

## ALGEBRAIC INDEPENDENCE PROPERTIES OF THE FREDHOLM SERIES

J. H. LOXTON and A. J. VAN DER POORTEN

Dedicated to Kurt Mahler on his 75th birthday

(Received 8 January 1978)

Communicated by J. H. Coates

### Abstract

We consider algebraic independence properties of series such as

$$f_r(z) = \sum_{k=0}^{\infty} z^{r^k} \quad (r = 2, 3, 4, \dots).$$

We show that the functions  $f_r(z)$  are algebraically independent over the rational functions. Further, if  $\alpha_{rs}$  ( $r = 2, 3, 4, \dots$ ;  $s = 1, 2, 3, \dots$ ) are algebraic numbers with  $0 < |\alpha_{rs}| < 1$ , we obtain an explicit necessary and sufficient condition for the algebraic independence of the numbers  $f_r(\alpha_{rs})$  over the rationals.

*Subject classification (Amer. Math. Soc. (MOS) 1970):* 10 F 35.

### 1. Introduction

One of the goals of transcendence theory is to relate the arithmetic behaviour of functions at appropriate values to the algebraic nature of the functions themselves. For example, theorems of Hadamard and Fabry show that quite weak growth conditions on the gaps between the terms of a power series force it to have a natural boundary on its circle of convergence. (See, for example, Dienes (1957), Ch. 11.) Such a series must represent a transcendental function. It is therefore natural to expect that if such a gap series has algebraic coefficients, it will take transcendental values at algebraic points in its domain of convergence. In practice, this general question appears difficult, though arithmetic results can be obtained when the gaps grow very rapidly (Mahler (1965), Cijssouw and Tijdeman (1973))

and also when they exhibit certain kinds of regularity (Loxton and van der Poorten (1977b)).

One of the earliest and simplest examples of a power series which cannot be continued beyond its circle of convergence is the series

$$f(z) = \sum_{h=0}^{\infty} z^{2^h}.$$

This example certainly dates from the time of Weierstrass, but we follow Schneider (1957) in calling  $f(z)$  the Fredholm series. It is easy to see that the series diverges at all the points  $\exp(2\pi ih/2^k)$  and so it has the circle  $|z| = 1$  as a natural boundary. The Fredholm series is characteristic of those series with “regular” gaps. Schneider (1957), p. 35, uses his refinement of Roth’s theorem to show that  $f(z)$  is transcendental at a rational point  $p/q$ , subject to the condition  $0 < |p| < q^{\frac{1}{2}}$ . However, much earlier, Mahler (1929) had shown that  $f(z)$  is transcendental at every algebraic point  $\alpha$  with  $0 < |\alpha| < 1$ , by exploiting the functional equation

$$f(z) = f(z^2) + z.$$

Mahler’s method is very general. It can be used to determine the transcendence at algebraic points of functions of several complex variables satisfying functional equations of the shape

$$(1) \quad g(Tz) = R(g(z), z),$$

where  $z = (z_1, \dots, z_n)$  is in  $\mathbb{C}^n$ ,  $T = (t_{ij})$  is an  $n \times n$  non-negative integer matrix defining a transformation on  $\mathbb{C}^n$  by

$$(Tz)_i = \prod_{j=1}^n z_j^{t_{ij}} \quad (1 \leq i \leq n),$$

and  $R$  is a rational function of its arguments. Of course, a number of more or less technical conditions must be imposed. (See our survey, Loxton and van der Poorten (1977c).)

Mahler (1930a, b) extended the method to obtain results on the independence of the values of such functions. Applied to the Fredholm series, the work yields the following conclusions. First, if  $\alpha_1, \dots, \alpha_n$  are multiplicatively independent algebraic numbers with  $0 < |\alpha_i| < 1$ , then the numbers  $1, f(\alpha_1), \dots, f(\alpha_n)$  are linearly independent over the algebraic numbers. Secondly, consider the series

$$f^{(\lambda)}(z) = \left(z \frac{d}{dz}\right)^{\lambda} f(z) = \sum_{h=0}^{\infty} 2^{\lambda h} z^{2^h} \quad (\lambda = 0, 1, 2, \dots),$$

which satisfy the functional equations

$$f^{(\lambda)}(z) = 2^{\lambda} f^{(\lambda)}(z^2) + z.$$

These functions are algebraically independent over the rational functions and, if  $\alpha$  is an algebraic number with  $0 < |\alpha| < 1$ , then the numbers  $f^{(\lambda)}(\alpha)$  ( $\lambda = 0, 1, 2, \dots$ ) are algebraically independent over the rationals.

Recently, Kubota (1977a, b) and the authors have extended Mahler’s method in various ways, obtaining some very general results about the transcendence and algebraic independence of the values of functions satisfying functional equations of the shape (1). The aim of this note is to show how some of these general theorems can be used to give surprisingly precise results about the algebraic independence properties of Fredholm-like series.

### 2. Algebraic independence of the functions

Let  $g(z) = g(z; r, a)$  denote a function of the complex variable  $z$  which is regular in some neighbourhood of the origin and satisfies a functional equation of the shape

$$(2) \quad g(z) = ag(z^r) + b(z),$$

where  $r > 1$  is a positive integer,  $a$  is a non-zero complex number and  $b(z)$  is a polynomial. By iterating the functional equation (2), we see that

$$(3) \quad g(z) = a^k g(z^{r^k}) + \sum_{h=0}^{k-1} a^h b(z^{r^h}) \quad (k = 1, 2, 3, \dots),$$

so that the notation is slightly ambiguous, but this should cause no confusion. By letting  $k$  tend to infinity in (3), we obtain the formula

$$(4) \quad g(z) = g(0) + \sum_{h=0}^{\infty} a^h \{b(z^{r^h}) - b(0)\}, \quad (1 - a)g(0) = b(0).$$

We begin by considering the possible algebraic relations between functions of this type.

