Contemporary Mathematics
Volume **592**, 2013
http://dx.doi.org/10.1090/conm/592/11865

The number of right ideals of given codimension over a finite field

Roland Bacher and Christophe Reutenauer

Abstract. The number of right ideals of codimension n of the ring of non-commutative polynomials in two variables over the finite field $\mathbb{F}_q$ is a polynomial q-analogue of the n-th Catalan number. A generalization involving a q-analogue of Fuß-Catalan numbers holds for more variables. We discuss also a few aspects of right congruences over a free monoid.

1. Introduction

A free associative algebra A is a free ideal ring by a theorem of P.M.Cohn. Every right ideal $I = IA$ is thus a free right module over A. Special bases of these ideals have been constructed in [**BR**], using combinatorics on words and linear recurrences for noncommutative rational series due to Schützenberger [**S**].

We use this construction for enumerating right ideals of codimension n of a free associative algebra over a finite field. It turns out that in the case of two variables, the number of such ideals is given by a q-analogue of Catalan numbers which is, up to a simple transformation, due to Carlitz and Riordan (see Theorem 1). For $m > 2$ variables, we get q-analogues of Fuß-Catalan numbers enumerating rooted m-ary trees (see Theorem 2). These results are implicit in the article of Marcus Reineke [**R**] [1]. Our construction, a non-commutative version of Buchberger's algorithm for Gröbner bases, gives a short proof of them, taking advantage of the fact that the free associative algebra is a free ideal ring.

Motivations and ideas come from [**B**] containing the enumeration of noncommutative rational series of given *rank* (in the terminology of Michel Fliess, see [**BR**]; it is called *complexity* in [**B**]) over a finite field.

Our paper is organized as follows:

Chapter 2 is a brief review of Catalan and q-Catalan numbers.

Chapter 3 states our main results, Theorem 1 enumerating right ideals of codimension n over $\mathbb{F}_q\langle x, y\rangle$ and Theorem 2 giving the corresponding formula over $\mathbb{F}_q\langle x_1, \ldots, x_m\rangle$. They are proven in Chapters 9 and 10.

Chapters 4-8 introduce a few (mostly well-known) concepts and tools for the proofs.

[1] Actually, he gives a decomposition of the noncommutative Hilbert scheme (whose points are, for fixed n and m, the right ideals of codimension n of the free associative algebra with m generators) into affine cells.

Chapter 11 treats a few aspects of right congruences (mostly over $\{x,y\}^*$) a combinatorial analogue of right ideals.

2. Catalan numbers and q-analogues

The *n-th Catalan number* C_n is classically given by the formula $\frac{1}{n+1}\binom{2n}{n}$. It counts several combinatorial objects, including trees, triangulations by diagonals of a convex polygon and Dyck paths. Exercise 6.19 of [**St**] consists of a huge list of such objects. Carlitz and Riordan introduced a polynomial $C_n(q)$ of degree $\frac{n(n-1)}{2}$ which reduces to C_n for $q = 1$ and is therefore called a *q-analogue* of C_n. These polynomials are defined by the recursion $C_0(q) = 1$ and $C_{n+1}(q) = \sum_{k=0}^{n} q^{(k+1)(n-k)} C_k(q)C_{n-k}(q)$ and have a combinatorial interpretation in terms of Dyck paths and their area.

Notice that a second polynomial q-analogue of Catalan numbers exists in the literature. It is obtained by replacing every occurence of an integer i by its q-analogue $1 + q + \cdots + q^{i-1}$ in the classical definition

$$\frac{(2n)!}{n!(n+1)!} = \frac{(n+2)(n+3)\cdots(2n-1)(2n)}{1\cdot 2\cdots(n-1)\cdot n}$$

of C_n. For all this, see [**St**] page 235.

3. Enumeration of right ideals

We denote by $\mathbb{F}\langle x, y\rangle$ the ring of noncommutative polynomials in two variables x, y over the field $\mathbb{F} = \mathbb{F}_q$ with q elements. We write $A_n(q)$ for the number of right ideals with codimension n of $\mathbb{F}\langle x, y\rangle$.

Theorem 1. *The polynomials $A_0(q), A_1(q), \ldots$ with $A_n(q)$ counting the number of right-ideals of codimension n in $\mathbb{F}_q\langle x, y\rangle$ satisfy the recursion $A_0(q) = 1$ and $A_{n+1}(q) = \sum_{k=0}^{n} q^{(k+1)(n+2-k)} A_k(q)A_{n-k}(q)$.*

The polynomial $A_n(q)$ is a q-analogue of the Catalan number C_n related to the q-analogue $C_n(q)$ of Carlitz and Riordan by the formula $A_n(q) = q^{n(n+1)}C_n(1/q)$.

The first few values of $A_n(q)$ are $A_1(q) = q^2$, $A_2(q) = q^5(1 + q)$, $A_3(q) = q^9(1 + 2q + q^2 + q^3)$, $A_4(q) = q^{14}(1 + 3q + 3q^2 + 3q^3 + 2q^4 + q^5 + q^6)$. It is easy to verify that the degree of $A_n(q)$ is $n(n + 1)$ and that its lowest monomial is of degree $\frac{n(n+3)}{2}$.

Theorem 1 will be proved in Section 9.

For the number $A_{m,n}(q)$ of right ideals of codimension n in $\mathbb{F}_q\langle x_1, \ldots, x_m\rangle$ we have the following generalization:

Theorem 2. *The number $A_{m,n}(q)$ of right ideals of codimension n in the free associative algebra $\mathbb{F}_q\langle x_1, \ldots, x_m\rangle$ on m generators is a q-analogue of the Fuß-Catalan number $\frac{1}{(m-1)n+1}\binom{mn}{n}$ enumerating m-ary trees with n interior vertices. It satisfies the recurrence: $A_{m,0}(q) = 1$ and*

$$A_{m,n+1}(q) = \sum_{n_1+\cdots+n_m=n} A_{m,n_1}(q)\cdots A_{m,n_m}(q)q^{N(n_1,\ldots,n_m)}$$

where $N(n_1, \ldots, n_m) = m + (2m - 2)n_1 + (2m - 3)n_2 + \cdots (m - 1)n_m + (m - 1)(n_1n_2 + n_1n_3 + \cdots + n_1n_m + \cdots + n_{m-1}n_m)$.

Section 10 contains the proof and a remark on computational aspects.

4. Prefix-free and prefix-closed sets

Given a finite set X of noncommuting variables, we denote by $\mathbb{F}\langle X\rangle$ the ring of noncommutative polynomials with variables X over a field $\mathbb{F}$. According to a result of P.M.Cohn [**C**], each right ideal $I = I\mathbb{F}\langle X\rangle$ in $\mathbb{F}\langle X\rangle$ is free as a right $\mathbb{F}\langle X\rangle$-module.

We follow [**BR**], Section 2.3, for the construction of bases. To the purpose we introduce the free monoid X^* generated by a finite set X. The set X is called the *alphabet* and elements of X^* are *words*. We identify henceforth a word $w \in X^*$ with the corresponding (non-commutative) monomial of $\mathbb{F}\langle X\rangle$. A word u is a *prefix* of a word w if $w = uv$ for some word v. A subset C of X^* is *prefix-free* if no element of C is a proper prefix of another element of C. Notice that prefix-free sets are called "prefix sets"in [**BR**] and [**BPR**]. A subset P of X^* is *prefix-closed* if P contains all prefixes of its elements. Equivalently, $P \subset X^*$ is prefix-closed if $u \in P$ whenever there exists $v \in X^*$ such that $uv \in P$. In particular, a non-empty prefix-closed set contains the empty word representing the identity of the monoid X^*. We denote the empty word by 1 in the sequel. 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 CX^* intersects every (non-empty) right ideal $I = IX^*$ of the monoid X^*. (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 $I\mathcal{M} = I$.) Indeed a prefix-free set C giving rise to a right ideal CX^* not intersecting a right ideal I of X^* 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 CX^* which is disjoint from the right ideal gX^*. A third 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 w of $X^* \setminus C$ contains either an element of C as a proper prefix or is contained as a proper prefix in an element of C.

