Approximation of Artin type constants and automata

Pieter Moree

March 16, 1999

Abstract

Let $h(t)$ be a rational function. A constant of the form $\prod_p h(p)$, where the product ranges over all sufficiently large primes, is called an Artin type constant. Many important number theoretical constants like the Artin constant and the twin-prime constant are of this form. We show that Artin type constants can be expanded in the form $\prod_{k=2}^{\infty} \zeta(k)^{e_k}$, where ζ denotes the zeta-function, and use this to numerically approximate them. In some cases the coefficients e_k turn out to be related to conjugacy classes of primitive words in cyclic languages.

1 Introduction

Let $p_1, p_2, \cdots$ denote the consecutive primes. Put $p_0 = 1$. Several constants in number theory are of the form $C_{f,g}(n) := \prod_{p>p_n}(1 - \frac{f(p)}{g(p)})$, where $f(t)$ and $g(t)$ are monic polynomials with integer coefficients satisfying $\deg f + 2 \le \deg g$ and the product is over all primes $p > p_n$.For example $A = \prod_p (1 - \frac{1}{p(p-1)})$, the Artin constant, $T = \prod_{p>2}(1 - \frac{1}{(p-1)^2})$, the twin-prime constant and $S = \prod_p (1 - \frac{p}{p^3-1})$, the Stephens constant, all satisfy this format. In this paper we give a method for numerically evaluating $C_{f,g}(n)$ up to high precision, and in particular the aforementioned constants will be considered in more detail.

The basic idea is to express $\log C_{f,g}(n)$ in the form $\sum_{k\ge 2} e_k \log \zeta_n(k)$, where $\zeta_n(s) = \zeta(s)\prod_{p\le p_n}(1-p_n^{-s})$ denotes the partial zeta function. Since one has good numerical approximations for the $\zeta_n(k)$, a cut-off of the series should result in a reasonable approximation of $\log C_{f,g}(n)$. Note that $\log \zeta_n(k) = p_{n+1}^{-k}(1 + o(1))$, as k tends to infinity. Thus we can improve efficiency by taking $m > n$, approximate $C_{f,g}(m)$ with the desired accuracy and then approximate $C_{f,g}(n)$ in the obvious way. In practice one easily obtains several hundred digits of precision in this way. Bach [1] has shown that by this method A and T can be computed to t bits of precision using $O(t^{3+o(1)})$ bit operations, where the factor implied by the symbol $o(1)$ depends on the cost of the underlying arithmetic, but for practical purposes can be taken as $\log t$. Bach's arguments also work for the constant $C_{f,g}(n)$ and one finds the precision bound $O(t^{3+o(1)})$.

The best published approximation to date of the Artin's constant seems to be that of Wrench [12]. He considers $\log A$ and expands it into series in terms of $\sum_{p\ge 2} p^{-k}$, $k \ge 2$. Using tables of $\sum_{p\ge 2} p^{-k}$ to 50D prepared by R. Liénard he then arrives at a 45D approximation to A. Proceeding similarly as for the Artin constant, he also gave a $42D$ approximation to T. In both cases his decimals match with those found by us.

The coefficients e_k appearing in $\log C_{f,g}(n) = \sum_{k\ge 2} e_k \log \zeta_n(k)$ for A, T and S turn out to have an interpretation in the theory of formal languages. Hence in §4 we recall some basic notions and prove some results relevant for our purposes. In §5 we investigate the sign of c_k. In §6 we deal with several examples. Finally in §7 we consider the error made if one approaches Artin type constants only with finitely many zeta values.

2 The method

As usual let μ denote the Möbius function.

Lemma 1 *Let $F(t) = t^\delta + a_1 t^{\delta-1} + \cdots + a_\delta \in \mathbb{Z}[t]$ be a monic polynomial of degree δ. Let $\alpha_1, \cdots, \alpha_\delta$ be its roots. Put $s_F(k) = \alpha_1^k + \cdots + \alpha_\delta^k$. The $s_F(k)$ are integers and satisfy the recursions*

$$s_F(k) + a_1 s_F(k-1) + \cdots + a_{k-1} s_F(1) + k a_k = 0, \tag{1}$$

with $a_{\delta+1} = a_{\delta+2} = \cdots = 0$. Define $b_F(k)$ by $b_F(k) = \frac{1}{k}\sum_{d|k} s_F(d)\mu(\frac{k}{d})$. Then $b_F(k) \in \mathbb{Z}$. Moreover, $\hat{F}(t)$, the reciprocal polynomial of $F(t)$, satisfies the formal identity

$$\hat{F}(t) = \prod_{j=1}^{\infty} (1-t^j)^{b_F(j)}. \tag{2}$$

Proof. The recursions (1) were already known to Newton. They allow one to easily compute the $s_F(k)$ and, moreover, they show that the $s_F(k)$ must be integers. Another way of seeing that, is by noticing that the $s_F(k)$ are traces of algebraic integers and hence rational integers.

Consider $\hat{F}(t)$, the reciprocal polynomial of $F(t)$. We have

$$\hat{F}(t) = t^\delta F(\frac{1}{t}) = 1 + a_1 t + \cdots + a_\delta t^\delta = \prod_{j=1}^{\delta}(1-\alpha_j t).$$

By logarithmic differentation one obtains

$$-\frac{t\hat{F}'(t)}{\hat{F}(t)} = \sum_{j=1}^{\delta} \frac{\alpha_j t}{1-\alpha_j t} = \sum_{j=1}^{\infty} s_F(j) t^j. \tag{3}$$

We can formally write $\hat{F}(t)$ in the form

$$\hat{F}(t) = \prod_{j=1}^{\infty} (1-t^j)^{c_F(j)}, \tag{4}$$

where by $(1-t^j)^{c_F(j)}$, we denote $\sum_{k=0}^{\infty}\binom{c_F(j)}{k}t^k$. Notice that $c_F(1)=-a_1$. In general $c_F(j)$ equals the coefficient of $-t^j$ in the Taylor series of

$$\hat{F}(t)\prod_{k=1}^{j-1}(1-t^k)^{-c_F(k)} \tag{5}$$

and is thus uniquely determined. Clearly $c_F(1)$ is an integer, now assume that $c_F(2),\cdots,c_F(j-1)$ are integers. Then all the j terms in (5) have Taylor series with integer coefficients and hence $c_F(j)$ is an integer.