**THEOREM 1.** *Let  $\mathcal{G}(r, a)$  be a family of functions satisfying functional equations of the shape (2) with  $r$  and  $a$  fixed and let  $\mathcal{G}$  be the union of a number of the families  $\mathcal{G}(r, a)$ . We choose the notation, as we may, so that  $\log r / \log r'$  is irrational for any two distinct transformation ratios  $r$  and  $r'$  appearing in the functional equations and so that the pairs  $(r, a)$  are distinct.*

(i) *The functions of  $\mathcal{G}$  are algebraically independent over the rational functions if and only if the functions of each  $\mathcal{G}(r, a)$  are algebraically independent.*

(ii) *The functions  $g_1(z), \dots, g_q(z)$  in a fixed family  $\mathcal{G}(r, a)$  are algebraically dependent if and only if there are constants  $d_1, \dots, d_q$ , not all zero, such that the function*

$$\sum_{j=1}^q d_j g_j(z)$$

*is a polynomial.*

**PROOF.** To prove the first part, we use induction on the number of distinct values of the transformation ratio  $r$ . To illustrate the argument, suppose  $\mathcal{G}$  is the union of just two sets  $\mathcal{G}(r, a)$  and  $\mathcal{G}(r', a')$ , say, where  $\log r / \log r'$  is irrational. Given a non-trivial algebraic relation between the functions of  $\mathcal{G}$ , we repeatedly apply the transformation  $z \rightarrow z^r$  and use the functional equations for the  $g(z; r, a)$  to obtain a sequence of relations between the functions of  $\mathcal{G}(r, a)$  and an increasing collection of functions  $g(z; r', a')$ . By hypothesis, the functions of  $\mathcal{G}(r, a)$  are algebraically independent, so we can eliminate them and thereby obtain a non-trivial relation involving only functions with the transformation ratio  $r'$ . This reduction process enables us to confine the search for algebraic relations in  $\mathcal{G}$  to the sets  $\mathcal{G}(r, a)$  with  $r$  fixed.

Suppose now that all the  $\mathcal{G}(r, a)$  of the theorem have the same  $r$ . We can now apply Theorem 2 of Loxton and van der Poorten (to appear, a). If the functions in  $\mathcal{G}$  are algebraically dependent, then there are functions  $g_1(z), \dots, g_q(z)$  in one of the  $\mathcal{G}(r, a)$  and constants  $d_1, \dots, d_q$ , not all zero, such that the function

$$h(z) = \sum_{j=1}^q d_j g_j(z)$$

is a rational function. By replacing  $g_j(z)$  by  $g_j(z) - g_j(0)$ , we may suppose that  $g_j(0) = 0$  for each  $j$ . Then, from (4),

$$h(z) = \sum_{h=0}^{\infty} a^h \sum_{j=1}^q d_j b_j(z^{r^h}),$$

where the  $b_j(z)$  are polynomials. By the Hadamard gap theorem,  $h(z)$  is either a polynomial or a function with a natural boundary. The latter possibility is excluded since  $h(z)$  is rational, so we have the second assertion of the theorem. The first assertion follows easily from the second and the preceding remarks.

We now specialize the theorem to the case of Fredholm series. If  $r > 1$  and  $s \geq 1$  are positive integers, we define the Fredholm series

$$f_{r,s}(z) = f(z; r, s) = \sum_{h=0}^{\infty} z^{sr^h};$$

it satisfies the functional equation

$$f_{r,s}(z) = f_{r,s}(z^r) + z^s.$$

Further, for  $\lambda = 0, 1, 2, \dots$ , we define the functions

$$f_{r,s}^{(\lambda)}(z) = f^{(\lambda)}(z; r, s) = \left( z \frac{d}{dz} \right)^\lambda f_{r,s}(z) = \sum_{h=0}^{\infty} s^\lambda r^{\lambda h} z^{sr^h},$$

which satisfy the functional equations

$$f_{r,s}^{(\lambda)}(z) = r^\lambda f_{r,s}^{(\lambda)}(z^r) + s^\lambda z^s.$$

**THEOREM 2.** *The algebraic relations between the functions  $f_{r,s}^{(\lambda)}(z)$  over the rational functions are generated by the trivial relations*

$$f^{(\lambda)}(z; r, s) = f^{(\lambda)}(z; r, sr) + s^\lambda z^s,$$

$$f^{(\lambda)}(z; r, s) = \sum_{j=0}^{k-1} f^{(\lambda)}(z; r^k, sr^j).$$

**PROOF.** By employing the trivial relations to eliminate certain  $f_{r,s}^{(\lambda)}(z)$ , we may suppose that the family of functions  $f_{r,s}^{(\lambda)}(z)$  under consideration is so normalized that  $r \nmid s$  for each  $f_{r,s}^{(\lambda)}(z)$  and that  $\log r / \log r'$  is irrational for any pair  $f_{r,s}^{(\lambda)}(z), f_{r',s'}^{(\lambda)}(z)$  with  $r \neq r'$ . If this normalized set of functions is algebraically dependent, then Theorem 1 yields a non-trivial linear combination

$$h(z) = \sum_{j=1}^q d_j f^{(\lambda)}(z; r, s_j)$$

which is a polynomial. However, this is impossible when  $r \nmid s_j$ , since the exponents appearing in the  $q$  series for the  $f^{(\lambda)}(z; r, s_j)$  are all distinct. Consequently, a normalized set of Fredholm series must be algebraically independent and this proves the theorem.

Further specialization gives the following quotable results. We write here

$$f_r(z) = \sum_{h=0}^{\infty} z^{r^h} \quad (r = 2, 3, 4, \dots).$$

**COROLLARY 1.** *The functions  $f_r(z)$  ( $r = 2, 3, 4, \dots$ ) are algebraically independent over the rational functions.*

**COROLLARY 2.** *The functions  $f_r(z)$  ( $r = 2, 3, 4, \dots$ ) are ‘‘hypertranscendental’’, that is, they do not even satisfy any algebraic differential equation.*

### 3. Algebraic independence of the values of a single function

Throughout this section, we write

$$f(z) = \sum_{h=0}^{\infty} z^{r^h},$$

where  $r > 1$  is a positive integer. We seek the possible algebraic relations between the values of  $f(z)$  at distinct algebraic points in the unit disc.

