



HAL
open science

Number of right ideals and a q -analogue of indecomposable permutations

Roland Bacher, Christophe Reutenauer

► **To cite this version:**

Roland Bacher, Christophe Reutenauer. Number of right ideals and a q -analogue of indecomposable permutations. Canadian Journal of Mathematics, 2016, 68, pp.481-503. 10.4153/cjm-2016-004-8 . hal-01223143

HAL Id: hal-01223143

<https://hal.science/hal-01223143v1>

Submitted on 2 Nov 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

NUMBER OF RIGHT IDEALS AND A q -ANALOGUE OF
INDECOMPOSABLE PERMUTATIONS

ROLAND BACHER AND CHRISTOPHE REUTENAUER

Abstract. We prove that the number of right ideals of codimension n in the algebra of noncommutative Laurent polynomials in two variables over the finite field \mathbb{F}_q is equal to $(q-1)^{n+1}q^{\frac{(n+1)(n-2)}{2}} \sum_{\theta} q^{\text{inv}(\theta)}$, where the sum is over all indecomposable permutations in S_{n+1} and where $\text{inv}(\theta)$ stands for the number of inversions of θ .

Mathematics Subject Classification Numbers: Primary: 05A15, Secondary: 05A19

1. INTRODUCTION

Indecomposable permutations and subgroups of finite index of the free group F_2 are equinumerous. More precisely, the latter number was computed by Hall [H] and the former by Comtet [Cm], and it turns out that the number of subgroups of index n is equal to the number of indecomposable permutations in S_{n+1} . To our best knowledge, this was first noticed by Dress and Franz [DF1] who gave a bijective proof. Sillke [Si], Ossona de Mendez and Rosenstiehl [OR], and Cori [Cr] discovered more bijections. We give a further bijection based on a natural correspondence between subgroups of finite index and regular right congruences of free monoids during the proof of our main result, Theorem 3.

Note that subgroups of the free group F_2 are also naturally in bijection with rooted hypermaps, see [Cr]. Indecomposable permutations appear also in the study of planar maps, see [B]. Furthermore, they form a free generating set of the bialgebra of permutations, which is therefore a free associative algebra [PR] and they index a basis of its primitive elements [AS]. More elementary is the folklore result that the disjoint union of all permutations groups is a free monoid under shifted concatenation, freely generated by the set of indecomposable permutations (a proof may be found in [P]). This yields a generating function (see [C]) allowing to count indecomposable permutations easily.

Our main result is a linear version of the bijections mentioned above: We consider the polynomial $P_{n+1}(q) = \sum_{\theta \in \text{Indec}_{n+1}} q^{\text{inv}(\theta)}$ enumerating indecomposable permutations by inversions. We show that this polynomial, corrected by the factor $(q-1)^{n+1} q^{\frac{(n+1)(n-2)}{2}}$, enumerates right ideals of finite index n in the group algebra of the free group $\langle a, b \rangle$ on two generators over the finite field \mathbb{F}_q (Theorem 1).

A key ingredient of our proof is a particular case of a result due to Haglund [H]: The number of invertible matrices over \mathbb{F}_q with support included in a fixed partition is given by a polynomial which counts, essentially by inversions, the number of permutation-matrices with the same support property. These polynomials are rook polynomials [GR]: They count the number of nonattacking positions of rooks on a chess board.

A last ingredient of the proof is a study of prefix-free sets and prefix-closed sets with respect to the alphabetical order in the free monoid $\{a, b\}^*$ (or equivalently in binary trees). In particular, our Lemma 3, a somewhat technical formula linking different parameters, seems to be new.

This article is a sequel to [BR], where we have shown that the number of right ideals of index n of the free associative algebra on two generators over \mathbb{F}_q is a classical q -analogue of Catalan numbers, a result which was already implicit in Reineke's article [R]. We use here several results of our previous paper: A description by prefix-free and prefix-closed sets of right ideals in the free associative algebra, based on the fact that this algebra is a fir (free ideal ring), in the sense of Cohn [C], together with a noncommutative version of Buchberger's algorithm for the construction of Gröbner bases.

Acknowledgments: A discussion with Alejandro Morales helped the second author to understand Haglund's theorem and rook polynomials, together with the variant given by him and his co-authors in [BIMPSZ].

2. MAIN RESULT

A permutation $\sigma \in S_n$ of the set $\{1, \dots, n\}$ is *decomposable* if $\sigma(\{1, \dots, i\}) = \{1, \dots, i\}$ (and $\sigma(\{i+1, \dots, n\}) = \{i+1, \dots, n\}$) for some i in $\{1, \dots, n-1\}$. A permutation σ is *indecomposable* otherwise, ie. if $\sigma(\{1, \dots, i\}) \neq \{1, \dots, i\}$ for all i in $\{1, 2, \dots, n-1\}$.

An *inversion* of a permutation $\sigma \in S_n$ is a pair of distinct integers i, j with $1 \leq i < j \leq n$ such that $\sigma(i) > \sigma(j)$. We write $inv(\sigma)$ for the number of inversions of σ .

We denote by $K\langle a, b, a^{-1}, b^{-1} \rangle$ the ring of noncommutative Laurent polynomials in noncommuting variables a, b over a field K . Equivalently, $K\langle a, b, a^{-1}, b^{-1} \rangle$ is the K -algebra of the free group generated by a, b .

Theorem 1. *Given a finite field \mathbb{F}_q , the number of right ideals having codimension n of the \mathbb{F}_q -algebra $\mathbb{F}_q\langle a, b, a^{-1}, b^{-1} \rangle$ of noncommutative Laurent polynomials in two free noncommuting generators a, b is equal to*

$$(1) \quad (q-1)^{n+1} q^{\frac{(n+1)(n-2)}{2}} \sum_{\theta \in \text{Indec}_{n+1}} q^{inv(\theta)},$$

with Indec_{n+1} denoting the subset of all indecomposable permutations in S_{n+1} . Equivalently, formula (1) is also given by

$$(2) \quad \left(\frac{q-1}{q}\right)^{n+1} \sum_{\theta \in \text{Indec}_{n+1}} q^{p(\theta)},$$

where $p(\theta)$ is equal to the cardinality of the set $\{(i, j), 1 \leq i, j \leq n+1, j < \theta(i) \text{ or } i > \theta^{-1}(j)\}$.

The first polynomials $P_{n+1}(q) = \sum_{\theta \in \text{Indec}_{n+1}} q^{inv(\theta)}$ corresponding to $n = 0, 1, 2, 3$ are $1, q, q^3 + 2q^2$ and $q^6 + 3q^5 + 5q^4 + 4q^3$.

The generating series of all these polynomials is easy to compute as follows: The shifted concatenation $\alpha \cdot \beta \in S_{m+n}$ of two permutations $\alpha \in S_m$ and $\beta \in S_n$ is the permutation of $\{1, \dots, m+n\}$ defined by $\alpha \cdot \beta(i) = \alpha(i)$ if $i \in \{1, \dots, m\}$ and by $\alpha \cdot \beta(i) = m + \beta(i-m)$ if $i \in \{m+1, \dots, m+n\}$. The disjoint union $\mathcal{M} = \cup_{n \in \mathbb{N}} S_n$ (with S_0 acting on the empty set), endowed with shifted concatenation, is the free (noncommutative) monoid generated by the set $\cup_{n=1}^{\infty} \text{Indec}_n$ of all indecomposable permutations, see [Cm]. Since $inv(\alpha \cdot \beta) = inv(\alpha) + inv(\beta)$, the map $inv : \mathcal{M} \rightarrow \mathbb{N}$ defines a morphism from the monoid \mathcal{M} onto the additive monoid \mathbb{N} . Freeness of \mathcal{M} over $\cup_{n=1}^{\infty} \text{Indec}_n$ implies the formula

$$\begin{aligned} \sum_{n \in \mathbb{N}} t^n \sum_{\sigma \in S_n} q^{inv(\sigma)} &= \sum_{k=0}^{\infty} \left(\sum_{n=1}^{\infty} t^n \sum_{\sigma \in \text{Indec}_n} q^{inv(\sigma)} \right)^k \\ &= \frac{1}{1 - \sum_{n=1}^{\infty} t^n \sum_{\sigma \in \text{Indec}_n} q^{inv(\sigma)}} \end{aligned}$$

for the generating series of the number of permutations with a given number of inversions. An easy induction yields the well-known identity

$$\sum_{\sigma \in S_n} q^{inv(\sigma)} = (1)(1+q) \cdots (1+q+\cdots+q^{n-1}) = (q-1)^{-n} \prod_{k=1}^n (q^k - 1)$$

$$\begin{array}{cccc}
* & \cdots & 1 & \\
\vdots & & \vdots & \\
1 & \cdots & * & \\
\end{array}
\qquad
\begin{array}{cccc}
1 & & & \\
\vdots & & & \\
* & \cdots & 1 & \\
\end{array}$$

FIGURE 1

where the right-hand side involves the classical q -analogue of the factorial function. We have therefore

$$\sum_{n \geq 0} (1)(1+q) \cdots (1+q+\cdots+q^{n-1})t^n = (1 - \sum_{k \geq 1} P_k(q)t^k)^{-1}.$$