We now complete the proof by showing that, for $j\geq 1$, $b_F(j)=c_F(j)$. From (3) and (4) it follows that

$$\sum_{j=1}^{\infty}s_F(j)t^j=\sum_{j=1}^{\infty}jc_F(j)\frac{t^j}{1-t^j}, \tag{6}$$

and hence, for $j\geq 1$, $s_F(j)=\sum_{d|j}dc_F(d)$. By Möbius inversion it follows that $jc_F(j)=\sum_{d|j}s_F(d)\mu(j/d)$, and thus $b_F(j)=c_F(j)$. □

Remark. Let $f(t)=1+\sum_{i=1}^{\infty}a_it^i$ be a Taylor series with $a_i\in\mathbb{Z}$. Then $f(t)$ satisfies a formal identity of the form $f(t)=\prod_{j=1}^{\infty}(1-t^j)^{b_f(j)}$ with integer coefficients $b_f(j)$. This is easily deduced from Lemma 1 on noticing that $b_f(k)$ only depends on $a_1,\cdots,a_k$.

Recall that $\zeta_n(s)=\zeta(s)\prod_{p\leq p_n}(1-p^{-s})$.

Theorem 1 *Let $f(t),g(t)\in\mathbb{Z}[t]$ be monic polynomials satisfying* $\deg f+2\leq\deg g$. *Let β be the modulus of a root of maximum modulus amongst those of $g-f$ and g. Let n_0 be such that $p_{n_0+1}>1/\beta$. Then, for $n\geq n_0$,*

$$C_{f,g}(n)=\prod_{p>p_n}(1-\frac{f(p)}{g(p)})=\prod_{j=2}^{\infty}\zeta_n(j)^{b_g(j)-b_{g-f}(j)}, \tag{7}$$

where the integers $b_g(j)$ and $b_{f-g}(j)$ are defined in Lemma 1. For all j sufficiently large $b_g(j)=b_{g-f}(j)$ if and only if $1-f(t)/g(t)$ is a finite product of cyclotomic polynomials.

Proof. Using (2) we find that

$$1-\frac{f(1/t)}{g(1/t)}=\prod_{j=1}^{\infty}\left(1-t^j\right)^{b_{g-f}(j)-b_g(j)}. \tag{8}$$

That $b_{g-f}(j)$ and $b_g(j)$ are integers follows from Lemma 1. The condition $\deg f+2\leq\deg g$ implies that $b_{g-f}(1)=b_g(1)$. Up to this point (8) is only established as a formal identity. We want to establish (8) for all $|t|<\rho$, $t\in\mathbb{C}$, for some $\rho>0$. Let β denote the modulus of a root of maximum modulus amongst those of $g-f$ and g. Since g and $g-f$ are monic with integer coefficients, we have $\beta\geq 1$. First assume $\beta=1$. Then $g-f$ and g are products of cyclotomic polynomials. Using the expression $\Phi_n(t)=\prod_{d|n}(t^d-1)^{\mu(n/d)}$ for the nth cyclotomic polynomial, we then find that the product in (8) is actually finite. Moreover, the l.h.s. and the r.h.s. in (8) agree everywhere not on the unit circle. Using this, the theorem easily follows in this case. Thus we may assume $\beta > 1$. Notice that $|b_{g-f}(j) - b_g(j)| \le 2(\deg\, g)\beta^j$. ¿From the theory of infinite products we use that a product $\prod(1+\epsilon_\nu)$ is called absolutely convergent if $\sum \epsilon_\nu$ is absolutely convergent and that in an absolutely convergent product the factors can be reordered without changing its value. Using this we see that the product in (8) is absolutely convergent if $\sum_{j=1}^{\infty} |b_{g-f}(j) - b_g(j)| t^j$ is absolutely convergent, which is certainly the case for $|t| < 1/\beta$. From this and (8) and the definition of n_0, we deduce that, for $n \ge n_0$,

$$C_{f,g}(n) = \prod_{p>p_n} \prod_{j=2}^{\infty} \left(1 - \frac{1}{p^j}\right)^{b_{g-f}(j)-b_g(j)}.$$

Now if we can establish that the latter double product is absolutely convergent, we have

$$\begin{aligned} C_{f,g}(n) &= \prod_{j=2}^{\infty} \prod_{p>p_n} \left(1 - \frac{1}{p^j}\right)^{b_{g-f}(j)-b_g(j)} \\ &= \prod_{j=2}^{\infty} \zeta_n(j)^{b_g(j)-b_{g-f}(j)} \end{aligned}$$

and we are done. It remains to show that

$$\sum_{j=2}^{\infty} |b_{g-f}(j) - b_g(j)| \sum_{p>p_n} \frac{1}{p^j}$$

converges. This is easy and left to the reader. □

3 Connection with arithmetic functions that are prime-independent and multiplicative

Let f be a multiplicative arithmetic function. It is said to be prime-independent if $f(p^\nu)$ depends at most on ν. To the constant $C_{f,g}(0)$ we associate the Dirichlet series

$$L_{f,g}(s) = \prod_p \left(1 - \frac{f(p^s)}{g(p^s)}\right) = \sum_{m\ge1} \frac{a_m}{m^s}.$$

Then $m \mapsto a_m$ is a prime-independent multiplicative function. Let $\gamma(n)$ denote the core function, that is $\gamma(n) = \prod_{p|n} p$. An integer n is called square full if $\gamma(n)^2 | n$. First consider the Artin constant. Then $a_m = \mu(\gamma(m))$ if m is square full and $a_m = 0$ otherwise. For the Stephens constant we have $a_1 = 1$ and, for $m > 1$, $a_m = \mu(\gamma(m))$ in case all the exponents in the canonical prime factorization of m are congruent to $2 (\mathrm{mod}\ 3)$ and $a_m = 0$ otherwise. For the twin-prime constant one easily sees that if m is squarefull, then $a_m = \mu(\gamma(m)) d(m/\gamma(m)^2)$ and $a_m = 0$ otherwise.

