COMBINATORICS OF NORMAL SEQUENCES OF BRAIDS

PATRICK DEHORNOY

Abstract. Many natural counting problems arise in connection with the normal form of braids—and seem to have not been much considered so far. Here we solve some of them. One of the noteworthy points is that a number of different induction schemes appear. The key technical ingredient is an analysis of the normality condition in terms of permutations and their descents, in the vein of the Solomon algebra. As was perfectly summarized by a referee, the main result asserts that the size of the automaton involved in the automatic structure of B_n associated with the normal form can be lowered from $n!$ to $p(n)$, the number of partitions of n.

Ubiquitous and connected with a number of domains, Artin's braid groups B_n, $n \geqslant 3$, have received much attention in the recent years. However, not so many works are devoted to a purely combinatorial study of braids, presumably because counting arguments did not prove so far to be much helpful for investigating braids. Nevertheless, although braid groups are infinite, they admit several filtrations leading to finite sets and, therefore, to natural enumeration problems.

For each presentation of braid groups, (at least) two natural counting problems arise, namely, on the one hand, counting how many braids admit an expression of a given length, in particular evaluating the associated growth rate, and, on the other hand, counting, for a given braid, how many words represent that specific braid, a relevant question when the number is finite, typically when we discard the inverses of the generators and only consider positive expressions, *i.e.*, when we restrict to some submonoid of B_n.

In the case of the Artin generators σ_i, both types of questions have been addressed, and at least partially solved: the first question, actually not for B_n but for the submonoid B_n^+ of B_n generated by the σ_i's, was investigated in [26], and completely solved in [5]. As for the second question, it is natural in this context to address it for the particular elements Δ_n^d, where Δ_n is Garside's fundamental braid [19]. It was investigated and solved for $n = 3$ in [10].

In this paper, we address similar questions for another natural generating set, namely the so-called simple braids, also called the Garside generators below [19]. These generators, which are the divisors of Δ_n in the monoid B_n^+, are in one-to-one correspondence with permutations of n objects, and they give rise to a remarkable unique decomposition for each braid, usually called its normal form [15, 1, 17, 16]. Because of its uniqueness and of its many nice properties, expressed in particular in the existence of a bi-automatic structure, the normal form of braids is the preferred way of specifying

1991 *Mathematics Subject Classification.* 20F36, 05A05.

Key words and phrases. braid group; normal form; fundamental braid; counting; generating function.

braids in many recent developments, in particular those of algorithmic or cryptographical nature [20, 22].

The question we address here is to count the number of braids with a normal form of a given length. It was addressed by P. Xu in [26], and by R. Charney in [9]: she observed that, because normal words can be recognized by a finite state automaton, the number of braids with length d obeys a linear induction rule, and the associated generating function is rational, and gives explicit values in the case of 3 and 4 strand braids. The aim of this paper is to go further in the investigation of counting problems connected with the normal form of braids. We concentrate on the case of the monoid B_n^+. Then studying the number of positive n strand braids with a normal form of length (at most) d is the counterpart for Garside generators of the problem solved in [5] in the case of Artin generators. The main difference is that, in the case of Garside generators, the length is no longer an additive parameter: for instance, multiplying two simple braids may result in a simple braid, *i.e.*, multiplying two braids of length 1 may result in a braid of length 1. This makes the current study much more uneasy.

Let $b_{n,d}$ denote the number of positive n strand braids with a normal form of length at most d, *i.e.*, the number of divisors of Δ_n^d in B_n^+. We establish various results about the numbers $b_{n,d}$, and about the connected numbers $b_{n,d}(x)$ that count, for x a simple braid, the positive n strand braid with a normal form of length at most d whose dth factor is precisely x. Two types of results are established, namely results for fixed braid index n, and results for fixed degree d. When n is fixed and d varies, as was recalled above, the numbers $b_{n,d}$ and $b_{n,d}(x)$ obey a linear induction rule associated with a certain $n! \times n!$ adjacency matrix M_n. Here we show that M_n can be replaced with a smaller matrix of size $p(n) \times p(n)$, where $p(n)$ is the number of partitions of n—which means that the size of the automaton involved in the bi-automatic structure of B_n can be lowered to $p(n)$. The result relies on analysing the descents of the permutations associated with simple braids, and it is connected with a classical result by Solomon [25]. It is then easy to deduce the numerical value of $b_{n,d}$ for small n, d, as well as explicit formulas, at least for $n \leqslant 4$. We are also led to several conjectures about the eigenvalues of the matrix M_n that seem to have never been considered so far. The most puzzling one claims that the characteristic polynomial of M_{n-1} divides that of M_n. It holds at least for $n \leqslant 10$.

When d is fixed and n varies, quite different induction rules appear. Everything is trivial for $d = 1$, and an explicit formula for $b_{n,2}$ can be deduced from the results of [6, 7]. It seems difficult to go further in general, but new results (and new induction schemes) appear when we consider the numbers $b_{n,d}(\Delta_{n-r})$ with $1 \leqslant r \leqslant n$, typically in the (non-trivial) case $r = 1$, and, more generally, when r is fixed. In particular, we obtain explicit values for $b_{n,3}(\Delta_{n-1})$, $b_{n,3}(\Delta_{n-2})$, and $b_{n,4}(\Delta_{n-1})$.

The specific questions investigated in this paper, in particular that of the value of $b_{n,d}(\Delta_{n-r})$, arose in [13]. There exists a linear ordering of braids relying on the notion of a σ-positive braid word [12], and the aim of [13] is to develop a new approach to that ordering based on the study of its connection with the Garside structure. It turns out that certain parameters describing the restriction of the ordering to positive n-braids of degree at most d can be expressed in terms of the numbers $b_{n,d}(\Delta_r)$, an initial motivation for our current study of these numbers. However, we think that the formulas and methods developed in the current paper go beyond the above specific applications. In particular, the great diversity of the induction schemes appearing in connection with various specializations of the general problem is remarkable. At the least, the current study should demonstrate the richness of the combinatorics underlying the normal form of braids.

Still other presentations of the braid groups are known, in particular the one involving the so-called dual monoid [2, 4], which gives rise to an alternative Garside structure, and, therefore, to an alternative normal form analogous to that considered here, where the role of simple braids is played by elements that are in one-to-one correspondence with non-crossing partitions. All questions considered in the current paper could be similarly addressed for the dual structure, and, more generally, for the many presentations of B_n known to date. Similarly, Artin's braid groups B_n belong to larger families of groups, typically Artin-Tits groups of spherical type and, more generally, Garside groups [14, 11, 23]. Once again, all questions considered here extend to such frameworks naturally. However, mainly because of the specific applications mentioned above, we find it interesting to consider here the specific framework of braids and permutations, and we leave the extensions for further investigation.

The paper is organized as follows. Section 1 sets the framework and the basic definitions. In Section 2 we introduce the adjacency matrix M_n that controls the sequences $b_{n,d}$ for fixed n and show how to reduce their size from $n!$ to 2^{n-1}. In Section 3, we show how to further reduce the size to $p(n)$, and solve the induction for small values of n. Finally, in Section 4, we turn to the cases when the degree is fixed and the braid index varies.

Acknowledgment

The author thanks C. Hohlweg, F. Hivert and J.C. Novelli for interesting discussions about the topics investigated in this paper, in particular Remark 3.6.

1. Background and preliminary results

Our notation is standard, and we refer to textbooks like [3] or [17] for basic results about braid groups. We recall that the n strand braid group B_n is defined for $n \geqslant 1$ by the presentation

$$B_n = \left\langle \sigma_1, \ldots, \sigma_{n-1} \,;\, \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & \text{for } |i-j| \geqslant 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{for } |i-j| = 1 \end{array} \right\rangle. \tag{1.1}$$

So, B_1 is a trivial group $\{1\}$, while B_2 is the free group 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), *i.e.*, the direct limit of all B_n's under 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 a 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 $[w]$.

It is standard to associate with every n strand braid word w an n strand braid *diagram* by stacking elementary diagrams associated with the successive letters according to the rules

Then two braid words are equivalent if and only if the diagrams they encode are the projections of ambient isotopic figures in $\mathbb{R}^3$, *i.e.*, one can deform one diagram into the other without allowing the strands to cross or moving the endpoints.

1.1. **The monoid B_n^+ and the braids Δ_n.** Let B_n^+ be the monoid admitting the presentation (1.1). The elements of B_n^+ are called *positive* n-braids.

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^+.

As B_n^+ is not commutative for $n \geqslant 3$, there are the symmetric notions of a right divisor and a left multiple—but we shall mostly use left divisors here. 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.