3. INVERSIONS AND HOOKS

We represent a permutation $\sigma \in S_n$ by its permutation matrix, with a 1 in row i and column $\sigma(i)$, for each $i, 1 \leq i \leq n$, and with 0's elsewhere. (With this convention, well-suited to the group-structure of S_n , a permutation matrix M_σ acts by right-multiplication $v \mapsto v \cdot M_\sigma$ through the coordinate-permutation $v_i \mapsto v_{\sigma(i)}$ on a row-vector $v = (v_1, \dots, v_n)$.) A *hook* of a coefficient 1 in such a matrix is the set of 0's which are located either on the same row at its left or on the same column and below it. In other words, the hook associated to $(i, \sigma(i))$ is the set of entries with coordinates $(i, j), j < \sigma(i)$, or $(k, \sigma(i)), k > i$. Since the permutation matrix of σ^{-1} is obtained by transposing the permutation matrix of σ , the cardinality of the union of all hooks in the permutation matrix of σ is equal to the number $p(\sigma)$ introduced in Theorem 1. Hooks are in general not disjoint. They can be enumerated as follows: An inversion of σ gives rise to a pair of 1's (in the permutation matrix of σ) which are incomparable with respect to the order on entries induced by the natural order of $\mathbb{N} \times \mathbb{N}$ (ie. one of the coefficients 1 has a higher row-index, the other a higher column-index). A *version* of σ is a pair $i < j$ of distinct integers such that $\sigma(i) < \sigma(j)$. Equivalently, a version corresponds to a pair of 1's (in the permutation matrix of σ) whose entries are comparable for the natural order on $\mathbb{N} \times \mathbb{N}$. Denote by $inv(\sigma)$ and by $v(\sigma)$ the number of inversions and of versions of σ . We have

$$(3) \quad p(\sigma) = 2inv(\sigma) + v(\sigma) = inv(\sigma) + \binom{n}{2}.$$

The first equality follows from Figure 1, which shows that each inversion increases $p(\sigma)$ by 2 (left part of Figure 1) whereas a version adds only 1 corresponding to a unique 0 contained in both hooks (right part of Figure 1). The observation that the sum $inv(\sigma) + v(\sigma)$ is equal to the number $\binom{n}{2}$ of all 2-subsets in $\{1, \dots, n\}$ shows the second equality.

Rewriting the equality $p(\theta) = inv(\theta) + \binom{n+1}{2}$ as $p(\theta) - n - 1 = inv(\theta) + \frac{(n+1)(n-2)}{2}$ we deduce equality of Formulae (1) and (2) in Theorem 2 from (3) and from the trivial identity $\frac{(n+1)(n-2)}{2} + n + 1 = \frac{n(n+1)}{2}$.

4. A THEOREM OF HAGLUND

Let $\lambda = (\lambda_1, \dots, \lambda_l)$ be a partition, with $0 \leq \lambda_1 \leq \dots \leq \lambda_n \leq n$. We associate to it the subset E_λ of $[n] \times [n]$ defined by $E_\lambda = \cup_{1 \leq i \leq n} \{i\} \times [\lambda_i]$, where $[k] = \{1, \dots, k\}$. The following result is a particular case of Theorem 1 in [Hg].

Theorem 2. *The number of $n \times n$ invertible matrices over \mathbb{F}_q whose nonzero entries lie in E_λ is equal to $(q-1)^n \sum_{\sigma} q^{p(\sigma)}$, where the sum is over all permutations in S_n whose matrices have nonzero entries only in E_λ .*

We have stated the variant of [BIMPSZ], the actual formulation in [Hg] is slightly different.

For further use, we denote by $H_\lambda(q)$ the polynomial appearing in Theorem 2. The polynomial $H_\lambda(q)$ is of course zero if $\lambda_i < i$ for some $i \in \{1, \dots, n\}$.

The polynomial $H_\lambda(q)$ of Haglund's theorem is closely related to rook polynomials as defined and studied in [GR]. Such polynomials are symmetric (self-reciprocal). Observe however that this is not the case for the polynomials appearing in Theorem 1.

We illustrate Haglund's theorem by an example: The four possible invertible permutation matrices (corresponding to the permutations 123, 132, 213, 231) with non-zero entries in the partition $\lambda = (2, 3, 3)$ (given at the left of the following figure) are depicted in the figure below.

$$\begin{pmatrix} \times & \times & 0 \\ \times & \times & \times \\ \times & \times & \times \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ \mathbf{0} & \mathbf{0} & 1 \\ \mathbf{0} & 1 & \mathbf{0} \end{pmatrix} \begin{pmatrix} \mathbf{0} & 1 & 0 \\ 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{0} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{0} & 1 \\ 1 & \mathbf{0} & \mathbf{0} \end{pmatrix}$$

The function $p(\sigma)$ has respectively the values 3, 4, 4 and 5, as shown by the boldfaced 0's which represent the union of the hooks. The corresponding polynomial $H_\lambda(q)$ is given by $(q-1)^3 q^3 (1+q)^2$.

4.1. Proof of Theorem 2. We present a short proof of Theorem 2 for the sake of self-containedness:

Given a partition λ with n parts $\lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_n = n$ satisfying $\lambda_i \geq i$, we claim that we have

$$(4) \quad H_\lambda(q) = q^{\binom{n}{2}} \prod_{i=1}^n (q^{\lambda_i+1-i} - 1).$$

For example, the partition $\lambda = (2, 3, 3)$ considered above yields

$$q^{\binom{3}{2}} (q^{2+1-1} - 1) (q^{3+1-2} - 1) (q^{3+1-3} - 1) = q^3 (q-1)^3 (q+1)^2,$$

as expected.

Formula (4) is clearly true if λ is reduced to a unique part $\lambda_1 = 1$ where an invertible matrix associated to λ is simply a non-zero element of \mathbb{F}_q . Consider now an invertible matrix A compatible with λ (and having its coefficients in \mathbb{F}_q). There are $q^{\lambda_1} - 1$ possibilities for its first row. Let j_1 be the column-index of the last non-zero coefficient of the first row. Using the non-zero coefficient of row 1 and column j_1 for Gaussian elimination, we can eliminate all non-zero coefficients in the remaining rows of the j_1 -th column by subtracting a suitable multiple of the first row. All q^{n-1} possibilities for such an elimination can arise in a suitable invertible matrix A . Erasing in the resulting matrix the first row and the j_1 -th column, we get an invertible matrix A' associated to the partition λ' with $n-1$ parts $\lambda_2 - 1, \dots, \lambda_n - 1$. We have thus by induction

$$\begin{aligned} H_\lambda(q) &= (q^{\lambda_1} - 1) q^{n-1} H_{\lambda'}(q) \\ &= (q^{\lambda_1} - 1) q^{n-1} q^{\binom{n-1}{2}} \prod_{i=2}^n (q^{\lambda_i+1-i} - 1) \end{aligned}$$

which simplifies to (4).

We associate now to the above matrix A the permutation matrix with a 1 in the j_1 -th column of the first row. The remaining non-zero coefficients are defined recursively as the permutation matrix of A' after removal of the first row and the j_1 -th column. The hook of the coefficient 1 in the first column yields a contribution of $j_1 - 1 + n - 1$ to the number $p(\sigma)$ of the permutation σ corresponding to the permutation matrix above. The identity $p(\sigma) = j_1 - 1 + n - 1 + p(\sigma')$, another induction on n and a sum over all possibilities for j_1 imply now equality between Formula (4) and the expression $(q - 1)^n \sum_{\sigma} q^{p(\sigma)}$ given by Haglund's Theorem. \square

Remark. Formula (4) is in fact much more suited for computing $H_{\lambda}(q)$ than the expression given in Theorem 2.

5. PREFIX-FREE AND PREFIX-CLOSED SETS

We denote by A^* the free monoid over a finite set A . Elements of A^* are *words* with letters in the *alphabet* A . The product of two words $u = u_1 \dots u_n$ and $v = v_1 \dots v_m$ in A^* is given by the concatenation $uv = u_1 \dots u_n v_1 \dots v_m$. The identity element of A^* is the empty word, denoted by 1 in the sequel. We use $a^* = \{a^n, n \geq 0\}$ for the set of all powers of a letter a in the alphabet A .

A word u is a *prefix* of a word w if $w = uv$ for some word v . A subset C of A^* is *prefix-free* if no element of C is a proper prefix of another element of C . A prefix-free set C is *maximal* if it is not contained in a strictly larger prefix-free set. A prefix-free set C is maximal if and only if the right ideal CA^* intersects every (non-empty) right ideal I of the monoid A^* ¹. Indeed a prefix-free set C giving rise to a right ideal CA^* not intersecting a right ideal I of A^* can be augmented by adjoining an element of I . Conversely, a prefix-free set C strictly contained in a prefix-free set $C \cup \{g\}$ defines a right ideal CA^* which is disjoint from the right ideal gA^* . Another characterization of maximal prefix-free sets is given by the fact that a prefix-free set C is maximal if and only if every element of $A^* \setminus C$ has either an element of C as a proper prefix or is a proper prefix of an element of C .