We begin with some definitions. We call two numbers  $\alpha$  and  $\beta$  equivalent if  $\alpha^{r^h} = \beta^{r^k}$  for some integers  $h$  and  $k$ . We say the numbers  $\alpha_1, \dots, \alpha_s$  are  $r$ -dependent if each  $\alpha_i$  is equivalent to  $\gamma \xi_i$ , say, where  $\gamma$  is fixed and  $\xi_i$  is a root of unity, and there are numbers  $d_i$  not all zero such that

$$(5) \quad \sum_{i=1}^s d_i \xi_i^{r^h} = 0 \quad (h = 0, 1, 2, \dots).$$

**THEOREM 3.** *Let  $\alpha_1, \dots, \alpha_q$  be algebraic numbers with  $0 < |\alpha_i| < 1$ .*

(i) *The numbers  $f(\alpha_1), \dots, f(\alpha_q)$  are algebraically dependent over the rationals if and only if  $1, f(\alpha_1), \dots, f(\alpha_q)$  are linearly dependent over the algebraic numbers.*

(ii) *The numbers  $1, f(\alpha_1), \dots, f(\alpha_q)$  are linearly dependent if and only if some subset of  $\alpha_1, \dots, \alpha_q$  is  $r$ -dependent, and the relations obtained in this way generate all the algebraic relations between  $f(\alpha_1), \dots, f(\alpha_q)$ .*

We observe that trivially the relation (5) together with the functional equation for  $f(z)$ , implies that  $\sum d_i f(\alpha_i)$  is an algebraic number. The converse is much more difficult and necessitates some lemmas on functions of several complex variables.

**LEMMA 1.** *Let  $g_i(z_1, \dots, z_n)$  ( $1 \leq i \leq p$ ) be functions regular in some neighbourhood of the origin in  $\mathbb{C}^n$  and satisfying the respective functional equations*

$$g_i(z_1, \dots, z_n) = a_i g_i(z_1^r, \dots, z_n^r) + b_i(z_1, \dots, z_n),$$

where  $r > 1$  is an integer, the  $a_i$  are non-zero complex numbers and the  $b_i(z_1, \dots, z_n)$  are polynomials. Let  $S(i) = \{j : a_j = a_i\}$ . If the functions  $g_i(z_1, \dots, z_n)$  are algebraically dependent over the rational functions then there are an index  $i$  and constants  $d_j$  not all zero such that the function

$$\sum_{j \in S(i)} d_j g_j(z_1, \dots, z_n)$$

is a polynomial.

**PROOF.** This follows from Theorem 2 of Loxton and van der Poorten (to appear, a). (Compare the argument used for functions of one variable in the course of the proof of Theorem 1 above.)

**LEMMA 2.** *Suppose that the functions described in Lemma 1 are algebraically independent and, in addition, that the polynomials  $b_i(z_1, \dots, z_n)$  and the power series expansions of the  $g_i(z_1, \dots, z_n)$  about the origin all have algebraic coefficients. Let  $\alpha_1, \dots, \alpha_n$  be multiplicatively independent algebraic numbers with  $0 < |\alpha_j| < 1$  ( $1 \leq j \leq n$ ). Then the numbers  $g_i(\alpha_1, \dots, \alpha_n)$  are algebraically independent over the rationals.*

**PROOF.** This is a (slightly) special case of the main theorem of Loxton and van der Poorten (to appear, b).

LEMMA 3. Let  $\alpha_1, \dots, \alpha_q$  be algebraic numbers with  $0 < |\alpha_i| < 1$ . Then there are multiplicatively independent algebraic numbers  $\beta_1, \dots, \beta_n$  with  $0 < |\beta_j| < 1$  such that

$$(6) \quad \alpha_i = \xi^{\mu_i} \prod_{j=1}^n \beta_j^{\mu_{ij}} \quad (1 \leq i \leq q),$$

where  $\xi$  is a root of unity and the  $\mu_i$  and  $\mu_{ij}$  are non-negative integers.

PROOF. First, we can choose  $n$  multiplicatively independent numbers  $\gamma_j$  with  $0 < |\gamma_j| < 1$  such that

$$\alpha_i = \xi^{\nu_i} \prod_{j=1}^n \gamma_j^{\nu_{ij}} \quad (1 \leq i \leq q),$$

where  $\xi$  is a root of unity and the  $\nu_i$  and  $\nu_{ij}$  are integers. Let  $\eta$  be the  $n$ -tuple with components  $\eta_j = -\log |\gamma_j|$ . Next, choose  $n$  linearly independent  $n$ -tuples  $u_j = (u_{jk})$  with rational components such that each  $u_j$  is close to  $\eta$  in the sense described below and, in addition, each  $n$ -tuple  $v_j = (v_{jk})$  of the dual basis to the basis  $u_j$  has a positive projection on  $\eta$ . Determine numbers  $\beta_j$  by

$$\beta_j = \prod_{k=1}^n \gamma_k^{\nu_{jk}}, \quad \text{that is} \quad \gamma_j = \prod_{k=1}^n \beta_k^{u_{jk}} \quad (1 \leq j \leq n).$$

Then the  $\beta_j$  are multiplicatively independent algebraic numbers and the requirement on the dual basis  $v_j$  ensures that  $0 < |\beta_j| < 1$ . The equations (6) hold with the  $\mu_{ij}$  given by

$$\mu_{ij} = \sum_{k=1}^n \nu_{ik} u_{jk} \quad (1 \leq i \leq q, 1 \leq j \leq n).$$

The construction makes the  $\mu_{ij}$  rational and  $\mu_{ij}$  is close to

$$\sum_{k=1}^n \nu_{ik} \eta_k = - \sum_{k=1}^n \nu_{ik} \log |\gamma_k| = -\log |\alpha_i| > 0.$$

So we can achieve  $\mu_{ij} > 0$  by choosing each  $u_{jk}$  sufficiently close to  $\eta_k$ . Finally, by taking roots of the  $\beta_j$ , we can make the  $\mu_{ij}$  in (6) integers.