Wih respect to left divisibility, B_n^+ has the structure of a lattice [19]: any two positive n-braids x, y admit a greatest common left divisor, denoted $\gcd(x, y)$, and a least common right multiple. A special role is played by the lcm of the elements σ_1, ..., σ_{n-1}, traditionally denoted Δ_n, which is inductively defined by

$$\Delta_1 = 1, \qquad \Delta_n = \sigma_1\sigma_2 \dots \sigma_{n-1}\,\Delta_{n-1}. \tag{1.2}$$

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

1.2. **The normal form.** 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* in the sequel. Geometrically, simple braids are those positive braids that can be represented by a braid diagram in which any two strands cross at most once.

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 obtains the so-called normal expression [16, 17].

Definition 1.2. A sequence $(x_1, \dots, x_d)$ of simple n-braids is said to be *normal* if, for each k, one has $x_k = \gcd(\Delta_n, x_k \dots x_d)$.

Clearly, each positive braid admits a unique normal expression. It will be convenient here 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 *dth 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 dth factor of x is not 1. It is well known that the positive n-braids of degree at most d coincide with the (left or right) divisors of Δ_n^d.

The only properties of the normal form we shall use here are as follows:

Lemma 1.3. [8] *Assume that $(x_1, \dots, x_d)$ is a sequence of simple n-braids. Then the following are equivalent:*

(i) *The sequence $(x_1, \dots, x_d)$ is normal;*
(ii) *For $1 \leqslant k < d$, the sequence (x_k, x_{k+1}) is normal;*
(iii) *For $1 \leqslant k < d$, every σ_i dividing x_{k+1} on the left divides x_k on the right.*

Definition 1.4. For x a simple n-braid, we define $D_L(x)$ (*resp.* $D_R(x)$) to be the set of all i's such that σ_i is a left (*resp.* right) divisor of x.

The example of σ_2 and $\sigma_2\sigma_1\sigma_3\sigma_2$, for which both D_L and D_R is $\{2\}$, shows that these sets do not determine a simple braid. However, as far as normal sequences are concerned, they contain all needed information, as Lemma 1.3 can be restated as:

Lemma 1.5. *A sequence of simple n-braids $(x_1, \dots, x_d)$ is normal if and only if, for each $k < d$, we have $D_R(x_k) \supseteq D_L(x_{k+1})$.*

1.3. **Connection with permutations.** Everywhere in the sequel, we write $[\![1, n]\!]$ for $\{1, \dots, n\}$. 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 $[\![1, n]\!]$, there exists exactly one simple braid x satisfying $\pi(x) = f$.

The Exchange Lemma for Coxeter groups connects the sets $D_L(x)$ and $D_R(x)$ with the permutation associated with x and their descents. For f a permutation, use $\ell(f)$ for the minimal number of factors occurring in a decomposition of f as a product of transpositions. The precise statement is

Lemma 1.6. *Let x be a simple n-braid x. For $1 \leqslant i < n$, the following are equivalent:*

(i) *The braid σ_i is a left divisor of x in B_n^+, i.e., i belongs to $D_L(x)$;*
(ii) *The strands starting at positions i and $i+1$ cross in any positive diagram for x;*
(iii) *We have $\pi(x)^{-1}(i) > \pi(x)^{-1}(i+1)$;*
(iv) *We have $\ell(\pi(\sigma_i x)) < \ell(\pi(x))$, i.e., i is a descent of $\pi(x)^{-1}$.*

Symmetrically, the following are equivalent:

(i') *The braid σ_i is a right divisor of x in B_n^+, i.e., i belongs to $D_R(x)$;*
(ii') *The strands finishing at positions i and $i+1$ cross in any positive diagram for x;*
(iii') *We have $\pi(x)(i) > \pi(x)(i+1)$;*
(iv') *We have $\ell(\pi(x\sigma_i)) < \ell(\pi(x))$, i.e., i is a descent of $\pi(x)$.*

So, for x a simple braid, the indices i such that σ_i is a right divisor of x are the descents of the associated permutation $\pi(x)$, while those such that σ_i is a left divisor of x are the descents of $\pi(x)^{-1}$.

1.4. **The numbers $b_{n,d}$ and $b_{n,d}(x)$.** Our aim in this paper is to solve various counting problems involving the normal form of positive braids. The main numbers we investigate are as follows:

Definition 1.7. For $n, d \geqslant 1$, we denote by $b_{n,d}$ the number of positive n strand braids of degree at most d, *i.e.*, the number of divisors of Δ_n^d in the braid monoid.

By Lemma 1.5, $b_{n,d}$ is the number of normal sequences of length d, *i.e.*, the number of sequences $(x_1, \dots, x_d)$ where all x_k are simple braids and $D_L(x_k) \supseteq D_R(x_{k+1})$ holds for

$k < d$. By Lemma 1.6, it is also the number of sequences of permutations $(f_1, \dots, f_d)$ such that, for each $k < d$, the descents of f_{k+1}^{-1} are included in those of f_k.

For $d = 1$, the bijection between simple n strand braids and permutations of $[\![1, n]\!]$ immediately gives

$$b_{n,1} = n!, \tag{1.3}$$

which implies for all n, d

$$b_{n,d} \leqslant (n!)^d. \tag{1.4}$$

In the sequel, we shall have to count normal sequences satisfying some constraints. So we introduce one more notation.

Definition 1.8. For $n, d \geqslant 1$ and x a simple n-braid, we denote by $b_{n,d}(x)$ the number of positive n strand braids of degree at most d with dth factor equal to x.

In other words, $b_{n,d}(x)$ is the number of normal sequences of the form $(x_1, \dots, x_{d-1}, x)$. Some connections are obvious:

Proposition 1.9. *For all n, d, we have*

$$b_{n,d} = \sum_{x \text{ simple}} b_{n,d}(x) = b_{n,d+1}(1). \tag{1.5}$$

Proof. The first equality is obvious. The second one follows from the fact that $(x_1, \dots, x_d)$ is normal if and only if $(x_1, \dots, x_d, 1)$ is: indeed, 1 has no left divisor but itself, so, by Lemma 1.3, every sequence $(x, 1)$ is normal. □

2. Adjacency matrices

In this section and the next one, we study the numbers $b_{n,d}$ and $b_{n,d}(x)$ when n is fixed and d varies. By Lemma 1.3, normal sequences of simple braids are characterized by a purely local criterion that only involves adjacent entries. It follows that the set of all normal sequences can be recognized by a finite state automaton [17], and, as a consequence, the associated counting numbers obey a linear induction rule specified by a certain adjacency matrix [18]. In this section, we define the matrix involved in the current situation, and show how its size, which is originally $n!$, can be lowered to 2^{n-1}.

2.1. **Enumeration of simple braids.** Below we consider matrices whose entries are indexed by simple braids (or, equivalently, permutations). Fixing an enumeration of simple braids is not important at a conceptual level, but this is necessary when the objects are to be specified explicitly. We shall use the restriction of the canonical linear ordering of braids denoted $<^\phi$ in [12]—which gives for each n a well-ordering of ordinal type $\omega^{\omega^{n-2}}$ on B_n^+. The corresponding increasing enumeration of simple n-braids can be constructed directly using induction on n. We start from the following easy remark:

Lemma 2.1. *For $1 \leqslant i \leqslant n$, write $\sigma_{i,n}$ for $\sigma_i \sigma_{i+1} \dots \sigma_{n-1}$ (so that $\sigma_{n,n}$ is 1). Then every simple n-braid x admits a unique decomposition $x = \sigma_{i,n}\, y$ with $1 \leqslant i \leqslant n$ and y a simple $(n-1)$-braid.*

Proof. (Figure 1) Let $i = \pi(x)(n)$. Then we can realize x by a diagram in which the ith strand is first sent to the rightmost position, and it remains a simple $(n-1)$-braid. Conversely, we have $i = \pi(\sigma_{i,n} y)(n)$, so the decomposition is unique. □

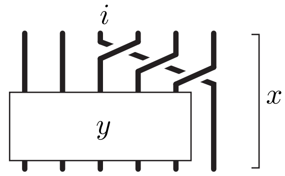

FIGURE 1. Proof of Lemma 2.1

Definition 2.2. We inductively define an enumeration S_n of simple n-braids by

$$S_1 := (1), \quad S_n := S_{n-1} {}^\frown\, \sigma_{n-1,n} S_{n-1} {}^\frown \dots {}^\frown\, \sigma_{1,n} S_{n-1}, \tag{2.1}$$

where $^\frown$ stands for list concatenation, and xS is the list obtained from S by multipliying all entries by x on the left. The kth element in $\bigcup_n S_n$ is denoted τ_k.

The first τ_k's are, in increasing order,

$$\tau_1 = 1\ , \tau_2 = \sigma_1\ , \tau_3 = \sigma_2\ , \tau_4 = \sigma_2\sigma_1\ , \tau_5 = \sigma_1\sigma_2\ , \tau_6 = \sigma_1\sigma_2\sigma_1\ , \tau_7 = \sigma_3, \dots$$

Lemma 2.1 guarantees that all simple braids occur in the above enumeration. Note that, for every n, we have $\Delta_n = \tau_{n!}$.

