cdot \sigma_1^2). \tag{2.2}$$

The process can then be iterated, and we directly go to the general case involving 2^n submonoids. In the sequel, we frequently have to use finite sequences of natural numbers, in particular, finite sequences of 0's and 1's, and we fix some notation.

Notation 2.3. (i) A length n sequence of natural numbers (*resp.* of 0's and 1's) is called a *n-address* (*resp.* a *binary n-address*); the empty address, *i.e.*, the unique 0-address, is denoted $\varnothing$. If α, β are addresses, $\alpha\beta$ denotes the concatenation of α and β, *i.e.*, the address obtained by appending β after α; we say that α is a *prefix* of γ if $\gamma = \alpha\beta$ holds for some β.

(ii) If θ is an address, we denote by $[\theta]$ the binary address obtained by replacing each number by its class mod 2.

When dealing with examples of addresses, we drop brackets and separating commas. For instance, a typical 4-address is $\theta = 5213$ and, then, we have $[\theta] = 1011$.

Definition 2.4. Assume that M is a right locally Garside monoid. A family $(M_\alpha)_\alpha$ indexed by binary m-addresses with $m \leqslant n$ is called a *n-covering* of M if $(M_{\alpha 1}, M_{\alpha 0})$ is a covering of M_α for each binary m-address α with $m < n$, and $M_\varnothing = M$ holds.

In the sequel, we write $\boldsymbol{M}$ for a generic covering (viewed as a sequence of monoids), and, then, use M_α for the α-entry in $\boldsymbol{M}$.

So what was previously called a covering is a 1-covering. When the monoid M has some distinguished generating set S, we can specify an n-covering by choosing a subset S_α of S for each binary n-address α, and, for β an m-address with $m \leqslant n$, defining M_β to be the submonoid generated by all S_α with β a prefix of α. We obtain an n-covering whenever each of the submonoids M_β turns out to be closed. For such coverings, we can display the inclusions by drawing a binary tree—which can be called the *skeleton* of the covering—as shown in Figure 1.

Example 2.5. In the case of an Artin–Tits monoid, every subset of the standard generating set generates a closed submonoid, and the above approach is relevant. For instance, the 2-covering of B_4^+ mentioned above correspond to choosing

$$S_{11} = S_{01} = \{\sigma_2\}, \quad S_{10} = \{\sigma_3\}, \quad S_{00} = \{\sigma_1\}$$

—this specific covering will be considered many times in the sequel. Writing $\langle X \rangle$ for the submonoid generated by X, we find

$$B^+_{4,11} = B^+_{4,01} := \langle \sigma_2 \rangle, \quad B^+_{4,10} = \langle \sigma_3 \rangle, \quad B^+_{4,00} = \langle \sigma_1 \rangle \ (= B_2^+),$$

whence $B^+_{4,1} = \langle \sigma_2, \sigma_3 \rangle$, $B^+_{4,0} = \langle \sigma_1, \sigma_2 \rangle$ $(= B_3^+)$, and $B^+_{4,\varnothing} = \langle \sigma_1, \sigma_2, \sigma_3 \rangle = B_4^+$.

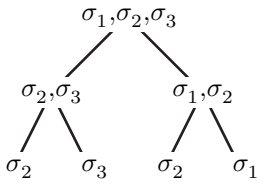

FIGURE 1. Skeleton of the 2-covering of B_4^+ of Example 2.5: a depth 2 binary tree displaying the inclusions between the generating sets of the successive submonoids.

In order to describe iterated decompositions such as the one of (2.1), *i.e.*, for dealing with sequences of sequences, we introduce some more notation.

Definition 2.6. For A a set and $n \geqslant 0$, we define a *n-sequence in A* to be an element of A for $n = 0$, and a finite sequence of $(n-1)$-sequences in A for $n \geqslant 1$. If $\boldsymbol{w}$ is an n-sequence with $n \geqslant 1$, we define the *unbracketing* of $\boldsymbol{w}$ to be the ordinary sequence—*i.e.*, the 1-sequence—obtained from $\boldsymbol{w}$ by removing all brackets except the first and the last ones; we use $|\boldsymbol{w}|$ for the length of $\boldsymbol{w}$, as a sequence of $(n-1)$-sequences.

A 1-sequence in A is just an ordinary sequence in A, while $((2,1),(0),(3,2))$ is a typical 2-sequence in $\mathbb{N}$. Its unbracketing is the sequence $(2,1,0,3,2)$. Similarly, the expression in (2.1) is a 2-sequence in B_4^+. With these notions at hand, we can define the general iterated decomposition formally:

Definition 2.7. Assume that M is a right locally Garside monoid and $\boldsymbol{M}$ is an n-covering of M. For x in M, we define the *iterated $\boldsymbol{M}$-decomposition* $D_{\boldsymbol{M}}(x)$ of x to be the n-sequence defined by $D_{\boldsymbol{M}}(x) = x$ for $n = 0$, and, inductively,

$$D_{\boldsymbol{M}}(x) = (D_{\boldsymbol{M}_{[p]}}(x_p)\,,\,\dots\,,\,D_{\boldsymbol{M}_0}(x_0)), \tag{2.3}$$

where $(x_p, ..., x_0)$ is the (M_1, M_0)-decomposition of x, and $\boldsymbol{M}_i$ is the $(n-1)$-covering of M_i such that the α-component of $\boldsymbol{M}_i$ is $M_{i\alpha}$ for α an $(n-1)$-address. The unbracketing $D^\circ_{\boldsymbol{M}}(x)$ of $D_{\boldsymbol{M}}(x)$ is called the *$\boldsymbol{M}$-decomposition* of x.

For instance, if $\boldsymbol{M}$ is the 2-covering of B_4^+ of Example 2.5, the results previously established can be summarized as

$$D_{\boldsymbol{M}}(\Delta_4^2) = ((\sigma_3), (\sigma_2, \sigma_1^2), (\sigma_2, \sigma_3), (\sigma_2, \sigma_1^2, \sigma_2, \sigma_1^2)), \tag{2.4}$$

$$D^\circ_{\boldsymbol{M}}(\Delta_4^2) = (\sigma_3, \sigma_2, \sigma_1^2, \sigma_2, \sigma_3, \sigma_2, \sigma_1^2, \sigma_2, \sigma_1^2). \tag{2.5}$$

In an ordinary sequence, entries are indexed by natural numbers. In an n-sequence, entries are naturally indexed by n-addresses, *i.e.*, by length n sequences of natural numbers.

Definition 2.8. If $\boldsymbol{w}$ is an n-sequence, and θ is an m-address with $m \leqslant n$, the *θ-subsequence* $\boldsymbol{w}_\theta$ of $\boldsymbol{w}$ is the $(n-m)$-sequence defined by $\boldsymbol{w}_\varnothing = \boldsymbol{w}$ and $\boldsymbol{w}_{i\gamma} = (\boldsymbol{w}_i)_\gamma$ for i in $\mathbb{N}$ and γ a $(n-1)$-address. We say that θ is an address in $\boldsymbol{w}$ if the θ-subsequence of $\boldsymbol{w}$ is defined. The sequence made by all n-addresses in $\boldsymbol{w}$ enumerated from left to right is called the *address list* of $\boldsymbol{w}$.

In this way, every entry in an n-sequence $\boldsymbol{w}$ is indexed by an n-address that describes its position in the successive blocks, *i.e.*, equivalently, in the tree associated with $\boldsymbol{w}$ as in Figure 2. Note that the address list is just another way of specifying the brackets and, therefore, an n-sequence is determined by its address list and its unbracketing—this could be used as an alternative definition. For instance, in (2.1), the address list and the unbracketing, *i.e.*, the entry list, are

$$(30, 21, 20, 11, 10, 03, 02, 01, 00) \quad \text{and} \quad (\sigma_3, \sigma_2, \sigma_1^2, \sigma_2, \sigma_3, \sigma_2, \sigma_1^2, \sigma_2, \sigma_1^2). \tag{2.6}$$

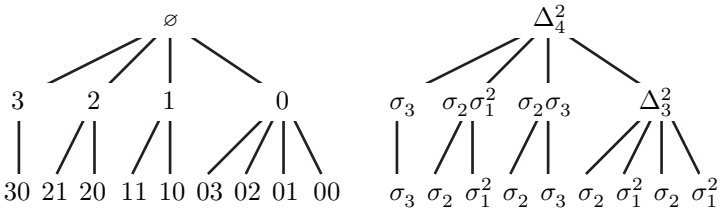

FIGURE 2. The tree associated with the 2-sequence of (2.1), repeated twice: on the left, the addresses are displayed, on the right, the product of the corresponding subsequences are shown; the address list specifies the shape of the tree, and the entry list specifies the name of the leaves; for instance, we see that the 20-subsequence is σ_1^2, while the product of the 1-subsequence is $\sigma_2\sigma_3$. The 23-subsequence does not exist, as 23 is not an address in the considered 2-sequence.

With the previous notation, iterating Proposition 1.16 immediately leads to:

Proposition 2.9. *Assume that M is a right locally Garside monoid and $\boldsymbol{M}$ is an n-covering of M. Let x be an element of M, and let $\boldsymbol{w}$ be the iterated $\boldsymbol{M}$-decomposition of x. For each address θ in $\boldsymbol{w}$, let x_θ denote the product of $\boldsymbol{w}_\theta$. Then, for each m-address θ in $\boldsymbol{w}$ with $m < n$, the sequence $(x_{\theta p}, ..., x_{\theta 0})$ is the $(M_{[\theta 1]}, M_{[\theta 0]})$-decomposition of x_θ, where $\theta p, ..., \theta 0$ are the $(m+1)$-addresses in $\boldsymbol{w}$ of which θ is a prefix. The elements $x_{\theta i}$ are determined from $x_\theta^{(0)} := x_\theta$ by*

$$x_{\theta i} = \mathrm{tail}(x_\theta^{(i)}, M_{[\theta i]}) \quad \text{and} \quad x_\theta^{(i+1)} = x_\theta^{(i)} / x_{\theta i}. \tag{2.7}$$

Example 2.10. For the $\boldsymbol{M}$-decomposition of Δ_4^2 considered in (2.4), typical instances of (2.7) are

$$x_0 = \sigma_2\sigma_1^2\sigma_2\sigma_1^2 = \mathrm{tail}(x, B_3^+), \quad x_1 = \sigma_2\sigma_3 = \mathrm{tail}(\sigma_3\sigma_2\sigma_1^1\sigma_2\sigma_3, \langle\sigma_2, \sigma_3\rangle), ...$$

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

$$x_{00} = \sigma_1^2 = \mathrm{tail}(\sigma_2\sigma_1^2\sigma_2\sigma_1^2, B_2^+), \quad x_{01} = \sigma_2 = \mathrm{tail}(\sigma_2\sigma_1^2\sigma_2, \langle\sigma_2\rangle), ...$$

which only involve the element x_0, namely $\sigma_2\sigma_1^2\sigma_2\sigma_1^2$, and not the whole of x.

2.2. **Global characterization.** As can be seen in Example 2.10, Proposition 2.9 is intricate and not satisfactory in that it does not give a global characterization of what the decomposition is and how to obtain it in one step. This is what we shall do now. The point is to observe that there is no need of considering local remainders when computing iterated tails. This is expressed in the following result, which is vaguely parallel to the formula $\mathrm{tail}(zy, \Sigma_n) = \mathrm{tail}(\mathrm{tail}(z, \Sigma_n)y, \Sigma_n)$ with Σ_n the family of simple braids that is crucial in the construction of the right greedy normal form in a Garside group.

Lemma 2.11. *Assume M is a right locally Garside monoid, M_0 is a closed submonoid of M, and M_{00} is a closed submonoid of M_0. Then, for each left divisor y of $\mathrm{tail}(z, M_0)$, we have*

$$\mathrm{tail}((z/\mathrm{tail}(z, M_0))y, M_{00}). = \mathrm{tail}(y, M_{00}). \tag{2.8}$$

Proof. Put $z_0 = \mathrm{tail}(z, M_0)$ and $z' = z/z_0$. By definition, $\mathrm{tail}(y, M_{00})$ is a right divisor of $\mathrm{tail}(z'y, M_{00})$, hence the point is to prove that every right divisor of $z'y$ lying in M_{00} is a right divisor of y. So assume $z'y = x'x$ with $x \in M_{00}$. By hypothesis, we have $z_0 = yz_0'$ for some z_0', necessarily lying in M_0. Then, we have $z = z'z_0 = z'yz_0' = x'xz_0'$. Now $x \in M_{00}$ implies $x \in M_0$, hence $xz_0' \in M_0$, and xz_0' has to be a right divisor of $\mathrm{tail}(z, M_0)$, *i.e.*, of z_0, which is also yz_0'. It follows that x is a right divisor of y, as was expected. □

In particular, when we choose y to be z_0 itself, (2.8) gives

$$\mathrm{tail}(z, M_{00}) = \mathrm{tail}(\mathrm{tail}(z, M_0), M_{00}). \tag{2.9}$$

We aim at giving a direct description of the $\boldsymbol{M}$-decomposition without mentioning the intermediate values x_α. Consider the case of Examples 2.5 and 2.10 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; now, 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 can be either a block of σ_1's or a block of σ_3's. The only way to decide is to know the current address, *i.e.*, the current position in (the skeleton of) the covering as in Figure 1, typically to

know to which of the two occurrences of σ_2 in the tree of Figure 1 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 1, a block of σ_1's is to be expected, while a block of σ_3's is to be expected on the left of a block of σ_2's associated with the leftmost σ_2. This is precisely what Proposition 2.14 below will say, namely that the $\boldsymbol{M}$-decomposition can be obtained directly provided we keep track of some position specified by a binary address.

In order to browse through trees, we need the following notion of successors of a (binary) address. It comes in two versions, according to whether we consider general addresses, or binary addresses.

Definition 2.12. 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 0's, *i.e.*, for $\theta = d_1...d_n$, the m-successor is $d'_1...d'_n$ with $d'_i = d_i$ for $i \leqslant m$, and, if $m < n$ holds, $d'_{m+1} = d_{m+1} + 1$ and $d'_i = 0$ for $i > m+1$. For α a binary n-address and $0 \leqslant m \leqslant n$, the *binary m-successor* $\alpha^{[m]}$ of α is defined to be $[\alpha^{(m)}]$, *i.e.*, the addition of 1 is taken mod 2.