A lemma of this nature is used for a somewhat similar purpose by Ritt (1927).

PROOF OF THEOREM 3. Suppose that  $f(\alpha_1), \dots, f(\alpha_q)$  are algebraically dependent. By Lemma 3, we can find multiplicatively independent algebraic numbers  $\beta_1, \dots, \beta_n$  with  $0 < |\beta_j| < 1$ , so that the  $\alpha_i$  have the shape given in (6). By replacing the  $\alpha_i$  by  $\alpha_i^N$ , we may suppose that the root of unity,  $\xi$ , in (6) is a primitive  $N$ th root of unity with  $N$  and  $r$  relatively prime. We denote the order of  $r \pmod N$  by  $t$  and write  $r^t = s$ .

Now consider the functions

$$g_i(z_1, \dots, z_n) = f\left(\xi^{\mu_i} \prod_{j=1}^n z_j^{\mu_{ij}}\right) \quad (1 \leq i \leq q),$$

which satisfy the respective functional equations

$$g_i(z_1, \dots, z_n) = g_i(z_1^s, \dots, z_n^s) + \sum_{h=0}^{t-1} \left(\xi^{\mu_i} \prod_{j=1}^n z_j^{\mu_{ij}}\right)^r.$$

By Lemma 2, the numbers  $f(\alpha_i) = g_i(\beta_1, \dots, \beta_n)$  are algebraically dependent if and only if the functions  $g_i(z_1, \dots, z_n)$  are algebraically dependent. By Lemma 1, this is the case only if there are constants  $d_i$ , not all zero, such that

$$\sum_{i=1}^q d_i g_i(z_1, \dots, z_n) = \sum_{h=0}^{\infty} \sum_{i=1}^q d_i \left(\xi^{\mu_i} \prod_{j=1}^n z_j^{\mu_{ij}}\right)^{rh}$$

is a polynomial. The terms of high degree in the above expression must therefore all vanish. The assertions of the theorem now follow without difficulty.

By the same method, but with some additional complications of notation, we can extend Theorem 3 to more general functional equations. Suppose  $g(z)$  is regular in some neighbourhood of the origin and satisfies the functional equation

$$(7) \quad g(z) = ag(z^r) + b(z),$$

where  $r > 1$  is a positive integer,  $a$  is a non-zero complex number and  $b(z)$  is a polynomial. By replacing  $g(z)$  by  $g(z) - g(0)$  and rearranging the series representation (4) for  $g(z)$ , we can replace the functional equation (7) by a normalized functional equation for  $g(z)$  of the same shape in which  $b(0) = 0$  and  $b(z)$  has degree less than  $r$ .

**THEOREM 3 BIS.** *Let  $g_1(z), \dots, g_p(z)$  be algebraically independent functions satisfying the respective normalized functional equations*

$$(8) \quad g_i(z) = a_i g_i(z^r) + b_i(z) \quad (1 \leq i \leq p),$$

where  $r > 1$  is a positive integer, the  $a_i$  are non-zero algebraic numbers, the  $b_i(z)$  are polynomials with algebraic coefficients and, in addition, the power series expansions of the  $g_i(z)$  about the origin have algebraic coefficients. Let  $\alpha_{ij}$  ( $1 \leq i \leq p, 1 \leq j \leq q_i$ ) be algebraic numbers with  $0 < |\alpha_{ij}| < 1$ .

(i) *Split the functions  $g_i(z)$  into groups corresponding to the distinct values of the multiplier  $a_i$  in (8). The numbers  $g_i(\alpha_{ij})$  are algebraically independent if and only if the numbers  $g_i(\alpha_{ij})$  corresponding to each group of the functions  $g_i(z)$  are algebraically independent.*



(ii) Now suppose that the  $a_i$  in (8) are all equal. The numbers  $g_i(\alpha_{ij})$  are algebraically dependent if and only if some subset of the  $\alpha_{ij}$  has the following properties:  $\alpha_{ij}$  is equivalent to  $\gamma_{ij} = \gamma \xi_{ij}$  where  $\xi_{ij}$  is a root of unity and there are constants  $d_{ij}$  not all zero so that

$$\sum_{i,j} d_{ij} b_i(\gamma_{ij}^{r^h}) = 0 \quad (h = 0, 1, 2, \dots).$$

**4. Algebraic independence of the values of functions with different ratios**

In this and the following section, we state and prove the main result of this note. As before, we write

$$f_r(z) = \sum_{h=0}^{\infty} z^{r^h} \quad (r = 2, 3, 4, \dots).$$

The results here complement Theorem 3 and provide complete arithmetic information on the values of Fredholm series at algebraic points.

**THEOREM 4.** *Let  $r_i > 1$  be positive integers such that  $\log r_i / \log r_j$  is irrational for  $i \neq j$ . Let  $\alpha_{ij}$  be algebraic numbers with  $0 < |\alpha_{ij}| < 1$ . Then the numbers  $f_{r_i}(\alpha_{ij})$  ( $i, j = 1, 2, 3, \dots$ ) are algebraically independent over the rationals if and only if, for each fixed  $i$ , the numbers  $f_{r_i}(\alpha_{ij})$  ( $j = 1, 2, 3, \dots$ ) are algebraically independent over the rationals.*

As already remarked in Section 2, the condition that  $\log r_i / \log r_j$  is irrational for  $i \neq j$  represents no real loss of generality, and some such condition is necessary to avoid trivial relations between the functions  $f_r(z)$ . Kubota (1976, 1977b) has stated results of this type under more restrictive conditions. For example, his methods give Theorem 4 when, for each  $i$ , the numbers  $|\alpha_{ij}|$  ( $j = 1, 2, 3, \dots$ ) are multiplicatively independent.