It is easy to check that the ordering of simple braids we use corresponds to a reversed antilexicographic ordering of the inverses of the associated permutations: x occurs before y if and only if we have $\pi(x)^{-1} < \pi(y)^{-1}$, where $f < g$ is said to hold if we have $f(i) > g(i)$ for the largest i for which f and g do not agree. Also, observe that S_n is obtained from S_{n-1} by using minimal length representatives for the cosets of $\mathfrak{S}_n/\mathfrak{S}_{n-1}$.

2.2. **The matrix M_n.** Everywhere in the sequel, we write $(M)_{x,y}$ for the (x, y)-entry of a matrix M.

Definition 2.3. For $n \geqslant 1$, we define M_n to be the $n! \times n!$ matrix satisfying

$$(M_n)_{k,\ell} = \begin{cases} 1 & \text{if } (\tau_k, \tau_\ell) \text{ is normal,} \\ 0 & \text{otherwise.} \end{cases}$$

Instead of referring to integer entries, it will be often convenient to think of the entries of M_n as directly indexed by simple braids; for x, y simple braids, we simply write $(M_n)_{x,y}$ for the corresponding entry.

Example 2.4. The first 3 matrices M_n are

$$M_1 = 1, \quad M_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

The construction of the matrix M_n immediately implies the following results:

Lemma 2.5. (i) *The first column and the last row of M_n contain only 1's; the first row, its first entry excepted, and the last column, its last entry excepted, contain only 0's.*

(ii) *The first $(n-1)!$ columns of M_n consist of n stacked copies of M_{n-1}.*

(iii) If $D_R(\tau_k) = D_R(\tau_{k'})$ holds, then the kth and the k'th rows in M_n coincide. Similarly, if $D_L(\tau_\ell) = D_L(\tau_{\ell'})$ holds, then the ℓth and the ℓ'th columns in M_n coincide.

Proof. (i) By construction, we have $\tau_1 = 1$ and $\tau_{n!} = \Delta_n$. Now $(x, 1)$ is always normal, and so is (Δ_n, x). On the other hand, $(1, x)$ is normal only for $x = 1$, and (x, Δ_n) is normal only for $x = \Delta_n$.

(ii) Assume $k \leqslant (n-1)!$ and $k' = k + (n-i)\cdot(n-1)!$. Our enumeration of simple braids implies $\tau_{k'} = \sigma_{i,n}\tau_k$. Then Figure 1 makes the equality $D_R(\tau_{k'}) \cap [\![1, n-1]\!] = D_R(\tau_k)$ clear. For every simple $(n-1)$-braid y, the set $D_L(y)$ is included in $[\![1, n-1]\!]$, and it follows that $(\tau_{k'}, y)$ is normal if and only if (τ_k, y) is. In other words, we have $(M_n)_{k',\ell} = (M_n)_{k,\ell}$ for $\ell \leqslant (n-1)!$.

(iii) By Lemma 1.3, the value of $(M_n)_{k,\ell}$ only depends on $D_R(\tau_k)$ and on $D_L(\tau_\ell)$. □

The connection between the numbers $b_{n,d}(x)$ and the matrix M_n is straightforward:

Lemma 2.6. *For every simple y and every $d \geqslant 1$, we have*

$$b_{n,d}(y) = ((1, 1, \ldots, 1)\, M_n^{d-1})_y. \tag{2.2}$$

Proof. Induction on d. For $d = 1$, and for each simple n-braid x, there is exactly one braid of degree at most 1 whose first factor is y, namely y itself, and we have $b_{n,1}(y) = 1$. Assume $d \geqslant 2$. By Lemma 1.3, $(x_1, \ldots, x_{d-1}, y)$ is normal if and only if $(x_1, \ldots, x_{d-1})$ and (x_{d-1}, y) are normal, so we get

$$b_{n,d}(y) = \sum_{(x,y) \text{ normal}} b_{n,d-1}(x) = \sum_x b_{n,d-1}(x)\,(M_n)_{x,y},$$

and (2.2) follows inductively. □

Remark 2.7. As the last row of M_n is $(1, \ldots, 1)$, we have $(1, \ldots, 1) = (0, \ldots, 0, 1)M_n$, and we can replace (2.2) with

$$b_{n,d}(y) = ((0, \ldots, 0, 1)\, M_n^d)_y. \tag{2.3}$$

Example 2.8. Using the value of M_2, we immediately find $b_{2,d}(1) = d$, $b_{2,d}(\sigma_1) = 1$, as could be expected: there are $d+1$ 2-braids of degree at most d, namely the braids σ_1^k with $k < d$, whose dth factor is 1, and σ_1^d, whose dth factor is Δ_2, *i.e.*, σ_1.

The computation for $n \geqslant 3$ is more complicated, and we postpone it. For the moment, we just point that, as the numbers $b_{n,d}(x)$ obey the linear recurrence (2.2), standard arguments imply that they can be expressed in terms of the eigenvalues of M_n:

Proposition 2.9. *Let $\rho_1, \ldots, \rho_k$ be the non-zero eigenvalues of M_n. Then, for each simple n-braid x, there exist polynomials $P_1, \ldots, P_k$ with $\deg(P_i)$ at most the multiplicity of ρ_i for M_n such that, for each $d \geqslant 0$, we have*

$$b_{n,d}(x) = P_1(d)\rho_1^d + \cdots + P_k(d)\rho_k^d. \tag{2.4}$$

Corollary 2.10. *For all n, x, the generating function of the numbers $b_{n,d}(x)$'s with respect to d is rational.*

2.3. **Reducing the size.** The size $n!$ of the adjacency matrix M_n is uselessly large, and we shall see now how to lower it. This will be done in two steps. The first one relies on the fact, pointed out in Lemma 2.5(*iii*), that many columns in M_n are equal. For subsequent use, it will be useful to introduce a new sequence of numbers:

Definition 2.11. For $I, J \subseteq [\![1, n-1]\!]$, we denote by $a_{n,I,J}$ (*resp.* $\widehat{a}_{n,I,J}$) the number of simple n-braids satisfying $D_L(x) = I$ (*resp.* $D_L(x) \supseteq I$) and $D_R(x) \supseteq J$.

Lemma 2.12. *For $n \geqslant 1$, let M'_n be the $2^{n-1} \times 2^{n-1}$ matrix with entries indexed by subsets of $[\![1, n-1]\!]$ defined by $(M'_n)_{I,J} = a_{n,I,J}$. Then the characteristic polynomials of M'_n and M_n coincide up to a power of x, and, for every simple y with $D_L(y) = J$ and every $d \geqslant 1$, we have*

$$b_{n,d}(y) = ((1, 1, \ldots, 1)\, M_n'^{d-1})_J. \tag{2.5}$$

Proof. Gathering the columns corresponding to simples with the same D_L set and summing the corresponding lines amounts to replacing M_n with a similar matrix of the form $\begin{pmatrix} M'_n & 0 \\ \cdots & 0 \end{pmatrix}$, so the result about the characteristic polynomial is clear.

As for the value of $b_{n,d}(y)$, the argument is similar to that for Lemma 2.6. The induction starts as $a_{n,I,[\![1,n-1]\!]} = 1$ holds for each I. For the general step, we find

$$\begin{aligned} b_{n,d}(y) &= \sum_{(x,y)\text{ normal}} b_{n,d-1}(x) = \sum_{D_R(x)\supseteq J} b_{n,d-1}(x) = \sum_I \sum_{\substack{D_R(x)\supseteq J\\ D_L(x)=I}} b_{n,d-1}(x) \\ &= \sum_I b'_{n,d-1}(I) a_{n,I,J} = \sum_I ((1,\ldots,1) M_n'^{\,d-2})_I (M'_n)_{I,J} = ((1,\ldots,1) M_n'^{\,d-1})_J, \end{aligned}$$

where $b'_{n,d}(I)$ denotes the common value of $b_{n,d}(x)$ for x with $D_L(x) = I$. $\square$

For $n = 3$, and using the enumeration $\emptyset$, $\{1\}$, $\{2\}$, $\{1, 2\}$ that is induced by our enumeration of simple braids, we obtain $M'_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$. Observe that the second and third columns in M'_3 coincide, which suggests a further reduction step.

3. Partitions associated with a simple braid

We can indeed reduce the size of the matrices once more: we can replace the adjacency matrix M'_n with a new matrix $\overline{M}_n$, whose size is $p(n)$, the number of partitions of n. Here the result is deduced from elementary remarks about simple braids (or, equivalently, about permutations); it can also be deduced from classical results about Solomon's algebra of descents—and therefore extends to all Artin–Tits groups of spherical type.

