Canad. J. Math. Vol. **68** (3), 2016 pp. 481–503
http://dx.doi.org/10.4153/CJM-2016-004-8

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

$$(q-1)^{n+1} q^{\frac{(n+1)(n-2)}{2}} \sum_{\theta} q^{\mathrm{inv}(\theta)},$$

where the sum is over all indecomposable permutations in S_{n+1} and where $\mathrm{inv}(\theta)$ stands for the number of inversions of θ.

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 the best of our 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. In Theorem 10.3 (a keystone for proving Theorem 2.1, our main result) we give a further bijection based on a natural correspondence between subgroups of finite index and regular right congruences of free monoids.

Note that subgroups of the free group F_2 are also naturally in bijection with rooted hypermaps; see [Cr]. Indecomposable permutations also appear 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 permutation groups is a free monoid under shifted concatenation, freely generated by the set of indecomposable permutations (a proof can be found in [P]). This yields a generating function (see [C]) allowing us to count indecomposable permutations easily.

Our main result is a q-analogue of the bijections mentioned above. We consider the polynomial

$$P_{n+1}(q) = \sum_{\theta \in \mathrm{Indec}_{n+1}} q^{\mathrm{inv}(\theta)}$$

Received by the editors January 12, 2015; revised January 13, 2016.
Published electronically February 23, 2016.
The second author was supported by NSERC (Canada).
AMS subject classification: **05A15**, 05A19.
Keywords: permutation, indecomposable permutation, subgroups of free groups.

enumerating indecomposable permutations by inversions. We show that this polynomial, corrected by the factor $(q-1)^{n+1}q^{((n+1)(n-2))/2}$, 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 2.1).

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 that 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 6.4, 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 given by $q^{n(n+1)}C_n(1/q)$, where $C_n(q)$ (defined recursively by $C_0(q) = 1$ and $C_{n+1}(q) = \sum_{k=0}^{n} q^{(k+1)(n-k)}C_k(q)C_{n-k}(q)$) is the Carlitz–Riordan q-analogue of the n-th Catalan number $\binom{2n}{n}\frac{1}{n+1}$, a result that was implicit in Reineke's article [R]. We use several results of our previous paper: a description of 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], and a noncommutative version of Buchberger's algorithm for the construction of Gröbner bases.

The paper is organized as follows. Section 2 states our main result, Theorem 2.1, which enumerates right ideals of codimension n in 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. Section 3 discusses inversions and hooks. Section 4 recalls and proves a result of Haglund enumerating specific invertible matrices. Sections 5–7 are devoted to prefix-free and prefix-closed sets and some of their properties. Sections 8–10 discuss right congruences in free monoids and indecomposable permutations associated with regular right congruences of the free monoid $\{a, b\}^*$. Sections 11 and 12 present right ideals in $\mathbb{F}_q\langle a, b\rangle$ and $\mathbb{F}_q\langle a, b, a^{-1}, b^{-1}\rangle$. The remaining sections contain a proof of Theorem 2.1 and a few concluding remarks.

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, *i.e.,* 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 $\mathrm{inv}(\sigma)$ 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.

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

Theorem 2.1 *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*

$$(q-1)^{n+1} q^{\frac{(n+1)(n-2)}{2}} \sum_{\theta \in \mathrm{Indec}_{n+1}} q^{\mathrm{inv}(\theta)}, \tag{2.1}$$

with Indec_{n+1} *denoting the subset of all indecomposable permutations in S_{n+1}. Equivalently, formula* (2.1) *is also given by*

$$\left(\frac{q-1}{q}\right)^{n+1} \sum_{\theta \in \mathrm{Indec}_{n+1}} q^{p(\theta)}, \tag{2.2}$$

where $p(\theta)$ is equal to the cardinality of the set

$$\left\{ (i,j) : 1 \le i, j \le n+1 \quad \text{and } j < \theta(i) \text{ or } i > \theta^{-1}(j) \right\}.$$

