Pacific Journal of Mathematics

STILL ANOTHER APPROACH TO THE BRAID ORDERING

PATRICK DEHORNOY

Volume 232 No. 1 September 2007

PACIFIC JOURNAL OF MATHEMATICS
Vol. 232, No. 1, 2007

STILL ANOTHER APPROACH TO THE BRAID ORDERING

PATRICK DEHORNOY

We develop a new approach to the linear ordering of the braid group B_n, based on investigating its restriction to the set $\mathrm{Div}(\Delta_n^d)$ of all divisors of Δ_n^d in the monoid B_∞^+, that is, to positive n-braids whose normal form has length at most d. In the general case, we compute several numerical parameters attached with the finite orders $\mathrm{Div}(\Delta_n^d)$. In the case of 3 strands, we moreover give a complete description of the increasing enumeration of $\mathrm{Div}(\Delta_3^d)$. We deduce a new and especially direct construction of the ordering on B_3, and a new proof of the result that its restriction to B_3^+ is a well-ordering of ordinal type ω^ω.

This paper investigates the connection between the Garside structure of Artin's braid groups and their distinguished linear ordering, sometimes called the Dehornoy ordering. This leads to a new, alternative construction of the ordering.

Artin's braid groups B_n are endowed with several interesting combinatorial structures. One of them stems from Garside's analysis [1969] and is now known as a Garside structure [Dehornoy 2002; McCammond 2005]. It describes B_n as the group of fractions of a monoid B_n^+ with a rich divisibility theory. This theory gives a unique normal decomposition of every braid in B_n into simple braids, which are the divisors of Garside's fundamental braid Δ_n, a finite family of B_n^+ that is in one-to-one correspondence with the permutations of n objects. One obtains a natural graduation of the monoid B_n^+ by considering the family $\mathrm{Div}(\Delta_n^d)$ of all divisors of Δ_n^d, which also are the elements of B_n^+ whose normal forms have length at most d.

On the other hand, the braid groups are equipped with a distinguished linear ordering which is compatible with multiplication on the left and admits a simple combinatorial characterization [Dehornoy 1994]: a braid x is smaller than another braid y if, among all expressions of the quotient $x^{-1}y$ in the standard generators σ_i, there exists at least one expression in which the generator σ_m with maximal (or minimal) index m appears only positively, that is, σ_m occurs, but σ_m^{-1} does not. Several deep results about that ordering have been proved, for example, that

MSC2000: primary 20F36; secondary 05A05, 20F60.

Keywords: braid group, orderable group, well-ordering, normal form, fundamental braid.

its restriction to B_∞^+ is a well-ordering. A number of equivalent constructions are known [Dehornoy et al. 2002].

Although both are combinatorial, the previous structures remain mostly unconnected—and connecting them is among the most natural questions of braid combinatorics. For degree 1, that is, for simple braids, the linear ordering corresponds to a lexicographical ordering of the associated permutations [Dehornoy 1999]. But this connection does not extend to higher degrees, and almost nothing is known about the restriction of the linear ordering to positive braids of a given degree. In particular, no connection is known between the Garside normal form and the alternative normal form constructed by S. Burckel [1997; 1999; 2001] which makes comparison with respect to the linear ordering easy. For example, the Garside normal form of Δ_3^{2d} is $(\sigma_1\sigma_2\sigma_1)^{2d}$, while its Burckel normal form is $(\sigma_2\sigma_1^2\sigma_2)^d\sigma_1^{2d}$.

This paper investigates the finite linearly ordered sets $(\mathrm{Div}(\Delta_n^d), <)$. A nice way of thinking about this structure is to view the increasing enumeration of $\mathrm{Div}(\Delta_n^d)$ as a distinguished path from 1 to Δ_n^d in the Cayley graph of B_n. Completely describing this path would arguably solve optimally the rather vague task of connecting the Garside and the ordered structures of braid groups. The combinatorics of such a description seems to be extremely intricate, and it remains out of reach for the moment, but we prove partial results in this direction.

(i) In the general case, we determine some numerical parameters associated with $(\mathrm{Div}(\Delta_n^d), <)$, which in some sense measure its size. For small values of n and d, we find explicit values.

(ii) In the special case $n = 3$, we completely describe the increasing enumeration of $(\mathrm{Div}(\Delta_n^d), <)$.

Specifically, the parameters we investigate are the complexity and the heights. The complexity $c(\Delta_n^d)$ is defined as the maximal number of σ_{n-1} occurring in an expression of Δ_n^d containing no σ_{n-1}^{-1}. We connected the complexity with the termination of the handle reduction algorithm in [Dehornoy 1997], but left its determination as an open question. The r-height $h_r(\Delta_n^d)$ is defined to be the number of r-jumps in the increasing enumeration of $(\mathrm{Div}(\Delta_n^d), <)$ (augmented by 1), where the term r-jump refers to some natural filtration of the linear ordering $<$ by a sequence of partial orderings $<_r$. When r increases, the r-jumps are higher and higher, so $h_r(\Delta_n^d)$ counts how many big jumps exist in $(\mathrm{Div}(\Delta_n^d), <)$. Here, we prove that the complexity $c(\Delta_n^d)$ equals the height $h_{n-1}(\Delta_n^d)$ (Proposition 2.19), and that, for each r, the r-height $h_r(\Delta_n^d)$ is the number of divisors of Δ_n^d whose d-th factor of the normal form is right divisible by Δ_r (Proposition 3.11). Together with the combinatorial results of [Dehornoy 2007], this allows for computing the explicit values listed in Table 1, and for establishing various inductive formulas (Propositions 3.15 and 3.17, among others).

Besides the enumerative results, we also prove a general structural result that connects the ordered set $(\mathrm{Div}(\Delta_n^d), <)$ with subsets of $(\mathrm{Div}(\Delta_{n-1}^d), <)$ (Corollary 3.6). This result suggests an inductive method for directly constructing the increasing enumeration of $(\mathrm{Div}(\Delta_n^d), <)$ starting from those of $(\mathrm{Div}(\Delta_{n-1}^d), <)$ and $(\mathrm{Div}(\Delta_n^{d-1}), <)$. This approach is completed here for $n = 3$ (Proposition 4.6). In some sense, 3 strand braids are simple objects, and the result may appear as of only modest interest; however, the order on B_3^+ is a well-ordering of ordinal type ω^ω and hence not such a simple object. The interesting point is that this approach leads to a new, alternative construction of the braid ordering, with, in particular, a new and simple proof for the so-called Comparison Property at the heart of the construction (it guarantees the ordering's linearity). In this way, one obtains not just another ordering construction among many [Dehornoy et al. 2002] but, arguably, the optimal one. After the initial inductive definition is correctly stated, it makes all proofs simple and also makes explicit the connection to the Garside structure.

The paper is organized as follows. After an introductory section recalling basic properties and setting the notation, we introduce the parameters $c(\Delta_n^d)$ and $h_r(\Delta_n^d)$ in Section 2 and establish how they are connected. In Section 3, we connect in turn $h_r(\Delta_n^d)$ to the number of n-braids whose d-th factor in the normal form satisfies certain constraints, and deduce explicit values. Finally, in Section 4, we study $(\mathrm{Div}(\Delta_3^d), <)$, describe its increasing enumeration, and construct its braid ordering.

1. Background and preliminary results

Our notation is standard, and we refer to textbooks like [Birman 1974] or [Epstein et al. 1992] for basic results about braid groups. We recall that the n strand braid group B_n is defined for $n > 1$ by the presentation

$$(1\text{-}1) \qquad B_n = \left\langle \sigma_1, \ldots, \sigma_{n-1} \,;\, \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & \text{for } |i-j| \geqslant 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{for } |i-j| = 1 \end{array} \right\rangle,$$

while, for $n = 1$, we let B_1 be the trivial group. The next group B_2 is freely generated by σ_1. The elements of B_n are called n strand braids, or simply *n-braids*. We use B_∞ for the group generated by an infinite sequence of σ_i's subject to the relations of (1-1), that is, the direct limit of all B_n's with respect to the inclusion of B_n into B_{n+1}.

By definition, every n-braid x admits (infinitely many) expressions in terms of the generators σ_i, $1 \leqslant i < n$. Such an expression is called an n strand *braid word*. Two braid words w, w' representing the same braid are said to be *equivalent*; the braid represented by a braid word w is denoted $[w]$.

1A. *Positive braids and the element Δ_n.* We denote by B_n^+ the monoid admitting the presentation (1-1), and by B_∞^+ the union (direct limit) of all B_n^+'s. The elements of B_n^+ are called *positive* n-braids. In B_∞^+, no element except 1 is invertible, and we have a natural notion of divisibility:

Definition 1.1. For x, y in B_n^+, we say that x is a *left divisor* of y, denoted $x \preccurlyeq y$, or, equivalently, that y is a *right multiple* of x, if $y = xz$ holds for some z in B_n^+. We denote by $\mathrm{Div}(y)$ the (finite) set of all left divisors of y in B_n^+.

The monoid B_n^+ is not commutative for $n \geqslant 3$, and therefore there are distinct, but symmetric, notions of a right divisor and a left multiple; however, we shall mostly use left divisors. Note that x is a (left) divisor of y in the sense of B_n^+ if and only if it is a (left) divisor in the sense of B_∞^+, so there is no need to specify the index n.

According to Garside theory [1969], B_n^+ equipped with the left divisibility relation is a lattice: any two positive n-braids x, y admit a greatest common left divisor $\gcd(x, y)$, and a least common right multiple $\mathrm{lcm}(x, y)$. A special role is played by the lcm Δ_n of $\sigma_1, \ldots, \sigma_{n-1}$, which can be defined inductively by

$$\Delta_1 = 1, \qquad \Delta_n = \sigma_1\sigma_2 \ldots \sigma_{n-1}\, \Delta_{n-1}. \tag{1-2}$$

It is well known that Δ_n^2 belongs to the center of B_n (and even generates it for $n \geqslant 3$), and that the flip automorphism ϕ_n of B_n corresponding to conjugation by Δ_n exchanges σ_i and σ_{n-i} for $1 \leqslant i \leqslant n-1$.

In B_n^+, the left and the right divisors of Δ_n coincide, and they make a finite sublattice of $(B_n^+, \preccurlyeq)$ with $n!$ elements. These braids will be called *simple*. When braid words are represented by diagrams as mentioned in Figure 1, simple braids are those positive braids that can be represented by a diagram in which any two strands cross at most once.

By mapping σ_i to the transposition $(i, i+1)$, one defines a surjective homomorphism π of B_n onto the symmetric group $\mathfrak{S}_n$. The restriction of π to simple braids is a bijection: for every permutation f of $\{1, \ldots, n\}$, there exists exactly one

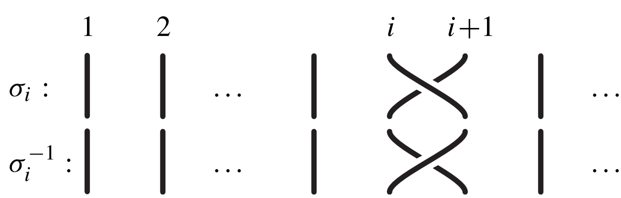

Figure 1. One associates to every n strand braid word w an n strand braid diagram by stacking elementary diagrams as above. Two braid words are equivalent if and only if the associated diagrams are the projections of ambient isotopic figures in $\mathbb{R}^3$, that is, one can deform one diagram into the other without allowing the strands to cross or moving the endpoints.

simple braid x satisfying $\pi(x) = f$. It follows that the number of simple n-braids is $n!$.

Example 1.2. The set $\mathrm{Div}(\Delta_3)$ consists of six elements, namely 1, σ_1, σ_2, $\sigma_2\sigma_1$, $\sigma_1\sigma_2$, and Δ_3. In examples, we shall often use the shorter notation $\mathtt{a}$ for σ_1, $\mathtt{b}$ for σ_2, etc. Thus, the six simple 3-braids are 1, $\mathtt{a}$, $\mathtt{b}$, $\mathtt{ba}$, $\mathtt{ab}$, $\mathtt{aba}$.

1B. ***The normal form.*** For each positive n-braid x distinct from 1, the simple braid $\gcd(x, \Delta_n)$ is the maximal simple left divisor of x, and we obtain a distinguished expression $x = x_1 x'$ with x_1 simple. By decomposing x' in the same way and iterating, we obtain the so-called normal expression [El-Rifai and Morton 1994; Epstein et al. 1992].

Definition 1.3. A sequence $(x_1, \ldots, x_d)$ of simple n-braids is said to be *normal* if, for each k, one has $x_k = \gcd(\Delta_n, x_k \ldots x_d)$.

Clearly, each positive braid admits a unique normal expression. It will be convenient to consider the normal expression as unbounded on the right by completing it with as many trivial factors 1 as needed. In this way, we can speak of the *d-th factor* (in the normal form) of x for each positive braid x. We say that a positive braid has *degree d* if d is the largest integer such that the d-th factor of x is not 1. We shall use the following two properties of the normal form:

Lemma 1.4 [El-Rifai and Morton 1994]. *Suppose $(x_1, \ldots, x_d)$ is sequence of simple n-braids. It is normal if and only if, for each $k < d$, each σ_i that divides x_{k+1} on the left divides x_k on the right.*

Lemma 1.5 [El-Rifai and Morton 1994]. *For x a positive braid in B_n^+, the following are equivalent*:

(i) *The braid x belongs to* $\mathrm{Div}(\Delta_n^d)$, *that is, is a* (*left or right*) *divisor of* Δ_n^d;

(ii) *The degree of x is at most d.*

Example 1.6. There are 19 divisors of Δ_3^2, which also are the 3-braids of degree at most 2. Their enumeration in normal form—in an ordering that may seem strange now, but should become familiar soon—is: 1, $\mathtt{a}$, $\mathtt{a{\cdot}a}$, $\mathtt{b}$, $\mathtt{ba}$, $\mathtt{ba{\cdot}a}$, $\mathtt{b{\cdot}b}$, $\mathtt{b{\cdot}ba}$, $\mathtt{ab}$, $\mathtt{aba}$, $\mathtt{aba{\cdot}a}$, $\mathtt{ab{\cdot}b}$, $\mathtt{ab{\cdot}ba}$, $\mathtt{a{\cdot}ab}$, $\mathtt{aba{\cdot}b}$, $\mathtt{aba{\cdot}ba}$, $\mathtt{ba{\cdot}ab}$, $\mathtt{aba{\cdot}ab}$, $\mathtt{aba{\cdot}aba}$.

By Lemma 1.5, every divisor of Δ_n^d can be expressed as the product of at most d divisors of Δ_n, so we certainly have $\#\mathrm{Div}(\Delta_n^d) \leqslant (n!)^d$ for all n, d.

1C. ***The braid ordering.***

Definition 1.7. Let w be a nonempty braid word. We say that σ_m is the *main* generator in w if σ_m or σ_m^{-1} occurs in w, but no $\sigma_i^{\pm 1}$ with $i > m$ does. We say that w is *σ-positive* if the main generator occurs only positively in w, and similarly it is *σ-negative* if that generator occurs negatively.

A positive nonempty braid word, that is, one that contains no σ_i^{-1} at all, is σ-positive, but the inclusion is strict: for instance, $\sigma_1^{-1}\sigma_2$ is not positive, but it is σ-positive, as its main generator, namely σ_2, occurs positively (with one σ_2) but not negatively (no σ_2^{-1}).