3.1. **Computation of $\widehat{a}_{n,I,J}$.** We shall start from an explicit determination of the value of the numbers $\widehat{a}_{n,I,J}$ in terms of the block compositions of I and J. We first recall the notions of composition and partition.

Definition 3.1. Assume $I \subseteq [\![1, n-1]\!]$. Let $p_1, \ldots, p_i$ be the increasing enumeration of $[\![1, n]\!] \setminus I$, completed with $p_0 := 0$. For $1 \leqslant j \leqslant k$, the interval $\{p_{j-1}+1, ..., p_j\}$ is called the jth *n-block* of I. The *n-composition* $[I]_n$ of I is defined to be the sequence of the sizes of the successive n-blocks of I. The *n-partition* $\{I\}_n$ of I is the non-increasing rearrangement of $[I]_n$.

Example 3.2. By definition, the n-blocks of I partition $[\![1, n]\!]$. For instance, consider $I := \{1, 2, 4, 5, 6, 9\}$ with $n := 10$. We find $[\![1, n]\!] \setminus I = \{3, 7, 8, 10\}$, so the successive 10-blocks of I are $\{1, 2, 3\}$, $\{4, 5, 6, 7\}$, $\{8\}$, and $\{9, 10\}$. Hence, the 10-composition of I is $(3, 4, 1, 2)$, while its 10-partition is $(4, 3, 2, 1)$. Note that the n-composition of I determines I, but its n-partition does not.

The geometric observation is the following one:

Lemma 3.3. *Assume $J \subseteq [\![1, n-1]\!]$, and let $(q_1, \ldots, q_\ell)$ be the n-composition of J. For x a simple n-braid, define $f_x : [\![1, n]\!] \to [\![1, \ell]\!]$ by $f_x(i) = j$ if the ith strand of x finishes in the jth n-block of J. Then $x \mapsto f_x$ establishes a bijection between the simple n-braids x that satisfy $D_R(x) \supseteq J$ and the functions from $[\![1, n]\!]$ to $[\![1, \ell]\!]$ that satisfy $\#f^{-1}(i) = q_i$ for each i. Moreover, for $D_R(x) \supseteq J$, we have, for every i,*

$$i \in D_L(x) \iff f_x(i) \geqslant f_x(i+1). \tag{3.1}$$

Proof. Assume that x is a simple n-braid satisfying $D_R(x) \supseteq J$, *i.e.*, that is right divisible by σ_j for each j in J. By hypothesis, the first n-block of J is $\{1, \ldots q_1\}$. Then x being right divisible by $\sigma_1, \ldots, \sigma_{q_1-1}$ is equivalent to its being right divisible by the left lcm of these elements, which is Δ_{q_1}. Similarly, the second n-block in J is $\{q_1+1, \ldots, q_1+q_2\}$, and being right divisible by $\sigma_{q_1+1}, ..., \sigma_{q_1+q_2-1}$ amounts to being right divisible by their left lcm, which is $\mathrm{sh}^{q_1}(\Delta_{q_2})$, where sh denotes the shift endomorphism of B_∞ that maps each σ_i to σ_{i+1}. Now, by construction, the sets $\{1, \ldots, q_1-1\}$ and $\{q_1+1 \ldots, q_1+q_2-1\}$ are separated by q_1, and, therefore, the corresponding σ's commute. In particular, Δ_{q_1} and $\mathrm{sh}^{q_1}(\Delta_{q_2})$ commute, and their left lcm is their product. Finally, a simple braid x satisfies $D_R(x) \supseteq J$ if and only if it is a right multiple of the element

$$\Delta_J = \Delta_{q_1}\, \mathrm{sh}^{q_1}(\Delta_{q_2})\, \ldots\, \mathrm{sh}^{q_1+\cdots+q_{\ell-1}}(\Delta_{q_\ell}),$$

i.e., we have $x = x'\Delta_J$ for some x'.

We claim that f_x determines x', hence x. Indeed, in a simple braid, any two strands cross at most once. Now, in a Δ-diagram, any two strands cross. So, if the ith and the i'th strands go to the same block of J, *i.e.*, if we have $f_x(i) = f_x(i')$, then these strands cross in the final Δ-part, and therefore they cannot cross in (any positive diagram representing) x'. So, when f_x is given, there is only one way to construct x', namely taking the strands to the entrance of the specified Δ-block in increasing order (Figure 2).

Consider now i, $1 \leqslant i < n$. We wonder whether σ_i is a left divisor of x, *i.e.*, if the ith and the $i+1$st strands cross in the diagram of x. If we have $f_x(i) = f_x(i+1)$, the ith and $i+1$st strand go to the same block of J, where they certainly cross. If we have $f_x(i) > f_x(i+1)$, then the ith strand goes to a block of J on the right of the block to which the $i+1$st strand goes, so they must cross in the x' part. On the contrary, for $f_x(i) < f_x(i+1)$, the strands cannot cross in the x' part—if they crossed once, they would have to cross a second time before exiting, and this is forbidden—and they do not cross in the Δ part either. So (3.1) holds. □

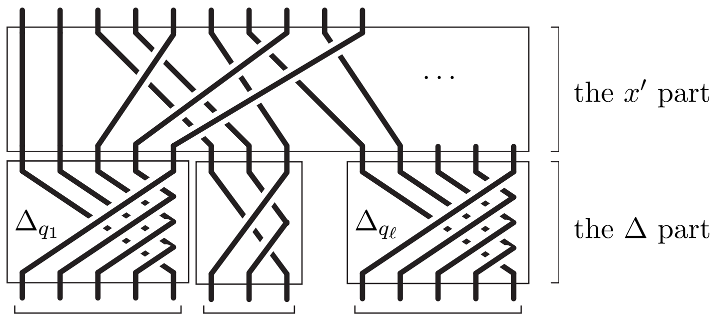

FIGURE 2. A simple braid divisible by all σ_j's with j in J can be represented by a diagram finishing with Δ's corresponding to the blocks of J; the strands going to the same block cannot cross in the x' part, as they cross inside the block; so the strands starting from i and i' with $i < i'$ cross if and only if they go to different blocks and i goes to a block on the right of the block i' goes to.

We deduce the following characterization of $\widehat{a}_{n,I,J}$:

Proposition 3.4. *Assume that I, J are subsets of $[\![1, n-1]\!]$ with respective n-compositions $(p_1, \ldots, p_k)$ and $(q_1, \ldots, q_\ell)$. Then $\widehat{a}_{n,I,J}$ is the number of $k \times \ell$ matrices with non-negative integer entries such that, for all i, j, the ith row has sum p_i and the jth column has sum q_j. In particular, we have*

$$\widehat{a}_{n,I,\emptyset} = \frac{n!}{p_1! \ldots p_k!} \quad \text{and} \quad \widehat{a}_{n,\emptyset,J} = \frac{n!}{q_1! \ldots q_\ell!}. \tag{3.2}$$

Proof. Lemma 3.3 immediately implies

$$a_{n,I,J} = \#\{f : [\![1,n]\!] \to [\![1,\ell]\!] \,;\, (\forall j)(\#f^{-1}(j) = q_j) \text{ and } (i \in I \Leftrightarrow f(i) \geqslant f(i+1))\}, \tag{3.3}$$

$$\widehat{a}_{n,I,J} = \#\{f : [\![1,n]\!] \to [\![1,\ell]\!] \,;\, (\forall j)(\#f^{-1}(j) = q_j) \text{ and } (i \in I \Rightarrow f(i) \geqslant f(i+1))\}. \tag{3.4}$$

Assume that f is a function of $[\![1, n]\!]$ to $[\![1, \ell]\!]$ satisfying the constraints of (3.4). Let A_f be the $k \times \ell$-matrix whose (i, j)-entry is the number of k's in the ith block of I satisfying $f(k) = q_j$. By construction, the sum of the ith row of A_f is the size p_i of the ith block of I, while the sum of the jth column is the number of k's satisfying $f(k) = j$, *i.e.*, it is q_j. We claim that A_f determines f. Indeed, (3.4) requires that f be non-increasing on each block of I, so there is only one possibility once the number of k's going to the various j is fixed.

The first equality in (3.2) follows: for $\ell = n$, there is exactly one nonzero entry in each column, so choosing a convenient matrix amounts to choosing among n elements the q_1 columns with a 1 in the first row, the q_2 columns with a 1 in the second row, *etc.* The second equality is similar with rows and columns exchanged. □

Corollary 3.5. (i) *The number* $\widehat{a}_{n,I,J}$ *only depends on the partitions* $\{I\}_n$ *and* $\{J\}_n$.

(ii) *For each* n *and* I, *the number* $a_{n,I,J}$ *only depends on the partition* $\{J\}_n$.

