ELSEVIER

Theoretical Computer Science 237 (2000) 447–454

Theoretical Computer Science

www.elsevier.com/locate/tcs

On Hadamard square roots of unity

B. Litow

Department of Computer Science, James Cook University, Townsville, QLD4811, Australia

Received December 1998; revised July 1999
Communicated by M. Nivat

Abstract

A series all of whose coefficients have unit modulus is called an Hadamard square root of unity. We investigate and partially characterize the algebraic Hadamard square roots of unity. The investigation makes use of a result about the asymptotic behavior of the coefficients of algebraic series and the Weyl–von Neumann theorem.

Keywords: Algebraic series; Hadamard product; Analysis, Formal power series

1. Introduction

We work with power series over the complex numbers $\mathbb{C}$. The Hadamard product $h = f \odot g$ of power series f and g is defined by $[x^n]h = [x^n]f \cdot [x^n]g$. The coefficient of x^n in a series f is designated by $[x^n]f$. The identity element of the Hadamard product is the expansion of $1/1-x$. If $f \odot \bar{f} = 1/(1-x)$, f is said to be an Hadamard square root of unity. Here, $\bar{f}$ is defined by $[x^n]\bar{f} = \overline{[x^n]f}$, where the bar indicates complex conjugation. It is evident that f is an Hadamard square root of unity iff all of its coefficients have unit modulus. We are interested in identifying which algebraic series are Hadamard square roots of unity.

As a point of notation, we will find it convenient to define $\mathbf{e}(z) = \exp(2\pi\sqrt{-1} \cdot z)$.

We should be more precise about the term *algebraic series*. A substantial exposition of the concept of formal power series is given in [4]. For our purpose a formal series $f = \sum_{n=0}^{\infty} f_n \cdot x^n$ is algebraic if there exists a polynomial $p(x, y)$ with coefficients in $\mathbb{Q}$ such that $p(x, f) = 0$ is satisfied identically. This means that in a term-by-term

E-mail address: bruce@cs.jcu.edu.au (B. Litow)

0304-3975/00/$ - see front matter
PII: S0304-3975(99)00327-8

expansion of $p(x, f)$ as a formal series the coefficient of each power of x is zero. For example, the formal series that are generated by a context-free grammar are algebraic.

We will actually be concerned with the situation in which f can be regarded as a power series which converges in some neighborhood of $x = 0$ in the complex plane. It is the case that if y is defined by $q(x, y) = 0$ where the polynomial q has its coefficients in an algebraic number field, then y is also defined by $p(x, y) = 0$ for some polynomial p with rational coefficients.

It should be pointed out that the coefficients of an algebraic series are indeed algebraic numbers, and that the coefficients satisfy a recurrence. The following is noted in [2], and see also [7]. If f is an algebraic series there exists a positive integer n_0 and polynomials $p_0, \ldots, p_d$ with coefficients in $\mathbb{Q}$ such that for all integers $n \geqslant n_0$,

$$p_0(n) \cdot [x^n]f + p_1(n) \cdot [x^{n-1}]f + \cdots + p_d(n) \cdot [x^{n-d}]f = 0.$$

The question of which algebraic series are Hadamard square roots of unity was raised in [5] and is connected to an investigation into language acceptance by automata with complex weights. See [6]. The question of algebraic Hadamard square roots of unity can also be seen as one topic at the intersection of analysis and formal language theory, e.g. [4]. It is also in line with the investigation into Hadamard rings which is considered in detail in [1].

2. On the problem of characterizing Hadamard square roots of unity

Our characterization result, Theorem 2 assumes the following form. If f is an algebraic Hadamard square root of unity, there exists a small algebraic series g such that $f = r + g$, where r is a rational series of a particularly simple kind. A series g is said to be *small* if there exists some $u < 0$ such that $|[x^n]g| = \mathrm{O}(n^u)$. Note that the case $g = 0$ is equivalent to letting $u = -\infty$. Details about the rational series r will be given in the next section. Our characterization is incomplete because as we sketch in the rest of this section, it appears to be difficult to pin down the nature of the small series g.