The proof of Theorem 4 follows exactly the proof of Theorem 3, except that Lemma 2 must be replaced by the following proposition.

**THEOREM 5.** *Let  $r_i$  ( $1 \leq i \leq p$ ) be positive integers such that  $r_i > 1$  and  $\log r_i / \log r_j$  is irrational for  $i \neq j$ . Let  $g_{ij}(z_1, \dots, z_{n_i})$  ( $1 \leq i \leq p, 1 \leq j \leq q_i$ ) be functions having power series expansions with algebraic coefficients at the origin and satisfying the respective functional equations*

$$(9) \quad g_{ij}(z_1, \dots, z_{n_i}) = g_{ij}(z_1^{r_i}, \dots, z_{n_i}^{r_i}) + b_{ij}(z_1, \dots, z_{n_i}),$$

*the  $b_{ij}$  being polynomials with algebraic coefficients, and suppose that, for each fixed  $i$ , the  $g_{ij}$  ( $1 \leq j \leq q_i$ ) are algebraically independent over the rational functions. Let  $\alpha_{ij}$  ( $1 \leq i \leq p, 1 \leq j \leq n_i$ ) be algebraic numbers such that  $0 < |\alpha_{ij}| < 1$  and, for each fixed  $i$ , the numbers  $\alpha_{ij}$  ( $1 \leq j \leq n_i$ ) are multiplicatively independent. Then the*

numbers  $g_{ij}(\alpha_{i1}, \dots, \alpha_{in_i})$  ( $1 \leq i \leq p, 1 \leq j \leq q_i$ ) are algebraically independent over the rationals.

To prove Theorem 5, we use a modification of the method of Loxton and van der Poorten (to appear, b). At the cost of some additional notational complexity, even more general results can be obtained. For example, we can replace the functional equations (9) by the equations

$$g_{ij}(z_1, \dots, z_{n_i}) = a_{ij}g_{ij}(z_1^{r_i}, \dots, z_{n_i}^{r_i}) + b_{ij}(z_1, \dots, z_{n_i}),$$

the  $a_{ij}$  being non-zero algebraic numbers. This, in turn, gives the following strengthening of Theorem 4.

**THEOREM 4 BIS.** *Let  $\mathcal{G}(r)$  be a family of functions having power series expansions with algebraic coefficients at the origin and satisfying functional equations of the shape*

$$g(z) = ag(z^r) + b(z),$$

where  $r > 1$  is a fixed integer,  $a$  is a non-zero algebraic number and  $b(z)$  is a polynomial with algebraic coefficients. Let  $\mathcal{G}$  be the union of a number of the families  $\mathcal{G}(r)$ . (We choose the notation, as we may, so that  $\log r / \log r'$  is irrational if  $\mathcal{G}(r) \neq \mathcal{G}(r')$ .) For each function  $g$  in  $\mathcal{G}$ , let  $\alpha_i^{(g)}$  ( $i = 1, 2, 3, \dots$ ) be algebraic numbers with  $0 < |\alpha_i^{(g)}| < 1$ . Then the numbers  $g(\alpha_i^{(g)})$  ( $g$  in  $\mathcal{G}; i = 1, 2, 3, \dots$ ) are algebraically independent over the rationals if and only if, for each fixed  $r$ , the numbers  $g(\alpha_i^{(g)})$  ( $g$  in  $\mathcal{G}(r); i = 1, 2, 3, \dots$ ) are algebraically independent.

### 5. Proof of Theorem 5

We begin by developing a more compact notation. For  $1 \leq i \leq p$ , let

$$z_i = (z_{i1}, \dots, z_{in_i})$$

denote a point of  $C^{n_i}$  and set  $z = (z_1, \dots, z_p)$ , giving a point of  $C^n$  with  $n = n_1 + \dots + n_p$ . In the same way, we write  $\alpha_i = (\alpha_{i1}, \dots, \alpha_{in_i})$ ,  $\alpha = (\alpha_1, \dots, \alpha_p)$  and  $g_i(z_i) = (g_{i1}(z_i), \dots, g_{iq_i}(z_i))$ . Next, set  $T_i = r_i I_{n_i}$ , where  $I_s$  denotes the  $s \times s$  identity matrix. The matrix  $T_i$  defines a transformation on  $C^{n_i}$  by  $z_{ij} \rightarrow z_{ij}^{r_i}$  ( $1 \leq j \leq n_i$ ). We write  $T = \text{diag}(T_1, \dots, T_p)$ , using block diagonal notation;  $T$  defines a transformation on  $C^n$  in an analogous way. If  $k = (k_1, \dots, k_p)$  is a  $p$ -tuple of non-negative integers, we write  $T^k = \text{diag}(T_1^{k_1}, \dots, T_p^{k_p})$ .