Proof. Point (i) directly follows from the characterization of Proposition 3.4, as the latter clearly involves the sizes of the blocks of I and J only. As for (ii), the usual inclusion-exclusion formula gives

$$a_{n,I,J} = \sum_{K\cap I=\emptyset} (-1)^{\#K} \widehat{a}_{n,I\cup K,J}.$$

By (i), each term in the sum only depends on $\{J\}_n$, and so does the sum. □

It is easy to check that the value of $a_{n,I,J}$ does not only depend on $\{I\}_n$ in general: when we apply the inclusion-exclusion formula, the sizes of the blocks in $I \cup K$ do not only depend on the sizes of the block in I.

Remark 3.6. Corollary 3.5 can also be deduced from classical results by Solomon about the descent algebra—and, therefore, it extends to all Artin–Tits groups of spherical type. The argument is as follows. For f a permutation, let $D(f)$ denote the sets of descents of f. In the group algebra $\mathbb{Q}[\mathfrak{S}_n]$, let $d_I := \sum\{f; D(f) = I\}$ and $e_J = \sum\{f; D(f)\cap J = \emptyset\}$. Using w_0 for the flip permutation, we have $w_0e_J = \sum\{f; D(f) \supseteq J\}$, and therefore $a_{n,I,J} = \langle d_I, w_0e_J\rangle$, where $\langle ., .\rangle$ is the inner product defined by $\langle f, g\rangle = 1$ for $g = f^{-1}$, and $= 0$ otherwise. Using the isometry result of [21], we deduce $a_{n,I,J} = \langle\theta(d_I), \theta(w_0e_J)\rangle$, where $\theta(e_K)$ denotes the character of $\mathfrak{S}_n$ induced by the trivial character of the standard parabolic subgroup generated by (the transpositions s_i with i in) K. By [25], the subspace of $\mathbb{Q}[\mathfrak{S}_n]$ generated by the e_K is a subalgebra, and the kernel of θ is generated by the elements $d_I - d_J$ with I, J associated with the same partition, and it follows from the above expression that $a_{n,I,J}$ only depends on the partition associated with J.

3.2. **The matrix $\overline{M}_n$.** We can now come back to the matrix M'_n, and replace it for the computation of the numbers $b_{n,d}$ with a new matrix of smaller size. Indeed, a direct application of Corollary 3.5 is

Lemma 3.7. *Assume that* J, J' *are subsets of* $[\![1, n-1]\!]$ *with the same* n*-partition. Then the* J*th and* J'*th columns of* M'_n *are equal.*

Thus the process used to replace M_n with M'_n can be applied again, *i.e.*, we form a new matrix by gathering the equal columns and summing the corresponding rows. The number $p(n)$ is bounded above by $(e^{\pi\sqrt{2/3}})^{\sqrt{n}}$, so the benefit is clear.

Definition 3.8. (i) For λ a partition (or a composition) of n, we denote by $\widetilde{\lambda}$ the unique subset I of $[\![1, n-1]\!]$ satisfying $[I]_n = \lambda$.

(ii) For $\lambda, \mu \vdash n$ (*i.e.*, partitions of n), we put

$$\overline{a}_{\lambda,\mu} = \sum_{\{I\}_n=\lambda} a_{n,I,\widetilde{\mu}} = \#\{x\,;\,\{D_L(x)\}_n = \lambda \text{ and } D_R(x) \supseteq \widetilde{\mu}\},$$

and we let $\overline{M}_n$ be the matrix with rows and columns indexed by partitions of n and whose (λ, μ)-entry is $\overline{a}_{\lambda,\mu}$.

In this way the size of the matrix has been reduced from $n!$ to $p(n)$, the number of partitions of n. For instance, enumerating partitions in the order induced by the previous order on $\mathfrak{P}([\![1,n]\!])$, we obtain

$$\overline{M}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad \overline{M}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 11 & 4 & 1 & 0 & 0 \\ 5 & 3 & 2 & 1 & 0 \\ 6 & 4 & 2 & 2 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad \overline{M}_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 26 & 8 & 0 & 2 & 0 & 0 & 0 \\ 23 & 12 & 4 & 5 & 0 & 1 & 0 \\ 43 & 21 & 5 & 10 & 0 & 2 & 0 \\ 8 & 6 & 4 & 4 & 2 & 2 & 0 \\ 18 & 12 & 6 & 8 & 2 & 4 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Applying the same argument as for Lemma 2.12, we obtain:

Proposition 3.9. *For $n \geqslant 1$, the characteristic polynomials of $\overline{M}_n$ and M_n coincide up to a power of x, and, for every simple n-braid x, we have for each d*

$$b_{n,d}(x) = ((1,1,\ldots,1)\,\overline{M}_n^{d-1})_\lambda, \tag{3.5}$$

where λ is the n-partition of $D_L(x)$. In particular we have

$$b_{n,d} = ((1,1,\ldots,1)\,\overline{M}_n^{d})_{(1,1,\ldots,1)}. \tag{3.6}$$

Table 1 gives the first few values deduced from the above formulas.

d	1	2	3	4	5	6
$b_{2,d}(1)$	1	2	3	4	5	6
$b_{3,d}(1)$	1	6	19	48	109	234
$b_{3,d}(\Delta_2)$	1	3	7	15	31	63
$b_{4,d}(1)$	1	24	211	1 380	8 077	45 252
$b_{4,d}(\Delta_2)$	1	12	83	492	2 765	15 240
$b_{4,d}(\Delta_3)$	1	4	15	64	309	1 600
$b_{5,d}(1)$	1	120	3 651	79 140	1 548 701	29 375 460
$b_{5,d}(\Delta_2)$	1	60	1 501	30 540	585 811	11 044 080
$b_{5,d}(\Delta_3)$	1	20	311	5 260	94 881	1 755 360
$b_{4,d}(\Delta_4)$	1	5	31	325	4 931	86 565
$b_{6,d}(1)$	1	720	90 921	7 952 040	634 472 921	49 477 263 360
$b_{6,d}(\Delta_2)$	1	360	38 559	3 228 300	254 718 389	19 808 530 620
$b_{6,d}(\Delta_3)$	1	120	8 727	649 260	49 654 757	3 831 626 580
$b_{6,d}(\Delta_4)$	1	30	1 075	61 620	4 387 195	332 578 230
$b_{6,d}(\Delta_5)$	1	6	63	1 955	116 423	8 448 606

TABLE 1. First values of $b_{n,d}(\Delta_r)$ for $1 \leqslant r < n$; the values of $b_{n,d}$ can be also read, as Proposition 1.9 gives $b_{n,d} = b_{n,d+1}(1)$, so, for instance, we find $b_{3,3} = 48$, and $b_{4,5} = 45\,252$.

3.3. **Small values of n.** For small values of n, it is easy to complete the computations and to obtain an explicit form for the expansion of $b_{n,d}(x)$ as announced in Proposition 2.9.

Example 3.10. Assume $n = 3$. The matrix $\overline{M}_3$ is invertible with eigenvalues 1 (double) and 2. By solving the recurrences, we find

$$b_{3,d}(x) = \begin{cases} 4 \cdot 2^d - 3d - 4 & \text{for } x \text{ with partition } (1,1,1), \textit{ i.e.}, x = 1 \\ 2^d - 1, & \text{for } x \text{ with partition } (2,1), \textit{ i.e.}, x = \sigma_1, \sigma_2, \sigma_2\sigma_1, \text{ or } \sigma_1\sigma_2, \\ 1 & \text{for } x \text{ with partition } (3), \textit{ i.e.}, x = \Delta_3, \end{cases}$$

and we deduce $b_{3,d} = 8 \cdot 2^d - 3d - 7$.

Example 3.11. Assume now $n = 4$. The matrix $\overline{M}_4$ admits 4 eigenvalues, namely those of $\overline{M}_3$, plus $\rho_1 = 3+\sqrt{6}$ and $\rho_2 = 3-\sqrt{6}$. Solving the recurrences yields for $b_{n,d}(x)$ with associated partition as indicated

$$\begin{array}{llllllll} (1,1,1,1): & \frac{1}{20}(18+7\sqrt{6})\,\rho_1^d & + & \frac{1}{20}(18-7\sqrt{6})\,\rho_2^d & - & \frac{256}{5}\cdot 2^d & + & 6k+11, \\ (2,1,1): & \frac{1}{60}(18+7\sqrt{6})\,\rho_1^d & + & \frac{1}{60}(18-7\sqrt{6})\,\rho_2^d & - & \frac{8}{5}\cdot 2^d & + & 1, \\ (2,2): & \frac{1}{12}(\sqrt{6})\quad\rho_1^d & - & \frac{1}{12}(\sqrt{6})\quad\rho_2^d, & & & & \\ (3,1): & \frac{1}{60}(6-\sqrt{6})\quad\rho_1^d & + & \frac{1}{60}(6+\sqrt{6})\quad\rho_2^d & + & \frac{4}{5}\cdot 2^d & - & 1, \end{array}$$

and 1 for associated partition (4), *i.e.*, for $x = \Delta_4$. As the characteristic polynomial of $\overline{M}_4$ is $(x^2 - 6x + 3)(x - 2)(x - 1)^2$, we can equivalently determine $b_{4,d}(x)$ and $b_{4,d}$ by inductions on d of the form

$$u_d = 6u_{d-1} - 3u_{d-2} + \alpha 2^d + \beta d + \gamma \tag{3.7}$$

where α, β, γ are determined using special values of u_d. For instance, $b_{4,d}$ is determined by (3.7) with $\alpha = 32$, $\beta = -12$, $\gamma = -34$ and the values $u_{-1} = 0$, $u_0 = 1$. Generating functions can be deduced easily.