The following two properties have received a number of independent proofs [Dehornoy et al. 2002]:

Property A. *A σ-positive braid word does not represent* 1.

Property C. *Every braid except* 1 *can be represented by a σ-positive word or by a σ-negative word.*

Building on these results, it is straightforward to order the braids:

Definition 1.8. If x, y are braids, we say that $x < y$ holds if the braid $x^{-1}y$ admits at least one σ-positive representative.

It is clear that the relation $<$ is transitive and compatible with multiplication on the left; Property A implies that $<$ has no cycle and hence is a strict partial order, and Property C then implies that it is actually a linear order.

As every nonempty positive braid word is σ-positive, $x \preccurlyeq y$ implies $x \leqslant y$ for all positive braids x, y. The converse is not true: σ_1 is not a left divisor of σ_2, but $\sigma_1 < \sigma_2$ holds because $\sigma_1^{-1}\sigma_2$ is a σ-positive word.

Example 1.9. The increasing enumeration of the set $\mathrm{Div}(\Delta_3)$ is

$$\mathtt{1} < \mathtt{a} < \mathtt{b} < \mathtt{ba} < \mathtt{ab} < \mathtt{aba}.$$

For instance, we have $\mathtt{ba} < \mathtt{ab}$, that is, $\sigma_2\sigma_1 < \sigma_1\sigma_2$ because the quotient, namely $\sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2$ (or $\mathtt{ABab}$), also admits the expression $\sigma_2\sigma_1^{-1}$, a σ-positive word. Similarly, the reader can check that the increasing enumeration of $\mathrm{Div}(\Delta_3^2)$ is the one given in Example 1.6.

Lemma 1.10. *The linear ordering $<$ extends the left divisibility ordering $\prec$.*

Proof. By definition, $1 < \sigma_i$ holds for every i. As the ordering $<$ is compatible with multiplication on the left, it follows that $x < x\sigma_i$ holds for all i, x, and, therefore, $x < xy$ holds whenever y is a nontrivial positive braid. □

Lemma 1.10 implies that 1 is always the first element of $(\mathrm{Div}(\Delta_n^d), <)$, and Δ_n^d is always its last element. A deep result by Laver [1996] shows that, although $<$ is not compatible with right multiplication in general, nevertheless $x < \sigma_i x$ always holds, that is, $<$ also extends the right divisibility ordering.

By Property C, every nontrivial braid admits at least one σ-positive or σ-negative expression. In general, such a σ-positive or σ-negative expression is not unique, but the main generator in such expressions is uniquely defined:

Lemma 1.11. *If a braid x admits a σ-positive expression, then the main generators in any two σ-positive expressions of x coincide.*

Proof. Assume that w, w' are σ-positive expressions of x, and let σ_m, $\sigma_{m'}$ be their main generators. Assume for instance $m < m'$. Then $w^{-1}w'$ is a σ-positive word, and it represents the trivial braid 1: this contradicts Property A. □

Thus, there will be no ambiguity in referring to *the* main generator of some nontrivial braid x: this means the main generator in any σ-positive (or σ-negative) expression of x.

Remark 1.12. Our definition corresponds to the order $<^{\phi}$ of [Dehornoy et al. 2002]. It differs from the one most used in the literature in that the definition of a σ-position refers to the maximal index rather than the minimal one. Switching from one definition to the other amounts to conjugating by Δ_n, that is, to applying the flip automorphism. The results are entirely similar for both versions. However, it is much more convenient to consider the "max" choice here, because it guarantees that B_n^+ is an initial segment of B_{n+1}^+. Using the "min" convention would make the statements in the following sections less natural.

2. Measuring the ordered sets $(\mathrm{Div}(\Delta_n^d), <)$

To investigate the finite ordered sets $(\mathrm{Div}(\Delta_n^d), <)$, and, more generally, the sets $(\mathrm{Div}(z), <)$ for positive braids z, we shall define numerical parameters that reflect their size. The first parameter involves the length of the σ-positive words that are, in a natural sense defined below, drawn in the Cayley graph of Δ_n^d. It will be called the *complexity* of Δ_n^d, because it is directly connected with the complexity analysis of the handle reduction algorithm of [Dehornoy 1997]. The other parameters involve a filtration of the linear ordering by the σ_i's, and they will be called the *heights* of Δ_n^d because they count the jumps of a given height in $(\mathrm{Div}(\Delta_n^d), <)$.

2A. ***Sigma-positive paths in the Cayley graph.*** The first parameter we attach to $(\mathrm{Div}(z), <)$ involves the σ-positive paths in the Cayley graph of z.

We recall that the Cayley graph of the group B_n with respect to the standard generators σ_i is a labeled graph: it has the vertex set B_n and is such that there exists a σ_i-labeled edge from x to y if and only if $y = x\sigma_i$. The Cayley graph of the monoid B_n^+ is obtained by restricting the vertices to B_n^+. Note that the Cayley graph of B_n (and a fortiori of B_n^+) can be seen as a subgraph of the Cayley graph of B_∞.

Definition 2.1. (See Figure 2.) For z a positive braid, we denote by $\Gamma(z)$ the subgraph of the Cayley graph of B_∞ obtained by restricting the vertices to $\mathrm{Div}(z)$ and removing the edges do not connect two vertices in $\mathrm{Div}(z)$.

Because every element of B_n^+ is a left divisor of Δ_n^d for sufficiently large d, the Cayley graph of B_n^+ is the union over all d of the graphs $\Gamma(\Delta_n^d)$.

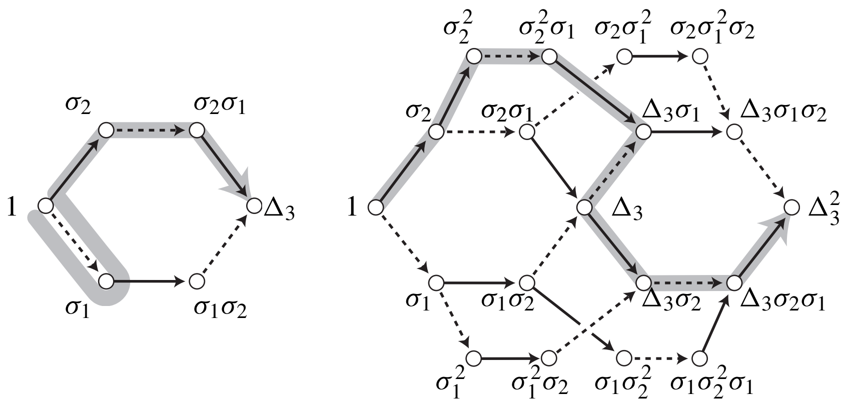

Figure 2. The graphs of $\Gamma(\Delta_3)$ and $\Gamma(\Delta_3^2)$; the dotted edges represent σ_1, the plain ones σ_2; observe that the graph of Δ_3^2 is not planar; in grey: two σ-positive words traced in the graphs, namely `aAbab` and `bbabAbab` (see Lemma 2.3).

A path in the Cayley graph can be specified by its initial vertex and the listed labels of its successive edges, that is, by a braid word. For each $i < n$ and each x in B_n, there is in B_n's Cayley graph exactly one σ_i-labeled edge leading into x and exactly one other going out of it. Hence, in the complete Cayley graph of B_n, for each initial vertex x and each n-braid word w, there is always one path labeled w starting from x. When we restrict to some fragment Γ, this need not be the case, but we do have an unambiguous notion of w being drawn in Γ from x. Formally:

Definition 2.2. If Γ is a subgraph of the Cayley graph of B_∞, and x is a vertex in Γ, we say that a braid word w is *drawn* from x in Γ if, for every prefix $v\sigma_i$ (*resp.* $v\sigma_i^{-1}$) of w, there exists a σ_i-labeled edge starting (*resp.* finishing) at $x\,[v]$ in Γ.

For instance, we can check on Figure 2 that the word σ_1^2 is drawn from σ_2 in $\Gamma(\Delta_3^2)$, but not in $\Gamma(\Delta_3)$. In algebraic terms,

Lemma 2.3. *Assume that z is a positive braid, and w is a braid word. Then w is drawn from x in $\Gamma(z)$ if and only if $x[v] \preccurlyeq z$ holds for each prefix v of w.*

Proof. The condition is sufficient. Indeed, assume it is satisfied by w, and $v\sigma_i$ is a prefix of w. Then, by hypothesis, $x[v]$ and $x[v]\sigma_i$ are left divisors of z. Hence are vertices in $\Gamma(z)$, and, therefore, there is a σ_i-labeled edge between $x[v]$ and $x[v]\sigma_i$ in $\Gamma(z)$. The argument is similar for a prefix of the form $v\sigma_i^{-1}$. Using induction on the length of w, we deduce that w is drawn from x in $\Gamma(z)$.

Conversely, if there is a w-labeled path from x in $\Gamma(z)$, then, for each prefix v of w, the braid $x[v]$ represents some vertex in $\Gamma(z)$. Hence it's a left divisor of z. □

For z a positive braid, we shall investigate the σ-positive words drawn in the graph $\Gamma(z)$. It is clear that, even if $\mathrm{Div}(z)$ is a finite set, arbitrary long words are drawn in $\Gamma(z)$ whenever the latter contains at least 2 vertices, that is, z is not 1. The example of Figure 2 shows that restricting to σ-positive words does not change the result: for instance, for each k, the word $(\sigma_1\sigma_1^{-1})^k\sigma_2\sigma_1\sigma_2$ is a σ-positive expression of Δ_3, and it is drawn in $\Gamma(\Delta_3)$. So we cannot hope for any finite upper bound on the length of the σ-positive words drawn in $\Gamma(z)$ in general. The situation changes if we concentrate on the main generators, that is, we forget about the generators with nonmaximal index.

Lemma 2.4. *Assume that Γ is subgraph of the Cayley graph of B_∞, and w is a σ-positive word drawn in $\Gamma(z)$. Then the number of occurrences of the main generator in w is at most the number of nonterminal vertices in Γ.*

Proof. Assume that w is drawn from x in Γ. Let σ_m be the main generator in w. As there is at most one σ_m-labeled edge starting from each vertex of Γ, it suffices to show that the number of σ_m's in w is bounded above by the number of σ_m-edges in Γ. Hence, it suffices to show that the path γ associated with w cannot cross the same σ_m-edge twice. Now assume that some σ_m-edge starts from the vertex y, and that γ crosses this edge twice. This means that γ contains a loop from y to y. Let v be the subword of w labeling that loop. By construction, v begins with σ_m, it contains no σ_m^{-1} and no $\sigma_i^{\pm 1}$ with $i > m$ as it is a subword of w, and it represents the braid 1 as it labels a loop in the Cayley graph of B_∞: this means that v is a σ-positive word representing 1, which contradicts Property A. □

Lemma 2.4 applies in particular to every graph $\Gamma(z)$ in which z is a positive braid. We can introduce our first parameter measuring the size of the ordered set $(\mathrm{Div}(z), <)$:

Definition 2.5. (See Figure 2.) When z is a positive braid with main generator σ_m, the *complexity* $c(z)$ of z is defined to be the maximal number of σ_m's in a σ-positive word drawn in $\Gamma(z)$.

Example 2.6. The word $\sigma_2\sigma_1\sigma_2$ is a σ-positive word drawn from 1 in $\Gamma(\Delta_3)$, and it contains two σ_2's. Hence we have $c(\Delta_3) \geqslant 2$. Actually, it is not hard to obtain the exact value $c(\Delta_3) = 2$. Indeed, if a σ-positive path γ contains the two σ_2-edges starting from 1 and $\sigma_1\sigma_2$, it cannot come back to σ_2 without crossing the third σ_2-edge; and if γ contains the σ_2-edge that starts from σ_1, it can never come back to 1 or to $\sigma_2\sigma_1$ and therefore contains at most one σ_2-edge. As we have $\Delta_3^d = (\sigma_2\sigma_1\sigma_2)^d$, we deduce $c(\Delta_3^d) \geqslant 2d$ for every d. This value is certainly not optimal: Figure 2 contains five σ_2's, proving $c(\Delta_3^2) \geqslant 5$. The exact value here is 6, and, more generally, we have $c(\Delta_n^d) = 2^{d+1} - 2$, as will be seen in Section 3.

Remark 2.7. Restricting to σ-positive words drawn in $\Gamma(z)$ is essential: for instance, for each k, we have

$$\Delta_3 = \sigma_2^{k+1}\sigma_1\sigma_2\sigma_1^{-k}, \tag{2-1}$$

a σ-positive word containing $k+2$ letters σ_2. Now, for $k \geqslant 1$, the word involved in (2-1) is not drawn in $\Gamma(\Delta_3^1)$, because its prefix σ_2^2 is not. Thus the parameter $c(z)$ does involve the left divisors of z.

Directly applying Lemma 2.4 gives:

Proposition 2.8. *Every positive braid has a finite complexity; more precisely, for z of length ℓ in B_n^+ with $n \geqslant 3$, we have $c(z) \leqslant (n-1)^\ell$.*

Proof. The number of nonterminal vertices in $\Gamma(z)$, that is, the number of proper left divisors of z, is at most $1 + (n-1) + (n-1)^2 + \cdots + (n-1)^{\ell-1}$. □

As the length of any positive expression of Δ_n is $n(n-1)/2$, we obtain in particular for all n, d

$$c(\Delta_n^d) \leqslant (n-1)^{dn(n-1)/2}. \tag{2-2}$$

Before going further, we observe that, in defining the complexity of z, we can restrict to decompositions of z, that is, instead of considering paths starting and finishing at arbitrary vertices, we can restrict to paths going from 1 to z:

Lemma 2.9. *Assume that z is a positive braid with main generator σ_m. Then $c(z)$ is the maximal number of σ_m's in any σ-positive decomposition of z drawn in $\Gamma(z)$.*

Proof. Let $c'(z)$ be the number involved in the above statement. Clearly we have $c'(z) \leqslant c(z)$. Conversely, assume that w is drawn in $\Gamma(z)$ from x, and that the w-labeled path starting at x finishes at y. Let u be a positive expression of x, and v be a positive expression of $y^{-1}z$. The latter exists as, by hypothesis, y is a left divisor of z. Then uwv is a σ-positive decomposition of z drawn in $\Gamma(z)$. Hence we have $c'(z) \geqslant c(z)$. □

Remark 2.10. We call Property A* the statement that all numbers $c(\Delta_n^d)$ are finite. Above, we derived Property A* from Property A. The two properties are actually equivalent, that is, we can also deduce Property A from Property A*. For that, assume that some σ-positive braid word w represents 1. The word w may involve negative letters. We must find a vertex x that begins a path labeled w in some $\Gamma(\Delta_n^d)$. Let σ_m be the main generator in w. The word w has finitely many prefixes, say $w_0, \ldots, w_\ell$. By Garside theory, each word w_i is equivalent to one the form

$u_i^{-1} v_i$, with u_i, v_i positive. Let x be the least common left multiple of the positive braids

$$[u_0], \ldots, [u_\ell].$$

For each i, the braid $x[w_i]$ is positive. Moreover, there exist n and d such that

$$x[w_0], \ldots, x[w_\ell]$$

are all divisors of Δ_n^d. Thus the word w is drawn from x in $\Gamma(\Delta_n^d)$, and the associated path is a loop around x. It follows that w^k is drawn in $\Gamma(\Delta_n^d)$ from x for each k. By construction, w^k contains at least k generators σ_m. Hence $c(\Delta_n^d)$ cannot be finite.