In [7] (see also [6, Ch.2, §7]) zeta-formulae for PIM functions are considered. We recall some of the results mentioned there, that are relevant for us.

An arithmetic function h is said to have to have a zeta-formula if, formally, $\sum_{m=1}^{\infty} h(m)m^{-s} = \prod_{k=1}^{\infty} \zeta(ks)^{e_k}$, with $e_k \in \mathbb{Z}$. In case $e_k \neq 0$ for at most finitely many k, h is said to have a finite zeta-formula. To a function h that is PIM we can associate a formal power series given by $\hat{h}(y) = \sum_{r=0}^{\infty} f(p^r)y^r$, where for p we can choose any prime. A series $\hat{h}(y) \in \mathbb{Z}[[y]]$ will be called a cyclotomic rational if it can be expressed as a finite product of cyclotomic polynomials and inverses of these, where a cyclotomic polynomial is one of the form $\Phi_m(y) = \prod_i (y - \tilde{\alpha}_i) \in \mathbb{Z}[y]$ (where $\tilde{\alpha}_1, \tilde{\alpha}_2, \cdots$ denote the distinct primitive mth roots of unity), if $m > 1$, or $\Phi_1(y) = 1 - y$. It can be shown that h possesses a finite ζ-formula if and only if h is PIM and its associated power series $\hat{h}(y)$ is a cyclotomic rational. It follows that $L_{f,g}(s)$ has a finite zeta-formula if and only if $1 - f(t)/g(t)$ is a cyclotomic rational. Clearly if $L_{f,g}(s)$ converges for $\mathrm{Re}(s) \geq 1$, then $C_{f,g}(0) = \prod_{k=2}^{\infty} \zeta(k)^{e_k}$.

4 Formal languages

4.1 Languages

Let $\mathcal{A}$ be a set which we call an alphabet. (For our discussion we will assume that $\mathcal{A}$ is finite.) A word w on $\mathcal{A}$ is a finite sequence of elements of $\mathcal{A}$, that is $w = (a_1, a_2, \cdots, a_n)$, $a_i \in \mathcal{A}$. The set $\mathcal{A}^*$ of all words on the alphabet $\mathcal{A}$ is equipped with the associative operation defined by the concatenation of two sequences; $(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n) = (a_1, a_2, \cdots, a_n, b_1, \cdots, b_n)$. We say two words are conjugate if they are obtained from each other by a cyclic permutation. The conjugacy relation is an equivalence relation. A word $x \in \mathcal{A}^*$ is called primitive if it is not a power of another word. Thus x is primitive if $x = y^n$ with $n \geq 0$ implies $x = y$. It is not difficult to show that each non-empty word is a power of a unique primitive word. Thus $x = r^e$, with r an unique primitive word. The number e is called the exponent of x. It is not difficult to see that all words in a conjugacy class C have the same exponent, say e. If the length of these words is n, then $\mathrm{card}(C) = n/e$. Any subset $\mathcal{L}$ of $\mathcal{A}$ is called a language. For convenience we restrict ourself to languages that are closed under conjugation. For all $n \geq 1$, denote the number of words of length n by $w_{\mathcal{L}}(n)$ and the number of conjugacy classes of primitive words in $\mathcal{L}$ of length n by $\mathfrak{p}_{\mathcal{L}}(n)$. We define

$$\zeta_{\mathcal{L}}(t) = \exp\left(\sum_{n\geq 1} \frac{w_{\mathcal{L}}(n)}{n} t^n\right),$$

to be the zeta-function of $\mathcal{L}$. As a first and one of the easiest examples of a language let us consider, $\mathcal{L}_1$, the language of all words over an alphabet $\mathcal{A}$ with k letters. Clearly $w_{\mathcal{L}}(n) = k^n$. Now for $n \geq 1$

$$k^n = \sum_{d|n} d\mathfrak{p}_{\mathcal{L}_1}(d). \tag{9}$$

Indeed, every word of length n belongs to exactly one conjugacy class of words of length n. Each class has $d = n/e$ elements, where e is the exponent of its words. Since there are as many classes whose words have exponent n/e as there are classes of primitive words of length $d = n/e$, (9) is established. By Möbius inversion it follows from (9) that

$$\mathfrak{p}_{\mathcal{L}_1}(n) = \frac{1}{n}\sum_{d|n} k^d \mu(\frac{n}{d}). \tag{10}$$

Note that $\zeta_{\mathcal{L}_1}(t) = (1-kt)^{-1}$.

A language $\mathcal{L}$ is called cyclic if it is closed under conjugation and for any integer $n \geq 1$, $w \in \mathcal{L}$ if and only if $w^n \in \mathcal{L}$. For a cyclic language we have similarly to equation (9) and (10)

$$w_{\mathcal{L}}(n) = \sum_{d|n} d\mathfrak{p}_{\mathcal{L}}(d) \text{ and } \mathfrak{p}_{\mathcal{L}}(n) = \frac{1}{n}\sum_{d|n} w_{\mathcal{L}}(d)\mu(\frac{n}{d}).$$

Arguing as in the proof of Lemma 1 we deduce that for a cyclic language $\mathcal{L}$

$$\zeta_{\mathcal{L}}(t) = \prod_{n\geq 1} \frac{1}{(1-t^n)^{\mathfrak{p}_{\mathcal{L}}(n)}}. \tag{11}$$