A subset P of A^* is *prefix-closed* if P contains all prefixes of its elements. Equivalently, $P \subset A^*$ is prefix-closed if $u \in P$ whenever there exists $v \in A^*$ such that $uv \in P$. In particular, every non-empty prefix-closed set contains the empty word.

There is a canonical bijection between finite maximal prefix-free sets and finite prefix-closed sets: The prefix-closed set corresponding to a finite maximal prefix-free set C is the set $P = A^* \setminus CA^*$ of proper prefixes of all words in C . The inverse bijection associates to a finite prefix-closed set P the finite maximal prefix-free set $C = PA \setminus P$ if P is nonempty, and $C = \{1\}$ if P is empty. This bijection has the following graphical interpretation: Prefix-closed sets have a natural rooted tree-structure: the root is the empty word, ancestors of a vertex-word are its prefixes. The set $C \cup P$ (with C and P as above) is of course prefix-closed and the associated tree has leaves indexed by elements of C and interior vertices indexed by elements of P . Every interior vertex has the same number of children indexed by the alphabet A . The perhaps empty subtree of all interior vertices indexed by P determines (and is uniquely determined by) the set of all leaves corresponding to C .

Consider now a finite maximal prefix-free set $C \subset \{a, b\}^*$ with associated finite prefix-closed set P . For $x \in \{a, b\}$, denote by $C_x \cap \{a, b\}^*x$ the set of words in C

¹A right ideal of a monoid \mathcal{M} is of course defined in the obvious way as a subset I of \mathcal{M} such that $I\mathcal{M} = I$.

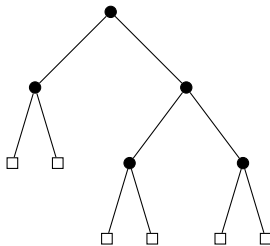


FIGURE 2. A prefix-free set

terminating with x , and denote by $P_x = P \cap (\{1\} \cup \{a, b\}^*x)$ the subset of P given by the union of 1 (provided P is non-empty) with the subset of all non-empty words in P ending with x . If $C \neq \{1\}$, we have a bijection μ_a between C_a and P_b given by $C_a \ni w \mapsto p \in P_b$ where p is the unique element of P_b such that $w \in pa^*$. The inverse bijection associates to $p \in P_b$ the unique word $w = pa^* \cap C_a$ of C_a .

Similarly, we have a bijection μ_b between C_b and P_a if $C \neq \{1\}$.

Observe that C is given by the disjoint union $C_a \cup C_b$, except in the trivial case $C = \{1\}$ where we have $C_a = C_b = P = \emptyset$. Assuming, as always in the sequel, that C is nontrivial, we can define $\mu : C \rightarrow P$ by using μ_a on C_a and μ_b on C_b . Otherwise stated, $\mu(c)$ is the prefix of c obtained by removing from c its suffix of maximal length equal to a power of its last letter. Equivalently, $\mu(x)$ (for $x \neq 1$) is defined as the shortest proper prefix of x such that $x \in \mu(x)a^* \cup \mu(x)b^*$.

Notice that $\mu(a^\alpha) = \mu(b^\beta) = 1$ where a^α and b^β are the two unique elements of C involving only one letter. Notice also that μ induces a bijection between $C \setminus \{a^\alpha, b^\beta\}$ and $P \setminus \{1\}$ and that μ restricted to $C \setminus \{b^\beta\}$ is a bijection onto P .

Consider the prefix-free set $C = \{a^2, ab, ba^2, bab, b^2a, b^3\}$, represented by the leaves of a complete binary tree, see Figure 2. Its set of prefixes $P = \{1, a, b, ba, b^2\}$ is the set of internal nodes. One has $P_a = \{1, a, ba\}$, $P_b = \{1, b, b^2\}$, $C_a = \{a^2, ba^2, b^2a\}$ and $C_b = \{ab, bab, b^3\}$. The bijection μ_a sends a^2, ba^2, b^2a respectively onto $1, b, b^2$ and μ_b sends ab, bab, b^3 respectively onto $a, ba, 1$.

For all these results, see [BR] or [BPR], where prefix-free sets are called prefix sets².

6. ORDER PROPERTIES OF PREFIX-FREE AND PREFIX-CLOSED SETS

Let A be a totally ordered alphabet. The *alphabetical* (or *lexicographical*) order on the free monoid A^* is the order of the dictionary. Formally, one has $u < v$ if and only if u is a proper prefix of v or if $u = xay, v = xbz$ for some words x, y, z and two distinct letters a, b ordered by $a < b$ of the alphabet A .

For any words u, v, x, y we have the following properties:

- $u < v$ if and only if $xu < xv$;
- If u is not a prefix of v then $u < v$ implies $ux < vy$.

Lemma 1. *If $p, q \in \{a, b\}^*$ are two elements with $p \leq q$ lexicographically then every element of $pa^* = \cup_{n=0}^{\infty} pa^n$ is lexicographically strictly smaller than every element of $qbb^* = \cup_{n=1}^{\infty} qb^n$.*

²A prefix-free set, not equal to $\{1\}$, is a *code*.

Proof. If p is not a prefix of q , we are done by the previous observation. If $q = pw$ then $pa^i < pwb^j$ if and only if $a^i < wb^j$. This holds for $j \geq 1$ since a^i is strictly smaller than any word involving b . \square

A finite maximal prefix-free set C of $\{a, b\}^*$ defines a complete finite binary tree T with leaves indexed by C and interior vertices indexed by the associated prefix-closed set P . An element $v \in C_a$ defines a *left branch* $\mu_a(v)a^* \cap (C \cup P)$ of T . The natural integer $\text{length}(v) - \text{length}(\mu_a(v))$ is the *length* of the left-branch defined by $v \in C_a$ (see also the last paragraph of Section 7.1).

We shall need the following arithmetic characterization of complete binary trees and associated prefix sets.

Lemma 2. *A complete finite binary tree T with leaves indexing a finite maximal prefix-free set C (and interior vertices defining the associated prefix-closed set P) is uniquely determined by the ranks i_1, \dots, i_k of all k elements in C_a among the alphabetically ordered elements of C and by the corresponding lengths l_1, \dots, l_k of the associated left branches.*

The integers i_1, \dots, i_k and l_1, \dots, l_k of Lemma 2 can also be described as follows: if $C = \{c_1, \dots, c_{n+1}\}$ with $c_1 < c_2 < \dots < c_n < c_{n+1}$, then $C_a = \{c_{i_1}, \dots, c_{i_k}\}$ and $l_j = \text{length}(c_{i_j}) - \text{length}(\mu_a(c_{i_j}))$. In the running example of Figure 2 we have $k = 3$, $l_1 = 2$, $l_2 = 2$, $l_3 = 1$, $i_1 = 1$, $i_2 = 3$, $i_3 = 5$. We leave the proof of Lemma 2 to the reader.

We establish for later use the following identity involving some numbers associated to prefix sets.

Lemma 3. *We consider a finite maximal prefix-free set $C \subset \{a, b\}^*$ with associated prefix-closed set P having $n = |P| = |C| - 1 \geq 0$ elements. We write*

$$\tilde{C}_a = C \setminus C_b = \begin{cases} C_a & \text{if } C \neq \{1\}, \\ \{1\} & \text{if } C = \{1\} \end{cases}$$

for the set of all words in C which do not end with b . We denote by i_1, \dots, i_k the ranks in $C = \{c_1, \dots, c_{n+1}\}$ (listed in alphabetical order) of all $k = |\tilde{C}_a|$ elements in $\tilde{C}_a = \{c_{i_1}, \dots, c_{i_k}\} \subset C$. We introduce the set $\mathcal{M} = \{(p, c) \in (P_b \setminus \{1\}) \times C_b, p < c\}$ containing $M = |\mathcal{M}|$ elements. Then

$$M + \sum_{h=1}^k i_h = (n+1)(k-1) + k - \frac{k(k-1)}{2}.$$

In our running example of Figure 2, we have $\mathcal{M} = \{(b, bab), (b, b^3), (b^2, b^3)\}$ and $M = 3$, $n = 5$, $k = 3$, $i_1 = 1$, $i_2 = 3$, $i_3 = 5$. Hence we get $3 + 1 + 3 + 5 = 12$ for the left side and $6 \cdot 2 + 3 - \frac{3 \cdot 2}{2} = 12$ for the right side.

Proof. For $C = \{1\}$ the set P is empty, we have $M = 0$, $n = 0$, $k = 1$, $i_1 = 1$ and both sides of the identity are equal to 1.

For $C \neq \{1\}$, we apply induction using the partition $C = aC' \cup bC''$. We have two subcases given by $n'' = 0$ (corresponding to $C'' = \{1\}$) and by $n'' > 0$ (corresponding to $C'' \neq \{1\}$) using obvious notations.