3.4. **Eigenvalues of M_n.** By Proposition 2.9, the value of $b_{n,d}$ and $b_{n,d}(x)$, and in particular its asymptotic behaviour when d grows to infinity, are connected with the non-zero eigenvalues of M_n, which, by Proposition 3.9, coincide with those of $\overline{M}_n$. The characteristic polynomial of $\overline{M}_n$—hence of M_n up to an x^d factor—for small values of n is displayed in Table 2.

These values support the following

Conjecture 3.12. *For each n, the characteristic polynomial of M_{n-1} divides that of M_n. More precisely, the sprectrum of $\overline{M}_n$ is the spectrum of $\overline{M}_{n-1}$, plus $p(n) - p(n-1)$ simple non-zero eigenvalues.*

It is not hard to check the above statement for $n \leqslant 10$. Specifically, let $\widehat{M}_n$ be the size $p(n) - 2$ matrix obtained from $\overline{M}_n$ by deleting the first and the last rows and columns. For each small value of n, one can directly check that $\widehat{M}_n$ is similar to a matrix of the form $\begin{pmatrix} \widehat{M}_{n-1} & 0 \\ \cdots & \cdots \end{pmatrix}$, and deduce the properties asserted in Conjecture 3.12. But no generic argument is known so far.

The growth rate of the numbers $b_{n,d}(x)$ is connected with the largest eigenvalue $\rho_{max}(M_n)$ of M_n. For $n \leqslant 6$, all $b_{n,d}(x)$ except $b_{n,d}(\Delta_n)$, which is 1, and therefore all $b_{n,d}$ as well, grow like $\rho_{max}(M_n)^d$.

$$
\begin{aligned}
&P_{\overline{M}_1}(x) = x - 1\\
&P_{\overline{M}_2}(x) = P_{\overline{M}_1}(x)\cdot(x-1)\\
&P_{\overline{M}_3}(x) = P_{\overline{M}_2}(x)\cdot(x-2)\\
&P_{\overline{M}_4}(x) = P_{\overline{M}_3}(x)\cdot(x^2-6x+3)\\
&P_{\overline{M}_5}(x) = P_{\overline{M}_4}(x)\cdot(x^2-20x+24)\\
&P_{\overline{M}_6}(x) = P_{\overline{M}_5}(x)\cdot(x^4-82x^3+359x^2-260x+60)\\
&P_{\overline{M}_7}(x) = P_{\overline{M}_6}(x)\cdot(x^4-390x^3+6024x^2-13680x+8640)\\
&P_{\overline{M}_8}(x) = P_{\overline{M}_7}(x)\cdot(x^7-2134x^6+139976x^5-1321214x^4+3780975x^3\\
&\qquad\qquad -3305160x^2+1341900x-226800)
\end{aligned}
$$

n	1	2	3	4	5	6	7	8
$\rho_{max}(M_n)$	1	1	2	5.449	18.717	77.405	373.990	2066.575
$\dfrac{\rho_{max}(M_n)}{n\cdot\rho_{max}(M_{n-1})}$	-	0.5	0.667	0.681	0.687	0.689	0.690	0.691

Table 2. Characteristic polynomial of $\overline{M}_n$ for $n \leqslant 8$, and the corresponding largest eigenvalue—which is to be compared with $n!$, the growth rate for the number of n-braids of degree at most d if all sequences were normal.

Question 3.13. *Do all $b_{n,d}(x)$ except $b_{n,d}(\Delta_n)$ grow like $\rho_{max}(M_n)^d$?*

Question 3.14. *What is the asymptotic behaviour of $\rho_{max}(M_n)$ with n?*

The trivial upper bound of (1.4) suggests to compare $\rho_{max}(M_n)$ with $n!$, or, rather, $\rho_{max}(M_n)$ with $n\cdot\rho_{max}(M_{n-1})$. The values listed in Table 2 may suggest that the ratio have a definite limit.

4. Letting the braid index vary

So far, we kept the braid index n fixed, and studied how the numbers $b_{n,d}$ or $b_{n,d}(x)$ vary with d, thus letting linear inductions appear. Quite different induction schemes appear when we fix the degree and let the braid index vary. No systematic method is known so far, and we only mention a few partial results motivated by the approach of [13].

4.1. **The numbers $b_{n,2}$.** Very little is known about $b_{n,d}$ in general. The case $d = 1$ is trivial, as we already observed the equality

$$b_{n,1} = n!.$$

For $d = 2$, the value can be deduced from earlier results of [6, 7] about permutations. We shall use the following very general observation about duality in Garside groups:

Lemma 4.1. *For x in Δ_n, let ${}^*x$ and x^* be defined by ${}^*x\,x = x\,x^* = \Delta_n$. Then $x \mapsto {}^*x$ and $x \mapsto x^*$ are permutations of $D_L(\Delta_n)$, and, for each simple x, we have*

$$D_R({}^*x) = [\![1,n]\!] \setminus D_L(x) \quad \textit{and} \quad D_L(x^*) = [\![1,n]\!] \setminus D_R(x). \tag{4.1}$$

Proof. Assume $x \in D_L(\Delta_n)$. Then, by hypothesis, x is a left and a right divisor of Δ_n, hence ${}^*x$ and x^* are positive braids, and they are divisors of Δ_n in B_n^+, so they are simple. That the mappings $x \mapsto {}^*x$ and $x \mapsto x^*$ are injective is clear, and the surjectivity follows from the finiteness of $D_L(\Delta_n)$.

Now, σ_i being a right divisor of ${}^*x$ is equivalent to ${}^*x\sigma_i$ not being simple, hence to the non-existence of y satisfying ${}^*x\sigma_i y = \Delta_n$, and finally to the non-existence of y satisfying $x = \sigma_i y$. This implies the first equality in (4.1). The second equality follows from a symmetric argument. □

Proposition 4.2. *The numbers $b_{n,2}$ are determined by the induction*

$$b_{0,2} = 1, \qquad b_{n,2} = \sum_{i=0}^{n-1} (-)^{n+i+1} \binom{n}{i}^2 b_{i,2}. \tag{4.2}$$

Their double exponential generating function is

$$\sum_{n=0}^{\infty} b_{n,2} \frac{x^n}{n!^2} = \left(\sum_{n=0}^{\infty} (-1)^n \frac{x^n}{n!^2} \right)^{-1} = \frac{1}{J_0(\sqrt{x})}, \tag{4.3}$$

where $J_0(x)$ is the Bessel function.

Proof. By definition, $b_{n,2}$ is the number of pairs of simple n-braids (x_1, x_2) satisfying $D_R(x_1) \supseteq D_L(x_2)$, *i.e.*, by Lemma 4.1, $D_R(x_1) \cap D_R({}^*x_2) = \emptyset$. By Lemma 1.6, this number is also the number of pairs of permutations (f, g) in $\mathfrak{S}_n$ with no descent in common, *i.e.*, such that there exists no i satisfying both $f(i) > f(i+1)$ and $g(i) > g(i+1)$. Such pairs of permutations have been counted in [6, 7] (see also [24]), with the result indicated above. □

4.2. **The numbers $b_{n,2}(\Delta_{n-r})$.** Specific results appear when we consider the numbers $b_{n,d}(x)$ with x of the form Δ_{n-r} with $1 \leqslant r \leqslant n$. In particular, we can complete the computation when r is fixed and d is small. We obviously have $b_{n,1}(\Delta_{n-r}) = 1$ for $1 \leqslant r \leqslant n$, so the first case to consider is $d = 2$. The general principle that makes the computation of $b_{n,d}(\Delta_{n-r})$ relatively easy is the following observation:

Lemma 4.3. *For all n, d, r, we have*

$$b_{n,d}(\Delta_{n-r}) = \sum_{x \text{ right divisible by } \Delta_{n-r}} b_{n,d-1}(x). \tag{4.4}$$

Proof. The argument is similar to that for Proposition 1.9. A sequence $(x_1, \dots, x_{d-1}, \Delta_{n-r})$ is normal if and only if both $(x_1, \dots, x_{d-1})$ and (x_{d-1}, Δ_{n-r}) are normal. Now (x_{d-1}, Δ_{n-r}) is normal if and only if every σ_i dividing Δ_{n-r} on the left divides x_{d-1} on the right. The σ_i's dividing Δ_{n-r} on the left are $\sigma_1, \dots, \sigma_{n-r-1}$. The simple braids that are right divisible by $\sigma_1, \dots, \sigma_{n-r-1}$ are those right divisible by Δ_{n-r}. Then (4.4) follows. □

Proposition 4.4. *For $1 \leqslant r \leqslant n$, we have*

$$b_{n,2}(\Delta_{n-r}) = \frac{n!}{(n-r)!}. \tag{4.5}$$

Proof. By Lemma 4.3, $b_{n,2}(\Delta_{n-r})$ is the number of simple n-braids x that are right divisible by Δ_{n-r}, *i.e.*., that satisfy $D_R(x) \supseteq [\![1, n-r]\!]$. The n-composition of $[\![1, n-r]\!]$ in n is $(n-r, 1, \dots, 1)$, so (3.2) directly gives (4.5). □

4.3. **The numbers $b_{n,3}(\Delta_{n-r})$.** Things become more interesting for $d = 3$.