Obviously $\mathcal{L}_1$ is a cyclic language, we next discuss a slightly more complicated cyclic language. Let $\mathcal{L}_2$ be the set of words on the alphabet $\{a, b, c\}$ of the form $a^{n_0}bca^{n_1}bc\cdots bca^{n_r}$ for some $r \geq 1$ and $n_i \geq 0$, or of the form $ca^{n_0}bca^{n_1}bc\cdots bca^{n_r}b$ for some $r \geq 0$ and $n_i \geq 0$. Then $\mathcal{L}_2$ is cyclic. Note that the cyclic permutations of abc yield the words in $\mathcal{L}_2$ of length 3. Note that the two cyclic permuations of $bcbc$ and the four of $aabc$ give all words of length 4. Thus $\mathfrak{p}_{\mathcal{L}_2}(3) = 1$ and $\mathfrak{p}_{\mathcal{L}_2}(4) = 1$. For lengths 5,6 and 7 we find that representative of the conjugacy classes of primitive words are *aaabc*, *abcbc*, *aaaabc*, *aabcbc* and *aaaaabc*, *aaabcbc*, *aabcabc*, *abcbcbc* respectively. Using induction one sees that $w_{\mathcal{L}_2}(n) = L_n - 1$, where L_n is the nth Lucas number (which is recursively defined by $L_{n+1} = L_n + L_{n-1}$, $n \geq 1$, $L_0 = 2$ and $L_1 = 1$). Thus $w_{\mathcal{L}_2}(n) = \theta^n + \bar{\theta}^n - 1$, with $\theta = (1+\sqrt{5})/2$. Note that $\zeta_{\mathcal{L}_2}(t) = (1-t)/(1-t-t^2)$.

Let $\mathcal{L}_3$ be the set of words on the alphabet $\{a, b, c, d\}$ that have the form $(abc)^{n_0}(ad)^{m_0}\cdots(abc)^{n_i}(ad)^{m_i}$, or $(bca)^{n_0}(da)^{m_0}(bca)^{n_1}(da)^{m_1}\cdots(bca)^{n_i}(da)^{m_i}$, or the form $ca(da)^{m_0}b\cdots ca(da)^{m_i}b$, with $m_0 \geq 1$. Then $\mathcal{L}_3$ is cyclic. Let R_n be the recurrence defined by $R_1 = 0,\ R_2 = 2,\ R_3 = 3$ and $R_n = R_{n-2} + R_{n-3},\ n \geq 4$. Then using induction one finds $w_{\mathcal{L}_3}(n) = R_n$ if $3 \nmid n$ and $w_{\mathcal{L}_3}(n) = R_n - 3$ otherwise. Notice that there are no primitive words of length 6. For length 7 there is just one, up to conjugation, namely *abcadad*. Thus $\mathfrak{p}_{\mathcal{L}_3}(6) = 0$ and $\mathfrak{p}_{\mathcal{L}_3}(7) = 1$. Let ω denote a 3rd primitive root of unity. Note that $R_n = \alpha_1^n + \alpha_2^n + \alpha_3^n$, where α_1, α_2 and α_3 are the roots of $t^3 - t - 1$. Using this one finds that $\zeta_{\mathcal{L}_3}(t) = (1-t^3)/(1-t^2-t^3)$.

4.2 Automata

An automaton $\mathfrak{A}$ over $\mathcal{A}$ is composed of a set Q (the set of states), a subset I of Q (the initial states), a subset T of Q (the terminal or final states), and a set $\mathcal{F} \subset Q \times A \times Q$, called the set of edges. The automaton is denoted by $\mathfrak{A} = (Q, I, T)$. The automaton is finite when the set Q is finite. A path in the automaton is a sequence $c = (f_1, \cdots, f_n)$ of consecutive edges $f_i = (q_i, a, q_{i+1}),\ 1 \le i \le n$. The word $w = a_1 a_2 \cdots a_n$ is the label of the path c. A path $c : i \to t$ with $i \in I$ and $t \in T$ is called succesful. The set recognized by $\mathfrak{A}$, denote by $\mathcal{L}(\mathfrak{A})$, is defined as the set of labels of succesful paths.

Let $\mathbb{Z}[[A]]$ be the commutative algebra of formal power series in the variables $a \in A$. Call matrix of an automaton $\mathfrak{A}$ the matrix E in $\mathbb{Z}[A]^{Q\times Q}$ defined by

$$E_{p,q} = \sum_{\substack{a \\ p\to q}} a,$$

where $\overset{a}{p\to q}$ means that there is an edge labelled a from p to q. Call determinant of $\mathfrak{A}$, $\det(\mathfrak{A})$, the polynomial in $\mathbb{Z}[[A]]$ given by $\det(I-E)$, where I is the $Q \times Q$ identity matrix. Let $\theta :\ \mathbb{Z}[[A]] \to \mathbb{Z}[[t]]$ denote the homomorphism determined by $\theta(a) = t$, for any letter a in A. It is well-known that:

Proposition 1 *Let $\mathfrak{A}$ be a finite automaton and $\mathcal{L}(\mathfrak{A})$ the language accepted by it, then*

$$\zeta_{\mathcal{L}(\mathfrak{A})}(t) = \theta(\det(I-E)^{-1}) = \theta(\det(\mathfrak{A})^{-1}).$$

It follows from Proposition 1 that $\zeta_{\mathcal{L}(\mathfrak{A})}(t) = 1/\hat{F}(t)$, with $\hat{F}(t)$ the reciprocal of a monic polynomial $F(t) \in \mathbb{Z}[t]$. Comparison of (2) and (11) then shows that $b_F(k) = \mathfrak{p}_{\mathcal{L}(\mathfrak{a})}(n) \ge 0$. This gives rise to the question which monic polynomials $F(t)$ have the property that $1/\hat{F}(t)$ occurs as the zeta function of some finite automaton. This seems a difficult question. If $F(t)$ is of degree 2, the answer is that this only happens if the coefficient of t is non-positive and the discriminant is non-negative.

We next give an example of a fairly large class of polynomials that can be realized as zeta functions of automata. Let $n \ge 1$, $a_1, \cdots, a_n$ be non-negative integers and $a_n > 0$. Consider the following automaton, $\mathfrak{A}(a_1, \cdots, a_n)$. It has $Q = I = \{1, 2, \cdots, n\}$. We label all its edges ($n-1+\sum a_i$ in total), with different letters. It has a_1 edges going from the first to the first state. It has an edge going from the first to the second state, from the second to the third, etc., and one from state $n-1$ to state n. For $2 \le i \le n$, it has a_i edges going from the ith state to the first. These are all the edges in $\mathfrak{A}(a_1, \cdots, a_n)$.