The first polynomials $P_{n+1}(q) = \sum_{\theta \in \mathrm{Indec}_{n+1}} q^{\mathrm{inv}(\theta)}$ 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 $\{1, \ldots, n+m\}$ defined by $\alpha \cdot \beta(i) = \alpha(i)$ if $i \in \{1, \ldots, m\}$ and by $\alpha \cdot \beta(i) = m + \beta(i-m)$ if $i \in \{m+1, \ldots, m+n\}$. The disjoint union $\mathcal{M} = \bigcup_{n \in \mathbb{N}} S_n$ (with S_0 acting on the empty set), endowed with shifted concatenation, is the free (noncommutative) monoid generated by the set $\bigcup_{n=1}^{\infty} \mathrm{Indec}_n$ of all indecomposable permutations; see [Cm]. Since $\mathrm{inv}(\alpha \cdot \beta) = \mathrm{inv}(\alpha) + \mathrm{inv}(\beta)$, the map $\mathrm{inv}: \mathcal{M} \to \mathbb{N}$ defines a morphism from the monoid $\mathcal{M}$ onto the additive monoid $\mathbb{N}$. Freeness of $\mathcal{M}$ over $\bigcup_{n=1}^{\infty} \mathrm{Indec}_n$ implies the formula

$$\sum_{n \in \mathbb{N}} t^n \sum_{\sigma \in S_n} q^{\mathrm{inv}(\sigma)} = \sum_{k=0}^{\infty} \Big(\sum_{n=1}^{\infty} t^n \sum_{\sigma \in \mathrm{Indec}_n} q^{\mathrm{inv}(\sigma)} \Big)^k = \Big(1 - \sum_{n=1}^{\infty} t^n \sum_{\sigma \in \mathrm{Indec}_n} q^{\mathrm{inv}(\sigma)} \Big)^{-1}$$

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

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

where the right-hand side involves the classical q–analogue of the factorial function. Therefore, we have

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

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 $i, 1 \le i \le n$, 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 $v = (v_1, \ldots, v_n)$.) A *hook* of a coefficient 1 in such a matrix is the set of 0 s that are located either on the same row at its left or on the same column

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

Figure 1

and below it. In other words, the hook associated with $(i, \sigma(i))$ is the set of entries with coordinates (i, j), $j < \sigma(i)$, or $(k, \sigma(i))$, $k > i$. Setting $j = \sigma(i)$, we have $\{(k, \sigma(i), k > i\} = \{(k, j), k > \sigma^{-1}(j)\}$. This shows that the number $p(\theta)$ introduced in Theorem 2.1 enumerates the union of all hooks of the indecomposable permutation $\theta \in S_{n+1}$.

Hooks are in general not disjoint and can also be enumerated as follows. An inversion of σ gives rise to a pair of 1 s (in the permutation matrix of σ) that are incomparable with respect to the order on entries induced by the natural order of $\mathbb{N} \times \mathbb{N}$ (*i.e.*, 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 $\mathrm{inv}(\sigma)$ and by $v(\sigma)$ the number of inversions and of versions of σ. We have

$$p(\sigma) = 2\,\mathrm{inv}(\sigma) + v(\sigma) = \mathrm{inv}(\sigma) + \binom{n}{2}. \tag{3.1}$$

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 $\mathrm{inv}(\sigma) + v(\sigma)$ is equal to the number $\binom{n}{2}$ of all 2-subsets in $\{1, \ldots, n\}$ shows the second equality. Rewriting the equality $p(\theta) = \mathrm{inv}(\theta) + \binom{n+1}{2}$ as

$$p(\theta) - n - 1 = \mathrm{inv}(\theta) + \frac{(n+1)(n-2)}{2},$$

we deduce equality of formulae (2.1) and (2.2) from (3.1) and the trivial identity

$$\frac{(n+1)(n-2)}{2} + n + 1 = \frac{n(n+1)}{2}.$$

4 A Theorem of Haglund

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

Theorem 4.1 *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.*

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

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

For later use, we denote by $H_\lambda(q)$ the polynomial appearing in Theorem 4.1. 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 2.1.

We illustrate Haglund's theorem with 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 Figure 2. The function $p(\sigma)$ has respectively the values 3, 4, 4, and 5, as

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

Figure 2

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 4.1

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

Given a partition λ with n parts $\lambda_1 \le \lambda_2 \le \cdots \le \lambda_n = n$ satisfying $\lambda_i \ge i$, we claim that we have

$$H_\lambda(q) = q^{\binom{n}{2}} \prod_{i=1}^{n} (q^{\lambda_i + 1 - i} - 1). \tag{4.1}$$

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 (4.1) is clearly true if λ is reduced to a unique part $\lambda_1 = 1$ where an invertible matrix associated with λ is simply a non-zero element of $\mathbb{F}_q$. Now consider 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 the first row and the j_1-th column in the resulting matrix, we get an invertible matrix A' associated with the partition λ' with $n-1$ parts $\lambda_2 - 1, \dots, \lambda_n - 1$. Thus, we have by

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

induction

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

which simplifies to (4.1).