PROPOSITION 4.1. *The map $C \mapsto P = X^* \setminus CX^*$ defines a canonical bijection between maximal prefix-free sets and prefix-closed sets containing no (non-empty) right ideals of X^*.*

Its restriction to finite maximal prefix-free sets induces a bijection beween finite maximal prefix-free sets and finite prefix-closed sets.

We leave the easy proof to the reader.

The map $C \mapsto P = X^* \setminus CX^*$ of Proposition 4.1 associates to a maximal prefix-free set C the prefix-closed set P consisting of all proper prefixes of elements in C. (The empty word 1 is by convention a proper prefix of any non-empty word in X^*.) The inverse map is given by $P \mapsto PX \setminus P$ except in the case of the empty prefix-closed set $P = \emptyset$ which corresponds to the maximal prefix-free set $\{1\}$ reduced to the identity of X^*.

Examples:

(1) The set $C = \{x^2, xy, y\}$ is a maximal prefix-free set in $\{x, y\}^*$ with associated prefix-closed set $P = \{1, x\}$.

(2) The set $C = x^*y$ of all words of the form $x^k y$ for $k \geq 0$ an arbitrary natural integer is maximal prefix-free in $\{x, y\}^*$. The associated prefix-closed set $P = X^* \setminus CX^*$ is the free monoid x^* generated by x.

(3) The set $C = x^*y^*yx$ of all words of the form $x^k y^l x$ with $k \geq 0$ and $l \geq 1$ is maximal prefix-free in $\{x, y\}^*$. The associated prefix-closed set $P = X^* \setminus CX^*$ is the set x^*y^* of all words $x^k y^l$ with $k, l \geq 0$.

Observe that $X^* \setminus CX^*$ is not the set of proper prefixes of C if the prefix-free set C is not maximal: The set $X^* \setminus CX^*$ contains then all proper prefixes of elements in C but it contains also all words of X^* having no element of C as a prefix. If C is for example reduced to the singleton $\{x\}$ of $\{x, y\}^*$ then $\{x, y\}^* \setminus x\{x, y\}^*$ is the set $\{1\} \cup y\{x, y\}^*$ given by the empty word 1 which is the unique proper prefix of x and by the set $y\{x, y\}^*$ of all words starting with y.

A maximal prefix-free set C is finite if and only if every infinite word contains an element of C as a prefix. Indeed, a finite prefix-free set C consisting of words of length at most l and containing no prefix of an infinite word $W = w_1w_2w_3 \cdots \in X^{\mathbb{N}}$ can be augmented by adjoining the prefix $w_1w_2 \ldots w_l$ of W. Conversely, given an infinite prefix-free set C, the finite alphabet X contains at least one letter x_1 occuring as a prefix of infinitely many elements in C. Similarly, there exists a second letter x_2, such that x_1x_2 is a prefix of infinitely many elements in C. Iteration of this argument yields an infinite word $w_1w_2 \ldots$ containing no element of C as a prefix.

5. Weak prefix bases for right ideals

A *weak prefix basis* is a subset $\{b_c\}_{c \in C}$ in $\mathbb{F}\langle X\rangle$ with elements of the form

$$b_c = c - \sum_{p \in X^* \setminus CX^*} \alpha_{c,p} p, \;\; \alpha_{c,p} \in \mathbb{F},$$

indexed by elements c of a prefix-free set C.

Every element in a weak prefix basis involves thus exactly one monomial in a prefix-free set C. No monomial appearing in a weak prefix basis contains an element of C as a proper prefix. The following result (see Theorem 3.2 of Chapter 2 in [**BR**]) explains the terminology:

PROPOSITION 5.1. *(i) The right ideal* $I = \sum_{c \in C} b_c \mathbb{F}\langle X\rangle$ *generated by a weak prefix basis* $\{b_c\}_{c \in C}$ *is a free right* $\mathbb{F}\langle X\rangle$*-module over the set* $\{b_c\}_{c \in C}$.

(ii) The quotient $\mathbb{F}\langle X\rangle / I$ *is a free* $\mathbb{F}$*-vector space over the set* $X^* \setminus CX^*$.

(iii) Every right ideal of $\mathbb{F}\langle X\rangle$ *has a weak prefix basis.*

Assertions (i) and (iii) of Proposition 5.1 imply of course Cohn's result on freeness of every right ideal in $\mathbb{F}\langle X\rangle$.

Since $b_c - b'_c = \sum_{p \in X^* \setminus CX^*} (\alpha_{c,p} - \alpha'_{c,p}) p$ for two weak prefix bases $(b_c)_{c \in C}$ and $(b'_c)_{c \in C}$ of an ideal I indexed by a common prefix-free set C, assertion (ii) of Proposition 5.1 determines the coefficients $\alpha_{c,p}$ uniquely for a weak prefix basis of an ideal I with basis elements indexed by a given prefix-free set C. In particular, a right ideal I of $\mathbb{F}\langle X\rangle$ has at most one weak prefix basis indexed by a given prefix-free set C.

Proof of Proposition 5.1 We consider a linear combination

$$\sum_{c \in C} b_c h_c = \sum_{c \in C} \left(c - \sum_{p \in C \setminus CX^*} \alpha_{c,p} p \right) h_c \tag{1}$$

where the coefficients h_c are non-zero polynomials in $\mathbb{F}\langle X\rangle$. Since only finitely many coefficients h_c are non-zero, there exists an index $c_m \in C$ such that the degree of h_{c_m} is maximal among all polynomials h_c involved in (1). Given a monomial w of maximal degree in h_{c_m}, the product $b_{c_m} h_{c_m} = (c_m - \sum_{p \in P} \alpha_{c_m,p} p) h_{c_m}$ involves the monomial $c_m w$ with non-zero coefficient. Since all monomials of the form $c_m u$ arising in products of the form

$$\left(c - \sum_{p \in C \setminus CX^*} \alpha_{c,p} p\right) h_c$$

for $c \neq c_m$ are of strictly smaller degree than $c_m w$, the coefficient of $c_m w$ in (1) is non-zero. This establishes assertion (i).

The identity $cw = \sum_{p \in C \setminus CX^*} \alpha_{c,p} pw$ and induction on the degree show that every monomial is equivalent modulo I to a linear combination of monomials in $X^* \setminus CX^*$. Since non-zero elements of I involve always a monomial having an element of C as a prefix, they are never $\mathbb{F}$-linear combinations of elements in $X^* \setminus CX^*$. The vector space spanned by $X^* \setminus CX^*$ contains thus no I-linear relations and we have $\mathbb{F}\langle X\rangle = I \oplus \bigoplus_{w \in X^* \setminus CX^*} \mathbb{F}w$. This is assertion (ii).

For proving assertion (iii), we endow X with a total order and X^* with the associated graded lexicographical order given by $uv < uw$ if v is shorter than w or if v has a smaller first letter than w in the case where the two words v, w have the same length.

