On the Transcendence of Formal Power Series

Jean-Paul Allouche
L.R.I., Université Paris-Sud

December 1, 1997

[summary by Philippe Flajolet]

1. Introduction

Algebraicity of generating functions (gf's) is of interest in combinatorial analysis as it is a sure sign of strong structural properties. For instance, any (unambiguous) context-free model leads to algebraic generating functions; in particular generating functions of simple families of trees and random walks (defined by a finite set of node degrees or jumps) are algebraic. In another context, the algebraic character of the gf's associated with 2-dimensional directed animals in percolation theory points to a wealth of puzzling combinatorial bijections; see [7] for a specific illustration.

Conversely, a transcendence result for the gf of a combinatorial class $\mathcal{C}$ means a sort of "structural complexity lower bound" on $\mathcal{C}$. For instance, elements of $\mathcal{C}$ cannot be encoded by an unambiguous context-free grammar. Accordingly, if $\mathcal{C}$ already admits context-free descriptions, all such descriptions must be inherently ambiguous.

Methods for establishing the transcendence of generating functions fall broadly into two categories.

- Arithmetic methods are based on number-theoretic properties of coefficients. The most famous criterion in this range is Eisenstein's criterion: *If a series of* $\mathbb{Q}[[z]]$ *is algebraic, then the denominators of its coefficients contain only finitely many primes.* For instance, $f(z) = \exp(z)$ is transcendental "because" its coefficients $f_n = \frac{1}{n!}$ have denominators that contain infinitely many primes (by Euclid's theorem!).
- Analytic methods are based on the presence of a transcendental element in a local behaviour, usually taken at a singular point. In this perspective, $f(z) = \exp(z)$ is transcendental "because" its growth is too fast at infinity, a fact incompatible with the fact that an algebraic function is locally described by a Puiseux series (i.e., a series involving fractional powers).

The analytic approach is reviewed in [6]. The talk focuses on the arithmetic method, and more specifically on the following powerful approach [2, 3, 4, 10].

Principle . If $f(z) = \sum_n f_n z^n$ has integer coefficients and is algebraic over $\mathbb{Q}(z)$, then its reduction $(f(z) \bmod p) := \sum (f_n \bmod p) z^n$ is algebraic over $\mathbb{F}_p(z)$.

Principle . For a series $g(z) = \sum g_n z^n$ over a finite field $\mathbb{F}_p$, the following three properties are equivalent:

(i) the correspondence $n \mapsto g_n$ is computable by a finite automaton that inputs the base-p representation of n ("the g_n are automatic");
(ii) the infinite word $(g_0, g_1, \ldots)$ is generated by a regular (length homogeneous) substitution;
(iii) $g(z)$ is algebraic over $\mathbb{F}_p(z)$.

This is the classical "Christol-Kamae-Mendès France-Rauzy Theorem" [4, 5], the equivalence between (i) and (ii) being due to Cobham in 1972. For instance, the Catalan gf,

$$f(z) = \frac{1-\sqrt{1-4z}}{2} = z + z^2 + 2z^3 + 5z^4 + 14z^5 + 42z^6 + 132z^7 + 429z^8 + \cdots$$

has a reduction modulo 2

$$g(z) = z + z^2 + z^4 + z^8 + \cdots$$

where the coefficient g_n is 1 exactly when $n = 2^r$. Thus the coefficient sequence is computable by a finite automaton from the binary representation of the index n. It is also generated starting from the letter a by the regular substitution

$$a \mapsto a1, \qquad 1 \mapsto 10, \qquad 0 \mapsto 00.$$

2. Primitive words

An example originally due to Petersen serves to illustrate nicely the methods just introduced. Say that a word over some alphabet is *primitive* if it is not a "power", that is, the repetition of a shorter pattern. Thus *abbab* is primitive while *abbabbabb* is not. Let $m \geq 2$ be the alphabet cardinality, $W(z) = (1 - mz)^{-1}$ the gf of all words, and $P(z)$ the gf of primitive words. Then, since each word has a "root", one has

$$W(z) = P(z) + P(z^2) + P(z^3) + \cdots,$$

so that, with $\mu(n)$ the Moebius function,

$$P(z) = \sum_{d \geq 1} \mu(d) W(z^d), \qquad P_n = \sum_{d|n} \mu(d) m^{n/d}.$$

In particular, the reduction modulo m yields

$$\frac{P_n}{n} = \mu(n) + A \cdot m \equiv \mu(n) \mod m.$$

Thus, the problem is reduced to showing that $\mu(n)$ is the coefficient sequence of a transcendental series.