Now we associate with 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 now imply equality between formula (4.1) and the expression $(q-1)^n \sum_\sigma q^{p(\sigma)}$ given by Haglund's Theorem. ■

Remark 4.2 Formula (4.1) is in fact much more suited for computing $H_\lambda(q)$ than the expression given in Theorem 4.1.

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 $u = u_1 \cdots u_n$ and $v = v_1 \cdots v_m$ in A^* is given by the concatenation $uv = u_1 \cdots u_n v_1 \cdots v_m$. 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^* that 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 with 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

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

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

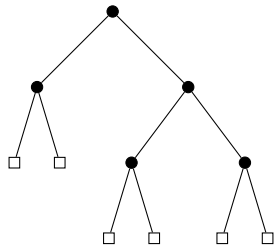

Figure 3: The prefix-free set $C = \{a^2, ab, ba^2, bab, b^2a, b^3\}$ corresponding to the set of prefixes $P = \{1, a, b, ba, b^2\}$. Left edges are encoded by a, right edges by b.

empty word, prefixes of a vertex-word are its ancestors. 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.

Now consider 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 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 with $p \in P_b$ 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 $C_a = C_b = P = \varnothing$. Assuming, here and in the sequel, that C is nontrivial, we can define $\mu\colon C \to P$ 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.

Example 5.1 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 3. 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 sets.[2]

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

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

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

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. ■

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 6.2 *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 $i_1, \ldots, i_k$ of all k elements in C_a among the alphabetically ordered elements of C and by the corresponding lengths $l_1, \ldots, l_k$ of the associated left branches.*

The integers $i_1, \ldots, i_k$ and $l_1, \ldots, l_k$ of Lemma 6.2 can also be described as follows: if $C = \{c_1, \ldots, c_{n+1}\}$ with $c_1 < c_2 < \cdots < c_n < c_{n+1}$, then $C_a = \{c_{i_1}, \ldots, c_{i_k}\}$ and $l_j = \text{length}(c_{i_j}) - \text{length}(\mu_a(c_{i_j}))$. We leave the proof of Lemma 6.2 to the reader.

Example 6.3 In the running example of Figure 3 we have $k = 3$, $l_1 = 2$, $l_2 = 2$, $l_3 = 1$, $i_1 = 1$, $i_2 = 3$, $i_3 = 5$.

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

Lemma 6.4 *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*

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

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

for the set of all words in C that 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 $k = |\widetilde{C}_a|$ elements in $\widetilde{C}_a = \{c_{i_1}, \dots, c_{i_k}\} \subset C$. We introduce the set $\mathcal{M} = \{(p, c) \in (P_b \setminus \{1\}) \times C_b,\ p < c\}$ containing $M = |\mathcal{M}|$ elements. Then

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

Example 6.5 Our running example of Figure 3 yields

$$\mathcal{M} = \big\{(b, bab), (b, b^3), (b^2, b^3)\big\}$$

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 We give a bijective proof of the identity

$$(n+1)k = \sum_{h=1}^{k} i_h + M + (n + 1 - k) + \frac{k(k-1)}{2} \tag{6.1}$$

equivalent to Lemma 6.4. The left side of (6.1) is the cardinality of the set $C \times \widetilde{C}_a$. The right side is the cardinality of the disjoint union $E = E_1 \cup E_2 \cup E_3 \cup E_4$, where

$$E_1 = \{(c_1, c_2) \in C \times \widetilde{C}_a, c_1 \le c_2\}, \qquad E_2 = \mathcal{M} = \{(p, c) \in (P_b \setminus 1) \times C_b,\ p < c\},$$
$$E_3 = (C \setminus \widetilde{C}_a) = C_b, \qquad E_4 = \{(c_1, c_2) \in \widetilde{C}_a \times \widetilde{C}_a, c_1 < c_2\}.$$

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

$$F_{\le} = E_1 = \{(c_1, c_2) \in C \times \widetilde{C}_a, c_1 \le c_2\},$$
$$F_{>} = \{(c_1, c_2) \in C \times \widetilde{C}_a, c_1 > c_2\}.$$

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

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

defines a bijective map. ∎

7 Twisted Alphabetical Order

7.1 Twisting a Total Order

Suppose that we have a set E with a partition $E = \bigcup_{i \in I} E_i$, 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 $y \in E_j \ne E_i$ with $i < j$.