We construct recursively a weak prefix-basis $b_1, b_2, \dots$ of a right ideal I as follows: We order non-zero elements of $\mathbb{F}\langle X\rangle$ partially by comparing largest monomials of supports. We choose for b_1 a minimal non-zero element of I with respect to this partial order. Since we work over a field, we can assume that $b_1 = c_1 + \dots$ where c_1 is the largest monomial involved in b_1. In a similar way, we define b_{i+1} recursively as a minimal element of $I \setminus \left(\sum_{j=1}^{i} b_j \mathbb{F}\langle X\rangle\right)$. This ensures that the maximal monomials $c_1, c_2, \dots$ of $b_1 = c_1 + \dots, b_2 = c_2 + \dots, \dots$ are prefix-free. Up to adding an $\mathbb{F}\langle X\rangle$-linear combination of $b_1, \dots, b_i$ to b_{i+1}, we can assume that no monomial $c_1, \dots, c_i$ occurs as a prefix of a monomial involved in b_{i+1}. This ensures that $b_1, b_2, \dots$ is a weak prefix basis. By an argument analogous to the proof of assertion (i) this implies that $\{b_1, b_2, \dots\}$ is a basis of the right ideal $J = \sum_{i \geq 1} b_i \mathbb{F}\langle X\rangle \subset I$ generated by $b_1, b_2, \dots$. In order to finish the proof we have to show that $J = I$. If J is strictly contained in I, there exists an element e in $I \setminus J$ with largest monomial w of degree l. Since there are only finitely many monomials of degree at most l in X^*, there exists a basis element b_i with largest monomial w. A linear combination of e and b_i yields an element $\tilde{e} \in I \setminus J$ which is smaller than e contradicting minimality of the element e in $I \setminus J$. □

6. Broad ideals and prefix bases

A right ideal I of $\mathbb{F}\langle X\rangle$ is *broad* if its intersection with an arbitrary non-zero right ideal of $\mathbb{F}\langle X\rangle$ contains a non-zero element.

PROPOSITION 6.1. *All right ideals of finite codimension are broad.*

PROOF. We consider a right ideal I of finite codimension in $\mathbb{F}\langle X\rangle$. A right ideal J such that $I \cap J = \{0\}$ injects into the finite-dimensional quotient space $\mathbb{F}\langle X\rangle \pmod{I}$ under the natural projection $\mathbb{F}\langle X\rangle \longmapsto \mathbb{F}\langle X\rangle/I$. This implies $J = \{0\}$ since every non-trivial right ideal of $\mathbb{F}\langle X\rangle$ is of infinite dimension over $\mathbb{F}$. The ideal I intersects thus every non-zero right ideal J non-trivially. □

PROPOSITION 6.2. *Let C be a prefix-free set indexing a weak prefix basis $(b_c)_{c \in C}$ of right ideal I.*

If I is broad then C is maximal prefix free.

Proof of Proposition 6.2 Let $\mathcal{B} = \{b_c\}_{c\in C}$ be a weak prefix basis of a broad right ideal $I = \sum_{c\in C} b_c\mathbb{F}\langle X\rangle$ with index set C contained in a strictly larger prefix-free set $\tilde{C} = C \cup \{\tilde{c}\}$. This implies that $\mathcal{B} \cup \{\tilde{c}\}$ is a weak prefix basis of a right ideal J strictly containing I since it contains $\tilde{c}$. We have $\tilde{c}\mathbb{F}\langle X\rangle \cap I = \{0\}$ in contradiction with broadness of I. □

REMARK 3. *The ideal generated by a weak prefix basis indexed by a maximal prefix-free set is not necessarily broad as illustrated by the following example:*

We consider the set $B = \{x^ny - x^{n+1}, y^nx - y^{n+1}\}_{n\geq 1}$. It is easy to check that B is a prefix basis associated to the maximal prefix-free set $C = xx^*y \cup yy^*x$. We claim that the intersection of the right ideal $I = \sum_{b\in B} b\mathbb{F}\langle X\rangle$ freely generated by B with the right ideal $(x+y)\mathbb{F}\langle x,y\rangle$ is reduced to $\{0\}$.

Indeed, let us consider a non-zero polynomial $Q \in \mathbb{F}\langle x,y\rangle$ of minimal degree such that $(x+y)Q \in I$. Since all monomials involved in the prefix basis B are homogeneous of degree at least 2, the polynomial Q is without constant term. We can thus write $Q = xQ_x + yQ_y$. Writing

$$(x+y)Q = (x+y)(xQ_x+yQ_y) = (x^2+y^2)(Q_x+Q_y) - (x^2-xy)Q_y - (y^2-yx)Q_x$$

we see that $(x^2+y^2)(Q_x+Q_y)$ belongs to I since (x^2-xy) and (y^2-yx) are both in B. Every element of B is either in the right ideal $x\mathbb{F}\langle X\rangle$ or in the right ideal $y\mathbb{F}\langle X\rangle$ of $\mathbb{F}\langle X\rangle$. Every element R of the right ideal I generated by B has thus a decomposition $R = R_x + R_y$ with $R_x \in I \cap x\mathbb{F}\langle x,y\rangle$ and $R_y \in I \cap y\mathbb{F}\langle x,y\rangle$. Considering $R = (x^2+y^2)(Q_x+Q_y)$ we have thus $R = R_x + R_y$ with $R_x = x^2(Q_x+Q_y) \in I$ and $R_y = y^2(Q_x+Q_y) \in I$. Hence there exist polynomials $\alpha_1, \alpha_2, \dots, \alpha_a$ in $\mathbb{F}\langle x,y\rangle$ such that $R_x = \sum_{n=1}^{a} x^n(x-y)\alpha_n$. Left-divisiblity of $R_x = x^2(Q_x+Q_y)$ by x^2 forces $\alpha_1 = 0$. (Indeed, $x(x-y)\alpha_1$ with $\alpha_1 \neq 0$ involves at least one monomial of the form $xy\dots$ with non-zero coefficient and the generators $x^2(x-y), x^3(x-y), \dots$ associated to $\alpha_2, \alpha_3, \dots$ are all elements of the ideal $x^2\mathbb{F}\langle x,y\rangle$.) This implies $x(Q_x+Q_y) = \sum_{n=1}^{a-1} x^n(x-y)\alpha_{n+1} \in I$. The same arguments show $y(Q_x+Q_y) \in I$. Setting $q = Q_x + Q_y$ we have $(x+y)q \in I$ and $q = Q_x+Q_y$ is of smaller degree than $Q = xQ_x+yQ_y$ in contradiction with minimality of the degree of $Q = xQ_x+yQ_y$.

6.1. Prefix bases.

A *prefix basis* is a weak prefix basis

$$b_c = c - \sum_{p\in P} \alpha_{c,p}p$$

indexed by a prefix-free set C with P denoting the set of all proper prefixes of C.

The ideal $(x+y)\mathbb{F}\langle x,y\rangle$ of $\mathbb{F}\langle x,y\rangle$ is an example of a right ideal having no prefix basis. (Indeed, $x+y$ is, up to multiplication by a non-zero constant, the only possible free generator of the principal right ideal $I = (x+y)\mathbb{F}\langle x,y\rangle$. A prefix basis of I is thus either indexed by x or by y and y, respectively x, is not a prefix of x, respectively y.)