Example 2.13. Let $\theta = 2501$. The successors of θ are

$$\theta^{(0)} = 3000, \quad \theta^{(1)} = 2600, \quad \theta^{(2)} = 2510, \quad \theta^{(3)} = 2502, \quad \theta^{(4)} = 2501.$$

Similarly, the binary successors of $\alpha = 0101$ are

$$\alpha^{(0)} = 1000, \quad \alpha^{(1)} = 0000, \quad \alpha^{(2)} = 0110, \quad \alpha^{(3)} = 0100, \quad \alpha^{(4)} = 0101.$$

Note that $\theta^{(n)} = \theta$ holds for every n-address θ, and that, if θ', θ are adjacent entries in the address list of an n-sequence, θ' is one of the successors of θ. Here comes the main result stating that the $\boldsymbol{M}$-decomposition can be computed directly:

Proposition 2.14. *Assume that M is a right locally Garside monoid and $\boldsymbol{M}$ is an n-covering of M. Then, for every element x of M, the entry list $(x_p, ..., x_0)$ and the address list $(\theta_p, ..., \theta_0)$ of $D_{\boldsymbol{M}}(x)$ are inductively determined from $x^{(0)} = x$ and $\theta_0 = 0$ by*

$$x_i := \mathrm{tail}(x^{(k)}, M_{[\theta_i]}) \ , \quad x^{(i+1)} := x^{(i)}/x_i \ , \text{ and } \quad \theta_{i+1} = \theta_i^{(m)}, \tag{2.10}$$

where m is the length of the longest prefix θ of θ_i that satisfies $x^{(i+1)} \not\perp M_{[\theta]}$.

Proof. We use induction on n. 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_i is i, the longest prefix of θ_i satisfying $x^{(i+1)} \not\perp M_{[\theta]}$ is $\varnothing$, and the inductive formula reduces to $\theta_{i+1} = i + 1$.

Assume $n \geqslant 2$. Let $(y_q, ..., y_0)$ be the (M_1, M_0)-decomposition of x. By definition, we have

$$D_{\boldsymbol{M}}(x) = (D_{\boldsymbol{M}_{[q]}}(y_q) \, , \, \dots \, , \, D_{\boldsymbol{M}_0}(y_0)). \tag{2.11}$$

For $q \geqslant j \geqslant 0$, let $(y_{j,p_j}, ..., y_{j,0})$ and $(\theta_{j,p_j}, ..., \theta_{j,0})$ be the entry list and the address list in $D_{\boldsymbol{M}_{[j]}}(y_j)$. Then, by (2.11), we have

$$(x_p, ..., x_0) = (y_{q,p_q}, ..., y_{q,0}) \frown \dots \frown (y_{0,p_0}, ..., y_{0,0}), \tag{2.12}$$

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

$$(\theta_p, ..., \theta_0) = (q\theta_{q,p_q}, ..., q\theta_{q,0}) \frown \dots \frown (0\theta_{0,p_0}, ..., 0\theta_{0,0}). \tag{2.13}$$

By induction hypothesis, the sequences of y_j's and $\theta_{j,k}$'s satisfy the counterpart of (2.10), and we wish to deduce (2.10), *i.e.*, dropping the elements $x^{(i)}$, we wish to prove

$$x_i = \mathrm{tail}(x_p...x_i, M_{\theta_i}) \quad \text{and} \quad \theta_{i+1} = \theta_i^{(m)}$$

where m is the length of the maximal prefix θ of θ_i for which $M_{[\theta]} \not\perp x_p...x_{i+1}$ holds. We argue using induction on $i \geqslant 0$.

We begin with the value of x_i. Assume that, in (2.12), x_i corresponds to some entry $y_{j,k}$. Then, by construction, we have $\theta_i = j\theta_{j,k}$. Let $y := y_{j,p_j}...y_{j,k}$. By induction hypothesis, we have

$$x_i = y_{j,k} = \mathrm{tail}(y, M_{[j\theta_{j,k}]}) = \mathrm{tail}(y, M_{[\theta_i]}). \tag{2.14}$$

On the other hand, by construction, y is a left divisor of $y_{j,p_j}...y_{j,0}$, *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

$$y_j = \mathrm{tail}(z, M_{[j]}). \tag{2.15}$$

Applying Lemma 2.11 to the monoids $M_{[\theta_i]} \subseteq M_{[j]} \subseteq M$, we deduce from (2.14) and (2.15) the relation $x_i = \mathrm{tail}((z/y_j)y, M_{[\theta_i]})$, which is also $x_i = \mathrm{tail}(x_p...x_i, M_{[\theta_i]})$, as, by construction, $(z/y_j)y = x_p...x_i$ holds.

We consider now the value of θ_{i+1}. Here, two cases are possible, according to whether x_i corresponds to an initial entry or non-initial entry in some sequence of y's, *i.e.*, with the above notation, according to whether $p_j = k$ holds or not. Assume first $p_j > k$. 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 $M_{[j\theta]} \not\perp y_{j,p_j}...y_{j,k+1}$ holds. The latter relation is equivalent to $M_{[j\theta]} \not\perp x_p...x_{i+1}$: indeed, $M \not\perp x$ is equivalent to $\mathrm{tail}(x, M) \neq 1$, and, as above, Lemma 2.11 implies $\mathrm{tail}(x_p...x_{i+1}, M_{[j\theta]}) = \mathrm{tail}(y_{j,p_j}...y_{j,k+1}, M_{[j\theta]})$. Therefore, θ_{i+1}, which is $j\theta_{j,k+1}$, is the $m+1$-successor of $j\theta_{j,k}$, *i.e.*, of θ_i, where m is the length of the maximal prefix θ of $\theta_{j,k}$ for which $M_{[j\theta]} \not\perp x_p...x_{i+1}$ holds, hence $m+1$ is the length of the maximal prefix θ' of θ_i (namely $j\theta$) for which $M_{[\theta']} \not\perp x_p...x_{i+1}$ holds.

Finally, assume $p_j = k$, *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 $\theta_{i+1} = (j+1)0^{n-1}$. Now, the hypothesis means that $y_q...y_{j+1} \perp M_{[j]}$ holds, *i.e.*, that $x_p...x_{i+1} \perp M_{[j]}$. So, in this case, the only prefix θ of θ_i, *i.e.*, of $j\theta_{j,p_j}$, for which $x_p...x_{i+1} \not\perp M_{[\theta]}$ may hold is the empty address $\varnothing$, which is the expected relation with $m = 0$ here. So the proof is complete. □

Example 2.15. Consider the case of B_4^+ and Δ_4^2 again. Proposition 2.14 enables us to directly obtain the $\boldsymbol{M}$-decomposition of Δ_4^2 as follows. We start with $x = \Delta_4^2$ and $\theta_0 = 00$. Then we compute M_{00}-tail, *i.e.*, here the $\langle\sigma_1\rangle$-tail, of $x^{(0)}$, which turns out to be σ_1^2, and call the remainder x'. Then the address θ_1 is obtained by looking at the maximal prefix θ of θ_0, *i.e.*, of 00, for which $M_{[\theta]} \not\perp x'$ holds. In the current case, we have $x^{(1)} \perp M_{00}$ and $x^{(1)} \not\perp M_0$, hence $\theta = 0$, so θ_1 is obtained from 00 by incrementing the second digit, leading to $\theta_1 = 01$, which corresponds to $M_{\alpha_1} = \langle\sigma_2\rangle$. We take the $\langle\sigma_2\rangle$-tail of x', call the remainder x'', and iterate. The successive values are displayed in Table 1.

i	$x^{(i)}$	θ_i	$[\theta_i]$	$M_{[\theta_i]}$	x_i
0	$\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$	00	00	$\langle\sigma_1\rangle$	σ_1^2
1	$\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_1\sigma_2$	01	01	$\langle\sigma_2\rangle$	σ_2
2	$\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_1$	02	00	$\langle\sigma_1\rangle$	σ_1^2
3	$\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3$	03	01	$\langle\sigma_2\rangle$	σ_2
4	$\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3$	10	10	$\langle\sigma_3\rangle$	σ_3
5	$\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2$	11	11	$\langle\sigma_2\rangle$	σ_2
6	$\sigma_3\sigma_2\sigma_1\sigma_1$	20	00	$\langle\sigma_1\rangle$	σ_1^2
7	$\sigma_3\sigma_2$	21	01	$\langle\sigma_2\rangle$	σ_2
8	σ_3	30	10	$\langle\sigma_3\rangle$	σ_3
9	1	-	-	-	-

TABLE 1. Direct determination of the decomposition of Δ_4^2: at each step, we indicated the current remainder $x^{(i)}$, the current address θ_i with the associated binary position $[\theta_i]$ in the covering, the submonoid $M_{[\theta_i]}$, and the $M_{[\theta_i]}$-tail x_i that is extracted.

2.3. **Dense and maximal coverings.** Everything we said so far works for every iterated covering $\boldsymbol{M}$, and, in particular, the (iterated) $\boldsymbol{M}$-decomposition always exists. In the sequel, we shall be interested in converting the latter into a unique normal form. This conversion is easy whenever the considered covering satisfies some additional assumptions called density and atomicity that we introduce now.

In the alternating decomposition of Proposition 1.16, apart from the first factor, no factor may be trivial unless the decomposition is complete. This situation is no longer guaranteed with iterated coverings. Indeed, according to Proposition 2.9, after considering some submonoid M_α, the next monoid to be considered is of the form $M_{\beta 0^m}$, where by hypothesis the M_β-tail of the current remainder is not 1. Now the latter hypothesis need not imply that the $M_{\beta 0^m}$-tail be nontrivial, and, if it is, it contributes a trivial factor in the $\boldsymbol{M}$-decomposition of x: there may be gaps in $\boldsymbol{M}$-decompositions.

Example 2.16. Let M be the 5 strand braid monoid B_5^+, and let $\boldsymbol{M}$ be the 2-covering defined by $M_{00} = \langle\sigma_1\rangle$, $M_{01} = \langle\sigma_2\rangle$, $M_{10} = \langle\sigma_3\rangle$, $M_{11} = \langle\sigma_4\rangle$. Let $x = \sigma_1\sigma_4$. The M_{00}-tail of x is σ_1, and the remainder is $x' = \sigma_4$. The longest prefix α of 00 such that the M_α-tail of x' is not trivial is $\varnothing$. The next submonoid to be looked at is M_{10}, which is $\langle\sigma_3\rangle$, and the M_{10}-tail of x' is trivial, so the corresponding factor in the $\boldsymbol{M}$-decomposition is 1. Finally, the $\boldsymbol{M}$-decomposition of x is $(\sigma_4, 1, \sigma_1)$, which has a gap.

It is however easy to state conditions that exclude such gaps.

Definition 2.17. A n-covering $\boldsymbol{M}$ is said to be *dense* if, for each binary address β of length m with $0 \leqslant m < n$,

(2.16) $\quad M_\beta$ is generated by $M_{\beta 0}$ and $M_{\beta 10^{n-m-1}}$, and by $M_{\beta 1}$ and $M_{\beta 0^{n-m}}$.

Lemma 2.18. *Assume that $\boldsymbol{M}$ is a dense n-covering of M. Then gaps are impossible in $\boldsymbol{M}$-decompositions.*

Proof. Owing to Proposition 2.14, the point is to prove that, if, for some binary n-address α and some m, we have, writing β (*resp.* β') for the length m (*resp.* $m+1$)

prefix of α, both $M_\beta \not\perp x$ and $M_{\beta'} \perp x$, then necessarily the $M_{\alpha^{[m]}}$-tail of x is not trivial. Write $\beta' = \beta i$. For $i = 0$, a sufficient condition for the previous implication is that M_β is generated by $M_{\beta 0}$ and $M_{\beta 10^{n-m-1}}$: then, a nontrivial right divisor of x lying in M_β cannot be right divisible by any factor in $M_{\beta 0}$ and, therefore, it must be right divisible by some factor in $M_{\beta 10^{n-m-1}}$, and, by definition, we have $\beta 10^{n-m-1} = \alpha^{[m]}$. For $i = 1$, the argument is similar, replacing $\beta 0$ with $\beta 1$, and $\beta 10^{n-m-1}$ with $\beta 0^{n-m}$. So, the two conditions in (2.16) are sufficient. □

On the other hand, as was recalled in the introduction of Section 2, a natural framework for getting a (trivial) unique normal form in a submonoid M_0 of M is the case when M_0 is generated by a single element s as every element of M_0 is then uniqueley expressed in M_0 as s^e. The latter expression remains unique in M whenever s is an *atom* of M, *i.e.*, $s = xy$ implies $x = 1$ or $y = 1$. Now, in the monoids we are currently considering, atoms do exist: every monoid M that satisfies Condition (C_3^*) is generated by its atoms, and, then, any generating subset of M contains all atoms of M. This should make the following definition natural.

Definition 2.19. Assume that M is a right locally Garside monoid, and $\boldsymbol{s}$ is a sequence of atoms of M indexed by binary n-addresses. We say that an n-covering $\boldsymbol{M}$ of M is *atomic* with *base* $\boldsymbol{s}$ if, for each n-address α, we have $M_\alpha = \langle s_\alpha \rangle$.

For instance, the 2-covering of Example 2.5 is atomic, based on the sequence $(\sigma_2, \sigma_3, \sigma_2, \sigma_1)$—with respect to a default enumeration of n-addresses going from 1^n to 0^n—while the covering of Example 2.16 is based on $(\sigma_4, \sigma_3, \sigma_2, \sigma_1)$. Note that a base sequence must contain all atoms of M, as, by definition, it generates M. On the other hand, if need not be true in general that every sequence of atoms defines a covering, as the submonoid of M generated by an arbitrary family of atoms is not necessarily closed in the sense of Definition 1.9. This however is true in braid monoids and, more generally, in all Artin–Tits monoids. The next lemma shows that, in the case of atomic coverings, the density condition requires that the base sequence be highly redundant.

Lemma 2.20. *Assume that $\boldsymbol{M}$ is a dense atomic n-covering of M with base $\boldsymbol{s}$. Then, for each n-address α, the set $\{s_{\alpha^{[m]}}\ ;\ 0 \leqslant m \leqslant n\}$ is the atom set of M, and the latter contains at most $n+1$ elements.*

Proof. Use induction on $n \geqslant 0$. The case $d = 0$ is obvious. Assume $n \geqslant 1$. Write $\alpha = d\beta$ with $d = 0$ or 1. Assume first $d = 0$. By (2.16), M is generated by $s_{10^{n-1}}$, which is the 0-successor of α, and M_0. By induction hypothesis, the latter is generated by the family of all $s_{0\beta^{[m]}}$'s, so M is generated by the successors of α. The argument is symmetric for $d = 1$, using the second part of (2.16). As, by construction, every n-address admits $n+1$ successors, we deduce that there are at most $n+1$ atoms in M. □

We shall see in Lemma 3.2 below that dense atomic n-coverings involving $n+1$ atoms exist for each n. It is easy to check that, for $n = 2$, the only base sequence is, up to renaming, that of Example 2.5 and Figure 1. For $n = 3$, several non-isomorphic base sequences exist, as shown in Figure 3.