First we make two elementary observations that will be useful in this section.

Observation 1. Let ϕ, θ, η be real and $\rho > 0$. Assume that

$$|\exp(\sqrt{-1}(\cdot\,\phi + \theta)) + \rho \exp(\sqrt{-1} \cdot \eta)| = 1.$$

This means that

$$|1 + \rho \exp(\sqrt{-1} \cdot (\eta - \phi - \theta))| = 1,$$

from which we get

$$\rho = -2\cos(\eta - \phi - \theta). \tag{1}$$

Eq. (1) shows that the modulus ρ depends on $\eta - \phi - \theta$.

Observation 2. Let ω_n be a sequence of reals indexed by the nonnegative integers. The series f defined by $[x^n]f = \exp(2\sqrt{-1}\cdot\omega_n)$ is an algebraic series iff the series g given by $[x^n]g = -2\cos(\omega_n)\exp(\sqrt{-1}\cdot\omega_n)$ is algebraic. This follows at once from

$$1 + \exp(2\sqrt{-1}\cdot\omega_n) = 2\cos(\omega_n)\exp(\sqrt{-1}\cdot\omega_n).$$

We now look in detail at the coefficients of a small series g that can be involved in an Hadamard square root of unity f. In the simplest case, Theorem 2 dictates that $f = c/(1-\alpha)x + g$ where we can write $\alpha = \exp(\sqrt{-1}\cdot\theta)$, and $c = \exp(\sqrt{-1}\cdot\phi)$. We will let $[x^n]g = \rho_n\cdot\exp(\sqrt{-1}\cdot\omega_n)$, with $\rho_n \geqslant 0$. By Observation 1,

$$\rho_n = -2\cos(\omega_n - \phi - n\cdot\theta).$$

Since g is small we must also have either

$$\omega_n - \phi - n\theta = \pi/2 + \varepsilon_n$$

or

$$\omega_n - \phi - n\theta = 3\pi/2 - \varepsilon_n,$$

where $\varepsilon_n \geqslant 0$ and $\varepsilon_n = O(n^u)$ for $u < 0$.

In particular, it is clear from the previous paragraph that the series g where $\varepsilon_n = \pi/n$ is small, and satisfies $|[x^n f| = |c\cdot\alpha^n + [x^n]g| = 1$ for all n. However, we next show that g is not algebraic. Assuming that g is algebraic, we will derive a contradiction.

- $-g$ is algebraic.Note $[x^n](-g) = 2\cos(\pi/2 + 2\pi/n)\exp(\sqrt{-1}\cdot(\phi + n\theta + \pi/2 + \pi/n))$.
- $-g - 1/(1-x)$ is algebraic. Note $[x^n](-g - 1/(1-x)) = \exp(2\cdot\sqrt{-1}\cdot(\phi + n\theta + \pi/2 + \pi/n))$.
- Define h_1 by $[x^n]h_1 = 1/\alpha^{2n}$.
- It is evident that h given by

$$h = \frac{-1}{c^2}\cdot\left(h_1 \odot \left(-g - \frac{1}{1-x}\right)\right)$$

satisfies $[x^n]h = \mathbf{e}(1/n)$.

Since h_1 is a rational series, h is algebraic by the Jungen–Schützenberger Theorem. However, Theorem 1, given next, shows that h is not algebraic. Hence, our assumption that g is algebraic is false. This example shows that it may be difficult to construct a small algebraic series $g \neq 0$ that satisfies Theorem 2.

Note that $\mathbf{e}(1/n)$ is the 'canonical' primitive nth root of unity in $\mathbb{C}$. Let Ω be the generating series of these roots, i.e., $[x^n]\Omega = \mathbf{e}(1/n)$.