Proposition 4.5. *For $1 \leqslant r \leqslant n$, there exist polynomials $P_1, \ldots, P_{n-r}$ with integer coefficients and P_i of degree at most $n - r - i + 1$ such that, for every n, we have*

$$b_{n,3}(\Delta_{n-r}) = (n-r)!\,(n-r+1)^n + \sum_{i=1}^{n-r} P_i(n)\, i^{r+i-1}. \tag{4.6}$$

The explicit values for $r = 1, 2$ are

$$b_{n,3}(\Delta_{n-1}) = 2^{n-1}, \tag{4.7}$$

$$b_{n,3}(\Delta_{n-2}) = 2 \cdot 3^n - (n+6) \cdot 2^{n-1} + 1. \tag{4.8}$$

Proof. We begin with (4.7). By Lemma 4.3, $b_{n,3}(\Delta_{n-1})$ is the sum of all $b_{n,2}(x)$ with x right divisible by Δ_{n-1}, *i.e.*, it is the number of normal sequences (x_1, x_2) such that x_2 is right divisible by Δ_{n-1}. Let S be the set of all such normal sequences. We partition S according to the value of $D_L(x_2)$, *i.e.*, for each subset I of $[\![1, n-1]\!]$, we count how many pairs (x_1, x_2) satisfy $D_L(x_2) = I$. So assume that x_2 is right divisible by Δ_{n-1}. Two cases are possible. Either x_2 is right divisible by (hence equal to) Δ_n, and then we have $D_L(x_2) = [\![1, n-1]\!]$. Or x_2 is not divisible by Δ_{n-1}, and then Lemma 3.3 shows that x_2 must be $\sigma_{i,n}\Delta_{n-1}$ for some i with $2 \leqslant i \leqslant n$, so that the n-composition of $D_L(x_2)$ is $(i-1, n-i+1)$. So the possible compositions for the set $D_L(x_2)$ are (n), and $(p, n-p)$ with $1 \leqslant p \leqslant n-1$. Conversely, the previous analysis shows that, for each I of the previous form, there exists exactly one possible x_2. Now, Proposition 3.4 says that there is one choice for x_1 in the case of (n)—namely $x_1 = \Delta_n$—and $\binom{n}{p}$ choices for x_1 in the case of $(p, n-p)$. We deduce

$$b_{n,3}(\Delta_{n-1}) = 1 + \sum_{p=1}^{n-1} \binom{n}{p} = 2^{n-1}.$$

The method is similar for computing $b_{n,3}(\Delta_{n-2})$ in (4.8). Assume that (x_1, x_2) is a normal sequence with x_2 right divisible by Δ_{n-2}. The hypothesis is $D_R(x_2) \supseteq [\![1, n-3]\!]$, so three cases may occur, namely $D_R(x_2) \supseteq [\![1, n-2]\!]$, $D_R(x_2) = [\![1, n-3]\!]$, and $D_R(x_2) = [\![1, n-3]\!] \cup \{n-1\}$. The first case was analysed above. In the second case, $D_L(x_2)$ has three blocks, and, conversely, each set I with three blocks gives exactly one eligible x_2. In the third case, $D_L(x_2)$ has either two blocks, or it has three blocks with the middle one of size at least 2; conversely, each set I of the previous form gives one eligible x_2. Using as above Proposition 3.4 to count the eligible x_1's for each possible I, we obtain that $b_{n,3}(\Delta_{n-2})$ is

$$b_{n,3}(\Delta_{n-1}) + \sum_{\substack{p_1+p_2+p_3=n\\ p_1,p_2,p_3\geqslant 1}} \frac{n!}{p_1!p_2!p_3!} + \sum_{\substack{p_1+p_2=n\\ p_1,p_2\geqslant 1}} \frac{n!}{p_1!p_2!} + \sum_{\substack{p_1+p_2+p_3=n\\ p_1,p_3\geqslant 1, p_2\geqslant 2}} \frac{n!}{p_1!p_2!p_3!}. \tag{4.9}$$

Using the fact that 3^n is the sum of all $\frac{n!}{p_1!p_2!p_3!}$ with $p_1 + p_2 + p_3 = n$, one deduces (4.8) by bookkeeping.

Applying the same method in the general case leads to (4.6). Indeed, always by Lemma 3.3, specifying a simple n-braid x_2 satisfying $D_R(x_2) \supseteq [\![1, r-1]\!]$ amounts to choosing a permutation of the $n-r$ last strands and the $n-r$ positions $(i_1, \ldots, i_{n-r})$

where these strands start from. In the generic case, the resulting set $D_L(x_2)$ is $\{i_1 - 1, \dots, i_{n-r} - 1\}$, whose composition consists of $n-r$ blocks. The special cases are when at least two adjacent strands among the last $n-r$ ones start from adjacent positions; according to whether these strands cross or not in the final part, one then obtains either a composition with a block of size 2 at least, or a composition with less than $n-r$ blocks. Conversely, for every subset I of $[\![1, n-1]\!]$ with $n-r$ blocks, there exists in general $(n-r)!$ eligible x_2's, one for each choice of the final permutation of the last $n-r$ strands. There may be less than $(n-r)!$ choices for x_2 when 1 occurs in the composition of I. Also, subsets of $[\![1, n-1]\!]$ with fewer than $n-r$ blocks may lead to eligible x_2's. Multiplying by the number of eligibles x_1's for each I and summing up yields an expression similar to (4.9), involving $(n-r)!$ sums of the form $\sum_{p_1+\dots+p_{n-r+1}=n} \frac{n!}{p_1!\dots p_{n-r+1}!}$ with possible order constraints on $p_1, \dots, p_{n-r+1}$. Each of them leads to a factor $(n-r+1)^n$, plus additional factors corresponding to specializing arguments to 0 or 1 or to grouping them. □

4.4. **The numbers $b_{n,4}(\Delta_{n-1})$.** For $d = 4$, it seems hopeless to complete the computation of $b_{n,d}(\Delta_{n-r})$. However, this can be done for $r = 1$. The remarkable point is that still another induction scheme appears.

Proposition 4.6. *For $n \geqslant 1$, we have*

$$b_{n,4}(\Delta_{n-1}) = \sum_{i=0}^{n-1} \frac{n!}{i!}. \tag{4.10}$$

Proof. According to Lemma 4.3 again, we have now to count the normal sequences (x_1, x_2, x_3) with x_3 of the form $\sigma_{i,n}\Delta_{n-1}$, $2 \leqslant i \leqslant n$. We partition the family according to the value I of $D_L(x_2)$, and count how many sequences may correspond to a given I. Let $(p_1, \dots, p_k)$ denote the n-composition of I.

Let us first consider the case $I = [\![1, n-1]\!]$. Then we must have $x_2 = \Delta_n$, hence $x_1 = \Delta_n$ as well. There are n possible choices for x_3, and the total number of corresponding sequences (x_1, x_2, x_3) is n.

We assume now $I \neq [\![1, n-1]\!]$, *i.e.*, $k \geqslant 2$. As for x_1, Proposition 3.4 directly gives the number of choices, namely $\frac{n!}{p_1!\dots p_k!}$. So we are left with counting how many pairs (x_2, x_3) are eligible. The case $x_3 = \Delta_n$ is excluded since it implies $x_2 = \Delta_n$ hence $I = [\![1, n-1]\!]$. As in the case of $b_{n,3}(\Delta_{n-1})$, the hypothesis that x_3 is $\sigma_{i,n}\Delta_{n-1}$ for some i with $2 \leqslant i \leqslant n$ implies that the n-composition of $D_L(x_3)$ consists of two nonempty blocks, and, conversely, each partition of $[\![1, n]\!]$ into two nonempty blocks gives a unique x_3 of the convenient form. So the number of pairs (x_2, x_3) associated with I is the number of x_2's satisfying $D_L(x_2) = I$ and such that $D_R(x_2)$ has two blocks.