2.4. **The normal form.** We are now ready to convert the results of Sections 2.1 and 2.2 into the construction of a normal form. We recall that, for S generating M

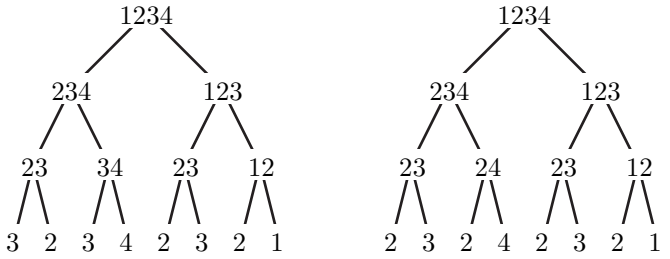

FIGURE 3. The two base sequences for a dense atomic 3-covering involving 4 atoms.

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 *from the right* in w.

Definition 2.21. Assume that M is a right locally Garside monoid with atom set S, and $\boldsymbol{M}$ is a dense atomic n-covering of M with base $\boldsymbol{s}$. A length ℓ word $w(\ell)...w(1)$ on S is said to be $\boldsymbol{M}$*-normal* if

> there exist n-addresses $\alpha_\ell, ..., \alpha_0$ with $\alpha_0 := 0^n$ such that, for each k,
> we have $\alpha_k = \alpha_{k-1}^{[m]}$ with m maximal such that $\overline{w(\ell)...w(k)} \succcurlyeq s_\alpha$
> holds for $\alpha = \alpha_{k-1}^{[m]}$, and $w(k) = s_{\alpha_k}$.

The above definition may look convoluted at first, but handling a few examples like the one reported in Table 3 below should make it easily understandable. In particular, Table 3 provides a step-by-step verification of the fact that our favourite example, here the braid word $\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$, is $\boldsymbol{M}$-normal with respect to the 2-covering of Example 2.5.

The expected existence and uniqueness result is then easy:

Proposition 2.22. *Assume that M is a right locally Garside monoid with atom set S, and $\boldsymbol{M}$ is a dense atomic n-covering of M with base $\boldsymbol{s}$. Then every element x of M admits a unique word representative that is $\boldsymbol{M}$-normal, namely the word $s_{\alpha_\ell}...s_{\alpha_1}$, where $\alpha_\ell, ..., \alpha_1$ are inductively determined from $x^{(0)} = x$ and $\alpha_0 = 0^n$ by*

$$\alpha_k := \alpha_{k-1}^{[m]} \quad \text{and} \quad x^{(k)} := x^{(k-1)}/s_{\alpha_k}, \tag{2.17}$$

with m maximal such that $x^{(k)} \succcurlyeq s_\alpha$ holds for $\alpha = \alpha_{k-1}^{[m]}$. Moreover, $s_{\alpha_\ell}...s_{\alpha_1}$ is the word obtained from the $\boldsymbol{M}$-decomposition of x by concatenating the (words representing the) entries and possibly deleting the final 1.

Proof. (*i*) 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 α of the address α_{k-1} such that s_α divides $x^{(k)}$ on the right. Uniqueness follows from the choice of that successor.

(*ii*) The inductive construction of (2.17) is essentially the construction of the $\boldsymbol{M}$-decomposition as given in Proposition 2.14. 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 s and the current remainder $x^{(k-1)}$ is divisible by s^2, then $x^{(k)}$ is $x^{(k-1)}/s$, 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 will be s again. In such a case, we have $m = n$. By contrast, in Proposition 2.14, the parameter m cannot be n. □

Definition 2.23. Under the hypotheses of Proposition 2.22, the word w is called the $\boldsymbol{M}$*-normal form* of x.

Input: A word w in S^*;

Procedure:

$w' := \texttt{emptyword}$;
$\alpha := 0^n$;
`while` $w \neq \texttt{emptyword}$ `do`
  $m := n$;
  `while` $\texttt{quotient}(w, s_{\alpha^{[m]}}) = \texttt{error}$ `do`
    $m := m - 1$;
  `od`;
  $\alpha := \alpha^{[m]}$;
  $w := \texttt{quotient}(w, s_\alpha)$;
  $w' := \texttt{concat}(s_\alpha, w')$;
`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 with base $\boldsymbol{s}$; moreover, we assume that $\texttt{quotient}(w, s)$ is a subroutine that for w a word in S^* and s an atom in S, returns `error` if s is not a right divisor of $\overline{w}$, and returns a word representing $\overline{w}/s$ otherwise.

The construction described in Proposition 2.22 is an algorithm, explicitly displayed in Table 2. A typical example for the construction of the $\boldsymbol{M}$-normal form is given in Table 3. As for algorithmic aspects, computing the $\boldsymbol{M}$-normal form is as easy as computing the alternating decomposition. In our current atomic context, the existence of the norm (Definition 1.19) is guaranteed [18].

Proposition 2.24. *Assume that M is a right locally Garside monoid with atom set S, and $\boldsymbol{M}$ is a dense atomic n-covering of M with base $\boldsymbol{s}$. Assume moreover that Condition $(*)$ of Proposition 1.20 is satisfied. Then, for each word w in S^*, the algorithm of Table 2 runs in time $O(\|w\|^2)$.*

Proof. The only change with respect to Proposition 1.20 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. □

2.5. **The $\boldsymbol{M}$-exponent sequence.** We conclude this section with an alternative construction that will be useful in Section 3 below. In the framework of Proposition 2.22, instead of associating with every element x of M a distinguished word representative of x, we can also associate an n-sequence of natural numbers. If M is generated by the element s, then every element x of M is determined by the unique exponent e such that $x = s^e$ holds. If $\boldsymbol{M}$ is an atomic n-covering of M,

k	w	w'	α_{k-1}	m	$\alpha_{k-1}^{[m]}$	$s_{\alpha_{k-1}^{(m)}}$	$\overline{w} \not\succcurlyeq s_{\alpha_{k-1}^{[m]}}$?
0	$\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$	-	00	2	00	σ_1	yes
2	$\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2$	σ_1	00	2	00	σ_1	yes
2	$\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_1\sigma_2$	$\sigma_1\sigma_1$	00	2	00	σ_1	no
				1	01	σ_2	yes
3	$\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_1$	$\sigma_2\sigma_1\sigma_1$	01	2	01	σ_2	no
				1	00	σ_1	yes
4	$\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3$	$\sigma_1\sigma_2\sigma_1\sigma_1$	00	2	00	σ_1	yes
5	$\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3$	$\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	00	2	00	σ_1	no
				1	01	σ_2	yes
6	$\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3$	$\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	01	2	01	σ_2	no
				1	00	σ_1	no
				0	10	σ_3	yes
7	$\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2$	$\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	10	2	10	σ_3	no
				1	11	σ_2	yes
8	$\sigma_3\sigma_2\sigma_1\sigma_1$	$\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	11	2	11	σ_2	no
				1	10	σ_3	no
				0	00	σ_1	yes
9	$\sigma_3\sigma_2\sigma_1$	$\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	00	2	00	σ_1	yes
10	$\sigma_3\sigma_2$	$\sigma_1\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	00	2	00	σ_1	no
				1	01	σ_2	yes
11	σ_3	$\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	01	2	01	σ_2	no
				1	00	σ_1	no
				0	10	σ_3	yes
12	-	$\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1$	10	-	-	-	

TABLE 3. Computation of the $\boldsymbol{M}$-normal form of Δ_4^2, where $\boldsymbol{M}$ is the 2-covering of B_4^+ of Example 2.5, starting from the word $\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$: at each step, we try to divide the current word w by some generator σ_i and, when succesful, we add this σ_i on the left of the current word w', until no letter is left in w; the only point is to know in which order the generators σ_i are tried: this is what the address α specifies, namely we try the successive successors of α starting with the last one, *i.e.*, with α itself, and then we consider shorter and shorter prefixes of α; density guarantees that we cannot get stuck.

we can similarly forget about the generators in the iterated $\boldsymbol{M}$-decomposition, and just keep track of the exponents, *i.e.*, introduce an n-sequence in $\mathbb{N}$, and no longer in M.

Definition 2.25. For M and $\boldsymbol{M}$ as in Definition 2.21, and for x in M, we define the *$\boldsymbol{M}$-exponent sequence* $D^\bullet_{\boldsymbol{M}}(x)$ of x to be the n-sequence in $\mathbb{N}$ obtained by replacing each factor $s_\alpha^{e_\alpha}$ with e_α in $D_{\boldsymbol{M}}(x)$.

Example 2.26. For the usual 2-covering of B_4^+, the exponent sequence $D^\bullet_{\boldsymbol{M}}(\Delta_4^2)$ is

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

corresponding to the tree displayed in Figure 4 below.

The point is that the n-sequence $D^{\bullet}_{\boldsymbol{M}}(x)$ contains enough information to recover the names of the generators that have been erased. Indeed, we have:

Lemma 2.27. *Assume that $\boldsymbol{M}$ is an atomic n-covering of M. Then, for every x in M, the exponent sequence $D^{\bullet}_{\boldsymbol{M}}(x)$ determines x.*

Proof. Let s be the generator function associated with $\boldsymbol{M}$. We recover $D^{\circ}_{\boldsymbol{M}}(x)$, and therefore x itself, from $D^{\bullet}_{\boldsymbol{M}}(x)$ as follows. Indeed, let $(e_p, ..., e_0)$ be the entry list in $D^{\bullet}_{\boldsymbol{M}}(x)$ and $(\theta_p, ..., \theta_0)$ be its address list. Then, if $(x_p, ..., x_0)$ is the $\boldsymbol{M}$-decomposition $D^{\circ}_{\boldsymbol{M}}(x)$ of x, we have $x_i = s^{e_i}_{[\theta_i]}$ for each i. The formal proof is an easy induction on the degree n of the covering $\boldsymbol{M}$ (see Figure 4 for an example). □

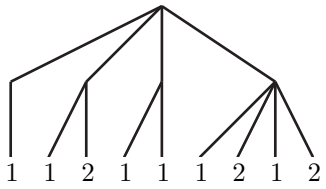

FIGURE 4. The tree associated with the 2-sequence $D^{\bullet}_{\boldsymbol{M}}(\Delta^2_4)$; the tree determines the missing names of the generators: for instance, the leftmost 2 has address 20 in the tree, so it corresponds to the generator $s_{[20]}$, which, in the current case, is σ_1; so this number 2 corresponds to a factor σ_1^2 in the iterated $\boldsymbol{M}$-decomposition of Δ^2_4.

Remark. The iterated $\boldsymbol{M}$-decomposition $D_{\boldsymbol{M}}(x)$ contains two types of information, namely the brackets and the entries. What we saw above is that each type determines the other: both $D^{\circ}_{\boldsymbol{M}}(x)$, obtained by forgetting the brackets, and $D^{\bullet}_{\boldsymbol{M}}(x)$, obtained by forgetting the names of the generators, still determine x unambiguously. But we cannot go farther: if both projections are applied simultaneously, *i.e.*, if we unbracket $D^{\bullet}_{\boldsymbol{M}}(x)$, then x is in general lost, as easy examples show.

3. The flip normal form of braids

From now on, we concentrate on the case of braids, and investigate a natural family of coverings that generalize the one of Example 2.5. The flip automorphism (conjugation by Δ_n) plays a significant rôle in the construction, which explains our terminology.

In the sequel, we write n-braid for n strand braid, and n-braid word for n strand braid word. We consider B^+_{n-1} as a submonoid of B^+_n: an $(n-1)$-braid is a particular n-braid.

3.1. **The flip covering.** We denote by ϕ_n the flip automorphism of B^+_n that exchanges σ_i and σ_{n-i} for each i. We also use ϕ_n for n-braid words, thus denoting by $\phi_n(w)$—or $\phi_n w$—the image of w under ϕ_n letter by letter.

On the shape of what was done for B^+_4 in Example 2.5, we shall introduce for each n a dense atomic $(n-2)$-covering of B^+_n based on some sequence $\boldsymbol{s}_n$. The construction obeys a simple inductive scheme.

Definition 3.1. For $n \geqslant 2$, we inductively define a sequence $\boldsymbol{s}_n$ indexed by binary $(n-2)$-addresses by

$$\boldsymbol{s}_2 = (\sigma_1), \quad \boldsymbol{s}_n := \phi_n(\boldsymbol{s}_{n-1}) \frown \boldsymbol{s}_{n-1}. \tag{3.1}$$

As the length of the address α determines the associated number n, namely $|\alpha| = n-2$, we shall skip n and write s_α for $s_{|\alpha|+2,\alpha}$ in the sequel. Then (3.1) develops into the explicit rules

$$s_\varnothing = \sigma_1, \quad s_{0\alpha} := s_\alpha, \quad s_{1\alpha} := \phi_{|\alpha|+2}(s_\alpha), \tag{3.2}$$

which determine each s_α's unambiguously. For instance, we find $\boldsymbol{s}_3 = (\sigma_2, \sigma_1)$, $\boldsymbol{s}_4 = (\sigma_2, \sigma_3, \sigma_2, \sigma_1)$, and, more generally, $\boldsymbol{s}_n$ is the length 2^n suffix of some left infinite sequence $\boldsymbol{s}_\infty$ where indices are

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

Lemma 3.2. (*i*) *For $n \geqslant 2$ and for each $(n-2)$-address α, we have $s_\alpha = \sigma_i$ with*

$$i = -m_1 + m_2 - \dots + (-1)^r m_r + \begin{cases} 1 & \text{if } r \text{ is even,} \\ n & \text{if } r \text{ is odd,} \end{cases} \tag{3.3}$$

if $\alpha = d_1 \dots d_{n-2}$ and $m_1 < \dots < m_r$ are the m's for which d_m is odd.

(*ii*) *For $n \geqslant 2$, the sequence $\boldsymbol{s}_n$ is the base of a dense atomic covering of B_n^+.*

For instance, in the 7-address 0110101, there are odd digits at positions $2, 3, 5, 7$, so (3.3) gives $i = (-2+3-5+7)+1 = 4$, hence $s_{0110101} = \sigma_4$.