Call a subset E' of an ordered set E an *interval* if $b \in E'$ for every $b \in E$ such that there exists $a, c \in E'$ with $a < b < c$. A set I indexing disjoint non-empty intervals E_i partitioning a totally ordered set $E = \bigcup_{i \in I} E_i$ 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

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

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* $\bigcup_{i\in I} E_i$*)*. The restriction of $\prec$ to each E_i is the opposite order of $<$ on E_i, and the set I is ordered by $<$.

Remark 7.1 (i) It is also possible to twist the order on $E = \bigcup_{i\in I}$ according to the set of indices: $x \precsim y$ 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 $E = \bigcup_{i\in I} E_i$ 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 $E \setminus E_i$.

Now consider $\{a, b\}^*$ with the alphabetical order. We partition $\{a, b\}^*$ into equivalence classes given by $u \sim v$ if $ua^* \cap va^* \neq \varnothing$. Elements in a common equivalence class thus differ 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 $w \in \{1\} \cup \{a, b\}^* b$ does not end with a and such an element w is the lexicographically smallest element in its equivalence class. If a word $w \in \{a, b\}^* a$ ends with a last letter a, its equivalence class is given by $\mu_a(w)a^*$.

For later use, we mention 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 7.2 *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 $h \in \{1, \ldots, i-1\}$. The easy verification is left to the reader. ∎

Lemma 7.2 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 $w \notin \{a, b\}^* a$ (*i.e.*, μ_a always erases a final maximal (perhaps empty) string of consecutive letters a in a word). Observe that every equivalence class has a unique largest element but no smallest element with respect to the twisted order.

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

Lemma 7.3 (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* $u < v$

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

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.

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

7.2 Prefix-free Sets and the Twisted Alphabetical Order

Lemma 7.4 *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* (i.e., *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 $d \leq c$.*

Example 7.5 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 Lemma 7.3(iii).

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' thus define two different equivalence classes $\mu_a(c'')a^*$ and $\mu_a(c')a^*$, and we can apply of Lemma 7.3(ii). ∎

8 Right Congruences of a Free Monoid

A *right congruence* of a monoid is an equivalence relation $\equiv$ that 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 quotient.[3] 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 $f : C \to P$ 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, [BR, Proposition 7]).

Example 8.1 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 3. 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

[3] A 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.

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

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 9.1 *A permutation $\sigma \in S_n$ with successive positions $i_1 < \cdots < i_k$ 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 always has $i_1 = 1$ 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 $w = a_1 \cdots a_n$ involving n distinct letters of a totally ordered alphabet. We denote by $\mathrm{st}(w) = i_1 \cdots i_n \in S_n$ 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 $\{a_1, \dots, a_n\}$. For example, the standard permutation of $w = 3649$ is given by $\mathrm{st}(w) = 1324$.

Lemma 9.2 *Let $\theta \in S_n$ have successive left-to-right maxima in positions $i_1, \dots, i_k$, with values $j_1, \dots, j_k$. Let $\sigma = \mathrm{st}(w)$, where*

$$w = \sigma(2) \cdots \sigma(i_2 - 1)\sigma(i_2 + 1) \cdots \sigma(i_k - 1)\sigma(i_k + 1) \cdots \sigma(n)$$

is obtained from the word $\theta = \sigma(1) \cdots \sigma(n)$ by removal of the left-to-right maxima $j_1, \dots, j_k$. Then

$$p(\theta) = p(\sigma) + kn - \frac{k(k+1)}{2} + \sum_{1 \leq s \leq k} (j_s - i_s),$$

where $p(\sigma)$ is the cardinality of the union of all hooks (see Section 3).