Now suppose that the numbers  $g_{ij}(\alpha_i)$  ( $1 \leq i \leq p, 1 \leq j \leq q_i$ ) are algebraically dependent. Thus there is a relation

$$G(\alpha; \omega) = \sum_{\mu} \omega_{\mu} g_1(\alpha_1)^{\mu_1} \dots g_p(\alpha_p)^{\mu_p} = 0,$$

where the components  $\omega_\mu$  of  $\omega$  are rational numbers, not all zero, indexed by  $\mu = (\mu_{ij})$ . (As before, we write  $\mu_i = (\mu_{i1}, \dots, \mu_{iq_i})$ , and  $\mathbf{g}_i(\alpha_i)^{\mu_i}$  in the usual multi-index notation means  $g_{i1}^{\mu_{i1}} \dots g_{iq_i}^{\mu_{iq_i}}$ .) The components  $\mu_{ij}$  of  $\mu$  are non-negative integers with  $0 \leq \mu_{ij} \leq m_{ij}$ , say, and we denote the total number of them by  $m$ . We introduce  $m$  new variables  $\mathbf{w} = (w_\mu)$ , indexed in the same way as  $\omega$ , and we define a linear transformation  $\Omega(\mathbf{u})$  of the variables  $\mathbf{w} = (w_\mu)$  by

$$(\Omega(\mathbf{u}) \mathbf{w})_\mu = \sum_{\nu} \left\{ \prod_{i=1}^p \prod_{j=1}^{q_i} \binom{\nu_{ij}}{\mu_{ij}} w_{\nu_{ij}}^{\nu_{ij} - \mu_{ij}} \right\} w_\nu,$$

where the sum is over all  $\nu = (\nu_{ij})$  with  $0 \leq \nu_{ij} \leq m_{ij}$  and

$$\mathbf{u} = (u_{ij} : 1 \leq i \leq p, 1 \leq j \leq q_i).$$

By iterating the functional equations (9), we obtain the further equations

$$g_{ij}(z_i) = g_{ij}(T_i^{k_i} z_i) + b_{ij}^{(k_i)}(z_i), \quad b_{ij}^{(k_i)}(z_i) = \sum_{h=0}^{k_i-1} b_{ij}(z_i^{r_i^h}).$$

We write

$$\omega^{(k)} = \Omega((b_{ij}^{(k_i)}(\alpha_i))) \omega, \quad \mathbf{k} = (k_1, \dots, k_p).$$

An easy calculation shows that the function

$$G(\mathbf{z}; \mathbf{w}) = \sum_{\mu} w_\mu \mathbf{g}_1(z_1)^{\mu_1} \dots \mathbf{g}_p(z_p)^{\mu_p}$$

is invariant under the transformation  $\mathbf{z}_i \rightarrow T_i^{k_i} z_i, \mathbf{w} \rightarrow \Omega((b_{ij}^{(k_i)}(z_i))) \mathbf{w}$ . In particular,

$$(10) \quad G(T^{\mathbf{k}} \alpha; \omega^{(k)}) = 0$$

for every non-zero  $p$ -tuple  $\mathbf{k} = (k_1, \dots, k_p)$  of non-negative integers.

Let  $K$  be the algebraic number field generated over the rationals by the  $\alpha_{ij}$ . Denote by  $\mathcal{P}$  the ring of polynomials in  $\mathbf{w} = (w_\mu)$  with coefficients in  $K$  and by  $\mathcal{P}(\omega)$  the subset of  $\mathcal{P}$  comprising those polynomials  $p(\mathbf{w})$  such that  $p(\Omega(\mathbf{u}) \omega)$  is identically zero in  $\mathbf{u} = (u_{ij})$ . Further, denote by  $\mathcal{A}$  the ring of power series  $E(\mathbf{z}; \mathbf{w}) = \sum p_\lambda(\mathbf{w}) z^\lambda$  in  $\mathbf{z}$  with coefficients  $p_\lambda(\mathbf{w})$  in  $\mathcal{P}$  and converging in some neighbourhood of the origin. We define the index of  $E(\mathbf{z}; \mathbf{w})$  at  $\omega$  to be the least non-negative integer  $h$  for which there is a coefficient  $p_\lambda(\mathbf{w})$  of  $E(\mathbf{z}; \mathbf{w})$  with  $|\lambda| = \sum |\lambda_{ij}| = h$  and such that  $p_\lambda(\mathbf{w})$  is not in  $\mathcal{P}(\omega)$ .

The first step in the proof proper is the construction of the auxiliary function, as follows.

**LEMMA 4.** *For every sufficiently large integer  $\rho$ , there are polynomials  $p_0(\mathbf{z}; \mathbf{w}), \dots, p_\rho(\mathbf{z}; \mathbf{w})$  of degree at most  $\rho$  in each of the variables  $z_{ij}$  and  $w_\mu$  with*

coefficients in  $K$  and with  $p_0(\mathbf{z}; \mathbf{w})$  having finite index at  $\omega$ , such that the function

$$(11) \quad E_\rho(\mathbf{z}; \mathbf{w}) = \sum_{j=0}^{\rho} p_j(\mathbf{z}; \mathbf{w}) G(\mathbf{z}; \mathbf{w})^j = \sum_{\lambda} B_{\lambda}(\mathbf{w}) \mathbf{z}^{\lambda}$$

is not identically zero, but its index at  $\omega$  is at least  $2^{-2-m/n} \rho^{1+1/n}$ .

PROOF. For this, see Lemma 6 of Loxton and van der Poorten (to appear, b). The construction depends on balancing the number of free coefficients in the  $p_j(\mathbf{z}; \mathbf{w})$  and the number of conditions imposed on  $E_\rho(\mathbf{z}; \mathbf{w})$ .

The next stage in the proof is a uniqueness theorem (Lemma 6). In what follows,  $r > 1$  is a fixed integer and, for each integer  $s$ , we define the  $p$ -tuple of integers

$$(12) \quad \mathbf{k}(s) = (k_1, \dots, k_p), \quad k_i = [s \log r / \log r_i].$$

LEMMA 5. Let  $\theta = (\theta_{ij})$  be an algebraic point of  $C^n$  with

$$|\theta_{ij}| = 1 \quad (1 \leq i \leq p, 1 \leq j \leq n_i).$$

Suppose that for some  $\varepsilon > 0$  and some infinite sequence of positive integers  $\mathcal{S}$  there is a polynomial  $p(\mathbf{z})$  with coefficients in  $K$  and not identically zero such that

$$(13) \quad p(T^{\mathbf{k}(s)} \theta) = O(\exp(-\varepsilon^s))$$

as  $s \rightarrow \infty$  along  $\mathcal{S}$ . Then, for some fixed  $i$ , the  $\theta_{ij}$  ( $1 \leq j \leq n_i$ ) are multiplicatively dependent.