Theorem 1. *Ω is not algebraic.*

Proof. Let $a_n = [x^n]\Omega$. We assume that Ω is algebraic and derive a contradiction. Recall from the introduction that if Ω is algebraic, its coefficients satisfy a recurrence of the form

$$p_0(n)\cdot a_n + \cdots + p_d(n)\cdot a_{n-d} = 0, \tag{2}$$

where $p_0,\ldots,p_d$ are polynomials with rational coefficients. Let k be the highest degree of any of the polynomials $p_0,\ldots,p_d$. Let $b_1,\ldots,b_r$ be the nonzero coefficients of the polynomials $p_{i_1},\ldots,p_{i_r}$ having degree k. Here we take $i_1<\cdots<i_r$. With this notation we can rewrite Eq. (2) as

$$n^k\cdot(b_1\cdot a_{n-i_1}+\cdots+b_r\cdot a_{n-i_r})+\mathrm{O}(n^{k-1})=0. \tag{3}$$

Next, we concentrate on the expression

$$b_1\cdot a_{n-i_1}+\cdots+b_r\cdot a_{n-i_r}$$

in Eq. (3). Using

$$\frac{1}{n-j}=\frac{1}{n}\cdot(1+j/n+(j/n)^2+\cdots),$$

we can write the expression as

$$\mathbf{e}(1/n)\cdot(b_1\cdot\mathbf{e}(i_1/n^2)(1+\mathrm{O}(1/n^3))+\cdots+b_r\cdot\mathbf{e}(i_r/n^2)(1+\mathrm{O}(1/n^3))). \tag{4}$$

We have used the fact that $\mathbf{e}(i_j/n^3+i_j^2/n^4+\cdots)=1+\mathrm{O}(1/n^3)$. It is clear from Eq. (4) that

$$b_1\cdot a_{n-i_1}+\cdots+b_r\cdot a_{n-i_r}=\mathbf{e}(1/n)\cdot(b_1\cdot\mathbf{e}(i_1/n^2)+\cdots+b_r\cdot\mathbf{e}(i_r/n^2))+\mathrm{O}(1/n^3). \tag{5}$$

Now,

$$b_1\cdot\mathbf{e}(i_1/n^2)++\cdots+b_r\cdot\mathbf{e}(i_r/n^2)$$

can be regarded as the evaluation of the polynomial $q=b_r\cdot x^{i_r}+\cdots+b_1\cdot x^{i_1}$ at $x=\mathbf{e}(1/n^2)$. For $n^2>\phi(i_r)$ ($\phi(\cdot)$ is the Euler totient function) we have that this value cannot be zero. By the Liouville inequality, (see [8] for details) specialized to roots of unity, and Eq. (5)

$$|b_1\cdot a_{n-i_1}+\cdots+b_r\cdot a_{n-i_r}|\geqslant L^{-d}+\mathrm{O}(1/n^3),$$

where L is the LCM of the denominators of the rationals $b_1,\ldots,b_r$, all taken to lowest terms, and d is an upper bound on the degree of q. But, since L and d are independent of n, and dividing Eq. (3) by n^k we see that

$$b_1\cdot a_{n-i_1}+\cdots+b_r\cdot a_{n-i_r}+\mathrm{O}(1/n)$$

must be bounded away from 0 for all but finitely many n which contradicts Eq. (2). □

3. Principal result

Theorem 2. *If f is an algebraic Hadamard square root of unity, there exists a small algebraic series g such that f can be written in one of the following ways.*

(1) *$f=p+c/(1-\alpha x)+g$, where c and α are unit modulus algebraic numbers and p is a polynomial. These series are called type* 1.

(2) $f = p + \sum_{i=1}^{m} c_i/(1-\alpha_i x) + g$, *where* p *is a polynomial,* $m > 1$, $c_1, \ldots, c_m$ *are unit modulus algebraic numbers,* $\alpha_1, \ldots, \alpha_m$ *are all roots of unity and for all* n,

$$|c_1\alpha_1^n + \cdots + c_m\alpha_m^n| = 1. \tag{6}$$

These series are called type 2.