Now, by a theorem a Cobham, if a sequence has an algebraic gf over a finite field, and if it assumes some fixed value with a limit density δ, then δ is a rational number. (Think of the characterization by finite automata.) But, here, $\mu(n) = 1$ whenever n is square-free, an event whose density is $\frac{6}{\pi^2}$. The transcendence of $\sum_n \mu(n) z^n$ then follows from the irrationality of π.

Reduction modulo m thus provides a proof of the fact that the language of all primitive words cannot be an unambiguous context free language.

In the analytic perspective, transcendence results from the fact that $P(z)$ has infinitely many poles inside the unit circle. Such poles, at points $m^{-1/r} \exp(\frac{2ik\pi}{r})$, arise from $W(z)$ and the Moebius inversion formula for $P(z)$.

3. Stanley's conjecture

In his fundamental paper of 1980 on D-finite series, Stanley [9] conjectured that the binomial series

$$B_t(z) := \sum_{n \geq 0} \binom{2n}{n}^t z^n$$

is transcendental for any integers $t \geq 2$. Of course, we have $B_1(z) = 1/\sqrt{1-4z}$. In the case of even t, B_t is clearly transcendental given the presence of logarithmic elements induced by the asymptotic form of coefficients,

$$\binom{2n}{n}^{2s} \approx \frac{4^{2s}}{n^s}.$$

In addition B_2 is also known to be an elliptic integral. The case of odd t is harder. An analytic proof was suggested by Flajolet [6] in 1987 and an algebraic proof was given by Woodcock and Sharif [10] in 1989.

The proof of [10] consists in reducing first $B_t(z)$ modulo a prime p. The resulting series is algebraic, since a theorem of Furstenberg states that algebraic functions over finite fields are closed under Hadamard (termwise) products. (This property is also clear from the characterization by finite automata.) However, by means of arguments from algebraic number theory, Woodcock and Sharif are able to estimate the degree of ($B_t(z)$ mod p) over $\mathbb{F}_p(z)$ and deduce that there exists an infinity of special prime values of p for which this degree grows without bound. This in turn implies the transcendence of $B_t(z)$.

In contrast, from the analytic standpoint, it is the examination of the Puiseux expansion of $B_t(z)$ near its singularity $\zeta = 4^{-t}$ that leads to the transcendence result via the arithmetic transcendence of the number π.

4. Miscellaneous examples

There are a great many cases where reduction modulo a prime leads to transcendence results for generating functions. Here are a few examples.

In [6], the language $\{a^n b v_1 a^n v_2\}$ was shown to be inherently ambiguous through transcendence of

$$S(z) = \sum_{n \geq 1} \frac{z^{2n}}{1 - 2z + z^{n+1}},$$

since poles accumulate near 1/2. Alternatively, simple manipulations show that, modulo 2, the transcendence of $S(z)$ is equivalent to the transcendence of the divisor series

$$D(z) = \sum_{n \geq 1} \frac{z^n}{1 - z^n} = \sum_{n \geq 1} d(n) z^n.$$

The latter form is transcendental over $\mathbb{F}_2(z)$ since, upon reduction modulo 2, it is the indicator series of squares, and squares are known not to be automatic (Minsky).

A similar process applies to the Goldstine language whose gf involves the theta function $\Theta(z) = \sum_{n \geq 0} z^{n(n+1)/2}$, and to the partition series $P(z) = \prod (1 - z^n)^{-1}$ whose logarithmic derivative is closely related to divisor functions.