Proof. (*i*) Relation (3.3) holds for $n = 2$, where it reduces to $s_\varnothing = \sigma_1$. Assume $n \geqslant 3$, and let $\alpha' = d_2 \dots d_{n-2}$. Putting $s_{\alpha'} = \sigma_{i'}$, we aim at proving $i = i'$ if d_1 is even, and $i = n - i'$ if d_1 is odd. Write S for $-m_1 + m_2 - \dots + (-1)^r m_r$, and r', m_1', m_2', ..., S', n' for the similar parameters associated with α'. Assume first that d_1 is even. Then we have $r = r'$, and $m_j = m_j' + 1$ for each j, hence $S = S'$ if r is even, and $S = S' - 1$ if r is odd. The induction hypothesis gives $i' = S' + 1$ if r is even, $S' + n'$ if r is odd. We deduce

$$i = \begin{cases} S + 1 = S' + 1 = i' & \text{if } r \text{ is even,} \\ S + n = S' - 1 + n' + 1 = i' & \text{if } r \text{ is odd.} \end{cases}$$

Assume now that d_1 is odd. 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 even, and $S = -S' - 1$ if r is odd. The induction hypothesis gives $i' = S' + n'$ if r is even, $S' + 1$ if r is odd. We deduce

$$i = \begin{cases} S + 1 = -S' + 1 = n - i' & \text{if } r \text{ is even,} \\ S + n = -S' - 1 + n = n - i' & \text{if } r \text{ is odd.} \end{cases}$$

(*ii*) The generators σ_i are the atoms of B_n^+, and we already noted that every parabolic submonoid of B_n^+ is closed, so every surjective sequence of atoms defines a covering. As for density, the point is to show that B_n^+ is generated by B_{n-1}^+ and $B_{n,10^{n-3}}^+$. Now (3.3) gives $s_{10^{n-3}} = \sigma_{n-1}$, which is precisely the atom of B_n^+ missing in B_{n-1}^+. □

Definition 3.3. For $n \geqslant 2$, we denote $\boldsymbol{B}_n^+$ the $(n-2)$-covering of B_n^+ based on $\boldsymbol{s}_n$.

It follows from (3.1) and (3.2) that $\boldsymbol{B}_n^+$ is recursively defined by

$$\boldsymbol{B}_2^+ := B_2^+, \quad \boldsymbol{B}_n^+ = \phi_n(\boldsymbol{B}_{n-1}^+) \frown \boldsymbol{B}_{n-1}^+, \tag{3.4}$$

which develop into

$$B_{2,\varnothing}^+ := B_2^+, \quad B_{n,0\alpha}^+ = B_{n-1,\alpha}^+, \quad \text{and} \quad B_{n,1\alpha}^+ = \phi_n(B_{n-1,\alpha}^+), \tag{3.5}$$

completed with $B_{n,\beta}^+ = \langle B_{n,\alpha}^+ \ ; \ \beta \text{ prefix of } \alpha \rangle$ for β of length $< n-2$. So, we have $B_{3,0}^+ = B_2^+ = \langle \sigma_1 \rangle$, $B_{3,1}^+ = \phi_3(B_2^+) = \langle \sigma_2 \rangle$, $B_{3,\varnothing}^+ = \langle B_{3,1}^+, B_{3,0}^+ \rangle = B_3^+$. Next, we find $B_{4,00}^+ = \langle \sigma_1 \rangle$, $B_{4,01}^+ = B_{4,11}^+ = \langle \sigma_2 \rangle$, $B_{4,10}^+ = \langle \sigma_3 \rangle$, which shows that $\boldsymbol{B}_4^+$ is the 2-covering of B_4^+ many times considered in Section 2.

As $\boldsymbol{B}_n^+$ is a dense atomic covering of B_n^+, all results of Section 2 apply to $\boldsymbol{B}_n^+$. We fix the following notation and vocabulary.

Definition 3.4. For x in B_n^+, we denote by $D_n(x)$ (*resp.* $D_n^\circ(x)$, *resp.* $D_n^\bullet(x)$) the iterated $\boldsymbol{B}_n^+$-decomposition (*resp.* the $\boldsymbol{B}_n^+$-decomposition, *resp.* the $\boldsymbol{B}_n^+$-exponent sequence) of x, and call it the iteration ϕ-decomposition (*resp.* the ϕ-decomposition, *resp.* the ϕ-exponent sequence) of x. Finally, a $\boldsymbol{B}_n^+$-normal word is called *ϕ-normal*.

Thus, the example computations of Section 2 yield

$$D_4(\Delta_4^2) = ((\sigma_3), (\sigma_2, \sigma_1^2), (\sigma_2, \sigma_3), (\sigma_2, \sigma_1^2, \sigma_2, \sigma_1^2)),$$
$$D_4^\circ(\Delta_4^2) = (\sigma_3, \sigma_2, \sigma_1^2, \sigma_2, \sigma_3, \sigma_2, \sigma_1^2, \sigma_2, \sigma_1^2),$$
$$D_4^\bullet(\Delta_4^2) = ((1), (1,2), (1,1), (1,2,1,2)).$$

Being a ϕ-normal word can be expressed in several equivalent ways. Below, we recall the initial definition, and mention some variants. The general principle is always:

> A word w is 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 brraid represented by the length k prefix of w, smallest refering here 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, which can be encoded in several equivalent ways, involving addresses, or numbers, or permutations. Note that, would the local ordering be the fixed order $\sigma_1 < ... < \sigma_{n-1}$, then a word would be normal if it simply were the lexicographically minimal representative of its equivalence class. Here, things are slightly more complicated because the reference ordering varies.

We recall that, for α a binary address, $a^{[m]}$ denotes the (binary) m-successor of α (Definition 2.12), and that, for w a braid word, $\overline{w}$ denotes the braid represented by w.

Lemma 3.5. *A length ℓ positive n-braid word $w(\ell)...w(1)$ is ϕ-normal if and only if any one of the following equivalent conditions holds:*

> *(i) There exist $(n-2)$-addresses $\alpha_\ell, ..., \alpha_0$ with $\alpha_0 = 0^{n-2}$ such that, for each k, α_k is the maximal binary successor α of α_{k-1} satisfying $\overline{w(\ell)...w(k)} \succcurlyeq s_\alpha$, and we have $w(k) = s_{\alpha_k}$.*
>
> *(ii) There exist numbers $m_\ell, ..., m_1$ in $\{0, ..., n\}$ such that, starting from $\alpha_0 := 0^n$ and inductively defining $\alpha_k := \alpha_{k-1}^{[m_k]}$, then, for*

each k, we have $\overline{w(\ell)...w(k)} \not\succcurlyeq s_\alpha$ for every m-successor α of α_{k-1} with $m > m_k$, and $w(k) = s_{\alpha_k}$.

(iii) There exist permutations $\pi_\ell, ..., \pi_0$ of $\{1, ..., n-1\}$ such that π_0 is the identity, and, for each k, π_k is obtained by $\pi_k(1) := \pi_{k-1}(p)$, where p is minimal satisfying $\overline{w(\ell)...w(k)} \succcurlyeq \sigma_{\pi_{k-1}(p)}$, $\pi_k(q) = \pi_{k-1}(q)$ for $q > p$, and $(\pi_k(2), ..., \pi_k(p))$ is the increasing (resp. decreasing) enumeration of $\{\pi_{k-1}(1), ..., \pi_{k-1}(p-1)\}$ if the latter are $> \pi_k(1)$ (resp. $<$), and we have $w(k) = \sigma_{\pi_k(1)}$.

Proof. Points (i) is Definition 2.21 and (ii) are direct reformulation of it. 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 $s_{\alpha_k^{[m]}} = \sigma_i$ 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 $\boldsymbol{B}_n^+$. □

A direct application of Propositions 2.22 and 2.24 then gives:

Proposition 3.6. (i) *Every braid in B_n^+ admits a unique word representative that is ϕ-normal.*

(ii) *Running on a positive n-braid word of length ℓ, the algorithm of Table 2 returns the unique 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 the ϕ-decomposition of $\overline{w}$.*

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 ϕ-decomposition and the ϕ-normal form viewed as a sequence of letters is that the ϕ-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 1 sequence (σ_2), while its ϕ-decomposition is the length 2 sequence $(\sigma_2, 1)$.

3.2. **The flip splitting.** By construction, $(B_{n,1}^+, B_{n,0}^+)$ is a covering of the monoid B_n^+ in the sense of Section 1, so, by Proposition 1.16, it gives rise to a (non-iterated) decomposition for each element of B_n^+. Now, as $B_{n,0}^+$ has been defined to be B_{n-1}^+ and $B_{n,1}^+$ to be the image of B_{n-1}^+ under ϕ_n, we can restate the results in a more specific form. It will be convenient to introduce the following convention.

Notation 3.7. For y, x in B_n^+, we write $y \ltimes_n x$ for $\phi_n(y)\, x$—a left twisted product indeed—and extend the notation to any number of factors according to the convention $z \ltimes_n y \ltimes_n x = (z \ltimes_n y) \ltimes_n x$. We use a similar notation for braid words.

So $x_p \ltimes_n ... \ltimes_n x_0$ denotes the alternated product $\phi_n^p(x_p)...x_2\, \phi_n(x_1)\, x_0$, *i.e.*, the product of x_p to x_0 where factors of odd rank starting from the right are flipped in B_n^+. Keep in mind that the operation $\ltimes_n$ is not associative.

Proposition 3.8. *Every braid x in B_n^+ admits a unique decomposition*

$$x = x_p \ltimes_n ... \ltimes_n x_1 \ltimes_n x_0 \tag{3.6}$$

with $x_0, ..., x_p \in B_{n-1}^+$ such that, for each $i \geqslant 1$,

(3.7) *the only σ_j dividing $x_p \ltimes_n ... \ltimes_n x_i$ on the right is σ_1.*

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

$$x_i := \mathrm{tail}(x^{(i)}, B_{n-1}^+), \quad x^{(i+1)} := \phi_n(x^{(i)}/x_i). \tag{3.8}$$

Proof. The monoids B_{n-1}^+ and $\phi_n(B_{n-1}^+)$ are closed submonoids of B_n^+, and their union generates all of B_n^+. Applying Proposition 1.16 gives the result, as $y_0 = \mathrm{tail}(y, \phi_n(B_{n-1}^+))$ is equivalent to $\phi_n(y_0) = \mathrm{tail}(\phi_n(y), B_{n-1}^+)$, and ϕ_n is an automorphism for the quotient operation / as well. □

Definition 3.9. The sequence $(x_p, ..., x_0)$ involved in (3.6) will be called the *ϕ_n-splitting* of x—or, simply, its ϕ-splitting when there is no ambiguity about n. The parameter p is called the *n-breadth of x*.

Before giving an example, we enounce connections between the ϕ-splitting, the ϕ-decomposition, and the ϕ-normal form.

Lemma 3.10. *Assume $x \in B_n^+$. If $(x_p, ..., x_0)$ be the ϕ-splitting of x, we have*

$$D_n(x) = (\phi_n^p D_{n-1}(x_p), ..., \phi_n D_{n-1}(x_1), D_{n-1}(x_0)), \tag{3.9}$$

$$D_n^\circ(x) = \phi_n^p D_{n-1}^\circ(x_p) \frown ... \frown \phi_n D_{n-1}^\circ(x_1) \frown D_{n-1}^\circ(x_0), \tag{3.10}$$

$$D_n^\bullet(x) = (D_{n-1}^\bullet(x_p), ..., D_{n-1}^\bullet(x_1), D_{n-1}^\bullet(x_0)). \tag{3.11}$$

and the ϕ-normal form of x is $w_p \ltimes_n ... \ltimes_n w_0$, where w_i is the ϕ-normal form of x_k.

(ii) Conversely, let w be the ϕ-normal form of x. Starting from $u_0 = w$, let w_i be the longest suffix of u_i that does not contain σ_{n-1} if i is even (resp. does not contain σ_1 if i is odd), and let u_{i+1} be such that $u_i = u_{i+1} w_i$. Then, p being minimal such that u_p is empty, the ϕ-splitting of x is $(\phi_n^p(\overline{w_p}), ..., \overline{w_2}, \phi_n(\overline{w_1}), \overline{w_0})$.

Proof. *(i)* By definition, the $(B_{n,1}^+, B_{n,0}^+)$-decomposition of x is $(\phi_n^p(x_p), ..., \phi_n(x_1), x_0)$ and (2.3) gives

$$D_n(x) = (D_{\phi_n^p \boldsymbol{B}_{n-1}^+}(\phi_n^p(x_p)) \, , \, \ldots \, , \, D_{\boldsymbol{B}_{n-1}^+}(x_0)).$$

Now, as ϕ_n is an automorphism of B_n^+, for each y in B_{n-1}^+, the iterated $\phi_n(\boldsymbol{B}_{n-1}^+)$-decomposition of $\phi_n(y)$ is the image under ϕ_n of the iterated $\boldsymbol{B}_{n-1}^+$-decomposition of y, and (3.9) follows. By projecting, we deduce (3.10) and (3.11); in the latter, the projection is obtained by forgetting the names of the generators, so the flip no longer appears.

As for the normal form, the result follows from (3.10), for, by construction, each factor x_i with $i \geqslant 1$ is divisible by σ_1 on the right, so its ϕ-normal form is precisely the word obtained from $D_n^\circ(x_i)$ by concatenating the factors, without any difference.

(ii) By construction, we have $x = \overline{w_p} ... \overline{w_1}\, \overline{w_0}$, hence $x = \phi_n^p(\overline{w_p}) \ltimes_n ... \ltimes_n \phi_n(\overline{w_1}) \ltimes_n \overline{w_0}$. The normality assumption guarantees that, for i even, $\overline{w_p} ... \overline{w_i}$ is right divisible by σ_1 only, and, for i odd, it is right divisible by σ_{n-1} only, so, in any case, $\phi_n^p(\overline{w_p}) \ltimes_n ... \ltimes_n \phi_n^i(\overline{w_i})$ is right divisible by σ_1 only, which characterizes the ϕ-splitting. □

Example 3.11. We saw in Table 3 that the ϕ-normal form of Δ_4^2 is

$$\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_3\sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1.$$

Applying Lemma 3.10(*ii*), we obtain the ϕ-splitting of Δ_4^2 by gathering the generators that alternatively give words in B_3^+, and in $\langle\sigma_2,\sigma_3\rangle$, starting from the right. Here we find $(\sigma_3, \sigma_2\sigma_1\sigma_1, \sigma_2\sigma_3, \sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1)$, hence the 4-breadth of Δ_4^2 is 3, and its ϕ-splitting is the length 4 sequence

$$(\sigma_1\ ,\ \sigma_2\sigma_1\sigma_1\ ,\ \sigma_2\sigma_1\ ,\ \sigma_2\sigma_1\sigma_1\sigma_2\sigma_1\sigma_1)$$

obtained by flipping each other entry in the above sequence.