Note that type 2 series can occur. The series expansion f of

$$\frac{1+\sqrt{-1}\cdot x}{1-x^2}$$

is an example of a type 2 series. Note that

$$[x^n]f = \frac{1}{\sqrt{2}} \cdot ((1+\sqrt{-1})\cdot 1^n + (1-\sqrt{-1}\cdot(-1)^n).$$

In this case $m=2$, $c_1=(1+\sqrt{-1})/\sqrt{2}$, $c_2=(1-\sqrt{-1})/\sqrt{2}$, $\alpha_1=1$ and $\alpha_2=-1$.

The proof of Theorem 2 depends on three facts. The first is taken from Flajolet [3].

Theorem 3. *If* f *is an algebraic series, then asymptotically*

$$[x^n]f = \frac{\beta^n \cdot n^s}{\Gamma(s+1)} \cdot \left(\sum_{i=1}^{m} c_i \cdot \alpha_i^n + \mathrm{O}(n^u) \right). \tag{7}$$

- $\beta > 0$ *is algebraic.*
- $s \in \mathbb{Q} - \{-1, -2, \ldots\}$.
- $u < 0$.
- $c_1, \ldots, c_m$ *are algebraic.*
- $\alpha_1, \ldots, \alpha_m$ *are algebraic and have unit modulus.*

The second fact is an elementary technical result.

Lemma 4. *If* $A(x)$ *is a nonmonomial polynomial,* $|A(x)|$ *cannot be constant over* $|x| = 1$.

Proof. If $A(0)=0$, we can write $A(x)=x^d \cdot B(x)$ such that d is a positive integer, $B(x)$ is a polynomial and $B(0) \neq 0$. Since $|A(x)| = |x^d| \cdot |B(x)|$ and we require that $|x|=1$, we can assume that $A(0) \neq 0$.

Since $A(x)$ is a nonmonomial and $A(0) \neq 0$, we can write $A(x) = a_0 \cdot x^k + \cdots + a_k$, where $a_k \cdot a_0 \neq 0$, and $k > 0$. Note that since $|x|=1$, $\bar{x} = 1/x$. This implies

$$|A(x)|^2 = (a_0 \cdot x^k + \cdots + a_k) \cdot (\bar{a}_0 \cdot x^{-k} + \cdots + \bar{a}_k).$$

We can rewrite this as

$$|A(x)|^2 = x^{-k} \cdot (a_0 \cdot x^k + \cdots + a_k) \cdot (\bar{a}_0 + \cdots + \bar{a}_k \cdot x^k).$$

Expanding this we get

$$|A(x)|^2 = x^{-k} \cdot (a_0 \cdot \bar{a}_k \cdot x^{2k} + \cdots + a_k \cdot \bar{a}_0).$$

Now, if $|A(x)| = C$, for $|x| = 1$ where C is a constant, then

$$a_0 \cdot \bar{a}_k \cdot x^{2k} + \cdots + a_k \cdot \bar{a}_0 = C^2 \cdot x^k.$$

Since both $a_0\bar{a}_k$ and $\bar{a}_0 \cdot a_k$ are both nonzero, and $k > 0$, this is clearly impossible since we have a manifestly nonconstant analytic function that is supposed to be constant on the unit circle. □

The third fact is the key technical result used in the proof of Theorem 2.

Lemma 5. *Let $F(n) = \sum_{i=1}^{m} c_i \cdot \alpha_i^n$, where n is a positive integer, $c_1, \ldots, c_m$ are nonzero and $\alpha_1, \ldots, \alpha_m$ have unit modulus. We also assume that $m > 1$. Unless each α_i is a root of unity, $|F(n)|$ has at least two distinct accumulation points as $n \to \infty$.*

Proof. Let $\alpha_i = \mathbf{e}(\theta_i)$, where θ_i is real. Assume that at least one α_i is not a root of unity. Order $\theta_1, \ldots, \theta_m$ so that $\{\theta_1, \ldots, \theta_s\}$ is a maximal subset which is linearly independent over $\mathbb{Q}$. Note that $s \geqslant 1$ since some θ_i must be irrational. If $s < m$, then for $s + 1 \leqslant i \leqslant m$,

$$\theta_i = b_{i,0} + \sum_{k=1}^{s} b_{i,k}\theta_k, \tag{8}$$

such that $b_{i,0}, \ldots, b_{i,k} \in \mathbb{Q}$.