2B. *Connection with handle reduction.* Handle reduction [Dehornoy 1997] is an algorithmic solution to the word problem of braids that relies on the braid ordering. It is the most efficient method today. The method converges, and the argument in [Dehornoy 1997] shows the complexity upper bound to be exponential in the input word length, an estimate seemingly very far from sharp.

Each step of handle reduction involves a specific generator σ_i, and, for an induction, the point is to obtain an upper bound on the reduction steps involving the main generator. The latter will naturally be called the *main* reduction steps. The connection between handle reduction and the complexity as defined above relies on the following technical result:

Lemma 2.11 [Dehornoy 1997]. *Assume that z is a positive braid with main generator σ_m and that w is drawn in $\Gamma(z)$. Then, for each sequence of handle reductions from w — that is, each sequence $\vec{w}$ with $w_0 = w$ such that w_k is obtained by reducing one handle from w_{k-1} for each k — there exists a witness-word u that is σ-positive, drawn in* Div(z), *and such that the number of σ_m's in u is the number of main reductions in $\vec{w}$.*

It follows that the number of main reduction steps in any sequence of handle reductions starting with a word drawn in $\Gamma(z)$ is bounded above by $c(z)$. In particular, if we start with an n strand braid word w of length ℓ, then it is easy to show that w is drawn in $\Gamma(\Delta_n^\ell)$, and, applying the upper bound of Equation (2-2), we deduce the upper bound on the number of possible main reductions from w, and it is exponential in ℓ.

A natural way to improve this coarse upper bound would be to determine $c(\Delta_n^d)$ more precisely. This will be done in Section 3 below. However, the explicit formulas show that, for $n \geqslant 3$, the growth in d really is exponential, thus dashing any hopes of proving a polynomial upper bound for the number of reduction steps by this approach.

2C. ***A filtration of the braid ordering.*** We now introduce new numerical parameters for the ordered sets $(\mathrm{Div}(z), <)$. These numbers connect with a natural filtration of the ordering $<$, using an increasing sequence of partial orderings.

By Lemma 1.11, the index of the main generator of a nontrivial braid is well defined. We can use this index to measure the height of the jump between two braids x, y satisfying $x < y$:

Definition 2.12. For x, y in B_∞ and $r \geqslant 1$, we say that $x <_r y$ holds or, equivalently, that (x, y) is an *r-jump*, if $x^{-1}y$ admits a σ-positive expression in which the main generator is σ_m with $m \geqslant r$.

Lemma 2.13. *For each $r \geqslant 1$, the relation $<_r$ is a strict partial order that refines $<$; the relation $<_1$ coincides with $<$, and $r \leqslant q$ implies that $<_q$ refines $<_r$.*

Proof. That $<_r$ is transitive follows because the concatenation of a σ-positive word with main generator σ_m and a σ-positive word with main generator $\sigma_{m'}$ is a σ-positive word with main generator $\sigma_{\max(m,m')}$. □

In the sequel, we consider the $<_r$-chains included in $\mathrm{Div}(z)$, and their length:

Definition 2.14. For z a positive braid and $r \geqslant 1$, we define the *r-height $h_r(z)$* of z to be the maximal length of a $<_r$-chain included in $\mathrm{Div}(z)$.

Before giving examples, we observe the connection between $h_r(z)$ and the increasing enumeration of the set $\mathrm{Div}(z)$:

Lemma 2.15. *Let z be a positive braid and $r \geqslant 1$. Then $h_r(z) - 1$ is the number of r-jumps in the increasing enumeration of* $(\mathrm{Div}(z), <)$.

Proof. If the number of r-jumps in the increasing enumeration of $\mathrm{Div}(z)$ is $N_r - 1$, we can extract from $\mathrm{Div}(z)$ a $<_r$-chain of length N_r. Conversely, assume that $(y_0, \dots y_{N_r})$ is a $<_r$-chain in $\mathrm{Div}(z)$. Let $z_0 < \dots < z_N$ be the increasing enumeration of $\mathrm{Div}(z)$. As $<_r$ refines $<$, there exists an increasing function f of $\{0, \dots, N_r\}$ into $\{0, \dots, N\}$ such that $y_i = z_{f(i)}$ holds for every i. Now the hypothesis $z_{f(i)} <_r z_{f(i+1)}$ implies that there exists at least one r-jump between $z_{f(i)}$ and $z_{f(i+1)}$. Indeed, by Lemma 1.11, it is impossible that a concatenation of m-jumps with $m < r$ results in a r-jump. So the number of r-jumps in $(z_0, \dots, z_N)$ is at least N_r. □

In other words, to determine $h_r(z)$, there is no need to consider arbitrary chains: it is enough to consider the maximal chain obtained by enumerating $\mathrm{Div}(z)$ exhaustively.

Example 2.16. Refining the increasing enumeration of $\mathrm{Div}(\Delta_3)$ of Example 1.9 by indicating for each step the height of the corresponding jump, we obtain:

$$1 <_1 \mathtt{a} <_2 \mathtt{b} <_1 \mathtt{ba} <_2 \mathtt{ab} <_1 \Delta_3, \tag{2-3}$$

where we recall $\mathtt{a}, \mathtt{b}, \ldots$ stand for $\sigma_1, \sigma_2, \ldots$. For instance, $(\mathtt{ba}, \mathtt{ab})$ is a 2-jump, because we have in $(\mathtt{ba})^{-1}(\mathtt{ab}) = \mathtt{ABab} = \mathtt{AabA} = \mathtt{bA}$ a σ-positive decomposition with main generator σ_2. The number of 1-jumps in (2-3), that is, the number of symbols $<_r$ with $r \geqslant 1$, is 5, while the number of 2-jumps is 2, so, by Lemma 2.15, we deduce $h_1(\Delta_3) = 6$ and $h_2(\Delta_3) = 3$. Similarly, we obtain for Δ_3^2

$$\mathtt{1} <_1 \mathtt{a} <_1 \mathtt{aa} <_2 \mathtt{b} <_1 \mathtt{ba} <_1 \mathtt{baa} <_2 \mathtt{bb} <_1 \mathtt{bba} <_2 \mathtt{ab} <_1 \mathtt{aba} <_1 \mathtt{abaa} <_2 \mathtt{abb} <_1 \mathtt{abba} <_2 \mathtt{aab} <_1 \mathtt{aaba} <_1 \mathtt{aabaa} <_2 \mathtt{baab} <_1 \mathtt{baaba} <_1 \mathtt{baabaa},$$

leading to $h_1(\Delta_3^2) = 19$ and $h_2(\Delta_3^2) = 7$.

Proposition 2.17. (i) *For every braid z in B_n^+, we have*

$$h_1(z) = \#\mathrm{Div}(z) \geqslant h_2(z) \geqslant \cdots \geqslant h_n(z) = 1.$$

(ii) *For all positive braids z, z' and $r \geqslant 1$, we have*

$$h_r(zz') \geqslant h_r(z) + h_r(z'). \tag{2-4}$$

Proof. (i) A $<_1$-chain is simply a $<$-chain. Hence every subset of $\mathrm{Div}(z)$ gives such a chain. So the maximal $<_1$-chain in $\mathrm{Div}(z)$ is $\mathrm{Div}(z)$ itself, and $h_1(z)$ is the cardinality of $\mathrm{Div}(z)$.

On the other hand, no $<_n$-chain in B_n^+ has length more than 1, as the main generator of a σ-positive n-strand braid word cannot be σ_n or any generator above it. Thus $h_n(z)$ is 1.

Then, for $q \leqslant r$, every $<_r$-chain is a $<_q$-chain, which implies $h_r(z) \geqslant h_q(z)$.

Point (ii) is obvious, as the concatenation of two $<_r$-chains is a $<_r$-chain. □

From (2-4) we deduce $h_r(z^d) \geqslant d \cdot h_r(z)$ for all r, z. By Lemma 1.5, every divisor of Δ_n^d can be decomposed as the product of at most d divisors of Δ_n. There are $n!$ such divisors, so we obtain the (coarse) bounds

$$d \cdot h_r(\Delta_n) \leqslant h_r(\Delta_n^d) \leqslant (n!)^d,$$

for all r, n, d. Better estimates will be given below.

Remark 2.18. Instead of restricting to subsets of B_∞ of the form $\mathrm{Div}(z)$, we can define the complexity and the r-height for every (finite) set of braids X. Most of the general results extend, but, when X is not closed under left division, nothing can be said about the number of σ_r's involved in an r-jump. Considering such an extension is not useful here.

2D. ***Connection with the complexity.*** We shall now connect the complexity $c(z)$ with the numbers $h_r(z)$ just defined. The result is simple:

Proposition 2.19. *For z a positive braid with main generator σ_m, we have*

$$c(z) = h_m(z) - 1.$$

In particular, for $n \geqslant 2$ and $d \geqslant 0$, we have

$$c(\Delta_n^d) = h_{n-1}(\Delta_n^d) - 1.$$

One inequality is easy:

Lemma 2.20. *For z a positive braid with main generator σ_m, we have $c(z) \leqslant h_m(z) - 1$.*

Proof. The argument is reminiscent of the one used for Lemma 2.15 but requires a little more care. Assume that w is a σ-positive word drawn in $\Gamma(z)$ from x containing N_m occurrences of σ_m. By Lemma 2.9, we can assume $x = 1$ without loss of generality. Let $z_0 < z_1 < \ldots < z_N$ be the increasing enumeration of $\mathrm{Div}(z)$. By definition, all prefixes of w represent divisors of z, so, letting ℓ be the length of w, there exists a mapping $f : \{0, \ldots, \ell\} \to \{0, \ldots, N\}$ such that, for each k, the length k prefix of w represents $z_{f(k)}$. By construction, we have $f(0) = 0$ and $f(\ell) = N$.

The difference from Lemma 2.15 is that f need not be increasing. Now, let $p_1, \ldots, p_{N_m}$ be the N_m positions in w where the generator σ_m occurs, completed with $p_0 = 0$. Then, in the prefix of w of length p_1, that is, in the subword of w corresponding to positions from $p_0 + 1$ to p_1, there is one σ_m, plus letters $\sigma_i^{\pm 1}$ with $i < m$ (Figure 3). This subword is therefore σ-positive. Hence we must have $z_{f(p_0)} < z_{f(p_1)}$, which requires $f(p_0) < f(p_1)$. Moreover, the quotient $z_{f(p_0)}^{-1} z_{f(p_1)}$ is a braid that admits at least one σ-positive expression containing σ_m, and hence $z_{f(p_0)} <_m z_{f(p_1)}$. Now the same is true between $f(p_1)$ and $f(p_2)$, etc. Hence the number of m-jumps in the increasing enumeration of $\mathrm{Div}(z)$ is at least N_m, that is, we have $h_m(z) \geqslant N_m + 1$. □

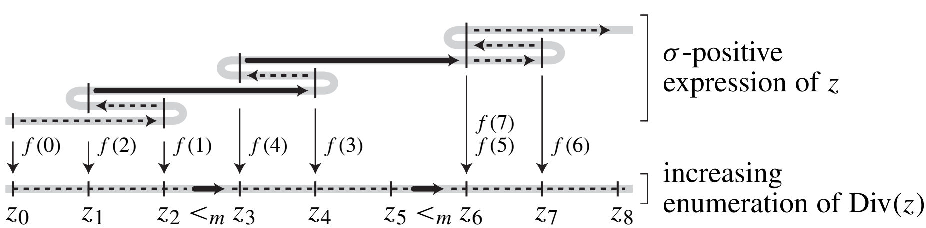

Figure 3. Proof of Lemma 2.20. The main generator σ_m corresponds to the bold arrow: the function f need not be increasing, but the projection of a bold arrow upstairs must include at least one bold arrow downstairs, that is, at least one m-jump.

It remains to prove the second inequality in Proposition 2.19, that is, to prove that, if z is a positive n-braid satisfying $h_m(z) = N + 1$, then z admits a σ-positive expression containing N generators σ_m. The problem is as follows: if z is a positive braid and x, y are left divisors of z satisfying $x < y$, then, by definition, the quotient $x^{-1}y$ admits some σ-positive expression w, but nothing *a priori* guarantees that w be drawn in $\Gamma(z)$. In other words, we might have $x < y$ but no σ-positive witness for this inequality inside $\mathrm{Div}(z)$. It turns out this cannot happen, but the proof requires a rather delicate argument.

Proposition 2.21. *Let z be a positive braid. Then, for all x, y in* $\mathrm{Div}(z)$, *the following are equivalent*:

(i) *The relation $x < y$ holds, that is, there exists a σ-positive path from x to y in the Cayley graph of B_∞*;

(ii) *There exists a σ-positive path from x to y in the Cayley graph of B_n*;

(iii) *There exists a σ-positive path from x to y in* $\Gamma(z)$.

Proof. Clearly (iii) implies (ii), which in turn implies (i). We shall prove that (i) implies (iii) — and thus reprove that (i) implies (ii), which was first proved in [Larue 1994] — by using the handle reduction method of [Dehornoy 1997; Dehornoy et al. 2002]. The problem is to prove that, among all σ-positive paths connecting x to y in the Cayley graph of B_∞, at least one is drawn in $\Gamma(z)$.

Now, let u, v be positive words representing x and y. Then the word $u^{-1}v$ represents $x^{-1}y$, and, by hypothesis, it is drawn in $\Gamma(z)$ from x. Handle reduction transforms a braid word into equivalent words and eventually produces a σ-positive word if it exists. It is proved in [Dehornoy 1997] that, for every n strand braid word w, there exists a finite fragment Γ_w of the Cayley graph of B_n^+ and a vertex x_w of Γ_w such that w and all words obtained from w by handle reduction are drawn from x_w in Γ_w. Moreover, when w has the form $u^{-1}v$ with u, v positive, then all vertices in Γ_w are the left divisors of the least common right multiple of the braids represented by u and v, here x and y, while x_w is the braid represented by u, that is, x. As x and y are divisors of z, so is their least common right multiple, and the graph Γ_w is included in $\Gamma(z)$. It follows that every word obtained from $u^{-1}v$ using handle reduction is drawn from x in $\Gamma(z)$. The termination of handle reduction guarantees that, among these words, at least one is σ-positive, so (iii) follows. □

A direct application of Proposition 2.21 is the existence of σ-positive quotient sequences drawn in the Cayley graph. The definition is as follows:

Definition 2.22. Assume that z is a positive braid and X is a subset of $\mathrm{Div}(z)$. Let $x_0 < \ldots < x_N$ be the increasing enumeration of X. We say that a sequence of words $\vec{w} = (w_1, \ldots, w_N)$ is a *quotient sequence* for X if, for each k, the word w_k is an expression of $x_{k-1}^{-1}x_k$ for each k. We say that $\vec{w}$ is *σ-positive* if every entry in

$\vec{w}$ is σ-positive, and that $\vec{w}$ is *drawn in* $\Gamma(z)$ (from x_0) if w_k is drawn from x_{k-1} in $\Gamma(z)$ for each k.

Corollary 2.23. *Assume that z is a positive braid. Then every subset of* $\mathrm{Div}(z)$ *admits a σ-positive quotient sequence drawn in* $\Gamma(z)$.