PROPOSITION 6.3. *Every weak prefix basis indexed by a maximal prefix-free set is a prefix basis.*

PROOF. A prefix-free set C is maximal if and only if $X^* \setminus CX^*$ is the set P of proper prefixes of all elements in C. □

Proposition 6.3 implies immediately the following result:

Corollary 4. *Every weak prefix basis of a broad right ideal is a prefix basis.*

Proposition 6.2 shows now:

Corollary 5. *Every weak prefix basis of right ideal of finite codimension is a prefix basis.*

7. Sequential prefix bases

A *prefix-free sequence* is a (finite or infinite) sequence $c_1, c_2, \dots$ of distinct elements in X^* defining a prefix-free set $\{c_1, c_2, \dots\}$. A prefix-free sequence is *maximal* if it defines a maximal prefix-free set.

A *sequential prefix basis* is a sequence $b_i = c_i - \sum_{p \in P_i} \alpha_{c_i,p} p,\ c_i \in C$, such that the elements $c_1, c_2, \dots$ form a prefix-free sequence C and such that for all n, all monomials of $b_1, \dots, b_n$ are in $\{c_1, \dots, c_n\} \cup P_n$ where P_n is the set of all proper prefixes of $\{c_1, \dots, c_n\}$.

Example Given a prefix-free sequence with first elements $c_1 = w_1 \dots w_a, c_2 = u_1 \dots u_b, \dots$ the first two elements b_1, b_2 of a sequential prefix basis are necessarily of the form

$$b_1 = w_1 w_2 \dots w_a - \alpha_0 - \sum_{k=1}^{a-1} \alpha_k w_1 w_2 \dots w_k$$

and

$$b_2 = u_1 u_2 \dots u_b - \alpha'_0 - \sum_{k=1}^{a-1} \alpha'_k w_1 w_2 \dots w_k - \sum_{k=1}^{b-1} \beta_k u_1 u_2 \dots u_k$$

for suitable constants $\alpha_0, \dots, \alpha_{a-1}, \alpha'_0, \dots, \alpha'_{b-1}, \beta_1, \dots, \beta_{b-1}$ in the ground-field $\mathbb{F}$. These constants are uniquely determined by the ideal $b_1\mathbb{F}\langle X\rangle + b_2\mathbb{F}\langle X\rangle$ and by the sequence $c_1, c_2, \dots$ if one sets $\beta_i = 0$ for all indices i such that $u_1 = w_1, u_2 = w_2, \dots, u_i = w_i$.

A sequential prefix basis is obviously a prefix basis. A prefix basis $b_1, b_2, \dots$ is a sequential prefix basis if and only if all finite initial sequences $b_1, b_2, \dots, b_n$ are prefix bases.

Assuming a total order on the finite alphabet X, we endow the monoid X^* with the *lexicographic order* given by $uv < uw$ if $v \neq w$ and v is either the empty word or its first letter is smaller than the first letter of w.

The main tool for proving Theorem 1 is the following result:

Proposition 7.1. *Right ideals of finite codimension in $\mathbb{F}\langle X\rangle$ are in one-to-one correspondence with sequential prefix bases indexed by lexicographically increasing finite maximal prefix-free sequences.*

The codimension l of such an ideal is given by the number of elements in the prefix-closed set of all proper prefixes of the associated finite maximal prefix-free sequence.

Proof. The first part of the proof is similar to the proof of assertion (iii) in Proposition 5.1 except that we work with the lexicographical order instead of the graded lexicographical order. For a right ideal I of finite codimension l this works since any set of $l + 1$ monomials is linearly dependent modulo I.

By Proposition 6.2 we get a prefix basis $b_1, b_2, \dots$ of I. We have to show that this prefix basis is a sequential prefix basis. Suppose that there exists a smallest index i such that $b_i = c_i + \dots$ involves a monomial $w < c_i$ which is not a proper prefix of $c_1, \dots, c_i$. Since I is of finite codimension l, the elements $w, w\alpha, w\alpha^2, \dots, w\alpha^l$ are I−linearly dependent for every letter $\alpha \in X$. Choosing for α the smallest letter of X, all these words are lexicographically smaller than c_i which is the largest monomial of b_i by construction. This contradicts the minimality of b_i in $I \setminus \sum_{j=1}^{i-1} b_j \mathbf{F}\langle X\rangle$.

The second part is assertion (ii) of Proposition 5.1. □

8. Trees associated to maximal prefix-free sets

Given a finite maximal prefix-free set C, we consider the rooted tree T with leaves given by the set C and interior vertices given by the set P of proper prefixes of C. A vertex w is a child of a vertex u if w is in uX. The root vertex of T is the empty word $1 \in X^*$ which belongs to C if $C = \{1\}$ and to P otherwise. Every interior vertex $p \in P$ has exactly $\sharp(X)$ children where $\sharp(X)$ denotes the number of elements in the alphabet X.

Lemma 1. *The number $\sharp(C)$ of leaves in T satisfies $\sharp(C) = 1 + \sharp(P)(\sharp(X) - 1)$.*

Proof. Every interior vertex $p \in P$ has $\sharp(X)$ children and no element of C has children. There are thus $\sharp(P)\sharp(X)$ children in T. Since every vertex of $(C \cup P) \setminus \{1\}$ is a child we have $\sharp(P)\sharp(X) = \sharp(P) + \sharp(C) - 1$. □

A maximal prefix-free set C different from the singleton $\{1\}$ has a canonical decomposition

$$C = \bigcup_{x \in X} x C_x$$

where the sets C_x indexed by the letters of the alphabet X are maximal prefix-free sets of X^*. The map $C \longmapsto \{C_x\}_{x \in X}$ is one-to-one between maximal prefix-free sets different from $\{1\}$ and sets $(C_x)_{x \in X}$ consisting of $\sharp(X)$ maximal prefix-free sets in X^*.

For the corresponding prefix-closed set P of all proper prefixes of elements in $C = \bigcup_{x \in X} x C_x$, we get similarly a decomposition

$$P = \{1\} \cup \bigcup_{x \in X} x P_x$$

with P_x denoting the set of proper prefixes of C_x.

We suppose now the alphabet X totally ordered and we endow X^* with the induced lexicographic order.

Lemma 2. *We consider a maximal prefix-free set $C \subset X^*$ different from $\{1\}$ and its associated set $P = X^* \setminus CX^*$ of proper prefixes.*

(i) We have $1 < c$ for all $c \in C$.

(ii) For $p = xp_x \in P$ and $c = yc_y \in C$ with $x, y \in X$, we have $p < c$ if either $x < y$ or if $x = y$ and $p_x < c_x$.

We leave the obvious proof to the reader.

9. Proof of Theorem 1

Proposition 7.1 and Lemma 1 imply that Theorem 1 amounts to a good understanding of all sequential prefix bases of $\mathbb{F}\langle x, y\rangle$ which are indexed by lexicographically increasing maximal prefix-free sequences of finite length $n + 1$. The number $A_n(q)$ of such sequential prefix bases over a finite field $\mathbb{F}_q$ with q elements is of course finite and can be computed by decomposing $A_n(q)$ according to contributions of the underlying binary trees. A tree T with $n+1$ leaves given by a maximal prefix-free set $C \subset \{x,y\}^*$ gives a contribution of

$$\prod_{c\in C} q^{\sharp\{p\in P \mid p<c\}} \tag{2}$$

to $A_n(q)$ where P is the set of all n proper prefixes of C and where the order relation $p<c$ is the lexicographical order on $\{x,y\}^*$.