Lemma 2 *We have*

$$\zeta_{\mathcal{L}(\mathfrak{A}(a_1,\cdots,a_n))}(t) = \frac{1}{1 - a_1 t - a_2 t^2 - \cdots - a_n t^n}.$$

Proof. From the definition of $\mathfrak{A}(a_1, \cdots, a_n)$ it follows that $\theta(\det(\mathfrak{A}(a_1, \cdots, a_n)))$ equals

$$\det \begin{pmatrix} 1-a_1t & -t & 0 & 0 & \cdots & 0 & 0 \\ -a_2t & 1 & -t & 0 & \cdots & 0 & 0 \\ -a_3t & 0 & 1 & -t & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ -a_nt & 0 & 0 & 0 & \cdots & 1 & -t \end{pmatrix} = 1 - a_1 t - a_2 t^2 - \cdots - a_n t^n,$$

where the latter equality is easily proved on using induction with respect to n. The result now follows on invoking Proposition 1. □

4.3 Traces of languages

Denote by $\mathbb{Z}\langle\langle A\rangle\rangle$ the set of non-commutative formal powers series over $\mathbb{Z}$ on the alphabet A. Each language $\mathcal{L}$ defines a series, its characteristic series defined by $\underline{\mathcal{L}} = \sum_{w\in\mathcal{L}} w$. Now, let $\mathfrak{A}$ be a finite automaton over $\mathcal{A}$, and define a formal power series, called the trace of $\mathfrak{A}$ and denoted by $\mathrm{tr}(\mathfrak{A})$, by $\mathrm{tr}(\mathfrak{A}) = \sum_{w\in A^*} \alpha_w w$, where the coefficient α_w of the word w is equal to the number of couples (q, c), where q is a state in $\mathfrak{A}$ and c is a path $q \to q$ in $\mathfrak{A}$ labelled w. A language $\mathcal{L}$ is said to be recognizable if there exists an automaton $\mathfrak{A}$ such such that $\mathcal{L} = \mathcal{L}(\mathfrak{A})$. It was proved by Berstel and Reutenauer [2] that the characteristic series of each cyclic recognizable language is a linear combination over $\mathbb{Z}$ of traces of finite deterministic automata. Thus for a cyclic recognizable language there exists $s \geq 1$ and automata, $\mathfrak{A}_1, \cdots, \mathfrak{A}_s$ and $b_1, \cdots, b_s \in \mathbb{Z}$ such that $\underline{\mathcal{L}} = \sum_{i=1}^{s} b_i \mathrm{tr}(\mathfrak{A}_i)$. A consequence of this identity is (see [2, p. 539]) that

$$\zeta_{\mathcal{L}}(t) = \prod_{i=1}^{s} \zeta_{\mathfrak{A}_i}(t)^{b_i}. \tag{12}$$

Since the zeta functions of finite automata are rational, we deduce the important consequence that the zeta function of a cyclic recognizable language is rational. A question that arises is which rational functions occur as a zeta function of a cyclic recognizable language. If a rational function can be realized as the zeta function of a cyclic recognizable language, then one has an interpretation for the coefficients in (7) for the associated Artin type constant.

5 Positivity

Once we have a representation of the form $\prod_{k=2}^{\infty} \zeta(k)^{e_k}$ for an Artin type constant it is of some importance to investigate the positivity of the e_k. Thus if for every k sufficiently large e_k is positive, then $\prod_{k=2}^{N} \zeta(k)^{-e_k}$ is an upper bound for the Artin type constant for every N sufficiently large. If all the roots having maximum modulus amongst the roots of $g - f$ and f are equal, are roots of $g - f$, are real and greater than one, then it is easy to see that $e_k > 0$ for every k sufficiently large. The next few results help one further to determine the positivity of the e_k.

Lemma 3 *For every $k \geq 1$ and $t > 1$ we have $\sum_{d|k} t^d \mu(k/d) > 0$.*

Proof. For $k = 1$ the result is obvious, so assume $k \geq 2$. For $t > 1$, we have $t^d = e^{(\log t)d} = \sum_{r=0}^{\infty} \frac{(\log t)^r d^r}{r!}$. Thus

$$\sum_{d|k} t^d \mu(k/d) = \sum_{r=0}^{\infty} \frac{(\log t)^r}{r!} A_r(k), \tag{13}$$

where $A_r(k) = \sum_{d|k} d^r \mu(k/d)$. Notice that $A_r(k)$ as a convolution product of two multiplicative functions, is a multiplicative function of k. The latter observation allows one to deduce almost immediately that $A_r(k) = k^r \prod_{p|k}(1 - 1/p^r)$. In particular $A_0(k) = 0$ and $A_r(k) > 0$ for $r \geq 1$. Thus every term in the infinite series in (13), except the first which is zero, is positive. □

Let $\mathbb{Z}^-[t]$, respectively $\mathbb{Z}^+[t]$, denote the set of monic polynomials $f(t) = t^n + a_1t^{n-1} + \cdots + a_n$, with, for $1 \le i \le n$, $a_i \le 0$, respectively $a_i \ge 0$.