Example 2.24. (Figure 4) By computing the successive quotients in the increasing enumeration of $\mathrm{Div}(\Delta_3^2)$ given in Example 1.9, we easily find that

$$(\mathtt{a}, \mathtt{a}, \mathtt{AAb}, \mathtt{a}, \mathtt{a}, \mathtt{AAb}, \mathtt{a}, \mathtt{AAb}, \mathtt{a}, \mathtt{a}, \mathtt{bAA}, \mathtt{a}, \mathtt{bAA}, \mathtt{a}, \mathtt{a}, \mathtt{bAA}, \mathtt{a}, \mathtt{a})$$

is a σ-positive quotient sequence for $\mathrm{Div}(\Delta_3^2)$ drawn in $\Gamma(\Delta_3^2)$. This sequence turns out to be the unique sequence with the above properties, but this uniqueness is specific to the case of 3-braids (see Figure 8 below).

We can now easily complete the proof of Proposition 2.19:

Proof of Proposition 2.19. Let $(z_0, \dots, z_N)$ be the $<$-increasing enumeration of $\mathrm{Div}(z)$. By Corollary 2.23, there exists a σ-positive quotient sequence $\vec{w}$ for $\mathrm{Div}(z)$ that is drawn in $\Gamma(z)$. Let $w = w_1 \dots w_N$. By construction, w is a σ-positive word drawn in $\Gamma(z)$, and the number of occurrences of the main generator σ_m in w is (at least) the number of m-jumps in $(z_0, \dots, z_N)$. So we have $c(z) \geqslant h_m(z) - 1$. Invoking Lemma 2.20 completes the proof. □

Remark 2.25. Assume that $\vec{w}$ is a σ-positive quotient sequence for $\mathrm{Div}(z)$, and σ_m is the main generator occurring in $\vec{w}$. Then each word w_i contains zero or one letter σ_m. Indeed, if w_i contained two σ_m's or more, then the vertex reached after the first σ_m ought to lie in the open $<$-interval determined by two successive entries of $\vec{z}$, and the latter is empty by construction since all elements of $\mathrm{Div}(z)$ occur in $\vec{z}$.

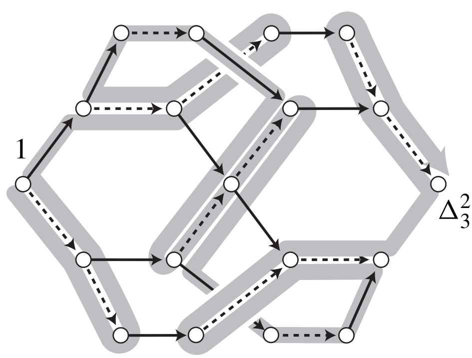

Figure 4. The increasing enumeration of the divisors of Δ_3^2, and a σ-positive quotient sequence drawn in $\Gamma(\Delta_3^2)$: the associated path visits every vertex, and is labeled aaAAbaaAAbabAAa aAAbabAAaabAAaa; it crosses 6 σ_2-edges (and no σ_2^{-1}).

3. A decomposition result for $(\mathrm{Div}(z), <)$

In this section, we establish a structural result describing $(\mathrm{Div}(\Delta_n^d), <)$ as the concatenation of $c(\Delta_n^d) + 1$ intervals isomorphic to subsets of $(\mathrm{Div}(\Delta_{n-1}^d), <)$. We deduce an explicit formula connecting $h_r(\Delta_n^d)$ with the number of braids in $\mathrm{Div}(\Delta_n^d)$ whose d-th factor is right divisible by Δ_r, which in turn enables us to finish computing $c(\Delta_n^d)$ and $h_r(\Delta_n^d)$ for small values of r, n and d.

3A. *B_r-classes.* To analyze the linearly ordered sets $(\mathrm{Div}(\Delta_n^d), <)$, and, more generally, $(\mathrm{Div}(z), <)$ for z a positive braid, we introduce convenient partitions. As B_r is a group for each r, it is clear that the relation $x^{-1}y \in B_r$ defines an equivalence relation on (positive) braids, so we may put:

Definition 3.1. For $r \geqslant 1$ and x, y in B_∞^+, we say that x and y are *B_r-equivalent* if $x^{-1}y$ belongs to B_r.

By construction, B_r-equivalence is compatible with multiplication on the left. In the sequel, we consider the restriction of B_r-equivalence to finite subsets of B_∞^+ of the form $\mathrm{Div}(z)$, that is, we use B_r-equivalence to partition $\mathrm{Div}(z)$ into subsets, naturally called B_r-classes.

Example 3.2. As B_1 is trivial, B_1-equivalence is equality, and so, therefore, the B_1-classes are singletons. On the other hand, any two elements of B_n are B_r-equivalent for each $r \geqslant n$, so, for z in B_n^+, there is only one B_r-class for $r \geqslant n$, and the only interesting relations arise for $1 < r < n$. For instance, $\mathrm{Div}(\Delta_3)$ contains three B_2-classes, while $\mathrm{Div}(\Delta_3^2)$ contains seven of them (Figure 5).

Saying that there is an r-jump between two braids x and y means that $x^{-1}y$ is σ-positive and does not belong to B_r, so, for $x < y$, we have the equivalence

$$\big(x, y \text{ are not } B_r\text{-equivalent}\big) \Longleftrightarrow \begin{pmatrix}\text{there is a } r\text{-jump between}\\ \text{between } x \text{ and } y\end{pmatrix}. \tag{3-1}$$

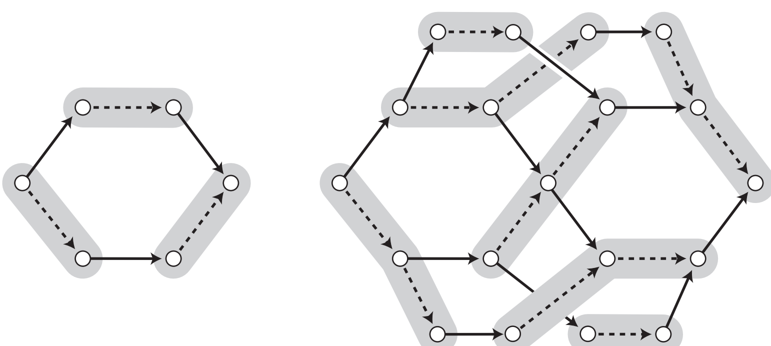

Figure 5. The B_2-classes in $\mathrm{Div}(\Delta_3)$ and $\mathrm{Div}(\Delta_3^2)$.

Lemma 3.3. *Assume that z is a positive braid. Then, each B_r-class in* $\mathrm{Div}(z)$ *is an interval for $<$ and there is an r-jump between each B_r-class and the next one.*

Proof. Assume $x < y \in \mathrm{Div}(z)$. By (3-1), if x and y are not B_r-equivalent, there is an r-jump between x and y and hence also between x and any element of $\mathrm{Div}(z)$ above y. Thus no such element may be B_r-equivalent to x. This implies that each B_r-class is an $<$-interval. □

Corollary 3.4. *For each $r \geqslant 1$, the number of B_r-classes in* $\mathrm{Div}(z)$ *is $h_r(z)$.*

Proof. By (3-1), there is no r-jump between two elements of the same B_r-class, and there is one between two elements not in the same B_r-class. Thus the number of B_r-classes is the number of r-jumps in the $<$-increasing enumeration of $\mathrm{Div}(z)$ augmented by 1. Hence, by Lemma 2.15, it is $h_r(z)$. □

With B_r-equivalence, we can partition $(\mathrm{Div}(z), <)$ into finitely many subintervals. The interest of this partition is that we can describe B_r-classes rather precisely and, typically, connect them with subsets of B_r. In particular, this will allow for connecting the ordered sets $(\mathrm{Div}(\Delta_n^d), <)$ with the sets $(\mathrm{Div}(\Delta_{n-1}^d), <)$.

Proposition 3.5 (Figure 6). *Assume $z \in B_\infty^+$ and $r \geqslant 1$. Let C be a B_r-class in* $\mathrm{Div}(z)$, *and let a, b be its $<$-extremal elements. Then a divides every element of C on the left, and the left translation by a establishes an isomorphism between* $(\mathrm{Div}(a^{-1}b), \preccurlyeq, <)$ *and* $(C, \preccurlyeq, <)$. *In particular,* $(C, \preccurlyeq)$ *is a lattice.*

Proof. By Lemma 3.3, C is the $<$-interval determined by a and b, that is, we have

$$C = \{x \in \mathrm{Div}(z);\, a \leqslant x \leqslant b\}.$$

We know that $\mathrm{Div}(z)$ is a lattice with respect to left divisibility: any two elements x, y of $\mathrm{Div}(z)$ admit a greatest common left divisor, here denoted $\gcd(x, y)$, and a least common right multiple, denoted $\mathrm{lcm}(x, y)$. Firstly, we claim that C is a lattice with respect to left divisibility, that is, the left gcd and the right lcm of two elements of C lie in C. So assume $x, y \in C$. Let x_0, y_0 be defined by $x = \gcd(x, y)x_0$ and $y = \gcd(x, y)y_0$. The hypothesis that $x^{-1}y$ belongs to B_r implies that there exist x_1, y_1 in B_r^+ satisfying $x^{-1}y = x_1^{-1}y_1$. By definition of the gcd, there must exist a positive braid z_1 satisfying $x_1 = z_1x_0$ and $y_1 = z_1y_0$. Because z_1 is positive, $x_1 \in B_r^+$ implies $x_0 \in B_r^+$, and hence $\gcd(x, y) \in C$. As for the lcm, the conjunction of $x = \gcd(x, y)x_0$ and $y = \gcd(x, y)y_0$ implies

$$\mathrm{lcm}(x, y) = \gcd(x, y)\,\mathrm{lcm}(x_0, y_0).$$

As $x_0, y_0 \in B_r^+$ implies $\mathrm{lcm}(x_0, y_0) \in B_r^+$, we deduce $\mathrm{lcm}(x, y) \in C$.

As C is finite, it follows that C admits a global gcd. Because the linear ordering $\leqslant$ extends the partial divisibility ordering $\preccurlyeq$, this global gcd must be the $<$-minimum a of C. Symmetrically, C admits a global lcm, which must be the

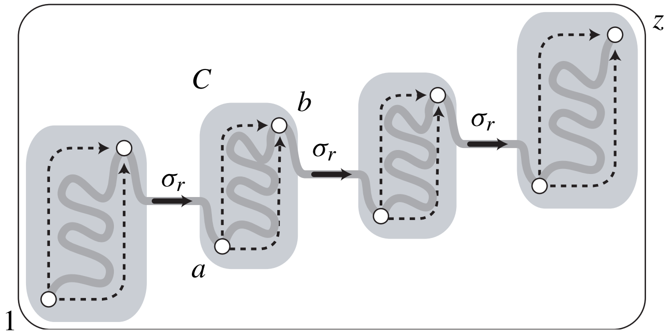

Figure 6. Decomposition of $(\mathrm{Div}(z), <)$ into B_r-classes: each class C is a lattice with respect to divisibility; the increasing enumeration of $\mathrm{Div}(z)$ exhausts the first class, then jumps to the next one by an r-jump, etc. The number of classes is $h_r(z)$.

$<$-maximum b. So, at this point, we know that a is a left divisor of every element in C, and b is a right multiple of each such element, that is, we have

$$C \subseteq \{x \in B_\infty^+ ; a \preccurlyeq x \preccurlyeq b\}. \tag{3-2}$$

Moreover, $a \preccurlyeq x \preccurlyeq b$ implies $a \leqslant x \leqslant b$. Hence $x \in C$, and so the inclusion in (3-2) is an equality.

Now, put $F(x) = ax$ for x in $\mathrm{Div}(a^{-1}b)$. As B_∞^+ is left cancellative, F is injective. Moreover, for x a positive braid, $x \preccurlyeq a^{-1}b$ is equivalent to $ax \preccurlyeq b$, so the image of F is $\{x \in B_\infty^+ ; a \preccurlyeq x \preccurlyeq b\} = C$. Finally, by construction, F preserves both $\preccurlyeq$ and $<$. □

For $r = 1$, each B_r-class is a singleton, and Proposition 3.5 says nothing; similarly, if the main generator of z is σ_m, there is only one B_r-class for $r > m$, and we gain no information. But, for $1 < r \leqslant m$, and specially for $r = m$, Proposition 3.5 states that the chain $\mathrm{Div}(z)$ is obtained by concatenating $h_r(z)$ copies of sets of the form $\mathrm{Div}(z')$ with z' of index at most r. In particular, for $z = \Delta_n^d$, we have:

Corollary 3.6. *For each n and r such that $r < n$, the chain $(\mathrm{Div}(\Delta_n^d), <)$ is obtained by concatenating $h_r(\Delta_n^d)$ intervals, each of which, when equipped with $\preccurlyeq$, is a translated copy of some initial sublattice of $(\mathrm{Div}(\Delta_r^d), \preccurlyeq)$.*

The case of Δ_3^2 and Δ_4 are illustrated in Figure 7 and Figure 8.

3B. ***Extremal elements.*** The next step is to observe that extremal points in B_r-classes admit a simple characterization in terms of divisibility.

Proposition 3.7. *Assume that z is a positive braid.*

(i) *An element x of $\mathrm{Div}(z)$ is the maximum of its B_r-class if and only if the relation $x\sigma_i \preccurlyeq z$ fails for $1 \leqslant i < r$.*

(ii) *An element x of* $\mathrm{Div}(z)$ *is the minimum of its* B_r*-class if and only if no* σ_i *with* $1 \leqslant i < r$ *divides* x *on the right.*

Proof. (i) The condition is necessary: if $x\sigma_i$ lies in $\mathrm{Div}(z)$ for some i with $i < r$, then $x\sigma_i$ lies in the same B_r-class as x, and it is larger both for $\preccurlyeq$ and $<$, so x cannot be maximal in its B_r-class. Conversely, assume that x is not maximal in its B_r-class. Then there exists y satisfying $x < y$ and y is B_r-equivalent to x. Now, by Proposition 3.5, the lcm of x and y is also B_r-equivalent to x, which means that there exists y_1 in B_r^+ satisfying $\mathrm{lcm}(x, y) = xy_1$. Now $x < y$ implies

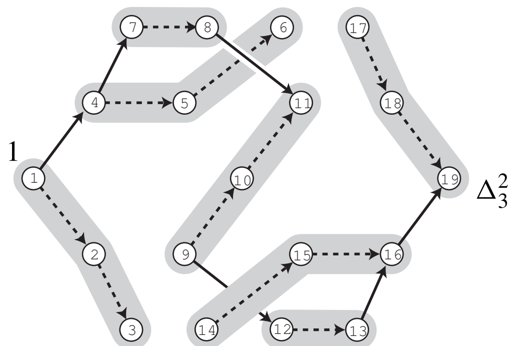

Figure 7. Decomposition of $(\mathrm{Div}(\Delta_3^2), <)$ into B_2-classes. The increasing enumeration of $(\mathrm{Div}(\Delta_3^2), <)$ is the concatenation of the increasing enumeration of the successive classes, separated by 2-jumps (compare with Figure 4); in this case, B_2-classes are simply chains with respect to divisibility.