PROOF. Let  $\mathcal{I}$  be the ideal of all such polynomials  $p(\mathbf{z})$  satisfying (13). We note that if  $p(\mathbf{z})$  is in  $\mathcal{I}$ , then so is  $p(T^{\mathbf{k}(s)} \mathbf{z})$  for each  $s$  in  $\mathcal{S}$ . We can therefore carry through the proof of Lemma 14 of Loxton and van der Poorten (1977a), which shows that there is an  $n$ -tuple  $\lambda = (\lambda_1, \dots, \lambda_p)$  such that  $(T^{\mathbf{k}(s)} \theta)^\lambda = 1$  for infinitely many  $s$ . If we write  $\varphi_i = \theta_i^{\lambda_i}$ , this gives

$$\varphi_1^{r_1^{k_1}} \dots \varphi_p^{r_p^{k_p}} = 1,$$

where  $\mathbf{k}(s) = (k_1, \dots, k_p)$ , for infinitely many  $s$ . But  $\log r_i / \log r_j$  is irrational for  $i \neq j$ , so these equations imply that each  $\varphi_i$  is a root of unity. This proves the lemma.

LEMMA 6. Let  $\alpha = (\alpha_{ij})$  be an algebraic point of  $C^n$  with

$$0 < |\alpha_{ij}| < 1 \quad (1 \leq i \leq p, 1 \leq j \leq q_i)$$

and suppose that, for each fixed  $i$ , the  $\alpha_{ij}$  ( $1 \leq j \leq q_i$ ) are multiplicatively independent. Let  $g(\mathbf{z})$  be a power series in  $\mathbf{z} = (z_{ij})$  with coefficients in  $K$  which is convergent in some neighbourhood of the origin and not identically zero. Then there are infinitely many positive integers  $s$  such that  $g(T^{\mathbf{k}(s)} \alpha) \neq 0$ , with  $\mathbf{k}(s)$  given by (12).

PROOF. Let  $g(\mathbf{z}) = \sum a_\lambda \mathbf{z}^\lambda$ . Choose an infinite sequence  $\mathcal{S}$  of positive integers such that the fractional part of  $s \log r / \log r_i$  tends to a limit  $s_i$ , say, as  $s \rightarrow \infty$  along  $\mathcal{S}$ . As  $s \rightarrow \infty$  along  $\mathcal{S}$ ,

$$\log |a_\lambda (T^{k(s)} \alpha)^\lambda| \sim r^s \sum_{i,j} r_i^{s_i} \lambda_{ij} \log |\alpha_{ij}| = -r^s t_\lambda,$$

say, with  $t_\lambda > 0$ . Now write

$$g(\mathbf{z}) = \sum_R g_R(\mathbf{z}), \quad g_R(\mathbf{z}) = \sum_{\iota_\lambda=R} a_\lambda \mathbf{z}^\lambda,$$

the notation being chosen so that none of the  $g_R(\mathbf{z})$  vanishes identically. Each  $g_R(\mathbf{z})$  is a polynomial and the index of summation  $R$  runs through a discrete set say  $0 \leq R_0 < R_1 < R_2 < \dots$ . Now

$$g_R(T^k \alpha) = \exp(-Rr^s) h_R(T^k \theta),$$

where  $\theta = (\theta_{ij})$  is an algebraic point of  $\mathbb{C}^n$  with  $|\theta_{ij}| = 1$  and  $h_R(\mathbf{z})$  is a polynomial. By Lemma 5,  $g_{R_0}(T^{k(s)} \alpha)$  dominates the series for  $g(T^{k(s)} \alpha)$  infinitely often as  $s \rightarrow \infty$  along  $\mathcal{S}$  and the lemma follows. (Compare Theorem 4 of Loxton and van der Poorten (1977a).)

PROOF OF THEOREM 5. The remainder of the proof is quite straightforward. First, using the fact that the  $B_\lambda(\mathbf{w})$  in (11) satisfy  $B_\lambda(\omega^{(k)}) = 0$  for  $|\lambda| \ll \rho^{1+1/n}$ , we see that if  $\rho$  is a sufficiently large integer and each  $k_i$  is sufficiently large compared to  $\rho$ , then

$$(14) \quad \log |E_\rho(T^k \alpha; \omega^{(k)})| \leq -c_1 \rho^{1+1/n} \min_{1 \leq i \leq p} r_i^{k_i},$$

where  $\mathbf{k} = (k_1, \dots, k_p)$  and  $c_1$  is a positive constant independent of  $\rho$  and  $\mathbf{k}$ . (See Lemma 7 of Loxton and van der Poorten (to appear, b).) Next, by (10) and (11),  $E_\rho(T^k \alpha; \omega^{(k)}) = p_0(T^k \alpha; \omega^{(k)})$ , so it is easy to compute the size of the algebraic number  $E_\rho(T^k \alpha; \omega^{(k)})$ . By applying the fundamental inequality, we see that if  $\rho$  and  $\mathbf{k}$  are chosen as before and  $E_\rho(T^k \alpha; \omega^{(k)}) \neq 0$ , then

$$(15) \quad \log |E_\rho(T^k \alpha; \omega^{(k)})| \geq -c_2 \rho \max_{1 \leq i \leq p} r_i^{k_i},$$

where  $\mathbf{k} = (k_1, \dots, k_p)$  and  $c_2$  is a positive constant independent of  $\rho$  and  $\mathbf{k}$ . (See Lemma 12 of Loxton and van der Poorten (to appear, b).) Now consider the numbers  $\Theta_s = E_\rho(T^{k(s)} \alpha; \omega^{(k(s))})$  with  $\mathbf{k}(s)$  given by (12). From the definition of the  $\omega^{(k)}$ , we obtain

$$E_\rho(T^k \alpha; \omega^{(k)}) = p_0(T^k \alpha; \omega^{(k)}) = P(\mathbf{g}_1(T^k \alpha), \dots, \mathbf{g}_p(T^k \alpha); T^k \alpha),$$