We have $A_0(q)=1$ since $\mathbb{F}\langle x,y\rangle$ is the only right-ideal of codimension 0 in $\mathbb{F}\langle x,y\rangle$. The corresponding tree is the trivial tree reduced to the root 1. We denote by $A_T(q)$ the contribution to $A_{n+1}(q)$ which corresponds to a tree T with $n+1>0$ interior vertices. We consider the partition $T=\{1\}\cup xT_x\cup yT_y$ of T into its root 1 and its left and right subtrees T_x and T_y. We denote by C_x, C_y, respectively P_x, P_y, the leaves, respectively the interior vertices, of T_x, T_y. Assertion (i) of Lemma 2 shows that every leaf of $C=xC_x\cup yC_y$ is lexicographically larger than the root 1 of T. Assertion (ii) of Lemma 2 states that no leaf in xC_x is larger than an interior vertex yP_y of the right subtree T_y and that every leaf in yC_y is larger than every interior vertex xP_x of the left subtree T_x. Formula (2) yields thus the identity

$$A_T(q)=q^{\sharp(C)+\sharp(P_x)\sharp(C_y)}A_{T_x}(q)A_{T_y}(q)$$

where $A_T(q)=1$ if $T=\{1\}$ is the trivial tree reduced to its root.

We denote by $k=\sharp(P_x)$ the number of interior vertices of the left tree T_x. Since T has $\sharp(P)=n+1$ interior vertices with $P=\{1\}\cup xP_x\cup P_y$ we have $\sharp(P_y)=n-k$ and Lemma 1 (equivalent to Corollary 3.4 of Chapter 2 in [**BR**]) yields $\sharp(C_y)=\sharp(P_y)+1=n-k+1$ and $\sharp(C)=\sharp(P)+1=n+2$. We get thus

$$\begin{aligned} A_T(q) &= q^{n+2+k(n-k+1)}A_{T_x}(q)A_{T_y}(q) \\ &= q^{(k+1)(n+2-k)}A_{T_x}(q)A_{T_y}(q). \end{aligned}$$

Denoting by $A_{(k,n-k)}(q)$ the contribution to $A_{n+1}(q)$ coming from all trees T with a decomposition $T=\{1\}\cup xT_x\cup yT_y$ into a left subtree T_x with k interior vertices and a right subtree T_y with $n-k$ interior vertices we get

$$A_{(k,n-k)}(q)=q^{(k+1)(n+2-k)}A_k(q)A_{n-k}(q).$$

Summing over all possibilities for k we have finally

$$A_{n+1}(q)=\sum_{k=0}^{n}A_{(k,n-k)}(q)=\sum_{k=0}^{n}q^{(k+1)(n+2-k)}A_k(q)A_{n-k}(q)$$

which is the recursive formula for $A_{n+1}(q)$ given by Theorem 1.

The identity $A_n(q)=q^{n(n+1)}C_n(1/q)$ holds for $n=0$. For $n\geq 0$ we get by induction

$$\begin{aligned} A_{n+1}(q) &= \sum_{k=0}^{n} q^{(k+1)(n+2-k)+k(k+1)+(n-k)(n-k+1)}C_k(1/q)C_{n-k}(1/q) \\ &= q^{(n+1)(n+2)}\sum_{k=0}^{n} q^{-(k+1)(n-k)}C_k(1/q)C_{n-k}(1/q) \\ &= q^{(n+1)(n+2)}C_{n+1}(1/q)\ . \end{aligned}$$

This ends the proof of Theorem 1. □

10. Proof of Theorem 2

We denote by $A_{m,T}(q)$ the contribution

$$A_{m,T} = \prod_{c\in C} q^{\sharp\{p<c\}}$$

to $A_{m,n+1}(q)$ of a tree T with $n+1$ interior vertices and leaves $C \subset \{x_1,\ldots,x_m\}^*$. Lemma 1 shows that C consists of $1+(n+1)(m-1)$ elements. Decomposing the tree T into m subtrees $T_1,\ldots,T_m$ having respectively $n_1,\ldots,n_m$ interior vertices such that $T = \{1\} \cup_{j=1}^m x_jT_j$, we get the identity

$$A_{m,C} = q^{1+(n+1)(m-1)+\sum_{j=1}^{m-1}\left(\sum_{k=1}^{j} n_k\right)(1+n_{j+1}(m-1))} \prod_{j=1}^{m} A_{m,T_j}(q) \ .$$

Summing over all possible trees we have

$$A_{m,n+1} = \sum_{n_1+\cdots+n_m=n} q^{1+(n+1)(m-1)+\sum_{j=1}^{m-1}\left(\sum_{k=1}^{j} n_k\right)(1+n_{j+1}(m-1))} \prod_{j=1}^{m} A_{m,n_j}(q)$$

which is equivalent to Theorem 2. □

Remark 6. *From a computational point of view the polynomials $A_{m,n}(q)$ are better computed as follows: Consider m formal series $G_1(t),\ldots,G_m(t)$ (associated to "unfinished" trees with a root having children $x_1,\ldots,x_i$ and all other interior vertices of degree m) with coefficients in $\mathbb{N}[q]$ defined by*

$$\begin{aligned} G_1(t) &= \sum_{n=0}^{\infty}([t^n]G_m(t))\, q^{1+n(m-1)}t^{n+1} \\ G_i(t) &= \sum_{n=0}^{\infty}\sum_{j=1}^{n}\left([t^j]G_{i-1}(t)\right)\left([t^{n-j}]G_m(t)\right) q^{j(1+(n-j)(m-1))}t^n, \quad i=2,\ldots,m-1 \\ G_m(t) &= 1+\sum_{n=0}^{\infty}\sum_{j=1}^{n}\left([t^j]G_{m-1}(t)\right)\left([t^{n-j}]G_m(t)\right) q^{j(1+(n-j)(m-1))}t^n \ . \end{aligned}$$

Then

$$G_m(t) = \sum_{n=0}^{\infty} A_{m,n}(q)t^n \ .$$

11. Right congruences of the free monoid

A *right congruence* of a monoid is an equivalence relation which is compatible with multiplication at the right. If $\equiv$ is a right congruence of $\{x,y\}^*$, then the span over $\mathbb{F}$ of the polynomials $u-v$ formed by two monomials u,v such that $u \equiv v$ is a right ideal of $\mathbb{F} < x,y >$. The mapping from the set of right congruences of $\{x,y\}^*$ into the set of right ideals of $\mathbb{F}\langle x,y\rangle$ defined in this way is into but not onto.

The methods of the previous section are easily extended to prove the following result.

Proposition 7. *There is a bijection between the right congruences of index n of the free monoid $\{x,y\}^*$ and the set of triplets (C,P,f), where C is a maximal prefix-free set of $n+1$ elements, where P is the associated prefix-closed set of all n proper prefixes of elements in C and where f is a function from C into P such* *that $f(c)$ is lexicographically smaller than c for every c in C (using the convention that there is exactly one such function in the case $C = \{1\}$ and $P = \emptyset$).*

Proposition 7 implies easily that the number b_n of right congruences of index $n \geq 1$ is given by

$$b_n = \sum_C \prod_{c \in C} \sharp\{p \in P \ |p < c\} \tag{3}$$

where the first sum is over all finite maximal prefix-free sets C with $n+1$ elements.

The number b_n has been first computed by Valery Liskovets [**L**]. Indeed, a right congruence of a free monoid X^* is the same thing as an accessible deterministic automaton with transitions labelled by the alphabet X. For the free monoid $\{x, y\}^*$, the number b_n of right congruences of index n is equal, for $n = 1, 2, 3, 4, 5, 6$ respectively to 1, 12, 216, 5248, 160675, 5931540, see sequence A6689 of [**OEIS**]. As noticed by Liskovets, the number b_n is divisible by n^2, see [**L**]. An easy proof follows from the observation that the lexicographically largest vertex p_m of P is the prefix of the two elements $p_m x$ and $p_m y$ in C which are lexicographically larger than all elements of P. We have thus n^2 choices for the restriction of f to the subset $\{p_m x, p_m y\}$ of C.