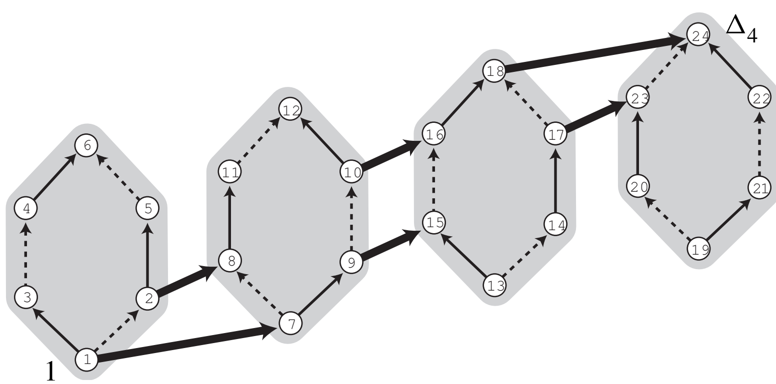

Figure 8. Decomposition of $(\mathrm{Div}(\Delta_4), <)$ into B_3-classes. The σ_3-arrows (thick) corresponding to 3-jumps are not unique; in this case, all B_3-classes are isomorphic to the lattice $(\mathrm{Div}(\Delta_3), <, \preccurlyeq)$, that is, to the Cayley graph of Δ_3.

$y_1 \neq 1$, so there must exist $i < m$ such that σ_i is a left divisor of y_1. Then we have $x\sigma_i \preccurlyeq xy_1 \preccurlyeq z$. Hence $x\sigma_i \preccurlyeq z$.

(ii) The argument is symmetric. If $x = y\sigma_i$ for some positive braid y and $i < r$, then y belongs to the B_r-class of x, and x cannot be minimal in its B_r-class. Conversely, assume that x is not minimal in its B_r-class. Then there exists y satisfying $y < x$ and y is B_r-equivalent to x. By Proposition 3.5 again, the gcd of x and y is also B_r-equivalent to x, which means that there exists y_0 in B_r^+ satisfying $\gcd(x, y)y_0 = x$. As $y < x$ implies $y_0 \neq 1$, there must exist $i < m$ such that σ_i is a right divisor of y_0 and hence of x. □

When we apply the previous criterion to the braids Δ_n^d, we obtain:

Proposition 3.8. *For x in $\mathrm{Div}(\Delta_n^d)$ and $1 \leqslant r \leqslant n$, the following are equivalent.*

(i) *The element x is $<$-maximal in its B_r-class.*

(ii) *The element $x\sigma_i$ belongs to $\mathrm{Div}(\Delta_n^d)$ for no $i < r$.*

(iii) *The d-th factor of x is right divisible by Δ_r.*

(iv) *The $(d+1)$-st factor of $x\Delta_r$ is Δ_r.*

Proof. The equivalence of (i) and (ii) is given by Proposition 3.7(i). It remains to establish the equivalence of (ii)–(iv). For $r = 1$, (ii) is vacuously true, while (iii) and (iv) always hold. So the expected equivalences are true. We henceforth assume $r \geqslant 2$.

Let x belong to $\mathrm{Div}(\Delta_n^d)$, and let x_d be the d-th factor in the normal form of x. For $i < n$, saying that $x\sigma_i$ does not belong to $\mathrm{Div}(\Delta_n^d)$ means that the normal form of $x\sigma_i$ has length $d+1$. Hence, equivalently, that the normal form of $x_d\sigma_i$ has length 2. This occurs if and only if σ_i is a right divisor of x_d. So, for $r \leqslant n$, (ii) is equivalent to x_d being right divisible by all σ_i's with $1 \leqslant i < r$ and hence to x_d being right divisible by the (left) lcm of these elements, which is Δ_r.

Finally, (iii) and (iv) are equivalent. Indeed, if the d-th factor x_d in the normal form of x is divisible by Δ_r on the right, then (x_d, Δ_r) is a normal sequence as no σ_i with $i < r$ from Δ_r may pass to x_d. Hence $(x_1, \dots, x_d, \Delta_r)$ is a normal sequence and necessarily the normal form of $x\Delta_r$. Conversely, assume that the normal form of $x\Delta_r$ is $(x_1, \dots, x_d, \Delta_r)$. The hypothesis that (x_d, Δ_r) is normal implies that x_d is divisible on the right by each σ_i with $i < r$. Hence is divisible on the right by Δ_r. Now $(x_1, \dots, x_d)$ is the normal form of x. □

Observe that, for $r \geqslant 2$, an element of $\mathrm{Div}(\Delta_n^d)$ that is $<$-maximal in its B_r-class cannot belong to $\mathrm{Div}(\Delta_n^{d-1})$, that is, it cannot have degree $d-1$ or less because the d-th factor of its normal form cannot be 1.

Similar conditions characterize the minimal elements of the B_r-classes. Because the normal form has a privileged orientation, the results are not entirely symmetric with those of Proposition 3.8

Proposition 3.9. *For x in $\mathrm{Div}(\Delta_n^d)$ and $1 \leqslant r \leqslant n$, the following are equivalent.*

(i) *The element x is $<$-minimal in its B_r-class.*

(ii) *No σ_i with $i < r$ is a right divisor of x.*

(iii) *The degrees of x and $x\Delta_r$ are equal.*

Proof. The equivalence of (i) and (ii) is given by Proposition 3.7(ii), and everything is obvious for $r = 1$. So it remains to establish the equivalence of (ii) and (iii) when $r \geqslant 2$. Now, assume that (ii) holds and x has degree d. The hypothesis that σ_i is not a right divisor of x implies that $x\sigma_i$ is a divisor of Δ_n^d. As this holds for each $i < r$, the lcm of $x\sigma_1, \ldots, x\sigma_{r-1}$, namely $x\Delta_r$, also divides Δ_n^d, which means that $x\Delta_r$ has degree (at most) d. So (ii) implies (iii).

Conversely, assume that σ_i divides x on the right. Then the degree of $x\sigma_i$ is strictly larger than that of x, and, *a fortiori*, the same is true for $x\Delta_r$. □

3C. *Determination of $h_r(\Delta_n^d)$*. A direct application of the previous results is a formula connecting the number $h_r(\Delta_n^d)$ of B_r-classes in $\mathrm{Div}(\Delta_n^d)$ with the number of braids whose normal form ends with some specific factor.

Definition 3.10. For $n, d \geqslant 1$ and for s a simple n-braid, we denote by $b_{n,d}(s)$ the number of positive braids of degree at most d, that is, of divisors of Δ_n^d, whose d-th factor is s.

Proposition 3.11. *For $1 \leqslant r \leqslant n$, we have*

$$h_r(\Delta_n^d) = \sum_{s \text{ right divisible by } \Delta_r} b_{n,d}(s) = b_{n,d+1}(\Delta_r). \tag{3-3}$$

In words, the number of r-jumps in $(\mathrm{Div}(\Delta_n^d), <)$ is the number of n-braids of degree at most d whose d-th factor is right divisible by Δ_r.

Proof. By Corollary 3.4, $h_r(\Delta_n^d)$ is the number of B_r-classes in $\mathrm{Div}(\Delta_n^d)$. Each class contains exactly one maximum element, and, by Proposition 3.8, its d-th factor is right divisible by Δ_r. The first equality in (3-3) follows. The second one follows from the equivalence of (iii) and (iv) in Proposition 3.8. □

For $r = 1$, as every simple braid is divisible by 1 on the right, Equation (3-3) reduces to

$$h_1(\Delta_n^d) = \sum_s b_{n,d}(s) = b_{n,d+1}(1),$$

a special case of the relation $h_1(z) = \#\mathrm{Div}(z)$ of Proposition 2.17. For $r = n$, because the only normal sequence of length d that finishes with Δ_n is $(\Delta_n, \dots, \Delta_n)$, Equation (3-3) reduces to

$$h_n(\Delta_n^d) = 1,$$

already noted in Proposition 2.17. Finally, for $r = n - 1$, we obtain using Proposition 2.19:

Corollary 3.12. *For $n \geqslant 2$, we have*

$$c(\Delta_n^d) = h_{n-1}(\Delta_n^d) - 1 = \sum_{i=2}^{n} b_{n,d}(\sigma_i \sigma_{i+1} \dots \sigma_{n-1} \Delta_{n-1}) = b_{n,d+1}(\Delta_{n-1}) - 1.$$

Proof. The simple n-braids that are right divisible by Δ_{n-1} are the braids of the form $\sigma_i \sigma_{i+1} \dots \sigma_{n-1}$ with $1 \leqslant i \leqslant n$. Indeed, it is clear that every such braid is simple and right divisible by Δ_{n-1}. Conversely, the only possibility for $z\Delta_{n-1}$ to be simple is that z moves the n-th strand to some position between 1 and n without introducing any crossing between the remaining strands. Finally, $\sigma_1 \sigma_2 \dots \sigma_{n-1} \Delta_{n-1}$ is Δ_n, and, remembering that $b_{n,d}(\Delta_n)$ is 1, we obtain the first equality. □

3D. ***Computation of $b_{n,d}(s)$.*** By Lemma 1.4, normal sequences are characterized by a local condition involving only pairs of consecutive elements. It follows that the set of all normal sequences is a rational set, that is, it can be recognized by a finite state automaton. Standard arguments then show that the numbers $b_{n,d}(s)$ obey a linear recurrence. Building on this observation, seemingly first used for braids in [Charney 1995], we can obtain explicit formulas for the parameters $c(\Delta_n^d)$ and $h_r(\Delta_n^d)$ for small values of r, n, or d. We shall not go into details here but refer to [Dehornoy 2007] where we established the formulas and, more generally, investigated the rich combinatorics underlying the normal form of braids.

In the sequel, we write $(M)_{x,y}$ for the (x, y)-entry of a matrix M. The general principle for computing the numbers $b_{n,d}(s)$ for some fixed n is as follows:

Lemma 3.13. *For $n \geqslant 1$, let M_n be the square matrix with entries indexed by simple n-braids defined by*

$$(M_n)_{s,t} = \begin{cases} 1 & \text{if } (s,t) \text{ is normal,} \\ 0 & \text{otherwise.} \end{cases}$$

Then, for every simple t and $d \geqslant 1$, we have $b_{n,d}(t) = ((1, 1, \dots, 1)\, M_n^{d-1})_t$.

The proof is an easy induction on d.

Example 3.14. The matrix M_1 is (1), corresponding to $b_{1,d}(1) = 1$. For $n = 2$, using the enumeration $(1, \sigma_1)$ of simple 2-braids, we find $M_2 = ((1, 0), (1, 1))$, leading to $b_{2,d}(1) = d$ and $b_{2,d}(\sigma_1) = 1$, giving $d + 1$ braids of degree at most

d. The first d are the braids σ_1^e with $e < d$ in which the d-th factor is 1; the last is σ_1^d, whose d-th factor is Δ_2, that is, σ_1. For $n = 3$, using the enumeration $(1, \sigma_1, \sigma_2, \sigma_2\sigma_1, \sigma_1\sigma_2, \Delta_3)$ of simple 3-braids, we obtain

$$M_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

from which we can deduce $b_{3,3}(1) = 19$ or $b_{3,4}(\sigma_1) = 15$ using Lemma 3.13.

Using Proposition 3.11, we deduce:

Proposition 3.15. *With M_n as in Lemma 3.13, we have for $n \geqslant r \geqslant 1$ and $d \geqslant 1$*

$$c(\Delta_n^d) = ((1, 1, \dots, 1)\, M_n^d)_{\Delta_{n-1}} - 1,$$
$$h_r(\Delta_n^d) = ((1, 1, \dots, 1)\, M_n^d)_{\Delta_r}.$$

Corollary 3.16. (i) *For fixed n, r, the generating functions for the sequences $c(\Delta_n^d)$ and $h_r(\Delta_n^d)$ are rational.*

(ii) *For fixed n, r, the numbers $c(\Delta_n^d)$ and $h_r(\Delta_n^d)$ admit expressions of the form*

$$P_1(d)\rho_1^d + \cdots + P_k(d)\rho_k^d. \tag{3-4}$$

where $\rho_1, \dots, \rho_k$ are the nonzero eigenvalues of M_n and $P_1, \dots, P_k$ are polynomials with $\deg(P_i)$ *of at most the multiplicity of ρ_i in M_n.*

Because the matrix M_n is an $n! \times n!$ matrix, completing the computation is not so easy, even for small values of n. Actually, it is shown in [Dehornoy 2007] how to replace M_n with a smaller matrix $\overline{M}_n$ of size $p(n) \times p(n)$, where $p(n)$ is the number of partitions of n. The property is connected with classical results of Solomon [1976] about the descents of permutations. With such methods, one easily obtains the values listed in Table 1.

Using the reduced matrices

$$\overline{M}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix} \qquad \text{and} \qquad \overline{M}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 11 & 4 & 1 & 0 & 0 \\ 5 & 3 & 2 & 1 & 0 \\ 6 & 4 & 2 & 2 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

we obtain the following explicit form for (3-4) involving the nonzero eigenvalues $(1, 1, 2)$ of M_3 and $(1, 1, 3 \pm \sqrt{6})$ of M_4:

Proposition 3.17. *Let* $\rho_\pm = 3 \pm \sqrt{6}$. *Then, for* $d \geqslant 1$, *we have*

$$\begin{aligned}
h_1(\Delta_3^d) &= 8 \cdot 2^d - 3d - 7,\\
h_2(\Delta_3^d) &= c(\Delta_3^d) + 1 = 2 \cdot 2^d - 1,\\
h_1(\Delta_4^d) &= \sum_{\pm} \frac{3}{20}(32 \pm 13\sqrt{6})\rho_\pm^d - \frac{128}{5} \cdot 2^d + 6d + 17,\\
h_2(\Delta_4^d) &= \sum_{\pm} \frac{1}{20}(32 \pm 13\sqrt{6})\rho_\pm^d - \frac{16}{5} \cdot 2^d + 1,\\
h_3(\Delta_4^d) &= c(\Delta_3^4) + 1 = \sum_{\pm} \frac{1}{20}(4 \pm \sqrt{6})\rho_\pm^d + \frac{8}{5} \cdot 2^d - 1.
\end{aligned}$$

These formulas show each parameter grows exponentially in d, with estimate $O(2^d)$ for $n = 3$, and $O((3 + \sqrt{6})^d)$ for $n = 4$. For practical purposes, it may be more convenient to resort to recursive formulas, for instance,

$$h_1(\Delta_3^d) = 2h_1(\Delta_3^{d-1}) + 3d + 1, \tag{3-5}$$

$$h_1(\Delta_4^d) = 6h_1(\Delta_4^{d-1}) - 3h_1(\Delta_4^{d-2}) + 32 \cdot 2^d - 12d - 34, \tag{3-6}$$

together with initial values $h_1(\Delta_3^0) = h_1(\Delta_4^0) = 1$, $h_1(\Delta_4^1) = 24$ (or $h_1(\Delta_4^{-1}) = 0$).

3E. *Small values of d.* Another approach is to keep d fixed and let n vary. Once again, we only mention a few results, and refer the reader to [Dehornoy 2007] for the proofs and additional comments. For $d = 1$, it is easy to determine all values:

Proposition 3.18 [Dehornoy 2007]. *For* $n \geqslant r \geqslant 1$, *we have*

$$h_r(\Delta_n) = \frac{n!}{r!}.$$

For $d = 2$, it is easier to complete the computation for $h_{n-r}(\Delta_n^2)$.