An amusing example due to Allouche, Betrema, and Shallit is the "Bourbaki definition of integers"

$$\emptyset,\ \{\emptyset\},\ \{\emptyset, \{\emptyset\}\},\ \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},\ \ldots,$$

which, upon binary encoding, leads to the nonregular substitution $[a \mapsto aab, \quad b \mapsto b]$. The associated infinite word (interpret a as 0, b as 1) has a gf that is transcendental, being related to the series

$$D_2(z) = \sum_{k \geq 2} \frac{z^{2^k - 1}}{1 - z^{2^k - 1}},$$

that also shows up in a formal language example of [6].

5. Lucas sequences

The talk concludes with a description of some recent results of Allouche, Gouyou-Beauchamps, and Skordev [1]. Lucas showed that

$$\binom{m}{n} \equiv \binom{m_0}{n_0}\binom{m_1}{n_1}\binom{m_2}{n_2}\cdots \mod p,$$

where the m_j, n_j are the digits of m, n in base p for prime p. More generally, following [8], define a *p-Lucas sequence* (p prime) by the property

$$a_{pn+j} \equiv a_n a_j \mod p.$$

For instance, the Apéry numbers

$$A_n = \sum_{k\geq 0} \binom{n}{k}^2 \binom{n+k}{k}^2$$

are p-Lucas. Then, Allouche *et alii* characterize the strong property for a sequence to be simultaneously algebraic (automatic) over $\mathbb{Q}$ *and* p-Lucas for all large enough p. In essence, the only possibility for such a sequence is to be, up to normalization, the sequence of values of the Legendre polynomials at some rational point. In other words, the corresponding gf $F(z)$ is of the form

$$F(z) = \frac{1}{\sqrt{1+az+bz^2}}.$$

A particular case is the central binomial coefficient $\binom{2n}{n}$. From Lucas' property and this characterization, a new proof of Stanley's conjecture can be deduced. There are also interesting extensions to Hadamard products of series involving $\binom{2n}{n}$, $\binom{3n}{n}$, etc.

Bibliography

[1] Allouche (J.-P.), Gouyou-Beauchamps (D.), and Skordev (G.). – Transcendence of binomial and Lucas's formal power series. – Preprint, December 1997.

[2] Allouche (Jean-Paul). – Note on an article of H. Sharif and C. F. Woodcock: "Algebraic functions over a field of positive characteristic and Hadamard products". *Séminaire de Théorie des Nombres de Bordeaux. Série 2*, vol. 1, n° 1, 1989, pp. 163–187.

[3] Allouche (Jean-Paul). – Finite automata and arithmetic. In *Séminaire Lotharingien de Combinatoire (Gerolfingen, 1993)*, pp. 1–18. – Univ. Louis Pasteur, Strasbourg, 1993.

[4] Christol (G.). – Ensembles presque-périodiques k-reconnaissables. *Theoretical Computer Science*, vol. 9, 1979, pp. 141–145.

[5] Christol (G.), Kamae (T.), Mendès France (M.), and Rauzy (G.). – Suites algébriques, automates et substitutions. *Bulletin de la Société Mathématique de France*, vol. 108, 1980, pp. 401–419.

[6] Flajolet (P.). – Analytic models and ambiguity of context–free languages. *Theoretical Computer Science*, vol. 49, 1987, pp. 283–309.

[7] Gouyou-Beauchamps (D.) and Viennot (G.). – Equivalence of the two-dimensional directed animal problem to a one-dimensional path problem. *Advances in Applied Mathematics*, vol. 9, n° 3, 1988, pp. 334–357.

[8] McIntosh (Richard J.). – A generalization of a congruential property of Lucas. *The American Mathematical Monthly*, vol. 99, n° 3, 1992, pp. 231–238.

[9] Stanley (R. P.). – Differentiably finite power series. *European Journal of Combinatorics*, vol. 1, 1980, pp. 175–188.

[10] Woodcock (Christopher F.) and Sharif (Habib). – On the transcendence of certain series. *Journal of Algebra*, vol. 121, n° 2, 1989, pp. 364–369.