A slight variation of the techniques used previously shows that the numbers b_n can be computed as follows: Set $B_0(t) = t$ and define $B_{n+1}(t)$ recursively by

$$B_{n+1}(t) = \sum_{i=0}^{n} B_i(t+1) B_{n-i}(t+i+1) \ . \tag{4}$$

We have then

$$B_n(t) = \sum_C \prod_{c \in C} (t + \sharp\{p \in P \ |p < c\}) \tag{5}$$

using the same conventions as for (3), i.e. the first sum is over all finite maximal prefix-free sets C having $n+1$ elements. In particular, we get $b_n = B_n(0)$ and $(t+n)^2$ divides $B_n(t)$ for all $n \geq 1$. The polynomials $B_1(t), \ldots, B_5(t)$ are

$$\begin{aligned}
&(t+1)^2 \cdot 1,\\
&(t+2)^2(2t+3),\\
&(t+3)^2(5t^2+22t+24),\\
&(t+4)^2(14t^3+121t^2+346t+328),\\
&(t+5)^2(42t^4+596t^3+3150t^2+7360t+6427).
\end{aligned}$$

Formula (5) implies easily the following combinatorial interpretation for the coefficients of $B_n(t)$: The coefficient of t^{n+1-k} in $B_n(t)$ counts the number of maps ϕ from a subset $\mathcal{L}_k$ of k leaves in a binary tree with n interior vertices into the set of interior vertices of the same tree such that $\phi(c)$ is lexicographically smaller than c for every leave c in $\mathcal{L}_k$. In particular, the leading coefficient t^{n+1} of $B_n(t)$ counts the number of such maps defined on an empty set of leaves in binary trees with n interior vertices. It enumerates thus simply the number of such binary trees given by the n-th Catalan number C_n since there are C_n possible binary trees corresponding to C_n different choices for the maximal prefix-free set C in (5).

Introducing the associated polynomials $\tilde{B}_n(t) = \frac{1}{t^2} B_n(t-n)$ we get the sequence $\tilde{B}_1(0), \tilde{B}_2(0), \ldots$ of constant coefficients of $\tilde{B}_n$ starting as

$$1, -1, 3, -16, 127, -1363, 18628, -311250, \ldots .$$

This sequence coincides (up to an additional initial term and alternating signs) with sequence A82161 of [**OEIS**] also appearing in works of Liskovets related to the enumeration of some type of acyclic automata. Formula (5) yields a combinatorial interpretation for the sequence $\tilde{B}_n(0), -\tilde{B}_2(0), \tilde{B}_3(0), -\tilde{B}_4(0), \ldots$: It counts maps φ from the set $\mathcal{L}'$ of the $n-1$ lexicographically smallest leaves into interior vertices of binary trees with n interior vertices such that $\varphi(c)$ is lexicographically larger than c for all $c \in \mathcal{L}'$. Such maps exist of course only if the two lexicographically largest leaves are the two children of the lexicographically largest interior vertex v_m. They define finite state automata which end always in the state v_m.

Two consecutive polynomials $\tilde{B}_n(t)$ and $\tilde{B}_{n+1}(t)$ are seemingly related by the identity $\tilde{B}_{n+1}(0) = -\tilde{B}_n(-1)$ for which we lack an explanation and a proof.

11.1. Computational aspects. The computation of the polynomial $B_n(t)$ with Formula (4) uses $O(n^4)$ elementary arithmetical operations involving natural numbers of order $e^{O(n)}$ and is thus quite challenging. The aim of this section is to show that $B_n(t)$ can be computed using only $O(n^3)$ elementary arithmetical operations (involving large natural numbers).

Moreover, our formulae give an algorithm using $O(n^2)$ elementary arithmetical operations over a commutative ring $\mathbb{K}$ for evaluating $B_n(t)$ at an element of $\mathbb{K}$.

To the purpose, we introduce the polynomials

$$Q_{n,k}(t) = \sum_{C, c \in C', \sharp(C') = n-k} (t + \sharp\{p \in P \mid p < c\})$$

where the sum is over all finite maximal prefix sets with $n+1$ elements in $\{x,y\}^*$ and where $C' \subset C$ is the set of all elements in C which are (lexicographically) strictly smaller than the (lexicographically) largest element $\max_P p$ in the set P of all proper prefixes of C.

We have then by definition

$$B_n(t) = \sum_{k=1}^{n} (t+n)^{k+1} Q_{n,k}(t) .$$

Removal of the two leaves of the largest interior vertex (which is always in y^* for non-zero contributions to $Q_{n+1,1}$) in trees contributing to $Q_{n+1,1}(t)$ gives the expression

$$B_n(t) = (t+n) Q_{n+1,1}(t) .$$

The sequence $b_1, b_2, \ldots$ of right congruences of index n is thus also given by $Q_{2,1}(0), 2Q_{3,1}(0), 3Q_{4,1}(0), \ldots, b_n = nQ_{n+1,1}(0), \ldots$.

The polynomials $Q_{n,k}$ are given by $Q_{n,k} = 0$ if $k = 0$ or $k > n$, $Q_{1,1} = 1$ and by the recursive formula

$$Q_{n+1,k}(t) = Q_{n,k-1}(t) + (t+n) Q_{n+1,k+1}(t) \qquad (6)$$

otherwise. (The contribution $Q_{n,k-1}(t)$ to $Q_{n+1,k}(t)$ corresponds to trees such that the maximal element $p_{\max}$ of P is a child of the second-largest element $\max(P \setminus \{p_{\max}\})$ in P.)

The first few non-zero polynomials $Q_{i,j}$ with rows corresponding to $i = 1, 2, 3, 4$ and columns corresponding to $j = 1, 2, 3, 4$ are

$$\begin{array}{cccc} 1 & & & \\ t+1 & 1 & & \\ 2t^2+7t+6 & 2t+3 & 1 & \\ 5t^3+37t^2+90t+72 & 5t^2+22t+24 & 3t+6 & 1 \end{array}$$

Formula (6) can be used for proving 2−automaticity of the reduction modulo 2 of the sequence $b_1, b_2, \ldots$. More precisely, we have $b_n \equiv 0 \pmod 2$ if $n \not\equiv 1 \pmod 4$ and $b_{4n+1} \equiv d_n \pmod 2$ with $d_0, d_1, d_2, \ldots$ given by A85357 of [**OEIS**] and defined recursively by $d_0 = 1, d_{2n} = d_{4n+1} = d_n, d_{4n+3} = 0$.