Proposition 3.19 [Dehornoy 2007]. *For* $n \geqslant r \geqslant 1$, *we have*

$$h_{n-r}(\Delta_n^2) = r!\,(r+1)^n + \sum_{i=1}^{r} P_i(n)\, i^{n-r+i-1},$$

for some polynomial P_i *of degree at most* $r - i + 1$. *The values for* $r = 1, 2$ *are*

$$\begin{aligned}
h_{n-1}(\Delta_n^2) &= 2^n - 1,\\
h_{n-2}(\Delta_n^2) &= 2 \cdot 3^n - (n+6) \cdot 2^{n-1} + 1.
\end{aligned}$$

For $h_r(\Delta_n^2)$ itself, no general formula is known. We mention the case of $h_1(\Delta_n^2)$, which follows from results of Carlitz et al. [1976]:

Proposition 3.20 [Dehornoy 2007]. *The numbers $h_1(\Delta_n^2)$ are determined by the induction*

$$h_1(\Delta_0^2) = 1, \qquad h_1(\Delta_n^2) = \sum_{i=0}^{n-1} (-1)^{n+i+1} \binom{n}{i}^2 h_1(\Delta_i^2).$$

Their double exponential generating function is, with $J_0(x)$ is the Bessel function,

$$\sum_{n=0}^{\infty} h_1(\Delta_n^2) \frac{z^n}{n!^2} = \left(\sum_{n=0}^{\infty} (-1)^n \frac{z^n}{n!^2} \right)^{-1} = \frac{1}{J_0(\sqrt{z})}.$$

Finally, for $d = 3$, the computation can be completed at least in the case $n - r = 1$:

Proposition 3.21 [Dehornoy 2007]. *For $n \geqslant 1$, we have, with $e = \exp(1)$,*

$$h_{n-1}(\Delta_n^3) = \sum_{i=0}^{n-1} \frac{n!}{i!} = \lfloor n!e \rfloor - 1.$$

d	0	1	2	3	4	5	6
$h_1(\Delta_2^d)$	1	2	3	4	5	6	7
$h_1(\Delta_3^d)$	1	6	19	48	109	234	487
$h_2(\Delta_3^d)$	1	3	7	15	31	63	127
$h_1(\Delta_4^d)$	1	24	211	1,380	8,077	45,252	249,223
$h_2(\Delta_4^d)$	1	12	83	492	2,765	15,240	83,399
$h_3(\Delta_4^d)$	1	4	15	64	309	1,600	8,547
$h_1(\Delta_5^d)$	1	120	3,651	79,140	1,548,701	29,375,460	551,997,751
$h_2(\Delta_5^d)$	1	60	1,501	30,540	585,811	11,044,080	207,154,921
$h_3(\Delta_5^d)$	1	20	311	5,260	94,881	1,755,360	32,741,851
$h_4(\Delta_5^d)$	1	5	31	325	4,931	86,565	1,590,231
$h_1(\Delta_6^d)$	1	720	90,921	7,952,040	634,472,921	49,477,263,360	3,836,712,177,121
$h_2(\Delta_6^d)$	1	360	38,559	3,228,300	254,718,389	19,808,530,620	1,535,016,069,499
$h_3(\Delta_6^d)$	1	120	8,727	649,260	49,654,757	3,831,626,580	296,361,570,667
$h_4(\Delta_6^d)$	1	30	1,075	61,620	4,387,195	332,578,230	25,612,893,355
$h_5(\Delta_6^d)$	1	6	63	1,956	116,423	8,448,606	643,888,543

Table 1. First values of $h_r(\Delta_n^d)$ for $1 \leqslant r < n$ — the value is 1 for $r \geqslant n$. For instance, the number $h_1(\Delta_3^2)$ of 3-strand braids of degree at most 2 is 19 (see Example 2.16), while the maximal number $c(\Delta_4^4)$ of σ_3's in a σ-positive word drawn in $\Gamma(\Delta_4^4)$ — which is $h_3(\Delta_4^4) - 1$, according to Proposition 2.19 — is 308.

Using Proposition 2.19, we deduce the following explicit values for $c(\Delta_n^d)$, that is, for the maximal number of occurrences of σ_{n-1} in a σ-positive word drawn in the Cayley graph of Δ_n^d:

$$c(\Delta_n) = n - 1, \qquad c(\Delta_n^2) = 2^n - 2, \qquad c(\Delta_n^3) = \sum_{i=0}^{n-1} \frac{n!}{i!} - 1 = \lfloor n!e \rfloor - 2.$$

The formulas listed above show that a number of different induction schemes appear, suggesting that the combinatorics of normal sequences of braids is very rich.

4. A complete description of $(\mathrm{Div}(\Delta_3^d), <)$

Our ultimate goal is a complete description of each chain $(\mathrm{Div}(\Delta_n^d), <)$. Typically, this means that we are able to explicitly specify the increasing enumeration of its elements. The goal remains generally out of reach, but we can show how the process can be completed when $n = 3$. The counting formulas of Section 3 play a key role in the construction, and, in particular, the Pascal's triangle of Figure 9 connects directly with the 2^d factor in the inductive formulas of Proposition 3.17. As an application, we deduce a new proof of Property C and of the well-ordering property and hence a complete reconstruction of the braid ordering when $n = 3$.

The general principle is to make the decomposition of Corollary 3.6 explicit. The latter shows that, for all n and d, the chain $(\mathrm{Div}(\Delta_n^d), <)$ can be decomposed into $c(\Delta_n^d)$ subintervals each of which copies some fragment of $(\mathrm{Div}(\Delta_{n-1}^d), <)$. Moreover, the approach of Section 3 suggests an induction on d as well. We are led to seek a recursion for $(\mathrm{Div}(\Delta_n^d), <)$ in $(\mathrm{Div}(\Delta_{n-1}^d), <)$ and $(\mathrm{Div}(\Delta_n^{d-1}), <)$; here this means expressing $(\mathrm{Div}(\Delta_3^d), <)$ in $(\mathrm{Div}(\Delta_2^d), <)$ and $(\mathrm{Div}(\Delta_3^{d-1}), <)$.

4A. *The braids $\theta_{n,p}$.* The subsequent construction will appeal to a double series $\theta_{n,p}$ of braids, and we begin with a few preliminary properties.

Definition 4.1. For $n \geqslant 2$, let $\sigma_{n,1}$ and $\sigma_{1,n}$ denote the braid words $\sigma_{n-1}\sigma_{n-2}\ldots\sigma_1$ and $\sigma_1\sigma_2\ldots\sigma_{n-1}$. For $p \geqslant 0$, we define $\widetilde{\theta}_{n,p}$ as (the braid represented by) the length p prefix of the right-infinite word $(\sigma_{n,1}\sigma_{1,n})^\infty$, and let $\theta_{n,p}$ be (the braid represented by) the length p suffix of the left-infinite word ${}^\infty(\sigma_{n,1}\sigma_{1,n})$.

For instance, we find $\theta_{3,0} = 1$, $\theta_{3,1} = \mathtt{b}$, $\theta_{3,2} = \mathtt{ab}$, ..., $\theta_{3,4} = \mathtt{baab}$, ..., $\theta_{3,7} = \mathtt{aabbaab}$, etc. Similarly, we have $\theta_{4,6} = \mathtt{cbaabc}$ and, more generally, $\theta_{n,2n-2} = \widetilde{\theta}_{n,2n-2} = \sigma_{n,1}\sigma_{1,n}$. Note that, as words, $\theta_{n,p}$ is the reverse of $\widetilde{\theta}_{n,p}$.

Lemma 4.2. *For $n \geqslant 2$ and $p, q \geqslant 0$ satisfying $p + q = d(n-1)$, we have*

$$\theta_{n,p}\, \Delta_{n-1}^d\, \widetilde{\theta}_{n,q} = \Delta_n^d. \tag{4-1}$$

Proof. We first prove using induction on d the relation

$$\theta_{n,d(n-1)}\,\Delta_{n-1}^{d}=\Delta_{n}^{d}, \tag{4-2}$$

that is, (4-1) with $q=0$. For $d=0$, (4-2) reduces to $1=1$. Assume $d\geqslant 1$. By definition, $\theta_{n,d(n-1)}$ is $\sigma_{n,1}\,\theta_{n,(d-1)(n-1)}$ for d odd and is $\sigma_{1,n}\,\theta_{n,(d-1)(n-1)}$ for d even. In either case, we can write

$$\theta_{n,d(n-1)}=\phi_n^{d-1}(\sigma_{1,n})\,\theta_{n,(d-1)(n-1)},$$

where we recall ϕ_n denotes the flip automorphism of B_n that exchanges σ_i and σ_{n-i}. Using the induction hypothesis and (1-2), we find

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

We return to the general case of (4-1). For d even, we have $\theta_{n,d(n-1)}=\widetilde{\theta}_{n,d(n-1)}$ and hence $\widetilde{\theta}_{n,q}\,\theta_{n,p}=\theta_{n,d(n-1)}$. If d is odd, we have $\theta_{n,d(n-1)}=\phi_n(\widetilde{\theta}_{n,d(n-1)})$, which implies $\phi_n(\widetilde{\theta}_{n,q})\,\theta_{n,p}=\theta_{n,d(n-1)}$. So $\phi_n^d(\widetilde{\theta}_{n,q})\,\theta_{n,p}=\theta_{n,d(n-1)}$ holds in both cases. Now, using (4-2), we find

$$\phi_n(\widetilde{\theta}_{n,q})\,\theta_{n,p}\,\Delta_{n-1}^{d}\,\widetilde{\theta}_{n,q}=\theta_{n,d(n-1)}\,\Delta_{n-1}^{d}\,\widetilde{\theta}_{n,q}=\Delta_n^{d}\,\widetilde{\theta}_{n,q}=\phi_n(\widetilde{\theta}_{n,q})\,\Delta_n^{d},$$

from which we deduce (4-1) by cancelling $\phi_n(\widetilde{\theta}_{n,q})$ on the left. □

Lemma 4.3. *For $1\leqslant i\leqslant n-2$ we have*

$$\theta_{n,d(n-1)}\,\sigma_i=\sigma_{i+e}\,\theta_{n,d(n-1)} \tag{4-3}$$

with $e=0$ if d is even and $e=1$ if d is odd.

Proof. For $1\leqslant i\leqslant n-2$, we have $\sigma_{1,n}\,\sigma_i=\sigma_{i+1}\,\sigma_{1,n}$ and $\sigma_{n,1}\,\sigma_{i+1}=\sigma_i\,\sigma_{n,1}$, as an easy induction shows. This implies $\sigma_{n,1}\,\sigma_{1,n}\,\sigma_i=\sigma_i\,\sigma_{n,1}\,\sigma_{1,n}$ and therefore $(\sigma_{n,1}\,\sigma_{1,n})^d\,\sigma_i=\sigma_i\,(\sigma_{n,1}\,\sigma_{1,n})^d$, that is, $\theta_{n,2d(n-1)}\,\sigma_i=\sigma_i\,\theta_{n,2d(n-1)}$ for every d. On the other hand, we have $\theta_{n,(2d+1)(n-1)}=\sigma_{1,n}\,\theta_{n,2d(n-1)}$ and hence

$$\theta_{n,(2d+1)(n-1)}\,\sigma_i=\sigma_{1,n}\,\sigma_i\,\theta_{n,2d(n-1)}=\sigma_{i+1}\,\sigma_{1,n}\,\theta_{n,2d(n-1)}=\sigma_{i+1}\,\theta_{n,(2d+1)(n-1)},$$

as was expected. □

4B. ***A Pascal triangle.*** We shall now construct for every d a sequence of positive braids S_3^d that will be the increasing enumeration of $(\mathrm{Div}(\Delta_3^d),<)$. The construction relies on an induction similar to Pascal's triangle. To make it easily understandable, we start with the (trivial) cases $n=1$ and $n=2$.

Because B_1 is the trivial group, for every d, 1 is the only element of degree at most d, and we can state:

Proposition 4.4. *Define S_1^d for $d \geqslant 0$ by*

$$S_1^d = (1).$$

Then S_1^d is the increasing enumeration of $\mathrm{Div}(\Delta_1^d)$.

The group B_2 is the rank 1 free group generated by σ_1. The braid Δ_2 is just σ_1, and the braids of degree at most d, that is, the divisors of Δ_2^d, consist of the $d+1$ braids $1, \sigma_1, \dots, \sigma_1^d$. On the other hand, we have $\sigma_{1,2} = \sigma_{2,1} = \sigma_1$, and $\theta_{1,i} = \sigma_1^i$ for every i.

Notation 4.5. If S_1, S_2 are sequences (of braids), we denote by $S_1 + S_2$ the (ordered) concatenation of S_1 and S_2. If S is a sequence of braids and x is a braid, we denote by xS the translated sequence obtained by multiplying each entry in S by x on the left.

In these terms, the sequence $(1, \sigma_1, \dots, \sigma_1^d)$ can be expressed as a sum of sequences $\theta_{2,0}(1) + \theta_{2,1}(1) + \cdots + \theta_{2,d}(1)$. Hence:

Proposition 4.6. *Define S_2^d for $d \geqslant 0$ by*

$$S_2^d = \theta_{2,0} S_1^d + \theta_{2,1} S_1^d + \cdots + \theta_{2,d} S_1^d. \tag{4-4}$$

Then S_2^d is the increasing enumeration of $\mathrm{Div}(\Delta_2^d)$.

We repeat the process for $n = 3$, introducing a sequence S_3^d by a definition similar to (4-4) that involves S_2^d and S_3^{d-1}. The result we shall prove is:

Proposition 4.7. *Let S_3^d be defined for $d \geqslant 0$ by*

$$S_3^d = \theta_{3,0} S_2^d + S_3^{d,1} + \theta_{3,1} S_2^d + \cdots + \theta_{3,2d-1} S_2^d + S_3^{d,2d} + \theta_{3,2d} S_2^d, \tag{4-5}$$

where $S_3^{d,1}, \cdots, S_3^{d,2d}$ are defined by $S_3^{d,1} = S_3^{d,2d} = \varnothing$ and, for $2 \leqslant p \leqslant 2d-1$,

$$S_3^{d,p} = \begin{cases} \sigma_1(S_3^{d-1,p-1} + \theta_{3,p-1} S_2^{d-1} + S_3^{d-1,p}) & \text{for } p = 0 \pmod 4, \\ \sigma_2\sigma_1(S_3^{d-1,p-2} + \theta_{3,p-1} S_2^{d-1} + S_3^{d-1,p-1}) & \text{for } p = 1 \pmod 4, \\ \sigma_2(S_3^{d-1,p-1} + \theta_{3,p-1} S_2^{d-1} + S_3^{d-1,p}) & \text{for } p = 2 \pmod 4, \\ \sigma_1\sigma_2(S_3^{d-1,p-2} + \theta_{3,p-1} S_2^{d-1} + S_3^{d-1,p-1}) & \text{for } p = 3 \pmod 4. \end{cases}$$

Then S_3^d is the increasing enumeration of $\mathrm{Div}(\Delta_3^d)$.

The general scheme is illustrated in Figure 9. The sequence S_3^d is constructed by starting with $2d+1$ copies of S_2^d translated by $\theta_{3,0}, \dots, \theta_{3,2d}$ and inserting (translated copies of) fragments of the previous sequence S_3^{d-1}.