If $s = m$, the following argument becomes slightly simpler, since we can dispense with Eq. (8), and we leave it to the reader.

We indicate the fractional part of real ρ by $\rho \bmod 1$. Let d be a positive integer such that $d \cdot b_{i,k}$ is an integer for $s + 1 \leqslant i \leqslant m$ and $0 \leqslant k \leqslant s$. Let $\theta \in [0, 1]$. We claim that for any $\varepsilon > 0$ there exists n such that for $1 \leqslant k \leqslant s$,

$$|(d \cdot n \cdot \theta_k - d \cdot k \cdot \theta) \bmod 1| < \varepsilon. \tag{9}$$

Eq. (9) follows directly from the Weyl–von Neumann Theorem which asserts that for any $(a_1, \ldots, a_s) \in [0, 1]^s$, and any $\delta > 0$, there exists n such that for $1 \leqslant k \leqslant s$,

$$|n \cdot \theta_k \bmod 1 - a_k| < \delta.$$

We obtain Eq. (9) by choosing $a_k = k \cdot \theta \bmod 1$, letting $\delta = \varepsilon/d$ and appealing to repeated application of the triangle inequality.

Using Eq. (8), $F(n)$ can be written as

$$F(n) = \sum_{j=1}^{s} c_j \cdot \mathbf{e}(n\theta_j) + \sum_{i=s+1}^{m} c_i \cdot \mathbf{e}\left(n \cdot \left(b_{i,0} + \sum_{k=1}^{s} b_{i,k}\theta_k\right)\right). \tag{10}$$

Define $A_{dn}(z)$ by

$$A_{dn}(z) = \sum_{j=1}^{s} c_j \cdot z^{dj} + \sum_{i=s+1}^{m} c_i \cdot z^{\sum_{k=1}^{s} db_{i,k} \cdot k}.$$

Now, letting $z = \mathbf{e}(\theta)$, appealing to Eq. (9) and comparing $A_{dn}(z)$ with the expression in Eq. (10), we claim that for any $\delta > 0$ there exist infinitely many n such that

$$|A_{dn}(z) - F(dn)| < \delta. \tag{11}$$

To see this, first note that since $d \cdot b_{k,0}$ is an integer in Eq. (10), $\mathbf{e}(d \cdot n \cdot b_{k,0}) = 1$ and the corresponding factors disappear in going over to $A_{dn}(z)$. Next, for n satisfying Eq. (9), we have for $1 \leqslant j \leqslant s$,

$$z^{dj} = \alpha_j^{dn} \cdot \exp(\mathrm{O}(\varepsilon)),$$

and for $s+1 \leqslant i \leqslant m$,

$$z^{\sum_{k=1}^{s} d b_{i,k} \cdot k} = \alpha_k^{dn} \cdot \exp(\mathrm{O}(\varepsilon)).$$

The δ in Eq. (11) represents the sum of the errors of the form $\beta \cdot (1 - \exp(\mathrm{O}(\varepsilon)))$, $|\beta| = 1$, for each of the m terms in $A_{dn}(z)$.

Now, $A_{dn}(z)$ is a Laurent polynomial (some of the exponents may be negative integers), so we can define $B_{dn}(z)$ by

$$A_{dn}(z) = z^h \cdot B_{dn}(z)$$

where h is an integer and $B_{dn}(z)$ is a polynomial. Note that $|A_{dn}(z)| = |z^h| \cdot |B_{dn}(z)| = |B_{dn}(z)|$. Note that $m > 1$ means that $B_{dn}(z)$ is a nonmonomial polynomial, so by Lemma 4, $|B_{dn}(z)|$ cannot be constant. That is there must be two distinct values of z, say z_0 and z_1 with arguments θ and θ' such that $|B_{dn}(z_0)| \neq |B_{dn}(z_1)|$. This implies that there are two infinite sets N and N' of positive integers such that $\lim_{n\to\infty} |F(n)| = |B_{dn}(z_0)|$ for $n \in N$ and $\lim_{n\to\infty} |F(n)| = |B_{dn}(z_1)|$ for $n \in N'$. □

We proceed to prove Theorem 2.