Lemma 4 *Let $F(t) = t^\delta - a_1t^{\delta-1} - \cdots - a_\delta \in \mathbb{Z}^-[t]$ and $k \ge 1$. Then $b_F(k) \ge 0$. Moreover, $b_F(k) > 0$ for every $k \ge 1$ if and only if $a_1 \ge 2$ or $a_1 = 1$ and $a_2 \ge 1$.*

Proof. The language accepted by a finite automaton with $Q = I = T$ and having different letters at each edge is cyclic. Thus, in particular, $\mathfrak{A}(a_1, \cdots, a_n)$ is cyclic. As such its zeta function satisfies (11). By Lemma 2 it then follows that

$$1 - a_1t - \cdots - a_nt^n = \prod_{k\ge1}(1-t^k)^{\mathfrak{p}_{\mathfrak{L}(\mathfrak{A}(a_1,\cdots,a_n))}(k)}.$$

On the other hand, by the proof of Lemma 1, we have

$$1 - a_1t - \cdots - a_nt^n = \prod_{k\ge1}(1-t^k)^{b_F(k)}. \tag{14}$$

By the proof of Lemma 1 again the coefficients $b_F(k)$ are unique. Hence it follows that $b_F(k) = \mathfrak{p}_{\mathfrak{L}(\mathfrak{A}(a_1,\cdots,a_n))}(k) \ge 0$. The latter part of the assertion is left to the reader. □

The next lemma shows that even in cases negative coefficients occur in (7), an interpretation in terms of formal languages might still be possible.

Lemma 5 *Let $G(t) = t^\delta + \cdots + (-1)^{i+1}a_it^{\delta-i} + \cdots + (-1)^\delta a_\delta$ with $a_i \ge 0$ and $F(t) = G(-t)$. Then, for k odd, $b_G(k) = -b_F(k) \le 0$ and, for k even, $b_G(k) \ge b_F(k) \ge 0$.*

Proof. Note that $F(t) = t^\delta - a_1t^{\delta-1} - \cdots - a_\delta$. The reciprocal polynomial of $G(t)$, $\hat{G}(t)$, equals $\hat{F}(-t)$. By the proof of Lemma 1 we have $\hat{F}(t) = \prod_{k=1}^\infty(1-t^k)^{b_F(k)}$. From this it easily follows that $\hat{G}(t) = \hat{F}(-t) = \prod_{k=1}^\infty(1-t^k)^{b_G(k)}$, with $b_G(k) = -b_F(k)$ for k is odd, $b_G(k) = b_F(k)$ if $4|k$ and $b_G(k) = b_F(k) + b_F(k/2)$, for the other even k. Since $b_F(k) \ge 0$ by Lemma 4, the proof is completed. □

Next we apply Lemma 5 to a constant related to the non-vanishing, on average, of L-series, see [10, p. 110]. Put

$$c = \frac{1}{8\pi^2}\prod_p\left(1 - \frac{4p^2-3p+1}{p^4+p^3}\right).$$

Then using Lemma 5 and 4, we find that $48c = \prod_{k=2}^\infty \zeta(k)^{e_k}$, with the e_k integers and $\mathrm{sign}(e_k) = (-1)^{k+1}$.

Lemma 6 *Let $f \in \mathbb{Z}[t]$, with f not necessarily monic. Suppose that f has only non-negative coefficients. Moreover, let $g \in \mathbb{Z}^-[t]$ with $\deg g > \deg f$. Then $b_{g-f}(k) \ge b_f(k)$ for $k \ge 1$.*

Proof. We will construct a cyclic language $\mathfrak{L}_{f,g}$ such that $\mathfrak{p}_{\mathcal{L}_{f,g}}(k) = b_{g-f}(k) - b_f(k)$. Since trivially $\mathfrak{p}_{\mathcal{L}_{f,g}}(k) \ge 0$, the result then follows.

Write $f(t) = b_1t^{n-1} + \cdots + b_n$ and $g(t) = t^n - a_1t^{n-1} + \cdots - a_n$. By assumption $a_i, b_i \ge 0$. Consider the automaton $\mathfrak{A}(a_1, \cdots, a_n)$. By appropriately labelling the edges of $\mathfrak{A}(a_1+b_1,\cdots,a_n+b_n)$, $\mathcal{L}(\mathfrak{A}(a_1,\cdots,a_n))$ becomes a subset of $\mathcal{L}(\mathfrak{A}(a_1+b_1,\cdots,a_n+b_n))$. Now consider the language $\mathcal{L}_{f,g}=\mathcal{L}(\mathfrak{A}(a_1+b_1,\cdots,a_n+b_n))-\mathcal{L}(\mathfrak{A}(a_1,\cdots,a_n))$. We have $\underline{L}_{f,g}=\mathrm{tr}(\mathfrak{A}(a_1+b_1,\cdots,a_n+b_n))-\mathrm{tr}(\mathfrak{A}(a_1,\cdots,a_n))$ and hence, by (12) and Lemma 2,

$$\zeta_{\mathcal{L}_{f,g}}(t)=\frac{1-a_1t-\cdots-a_nt^n}{1-(a_1+b_1)t-\cdots-(a_n+b_n)t^n}=\frac{g(\frac{1}{t})}{g(\frac{1}{t})-f(\frac{1}{t})}.$$

On the other hand, by (11),

$$\zeta_{\mathcal{L}_{f,g}}(t)=\prod_{j\geq 1}\frac{1}{(1-t^n)^{\mathfrak{p}_{\mathcal{L}_{f,g}}(j)}}.$$

Thus

$$1-\frac{f(1/t)}{g(1/t)}=\prod_{j\geq 1}(1-t^j)^{\mathfrak{p}_{\mathcal{L}_{f,g}}(j)}.$$

On comparing this with (8), the result follows. □

6 Examples

6.1 The Artin constant

Consider an integer a that is not -1 or a square. Artin conjectured in 1927 that there are infinitely many primes p such that a is a primitive root mod p, that is $<a>\cong\mathbb{F}_p^*$. Hooley [5] proved, subject to GRH, the truth of this and, moreover, computed, under GRH, the natural density of primes p such that a is a primitive root mod p. This turns out to be a rational number, depending possibly on a, times the Artin constant.