In the case $n'' = 0$ we have the partition

$$\mathcal{M} = a\mathcal{M}' \cup (a(P'_b \setminus \{1\}) \times \{b\})$$

(where $a\mathcal{M}' = \{(ap', ac'), (p', c') \in \mathcal{M}'\}$) for the set \mathcal{M} . This shows $M = |\mathcal{M}| = M' + |(P'_b \setminus \{1\})|$. Existence of the bijection μ_a between C'_a and P'_b (which exists even if $C' = \{1\}$ since then both sets are empty) and the equality $|(P'_b \setminus \{1\})| = |\tilde{C}'_a| - 1 = k' - 1$ (holding also for $C' = \{1\}$ with our definition of \tilde{C}'_a) give $M = M' + k' - 1$. Since $k = k'$, $i_h = i'_h$ for $h = \{1, \dots, k\}$ and since $n = n' + 1$ we have by induction

$$\begin{aligned} M + \sum_{h=1}^k i_h &= k - 1 + M' + \sum_{h=1}^{k'} i'_h \\ &= k - 1 + (n' + 1)(k' - 1) + k' - \frac{k'(k' - 1)}{2} \\ &= (n' + 2)(k' - 1) + k' - \frac{k'(k' - 1)}{2} \\ &= (n + 1)(k - 1) + k - \frac{k(k - 1)}{2} \end{aligned}$$

which ends the proof in the case $C'' = \{1\}$.

In the remaining case $n'' > 0$ corresponding to $C'' \neq \{1\}$ we have the partition

$$\begin{aligned} \mathcal{M} &= a\mathcal{M}' \cup (a(P'_b \setminus \{1\}) \times bC''_b) \cup b\mathcal{M}'' \cup (\{b\} \times bC''_b) \\ &= a\mathcal{M}' \cup b\mathcal{M}'' \cup ((a(P'_b \setminus \{1\}) \cup \{b\}) \times bC''_b) \end{aligned}$$

for $\mathcal{M} = \{(p, c) \in (P_b \setminus \{1\}) \times C_b, p < c\}$ where $a\mathcal{M}' = \{(ap', ac'), (p', c') \in \mathcal{M}'\}$ and $b\mathcal{M}'' = \{(bp'', bc''), (p'', c'') \in \mathcal{M}''\}$. Existence of the bijection μ_a between C'_a and P'_b shows $|(a(P'_b \setminus \{1\}) \cup \{b\})| = k'$. Existence of the partition $C'' = C''_a \cup C''_b$ (since $n'' > 0$) together with the identities $|C''| = n'' + 1$ and $|C''_a| = k''$ implies $|C''_b| = n'' + 1 - k''$. We have thus the identity

$$M = M' + M'' + k'(n'' + 1 - k'')$$

holding also in the case $n' = 0$ corresponding to $C' = \{1\}$.

We have $k = k' + k''$, $i_h = i'_h$ for $h \in \{1, \dots, k'\}$ and $i_h = n' + 1 + i''_{h-k'}$ for $h \in \{k' + 1, \dots, k' + k''\}$. This implies

$$\begin{aligned} \sum_{h=1}^k i_h &= \sum_{h=1}^{k'} i'_h + \sum_{h=k'+1}^{k'+k''} (n' + 1 + i''_{h-k'}) \\ &= \sum_{h=1}^{k'} i'_h + (n' + 1)k'' + \sum_{h=1}^{k''} i''_h \end{aligned}$$

and we have thus by induction

$$\begin{aligned} M + \sum_{h=1}^k i_h &= M' + M'' + k'(n'' + 1 - k'') + \sum_{h=1}^{k'} i'_h + (n' + 1)k'' + \sum_{h=1}^{k''} k'' i''_h \\ &= (n' + 1)(k' - 1) + k' - \frac{k'(k' - 1)}{2} + \\ &\quad + (n'' + 1)(k'' - 1) + k'' - \frac{k''(k'' - 1)}{2} + \\ &\quad + k'(n'' + 1 - k'') + (n' + 1)k'' \end{aligned}$$

which simplifies to

$$\begin{aligned} & (n' + n'' + 1 + 1)(k' + k'' - 1) + (k' + k'') - \frac{(k' + k'')(k' + k'' - 1)}{2} \\ = & (n + 1)(k - 1) + k - \frac{k(k - 1)}{2} \end{aligned}$$

as required. \square

Remark. Lemma 3, rewritten as

$$(5) \quad (n + 1)k = \sum_{h=1}^k i_h + M + (n + 1 - k) + \frac{k(k - 1)}{2},$$

has also the following bijective proof: The left side of (5) is the cardinality of the set $C \times \tilde{C}_a$. The right side is the cardinality of the disjoint union $E = E_1 \cup E_2 \cup E_3 \cup E_4$, where

$$\begin{aligned} E_1 &= \{(c_1, c_2) \in C \times \tilde{C}_a, c_1 \leq c_2\}, \\ E_2 &= \mathcal{M} = \{(p, c) \in (P_b \setminus 1) \times C_b, p < c\}, \\ E_3 &= (C \setminus \tilde{C}_a) = C_b, \\ E_4 &= \{(c_1, c_2) \in \tilde{C}_a \times \tilde{C}_a, c_1 < c_2\}. \end{aligned}$$

The set $F = C \times \tilde{C}_a$ can be partitioned into $F = F_{\leq} \cup F_{>}$ with

$$\begin{aligned} F_{\leq} &= E_1 = \{(c_1, c_2) \in C \times \tilde{C}_a, c_1 \leq c_2\}, \\ F_{>} &= \{(c_1, c_2) \in C \times \tilde{C}_a, c_1 > c_2\}. \end{aligned}$$

We leave it to the reader to check that $\varphi : F_{>} \rightarrow E_2 \cup E_3 \cup E_4$ given by

$$\varphi(c, \gamma) = \begin{cases} (\mu_a(\gamma), c) \in E_1 & c \in C_b, \gamma \notin aa^*, \\ c \in E_3 & c \in C_b, \gamma \in aa^*, \\ (\gamma, c) \in E_4 & c \in C_a. \end{cases}$$

defines a bijective map.

7. TWISTED ALPHABETICAL ORDER

7.1. Twisting a total order. Suppose that we have a set E with a partition $E = \cup_{i \in I} E_i$, where I and each E_i are totally ordered. This gives a natural total order on E by setting $x < y$ if either x and y with $x < y$ belong to a common subset E_i or if $x \in E_i$ and $y \in E_j \neq E_i$ with $i < j$.

Call a subset I of an ordered set E an *interval* if $a \in I, b \in E, c \in I$ and $a < b < c$ implies $b \in I$. A set I indexing disjoint non-empty intervals E_i partitioning a totally ordered set $E = \cup_{i \in I} E_i$ is naturally ordered as follows: Given two distinct elements i, j of I , we set $i < j$ if $x < y$ for some $x \in E_i, y \in E_j$. Since the sets E_i are intervals, this is a well-defined total order relation on I , independent of the chosen representatives x and y . We use this partition and the previous construction to define the *twisted total order* \prec (with respect to the partition $\cup_{i \in I} E_i$): The restriction of \prec to each E_i is the opposite order of $<$ on E_i and the set I is ordered by $<$.

Remark. (i) It is also possible to twist the order on $E = \cup_{i \in I} E_i$ according to the set of indices: $x \tilde{\prec} y$ if either $x < y$ for $x, y \in E_i$ or $x \in E_i, y \in E_j$ with $i > j$. Twisting an order relation on the set of indices of a suitable partition amounts

however to the ordinary order twist of the opposite order relation with respect to the same partition.

(ii) Twisted orders can be generalized to arbitrary (not necessarily) totally ordered) posets using *admissible* partitions indexed by posets where a partition $E = \cup E_i$ of a poset E is admissible if all elements in any common part E_i have the same sets of upper and lower bounds in $E \setminus E_i$.

Consider now $\{a, b\}^*$ with the alphabetical order. We partition $\{a, b\}^*$ into equivalence classes given by $u \sim v$ if $ua^* \cap va^* \neq \emptyset$. Elements in a common equivalence class differ thus at most by a final string of a 's. Each equivalence class can be written as wa^* for a unique word w in $\{a, b\}^* \setminus \{a, b\}^*a = \{1\} \cup \{a, b\}^*b$. More precisely, the equivalence class of an element w is the set wa^* if $w \in \{a, b\}^*b \cup \{1\}$ does not end with a . It is given by $\mu_a(w)a^*$ if $w \in \{a, b\}^*a$ has last letter a .

For further use we mention also the trivial fact that $u \sim v$ implies either that u is a (not necessarily proper) prefix of v or that v is a prefix of u .

Lemma 4. *Each equivalence class for \sim is an interval of the lexicographically ordered poset $\{a, b\}^*$.*

Proof. It is enough to show that $u < v < ua^i$ implies $v = ua^h$ with $h \in \{1, \dots, i-1\}$. The easy verification is left to the reader. \square

Lemma 4 shows that we can apply the previous construction. Thus we obtain the *twisted alphabetical order* which we denote by \prec . In summary, $u \prec v$ if and only if either u, v are both in a common equivalence class wa^* and $v < u$, or if they belong to two different equivalence classes and $u < v$. Equivalently, $u \prec v$ if either $\mu_a(u) \neq \mu_a(v)$ and $u < v$ or if $\mu_a(u) = \mu_a(v)$ and $u \in vaa^*$ where μ_a is extended to all elements of $\{a, b\}^*$ by setting $\mu_a(w) = w$ if $w \notin \{a, b\}^*a$ (ie. μ_a erases always a final maximal (perhaps empty) string of consecutive letters a in a word).