Conversely, in order to obtain the ϕ-normal form of Δ_4^2, we start from its ϕ-splitting above, compute the ϕ-splitting of each entry successively, namely

$$((\sigma_1)\ ,\ (\sigma_1,\sigma_1^2)\ ,\ (\sigma_1,\sigma_1)\ ,\ (\sigma_1,\sigma_1^2,\sigma_1,\sigma_1^2)),$$

and finally apply the needed flips to reobtain the 2-sequence

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

of (2.2). Observe that, in any case, the entries in the iterated ϕ-splitting consist of elements of B_2^+, *i.e.*, of powers of σ_1.

We saw above that the non-final entries in a ϕ-splittings are never 1—we shall say more in Lemma 3.21 below—but let us insist that the final entry may take any value, including 1: for instance, the ϕ_3-decomposition of σ_2 is the sequence $(\sigma_1, 1)$, as σ_2 is not divisible by σ_1.

Finally, the following example shows that the behaviour of the ϕ-splitting, and therefore of the connected ϕ-normal form, is quite different from that of the right greedy normal form, in particular in terms of right divisors. Let $x = \sigma_1^e\sigma_2\sigma_1$ with $e \geqslant 1$. Then ϕ-splitting of x is $(\sigma_1^e, \sigma_1, \sigma_1)$, corresponding to the factorization $x = \sigma_1^e \cdot \phi_2(\sigma_1)\cdot\sigma_1$. Now we have also $x = \sigma_2\sigma_1\sigma_2^e$. This shows that, if $(x_p, ..., x_0)$ is the ϕ-splitting of x, the σ_i's satisfying $x \succcurlyeq \sigma_i$ cannot be recovered from (x_1, x_0), and that $\phi_n(x_1)x_0$ is not the left lcm of all terms of the form $\phi_n(y_1)y_0$ with $y_1, y_0 \in B_{n-1}^+$ right dividing x, and not even at least as long as any such term: in the case above, (x_1, x_0) is (σ_1, σ_1), and x is right divisible by σ_2^e, which is of the form $\phi_3(y_1)y_0$ with $y_1, y_0 \in B_2^+$.

3.3. **A linear ordering on B_n^+.** As $\boldsymbol{B}_n^+$ is a dense atomic n-covering of B_n^+, we know by Lemma 2.27 that the iterated ϕ-decomposition $D_n^\circ(x)$ of every element x of B_n^+ is unambiguously determined by its exponent sequence $D_n^\bullet(x)$, which is a degree n sequence of natural numbers. Now, such sequences can be easily ordered using the geometry of the associated trees, and we are led to order B_n^+. Actually, for simplicity, we shall not start from the exponent sequence, but from a direct inductive construction that will be subsequently proved to be equivalent.

Definition 3.12. For $n \geqslant 2$, we recursively define a relation $<_n^*$ on B_n^+ by:

(*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 $(x_p, ..., x_0)$ and $(y_q, ..., y_0)$ be the ϕ_n-splittings of x and y, we have either $p < q$, or $p = q$ and there exists r satisfying $x_i = y_i$ for $i > r$ and $x_r <_{n-1}^* y_r$.

Thus, $<_n^*$ is a sort of lexicographical extension of the natural order on B_2^+, *i.e.*, on natural numbers, via iterated ϕ-splittings. The extension is not exactly lexicographic: before comparing the sequences componentwise, we first compare their lengths, *i.e.*, the breadths of the considered braids. Such a comparison method is called the `ShortLex`-ordering in [21].

Proposition 3.13. (*i*) *For $n \geqslant 2$, the relation $<_n^*$ is a strict linear ordering on 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 $B_{n-1}^+ = \{x \in B_n^+ \,;\, x <_n^* \sigma_{n-1}\}$.*

Proof. (*i*) The relation $<_2^*$ is a strict linear ordering on B_2^+, and, then, the fact that $<_n^*$ is a strict linear ordering on B_n^+ follows from the hypothesis that $<_{n-1}^*$ is a strict linear ordering on B_{n-1}^+ and the uniqueness of the ϕ_n-splitting. That $<_n^*$ is a well-order results from a similar induction, owing to the standard result that the `ShortLex`-extension of a well-order is a well-order. Finally, if the ϕ_n-splitting of x is $(x_p, ..., x_0)$, the ϕ_n-splitting of $x\sigma_1$ is $(x_p, ..., x_0\sigma_1)$, making it clear that $x\sigma_1$ is the immediate successor of x.

(*ii*) For x, y in B_{n-1}^+, the ϕ_n-splittings of x and y simply are the length 1 sequences (x) and (y), so, by definition, $x <_n^* y$ holds if and only if $x <_{n-1}^* y$ does. On the other hand, the ϕ_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_1, x_0) is an ϕ_n-splitting, x_1 is not 1, hence, by (*i*), we have $x_1 \geqslant_n^* \sigma_1$. 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 3.13(*ii*), we shall skip the index n and write $<^*$ for $<_n^*$.

Example 3.14. The ϕ_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 ϕ-splittings of $\sigma_1\sigma_2\sigma_1^4$ and $\sigma_1\sigma_2^2$ respectively are $(\sigma_1, \sigma_1, \sigma_1^4)$ and $(\sigma_1, \sigma_1^2, 1)$. Here the 3-breadths are 3 in both cases, and we compare lexicographically. The first entries coincide, but $\sigma_1 <^* \sigma_1^2$ holds, so we conclude that $\sigma_1\sigma_2\sigma_1^4 <^* \sigma_1\sigma_2^2$ holds.

In Definition 3.12, we introduced the order $<^*$ by means of the ϕ-splitting. It can equivalently be introduced by appealing to the ϕ-exponent sequence and some order on n-sequences on $\mathbb{N}$.

Definition 3.15. We denote by $<^{\texttt{ShortLex}}$ the `ShortLex` iterated extension of the standard order on $\mathbb{N}$ to n-sequences on $\mathbb{N}$: if $\boldsymbol{u}, \boldsymbol{v}$ are n-sequences on $\mathbb{N}$, we say that $\boldsymbol{u} <^{\texttt{ShortLex}} \boldsymbol{v}$ holds if we have $n = 0$ and $\boldsymbol{u} < \boldsymbol{v}$, or $n > 0$ and $\boldsymbol{u}$ is `ShortLex`-smaller than $\boldsymbol{v}$, *i.e.*, writing $\boldsymbol{u} = (\boldsymbol{u}_p, ..., \boldsymbol{u}_0)$, $\boldsymbol{v} = (\boldsymbol{v}_q, ..., \boldsymbol{v}_0)$, we have either $p < q$, or $p = q$ and there exists r satisfying $\boldsymbol{u}_i = \boldsymbol{v}_i$ for $i > r$ and $\boldsymbol{u}_r <^{\texttt{ShortLex}} \boldsymbol{v}_r$.

Lemma 3.16. *For x, y in B_n^+, we have*

$$x <^* y \iff D_n^\bullet(x) <^{\texttt{ShortLex}} D_n^\bullet(y). \tag{3.12}$$

Proof. We use induction on $n \geqslant 2$. The result is obvious for $n = 2$. Assume $n \geqslant 3$. Let $(x_p, ..., x_0)$ and $(y_q, ..., y_0)$ be the ϕ_n-splittings of x and y. By (3.11), we have

$$D_n^\bullet(x) = (D_{n-1}^\bullet(x_p), ..., D_{n-1}^\bullet(x_0)), \quad D_n^\bullet(y) = (D_{n-1}^\bullet(y_q), ..., D_{n-1}^\bullet(y_0)).$$

By induction hypothesis, $D_{n-1}^\bullet(x_i) <^{\texttt{ShortLex}} D_{n-1}^\bullet(y_i)$ is equivalent to $x_i <^* y_i$, and comparing the definitions of $x <^* y$ and of $D_n^\bullet(x) <^{\texttt{ShortLex}} D_n^\bullet(y)$ then gives the expected equivalence. □

For instance, we saw in Example 3.14 that $\sigma_1\sigma_2\sigma_1^4 <^* \sigma_1\sigma_2^2$ holds. Another way to see that is to compare the exponent sequences, $(1, 1, 4)$ and $(1, 2, 0)$ in the current case, with respect to $<^{\texttt{ShortLex}}$: the former is $<^{\texttt{ShortLex}}$-smaller, as the lengths are the

same, namely 3, as well as the leftmost entry, but the second entry in the former is smaller than the second entry in the latter.

3.4. **The braids $\nabla_{n,p}$.** Few properties of the order $<^*$ are visible directly. Typically, whether $x <^* y$ implies $zx <^* zy$ is unclear because we do not know much about the ϕ-splittings of zx and zy as compared with those of x and y: multiplying by new factors on the left may change the right divisors radically, and it seems hazardous to predict anything about the ordering of zx and zy.

In this section, we shall prove one technical result about the order $<^*$, namely we determine the least upper bound of the elements of B_n^+ with breadth at most p.

Definition 3.17. For $n \geqslant 2$ and $p \geqslant 1$, we define

$$\delta_n = \sigma_{n-1}...\sigma_1 \text{ and } \nabla_{n,p} = (\sigma_1...\sigma_{n-1}) \ltimes_n ... \ltimes_n (\sigma_1...\sigma_{n-1}), \ p \text{ factors.} \tag{3.13}$$

In other words, $\nabla_{n,p}$ is the length $p(n-1)$ zigzag $...\sigma_{n-1}...\sigma_1\sigma_1...\sigma_{n-1}$ with $p-1$ alternations, always finishing with σ_{n-1}. For instance, we have $\nabla_{4,2} = \sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3$.

Lemma 3.18. (*i*) *For $n \geqslant 2$ and $p \geqslant 1$, we have*

$$\Delta_n^p = \nabla_{n,p}\, \Delta_{n-1}^p. \tag{3.14}$$

(*ii*) *For $n \geqslant 2$, $p \geqslant 1$, and for each braid x in B_{n-1}^+, the n-breadth of $\nabla_{n,p}x$ is $p+1$, and its ϕ-splittings is*

$$(\sigma_1\ ,\ \underbrace{\delta_{n-1}\sigma_1\ ,\ ...\ ,\ \delta_{n-1}\sigma_1}_{p-1 \text{ times}}\ ,\ \delta_{n-1}\ ,\ x). \tag{3.15}$$

This holds in particular for $\nabla_{n,p}$ with $x = 1$, and for Δ_n^p with $x = \Delta_{n-1}^p$.

Proof. (*i*) Among the many equivalent inductive definitions of Δ_n, we choose

$$\Delta_1 = 1 \qquad \text{and} \qquad \Delta_n = \sigma_1...\sigma_{n-1}\Delta_{n-1},$$

i.e., $\Delta_n = \nabla_{n,1}\Delta_{n-1}$, so (3.14) holds for $p = 1$. Then, for $p \geqslant 2$, we use induction:

$$\begin{aligned}\Delta_n^p = \Delta_n\Delta_n^{p-1} = \Delta_n\nabla_{n,p-1}\Delta_{n-1}^{p-1} &= \phi_n(\nabla_{n,p-1})\Delta_n\Delta_{n-1}^{p-1}\\ &= \phi_n(\nabla_{n,p-1})\nabla_{n,1}\Delta_{n-1}\Delta_{n-1}^{p-1} = \nabla_{n,p}\Delta_{n-1}^p.\end{aligned}$$

(*ii*) When we evaluate the sequence of (3.15) by flipping each other entry, we precisely obtain $\nabla_{n,p}x$. On the other hand, entry in (3.15) but possibly the last one is right divisible by σ_1, and not right divisible by any other σ_i. So, by Proposition 3.8, the sequence must be the ϕ-splitting of the braid it represents. □

Example 3.19. The ϕ-splitting of Δ_3^p is

$$(\sigma_1\ ,\ \underbrace{\sigma_1^2\ ,\ ...\ ,\ \sigma_1^2}_{p-1 \text{ times}}\ ,\ \sigma_1\ ,\ \sigma_1^p), \tag{3.16}$$

which is $(\sigma_1, \sigma_1, \sigma_1)$ for $p = 1$, corresponding to $\Delta_3 = \sigma_1\sigma_2\sigma_1$, and $(\sigma_1, \sigma_1^2, \sigma_1, \sigma_1^2)$ for $p = 2$, corresponding to $\Delta_3^2 = \sigma_2\sigma_1^2\sigma_2\sigma_1^2$. In other words, the 3-exponent sequence of Δ_3^p is $(1, 2, ..., 2, 1, p)$, $p-1$ times 2.

We aim at proving that $\nabla_{n,p}$ is the least upper bound for the n-braids with n-breadth at most p. To do that, we must know that the ϕ-splitting of $\nabla_{n,p}$, which has length $p+1$, is minimal among all ϕ-splittings of length $p+1$. We are thus led to investigating the constraints satisfied by ϕ-splittings.