Example 9.3 Consider $\theta = \underline{3}25\underline{4}6\underline{1}$, with underlined left-to-right maxima. We have $i_1 = 1$, $i_2 = 3$, $i_3 = 5$, $j_1 = 3$, $j_2 = 5$, $j_3 = 6$, $w = 241$, $\sigma = \mathrm{st}(w) = 231$. The matrices of θ and σ (with hooks represented by boldfaced 0 s) are

$$\begin{pmatrix} \mathbf{0} & \mathbf{0} & 1 & 0 & 0 & 0 \\ \mathbf{0} & 1 & \mathbf{0} & 0 & 0 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 \\ 1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{pmatrix} \text{ and } \begin{pmatrix} \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{0} & 1 \\ 1 & \mathbf{0} & \mathbf{0} \end{pmatrix}.$$

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

We see that $p(\theta) = 22$, $p(\sigma) = 5$, $k = 3$, $n = 6$. The equality

$$22 = 5 + 3 \cdot 6 - \frac{3 \cdot 4}{2} + (3-1) + (5-3) + (6-5)$$

illustrates Lemma 9.2.

Proof The matrix of θ looks like the following,

$$\begin{array}{cccccccccccccc}
0 & \cdots & 0 & 1 & & & & & & & & & & \\
* & \cdots & * & 0 & & & & & & & & & & \\
\vdots & \vdots & \vdots & \vdots & & & & & & & & & & \\
* & \cdots & * & 0 & & & & & & & & & & \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & & & & & & \\
* & \cdots & * & 0 & * & \cdots & * & 0 & & & & & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & & & & & \\
* & \cdots & * & 0 & * & \cdots & * & 0 & & & & & & \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & \cdots & 0 & \cdots & 0 & 1 \\
* & \cdots & * & 0 & * & \cdots & * & 0 & \cdots & \cdots & * & \cdots & * & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \cdots & \vdots & \vdots & \vdots & \vdots \\
* & \cdots & * & 0 & * & \cdots & * & 0 & \cdots & \cdots & * & \cdots & * & 0
\end{array}$$

where the 1 s represent the left-to-right maxima, the $*$ s represent the possible positions of the other 1 s, and the north-eastern region (which is empty on the figure) has only 0 s. Observe that the matrix of σ is the submatrix obtained by removing the rows and the columns containing all 1 s displayed in the figure and corresponding to all left-to-right maxima. The definition of $p(\sigma)$ (given in Section 3) shows that the difference $p(\theta) - p(\sigma)$ is equal to the number of 0 s in the figure. Since the row (resp. column) coordinates of the left-to-right maxima are $i_1, \ldots, i_k$ (resp. $j_1, \ldots, j_k$), this number of 0 s is obtained by summing up the rows of 0 s, columns of 0 s, and by subtracting the 0 s at intersections (which have been counted twice). Thus, $j_1 - 1 + j_2 - 1 + \cdots + j_k - 1 + (n - i_1) + (n - i_2) + \cdots + (n - i_k) - (1 + 2 + \cdots + k - 1)$ gives the formula of Lemma 9.2. ∎

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 that 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 $a^*u \cap a^*v \neq \varnothing$. Indeed, right-multiplication by b fails to yield the class a^* represented by the empty word.)

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

Proposition 10.1 *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.*

Proof A subgroup H of a free group over A gives 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 A^* 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. ∎

The bijection of Proposition 10.1 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 $(\widetilde{\Gamma}, v_*)$ with a marked base-vertex v_* of the connected graph Γ consisting 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 a connected covering $(\widetilde{\Gamma}, v_*)$ is the subgroup of all elements in $\langle a, b\rangle$ which lift to closed paths of $\widetilde{\Gamma}$ starting and ending at v_*. If $\widetilde{\Gamma}$ 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 $\pi_1(\widetilde{\Gamma}, v_*)$ have only finite orbits), one can join an arbitrary initial vertex α of $\widetilde{\Gamma}$ to an arbitrary final vertex ω by a path corresponding to a word in the free monoid $\{a, b\}^*$, *i.e.*, by a path using only positively oriented edges. In particular, such a graph $\widetilde{\Gamma}$ has a canonically defined spanning tree $P = \bigcup_{v \in V(\widetilde{\Gamma})} p_v$, where p_v is the lexicographically smallest path labelled by a word in $\{a, b\}^*$ that joins the marked vertex v_* of $\widetilde{\Gamma}$ to a given vertex v of $\widetilde{\Gamma}$. The set P is prefix-closed and the remaining set of labelled oriented edges in $\widetilde{\Gamma}$ defines a regular right congruence. The corresponding prefix-free set $C = P\{a, b\} \setminus P$ indexes a free generating set of $\pi_1(\widetilde{\Gamma}, v_0)$ 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 $\widetilde{\Gamma}$.