For the Artin constant we have $f(t)=1$ and $g(t)=t(t-1)$. The conditions of Lemma 6 are satisfied and we find $A=\prod_{k=2}^{\infty}\zeta(k)^{-e_k}$, with $e_k\geq 0$. Put $a_k=(\frac{1+\sqrt{5}}{2})^k+(\frac{1-\sqrt{5}}{2})^k-1$, thus a_k is given by the recursion $a_1=0,\ a_2=2$ and, for $k\geq 2$, $a_k=a_{k-1}+a_{k-2}+1$. Now $e_k=\{\sum_{d|k}a_d\mu(k/d)\}/k$. We find $e_1,e_2,\cdots$ is $0,1,1,1,2,2,4,5,8,\cdots$. Notice that $e_k=\mathfrak{p}_{\mathcal{L}_2}(k)\geq 0$. Using the trivial inequality $e_k\geq\tau^k/k-\tau^{k/2}-1$ with $\tau=(1+\sqrt{5})/2$, it is easily seen that $e_k\geq 1$ for $k\geq 2$. This confirms a belief expressed by Bach [1, p. 149].

6.2 The Stephens constant

Let $U=\{U_n\}_{n=0}^{\infty}$ be a sequence of integers. We say that m divides the sequence U if m divides at least one term of the sequence. Denote by $\delta(U)$ the natural density of primes p that divide U, if it exists. Stephens [11] proved, subject to GRH, that $\delta(U)$ exists for a large class of second order linear recurrences. Moreover he showed, subject to GRH, that for these sequences $\delta(U)$ equals a rational number times the Stephens constant.

For the Stephens constant we have $f(t)=t$ and $g(t)=t^3-1$. The conditions of Lemma 6 are satisfied and we find $S=\prod_{k=2}^{\infty}\zeta(k)^{-e_k}$, with $e_k\geq 0$. Let $\alpha_1,\alpha_2,\alpha_3$

denote the roots of t^3-t-1. Put $r_k=\alpha_1^k+\alpha_2^k+\alpha_3^k$. Then $r_1=0,\ r_2=2$ and $r_3=3$ and, for $k\ge 4$, $r_k=r_{k-2}+r_{k-3}$. Put $\omega=e^{2\pi/3}$. Then $a_k=\alpha_1^k+\alpha_2^k+\alpha_3^k-1-\omega^k-\omega^{2k}$ and thus $a_k=r_k-3$ if $3|k$ and $a_k=r_k$ otherwise. Then $e_k=\{\sum_{d|k}a_d\mu(k/d)\}/k$. Thus the coefficients we get are precisely the $\mathfrak{p}_{\mathcal{L}_3}(k)$. In particular it follows again that they are all non-negative. We find $e_1,e_2,\cdots$ is $0,1,0,0,1,0,1,1,1,1,2,\cdots$

6.3 The twin-prime constant

If p and $p+2$ are primes, they are called twin primes. Let $\pi_2(x)$ denote the number of twin-primes not exceeding x. It was conjectured by Hardy and Littlewood that

$$\pi_2(x)\sim 2T\frac{x}{(\log x)^2}.$$

For the twin-prime constant we find $T=\prod_{k=2}^{\infty}\zeta(k)^{-e_k}$, with $e_k=k^{-1}\sum_{d|k}2^d\mu(\frac{k}{d})$. By Lemma 3 it follows that $e_k>0$. In particular the coefficients we get are the $\mathfrak{p}_{\mathcal{L}_1}(n)$ for an alphabet with two letters. There is in this case of course an alternative interpretation of these numbers, namely as the number of irreducible monic polynomials of degree k over the finite field $\mathbb{F}_2$. We find $e_2,e_3,\cdots$ is $1,2,3,6,9,18,\cdots$.

6.4 Mertens' constant

In 1873 Mertens proved the existence of the limit

$$B=\lim_{x\to\infty}\left(\sum_{p\le x}\frac{1}{p}-\log\log x\right).$$

It turns out that $B=\gamma-H$, where

$$H=-\sum_{p}\left(\log(1-\frac{1}{p})+\frac{1}{p}\right)$$

and γ denotes Euler's constant. The language $\mathcal{L}_4$ associated to e^H has as single word and is non-cyclic. Trivially $\zeta_{\mathcal{L}_4}(t)=e^t$.

7 Incomplete expansions in partial zeta values

In this section we will state and prove a result on partial zeta expansions of Artin type that can be used to approximate them with any prescribed accuracy. It is crucial for this to be able to efficiently compute zeta values at integers up to high precision, for more on this see [3] and the references there in.

Theorem 2 *Let $f,g,\beta,n_0,\ b_f(j)$ and $b_{g-f}(j)$ be as in Theorem 1 and $n\ge n_0$. Put $e_j=b_{g-f}(j)-b_g(j)$. Then $C_{f,g}(n)=\prod_{k=2}^{\infty}\zeta(k)^{-e_k}$. Furthermore,*

$$-\log C_{f,g}(n)=\sum_{k=2}^{M}e_k\log\zeta_n(k)+E_M(n), \tag{15}$$

where

$$E_M(n) = \int_{p_{n+1}}^{\infty} (\pi(t) - n) r_M(t) dt,$$

with

$$r_M(t) = \frac{f(t)g'(t) - f'(t)g(t)}{g(t)(g(t) - f(t))} - \sum_{k=2}^{M} \frac{ke_k}{t(t^k - 1)}.$$

Moreover,

$$|E_M(n)| \leq 4\deg g \left(\frac{\beta}{p_{n+1}}\right)^M \frac{\beta}{1 - \frac{\beta}{p_{n+1}}}. \tag{16}$$

Proof. The first assertion is just a restatement of Theorem 1. We have

$$-\log C_{f,g}(n) = -\sum_{p>p_n} \log\left(1 - \frac{f(p)}{g(p)}\right) = -\int_{p_{n+1}-}^{\infty} \log\left(1 - \frac{f(t)}{g(t)}\right) d(\pi(t) - n).$$

and hence, by partial integration,

$$-\log C_{f,g}(n) = \int_{p_{n+1}}^{\infty} (\pi(t) - n) \left(\frac{f(t)g'(t) - f'(t)g(t)}{g(t)(g(t) - f(t))}\right) dt. \tag{17}$$

Notice that the choice $n \geq n_0$ ensures that the sum and integrals are well-defined. Likewise we deduce,

$$\log \zeta_n(k) = \int_{p_{n+1}}^{\infty} \frac{k(\pi(t) - n)}{t(t^k - 1)} dt \tag{18}$$

