Noncommutative rational power series and algebraic generating functions.

Mark Haiman*

Dept. of Mathematics, 0112
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0112, USA

Phone: (619) 534–2704
E-mail: mhaiman@macaulay.ucsd.edu

Oct. 7, 1992

*Research supported in part by N.S.F. grant DMS–8717795.

Proposed running head: ALGEBRAIC GENERATING FUNCTIONS

ABSTRACT: Sequences of numbers abound in combinatorics whose generating functions are *algebraic* over the rational functions. Examples include Catalan and related numbers, numbers of words expressing an element in a free group, and diagonal coefficients of 2-variable rational generating functions (Furstenberg's theorem). Algebraicity is of of practical as well as theoretical interest, since it guarantees an efficient recurrence for computing coefficients. Using now-classic results of Schützenberger on formal languages we prove: THEOREM. *Let K be a field and $f(X_1, \ldots, X_k, Y_1, \ldots, Y_k)$ a rational power series in noncommmuting indeterminates. Then any coefficient of $f(X_1, \ldots, X_k, X_1^{-1}, \ldots, X_k^{-1})$ converging w.r.t a given valuation on K is algebraic over K.* Many algebraic generating functions, including those mentioned above are so as a consequence of this theorem; in particular it gives a new elementary proof of Furstenberg's theorem.

1. Introduction

Certain problems in enumerative combinatorics lead to generating functions which are algebraic formal power series, that is, power series

$$F(x_1, \dots, x_n) = \sum_{m_1,\dots,m_n} f(m_1, \dots, m_n) x_1^{m_1} \cdots x_n^{m_n}$$

algebraic over the field $K(x_1, \dots, x_n)$ of rational functions in the variables x_i. Recent interest in algebraic generating functions [7], [11] has been connected with the fact that there are efficient algorithms for computing the coefficients $f(m_1, \dots, m_n)$. Additionally, the minimal polynomial of F contains asymptotic information about these coefficients.

The object of this paper is to prove:

THEOREM 1. *Let K be a field with a rank 1 discrete valuation v; K_v its completion with respect to the metric induced by v. Let $f(X_1, \dots, X_k, Y_1, \dots, Y_k)$ be a rational power series over K in noncommuting indeterminates (defintion below). Any coefficient of $f(X_1, \dots, X_k, X_1^{-1}, \dots, X_k^{-1})$ converging in K_v is algebraic over K.*

(In generating function applications, K would typically be a field of rational functions $k(z)$ and K_v the field of formal Laurent series $k((z))$.)

Using Theorem 1 it can be seen, for instance, that the generating functions for Catalan and related numbers and for the number of words expressing an element in a free group are algebraic. Theorem 1 also implies the theorem of Furstenberg [5] that the diagonal of a rational power series in two (commutative) variables is algebraic; this gives a new non-analyic proof of Furstenberg's theorem, valid over any field. These applications are developed below in Section 2, after appropriate definitions.

In Section 3, we derive Theorem 1 from some results of Schützenberger on noncommutative formal power series [1], [2], [9], [10]. The derivation is straightforward, and Schützenberger's results can by now be considered classical in the theory of formal languages, so Theorem 1 should be regarded more as an application of an existing theory than as a new result. Nevertheless, the relevance of this aspect of formal language theory to enumerative combinatorics seems to have gone unnoticed until now.

2. Definitions and applications

Fix K, v, and K_v as in Theorem 1.

DEFINITION. Let $\mathbf{X}^*$ be the free monoid on $\mathbf{X} = \{X_1, \dots, X_k, Y_1, \dots, Y_k\}$, with unit element denoted by e. The ring of *polynomials in the noncommuting indeterminates* $\mathbf{X}$ is $R_{\mathrm{pol}}(\mathbf{X}) = K\mathbf{X}^*$. Completing $R_{\mathrm{pol}}(\mathbf{X})$ in the usual way yields the ring $R(\mathbf{X})$ of *formal power series in the noncommuting indeterminates* $\mathbf{X}$.

Given $a \in R(\mathbf{X})$, $w \in \mathbf{X}^*$, let $\langle a, w\rangle$ denote the coefficient of w in a, so that $a = \sum_{w \in \mathbf{X}^*} \langle a, w\rangle w$. An element $a \in R(\mathbf{X})$ is invertible if and only if $\langle a, e\rangle \neq 0$; then

$$a^{-1} = \frac{1}{\langle a, e\rangle} \sum_{k=0}^{\infty} \left(1 - \frac{a}{\langle a, e\rangle}\right)^k .$$

Definition. The ring of *rational formal power series in the noncommuting indeterminates* $\mathbf{X}$, $R_{\mathrm{rat}}(\mathbf{X})$, is the smallest subring of $R(\mathbf{X})$ containing $R_{\mathrm{pol}}(\mathbf{X})$ and containing the inverse of each of its invertible elements.