Subgroups of finite index of a free group were first counted by M. 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

Now, we describe a new map between the set of regular right congruences of $\{a, b\}^*$ into n classes and the set of indecomposable permutations of S_{n+1}. This map turns

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

out to be bijective by Theorem 10.3 below. It will play a crucial role in our proof of Theorem 2.1. 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 show,s in particular, that f induces a bijection from C_a onto P_b.

Example 10.2 Looking at the running example (see Figure 3, 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 the restriction of f to C_b 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 representatives 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 now introduce the set $\widetilde{P} = P \cup \{a^{-1}\}$ and we consider the bijection ϕ from C onto $\widetilde{P}$ that 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 $C = \{c_1 < c_2 < \cdots < c_{n+1}\}$ and $\widetilde{P} = \{p_1 \prec p_2 \prec \cdots \prec p_{n+1}\}$ 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 10.3 *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}.*

Example 10.4 We illustrate Theorem 10.3 by considering the sets C, P of our running example represented in Figure 3 together with the right congruence into 5 classes defined by

$$a^2 \equiv 1, \quad ba^2 \equiv b, \quad b^2a \equiv b^2, \quad ab \equiv 1, \quad bab \equiv ba, \quad b^3 \equiv a.$$

We have

$$C = \{a^2 < ab < ba^2 < bab < b^2a < b^3\},$$

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

$$f(a^2) = 1, \quad f(ba^2) = b, \quad f(b^2a) = b^2,$$
$$f(ab) = 1, \quad f(bab) = ba, \quad f(b^3) = a.$$

Therefore, with $\widetilde{P} = \{a \prec 1 \prec a^{-1} \prec ba \prec b \prec b^2\}$, we have $\phi = f$ except that $\phi(a^2) = a^{-1}$. Therefore, ϕ is the bijection $C \to \widetilde{P}$ 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 $\widetilde{P}$, we get the following indecomposable permutation in S_6:

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

Proof We first prove that the permutation θ (associated with 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 $\widetilde{P}$) 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 now apply Lemma 9.1 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

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

where a^{-1} is by convention the lexicographically smallest element of $\widetilde{P}$. Indecomposability of ϕ thus amounts to the inequality by Lemma 9.1

$$|C(\leq c)| < |\widetilde{P}(< c)| \tag{10.1}$$

for all $c \in C_a$, where

$$\widetilde{P}(< c) = \{p \in \widetilde{P}, p < c \text{ lexicographically}\},$$
$$C(\leq c) = \{c' \in C_a, c' \leq c \text{ lexicographically}\}.$$

The identity

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

where

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

shows that the strict inequality (10.1) amounts to

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

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

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 with every regular right congruence $\equiv$. It is now enough to establish injectivity of this map. Surjectivity then follows 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 $i_1, \ldots, i_k$, with values $j_1, \ldots, j_k$. 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 6.2, the tree defined by the maximal prefix-free set C and its associated prefix-closed set P are thus completely determined by the numbers $i_1, \ldots, i_k$ and $j_1, \ldots, j_k$. From C and P we immediately recover the function f on C_a. The bijection $f : C_b \to P_a$ is encoded by the standard permutation $\mathrm{st}(\theta)$ (as defined in Lemma 9.2) of θ. The equivalence relation $\equiv$ is thus completely determined by θ. ∎

Remark 10.5 It is not difficult to invert the map $\equiv \mapsto \theta$ of Theorem 10.3. 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 $\mathrm{st}(\theta)$ 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 10.3.

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 10.3 gives by restriction a bijection between the set of these congruences and the set of bijections $\alpha : C_b \to P_a$ satisfying $\alpha(c) < c$. Indeed, we have $\alpha(c) = \phi(c) = f(c) < c$ 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 with 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, positions and values of left-to-right maxima of the permutation θ encode the underlying finite maximal prefix-free set C.

We use Lemma 7.3(ii) for ordering (alphabetically) left branches of P. We denote by $l_1, \ldots, l_k$ the corresponding lengths and we set $s_i = l_1 + \cdots + l_i$.