Lemma 3.20. *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 ϕ-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_1, x_0) be its ϕ-splitting, we have either $x_1 <^* \sigma_1$, which is impossible, or $x_1 = \sigma_1$ and $x_0 <^* \delta_{n-1}$. 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 $x_0 = \sigma_{n-2}...\sigma_m y$ holds, and, then, we find $x = \sigma_{n-1}\sigma_{n-2}...\sigma_m y$. □

Lemma 3.21. *Assume $n \geqslant 3$ and that $(x_p, ..., x_0)$ is the ϕ_n-splitting of some element of B_n^+. Then we have $x_p \geqslant^* \sigma_1$, $x_i \geqslant^* \delta_{n-1}\sigma_1$ for $p > i \geqslant 2$, and $x_1 \geqslant \delta_{n-1}$ whenever $p \geqslant 2$ holds.*

Proof. Assume that $(y_p, ..., y_0)$ is a sequence of $(n-1)$-braids such that $y_i <^* \delta_{n-1}$ holds for some i with $p > i \geqslant 1$. We claim that $(y_p\sigma_1, ..., y_2\sigma_1, y_1, y_0)$ is not a ϕ-splitting. By Lemma 3.20, we have $y_i = \sigma_{n-2}...\sigma_m y$ for some y in B_{m-1}^+ and $n-1 \geqslant m \geqslant 2$. As $i < p$ holds, by construction, we have

$$x_p \ltimes_n ... \ltimes_n x_i \geqslant \sigma_{n-1}y_i\sigma_1 = \sigma_{n-1}...\sigma_m y\sigma_1,$$

and, in order to show that $(y_p\sigma_1, ..., y_2\sigma_1, y_1, y_0)$ is not a ϕ-splitting, it is sufficient to show that some σ_k with $k \geqslant 2$ is a right divisor of $\sigma_{n-1}...\sigma_m y\sigma_1$. Now, $y\sigma_1$ belongs to B_{m-1}^+, hence involves σ_k's with $k < m-2$ only, while $\sigma_{n-1}...\sigma_m$ involves σ_k's with $k \geqslant m$, so they commute. It follows that σ_m is a right divisor of $\sigma_{n-1}...\sigma_m y\sigma_1$, and, therefore, $(y_p\sigma_1, ..., y_2\sigma_1, y_1, y_0)$ is not a ϕ-splitting.

Now, assume that $(x_p, ..., x_0)$ is a ϕ-splitting for some element of B_n^+. By construction, each factor x_i with $i \geqslant 1$ is divisible by σ_1 on the right, hence, in particular, we can write $x_i = y_i\sigma_1$ for $i \geqslant 2$. We complete with $y_1 = x_1$. By the claim above, we must have $y_i \geqslant^* \delta_{n-1}$ for $p > i \geqslant 2$, and $x_1 \geqslant^* \delta_{n-1}$. Now Proposition 3.13($i$) shows that $x \geqslant^* y$ implies $x\sigma_1 \geqslant^* y\sigma_1$ for all x, y. So $y_p \geqslant^* 1$ implies $x_p \geqslant^* \sigma_1$, and $y_i \geqslant^* \delta_{n-1}$ implies $x_i \geqslant^* \delta_{n-1}\sigma_1$ for $p > i \geqslant 2$. □

Proposition 3.22. *The braid $\nabla_{n,p}$ is the $<^*$-least upper bound of the elements of B_n^+ whose n-breadth is at most p.*

Proof. By Lemma 3.18(ii), $\nabla_{n,p}$ has n-breadth $p+1$, hence $x <^* \nabla_{n,p}$ holds whenever x has n-breadth $\leqslant p$.

Conversely, assume that the n-breadth of x is at least $p+1$. If it is $p+2$ or more, then $x >^* \nabla_{n,p}$ holds by definition of $<^*$. Otherwise, let $(x_p, ..., x_0)$ be the ϕ-splitting of x. Then Lemma 3.21 precisely says that the sequence $(x_p, ..., x_0)$ is lexicographically larger than or equal to the sequence $(\sigma_1, \delta_{n-1}\sigma_1, ..., \delta_{n-1}\sigma_1, \delta_{n-1}, 1)$, which is the ϕ_n-splitting of $\nabla_{n,p}$. Hence we have $x \geqslant^* \nabla_{n,p}$. □

4. Connection with the braid order

Defining a unique normal representative is of little interest in itself, unless the normal form has some specific additional properties. At the moment, the most interesting property of the flip normal form of Section 3 seems to be its connection with the standard linear order of braids sometimes called the Dehornoy order.

4.1. **The braid order.** In the sequel, we shall establish some connection between the $<^*$-order on B_n^+, *i.e.*, the ordering deduced from the ϕ-splitting, and the standard linear order of the braids investigated in various earlier works [16]. We recall the definition of the latter. We denote by B_∞^+ the union of all B_n^+'s (considering B_{n-1}^+ as a submonoid of B_n^+), and by B_∞ the group of fractions of B_∞^+, *i.e.*, the braid group on unboundedly many strands.

Definition 4.1. For x, y in B_∞, we say that $x < y$ holds if the quotient 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.

Proposition 4.2. (*i*) [12] *The relation $<$ is a linear ordering on B_∞ that is compatible with multiplication on the left; for each n, the ordered set $(B_n^+, <)$ is the interval $(\sigma_n^{-1}, \sigma_n)$ of $(B_\infty, <)$.*

(*ii*) [24] *The restriction of $<$ to B_∞^+ is a well-order.*

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

In early sources (up to [16]), the flipped variant of the above order was considered, namely the relation $\widetilde{<}$ refering to the letter σ_i with *minimal* index, instead of maximal as above. Both relations are essentially equivalent inasmuch as, for x, y in B_n, the relation $x < y$ is equivalent to $\phi_n(x) \mathrel{\widetilde{<}} \phi_n(y)$. However, as already noted by S. Burckel in [6], where the current version of the braid order is first used, many statements look better with $<$, and considering $\widetilde{<}$ seems to be an unfortunate remnant of the intrinsic limitations inherent to the initial approach.

4.2. **Adding brackets in a braid word.** In order to connect the braid orders $<^*$ and $<$ in Section 4.4 below, we shall compare the ϕ-normal form of Section 3 with some other normal form introduced by S. Burckel in his remarkable work on braids [7, 8], and we first need to introduce some notions from the latter. The original description of [7] is formulated in a specific tree setting, but the latter is equivalent to the iterated sequences of Section 2, and we can easily describe in our current framework the fragment of Burckel's construction needed for the sequel.

In Sections 2 and 3, we associated with every braid a certain iterated sequence, or, equivalently, a certain finite tree, called its ϕ-decomposition. Our construction can be called top–down, as we start from a braid that will correspond to the root of the tree and iteratively split it into several components until eventually atoms are reached, here the generators σ_i. By contrast, Burckel's approach is bottom–up, in that one starts with an arbitrary word w, *i.e.*, a sequence of generators σ_i, and let a tree $T(w)$ grow from w, so that the braid $\overline{w}$ appears at the end only. It will turn out that both constructions lead to the same final result if and only if the word w is ϕ-normal, as stated in Lemma 4.7(*iii*) below.

Burckel's construction consists in associating with every n-braid word w a certain iterated sequence $T_n(w)$ such that w is recovered when brackets are removed in $T_n(w)$, *i.e.*, $T_n(w)$ is a certain bracketing of w. For instance, we may think that, starting from the 1-sequence of (2.5), we wish to recover the 2-sequence of (2.4), or, equivalently, its addres list. We begin with an easy auxiliary notion.

Definition 4.3. Let $\boldsymbol{w}$ be an n-sequence of natural numbers (*resp.* of positive braids). Let $(\theta_p, ..., \theta_0)$ be the address list of $\boldsymbol{w}$, and $(e_p, ..., e_0)$ (*resp.* $(\sigma_{i_p}^{e_p}, ..., \sigma_{i_0}^{e_0})$) be its unbracketing. We define the *expanded address list* of $\boldsymbol{w}$ to be the sequence

consisting of θ_p repeated e_p times, followed by θ_{p-1} repeated e_{p-1} times, ..., up to θ_0 repeated e_0 times.

The expanded address list determines an n-sequence unambiguously: for an n-sequence in $\mathbb{N}$, we recover the entries by counting how many times each address is repeated in the expanded address list, and possibly add 0 at the end if 0^n is missing; for an n-sequence of braids, we moreover use the generator function to recover the indices of the σ_i'st: if the ith address is θ and the ith exponent is e, then, by construction, the ith entry of $\boldsymbol{w}$ must be s_θ^e.

Example 4.4. Let $\boldsymbol{w} = ((\sigma_1), (\sigma_2^2, \sigma_3), (\sigma_1, \sigma_2^2, 1))$. The exponent sequence of $\boldsymbol{w}$ is $\boldsymbol{w}^\bullet = ((1), (2, 1), (2, 1, 0))$, and its unbracketing is $(1, 2, 1, 1, 2, 0)$. On the other hand, the common address list of $\boldsymbol{w}$ and $\boldsymbol{w}^\bullet$ is $(20, 11, 10, 02, 01, 00)$. So the expanded address list of both $\boldsymbol{w}$ and of $\boldsymbol{w}^\bullet$ is $(20, 11, 11, 10, 02, 01, 01)$.

Conversely, starting from the latter sequence, we recover the (unexpanded) address list $(20, 11, 10, 02, 01, 00)$ by deleting repeated entries and adding a final 00, and we recover the exponent list $(1, 2, 1, 1, 2, 0)$ by counting repetitions. Then we recover $((1), (2, 1), (2, 1, 0))$ as the unique 2-sequence of numbers admitting the above address list and unbracketing. Finally, we recover $((\sigma_1), (\sigma_2^2, \sigma_3), (\sigma_1, \sigma_2^2, 1))$ as the unique 2-sequence of braids admitting the above exponent list.

An easy induction shows that a list of n-addresses is the expanded list address of some n-sequence (of numbers or of braids) if and only if it finishes with 0^n and each non-final entry is a successor (in the sense of Definition 2.12) of the next entry.

Definition 4.5. Let w be a length ℓ positive n-braid word. Put $\theta_0 := 0^{n-2}$, and inductively define θ_k to be the (unique) successor of θ_{k-1} satisfying $s_{\theta_k} = w(k)$. Then $T_n(w)$ (*resp.* $T_n^\bullet(w)$) is defined to be the unique $(n-2)$-sequence of braids (*resp.* of numbers) whose expanded address list is $(\theta_\ell, ..., \theta_0)$. The n-sequence $T_n(w)$ is called the *n-bracketing* of w.

The existence of $T_n(w)$ for every braid word w follows from Lemma 2.20 which implies that, for each address θ, every generator σ_i appears as associated with one, and only one, successor of θ.

Example 4.6. Let $w = \sigma_1\sigma_2\sigma_2\sigma_3\sigma_1\sigma_2\sigma_2$. In order to determine the 4-bracketing of w, we first compute its expanded address list as shown in Table 4, obtaining $(20, 11, 11, 10, 02, 01, 01)$. Then, as in Example 4.4, we conclude that $T_4(w)$ is $((\sigma_1), (\sigma_2^2, \sigma_3), (\sigma_1, \sigma_2^2, 1))$.

Remark. When described as above, the process for computing the bracketing $T_n(w)$ is parallel to the process of constructing the ϕ-normal word equivalent to w: in both cases, the point is to construct the address θ_k from the previous address θ_{k-1}. Here, we choose θ_k so that the corresponding σ is the last letter of the current remainder $w^{(k-1)}$, while, in the normalization process, we choose θ_k so that the corresponding σ is the least right divisor of the braid represented by $w^{(k-1)}$ with respect to the ordering of the generators encoded in θ_{k-1}.

It follows from the construction that, for each braid word w, the unbracketing of $T_n(w)$ is w if w finishes with σ_1, and its w followed by a trivial entry 1 otherwise—which makes the terminology "bracketing of w" coherent. The next lemma gathers what we need to know about the bracketing operation. We recall that, for $\boldsymbol{w}$ an n-sequence, $|\boldsymbol{w}|$ denotes the length of $\boldsymbol{w}$ as a sequence of $(n-1)$-sequences.

k	$w(k)$	θ_{k-1}	successors	names	θ_k
1	σ_2	00	10, 01, 00	$\sigma_3, \sigma_2, \sigma_1$	01
2	σ_2	01	10, 02, 01	$\sigma_3, \sigma_1, \sigma_2$	01
3	σ_1	01	10, 02, 01	$\sigma_3, \sigma_1, \sigma_2$	02
4	σ_3	02	10, 03, 02	$\sigma_3, \sigma_2, \sigma_1$	10
5	σ_2	10	20, 11, 10	$\sigma_1, \sigma_2, \sigma_3$	11
6	σ_2	11	20, 12, 11	$\sigma_1, \sigma_3, \sigma_2$	11
7	σ_1	11	20, 12, 11	$\sigma_1, \sigma_3, \sigma_2$	20

TABLE 4. Adding brackets in the word $\sigma_1\sigma_2\sigma_2\sigma_3\sigma_1\sigma_2\sigma_2$, phase 1: construction of the expanded list address; starting with 00, we scan the letters from the right, and choose the only successor of the current address whose name is the current letter.

Lemma 4.7. *Assume $n \geqslant 3$, and let w be a positive n-braid word.*

(i) Let $i = |T_n(w)|$. Then we have $|T_n(\sigma_k w)| = i$ for $k \leqslant n-2$ with i odd and for $k \geqslant 2$ with i even, and $|T_n(\sigma_k w)| = i+1$ otherwise.

(ii) Assume $w = \phi_n^i(u)v$ with u finishing with σ_1 and $|T_n(v)| = i$. Then $T_n(w)$ is the concatenation of $\phi_n^i T_n(u)$ and $T_n(v)$.

(iii) If w is ϕ-normal, then we have $T_n(w) = D_n(\overline{w})$.

Proof. (*i*) By construction, $T_n(\sigma_k w)$ is obtained from $T_n(w)$ by appending the additional entry σ_k at some address θ' which is some successor of the leftmost address θ occurring in $T_n(w)$, say $\theta' = \theta^{(m)}$. The hypothesis $|T_n(w)| = i$ implies that the first digit of θ is $i-1$. Saying that the length of $T_n(\sigma_k w)$ is $i-1$, and not i, means that θ' is not the 0-successor of θ, *i.e.*, that $m \neq 0$ holds. Now, by definition of $\boldsymbol{B}_n^+$, we have $s_{[\theta^{(0)}]} = \sigma_{n-1}$ for every address θ whose first digit is even, and $s_{[\theta^{(0)}]} = \sigma_1$ for every address θ whose first digit is odd. So $m > 0$ occurs if and only if we have $k \leqslant n-2$ if i is odd, and $k \geqslant 2$ if i is even.

(*ii*) Consider the inductive construction of $T_n(w)$, and let θ be the leftmost address in $T_n(v)$. Assume that i is even. The same argument as for (*i*) shows that, after completing $T_n(v)$ and in order to continue with the final letter σ_1 of u, we must choose the 0-successor of θ, which is 0^{n-2}, and, in particular, start a new $(n-3)$-sequence. From that point, the rest of the construction of $T_n(w)$ coincides with the construction of $T_n(u)$, and therefore $T_n(w)$ is the concatenation of $T_n(u)$ and $T_n(v)$. If i is odd, the argument is similar, with σ_{n-1} replacing σ_1, and the first digit of $[\theta]$ being 0 instead of 1.