The following result summarizes a few properties of the twisted order:

Lemma 5. (i) *The two order relations $<$ and \prec induce opposite orders on an equivalence class of \sim .*

(ii) *If u, v are not in the same equivalence class of \sim , then $u < v$ if and only if $u \prec v$ and this depends only on the equivalence classes of u and v .*

(iii) *The restriction of the map μ defined in Section 5 to the set $\{a, b\}^*a$ is order-preserving in the following sense: For two elements u, v in $\{a, b\}^*a$ with $u < v$ we have either $\mu(u) = \mu(v)$ (and they are in a common class $\mu(u)a^*$) or we can apply (ii) above.*

We leave the easy proof to the reader. \square

Call *left branch* of a subset L of $\{a, b\}^*$ a non-empty intersection of L with an equivalence class of \sim .

7.2. Prefix-free sets and the twisted alphabetical order.

Lemma 6. *Let C be a finite maximal prefix-free set in $\{a, b\}^*$ with associated prefix-closed set P . Given an element c in C we denote by $c' \in C_a$ the largest lower bound of c in C_a (ie. c' is maximal in C_a such that $c' \leq c$). Then $\mu(d) \preceq \mu(c')$ (with μ defined in Section 5) for every d in C such that $d \leq c$.*

An instance of this lemma in our running example is: For $c = bab$ we have $c' = ba^2$. Taking $d = c$ we get $\mu(d) = ba \prec b = \mu(c')$.

Proof. If d is in C_a this follows from prefix-freeness of C_a and from assertion (iii) in Lemma 5.

Suppose now that $d \in C_b$. Define $c'' \in C_a$ as the unique element of C in the set $\mu(d)a^* = \mu_b(d)a^*$. If $c'' = c'$ then $\mu_a(c') = \mu_a(\mu(d)) \succ \mu(d)$ by definition of \prec on equivalence classes. If $c'' \neq c'$ then $c'' < c'$ by maximality of c' . The elements c'' and c' define thus two different equivalence classes $\mu_a(c'')a^*$ and $\mu_a(c')a^*$ and we can apply assertion (ii) of Lemma 5. \square

8. RIGHT CONGRUENCES OF A FREE MONOID.

A *right congruence* of a monoid is an equivalence relation \equiv which is compatible with right-multiplication: $u \equiv v$ implies $uw \equiv vw$. Observe that each element in the monoid induces, by right-multiplication, a function from the set of \equiv -classes into itself. Equivalently, we get a right action of the monoid on the quotient³. Recall the well-known bijection between right congruences of finite index in a free monoid A^* and triplets (C, P, f) where C is a finite maximal prefix-free set with associated prefix-closed set P and where $f : C \rightarrow P$ is a function such that $f(c) \in P$ is alphabetically smaller than c for every c in C . The corresponding congruence is generated by the relations $c \equiv f(c)$ for c in C . The prefix-closed set P is a set of representatives for the quotient set A^* / \equiv . The right action of A^* on the quotient is completely defined as follows: A letter x of the alphabet A acts on p in P by $p.x = px$ if px is in P and by $p.x = f(px)$ otherwise (see for example Proposition 7 of [BR]).

We illustrate this with the right congruence defined by $a^2 \equiv 1, ba^2 \equiv b, b^2a \equiv b^2, ab \equiv 1, bab \equiv ba, b^3 \equiv a$ with C and P as in Figure 2. Right-multiplication $w \mapsto w.a$ or $w \mapsto w.b$ by a or b on the set $P = \{1, a, b, ba, b^2\}$ is given by

| | | | | | |
|-------|-----|-----|-------|------|-------|
| w | 1 | a | b | ba | b^2 |
| $w.a$ | a | 1 | ba | b | b^2 |
| $w.b$ | b | 1 | b^2 | ba | a |

9. LEFT-TO-RIGHT MAXIMA AND INDECOMPOSABLE PERMUTATIONS

A *left-to-right maximum* of a permutation $\sigma \in S_n$ is a value $\sigma(i) = j \in \{1, \dots, n\}$ such that $\sigma(h) < j$ for $h < i$. We call i the *position* and j the *value* of the left-to-right maximum $\sigma(i)$. The following result is well-known.

Lemma 7. *A permutation $\sigma \in S_n$ with successive positions $i_1 < \dots < i_k$ of left-to-right maxima is indecomposable (in the sense of Section 2) if and only if $\sigma(i_j) \geq i_{j+1}$ for $j = 1, \dots, k-1$.*

Observe that one has always $i_1 = 1$ and $\sigma(i_k) = n$ with these notations.

For later use, we state and prove the following result, which holds for any permutation expressed as a word $w = a_1 \dots a_n$ involving n distinct letters of a totally ordered alphabet. We denote by $st(w) = i_1 \dots i_n \in S_n$ the associated *standard permutation* of w obtained by replacing each letter a_j in w by its rank i_j in the totally ordered set $\{a_1, \dots, a_n\}$. The standard permutation of $w = 3649$ for example is given by $st(w) = 1324$.

³A right congruence of a free monoid is essentially the same thing as a deterministic automaton. More precisely, a right congruence of a free monoid corresponds to an automaton with an initial state but without prescribed set of final states, which is *accessible* in the sense that each state can be reached from the initial state.

10. INDECOMPOSABLE PERMUTATIONS AND REGULAR RIGHT CONGRUENCES OF THE FREE MONOID $\{a, b\}^*$.

10.1. Indecomposable permutations, regular right congruences and subgroups of the free group. A right congruence of a monoid \mathcal{M} is *regular* if right multiplication $\mathcal{M} \ni x \mapsto xa$ by an arbitrary element $a \in \mathcal{M}$ induces a bijection on the quotient. (It is of course enough to consider right-multiplications by elements in a set of generators.) Regular right congruences are *right-simplifiable* congruences, meaning that $uw \equiv vw$ implies $u \equiv v$. The two properties are equivalent when the index is finite. (Right-multiplication on classes of right-simplifiable congruences of infinite index induce injections which are in general not bijective as shown by the example $\mathcal{M} = \{a, b\}$ endowed with the right-simplifiable congruence defined by $u \equiv v$ if $a^*u \cap a^*v \neq \emptyset$. Indeed, right-multiplication by b fails to yield the class a^* represented by the empty word.)

Regular right congruences of index n in a free monoid are in bijection with subgroups of index n of the free group on the same alphabet. Such a subgroup H gives indeed rise to the right congruence $u \equiv v$ if and only if $Hu = Hv$. This yields the desired mapping from the set of subgroups of index n onto the set of regular right congruences of the same index. Conversely, a regular right congruence of index n defines a right action by bijections of the free monoid on the quotient set. This action extends uniquely to a transitive action of the free group, and the stabilizer of the class of the neutral element is a subgroup of index n . This gives the bijection.

This bijection has the following classical topological interpretation: Subgroups of the free group $\langle a, b \rangle$ generated by a and b (the case of arbitrary free groups is analogous) correspond to isomorphism classes of connected coverings $(\tilde{\Gamma}, v_*)$ with a marked base-vertex v_* of the connected graph Γ given by of two oriented loops labelled a and b attached to a unique common vertex. The fundamental group of Γ is of course the free group $\langle a, b \rangle$ consisting of all reduced words in $\{a^{\pm 1}, b^{\pm 1}\}^*$. The fundamental group of $(\tilde{\Gamma}, v_*)$ is the subgroup of all elements in $\langle a, b \rangle$ which lift to closed paths of $\tilde{\Gamma}$ starting and ending at v_* . If $\tilde{\Gamma}$ is finite (or more generally if the right actions of the cyclic groups $\langle a \rangle$ and $\langle b \rangle$ on the right cosets of $\pi_1(\tilde{\Gamma}, v_*)$ have only finite orbits), one can join an arbitrary initial vertex α of $\tilde{\Gamma}$ to an arbitrary final vertex ω by a path corresponding to a word in the free monoid $\{a, b\}^*$, ie. by a path using only positively oriented edges. In particular, such a graph $\tilde{\Gamma}$ has a canonically defined spanning tree $P = \cup_{v \in V(\tilde{\Gamma})} p_v$ where p_v is the lexicographically smallest path labelled by a word in $\{a, b\}^*$ which joins the marked vertex v_* of $\tilde{\Gamma}$ to a given vertex v of $\tilde{\Gamma}$. The set P is prefix-closed and the remaining set of labelled oriented edges in $\tilde{\Gamma}$ defines a regular right congruence. The corresponding prefix-free set $C = P\{a, b\} \setminus P$ indexes a free generating set of $\pi_1(\tilde{\Gamma}, v_0)$ by associating the generator cp_c^{-1} to every element c where p_c is the unique representant $p_c \in P$ defining the same vertex as c in $\tilde{\Gamma}$.