¿From (18) and (17) one deduces on invoking the definition of $r_M(t)$, the validity of (15). ¿From (6) and the proof of Theorem 1 we deduce that, for $t > \beta$,

$$\frac{g'(t) - f'(t)}{g(t) - f(t)} - \frac{g'(t)}{g(t)} = \sum_{k=2}^{\infty} \frac{ke_k}{t(t^k - 1)}.$$

Thus, for $t > \beta$,

$$r_M(t) = \sum_{k=M+1}^{\infty} \frac{ke_k}{t(t^k - 1)} \tag{19}$$

¿From this and the trivial estimate $\pi(t) - n \leq t$ the upper bound for $|E_M(n)|$ is easily deduced. □

If one is only interested in bounding the error $E_M(n)$, a shorter argument suffices. Note that

$$\zeta_n(k) \leq \sum_{m=p_{n+1}}^{\infty} \frac{1}{m^k} \leq p_{n+1}^{-k} + \int_{p_{n+1}}^{\infty} \frac{dt}{t^k} \leq p_{n+1}^{1-k}$$

for $k \geq 3$. Using this estimate we deduce that

$$\begin{aligned} \sum_{k=M+1}^{\infty} \beta^k \log \zeta_n(k) &\leq \sum_{k=M+1}^{\infty} \beta^k (\zeta_n(k) - 1) \leq \sum_{k=M+1}^{\infty} \beta^k p_{n+1}^{1-k} \\ &= (\frac{\beta}{p_{n+1}})^M \frac{\beta}{1 - \beta/p_{n+1}}. \end{aligned}$$

This, together with $C_{f,g}(n) = \prod_{k=2}^{\infty} \zeta(k)^{-e_k}$ and $|e_k| \leq 2(\deg g)\beta^k$, then yields (15) and (16).

7.1 The Mertens constant revisited

The method of proof of Theorem 2 can sometimes be applied to constants that are not of Artin type, cf. [4]. The Mertens constant provides such an example. Put $H_n = -\sum_{p>p_n}(\log(1-1/p)+1/p)$, thus $H_0 = H$. Reasoning as in the proof of Theorem 2 and making use of the identity

$$\frac{1}{t^2(t-1)} = -\sum_{m=2}^{\infty}\frac{\mu(m)}{t(t^m-1)}$$

valid for $t>1$, we obtain, for $n \ge 0$,

$$H_n = -\sum_{k=2}^{M}\frac{\mu(k)}{k}\log\zeta_n(k) + \int_{p_{n+1}}^{\infty}(\pi(t)-n)\rho_M(t)dt, \tag{20}$$

with $\rho_M(t) = 1/(t^2(t-1)) + \sum_{m=2}^{M}\mu(m)/(t(t^m-1))$. We close this section by comparing this approach to compute H with that of Lindqvist and Peetre [9]. Their starting point is equation (20) with $n=0$, that is

$$H = -\sum_{k=2}^{M}\frac{\mu(k)}{k}\log\zeta(k) + \int_{2}^{\infty}\pi(t)\rho_M(t)dt.$$

Put $\hat{\rho}_M(t) = \log(1-1/t) + 1/t + \mu(M)\log(1-t^{-M})/M$. Note that $\hat{\rho}_M(t)$ is a primitive of $\rho_M(t)$. On partly evaluating the latter integral one obtains

$$H = -\sum_{k=2}^{M}\frac{\mu(k)}{k}\log\zeta(k) + \sum_{j=1}^{n} j\hat{\rho}_M(t)|_{p_j}^{p_{j+1}} + \int_{p_{n+1}}^{\infty}\pi(t)\rho_M(t)dt. \tag{21}$$

Then by choosing M and n so as to minimize computational effort, they obtain an approximation with the desired accuracy. It is an elementary but tedious rewriting exercise to obtain (21) directly from (20) and the other way around. Thus the method of Lindqvist and Peetre for approximating H is equivalent with the incomplete partial zeta method.

The author likes to thank Gerd Mersmann, Prof. R. Tijdeman and Prof. Don Zagier for some helpful suggestions.

References

[1] E. Bach, The complexity of number-theoretic constants, *Information Processing Letters* **62** (1997), 145-152.

[2] J. Berstel and C. Reutenauer, Zeta functions of formal languages, *Trans. Amer. Math. Soc.* **321** (1990), 533-546.

[3] J.M. Borwein, D.M. Bradley and R.E. Crandall, Computational strategies for the Riemann zeta function, preprint.
http://www.cecm.sfu.ca/preprints/1998pp.html

[4] P. Flajolet and I. Vardi, Zeta function expansions of classical constants, manuscript, 1996.
http://pauillac.inria.fr/algo/flajolet/Publications/publist.html

[5] C. Hooley, Artin's conjecture for primitive roots, *J. Reine Angew. Math.* **225** (1967), 209-220.

[6] J. Knopfmacher, *Abstract analytic number theory*, North-Holland, Amsterdam, 1975. (Reprinted by Dover, New York, 1990.)

[7] J. Knopfmacher and J.N. Ridley, Prime-independent arithmetical functions, *Ann. Mat. Pura Appl.* **101** (1974), 153-169.

[8] K. Knopp, Infinite sequences and series, Dover, New York, 1956.

[9] P. Lindqvist and J. Peetre, On the remainder in a series of Mertens, *Expo. Math.* **15** (1997), 467-478.

[10] M. Ram Murty and V. Kumar Murty, *Non-vanishing of L-functions and applications*, Progress in Mathematics 157, Boston, Mass., Basel, Birkhäuser, 1997.

[11] P.J. Stephens, Prime divisors of second order linear recurrences I, II, *J. Number Theory* **8** (1976), 313-332, 333-345.

[12] J.W. Wrench, jr., Evaluation of Artin's constant and the twin-prime constant, *Math. Comp.* **15** (1961), 396-398.

Mathematisch Instituut, P.O.Box 9512, 2300 RA Leiden, The Netherlands.
(e-mail: `moree@wi.leidenuniv.nl`)