Remark 8. *Derivating the recursive formulae for $Q_{n,k}(t)$ we can compute the evaluation $B'_n(\alpha)$ of the derivative of $B_n(t)$ at a complex number α using only $O(n^2)$ operations. This is of course useful when using Newton's algorithm for computing real or complex roots of $B_n(t)$.*

11.2. Experimental observations concerning the roots of $\tilde{B}_n(t)$. An intriguing experimental observation concerns the roots of the normalized polynomials $\tilde{B}_n(t) = \frac{1}{t^2} B_n(t-n)$. Figure 1 shows all roots for $n = 64$. This picture seems to be

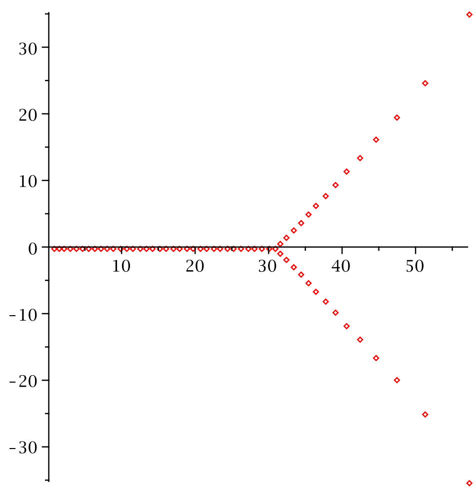

Figure 1. All 64 roots of $\tilde{B}_{64}(t) = t^{-2} B_{64}(t-64)$

generic: All roots of $\tilde{B}_n(t)$ have seemingly positive real parts, and all small roots are real. Denoting by $0 < \rho_{1,n} < \rho_{2,n} < \ldots$ the increasing sequence of real roots of $\tilde{B}_n(t)$, the sequence $\rho_{k,n}, \rho_{k,n+1}, \rho_{k,n+2}, \ldots$ seems to converge to a "limit-root" ρ_k for $k = 1, 2, \ldots$. An illustration of this behaviour is given by the following table yielding a few digits of the four smallest real roots $0 < \rho_{1,n} < \rho_{2,n} < \ldots$ of $\tilde{B}_n(t)$

for a few values of n:

	$\rho_{1,n}$	$\rho_{2,n}$	$\rho_{3,n}$	$\rho_{4,n}$
$n = 2$	.5			
$n = 3$	.6	1		
$n = 4$	.5884116194			
$n = 5$	.5884313323	1.257696478		
$n = 6$	.5883685633	1.263514366	1.951691000	
$n = 7$	.5883454087	1.262957815	2	2.608611356
$n = 8$	.5883352467	1.262837114	1.994581954	2.81197375
$n = 16$	.5883242960	1.262712718	1.994007709	2.763397124
$n = 32$	.5883239687	1.262709634	1.993992341	2.763344632
$n = 64$	.5883239628	1.262709583	1.993992118	2.763343960
$n = 128$	.5883239628	1.262709583	1.993992116	2.763343955

11.3. More variables. Formula (5) has an obvious generalization to finite m-ary trees with n interior vertices and with leaves C given by maximal finite prefix-free sets of the free monoid $\{x_1, \ldots, x_m\}^*$ on the totally ordered alphabet $x_1 < x_2 < \cdots < x_m$. The evaluations $b_{m,n} = B_{m,n}(0)$ of the corresponding polynomials $B_{m,n}(t)$ have an obvious combinatorial interpretation in terms of finite state automata.

The polynomials $B_{m,n}(t)$ are divisible by $(t-n)^m$ by the same argument working for $m = 2$ and we have the identity $\tilde{B}_{m,n+1}(0) = (-1)^{m+1}\tilde{B}_{m,n}(-1)$ for the normalized polynomials $\tilde{B}_{m,n}(t) = \frac{1}{t^m}B_{m,n}(t-n)$. The constant coefficients $\tilde{B}_{m,n}(0)$ (and the evaluations $\tilde{B}_{m,n}(-1)$) have again combinatorial interpretations.

In the case $m = 3$, constant coefficients $b_{3,1} = B_{3,1}(0), b_{3,2} = B_{3,2}(0), \ldots$ of the polynomials $B_{3,1}(t), \ldots$ yield sequence A6690 of [**OEIS**] starting as $1, 56, 7965, 212864, \ldots$. The sequence $\tilde{B}_{3,1}(0), \tilde{B}_{3,2}(0), \ldots$ of constant coefficients of the normalized polynomials $\tilde{B}_{3,n}(t) = \frac{1}{t^3}B_{3,n}(t-n)$ starts as $1, 1, 7, 139, 5711, 408334, \ldots$, see sequence A82162 of [**OEIS**].

The generalization of Formula (4) gives the expression

$$\sum_{i_1+\cdots+i_m=n} B_{m,i_1}(t+1)B_{m,i_2}(t+i_1+1)\cdot \\ \cdot B_{m,i_3}(t+i_1+i_2+1)\cdots B_{m,i_m}(t+i_1+\cdots+i_{m-1}+1)$$

for $B_{m,n+1}(t)$ where the sum is over all natural integers summing up to n and where $B_{m,0}(t) = t$. A better way for computing $B_{m,n+1}(t)$ if $m \geq 3$ is given by introducing m auxiliary polynomial sequences $A_{j,n}(t)$ defined by $A_{0,n}(t) = B_{m,n}(t+1)$ and $A_{k,n}(t) = \sum_{j=0}^{n} A_{k-1,j}(t)B_{m,n-j}(t+j+1)$ for k in $\{1, \ldots, m-1\}$. We have then $B_{m,n+1}(t) = A_{m-1,n}(t)$.

The intriguing behaviour of small roots of the normalized polynomials $\tilde{B}_{m,n}(t) = \frac{1}{t^m}B_{m,n}(t-n)$ described in the case $m = 2$ in §11.2 seems to continue:

For $m = 3$ the roots of form a picture similar to Figure 2. Small roots of $\tilde{B}_{3,n}(t)$ come in conjugate pairs with strictly positive real parts and seem again to converge

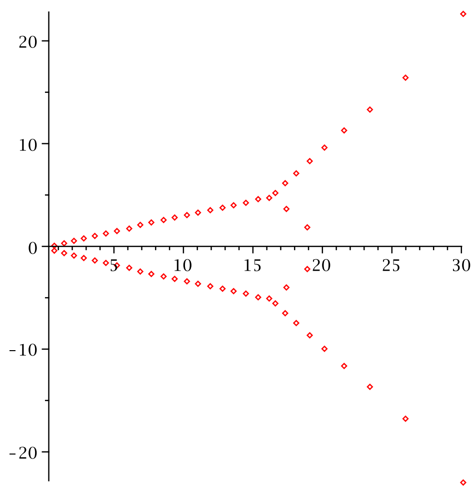

FIGURE 2. All roots of $\tilde{B}_{3,32}(t) = t^{-3}B_{3,32}(t-32)$

to limit-roots. The first two pairs of smallest conjugate roots are

	$\rho_{1,n}, \overline{\rho_{1,n}}$	$\rho_{2,n}, \overline{\rho_{2,n}}$
$n=2$	$.5 \pm .2886751346i$	
$n=3$	$.5769384001 \pm .2787884890i$	$1.048061600 \pm .5677305814i$
$n=4$	$.5765162477 \pm .2826219418i$	$1.232304945 \pm .4727537339i$
$n=5$	$.5764943956 \pm .2826830735i$	$1.249533211 \pm .5110572200i$
$n=6$	$.5764958323 \pm .2826960750i$	$1.248408443 \pm .5119047574i$
$n=7$	$.5764964795 \pm .2826995286i$	$1.248488680 \pm .5120483089i$
$n=8$	$.5764967451 \pm .2827006446i$	$1.248519232 \pm .5120911938i$
$n=16$	$.5764969633 \pm .2827013838i$	$1.248540224 \pm .5121141704i$
$n=32$	$.5764969654 \pm .2827013888i$	$1.248540362 \pm .5121142652i$
$n=64$	$.5764969654 \pm .2827013888i$	$1.248540362 \pm .5121142655i$

For $m=4$, small roots are seemingly either real or are pairs of small complex conjugate numbers lying almost on straight lines as illustrated by Figure 3. All roots seem to have strictly positive real parts. Convergency of small roots to limit-roots seems also to hold.