Subgroups of finite index of a free group were first counted by Marshall Hall Jr. [H]. The values for the number c_n of subgroups of index n in the free group $F_2 = \langle a, b \rangle$ on two generators, or equivalently for the number of regular right congruences of index n in the free monoid $\{a, b\}^*$, are 1, 3, 13, 71, 461, 3447 for $n = 1, 2, 3, 4, 5, 6$, see [OEIS], sequence A3319. Remarkably, c_n is equal to the number of indecomposable permutations in S_{n+1} . The symmetric group S_3 for example contains 3 indecomposable permutations given by 312, 213, 321 and the 3 subgroups

of index 2 in $\langle a, b \rangle$ are $\langle aa, ab, ba \rangle$, $\langle a, bab, bb \rangle$, $\langle aa, aba, b \rangle$. A first bijection between the set of subgroups of index n of the free group $\langle a, b \rangle$ on two generators and indecomposable permutations in S_{n+1} was given by Dress and Franz [DF1]. Other bijections were discovered later by Sillke [Si], Ossona de Mendez and Rosenstiehl [OR], and Cori [Cr].

10.2. Another bijection. We describe a further bijection, useful for proving Theorem 1. Since a regular right congruence \equiv of $\{a, b\}^*$ is a particular case of a right congruence, it can be described by a triplet (C, P, f) as in Section 8. Regularity, equivalent to bijectivity of the right action on the quotient represented by P , implies that we have $f(C_a) \subset P_b$ and $f(C_b) \subset P_a$, where, as previously, $C_l = C \cap \{a, b\}^*l$ and $P_l = P \cap (\{a, b\}^*l \cup \{1\})$ for l in $\{a, b\}$. Indeed, $f(ua) = va$ for $ua \in C_a$ and $va \in P$ implies $u \equiv v$ by right simplification in contradiction with the fact that elements of P represent non-equivalent classes. The case of $f(ub) = vb$ is ruled out similarly.

Moreover, the inequality $f(c) < c$ for any $c \in C$ implies recursively that $f(c) = \mu_a(c)$ for any $c \in C_a$. This shows in particular that f induces a bijection from C_a onto P_b . For instance, looking at the running example (see Figure 2, noticing that the alphabetical order is read there by turning counterclockwise around the tree, starting from the root), we must have $f(a^2) < a^2$ and $f(a^2) \in P_b$, hence $f(a^2) = 1$; then $f(ba^2) < ba^2$ and $f(ba^2) \in P_b$, hence $f(ba^2) = b$; similarly, $f(b^2a) = b^2$.

The restriction of f to C_b determines thus the regular right congruence \equiv completely. This restriction is a bijection from C_b onto P_a : Indeed, the two sets have the same cardinality. Moreover f is injective, since if $ub, vb \in C_b$ and $f(ub) = f(vb)$, then $ub \equiv vb$ so that by regularity $u \equiv v$, then $u = v$ since P is a set of representants of the quotient, and finally $ub = vb$.

Since the intersection $P_a \cap P_b$ is reduced to the empty word 1, the map f from C to P is almost a bijection: it is surjective and each element of P has a unique preimage, except the empty word which has exactly two preimages: a unique preimage $a^k = a^* \cap C_a$ in C_a and a unique preimage $f^{-1}(1) \cap C_b$ in C_b .

We introduce now the set $\tilde{P} = P \cup \{a^{-1}\}$ and we consider the bijection ϕ from C onto \tilde{P} which coincides with f except that $\phi(a^k) = a^{-1}$ where $a^k = a^* \cap C$.

The twisted alphabetical order is extended to $\{a, b\}^* \cup \{a^{-1}\}$ by the rule: $a^i \prec a^{-1} \prec w$ for any $i \geq 0$ and for any word $w \in a^*b\{a, b\}^*$ involving b .

Writing $C = \{c_1 < c_2 < \dots < c_{n+1}\}$ and $\tilde{P} = \{p_1 \prec p_2 \dots \prec p_{n+1}\}$ we get a unique permutation $\theta \in S_{n+1}$ such that $\theta(i) = j$ if $\phi(c_i) = p_j$.

Note that the twisted alphabetical order \prec and the alphabetical order $<$ coincide on the prefix-free set C .

Theorem 3. *The map $\equiv \mapsto \theta$ is a bijection from the set of regular right congruences on $\{a, b\}^*$ into n classes onto the set of indecomposable permutations in S_{n+1} .*

We illustrate Theorem 3 by considering the sets C, P together with the right congruence defined by $a^2 \equiv 1, ba^2 \equiv b, b^2a \equiv b^2, ab \equiv 1, bab \equiv ba, b^3 \equiv a$ in our running example. We have $C = \{a^2 < ab < ba^2 < bab < b^2a < b^3\}$ and $f(a^2) = 1, f(ba^2) = b, f(b^2a) = b^2$ and $f(ab) = 1, f(bab) = ba, f(b^3) = a$. Therefore, with $\tilde{P} = \{a \prec 1 \prec a^{-1} \prec ba \prec b \prec b^2\}$, we have $\phi = f$ except that $\phi(a^2) = a^{-1}$. Therefore ϕ is the bijection $C \rightarrow \tilde{P}$ represented by the following array of two rows:

$$\phi = \begin{pmatrix} a^2 & ab & ba^2 & bab & b^2a & b^3 \\ a^{-1} & 1 & b & ba & b^2 & a \end{pmatrix}.$$

Replacing words of ϕ by their respective position for the lexicographical order $a^2 < ab < ba^2 < bab < b^2a < b^3$ on the prefix-free set C , respectively for the twisted lexicographical order $a < 1 < a^{-1} < ba < b < b^2$ on \tilde{P} , we get the permutation

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 6 & 1 \end{pmatrix}.$$

Proof. We prove first that the permutation θ (associated to a regular right congruence with n classes in $\{a, b\}^*$) is an indecomposable element of S_{n+1} . The equivalence class $\mu_a(f(c))a^*$ of an element c in C_b intersects C_a in a unique element c' which is lexicographically smaller than c . Since

$$\phi(c') = \begin{cases} \mu_a(c') & \text{if } c' \notin a^* \\ a^{-1} & \text{if } c' = C_a \cap a^* \end{cases}$$

is the maximal element (with respect to the twisted order, extended to \tilde{P}) in the equivalence class of $f(c)$, left-to-right maxima of θ correspond to a subset of C_a . The equality $f(c) = \mu_a(c)$ implies that all elements of C_a define left-to-right maxima. We apply now Lemma 7 for proving indecomposability of θ as follows: Given an element $c \in C_a$, the element $\phi(c)$ is always the largest element with respect to the twisted order of the set

$$\tilde{P}(< c) = \{p \in \tilde{P}, p < c \text{ lexicographically}\} \subset P \cup \{a^{-1}\}$$

where a^{-1} is by convention the lexicographically smallest element of \tilde{P} . Indecomposability of ϕ amounts thus by Lemma 7 to the inequality

$$(6) \quad |C(\leq c)| < |\tilde{P}(< c)|$$

for all $c \in C_a$ where

$$\begin{aligned} \tilde{P}(< c) &= \{p \in \tilde{P}, p < c \text{ lexicographically}\}, \\ C(\leq c) &= \{c' \in C_a, c' \leq c \text{ lexicographically}\}. \end{aligned}$$

The identity

$$|\tilde{P}(< c)| = |P(< c)| + 1$$

where

$$P(< c) = \{p \in P, p < c \text{ lexicographically}\} = \tilde{P}(< c) \setminus \{a^{-1}\}$$

shows that the strict inequality (6) amounts to

$$|C(\leq c)| \leq |P(< c)|$$

for all $c \in C_a$. This inequality holds since μ restricts to an injection from $C(\leq c)$ into $P(< c)$ for all c in $C \setminus (C \cap b^*)$, as observed in Section 5.

Thus we have a map associating an indecomposable permutation θ to every regular right congruence \equiv . It is now enough to establish injectivity of this map. Surjectivity follows then from the known equicardinality of the two involved sets. The cardinality of C_a equals the number of left-to-right maxima of θ . Let θ have successive left-to-right maxima in positions i_1, \dots, i_k , with values j_1, \dots, j_k . The i_h are the ranks in the totally ordered set C of the elements of C_a . The lengths l_i of the left branches of P are determined by the differences between the values of two successive such maxima: $l_1 = j_1 - 1$ and $l_i = j_i - j_{i-1}$ if $i \geq 2$. By Lemma 2, the tree defined by the maximal prefix-free set C and its associated prefix-closed set P are thus completely determined by the numbers i_1, \dots, i_k and j_1, \dots, j_k . From C and P we immediately recover the function f on C_a . The bijection $f : C_b \rightarrow P_a$

is encoded by the standard permutation $st(\theta)$ (as defined in Lemma 8 of Section 9) of θ . The equivalence relation \equiv is thus completely determined by θ . \square

Remark. It is not difficult to invert the map $\equiv \mapsto \theta$ of Theorem 3. Indeed, positions and values of left-to-right maxima of an indecomposable permutation $\theta \in S_{n+1}$ determine a unique maximal prefix-free set C having $n+1$ elements. The associated standard permutation $st(\theta)$ encodes a regular right congruence given by a suitable map from C into the set P of all proper prefixes of C . This avoids equicardinality results and gives a bijective proof of Theorem 3.