The above definitions make the meaning of Theorem 1 precise. Now let us draw some conclusions from the theorem.

Corollary 2.1 (Furstenberg's theorem). *Let k be a field. Let $H(x, y) = \sum_{m,n} h(m, n)x^m y^n \in k[\![x, y]\!] \cap k(x, y)$ be a (commutative) rational formal power series. Then the diagonal series $D(z) = \sum_n h(n, n)z^n$ is algebraic over $k(z)$.*

Proof. By a theorem of Fliess ([4], see also [6]) there are polynomials p and q, where q has non-zero constant term, such that $H(x, y) = p(x, y)q^{-1}(x, y)$. Choose arbitrary lifts $\tilde{p}$, $\tilde{q}$ of p and q to noncommuting variables and let $\tilde{H}(X, Y) = \tilde{p}(X, zY)\tilde{q}^{-1}(X, zY) \in R_{\mathrm{rat}}(X, Y)$. Here we work over the field $K = k(z)$ with valuation v defining the field of formal Laurent series $K_v = k(\!(z)\!)$.

The coefficient of X^0 in $\tilde{H}(X, X^{-1})$ is easily seen to be $D(z)$. Since this certainly converges in $k(\!(z)\!)$, it is algebraic over $k(z)$ by Theorem 1. ∎

A related proof, also valid in any characteristic, may be found in [3].

The next example illustrates the application of Theorem 1 to a combinatorially defined power series.

Definition. The *Catalan number* C_n is the number of balanced strings of n left and n right parentheses. The Catalan number *generating function* is $G(x) = \sum_{n \geq 0} C_n x^n$.

Given any string of left and right parentheses, let us write down a word in the symbols X, U, X^{-1}, U^{-1} as follows: for each left parenthesis encountered, put $X^{-1}(U^{-1})^k$, where k is an arbitraily chosen non-negative integer; for each right parenthesis put XU. One easily verifies, by induction on the length of the string, that the resulting word reduces to U^n for some n if and only if *(i)* the parenthesis string is balanced, and *(ii)* for each left parenthesis encountered, the corresponding non-negative integer k was chosen to be the number of outermost parenthesis pairs intervening between that left parenthesis and its matching right parenthesis. If such is the case, n will be the number of outermost parenthesis pairs in the string.

From the preceding considerations it follows that the coefficient of X^0U^0 in the noncommutative rational power series $\mathcal{G}(X, U, X^{-1}, U^{-1})$ is $G(x)$, where

$$\mathcal{G}(X_1, X_2, Y_1, Y_2) = (1 - Y_2)^{-1}(1 - Y_1(1 - Y_2)^{-1} - xX_1X_2)^{-1}.$$

Here the underlying field is $K = \mathbb{Q}(x)$ with valuation v defining $K_v = \mathbb{Q}((\curvearrowleft))$. Thus $G(x)$ is algebraic by Theorem 1. Of course, it is well-known that $G(x) = (1/2x)(1 - \sqrt{1 - 4x})$. Alternatively, with $K = \mathbb{Q}(\curvearrowleft, \curvearrowright)$ and

$$\mathcal{G}(X_1, X_2, Y_1, Y_2) = (1 - yY_2)^{-1}(1 - Y_1(1 - Y_2)^{-1} - xX_1X_2)^{-1},$$

we find that the generating function $G(x, y)$ counting balanced strings by their length and their number of outermost pairs is algebraic (of course $G(x, y)$ too can be computed directly).

As a final application, we have:

Corollary 2.2. *Let $e_n(k)$ be the number of words of length n in the symbols $X_1, \ldots, X_k, X_1^{-1}, \ldots, X_k^{-1}$ which reduce to the identity in the free group generated by $X_1, \ldots, X_k$. Then $E_k(x) = \sum_n e_n(k)x^n$ is algebraic.*

Proof. $E_k(x)$ is the constant term of

$$\left(1 - x\sum_{i=1}^{k} X_i - x\sum_{i=1}^{k} X_i^{-1}\right)^{-1},$$

hence is algebraic by Theorem 1. ∎

3. Proof of Theorem 1

The proof of Theorem 1 will be based on three propositions. First, some essential definitions.