These features seem to continue for larger values of m: all roots have strictly positive real parts, small roots are roughly on $m-1$ lines coming in conjugate pairs (except for even m where the central line is the line of real numbers) and seem to converge to limit roots, see Figure 4 illustrating the case $m=7$.

11.4. A q-analogue of b_n. Formula (3) suggest to consider the q-analogue

$$b_n(q) = \sum_C \prod_{c \in C} \frac{1 - q^{\sharp\{p \in P \ \mid p < c\}}}{1-q} \tag{7}$$

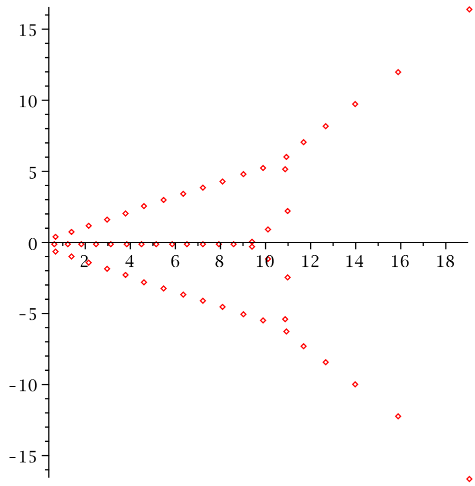

FIGURE 3. All roots of $\tilde{B}_{4,20}(t) = t^{-4}B_{4,20}(t-20)$

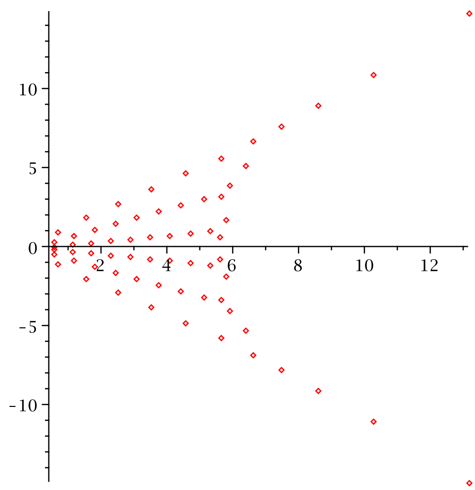

FIGURE 4. All roots of $\tilde{B}_{7,12}(t) = t^{-7}B_{7,12}(t-12)$

of the numbers b_n. For $n \geq 1$, the polynomials $b_n(q)$ are given by $B_n(q,0)$ where $B_0(q,t) = t$ and

$$B_{n+1}(q,t) = \sum_{i=0}^{n} q^{n+2+i(n-i+1)} B_i\left(q, \frac{t+1}{q}\right) B_{n-i}\left(q, \frac{t}{q^{i+1}} + \frac{1-q^{i+1}}{q^{i+1}(1-q)}\right) .$$

The specialization $q = 1$ gives the polynomials $B_n(t) \in \mathbb{N}[t]$ defined by (4). For $n \geq 1$, the polynomial $b_n(q)$ is divisible by $\left(\frac{1-q^{n+1}}{1-q}\right)^2$ and $B_n(q,t)$ is divisible by

$\left(t+\frac{1-q^n}{1-q}\right)^2$. The first polynomials $b_n(q)$ are

$$\begin{aligned} b_1(q) &= 1,\\ b_2(q) &= (1+q)^2(q+2),\\ b_3(q) &= (1+q+q^2)^2(q^4+3q^3+7q^2+8q+5),\\ b_4(q) &= (1+q+q^2+q^3)^2\cdot\\ &\quad\cdot(q^9+4q^8+11q^7+25q^6+43q^5+62q^4+71q^3+60q^2+37q+14). \end{aligned}$$

The reduced polynomials $\tilde{b}_n(q) = b_n(q)\left(\frac{1-q}{1-q^n}\right)^2$ satisfy seemingly the identities $\tilde{b}_{2n}(-1) = \tilde{b}_{2n-1}(-1)$. The first values of the sequence $n \longmapsto \tilde{b}_{2n}(-1)$ are $1, 2, 7, 30, 143, 728$ and coincide perhaps with the sequence $n \longmapsto \binom{3n-2}{n-1}\frac{1}{n}$, see sequence A6013 of [**OEIS**]. The polynomial sequence $B_{2n+1}(-1,t)$ is apparently given by the nice formula

$$B_{2n+1}(-1,t) = 2(1+t)^2\frac{(4n+1)!}{(n+1)!}\sum_{k=0}^{2n}\frac{(3n+1-k)!}{(2n-k)!(4n+2-k)!k!}t^k\ . \tag{8}$$

Assuming the truth of Formula (8) (or defining a sequence $B_{2n+1}(-1,t)$ by Formula (8)) we have

$$B_{2n+1}(-1,t-1) = 2t^2\frac{(4n+1)!}{n!}\sum_{k=0}^{2n}\frac{(3n-k)!}{(2n-k)!(4n+2-k)!k!}(-t)^k$$

and

$$\begin{aligned} B_{2n+1}\left(-1,t-\frac{1}{2}\right) &= 2\left(t+\frac{1}{2}\right)^2(4n+1)!\cdot\\ &\quad\cdot\sum_{k=0}^{2n}\binom{n+1+\lfloor k/2\rfloor}{\lfloor k/2\rfloor}\frac{t^{2n-k}}{2^k(2n-k)!(2n+2+k)!}\ . \end{aligned}$$

References

[B] R. Bacher: *The special subgroup of invertible non-commutative rational power series as a metric group* , arXiv:0804.1092 (2008).

[BPR] Jean Berstel, Dominique Perrin, and Christophe Reutenauer, *Codes and automata*, Encyclopedia of Mathematics and its Applications, vol. 129, Cambridge University Press, Cambridge, 2010. MR2567477 (2011g:94068)

[BR] Jean Berstel and Christophe Reutenauer, *Noncommutative rational series with applications*, Encyclopedia of Mathematics and its Applications, vol. 137, Cambridge University Press, Cambridge, 2011. MR2760561 (2012b:68152)

[C] P. M. Cohn, *Free ideal rings*, J. Algebra **1** (1964), 47–69. MR0161891 (28 #5095)

[L] V. A. Liskovets: *The number of initially connected automata,* Cybernetics **4**, 259-262 (1969).

[OEIS] N. J. A. Sloane: The Electronic Encyclopedia of Integer Sequences, published elctronically at http://oeis.org.

[R] Markus Reineke, *Cohomology of noncommutative Hilbert schemes*, Algebr. Represent. Theory **8** (2005), no. 4, 541–561, DOI 10.1007/s10468-005-8762-y. MR2199209 (2006j:16025)

[S] M. P. Schützenberger, *On the definition of a family of automata*, Information and Control **4** (1961), 245–270. MR0135680 (24 #B1725)

[St] Richard P. Stanley, *Enumerative combinatorics. Vol. 2*, Cambridge Studies in Advanced Mathematics, vol. 62, Cambridge University Press, Cambridge, 1999. With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin. MR1676282 (2000k:05026)

Institut Fourier (CNRS UMR 5582), 100 rue des Maths, Université de Grenoble I, 38402 Saint Martin d'Hères, France

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

Département de Mathématiques UQAM, Case Postale 8888 Succ. Centre-ville, Montréal (Québec) H3C 3P8 Canada

E-mail address: Reutenauer.Christophe@uqam.ca