10.3. Fixing C and P . We fix a finite maximal prefix-free set C of $n+1$ elements in $\{a, b\}^*$ with $C_a = C \cap \{a, b\}^*a$ containing k elements. Consider the set of all regular right congruences into n equivalence classes with lexicographically smallest representants given by the prefix-closed set P associated to C . Theorem 3 gives by restriction a bijection between the set of these congruences and the set of bijections $\alpha : C_b \rightarrow P_a$ satisfying $\alpha(c) < c$: We have indeed $\alpha(c) = \phi(c) = f(c) < c$ for any $c \in C_b$. Since $C_b = C \setminus C_a$ has $n+1-k$ elements and is totally ordered by $<$ and since P_a is totally ordered by \prec , the bijection α is naturally associated to a permutation σ of S_{n+1-k} . This permutation is simply the standard permutation of the indecomposable permutation θ (encoding a regular right representation with n classes). It is obtained from θ , viewed as a word, by removing the values of all left-to-right maxima, see Section 9. As already observed earlier, positions and values of left-to-right maxima of the permutation θ encode the underlying finite maximal prefix-free set C .

We use assertion (ii) of Lemma 5 for ordering (alphabetically) left branches of P . We denote by l_1, \dots, l_k the corresponding lengths and we set $s_i = l_1 + \dots + l_i$.

We observe for later use the following facts: If $i_1, \dots, i_k, j_1, \dots, j_k$ are as in Lemma 8 applied to a permutation in S_{n+1} , then the previous proof implies $C_a = \{c_{i_1} < \dots < c_{i_k}\}$ and $\{p_{i_1} \prec \dots \prec p_{i_k}\} = \{\phi(c_{i_1}) \prec \dots \prec \phi(c_{i_k})\}$. Hence j_h is the rank of $\phi(c_{i_h})$ in the set \tilde{P} ordered by \prec . Observe that $\phi(c_1) = a^{-1}$ and $\phi(c_{i_h}) = f(c_{i_h}) = \mu_a(c_{i_h})$ if $h \geq 2$. Thus $j_1 = l_1 + 1 = s_1 + 1$ and, more generally, $j_h = s_h + 1$ for any $h = 1, \dots, k$. Lemma 8, with n replaced by $n+1$, shows

$$p(\theta) = p(\sigma) + (n+1)k - \frac{k(k+1)}{2} - \sum_h i_h + \sum_h s_h + k$$

which simplifies to

$$(7) \quad p(\theta) = p(\sigma) + (n+1)k - \frac{k(k-1)}{2} - \sum_h i_h + \sum_h s_h.$$

11. RIGHT IDEALS IN $\mathbb{F}_q\langle a, b \rangle$.

It follows from [R] (see also [BR], Proposition 7.1) that the set of right ideals of codimension n of the free non-commutative associative algebra $\mathbb{F}_q\langle a, b \rangle$ over \mathbb{F}_q generated by a and b is in bijection with the set of triplets $(C, P, (\alpha_{c,p}))$, where C is a finite maximal prefix-free set with associated prefix-closed set P , with P of cardinality n and C of cardinality $n+1$, and where $(\alpha_{c,p})$ is a family of elements in \mathbb{F}_q with $c \in C, p \in P$ and $p < c$ for the alphabetical order.

In this case the right ideal I is generated by the polynomials $c - \sum_{p < c} \alpha_{c,p} p$. These polynomials are in fact free generators of the right $\mathbb{F}_q\langle a, b \rangle$ -module I . Moreover, the elements of P are representatives of an \mathbb{F}_q -basis of the quotient $I \setminus \mathbb{F}_q\langle a, b \rangle$

and the right action of $\mathbb{F}_q\langle a, b \rangle$ on the quotient is completely defined by

$$p.x = \begin{cases} px & \text{if } px \in P \\ \sum_{q < c} \alpha_{c,q}q & \text{if } c = px \in C \end{cases}$$

where p is in P and $x \in \{a, b\}$ is a letter of the alphabet.

The matrices $\mu(a), \mu(b)$ of the right action of a and b with respect to the basis P of $I \setminus \mathbb{F}_q\langle a, b \rangle$ are therefore $P \times P$ matrices with coefficients $\mu(x)_{p,q}$ defined by

$$(8) \quad \mu(x)_{p,q} = \begin{cases} 1 & \text{if } px = q \\ 0 & \text{if } px \in P, px \neq q \\ \alpha_{c,q} & \text{if } px = c \in C, q < c \\ 0 & \text{if } px = c \in C, q > c. \end{cases}$$

12. RIGHT IDEALS IN $\mathbb{F}_q\langle a, b, a^{-1}, b^{-1} \rangle$.

A right ideal I of codimension n in $\mathbb{F}_q\langle a, b, a^{-1}, b^{-1} \rangle$ determines a right ideal $I \cap \mathbb{F}_q\langle a, b \rangle$ of codimension n in $\mathbb{F}_q\langle a, b \rangle$. Right ideals in $\mathbb{F}_q\langle a, b \rangle$ determined in this way by right ideals in $\mathbb{F}_q\langle a, b, a^{-1}, b^{-1} \rangle$ are right ideals J of $\mathbb{F}_q\langle a, b \rangle$ such that the actions of a and b on the quotient $J \setminus \mathbb{F}_q\langle a, b \rangle$ are both linear isomorphisms. We obtain in this way a bijection between the set of right ideals of codimension n in $\mathbb{F}_q\langle a, b, a^{-1}, b^{-1} \rangle$ and the set of right ideals of codimension n in $\mathbb{F}_q\langle a, b \rangle$ such that a and b act both bijectively on the quotient.

13. Q-COUNT WITH FIXED PREFIX-FREE SET C

We consider a fixed maximal prefix-free set C of cardinality $n + 1$ in $\{a, b\}^*$ with associated prefix-closed set P of cardinality n . We count all right ideals of codimension n in $\mathbb{F}_q\langle a, b \rangle$ such that right-multiplication by a and right-multiplication by b induce bijections of the quotient. Such right ideals correspond to triplets $(C, P, (\alpha_{c,p}))$ with $\alpha_{c,p}$ encoding two invertible matrices $\mu(a)$ and $\mu(b)$ by Formula (8) of Section 11.

13.1. Counting the matrices $\mu(a)$. The definition of $\mu(a)$ shows that this matrix has a lower triangular block decomposition, with blocks ordered as in Subsection 10.3 and with block-sizes equal to the lengths l_i of the left branches of P . Moreover, each diagonal block is a companion matrix of size $l_i \times l_i$, $i = 1, \dots, k$. Strictly lower triangular blocks are filled with 0's except for their last row which is arbitrary. In other words, only rows of index s_1, s_2, \dots have some freedom: The first s_i entries of row s_i are arbitrary, except that one of them (in column $s_{i-1} + 1$) must be nonzero. Thus there are $(q - 1)q^{l_i - 1}$ possible choices for the i -th diagonal block. This amounts to $(q - 1)^k q^N$ possibilities for the matrix $\mu(a)$, where

$$(9) \quad N = \sum_{i=1, \dots, k} (s_i - 1) = \sum_{i=1, \dots, k} s_i - k$$

and where $s_i = l_1 + \dots + l_i$ is the rank in P of the unique element p_{s_i} in P such that $p_{s_i}a$ is the i -th smallest element of C_a .

In our running example given by Figure 2, the matrix $\mu(a)$ is of the form

$$\begin{array}{cccccc}
 & 1 & a & b & ba & b^2 \\
 1 & 0 & 1 & 0 & 0 & 0 \\
 a & * & \times & 0 & 0 & 0 \\
 b & 0 & 0 & 0 & 1 & 0 \\
 ba & \times & \times & * & \times & 0 \\
 b^2 & \times & \times & \times & \times & *
 \end{array}$$

where $*$ represents a nonzero element of the field, whereas \times is any element. This matrix is block-triangular, with 3 diagonal blocks, of size $l_1 = 2, l_2 = 2, l_3 = 1$. There are $(q - 1)^3 q^8$ such matrices, as predicted by the formula for $k = 3$ and $s_1 = l_1 = 2, s_2 = l_1 + l_2 = 4, s_3 = l_1 + l_2 + l_3 = 5$ leading to $N = (s_1 - 1) + (s_2 - 1) + (s_3 - 1) = 1 + 3 + 4 = 8$.

13.2. Counting the matrices $\mu(b)$. Define the auxiliary order $<_b$ by $p <_b q$ if $pb < qb$. We order the rows of $\mu(b)$ with $<_b$ and its columns by $<$.

We consider the partition λ with parts

$$(10) \quad \lambda_c = |\{q \in P_a, q < c\}|$$

indexed by elements c in C_b . A part λ_c indexed by $c \in C_b$ is thus defined as the number of lower bounds of c in P_a . Then for any $p, p' \in P$ such that $c = pb, c' = p'b \in C$ and $p <_b p'$, one has $\lambda_c \leq \lambda_{c'}$, since $c < c'$. Observe that λ has $|C_b|$ parts and a largest part (indexed by the unique element b^h of $C \cap b^*$) of length $|C_b|$, since C_b is in bijection with P_a and since each element in P_a is $< b^h$. In our running example underlying Figure 2, we have $\lambda = 2, 3, 3$, with $\lambda_{ab} = 2$ (corresponding to $1, a < ab$) and $\lambda_{bab} = \lambda_{b^3} = 3$ (since $1, a, ba < bab, b^3$).