where  $P(\mathbf{u}; \mathbf{z})$  is a polynomial in  $\mathbf{u} = (u_{ij})$  and  $\mathbf{z} = (z_{ij})$  with coefficients independent of  $\mathbf{k}$ . If  $\Theta_s = 0$  for all sufficiently large  $s$ , then  $P(\mathbf{g}_1(\mathbf{z}), \dots, \mathbf{g}_p(\mathbf{z}); \mathbf{z})$  is identically

zero by Lemma 6. Since the functions  $g_{ij}(z_i)$  are algebraically independent, it follows that  $P(\mathbf{u}; \mathbf{z})$  is identically zero and so  $p_0(\mathbf{z}; \Omega(\mathbf{u})\omega)$  is identically zero in  $\mathbf{u}$  and  $\mathbf{z}$ , that is  $p_0(\mathbf{z}; \omega)$  has infinite index at  $\omega$ , in contradiction to the construction of Lemma 4. Consequently,  $\Theta_s \neq 0$  for infinitely many  $s$ . It now follows that the inequalities (14) and (15) conflict for suitable  $\rho$  and  $\mathbf{k}$ . This contradiction establishes Theorem 5.

## 6. Concluding remarks

There are two interesting ways in which our results might be extended, though we are not able to effect these improvements at present.

Firstly, it should be possible to obtain more precise results for functions of several complex variables satisfying functional equations of the shape (1). The main obstruction here is the uniqueness theorem (Lemma 6). Probably the following is true: Let  $T$  be an  $n \times n$  nonsingular non-negative integer matrix with no roots of unity as eigenvalues and let  $\alpha$  be an algebraic point of  $\mathbb{C}^n$  such that  $T^k \alpha \rightarrow 0$  as  $k \rightarrow \infty$  and the coordinates of  $\alpha$  are multiplicatively independent. Then, for every function  $f(z)$  which is regular in some neighbourhood of the origin in  $\mathbb{C}^n$  and not identically zero, there are infinitely many integers  $k$  such that  $f(T^k \alpha) \neq 0$ . The work of this note is confined to functions of one complex variable because we are only able to prove the above uniqueness theorem for diagonal matrices  $T$ .

It should also be possible to obtain algebraic independence results for functions satisfying chains of functional equations. (See Loxton and van der Poorten (1977b).) More specifically, Mahler's series (Mahler 1929),

$$f_\omega(z) = \sum_{h=1}^{\infty} [h\omega] z^h,$$

where  $\omega$  is a real irrational number, and certain gap series

$$f(z) = \sum_{h=0}^{\infty} a_h z^{\lambda_h},$$

where  $\lambda_h | \lambda_{h+1}$ , say, fall into this class of functions. It should be possible to show that if  $\alpha$  is an algebraic number with  $0 < |\alpha| < 1$ , then the set  $\{f_\omega(\alpha) : 0 < \omega < 1\}$  contains uncountably many algebraically independent numbers. However, there are difficulties even in obtaining precise results on the algebraic independence of the functions admitted here.

## References

- P. L. Cijsouw and R. Tijdeman (1973), "On the transcendence of certain power series of algebraic numbers", *Acta Arith.* 23, 301–305.  
 P. Dienes (1957), *The Taylor Series* (Dover, New York).

- K. K. Kubota (1976), "An application of Kronecker's theorem to transcendence theory", *Sém. de Théorie des Nombres de Bordeaux*, Année 1975/1976, no. 25.
- K. K. Kubota (1977a), "On the algebraic independence of holomorphic solutions of certain functional equations and their values", *Math. Ann.* 227, 9–50.
- K. K. Kubota (1977b), *Algebraic Independence Properties of Solutions to Linear Functional Equations, Transcendence Theory: Advances and Applications*, edited by A. Baker and D. W. Masser (Academic Press, London), Ch. 16, 227–229.
- J. H. Loxton and A. J. van der Poorten (1977a), "Arithmetic properties of certain functions in several variables", *J. Number Theory* 9, 87–106.
- J. H. Loxton and A. J. van der Poorten (1977b), "Arithmetic properties of certain functions in several variables III", *Bull. Austral. Math. Soc.* 16, 15–47.
- J. H. Loxton and A. J. van der Poorten (1977c), *Transcendence and Algebraic Independence by a Method of Mahler, Transcendence Theory: Advances and Applications*, edited by A. Baker and D. W. Masser (Academic Press, London), Ch. 15, 211–226.
- J. H. Loxton and A. J. van der Poorten (to appear, a), "A class of hypertranscendental functions", *Aequationes Math.*
- J. H. Loxton and A. J. van der Poorten (to appear, b), "Arithmetic properties of certain functions in several variables II", *J. Austral. Math. Soc.*
- K. Mahler (1929), "Arithmetische Eigenschaften der Lösungen einer Klasse von Funktionalgleichungen", *Math. Ann.* 101, 342–366.
- K. Mahler (1930a), "Über das Verschwinden von Potenzreihen mehrerer Veränderlichen in speziellen Punktfolgen", *Math. Ann.* 103, 573–587.
- K. Mahler (1930b), "Arithmetische Eigenschaften einer Klasse transzendentaltranszendenten Funktionen", *Math. Z.* 32, 545–585.
- K. Mahler (1965), "Arithmetic properties of lacunary power series with integral coefficients". *J. Austral. Math. Soc.* 5, 56–64.
- J. F. Ritt (1927), "A factorisation theory for functions  $\sum_{i=1}^n a_i e^{\alpha_i z}$ ", *Trans. Amer. Math. Soc.* 29, 584–596.
- Th. Schneider (1957), *Einführung in die Transzendenten Zahlen* (Springer, Berlin).

School of Mathematics  
 University of New South Wales  
 Kensington  
 New South Wales 2033  
 Australia