Definition. Let $\mathbf{Z} = (Z_1, \ldots, Z_n)$ be a finite list of variables. A *proper algebraic system over $R(\mathbf{X})$* is a list of n polynomials

$$p_i(\mathbf{X}; \mathbf{Z}) \in R_{\mathrm{pol}}(\mathbf{X} \cup \mathbf{Z}) \qquad (1 \le i \le n)$$

such that for each i, we have

$$(i) \quad p_i(0; 0) = 0, \text{ and}$$

$$(ii) \quad p_i(0; Z_1, \ldots, Z_n) \text{ has no non-zero linear term.}$$

An n-tuple $(\xi_1, \ldots, \xi_n) \in R(\mathbf{X})^n$ is the *solution* of the system $(p_1, \ldots, p_n)$ if for each i we have

$$(iii) \quad \langle \xi_i, e \rangle = 0, \text{ and}$$

$$(iv) \quad \xi_i = p_i(\mathbf{X}; \xi_1, \ldots, \xi_n).$$

Conditions *(i)* and *(ii)* ensure the existence of a unique solution. Namely, let $\xi_i^{(0)} = 0$ for each i, and define

$$\xi_i^{(m+1)} = p_i(\mathbf{X}; \xi_1^{(m)}, \ldots, \xi_n^{(m)})$$

for all $m \geq 0$. Then $\xi_i^{(m+1)}$ and $\xi_i^{(m)}$ agree in all terms of degree at most m, so $\xi_i = \lim_{m\to\infty} \xi_i^{(m)}$ exists and $(\xi_1, \ldots, \xi_n)$ is easily seen to be the unique solution.

DEFINITION. Any component of the solution of a proper algebraic system is an *algebraic formal power series in the noncommuting indeterminates* $\mathbf{X}$. More generally, we say $a \in R(\mathbf{X})$ is algebraic if $a - \langle a, e\rangle e$ is algebraic in the preceding sense. The set of algebraic elements of $R(\mathbf{X})$ we denote by $R_{\text{alg}}(\mathbf{X})$.

DEFINITION. The *Hadamard product* of $a, b \in R(\mathbf{X})$ is $a \odot b = \sum_{w\in\mathbf{X}^*} \langle a, w\rangle\langle b, w\rangle w$.

PROPOSITION 3.1 (Schützenberger [9], see also [1]). *If* $a \in R_{\text{rat}}(\mathbf{X})$ *and* $b \in R_{\text{alg}}(\mathbf{X})$ *then* $a \odot b \in R_{\text{alg}}(\mathbf{X})$.

We do not reproduce the proof, as it is somewhat lengthy. The essential point is that $R_{\text{rat}}(\mathbf{X})$ consists of the solutions of *linear* algebraic systems. It is possible to substitute the matrix of the linear system defining a into the system defining b to obtain a system defining $a \odot b$. Since this procedure is completely effective, our proof Theorem 1 contains, in principle, an algorithm to compute a polynomial equation satisfied by the algebraic power series in the conclusion.

PROPOSITION 3.2 (Chomsky–Schützenberger [2]). *Let* $D \subseteq \mathbf{X}^* = \{X_1, \ldots, X_k, Y_1, \ldots, Y_k\}^*$ *be the set of those elements which reduce to the identity under the relations* $X_iY_i = Y_iX_i = e$. *Then* $\Delta = \sum_{w\in D} w$ *is algebraic.*

Proof. For $l \in \mathbf{X}$ let G_l be the set of those elements of D whose initial symbol is l and which have no proper initial subword in D. Let $\Gamma_l = \sum_{w\in G_l} w$. Then Δ and the Γ_l satisfy the equations:

$$\Delta = 1 + \Delta \sum_{l\in\mathbf{X}} \Gamma_l,$$

$$\Gamma_l = l\beta_l\bar{l},$$

$$\beta_l = 1 + \beta_l \sum_{\substack{q\in\mathbf{X}\\ q\neq\bar{l}}} \Gamma_q,$$

where $\bar{l} = X_i$ if $l = Y_i$ and vice versa. These equations are equivalent to the proper algebraic system in $\Delta - 1$ and the $\beta_l - 1$

$$\Delta - 1 = ([\Delta - 1] + 1) \sum_{l \in \mathbf{X}} l([\beta_l - 1] + 1)\bar{l},$$

$$\beta_l - 1 = ([\beta_l - 1] + 1) \sum_{\substack{q \in \mathbf{X} \\ q \neq \bar{l}}} q([\beta_l - 1] + 1)\bar{q}.$$

■

By altering the above equations slightly, one can prove

PROPOSITION 3.2A (Shamir [10]). *Proposition 3.2 also holds with only the relations $X_iY_i = e$, not $Y_iX_i = e$.*

Using this in place of Proposition 3.2 in the proof of Theorem 1 below yields a version of Theorem 1 in which X_i^{-1} is only a *right* inverse of X_i. Among other things, the algebraicity of the Catalan number generating function follows more easily from this version.