A row of $\mu(b)$ indexed by $p \in P$ such that $pb \in P$ has all coefficients zero except for a unique coefficient 1 with column-index pb . Possibly nonzero entries in column pb , other than the 1 in row p , are in the rows q with $qb \in C$ and $pb < qb$, by definition of $\mu(b)$ in Section 11; they are located below row p . Their number is therefore equal to the number of $c \in C_b$ such that $pb < c$.

Removing from the matrix $\mu(b)$ all rows indexed by $p \in P$ such that $pb \in P$ and all columns indexed by $pb \in P_b \setminus \{1\}$, we get a matrix with rows indexed by C_b (since $pb \notin P$ implies $pb \in C_b$) and columns indexed by P_a . This matrix is a square matrix of size $|C_b| \times |C_b|$ with nonzero entries contained in the set E_λ defined at the beginning of Section 4 for the partition λ with parts λ_c defined by (10). In other words, E_λ is the set of entries (p, p') , with $pb \in C_b$ and $p' \in P_a$, such that $p' < pb$.

Observe now that the matrix $\mu(b)$ is invertible if and only if the submatrix above is invertible, since all removed rows have exactly one non-zero entry in distinct columns.

Thus, we obtain a total number $q^M H_\lambda(q)$ of possible matrices $\mu(b)$, where $M = |\{(p, c) \in (P_b \setminus \{1\}) \times C_b, p < c\}|$ and where H_λ is as in Section 2.

The matrix $\mu(b)$ of our running example looks like

$$\begin{array}{cccccc} & a & 1 & ba & b & b^2 \\ a & \times & \times & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ ba & \times & \times & \times & \times & 0 \\ b & 0 & 0 & 0 & 0 & 1 \\ b^2 & \times & \times & \times & \times & \times \end{array}$$

The associated submatrix obtained by removing both rows and columns containing 1's is the leftmost matrix in the Figure of Section 4.

14. PROOF OF THEOREM 1

The two preceding sections show that the number of right ideals of index n in $\mathbb{F}_q\langle a, a^{-1}, b, b^{-1} \rangle$ is given by

$$A_n = \sum_C (q-1)^{k(C)} q^{N(C)} q^{M(C)} H_{\lambda(C)}(q)$$

where the sum is over all maximal prefix-free sets with $n+1$ elements in $\{a, b\}^*$ and where $H_{\lambda}(q)$ counts the number of invertible matrices with support prescribed by a partition λ . The numbers $k(C)$, $N(C)$, $M(C)$ and the partition $\lambda(C)$ associated to a maximal prefix-free set C are defined as in Section 13.

Applying Haglund's Theorem (Theorem 2) we get

$$A_n = (q-1)^{n+1} \sum_C q^{N(C)+M(C)} \sum_{\sigma \in S(\lambda(C))} q^{p(\sigma)}$$

where $S(\lambda(C))$ denotes the set of all permutations with permutation-matrices supported by the partition $\lambda(C)$.

Fixing C we observe that the bijection α of subsection 10.3, viewed as a matrix indexed by $C_b \times P_a$, has nonzero entries only in E_{λ} (after identification of C_b with the set of $p \in P$ such that $pb \in C$). Moreover, we have seen that α may be identified with σ . Using the definition $N = -k + \sum_{j=1}^k s_j$ (cf. Formula (9)) and the equality

$$M = -\sum_{j=1}^k i_j + (n+1)(k-1) + k - \frac{k(k-1)}{2}$$

given by Lemma 3, we have

$$\begin{aligned} A_n &= (q-1)^{n+1} \sum_C \sum_{\sigma} q^{\sum_{j=1}^k (s_j - i_j) + (n+1)(k-1) - k(k-1)/2 + p(\sigma)} \\ &= (q-1)^{n+1} \sum_C \sum_{\theta} q^{p(\theta) - (n+1)} \end{aligned}$$

where the last identity is given by Formula (7) of Subsection 10.3 and where the second sum is over all possible permutations θ as in Subsection 10.3. Since θ is necessarily indecomposable and since an indecomposable permutation θ of S_{n+1} determines C uniquely, the first sum can be dropped. This shows the equality

$$A_n = (q-1)^{n+1} \sum_{\theta \in \text{Indec}_{n+1}} q^{p(\theta) - (n+1)}.$$

A comparison with formula (2) ends the proof. \square

15. CONCLUSION

Our main result can also be interpreted as a cellular decomposition of the set of right ideals of codimension n in $\mathbb{F}\langle a, a^{-1}, b^{-1} \rangle$ over an arbitrary field \mathbb{F} . Cells are indexed by indecomposable permutations of S_{n+1} and the cell corresponding to an indecomposable permutation θ in S_{n+1} is isomorphic to $(\mathbb{F}^*)^{n+1} \times \mathbb{F}^{\binom{n+1}{2} + \text{inv}(\theta)}$.

There exists perhaps an extension of our main result to the ring of Laurent polynomials in $g \geq 3$ variables. Indeed, one ingredient of our proof is a bijection between subgroups of index n of the free group in 2 generators and indecomposable permutations in S_{n+1} and Dress and Franz have generalized their bijection in [DF1] to a bijection between subgroups of index n of the free group in g generators and systems of $g - 1$ indecomposable permutations in S_{n+1} , see [DF2].

REFERENCES

- [AS] M. Aguiar and F. Sottile: *Structure of the Malvenuto-Reutenauer Hopf algebra of permutations*, Advances in Mathematics **191**, 225275 (2005).
- [B] M. Bona: *Combinatorics of permutations*, Chapman and Hall, 2012.
- [BPR] J. Berstel, D. Perrin and C. Reutenauer: *Codes and Automata*, Cambridge University Press, 2010.
- [BR] R. Bacher and C. Reutenauer: *The number of right ideal of given codimension over a finite field*, Contemporary Mathematics **592**, 1-18 (2013).
- [BIMPSZ] J. B. Lewis, R. I. Liu, A. H. Morales, G. Panova, S. V. Sam, Y. X. Zhang: *Matrices with restricted entries and q -analogues of permutations*, Journal of Combinatorics **2**, 355-395 (2011).
- [C] P. M. Cohn: *Free ideal rings*, Journal of Algebra **1**, 47-69 (1964).
- [Cm] L. Comtet: *Sur les coefficients de l'inverse de la série formelle $\sum n!t^n$* , Comptes Rendus de l'Académie des Sciences, Paris Série A-B **275**, A569A572 (1972).
- [Cr] R. Cori: *Indecomposable permutations, hypermaps and labeled Dyck paths*, Journal of Combinatorial Theory A **116**, 1326-1343 (2009).
- [DF1] A.W.M. Dress and R. Franz: *Parametrizing the subgroups of finite index in a free group and related topics*, Bayreuther Mathematische Schriften **20**, 1-8 (1985).
- [DF2] A.W.M. Dress and R. Franz: *Zur Parametrisierung von Untergruppen freier Gruppen*, Beiträge zur Algebra und Geometrie **24**, 125-134 (1987).
- [GR] A. M. Garsia and J. B. Remmel: *q -counting rook configurations and a formula of Frobenius*, Journal of combinatorial Theory Series A **41**, 246-275 (1986).
- [Hg] J. Haglund: *q -rooks polynomials and matrices over finite fields*, Advances in Applied Mathematics **20**, 450-487 (1998).
- [H] M. Hall, Jr.: *Subgroups of finite index in free groups*, Canadian Journal of Mathematics **1**, 187-190 (1949).
- [OEIS] N. J. A. Sloane: *The Electronic Encyclopedia of Integer Sequences*, published electronically at <http://oeis.org>.
- [OR] P. Ossona de Mendez and P. Rosenstiehl: *Transitivity and connectivity of permutations*, Combinatorica **24**, 487-501 (2004).
- [P] T. Pirashvili: *Sets with two associative operations*, Central European Journal of Mathematics **2**, 169-183 (2003).
- [PR] S. Poirier and C. Reutenauer: *Algèbre de Hopf de tableaux*, Annales des Sciences mathématiques du Québec **19**, 7990 (1995).
- [R] M. Reineke: *Cohomology of noncommutative Hilbert schemes*, Algebras and Representation Theory **8**, 541-561 (2005).
- [Si] T. Sillke: *Zur Kombinatorik von Permutationen*, Séminaire Lotharingien de Combinatoire **B21c**, 8 pp. (1989).

ROLAND BACHER, UNIV. GRENOBLE ALPES, INSTITUT FOURIER (CNRS UMR 5582), 100 RUE DES MATHS, F-38000 GRENOBLE, FRANCE

E-mail address: roland.bacher@fourier.ujf-grenoble.fr

CHRISTOPHE REUTENAUER, DÉPARTEMENT DE MATHÉMATIQUES UQAM, CASE POSTALE 8888
SUCC. CENTRE-VILLE, MONTRÉAL (QUÉBEC) H3C 3P8 CANADA
E-mail address: `Reutenauer.Christophe@uqam.ca`