Example 4.8. The difference between the definition of S_3^d in (4-5) and that of S_2^d in (4-4) is the insertion of the additional factors $S_3^{d,p}$ between the consecutive terms

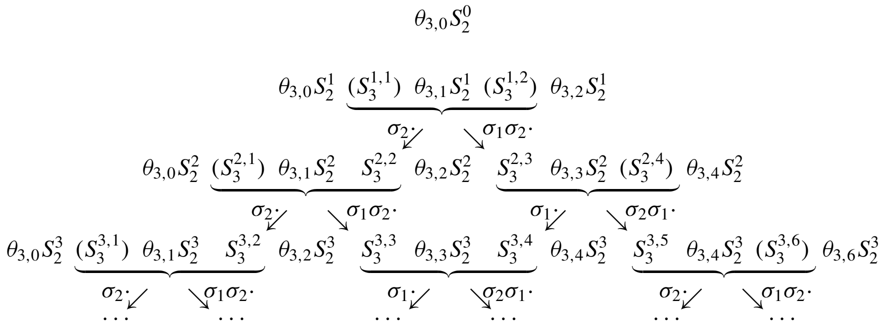

Figure 9. The inductive construction of S_3^d as a Pascal triangle: the subsequence $S_3^{d,p}$ is obtained by translating and concatenating the previous subsequences $S_3^{d-1,p-1}$ and $S_3^{d-1,p}$, or $S_3^{d-1,p-2}$ and $S_3^{d-1,p-1}$, depending on the parity of p. The bracketed sequences are empty; if we remove the subsequences $\theta_{3,q}S_2^d$, we have the Pascal triangle.

$\theta_{3,q}S_2^d$. Because $S_3^{d,1}$ and $S_3^{d,2d}$ are empty, the difference occurs for $d \geqslant 2$ only. The first values are:

$$\begin{aligned}
S_3^0 &= \theta_{3,0}S_2^0 = (1),\\
S_3^1 &= \theta_{3,0}S_2^1 + S_3^{1,1} + \theta_{3,1}S_2^1 + S_3^{1,2} + \theta_{3,2}\\
&= (1, \mathtt{a}) + \varnothing + \mathtt{b}(1, \mathtt{a}) + \varnothing + \mathtt{ab}(1, \mathtt{a}) = (1, \mathtt{a}, \mathtt{b}, \mathtt{ba}, \mathtt{ab}, \mathtt{aba}),\\
S_3^2 &= \theta_{3,0}S_2^2 + S_3^{2,1} + \theta_{3,1}S_2^2 + S_3^{2,2} + \theta_{3,2}S_2^2 + S_3^{2,3} + \theta_{3,3}S_2^2 + S_3^{2,4} + \theta_{3,4}S_2^2\\
&= (1, \mathtt{a}, \mathtt{aa}) + \varnothing + \mathtt{b}(1, \mathtt{a}, \mathtt{aa}) + \mathtt{b}(\mathtt{b}, \mathtt{ba}) + \mathtt{ab}(1, \mathtt{a}, \mathtt{aa})\\
&\qquad + \mathtt{ab}(\mathtt{b}, \mathtt{ba}) + \mathtt{aab}(1, \mathtt{a}, \mathtt{aa}) + \varnothing + \mathtt{baab}(1, \mathtt{a}, \mathtt{aa})\\
&= (1, \mathtt{a}, \mathtt{aa}, \mathtt{b}, \mathtt{ba}, \mathtt{baa}, \mathtt{bb}, \mathtt{bba}, \mathtt{ab}, \mathtt{aba}, \mathtt{abaa}, \mathtt{abb}, \mathtt{abba}, \mathtt{aab},\\
&\qquad \mathtt{aaba}, \mathtt{aabaa}, \mathtt{baab}, \mathtt{baaba}, \mathtt{baabaa}).
\end{aligned}$$

It is easy to check directly that the sequence S_3^d provides the increasing enumeration of $\mathrm{Div}(\Delta_3^d)$ for $d = 0, 1, 2$.

The proof of Proposition 4.7 will be split into several pieces, each of which is established using an induction on the degree d.

Lemma 4.9. *All entries in S_3^d are divisors of Δ_3^d.*

Proof. The result is true for $d = 0$. Assume $d \geqslant 1$. By construction, each entry in S_3^d either is of the form $\theta_{3,q}\sigma_1^e$ with $0 \leqslant q \leqslant 2d$ and $0 \leqslant e \leqslant d$ or belongs to some subsequence $S_3^{d,p}$ with $2 \leqslant p \leqslant 2d-1$. In the first case, $\theta_{3,q}\sigma_1^e$ is a right divisor of $\theta_{3,2d}\sigma_1^e$, which itself is a left divisor of $\theta_{3,2d}\sigma_1^d$. By Equation (4-1), the latter is Δ_3^d. Hence each $\theta_{3,q}\sigma_1^e$ is a divisor of Δ_3^d. As for the entries coming from some subsequence $S_3^{d,p}$, by definition they are of the form xy with x one of $\sigma_2, \sigma_1\sigma_2, \sigma_1, \sigma_2\sigma_1$ and y an entry in S_3^{d-1}. Then x is a divisor of Δ_3, while, by the induction hypothesis, y is a divisor of Δ_3^{d-1}. Thus xy is a divisor of Δ_3^d. □

Lemma 4.10. *The length of the sequence S_3^d equals the cardinality of* $\mathrm{Div}(\Delta_3^d)$.

Proof. Let ℓ_d denote the length of S_3^d. Computing ℓ_d by recursion is not very difficult but also unnecessary. Indeed, we saw in Section 3 that the cardinality $h_1(\Delta_3^d)$ of $\mathrm{Div}(\Delta_3^d)$ obeys the inductive rule (3-5). So it will be enough to check that ℓ_d satisfies the relation

$$\ell_d = 2\ell_{d-1} + 3d + 1 \tag{4-6}$$

and starts from the initial $\ell_1 = 6$ (or $\ell_0 = 1$). The latter point was checked in Example 4.8.

Figure 9 shows that most entries in S_3^{d-1} generate two entries in S_3^d. More precisely, each entry of S_3^{d-1} not belonging to a factor of the form $\theta_{3,2q} S_2^{d-1}$ generates two entries in S_3^d, and, conversely, each entry in S_3^d not belonging to a factor $\theta_{3,q} S_2^d$ comes from such an entry in S_3^{d-1}. The d factors $\theta_{3,2q} S_2^{d-1}$ in S_3^{d-1} each have length d, and the $2d+1$ factors $\theta_{3,2q} S_2^d$ in S_3^d each have length $d+1$. So we obtain

$$\ell_d - (2d+1)(d+1) = 2(\ell_{d-1} - d^2),$$

which gives Equation (4-6). □

At this point, we cannot (yet) conclude that each divisor of Δ_3^d occurs exactly once in S_3^d, as there could be some repetitions.

4C. *A quotient sequence for S_3^d.* Our next aim is to show that S_3^d is $<$-increasing. To this end, we shall explicitly determine the quotient of adjacent entries in S_3^d, that is, we shall specify a quotient sequence for S_3^d in the sense of Definition 2.22.

We begin by determining the first and the last entries of the sequence $S_3^{d,p}$. For S a nonempty sequence, we denote by $(S)_1$ and $(S)_\infty$ the first and last entry in S.

Lemma 4.11. *For $1 < p < 2d$, we have*

$$(S_3^{d,p})_1 = \theta_{3,p-1}\,\sigma_2 \quad \textit{and} \quad (S_3^{d,p})_\infty\,\sigma_2 = \theta_{3,p}\,\sigma_1^d.$$

Proof. The result is vacuously true for $d = 0$, 1. Assume $d \geqslant 2$ with $p = 0 \pmod 4$. Using the definition, the induction hypothesis, and (4-3), we find

$$(S_3^{d,p})_1 = \sigma_1\,(S_3^{d-1,p-1})_1 = \sigma_1\,\theta_{3,p-2}\,\sigma_2 = \theta_{3,p-1}\,\sigma_2,$$
$$(S_3^{d,p})_\infty\,\sigma_2 = \sigma_1\,(S_3^{d-1,p})_\infty\,\sigma_2 = \sigma_1\,\theta_{3,p}\,\sigma_1^{d-1} = \theta_{3,p}\,\sigma_1^d.$$

Similarly, for $p = 1 \pmod 4$, we have

$$(S_3^{d,p})_1 = \sigma_2\sigma_1\,(S_3^{d-1,p-2})_1 = \sigma_2\sigma_1\,\theta_{3,p-3}\,\sigma_2 = \theta_{3,p-1}\,\sigma_2,$$
$$(S_3^{d,p})_\infty\,\sigma_2 = \sigma_2\sigma_1\,(S_3^{d-1,p-1})_\infty\,\sigma_2 = \sigma_2\sigma_1\,\theta_{3,p-1}\,\sigma_1^{d-1} = \sigma_2\,\theta_{3,p-1}\,\sigma_1^{d} = \theta_{3,p}\,\sigma_1^{d}.$$

Then, for $p = 2 \pmod 4$, we have

$$(S_3^{d,p})_1 = \sigma_2\,(S_3^{d-1,p-1})_1 = \sigma_2\,\theta_{3,p-2}\,\sigma_2 = \theta_{3,p-1}\,\sigma_2,$$
$$(S_3^{d,p})_\infty\,\sigma_2 = \sigma_2\,(S_3^{d-1,p})_\infty\,\sigma_2 = \sigma_2\,\theta_{3,p}\,\sigma_1^{d-1} = \theta_{3,p}\,\sigma_1^{d}.$$

Finally, for $p = 3 \pmod 4$, we find

$$(S_3^{d,p})_1 = \sigma_1\sigma_2\,(S_3^{d-1,p-2})_1 = \sigma_1\sigma_2\,\theta_{3,p-3}\,\sigma_2 = \theta_{3,p-1}\,\sigma_2,$$
$$(S_3^{d,p})_\infty\,\sigma_2 = \sigma_1\sigma_2\,(S_3^{d-1,p-1})_\infty\,\sigma_2 = \sigma_1\sigma_2\,\theta_{3,p-1}\,\sigma_1^{d-1} = \sigma_1\sigma_2\sigma_1\sigma_2\,\theta_{3,p-3}\,\sigma_1^{d-1}$$
$$= \sigma_1\sigma_1\sigma_2\sigma_1\,\theta_{3,p-3}\,\sigma_1^{d-1} = \sigma_1\sigma_1\sigma_2\,\theta_{3,p-3}\,\sigma_1^{d} = \theta_{3,p}\,\sigma_1^{d}. \qquad \square$$

We shall now construct an explicit quotient sequence for S_3^d, that is, a sequence of braid words representing the quotients of the consecutive entries of S_3^d. Before doing it for S_3^d, let us consider the (trivial) cases of S_1^d and S_2^d. As S_1^d consists of one single entry, it vacuously admits the empty sequence as a quotient sequence. As for S_2^d, we can state:

Lemma 4.12. *For $d \geqslant 0$, let $\boldsymbol{w}_1^d$ be the empty sequence, and let $\boldsymbol{w}_2^d$ be defined by*

$$\boldsymbol{w}_2^d = \boldsymbol{w}_1^d + (\sigma_1) + \boldsymbol{w}_1^d + \cdots + \boldsymbol{w}_1^d + (\sigma_1) + \boldsymbol{w}_1^d,$$

d times (σ_1). Then $\boldsymbol{w}_2^d$ is a quotient sequence for S_2^d.

In a similar way, we shall prove:

Proposition 4.13. *Let $\boldsymbol{w}_3^d$ be the sequence defined by $\boldsymbol{w}_3^0 = \varnothing$ and*

$$\begin{aligned}(4\text{-}7)\quad \boldsymbol{w}_3^d = \boldsymbol{w}_2^d + (\sigma_1^{-d}\sigma_2) &+ \boldsymbol{w}_2^d + (\sigma_1^{-d}\sigma_2) + \boldsymbol{w}_3^{d,2} + (\sigma_2\sigma_1^{-d})\\ &+ \boldsymbol{w}_2^d + (\sigma_1^{-d}\sigma_2) + \boldsymbol{w}_3^{d,3} + (\sigma_2\sigma_1^{-d}) + \cdots\\ &+ \boldsymbol{w}_2^d + (\sigma_1^{-d}\sigma_2) + \boldsymbol{w}_3^{d,2d-1} + (\sigma_2\sigma_1^{-d})\\ &\qquad\qquad + \boldsymbol{w}_2^d + (\sigma_2\sigma_1^{-d}) + \boldsymbol{w}_2^d,\end{aligned}$$

with

$$\boldsymbol{w}_3^{d,2} = \boldsymbol{w}_3^{d,3} = \boldsymbol{w}_2^{d-1} + (\sigma_2\sigma_1^{-d+1}) + \boldsymbol{w}_3^{d-1,2},$$
$$\boldsymbol{w}_3^{d,2d-2} = \boldsymbol{w}_3^{d,2d-1} = \boldsymbol{w}_3^{d-1,2d-3} + (\sigma_1^{-d+1}\sigma_2) + \boldsymbol{w}_2^{d-1},$$
$$\boldsymbol{w}_3^{d,2p} = \boldsymbol{w}_3^{d,2p+1} = \boldsymbol{w}_3^{d-1,2p-1} + (\sigma_1^{-d+1}\sigma_2) + \boldsymbol{w}_2^{d-1} + (\sigma_2\sigma_1^{-d+1}) + \boldsymbol{w}_3^{d-1,2p},$$

for $4 \leqslant 2p \leqslant 2d-4$. Then $\boldsymbol{w}_3^d$ is a quotient sequence for S_3^d.

Example 4.14. We find $\boldsymbol{w}_3^1 = \boldsymbol{w}_2^1 + (\mathtt{Ab}) + \boldsymbol{w}_2^1 + (\mathtt{bA}) + \boldsymbol{w}_2^1 = (\mathtt{a}, \mathtt{Ab}, \mathtt{a}, \mathtt{bA}, \mathtt{a})$, and

$$\boldsymbol{w}_3^2 = \boldsymbol{w}_2^2 + (\mathtt{AAb}) + \boldsymbol{w}_2^2 + (\mathtt{AAb}) + \boldsymbol{w}_3^{2,2} + (\mathtt{bAA}) \\ + \boldsymbol{w}_2^2 + (\mathtt{AAb}) + \boldsymbol{w}_3^{2,3} + (\mathtt{bAA}) + \boldsymbol{w}_2^2 + (\mathtt{bAA}) + \boldsymbol{w}_2^2$$

with $\boldsymbol{w}_3^{2,2} = \boldsymbol{w}_3^{2,3} = \boldsymbol{w}_2^1 = (\mathtt{a})$, whence

$$\boldsymbol{w}_3^2 = (\mathtt{a}, \mathtt{a}, \mathtt{AAb}, \mathtt{a}, \mathtt{a}, \mathtt{AAb}, \mathtt{a}, \mathtt{bAA}, \mathtt{a}, \mathtt{a}, \mathtt{AAb}, \mathtt{a}, \mathtt{bAA}, \mathtt{a}, \mathtt{a}, \mathtt{bAA}, \mathtt{a}, \mathtt{a}).$$

Proof of Proposition 4.13. We prove using induction on d that $\boldsymbol{w}_3^d$ is a quotient sequence for S_3^d with the $4d-2$ terms in (4-7) corresponding to the $4d-1$ nonempty terms in (4-5). In particular, for $2 \leqslant p \leqslant 2d-1$, the subsequence $\boldsymbol{w}_3^{d,p}$ is a quotient sequence for $S_3^{d,p}$. The result is vacuously true for $d = 0$. Assume $d \geqslant 1$. By definition, the sequence S_3^d consists of the concatenation of the $2d+1$ sequences $\theta_{3,0} S_2^d, \cdots, \theta_{3,2d} S_2^d$, in which the $2d-2$ sequences $S_3^{d,2}, \ldots, S_3^{d,2d-1}$ are inserted. We shall consider these subsequences separately and then consider the transitions between consecutive subsequences.