PROPOSITION 3.3. *Let $\phi : R(\mathbf{X}) \to K[\![\mathbf{X}]\!]$ be the natural homomorphism to the commutative formal power series ring in $\mathbf{X}$. If $a \in R_{\mathrm{alg}}(\mathbf{X})$ then $\phi(a)$ is algebraic over $K(\mathbf{X})$.*

Proof. Without loss of generality, we may assume $\langle a, e \rangle = 0$. Let $(p_1, \ldots, p_n)$ be a proper algebraic system with solution $(\xi_1 = a, \xi_2, \ldots, \xi_n)$. Let $\eta_i = \phi(\xi_i)$. Treating the p_i as commutative polynomials, the η_i satisfy equations

$$f_i(\eta_1, \ldots, \eta_n) = \eta_i - p_i(\mathbf{X}; \eta_1, \ldots, \eta_n) = 0 \qquad (1 \leq i \leq n).$$

The Jacobian matrix of this system is

$$\mathcal{J} = \left(\frac{\partial f_i}{\partial \eta_j}\right)_{i,j} = \mathbf{I} - \left(\frac{\partial p_i}{\partial \eta_j}\right)_{i,j}.$$

By conditions *(i) (ii)*, and *(iii)* (the last applied to the η_i), the second term on the right has entries in the maximal ideal $(\mathbf{X})$ of $K[\![\mathbf{X}]\!]$, so $\det(\mathcal{J}) \neq 0$. It follows (e.g. by Lang [8], Chapter X, Proposition 8) that the η_i are algebraic over $K(\mathbf{X})$. ■

Proof of Theorem 1. Multiplying f if necessary by a representative of the inverse of the term whose coefficient is to be extracted, we may assume that the coefficient in question is the identity coefficient. This coefficient is the sum (assumed convergent in K_v) of all coefficients in the Hadamard product $f \odot \Delta$, and hence also the sum of all coefficients in $H(X_1, \ldots, X_k, Y_1, \ldots, Y_k) = \phi(f \odot \Delta)$. By Propositions 3.1, 3.2, and 3.3, H is algebraic over $K(X_1, \ldots, X_k, Y_1, \ldots, Y_k)$.

Every term of H contains equal powers of X_i and Y_i for each i, so putting $W_i = X_i Y_i$, we have $H = H(W_1, \ldots, W_k)$ and

$$c_0 + c_1 H + \cdots + c_m H^m = 0,$$

where $c_j \in K[W_1, \ldots, W_k]$ and not all $c_j = 0$. Dividing by a common factor if needed, we may assume that $W_k - 1$ does not divide all the c_j. Setting $W_k = 1$ therefore gives a non-trivial equation

$$\hat{c}_0 + \hat{c}_1 \hat{H} + \cdots + \hat{c}_m \hat{H}^m = 0,$$

where $\hat{c}_j \in K[W_1, \ldots, W_{k-1}]$ and $\hat{H} = H(W_1, \ldots, W_{k-1}, 1)$. Repeating this process, we find that $H(1, 1, \ldots, 1)$ is algebraic over K. ∎

Acknowledgements

The author wishes to thank David Richman, whose question "find the constant term of $(x + y + x^{-1} + y^{-1})^p$ when x and y do not commute" led to the discovery of Theorem 1, and who made helpful notes on a talk given by the author. Ira Gessel also provided valuable suggestions.

References

1. J. Berstel & C. Reutenauer, *Rational series and their languages.* EATCS Monographs on Theoretical Computer Science, Springer–Verlag (1988).

2. N. Chomsky & M.-P. Schützenberger, *The algebraic theory of context-free languages.* In Computer Programming and Formal Systems, P. Braffort & D. Hirschberg, eds., North-Holland, Amsterdam (1963) 118–161.

3. M. Fliess, *Sur divers produits de series formelles.* Bull. Soc. Math. France **102** (1974) 181–191.

4. M. Fliess, *Matrices de Hankel.* J. Maths. Pures et Appliqués **53** (1974) 197–222.

5. H. Furstenberg, *Algebraic function fields over finite fields.* J. Algebra **7** (1967) 271–277.

6. I. Gessel, *Two theorems on rational power series.* Utilitas Math. **19** (1981) 247–254.

7. H. T. Kung & J. F. Traub, *All algebraic functions can be computed fast.* Journal of the ACM **25** (1978) 245–260.

8. S. Lang, *Algebra.* Addison-Wesley, Reading, Mass. (1965).

9. M.-P. Schützenberger, *On a theorem of R. Jungen.* A.M.S. Proceedings **13** (1962) 885–890.

10. E. Shamir, *Algebraic, rational, and context-free power series in noncommuting variables.* In Algebraic Theory of Machines, Languages, and Semigroups, M. Arbib, ed., Academic Press, New York (1968) 329–341.

11. R. P. Stanley, *Differentiably finite power series.* European J. Combinatorics **1** (1980), 175–188.