(*iii*) We use induction on n. For $n = 2$, the result is obvious. Otherwise, assume that w is the ϕ_n-normal form of x. Let $(x_p, ..., x_0)$ be the ϕ_n-splitting of x, and, for each i, let w_i be the ϕ_{n-1}-normal form of x_i. By Lemma 3.10, we have $w = \phi_n^p(w_p)...\phi_n(w_1)w_0$. As w is assumed to be ϕ-normal, each of the words w_i with $i \geqslant 1$ finishes with σ_1. Repeated applications of (*ii*) give

$$T_n(w) = (\phi_n^p T_{n-1}(w_p)\ ,\ ...\ ,\ \phi_n T_{n-1}(w_1)\ ,\ T_{n-1}(w_0)).$$

By induction hypothesis, we have $T_{n-1}(w_i) = D_{n-1}(x_i)$ for each i, so we get

$$T_n(w) = (\phi_n^p D_{n-1}(x_p)\ ,\ ...\ ,\ \phi_n D_{n-1}(x_1)\ ,\ D_{n-1}(x_0)).$$

By (3.9), the latter sequence is $D_n(x)$. □

Of course, the result of Lemma 4.7(*iii*) fails if w is not a normal word.

At this point, we extended the framework of bracketings and iterated sequences to arbitrary braid words. So, we can now use the ordering $<^{\text{ShortLex}}$ for arbitrary positive braid words via their distinguished bracketings, *i.e.*, consider the relation $T_n^\bullet(u) <^{\text{ShortLex}} T_n^\bullet(v)$. The point is that, for convenient words, the word order so obtained is connected with the braid orders $<^*$ and $<$. We begin with $<^*$.

Lemma 4.8. *For x, y in B_n^+, we have*

$$x <^* y \iff T_n^\bullet(u) <^{\text{ShortLex}} T_n^\bullet(v), \tag{4.1}$$

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

Proof. We saw in Lemma 3.16 that $x <^* y$ is equivalent to $D_n^\bullet(x) <^{\text{ShortLex}} D_n^\bullet(y)$. Now, by Lemma 4.7(*iii*), we have $D_n(x) = T_n(u)$ and $D_n(y) = T_n(v)$, hence $D_n^\bullet(x) = T_n^\bullet(u)$ and $D_n^\bullet(y) = T_n^\bullet(v)$, and (4.1) directly follows. □

4.3. **The Burckel normal form.** We now appeal to the results of [7] to state a similar connection between the braid order $<$ and the sequence order $<^{\text{ShortLex}}$.

Definition 4.9. An n strand positive braid word w is said to be *Burckel normal* if $T_n^\bullet(w)$ is $<^{\text{ShortLex}}$-minimal among all expressions $T_n^\bullet(w')$ with $w' \equiv w$.

Burckel normal words are called *irreducible* in [7]. As the order $<^{\text{ShortLex}}$ is a well-order, each nonempty set of n-sequences in $\mathbb{N}$ contains a $<^{\text{ShortLex}}$-minimal element, and, therefore, every positive braid word is equivalent to a unique Burckel normal word, *i.e.*, every positive braid admits a unique Burckel normal representative.

Proposition 4.10 (Burckel, [7])**.** *For x, y in B_n^+, we have*

$$x < y \iff T_n^\bullet(u) <^{\text{ShortLex}} T_n^\bullet(v), \tag{4.2}$$

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

What Burckel does in [7] is to define a combinatorial operation called reduction so that, if a braid word w is not Burckel normal, then the reduct w' is equivalent to w, *i.e.*, represents the same braid, and it satisfies $T_n(w') <^{\text{ShortLex}} T_n(w)$. As the $<^{\text{ShortLex}}$-ordering is a well-ordering, it admits no infinite decreasing sequence, and reduction must terminate in finitely many steps. However, for $n \geqslant 4$, reduction is quite subtle, and finding the Burckel normal form of a given braid is an intricate procedure.

In the sequel, in addition to Proposition 4.10, we shall use the following easy result about Burckel normal words.

Lemma 4.11. *Assume that σ_1 divides x on the right. Then the Burckel normal form of x finishes with σ_1.*

Proof. Assume $x = y\sigma_1$, and let u, v be the Burckel normal forms of x and y. Then, we have $y^{-1}x = \sigma_1$, hence the relation $y < x$ holds, and, therefore, by Proposition 4.10, we have $T_n^\bullet(v) <^{\text{ShortLex}} T_n^\bullet(u)$, hence $T_n^\bullet(v\sigma_1) \leqslant^{\text{ShortLex}} T_n^\bullet(u)$ as, by construction, $T_n^\bullet(v\sigma_1)$ is the immediate successor of $T_n^\bullet(v)$, since it consists in keeping all brackets and adding 1 to the last entry. Now, $v\sigma_1$ is a word representing $y\sigma_1$, hence x, and the previous inequality shows that it is Burckel normal. □

4.4. **Connecting the normal forms and the orders.** At this point, two distinguished word representatives have been introduced for each positive braid, namely its flip normal form, and its Burckel normal form. They actually coincide:

Proposition 4.12. *The Burckel normal form coincides with the flip normal form.*

Proof. (Figure 5) We prove that every Burckel normal word is ϕ-normal using induction on $n \geqslant 2$. For $n = 2$, every word, namely every power of σ_1, is normal in both senses, and the result is true. Assume $n \geqslant 3$, and assume for a contradiction that w is an n-braid word that is Burckel normal and not ϕ-normal. There is a unique way of decomposing w as $w = w_p \ltimes_n ... \ltimes_n w_0$ in such a way that each word w_i with $i \geqslant 1$ finishes with σ_1. Then, as in the proof of Lemma 4.7(iii), repeated applications of Lemma 4.7(ii) give the equality

$$T_n(w) = (\phi_n^p T_{n-1}(w_p)\ ,\ ...\ ,\ \phi_n T_{n-1}(w_1)\ ,\ T_{n-1}(w_0)).$$

Assume first that some word w_i is not ϕ-normal. Then, by induction hypothesis, w_i is not Burckel normal, which means that there exists another word w_i', equivalent to w_i, and satisfying $T_{n-1}^\bullet(w_i') <^{\text{ShortLex}} T_{n-1}^\bullet(w_i)$. Let w' be the word obtained from w by replacing the subword w_i with w_i'. Then w' is equivalent to w, and, by construction, we have $T_n^\bullet(w') <^{\text{ShortLex}} T_n^\bullet(w)$: indeed, Lemma 4.7($ii$) implies that $T_n(w')$ is obtained from $T_n(w)$ by substituting the entry $T_{n-1}(w_i)$ with $T_{n-1}(w_i')$, which is $<^{\text{ShortLex}}$-smaller. Hence w is not Burckel normal.

Assume now that every word w_i is ϕ-normal. Put $x = \overline{w}$, and $x_i = \overline{w_i}$ for every i. The hypothesis that w is not ϕ-normal implies that $(x_p, ..., x_0)$ is not the ϕ-splitting of x, *i.e.*, that $x_p \ltimes_n ... \ltimes_n x_i \not\succcurlyeq \sigma_k$ holds for some $i \geqslant 1$ and some $k \geqslant 2$. Choose i maximal—thus corresponding to the shortest possible prefix of w that does not satisfy the ϕ-splitting condition. Then put $y = x_p \ltimes_n ... \ltimes_n x_i$, $z = x_{i-1} \ltimes_n ... \ltimes_n x_0$, and let $u = w_p \ltimes_n ... \ltimes_n w_i$ and $v = w_{i-1} \ltimes_n ... \ltimes_n w_0$. By construction, we have $x = \phi_n^i(y)\, z$ and $w = \phi_n^i(u)\, v$. By the choice of i, the sequence $(x_p, ..., x_i)$ is the ϕ_n-splitting of y. On the other hand, u is the Burckel normal form of y: indeed, u represents y by construction, and, if u' would be another representative of y satisfying $T_n^\bullet(u') <^{\text{ShortLex}} T_n^\bullet(u)$, then $w' = \phi_n^i(u')v$ would give a representative of x satisfying $T_n^\bullet(w') <^{\text{ShortLex}} T_n^\bullet(w)$, contradicting the hypothesis that w is Burckel normal.

Then our hypothesis is that $y = y'\sigma_k$ holds for some y' and some $k \geqslant 2$. By definition of the ϕ-splitting, we have $y \not\succcurlyeq \sigma_1$, and, by hypothesis, $y \not\succcurlyeq \sigma_k$. Hence y is divisible by the left lcm of σ_1 and σ_k. This implies $y' \not\succcurlyeq \sigma_1$: indeed, for $k \geqslant 3$, we have $y \not\succcurlyeq \sigma_1\sigma_k$, hence $y/\sigma_k \not\succcurlyeq \sigma_1$, and, for $k = 2$, we have $y \not\succcurlyeq \sigma_2\sigma_1\sigma_2$, hence $y/\sigma_2 \not\succcurlyeq \sigma_2\sigma_1$ and, *a fortiori*, $y/\sigma_2 \not\succcurlyeq \sigma_1$.

Let u' be the Burckel normal form of y'. We have $y' \not\succcurlyeq \sigma_1$, so Lemma 4.11 implies that u' finishes with σ_1. Moreover, we have $y'^{-1}y = \sigma_k$, hence $y' < y$. By Proposition 4.10, this implies $T_n^\bullet(u') <^{\text{ShortLex}} T_n^\bullet(u)$—this is the point.

Let $v' = \phi_n^i(\sigma_k)v$. So v' is $\sigma_k v$ if i is even, and is $\sigma_{n-k}v$ if i is odd. The point is that we have $k \geqslant 2$, and, therefore, in all cases, Lemma 4.7(i) implies $|T_n(v')| = |T_n(v)|$, hence $|T_n^\bullet(v')| = |T_n^\bullet(v)|$.

Finally, let $w' := \phi_n^i(u')\, v'$. By construction, w' represents $\phi_n^i(y')\, \phi_n^i(\sigma_k)z$, which is x, so w' is equivalent to w. On the other hand, we saw that u' finishes with σ_1, and, therefore, $\phi_n^i(u')$ finishes with σ_1 or σ_{n-1}, according to whether the length i

of $T_n(v)$ is even or odd. In both cases, Lemma 4.7(ii) implies

$$T_n(w') = \phi_n T_n(u') \frown T_n(v'), \quad \text{hence} \quad T_n^\bullet(w') = T_n^\bullet(u') \frown T_n^\bullet(v').$$

Then, the conjunction of $T_n^\bullet(u') <^{\text{ShortLex}} T_n^\bullet(u)$, which holds by hypothesis, and of $|T_n^\bullet(v')| = |T_n^\bullet(v)|$ implies $T_n^\bullet(w') <^{\text{ShortLex}} T_n^\bullet(w)$. This shows that w cannot be Burckel normal, and completes the proof. □

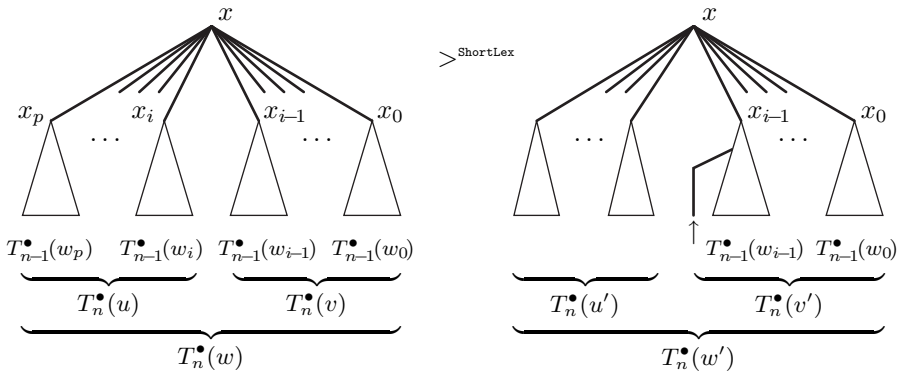

FIGURE 5. Proof of Proposition 4.12: if $(x_p, ..., x_0)$ is not the ϕ-splitting of x, then, at some point i, some generator σ_k with $k \geqslant 2$ is a right divisor of the remainder; then we can extract that σ_k from the left part $T_n(u)$ of the tree, and incorporate it into the right part $T_n^\bullet(v)$, as the vertical arrow shows; as the new left part $T_n^\bullet(u')$ must be $<^{\text{ShortLex}}$-smaller than the old one $T_n^\bullet(u)$, and as the new right part cannot be really larger, the resulting new tree $T_n^\bullet(w')$ is $<^{\text{ShortLex}}$-smaller than the initial tree $T_n^\bullet(w)$, which shows that w is not Burckel normal.

It can be observed that the previous argument is reminiscent of Burckel's reduction method as described in [7] or [16, Chapter 4]; it is also similar to the well-known exchange lemma in a Coxeter group: like in the latter, the point is to extract a generator and push it to the final position while possibly changing its name. Some variants are possible: for instance, one can use an induction on the rank of the word $T_n(w)$ in the well-order $<^{\text{ShortLex}}$. But, in each case, one seems to have to appeal to Proposition 4.10 at some point.

We immediately deduce:

Proposition 4.13. *For all positive braids x, y, 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 4.12, u and v also are the Burckel normal representatives of x and y. Then the equivalences

$$x < y \iff T_n^\bullet(u) <^{\text{ShortLex}} T_n^\bullet(v) \iff x <^* y$$

follow from Lemma 4.8 and Proposition 4.10. □

Once we know that the two normal forms and the two braid orders coincide, each one inherits the properties previously established for the other.

Corollary 4.14. (*i*) *The Burckel normal form can be computed using the algorithm of Table 2, and therefore in quadratic time w.r.t. the length of the initial word.*

(*ii*) *The braid order* $<$ *can be decided in quadratic time: if* w *is an (non necessarily positive)* n*-braid word of length at most* ℓ*, then whether* $\overline{w} > 1$ *holds can be decided in time* $O(\ell^2 n^3 \log n)$*.*

Proof. Point (*i*) is clear, as we know that the flip normal form can be computed as indicated. As for (*ii*), we first observe that, if u, v are positive n-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 3.6(*ii*), we can compute the flip decompositions $T_n^\bullet(u)$ and $T_n^\bullet(v)$ within the indicated amount of time; the extra cost of then comparing these sequences with respect to the `ShortLex`-ordering is linear in ℓn. Now, 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 claim, can be decided in time $O(\ell^2 n^5 \log n)$. Actually, we can drop the exponent of n to 3 because an upper bound for the ϕ-normal form is $O(\ell \ell_c n \log n)$, where ℓ_c denotes the canonical length, defined to be, say, 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 process. □

In the original approach of [7], the Burckel normal form comes as the final result of an iterated reduction process whose termination is guaranteed by some well-order of transfinite length, and no complexity analysis of the latter has been published so far.