First, since $\boldsymbol{w}_2^d$ is a quotient sequence for S_2^d, it is a quotient sequence for every sequence $\theta_{3,q} S_2^d$ as well, because, by definition, the quotients we consider are invariant under left translation. Then, by construction, each subsequence $S_3^{d,2p}$ or $S_3^{d,2p+1}$ appearing in S_3^d is obtained by translating some subsequence S of S_3^{d-1}, namely

$$S = S_3^{d-1,2p-1} + \theta_{3,q-1} S_2^{d-1} + S_3^{d-1,2p}.$$

By the induction hypothesis, the sequence

$$\boldsymbol{w}_3^{d-1,2p-1} + (\sigma_1^{-d+1}\sigma_2) + \boldsymbol{w}_2^{d-1} + (\sigma_2\sigma_1^{-d+1}) + \boldsymbol{w}_3^{d-1,2p},$$

which by definition is precisely $\boldsymbol{w}_3^{d,2p}$ and $\boldsymbol{w}_3^{d,2p+1}$, is a quotient sequence for S. The property remains true in the special cases $p = 1$ and $p = d$, which correspond respectively to removing the initial term $S_3^{d-1,2p-1}$ and the final term $S_3^{d-1,2p}$. Then $\boldsymbol{w}_3^{d,2p}$ and $\boldsymbol{w}_3^{d,2p+1}$ are also quotient sequences for any sequence obtained from S by a left translation, and, in particular, for $S_3^{d,2p}$ and $S_3^{d,2p+1}$.

It remains to study the transitions between the consecutive terms in the expression (4-5) of S_3^d, that is, to compare the last entry in each term with the first entry in the next term. Four cases are to be considered, namely the special cases of the first two terms and of the final two terms, and the generic cases of the transitions from $\theta_{3,q} S_2^d$ to $S_3^{d,p+1}$ and from $S_3^{d,p}$ to $\theta_{3,q} S_2^d$.

As for the first two terms $\theta_{3,0} S_2^d = S_2^d$ and $\theta_{3,1} S_2^d = \sigma_2 S_2^d$, the last entry in S_2^d is σ_1^d, while the first entry in $\sigma_2 S_2^d$ is σ_2, so $\sigma_1^{-d}\sigma_2$ is a quotient. For the last two terms $\theta_{3,2d-1} S_2^d$ and $\theta_{3,2d} S_2^d$, the last entry in $\theta_{3,2d-1} S_2^d$ is $\theta_{3,2d-1}\,\sigma_1^d$, while the first entry in $\theta_{3,2d} S_2^d$ is $\theta_{3,2d}$. Now, by (4-1), we have $\theta_{3,2d-1}\,\sigma_1^d\sigma_2 = \theta_{3,2d}\,\sigma_1^d$, so $\sigma_2\sigma_1^{-d}$ expresses the quotient.

Consider now the transition from $\theta_{3,q} S_2^d$ to $S_3^{d,q+1}$. The last entry in $\theta_{3,q} S_2^d$ is $\theta_{3,q}\,\sigma_1^d$, while, by Lemma 4.11, the first entry in $S_3^{d,q+1}$ is $\theta_{3,q}\,\sigma_2$. Hence $\sigma_1^{-d}\sigma_2$ represents the quotient. Finally, consider the transition from $S_3^{d,p}$ to $\theta_{3,q} S_2^d$. By Lemma 4.11 again, the last entry x in $\theta_{3,q} S_2^d$ satisfies $x\,\sigma_2 = \theta_{3,q}\,\sigma_1^d$, while the first entry in $\theta_{3,q} S_2^d$ is $\theta_{3,q}$. Hence $\sigma_2\sigma_1^{-d}$ represents the quotient. □

Corollary 4.15. *For each d the sequence S_3^d is $<$-increasing; so, in particular, it consists of pairwise distinct braids.*

Proof. By definition, every word in $\boldsymbol{w}_3^d$ is σ-positive. Hence, by Property A, it does not represent 1. □

As S_3^d consists of pairwise distinct divisors of Δ_3^d, Lemma 4.10 implies that every divisor of Δ_3^d occurs exactly once in S_3^d. Then, as S_3^d is $<$-increasing, it must be the increasing enumeration of $\mathrm{Div}(\Delta_3^d)$, and the proof of Proposition 4.7 is complete.

Remark 4.16. Once we know that S_3^d is the increasing enumeration of $\mathrm{Div}(\Delta_3^d)$ and that $\boldsymbol{w}_3^d$ is a σ-positive quotient sequence for S_3^d, we can count the 2-jumps in S_3^d and obtain the value of $h_2(\Delta_3^d)$ directly. This amounts to forgetting about all $\sigma_1^{\pm 1}$ in the construction of $\boldsymbol{w}_3^d$, and it is then fairly obvious that there only remains $2^d - 2$ times σ_2.

4D. *Larger values of n.* The same construction can be developed for $n = 4$ and beyond. The general scheme is to define S_4^d using an inductive rule

$$S_4^d = \theta_{4,0} S_3^d + S_4^{d,1} + \theta_{4,1} S_3^d + \cdots + \theta_{4,3d-1} S_3^d + S_4^{d,3d} + \theta_{4,3d} S_3^d,$$

where the intermediate factor $S_4^{d,p}$ is constructed by concatenating and translating convenient fragments of S_4^{d-1}. Owing to the inductive rule (3-6) satisfied by the number of elements $h_1(\Delta_4^d)$ of $\mathrm{Div}(\Delta_4^d)$, we can expect the generic entry of S_4^{d-1} to be repeated six times in S_4^d, but with some entries from S_4^{d-2} repeated three times only. After completing the inductive definition of S_4^d, showing that the sequence is $<$-increasing and counting its entries should be easy. As we have no complete description so far, we leave the question open here.

4E. *A new construction for the linear ordering of B_3.* In pursuing the approach described above, we were interested in connecting the Garside structure of B_n with its linear ordering. In the process, we found something more: a new, independent construction of the braid ordering, at least for B_3, which is currently the only completed case.

As recalled in the introduction, the existence of the linear ordering of braids relies on two properties of braids, namely Property A and Property C. These properties have received a number of independent proofs [Dehornoy et al. 2002]. In particular, Property A has now a very short proof based on Dynnikov's coordinization for singular triangulations of a punctured disk [Dehornoy et al. 2002, Chapter 9]. As for Property C, no really simple proof exists so far. Even without the initial argument involving self-distributive algebra, the remaining arguments—the combinatorial proofs based on handle reduction or on Burckel's uniform tree approach, or the geometric proofs based on standardization of curve diagrams—all require some care. For now, it seems that the optimal proof of Property C is forthcoming.

Here is a direct application of our construction of the sequence S_3^d:

Proposition 4.17. *Property C holds for B_3; that is, every nontrivial 3-braid admits a σ-positive or a σ-negative expression.*

New proof. We take as an hypothesis that Property A is true, so that the relation $<$ is a partial ordering, but we do not assume that $<$ is linear. As every braid in B_3 is the quotient of two positive braids in B_3^+, proving Property C for B_3 amounts to proving that, if x, y are arbitrary elements of B_3^+, then the quotient $x^{-1}y$ admits a σ-positive or a σ-negative expression.

Now the construction of S_3^d is self-contained, as is that of $\boldsymbol{w}_3^d$. Then, by construction, every word in $\boldsymbol{w}_3^d$ is σ-positive. As any concatenation of σ-positive words is σ-positive, it follows that, if x, y are any braids occurring in $\bigcup_d S_3^d$, then the quotient $x^{-1}y$ admits a σ-positive or a σ-negative expression, according to whether x occurs before or after y in S_3^d. To conclude Property C is true, it remains to check that each positive 3-braid occurs in $\bigcup_d S_3^d$. Because every entry of S_3^d belongs to $\mathrm{Div}(\Delta_3^d)$, this is equivalent to proving that each divisor of Δ_3^d occurs in S_3^d. Property A guarantees that the entries of S_3^d are pairwise distinct (Corollary 4.15), so it suffices to compare the length of S_3^d with the cardinality of $\mathrm{Div}(\Delta_3^d)$, and this is what we made in Lemma 4.10. □

The construction of S_3^d gives more. The approach developed by S. Burckel [1997] introduces a convenient notion of normal braid words such that every positive braid admits exactly one normal expression. For 3-strand braids, the definition is as follows. Every positive 3-strand braid word w can be written as an alternating product of blocks σ_1^e and σ_2^e. Then we define the *code* of w to be the sequence of the sizes of these blocks. To avoid ambiguity, we consider the last block to be a block of σ_1's, that is, we decide that the code of σ_1 is (1), while the code of σ_2 is $(1, 0)$. For instance, the code of $\sigma_2^2\sigma_1^3\sigma_2^5$ is $(2, 3, 5, 0)$.

Definition 4.18. A positive 3 strand braid word w is said to be *normal in the sense of Burckel* if its code has the form $(e_1, \dots, e_\ell)$ with $e_k \geqslant 2$ for $2 \leqslant k \leqslant \ell - 2$.

Burckel [1997] shows that every positive 3-braid admits a unique normal expression and, moreover, that $x < y$ holds if and only if the normal form of x is `ShortLex`-smaller than the normal form of y, where `ShortLex` refers to the variant of the lexicographic ordering of sequences in which the length is given priority: $(e_1, \dots, e_\ell) <_{\texttt{ShortLex}} (e'_1, \dots, e'_{\ell'})$ always holds for $\ell < \ell'$ and, when $\ell = \ell'$, it holds when $(e_1, \dots, e_\ell)$ is lexicographically smaller than $(e'_1, \dots, e'_{\ell'})$. Burckel's method defines an iterative reduction process on nonnormal braid words. Our current approach provides for a simpler method. First, a direct inspection shows:

Lemma 4.19. *Let $\underline{S}_3^d$ be the sequence of braid words defined by the inductive rule (4-5). Then $\underline{S}_3^d$ consists of words that are normal in the sense of Burckel.*

Then, by construction, every braid in S_3^d is represented by a word of $\underline{S}_3^d$. As every positive 3-braid occurs in $\bigcup S_3^d$, we immediately deduce:

Proposition 4.20. *Every positive 3-braid admits an expression that is normal in the sense of Burckel.*

This in turn enables us to obtain a simple proof for the following deep, and so far not very well understood, result due to Laver [1996] and to Burckel [1997] for the ordinal type:

Corollary 4.21. *The restriction of $<$ to B_3^+ is a well-ordering of ordinal type ω^ω.*

Proof. The ShortLex ordering of sequences of nonnegative integers is a well-ordering of ordinal type ω^ω, so its restriction to codes of normal words in the sense of Burckel is a well-ordering as well. The type of the latter cannot be less than ω^ω, as one can easily exhibit an increasing sequence of length ω^ω. □

Burckel's approach extends to all braid monoids B_n^+. Burckel introduces a convenient notion of a normal word, but the associated reduction process is very intricate. Hopefully, the above approach will provide a much simpler approach to completing the construction of the sequences S_4^d and, more generally, S_n^d. In particular, once the correct definition is given, all subsequent proofs should reduce to easy inductions.

Acknowledgement

The author thanks the PJM production editors, Matt Cargo and Silvio Levy, for their suggestions.

References

[Birman 1974] J. S. Birman, *Braids, links, and mapping class groups*, Princeton University Press, Princeton, N.J., 1974. Annals of Mathematics Studies, No. 82. MR 51 #11477

[Burckel 1997] S. Burckel, "The wellordering on positive braids", *J. Pure Appl. Algebra* **120**:1 (1997), 1–17. MR 98h:20062 Zbl 0958.20032

[Burckel 1999] S. Burckel, "Computation of the ordinal of braids", *Order* **16**:3 (1999), 291–304. MR 2001i:20075 Zbl 0980.20026

[Burckel 2001] S. Burckel, "Syntactical methods for braids of three strands", *J. Symbolic Comput.* **31**:5 (2001), 557–564. MR 2002b:20051 Zbl 0990.20022

[Carlitz et al. 1976] L. Carlitz, R. Scoville, and T. Vaughan, "Enumeration of pairs of permutations", *Discrete Math.* **14**:3 (1976), 215–239. MR 53 #156 Zbl 0322.05008

[Charney 1995] R. Charney, "Geodesic automation and growth functions for Artin groups of finite type", *Math. Ann.* **301**:2 (1995), 307–324. MR 95k:20055 Zbl 0813.20042

[Dehornoy 1994] P. Dehornoy, "Braid groups and left distributive operations", *Trans. Amer. Math. Soc.* **345**:1 (1994), 115–150. MR 95a:08003 Zbl 0837.20048

[Dehornoy 1997] P. Dehornoy, "A fast method for comparing braids", *Adv. Math.* **125**:2 (1997), 200–235. MR 98b:20060 Zbl 0882.20021

[Dehornoy 1999] P. Dehornoy, "Strange questions about braids", *J. Knot Theory Ramifications* **8**:5 (1999), 589–620. MR 2000d:20052 Zbl 0933.20024

[Dehornoy 2002] P. Dehornoy, "Groupes de Garside", *Ann. Sci. École Norm. Sup.* (4) **35**:2 (2002), 267–306. MR 2003f:20068 Zbl 1017.20031

[Dehornoy 2007] P. Dehornoy, "Combinatorics of normal sequences of braids", *J. Combin. Theory Ser. A* **114**:3 (2007), 389–409. MR MR2310741 Zbl 1116.05006

[Dehornoy et al. 2002] P. Dehornoy, I. Dynnikov, D. Rolfsen, and B. Wiest, *Why are braids orderable?*, Panoramas et Synthèses **14**, Société Mathématique de France, Paris, 2002. MR 2004e:20062 Zbl 1048.20021

[El-Rifai and Morton 1994] E. A. El-Rifai and H. R. Morton, "Algorithms for positive braids", *Quart. J. Math. Oxford Ser.* (2) **45**:180 (1994), 479–497. MR 96b:20052 Zbl 0839.20051

[Epstein et al. 1992] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, and W. P. Thurston, *Word processing in groups*, Jones and Bartlett, Boston, 1992. MR 93i:20036 Zbl 0764.20017

[Garside 1969] F. A. Garside, "The braid group and other groups", *Quart. J. Math. Oxford Ser.* (2) **20** (1969), 235–254. MR 40 #2051 Zbl 0194.03303

[Larue 1994] D. Larue, *Left-distributive and left-distributive idempotent algebras*, Ph.D. thesis, University of Colorado, Boulder, 1994.

[Laver 1996] R. Laver, "Braid group actions on left distributive structures, and well orderings in the braid groups", *J. Pure Appl. Algebra* **108**:1 (1996), 81–98. MR 97e:20061 Zbl 0859.20029

[McCammond 2005] J. McCammond, "An introduction to Garside structures", Preprint, 2005, Available at http://www.math.ucsb.edu/~mccammon/papers/intro-garside.pdf.

[Solomon 1976] L. Solomon, "A Mackey formula in the group ring of a Coxeter group", *J. Algebra* **41**:2 (1976), 255–264. MR 56 #3104 Zbl 0355.20007

Received April 6, 2006.

PATRICK DEHORNOY
LABORATOIRE DE MATHÉMATIQUES NICOLAS ORESME UMR 6139
UNIVERSITÉ DE CAEN
14032 CAEN
FRANCE

dehornoy@math.unicaen.fr
www.math.unicaen.fr/~dehornoy