We observe the following facts for later use. If $i_1, \ldots, i_k$, $j_1, \ldots, j_k$ are as in Lemma 9.2 applied to a permutation in S_{n+1}, then the previous proof implies

$$C_a = \{c_{i_1} < \cdots < c_{i_k}\} \quad \text{and} \quad \{p_{i_1} \prec \cdots \prec p_{i_k}\} = \{\phi(c_{i_1}) \prec \cdots \prec \phi(c_{i_k})\}.$$

Hence j_h is the rank of $\phi(c_{i_h})$ in the set $\widetilde{P}$ 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,

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

$j_h = s_h + 1$ for any $h = 1, \dots, k$. Lemma 9.2, 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

$$p(\theta) = p(\sigma) + (n+1)k - \frac{k(k-1)}{2} - \sum_h i_h + \sum_h s_h. \tag{10.2}$$

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 $I\backslash\mathbb{F}_q\langle a, b\rangle$ 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 $I\backslash\mathbb{F}_q\langle a, b\rangle$ are therefore $|P| \times |P|$ matrices with coefficients $\mu(x)_{p,q}$ (indexed by $P \times P$) defined by

$$\mu(x)_{p,q} = \begin{cases} 1 & \text{if } px = q, \\ 0 & \text{if } px \in P,\ px \neq q, \\ \alpha_{c,q} & \text{if } px = c \in C,\ q < c, \\ 0 & \text{if } px = c \in C,\ q > c. \end{cases} \tag{11.1}$$

Remark 11.1 (i) Since there are $q^{\sum_{c\in C} \sum_{p\in P, p<c} 1}$ possibilities for the choice of $\mu(a)$ and $\mu(b)$ associated with a fixed prefix-closed set P of n elements, the polynomial enumerating all right ideals of codimension n in $\mathbb{F}_q\langle a, b\rangle$ evaluates to the Catalan number $\binom{2n}{n}\frac{1}{n+1}$ at $q = 1$; see [BR].

(ii) The rank of a matrix $\mu(x)$ (for $x \in \{a, b\}$) equals at least $|P \cap \{a, b\}^* x|$ with equality achieved for example by nilpotent ideals defined by $\alpha_{c,p} = 0$.

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 $J = I \cap \mathbb{F}_q\langle a, b\rangle$ of codimension n in $\mathbb{F}_q\langle a, b\rangle$ such that the actions of a and b on the quotient $J\backslash\mathbb{F}_q\langle a, b\rangle$ are both linear isomorphisms. We obtain in this way a bijection

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

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 (11.1).

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 $l_i \times l_i$, $i = 1, \ldots, k$. Strictly lower triangular blocks are filled with 0 s except for their last row, which is arbitrary. In other words, only rows of index $s_1, s_2, \ldots$ 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

$$N = \sum_{i=1,\ldots,k} (s_i - 1) = \sum_{i=1,\ldots,k} s_i - k \tag{13.1}$$

and where $s_i = l_1 + \cdots + l_i$ 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.

Example 13.1 In our running example given by Figure 3, the matrix $\mu(a)$ is of the form

	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	$\times$	$\times$	$\times$	$\times$	$*$,

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 $N = (s_1 - 1) + (s_2 - 1) + (s_3 - 1) = 1 + 3 + 4 = 8$.

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

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

$$\lambda_c = |\{q \in P_a, q < c\}| \tag{13.2}$$

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 $< b^h$.

Example 13.2 In our running example underlying Figure 3, 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 the 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 (13.2). 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

$$M = \left|\left\{(p, c) \in (P_b \setminus \{1\}) \times C_b,\ p < c\right\}\right|$$

and H_λ is as in Section 4.1.

Example 13.3 The matrix $\mu(b)$ of our running example looks like

	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	$\times$	$\times$	$\times$	$\times$	$\times$.

The associated submatrix obtained by removing both rows and columns containing 1 s is the leftmost matrix in Figure 2.

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

14 Proof of Theorem 2.1

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 with a maximal prefix-free set C are defined as in Section 13.

Applying Haglund's Theorem (Theorem 4.1), 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 (as defined in Subsection 10.3) may be identified with σ. Using the definition $N = -k + \sum_{j=1}^k s_j$ (*cf.* formula (13.1)) and the equality

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

given by Lemma 6.4, 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 (10.2) 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

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

A comparison with formula (2.2) ends the proof. ∎

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press

15 Conclusion

Our main result can also be interpreted as a cellular decomposition of the set of right ideals of codimension n in $\mathbb{F}\langle a, a, a^{-1}, b^{-1}\rangle$ 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

$$\left(\mathbb{F}^*\right)^{n+1} \times \mathbb{F}^{\frac{(n+1)(n-2)}{2}+\mathrm{inv}(\theta)}.$$

There is 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].

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 [LLMPSZ].