Proof. We refer to the parameters appearing in Theorem 3. If $m = 1$, then

$$[x^n]f = \frac{\beta^n \cdot n^s}{\Gamma(s+1)} \cdot (c \cdot \alpha^n + \mathrm{O}(n^u)).$$

It is clear that $|c \cdot \alpha^n + \mathrm{O}(n^u)| = \Omega(1)$, so that if $\beta < 1$, $\lim_{n\to\infty} |[x^n]f| = 0$ and if $\beta > 1$, $\lim_{n\to\infty} |[x^n]f| = \infty$. Thus, $\beta = 1$. It is clear from this that $s = 0$. We can conclude that for n sufficiently large,

$$[x^n]f = c \cdot \alpha^n + \mathrm{O}(n^u).$$

This means there exists n_0 such that $n > n_0$ implies

$$[x^n]f = [x^n]\frac{c}{1 - \alpha x} + [x^n]g,$$

where g is small. Thus, there is a polynomial of degree at most n_0 such that $f = p + 1/(1 - \alpha x) + g$, and clearly g is algebraic. This implies that f is a type 1 series.

We assume that $m > 1$. We have, using notation from the proof of Lemma 5,

$$[x^n]f = \frac{\beta^n \cdot n^s}{\Gamma(s+1)} \cdot (F(n) + \mathrm{O}(n^u)).$$

First we show that each α_i must be a root of unity. Assume that at least one α_i is not a root of unity. By Lemma 5, there are at least two accumulation points of $|F(n)|$. It is easy to check that if one of them is zero, the only possibility is $\beta = 1, s = 0, u = -\infty$. If both accumulation points are nonzero, it is still clear that $\beta = 1$ and $s = 0$ by the argument of the previous paragraph. However, it is impossible that $|[x^n]f|$ is a constant for all n. We conclude that each α_i must be a root of unity.

Since the α_i are all roots of unity, if $|F(n)| \neq 1$ (violating Eq. (6)) for some n, it will assume that value infinitely often (in fact, ultimately periodically), which contradicts $|[x^n]f| = 1$ for all n. Now the same reasoning used for type 1 shows that these facts imply f is a type 2 series. □

We point out that Theorem 2 holds for some transcendental series f, by dropping the requirement that g be algebraic. It suffices that $[x^n]f$ have the asymptotic form of Theorem 3. For example, f with $[x^n]f = ((2n)!/(n!)^2)^2$ is transcendental but satisfies the required asymptotic form. See [3].

Concluding Remark. It is evident that Theorem 2 is not entirely satisfactory. We have been unable to produce an algebraic Hadamard square root of unity in which there is a nonzero small series g. If in fact g is always zero, there is likely a more algebraic, less 'microscopic' proof. However, even should that be the case, arguments like Lemma 5 are likely to be useful for looking at the characterization of algebraic series having infinitely many unit modulus coefficients with the rest being zero.

References

[1] B. Benzaghou, Algèbres de Hadamard, Bull. Soc. Math. France 98 (1970) 209–252.
[2] L. Comtet, Calcul pratique des coefficients de Taylor d'une fonction algébrique, Enseign. Math. 10 (1964) 267–270.
[3] P. Flajolet, Analytic models and ambiguity of contextfree languages, Theoret. Comput. Sci. 49 (2,3) (1987) 282–309.
[4] W. Kuich, A. Salomaa, Semirings, Automata, Languages, Springer, Berlin, 1986.
[5] C. Moore, personal communication, Santa Fe Institute, 1997.
[6] C. Moore, J. Crutchfield, Quantum automata and quantum grammars, Santa Fe Institute, 1997.
[7] B. Salvy, P. Zimmermann, Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable, ACM Trans. Math. Software 20 (2) (1994) 163–177.
[8] M. Waldschmidt, Linear independence of logarithms of algebraic numbers, Technical Report IMSc 116, Inst. of Math. Science, Madras, 1992.