Another direct consequence of Proposition 4.13 is that the order $<^*$ of Section 3.3 inherits the properties of the order $<$.

Corollary 4.15. *The order* $<^*$ *is compatible with multiplication on the left, and* $x <^* x\sigma_i$ *always holds.*

4.5. **The shift splitting.** One of the outcomes of the current approach is a simple connection between the braid order $<$ on B_n^+ and its restriction to B_{n-1}^+: this is clear in the statement of Definition 3.12, which we now know is a definition of $<$. Here we give an alternative formulation that avoids using the flip operation repeatedly, and is therefore perhaps more natural. This description involves the shift endomorphism of B_∞^+.

Definition 4.16. For every positive braid x, we denote by $x^\#$ the image of x under the *shift* endomorphism of B_∞^+ that maps σ_i to σ_{i+1} for each i. For $p \geqslant 0$, we define $x^{[p]}$ to be x if p is even, and $x^\#$ if p is odd.

An immediate verification on the σ_i's shows that

$$\phi_n(x) = \phi_{n-1}(x)^\# \tag{4.3}$$

holds for every x in B_{n-1}^+. Adapting Proposition 3.8 gives:

Proposition 4.17. *For each braid* x *in* B_n^+*, there exists a unique sequence* $(x_p, ..., x_0)$ *of braids in* B_{n-1}^+ *satisfying*

$$x = x_p^{[p]} \cdot ... \cdot x_3^\# \cdot x_2 \cdot x_1^\# \cdot x_0 \tag{4.4}$$

such that the only σ_j dividing $x_p^{[p]} \cdot ... \cdot x_i^{[i]}$ on the right is σ_1 if i is positive even, and σ_{n-1} if i is odd. For each i, we have $x_i = \phi_{n-1}^i(x'_i)$, where $(x'_p, ..., x'_0)$ is the ϕ-splitting of x.

Definition 4.18. The sequence $(x_p, ..., x_0)$ involved in Proposition 4.17 will be called the *#-splitting* of x.

The only difference between the #- and ϕ-splittings is a flip for the entries with odd rank (counting from the right, as always in this paper). For instance, we saw that the ϕ-splitting of Δ_4^2 is $(\sigma_1, \sigma_2\sigma_1^2, \sigma_2\sigma_1, \Delta_3^2)$. So, the #-splitting of Δ_4^2 is

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

Rewriting Definition 3.12 in this context and using the equality of $<^*$ and $<$, we obtain the following inductive characterization of the braid order:

Proposition 4.19. *Assume $x, y \in B_n^+$. Let $(x_p, ..., x_0)$ and $(y_q, ..., y_0)$ be the #-splittings of x and y into sequences of $(n-1)$-braids. Then $x < y$ holds in B_n^+ if and only if we have either $p < q$, or $p = q$ and there exists r satisfying $x_i = y_i$ for $p \geqslant i > r$ and, respectively, $x_r < y_r$ in B_{n-1}^+ if r is even, and $\phi_{n-1}(x_r) < \phi_{n-1}(y_r)$ in B_{n-1}^+ if r is odd.*

So the order on B_n^+ appears as a `ShortLex`-extension of the order on B_{n-1}^+, with an extra ingredient, namely flipping the entries of odd rank. Note that, for $n = 3$, the ϕ- and #-splittings coincide, as ϕ_2 is the identity, and, therefore, the order on B_3^+ is a `ShortLex`-extension of the usual order on $\mathbb{N}$. Things become more complicated from $n = 4$ as, then, ϕ_n is not trivial.

5. Open questions and further work

5.1. **Braids.** The proof of Proposition 4.12 heavily depends on Burckel's Proposition 4.10, a highly non trivial combinatorial result in the case of 4 strands and more.

Question 5.1. *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.

We have so far no general answer. We mention below some partial results toward a positive answer to Question 5.1 (i), *i.e.*, toward the result that, for all braids x, y, the relation $x <^* y$ implies $x < y$—as we are dealing with linear orderings, one implication is enough. Here we consider special values for y. By Propositions 3.13(ii) and 4.2(i), we already know that $x <^* \sigma_{n-1}$ is equivalent to $x < \sigma_{n-1}$, as both are equivalent to $x \in B_{n-1}^+$. We shall prove two more results of this kind.

Lemma 5.2. *Assume $x = x_p \ltimes_n ... \ltimes_n x_0$ with $n \geqslant 3$, $p \geqslant 0$ and $x_p, ..., x_0 \in B_{n-1}^+$. Then we have*

$$x^{-1}\,\nabla_{n,p} = x_0^{-1} \cdot \Delta_n x_1^{-1} \cdot \Delta_n x_2^{-1} ... \cdot \Delta_n x_p^{-1} \cdot \Delta_{n-1}^{-p}, \tag{5.1}$$

and $x < \nabla_{n,p}$ holds.

Proof. We use induction on $p \geqslant 0$. For $p = 0$, (5.1) reduces to $x_0^{-1} = x_0^{-1} \cdot 1$. Assume $p \geqslant 1$, and let $y := x_p \ltimes_n ... \ltimes_n x_1$. Then we have $x = y \ltimes_n x$, *i.e.*, $x = \phi_n(y)\, x_0$, and we find

$$\begin{aligned}
x^{-1}\, \nabla_{n,p} &= x_0^{-1}\, \phi_n(y^{-1})\, \nabla_{n,p} && \text{by hypothesis}\\
&= x_0^{-1}\, \phi_n(y^{-1})\, \Delta_n^p\, \Delta_{n-1}^{-p} && \text{by (3.14)}\\
&= x_0^{-1}\, \Delta_n\, y^{-1}\, \Delta_n^{p-1}\, \Delta_{n-1}^{-p} && \text{as } \phi_n(y) = \Delta_n y \Delta_n^{-1}\\
&= x_0^{-1}\, \Delta_n\, y^{-1}\, \nabla_{n,p-1}\, \Delta_{n-1}^{-1} && \text{by (3.14) again}\\
&= x_0^{-1}\, \Delta_n\, x_1^{-1}\, \Delta_n x_2^{-1} \ldots \Delta_n x_p^{-1}\, \Delta_{n-1}^{-p+1}\, \Delta_{n-1}^{-1} && \text{by induction hypothesis,}
\end{aligned}$$

which is (5.1). □

Proposition 5.3. *For every x in B_n^+, the relation $x <^* \nabla_{n,p}$ implies $x < \nabla_{n,p}$.*

Proof. Assume $x <^* \nabla_{n,p}$. By Proposition 3.22, the n-breadth of x is at most p, and we can write $x = x_p \ltimes_n ... \ltimes_n x_0$ for some $x_p, ..., x_0$ in B_{n-1}^+. We then apply Lemma 5.2: (5.1) leads to an expression of the quotient $x^{-1}\nabla_{n,p}$ in which the letter σ_{n-1} occurs p 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 $\Delta_n = \nabla_{n,1}\Delta_{n-1}$, while the negative factors x_i^{-1} and Δ_{n-1}^{-p} belong to B_{n-1} and therefore can be expressed using neither σ_{n-1} nor σ_{n-1}^{-1}. Therefore $x < \nabla_{n,p}$ holds. □

Corollary 5.4. *For every x in B_n^+, the relation $x <^* \Delta_n^p$ implies $x < \Delta_n^p$.*

Proof. We use induction on $n \geqslant 2$. The result is obvious for $n = 2$. Assume $n \geqslant 3$, and $x <^* \Delta_n^p$. By Lemma 3.18(*iii*), the n-breadth of Δ_n^p is $p+1$. Hence, either the n-breadth of x is at most p, in which case we have $x < \nabla_{n,p}$ by Proposition 5.3, and therefore $x < \Delta_n^p$ as $\nabla_{n,p} < \Delta_n^p$ holds, or the n-breadth of x is $p+1$. Then let $(x_p, ..., x_0)$ be the ϕ-splitting of x. In view of the constraints on ϕ-splittings established in Lemma 3.21, and of the value of the ϕ-decomposition of Δ_n^p given in Lemma 3.18(*ii*), the only possibility is $x_p = \sigma_1$, $x_i = \delta_{n-1}\sigma_1$ for $p > i \geqslant 2$, $x_1 = \delta_{n-1}$, and $x_0 <^* \Delta_{n-1}^n$. By induction hypothesis, $x_0 <^* \Delta_{n-1}^n$ implies $x_0 < \Delta_{n-1}^n$. Then we have $x^{-1}\Delta_n^p = x_0^{-1}\Delta_{n-1}^p$, and $x < \Delta_n^p$ follows. □

By varying on the theme above, we could state a number of similar compatibility results between $<^*$ and $<$, but, so far, we have no complete argument. The main missing piece is a direct proof of the fact that $\nabla_{n,p} \leqslant^* x$ implies $\nabla_{n,p} \leqslant x$. If the ϕ_n-splitting of x is $(y_{p+1}\sigma_1, ..., y_2\sigma_1, x_1, x_0)$, one deduces from (5.1)

$$\nabla_{n,p}^{-1}\, x = \Delta_{n-1}^p \phi_n(y_{p+1}) \cdot \sigma_{n-1}\Delta_n^{-1}\phi_n(y_p) \cdot \ldots \cdot \sigma_{n-1}\Delta_n^{-1}\phi_n(y_2) \cdot \sigma_{n-1}\Delta_n^{-1}\phi_n(x_1) \cdot x_0.$$

Unfortunately, the condition $x \geqslant^* \delta_{n-1}$ fails to imply $\sigma_{n-1}\Delta_n^{-1}\phi_n(x) > 1$ in general, and we cannot conclude that $x \geqslant \nabla_{n,p}$ holds in this way.

5.2. **Artin–Tits monoids and other Garside monoids.** We proved in Section 2 that $\boldsymbol{M}$-decompositions exist in every monoid M that is locally Garside on the right and 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, in this case, every subset of S generates a parabolic submonoid that is closed, *i.e.*, we recall from Section 1, is closed under left lcm and left divisor. Thus, coverings

similar to the ones of Section 3 exist for every Artin–Tits monoid M, and each of them leads to a normal form for the elements of M. Then, we can copy the construction of Section 3.3 and define a linear ordering $<_{\boldsymbol{M}}$ on M by considering the `ShortLex`-ordering on $\boldsymbol{M}$-normal words, *i.e.*, by taking (3.12) as a definition.

Question 5.5. *Let M be an Artin–Tits monoid. Is any of the linear orders $<_{\boldsymbol{M}}$ compatible with multiplication on the left?*

In type A_n, *i.e.*, if M is a braid monoid, the answer to Question 5.5 is positive, as was stated in Corollary 4.15. But our proof of that result heavily depends on the connection between the orders $<^*$ and $<$, and, therefore, it is quite specific. The first step toward a possible positive answer to Question 5.5 would presumably consist in getting a direct proof in the case of braids, *i.e.*, in answering Question 5.1(*ii*).

Another possible extension of the current work consists in addressing the braid order again, but in connection with other monoids. In particular, Laver's result of Proposition 4.2(*ii*) implies that the restriction of $<$ to any finitely generated submonoid of B_∞ generated by conjugates of the σ_i's is a well-order. It follows that the restriction of $<$ to the Birman–Lo–Lee monoids BKL_n of [4] is a well-order. The latter monoids are Garside monoids, and they are directly relevant for the approach developed here. In particular, natural alternating normal forms can be defined, and investigating their connection with the braid order is an obvious task. J. Fromentin has promising results in this direction.

5.3. **Geometric and dynamic properties.** Not much is known about the flip (or Burckel) normal form of braids. Of course, as every braid admits a canonical decomposition as a fraction xy^{-1} with x, y positive braids with no common right divisor, we can extend the ϕ-normal form on 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, we raise

Question 5.6. *For $n \geqslant 3$, does the ϕ-normal form on B_n define a (bi)-automatic structure?*

Although the proof is not yet written, we think the answer might be positive: using the constructions of [13], it should be easy to prove that the set of all ϕ-normal braid words is a regular language, and to construct finite state automata recognizing the product by one letter on the left and on the right. Finally, going from the monoid to to group should be standard.

Also it might be interesting to investigate the dynamical properties of the ϕ-normal form, along the lines addressed in [3, 30, 26, 25, 27]. The generic problem is to study growth and stabilization in random walks in B_n or, here, B_n^+: one compares the successive normal forms, typically looking at whether the first factors become eventually constant. Each new normal form induces a new problem. Let $b(x)$ denote the n-breadth of x, and $c_i(x)$ denote the ith entry (starting from the right) in the ϕ-splitting of x.

Question 5.7. *Let $(X_k)_{k\geqslant 0}$ be the random walk in B_n^+ defined by $X_{k+1} = \sigma_i X_k$ with i equidistributed in $\{1, ..., n-1\}$. What are the distributions of $\frac{1}{k}b(X_k)$ and $\frac{1}{k}|c_i(X_k)|$ for each fixed i?*

Preliminary experiments suggest that the length of $c_0(X_k)$ grows like $k/(n+2)$, while $c_i(X_k)$ with $i \geqslant 1$ tends to stabilize to $\delta_{n-1}\sigma_1$, of constant length. Such

phenomena are presumably connected with their counterpart for the right greedy normal form, where Δ_n factors accumulate on the right. Finally, $b(X_k)$ 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] R. Charney, *Artin groups of finite type are biautomatic*, Math. Ann. **292-4** (1992) 671–683.

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

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

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

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

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

[15] P. Dehornoy, *Still another approach to the braid ordering*, Pacific J. Math., to appear; math.GR/0506495.

[16] P. Dehornoy, I. Dynnikov, D. Rolfsen, B. Wiest, *Why are braids orderable?*, Panoramas & Synthèses vol. 14, Soc. Math. France (2002).

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

[23] C. Kassel & V. Turaev, *Braid groups*, Springer (2007).

[24] 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.

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

[26] J. Mairesse & F. Mathéus, *Random walks on free products of cyclic groups*, J. London Math. Soc., to appear.

[27] J. Mairesse & F. Mathéus, *Randomly growing braid on three strands and the manta ray*, Ann. Appl. Probab., to appear; math.PR/0512391.

[28] J. McCammond, *An introduction to Garside structures*, Preprint (2005).

[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) .

[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