References

[AS] M. Aguiar and F. Sottile, *Structure of the Malvenuto-Reutenauer Hopf algebra of permutations.* Adv. Math. **191**(2005), 225–275. http://dx.doi.org/10.1016/j.aim.2004.03.007

[B] M. Bona, *Combinatorics of permutations.* Second ed., Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 2012. http://dx.doi.org/10.1201/b12210

[BPR] J. Berstel, D. Perrin, and C. Reutenauer, *Codes and automata.* Enclyclopedia and its Applications, 129, Cambridge University Press, Cambridge, 2010.

[BR] R. Bacher and C. Reutenauer, *The number of right ideals of given codimension over a finite field.* In: Noncommutative birational geometry, representations and combinatorics, Contemp. Math., 592, American Mathematical Society, Providence, RI, 2013, pp. 1-18. http://dx.doi.org/10.1090/conm/592/11865

[C] P. M. Cohn, *Free ideal rings.* J. Algebra **1**(1964), 47–69. http://dx.doi.org/10.1016/0021-8693(64)90007-9

[Cm] L. Comtet, *Sur les coefficients de l'inverse de la série formelle* $\sum n!t^n$. C. R. Acad. Sci. Paris Sér. A-B **275** (1972), A569–A572.

[Cr] R. Cori, *Indecomposable permutations, hypermaps and labeled Dyck paths.* J. Combin. Theory Ser. A **116**(2009), no. 8, 1326–1343. http://dx.doi.org/10.1016/j.jcta.2009.02.008

[DF1] A. W. M. Dress and R. Franz, *Parametrizing the subgroups of finite index in a free group and related topics.* Bayreuth. Math. Schr. **20**(1985), 1–8.

[DF2] ———, *Zur Parametrisierung von Untergruppen freier Gruppen.* Beiträge Algebra Geom. **24**(1987), 125–134.

[GR] A. M. Garsia and J. B. Remmel, *q-counting rook configurations and a formula of Frobenius.* J. Combin. Theory Ser. A **41**(1986), no. 2, 246–275. http://dx.doi.org/10.1016/0097-3165(86)90083-X

[Hg] J. Haglund, *q-rooks polynomials and matrices over finite fields.* Adv. in Appl. Math. **20**(1998), no. 4, 450–487. http://dx.doi.org/10.1006/aama.1998.0582

[H] M. Hall, Jr., *Subgroups of finite index in free groups.* Canad. J. Math. **1**(1949), 187–190. http://dx.doi.org/10.4153/CJM-1949-017-2

[LLMPSZ] 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.* J. Comb. **2**(2011), no. 3, 355–395. http://dx.doi.org/10.4310/JOC.2011.v2.n3.a2

[OEIS] N. J. A. Sloane, *The electronic encyclopedia of integer sequences.* http://oeis.org

[OR] P. Ossona de Mendez and P. Rosenstiehl, *Transitivity and connectivity of permutations*. Combinatorica **24**(2004), no. 3, 487–501. http://dx.doi.org/10.1007/s00493-004-0029-4

[P] T. Pirashvili, *Sets with two associative operations*. Cent. Eur. J. Math. **1**(2003), no. 2, 169–183. http://dx.doi.org/10.2478/BF02476006

[PR] S. Poirier and C. Reutenauer, *Algèbre de Hopf de tableaux*. Ann. Sci. Math. Québec **19**(1995), no. 1, 79–90.

[R] M. Reineke, *Cohomology of noncommutative Hilbert schemes*. Algebr. Represent. Theory **8**(2005), no. 4, 541–561. http://dx.doi.org/10.1007/s10468-005-8762-y

[Si] T. Sillke, *Zur Kombinatorik von Permutationen*, Séminaire Lotharingien de Combinatoire (Oberfranken, 1990), Publ. Inst. Rech. Math. Av., 413, Univ. Louis Pasteur, Strasbourg, 1990, pp. 111-119.

Univ. Grenoble Alpes, Institut Fourier (CNRS UMR 5582), 100 rue des Maths, F-38000 Grenoble, France
e-mail: roland.bacher@ujf-grenoble.fr

Département de Mathématiques, UQAM, Case Postale 8888 Succ. Centre-ville, Montréal H3C 3P8, Québec
e-mail: reutenauer.christophe@uqam.ca

https://doi.org/10.4153/CJM-2016-004-8 Published online by Cambridge University Press