By (3.3), this number is the number of functions f of $[\![1, n]\!]$ to $\{1, 2\}$ such that $f(i) < f(i+1)$ holds exactly for $i \notin I$. As only two values are possible, this condition means that we have $f(i) = 1$ and $f(i+1) = 2$ for $i \notin I$, and $f(i+1) \leqslant f(i)$ for $i \in I$. Consider the blocks of I. In each block, except possibly the first and the last ones, the value of f has to be 2 on the first element, and to be 1 on the last element. Inbetween, f is non-increasing. So the values consist of a series of 2's, followed by a series of 1's. The only parameter to specify is the position where f switches from 2 to 1, so, for a block of size p, there are $p-1$ possible choices (see Figure 3). The cases of the first and the last blocks are special, because there is no constraint on the left for the first block, and on the right for the last block. So, in these special cases, there are p choices instead of $p-1$. The conclusion is that, for I with n-composition $(p_1, \dots, p_k)$, there are $p_1(p_2-1)\dots(p_{k-1}-1)p_k$ choices for the pairs (x_2, x_3) associated with I. Merging the result for x_1 and for (x_2, x_3) and summing up over I gives

$$b_{n,4}(\Delta_{n-1}) = \sum \frac{n!}{p_1! \dots p_k!} \, p_1(p_2-1)\dots(p_{k-1}-1)p_k. \tag{4.11}$$

the sum being taken over all n-compositions $(p_1, \dots, p_k)$: indeed, the value for $[\![1, n-1]\!]$, namely n, corresponds to the missing term $\frac{n!}{n!}n$ of the sum.

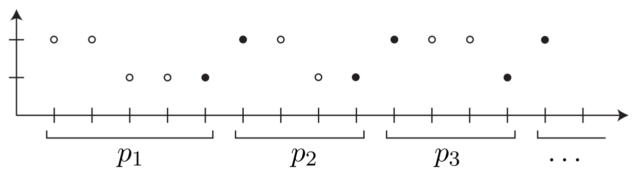

FIGURE 3. Proof of (4.11): the rises are fixed, so it just remains to choose the position of the fall in each block of I, whence $p-1$ choices for a size p block except the first and the last ones.

We can now simplify the right hand term in (4.11). To this end, we observe that

$$\sum_{\substack{p_1+\dots+p_k=i+1\\ p_1,\dots,p_k\geqslant 1}} \frac{p_1-1}{p_1!} \dots \frac{p_{r-1}-1}{p_{r-1}!} \, \frac{p_k}{p_k!} = 1 \tag{4.12}$$

holds for $i \geqslant 0$. Indeed, let $F(i)$ be the left hand side of (4.12). We prove (4.12) using induction on i. For $i = 0$, we get $1 = 1$. Assume $i \geqslant 1$ and consider the sequences $(p_1, \dots, p_k)$ satisfying $p_1 + \dots + p_k = i+1$. On the one hand, we have $(i+1)$, whose contribution to $F(i)$ is $\frac{1}{i!}$. On the other hand, we have the sequences of length at least 2. Now, for each p with $1 \leqslant p \leqslant i$, the contribution of $(p, p_2, \dots, p_k)$ to $F(i)$ is $\frac{p-1}{p!}$ times the contribution of $(p_2, \dots, p_k)$ to $F(i-p)$. Hence the total contribution of the sequences beginning with p to $F(i)$ is $\frac{p-1}{p!}\,F(i-p)$, so, by induction hypothesis, it is $\frac{(p-1)}{p!}$. We deduce $F(i) = \frac{0}{1!} + \frac{1}{2!} + \dots + \frac{i-1}{i!} + \frac{1}{i!}$, which is clearly 1.

Consider now the right hand side in (4.11). For $0 \leqslant i < n-1$, the contribution of $(i+1, p_2, \dots, p_k)$ to the sum is $\frac{n!}{i!}$ times the quantity $\frac{p_1-1}{p_1!}\,\frac{p_{k_1}-1}{p_{k-1}!}\,\frac{p_k}{p_k!}$ involved in (4.12). Using the latter equality, we deduce that the total contribution of the sequences beginning with $i+1$ is $\frac{n!}{i!}$. As for $i = n-1$, the contribution of (n) to the right hand side in (4.11) is n, which is $\frac{n!}{(n-1)!}$, so the general formula remains valid. By summing over i, we obtain (4.10). □

Corollary 4.7. *The numbers $b_{n,4}(\Delta_{n-1})$ are determined by the induction*

$$u_1 = 1, \qquad u_n = nu_{n-1} + 2n - 1.$$

Another consequence of (4.10) is the equality

$$b_{n,4}(\Delta_{n-1}) = \lfloor n!e \rfloor - 1,$$

with $e = \exp(1)$.

References

[1] S.I. Adyan, *Fragments of the word Delta in a braid group*, Mat. Zam. Acad. Sci. SSSR **36-1** (1984) 25–34; translated Math. Notes of the Acad. Sci. USSR; 36-1 (1984) 505–510.
[2] D. Bessis, *The dual braid monoid*, An. Sci. Ec. Norm. Sup.; 36; 2003; 647–683.
[3] J. Birman, *Braids, links, and mapping class groups*, Annals of Math. Studies 82, Princeton Univ. Press (1975).
[4] J. Birman, K.H. Ko & S.J. Lee, *A new approach to the word problem in the braid groups*, Advances in Math. **139-2** (1998) 322-353.
[5] A. Bronfman, *Growth function of a class of monoids*, Preprint (2001).
[6] L. Carlitz, R. Scoville & T. Vaughan, *Enumeration of pairs of permutations and sequences*, Bull. Amer. Math. Soc. **80** (1974) 881–884.
[7] L. Carlitz, R. Scoville & T. Vaughan, *Enumeration of pairs of permutations*, Discrete Math. **14** (1976) 215–239.
[8] R. Charney, *Artin groups of finite type are biautomatic*, Math. Ann. **292-4** (1992) 671–683.
[9] R. Charney, *Geodesic automation and growth functions for Artin groups of finite type*, Math. Ann. **301-2** (1995) 307–324.
[10] C.R. Cromwell & S. Humphries, *Counting fundamental paths in* 2*-generator Artin semigroups*, Preprint (2004).
[11] P. Dehornoy, *Groupes de Garside*, Ann. Scient. Ec. Norm. Sup. **35** (2002) 267–306.
[12] P. Dehornoy, I. Dynnikov, D. Rolfsen, B. Wiest, *Why are braids orderable?*, Panoramas & Synthèses vol. 14, Soc. Math. France (2002).
[13] P. Dehornoy, *Still another approach to the braid ordering*, Pacific J. Math., to appear; arXiv: math.GR/0506495.
[14] P. Dehornoy & L. Paris, *Gaussian groups and Garside groups, two generalizations of Artin groups*, Proc. London Math. Soc. **79-3** (1999) 569–604.
[15] P. Deligne, *Les immeubles des groupes de tresses généralisés*, Invent. Math. **17** (1972) 273–302.
[16] E.A. Elrifai & H.R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford **45-2** (1994) 479–497.
[17] D. Epstein, J. Cannon, D. Holt, S. Levy, M. Paterson & W. Thurston, *Word Processing in Groups*, Jones & Bartlett Publ. (1992).
[18] D. Epstein, A. Iano-Fletscher, & U. Zwick, *Growth functions and automatic groups*, Experiment. Math **5** (1996) 297–315.
[19] F.A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20-78** (1969) 235–254.
[20] V. Gebhardt, *A new approach to the conjugacy problem in Garside groups*, J. of Algebra **292-1** (2005) 282–302.
[21] C. Hohlweg, *Properties of the Solomon algebra homomorphism*, arXiv: math.RT/0302309.
[22] K.H. Ko, S. Lee, J.H. Cheon, J.W. Han, J. Kang, C. Park, *New public-key cryptosystem using braid groups*, Crypto 2000, 166–184.
[23] J. Mc Cammond, *An introduction to Garside structures*, Preprint (2005).
[24] J. Riordan, *Inverse relations and combinatorial identities*, Amer. Math. Monthly **71** (1964) 485–498.
[25] L. Solomon, *A Mackey formula in the group ring of a Coxeter group*, J. Algebra **41** (1976) 255–268.
[26] P. Xu, *Growth of the positive braid groups*, J. Pure Appl. Algebra **80** (1992) 197–215.

Laboratoire de Mathématiques Nicolas Oresme UMR 6139, Université de Caen, 14032 Caen, France

E-mail address: dehornoy@math.unicaen.fr

URL: //www.math.unicaen.fr/~dehornoy