ARITHMETIC PROPERTIES OF LACUNARY POWER SERIES WITH INTEGRAL COEFFICIENTS

K. MAHLER

(received 14 August 1964)

To the memory of my dear friend J. F. Koksma

1

This note is concerned with arithmetic properties of power series

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

with integral coefficients that are lacunary in the following sense. There are two infinite sequences of integers, $\{r_n\}$ and $\{s_n\}$, satisfying

(1) $$0 = s_0 \leqq r_1 < s_1 \leqq r_2 < s_2 \leqq r_3 < s_3 \leqq \cdots, \qquad \lim_{n\to\infty} \frac{s_n}{r_n} = \infty,$$

such that

(2) $$f_h = 0 \text{ if } r_n < h < s_n, \text{ but } f_{r_n} \neq 0,\ f_{s_n} \neq 0 \qquad (n = 1, 2, 3, \cdots).$$

It is also assumed that $f(z)$ has a positive radius of convergence, R_f say, where naturally

$$0 < R_f \leqq 1.$$

A power series with these properties will be called *admissible*.

Let $f(z)$ be admissible, and let α be any algebraic number inside the circle of convergence,

$$|\alpha| < R_f.$$

Or aim is to establish a simple test for deciding whether the value $f(\alpha)$ is an algebraic or a transcendental number. As will be found, the answer depends on the behaviour of the polynomials

(3) $$P_n(z) = \sum_{h=s_n}^{r_{n+1}} f_h z^h \qquad (n = 0, 1, 2, \cdots).$$

In terms of these polynomials, $f(z)$ allows the development

(4) $$f(z) = \sum_{n=0}^{\infty} P_n(z)$$

which likewise converges when $|z| < R_f$.

https://doi.org/10.1017/S1446788700025866 Published online by Cambridge University Press

2

If

$$a(z) = a_0 + a_1 z + \cdots + a_m z^m$$

is an arbitrary polynomial, put

$$H(a) = \max_{0 \leqq j \leqq m} |a_j|, \quad L(a) = \sum_{j=0}^{m} |a_j|.$$

Then

$$H(ab) \leqq H(a)L(b), \quad L(ab) \leqq L(a)L(b). \tag{5}$$

The following theorem is due to R. Güting (Michigan Math. J., **8** (1961), 149—159).

Lemma 1. *Let α be an algebraic number which satisfies the equation*

$$A(\alpha) = 0, \quad \textit{where} \quad A(z) = A_0 + A_1 z + \cdots + A_M z^M \qquad (A_M \neq 0)$$

is an irreducible polynomial with integral coefficients. If

$$a(z) = a_0 + a_1 z + \cdots + a_m z^m$$

is a second polynomial with integral coefficients, then either

$$a(\alpha) = 0$$

or

$$|a(\alpha)| \geqq \left(L(a)^{M-1} L(A)^m\right)^{-1}.$$

3

The main result of this note may be stated as follows.

Theorem 1. *Let $f(z)$ be an admissible power series, and let α be any algebraic number satisfying $|\alpha| < R_f$. The function value $f(\alpha)$ is algebraic if and only if there exists a positive integer $N = N(\alpha)$ such that*

$$P_n(\alpha) = 0 \quad \textit{for all} \quad n \geqq N.$$

Corollary: If the coefficients f_h are non-negative, then $f(z)$ is transcendental for all *positive* algebraic numbers $\alpha < R_f$. There exist, however, examples of admissible functions $f(z)$ with $f_h \geqq 0$ for which S_f, as defined in 4, is everywhere dense in $|z| < R_f$.

Proof. It is obvious that the condition is sufficient, and so we need only show that it is also necessary.

We shall thus assume that the function value

$$f(\alpha) = \sum_{h=0}^{\infty} f_h \alpha^h, \quad = \beta^{(0)} \text{ say}, \tag{6}$$

is an algebraic number, say of degree l over the rational field. Let

$$\beta^{(0)}, \beta^{(1)}, \cdots, \beta^{(l-1)} \tag{7}$$

https://doi.org/10.1017/S1446788700025866 Published online by Cambridge University Press

be its conjugates, and let c_0 be a positive integer such that the products

$$c_0\beta^{(0)},\ c_0\beta^{(1)},\ \cdots,\ c_0\beta^{(l-1)}$$

are algebraic integers.

We denote by $c_1, c_2, \cdots$ positive constants that may depend on α, $\beta^{(0)}, \cdots, \beta^{(l-1)}$, but are independent of n. In particular, we choose c_1 such that

$$(8) \qquad |\alpha| < \frac{1}{c_1} < R_f, \quad \text{hence} \quad c_1 > 1, \quad |c_1\alpha| < 1,$$

and c_2 such that

$$(9) \qquad |f_h| \leqq c_1^h c_2 \text{ for all } h \geqq 0.$$

Put

$$(10) \qquad p_{n\lambda}(z) = -\beta^{(\lambda)} + \sum_{h=0}^{r_n} f_h z^h \qquad (\lambda = 0, 1, \cdots, l-1)$$

and

$$p_n(z) = c_0^l \prod_{\lambda=0}^{l-1} p_{n\lambda}(z).$$

Then $p_n(z)$ is a polynomial in z of degree lr_n with integral coefficients.

From the second formula (5),

$$L(p_n) \leqq c_0^l \prod_{\lambda=0}^{l-1} L(p_{n\lambda}),$$

and here by (8) and (9),

$$L(p_{n\lambda}) \leqq |\beta^{(\lambda)}| + \sum_{h=0}^{r_n} |f_h| \leqq c_1^{r_n} c_3 \qquad (\lambda = 0, 1, \cdots, l-1).$$

It follows that

$$(11) \qquad L(p_n) \leqq c_1^{lr_n} c_4.$$

Since α is algebraic, it is the root of an irreducible equation $A(\alpha) = 0$ where $A(z)$ is, say of degree M. On applying Lemma 1, with $a(z) = p_n(z)$, we deduce from (11) that either

$$p_n(\alpha) = 0$$

or

$$(12) \qquad |p_n(\alpha)| \geqq \{(c_1^{lr_n} c_4)^{M-1} L(A)^{lr_n}\}^{-1} \geqq c_5^{-lr_n}.$$

However, the second alternative (12) cannot hold if n is sufficiently large. For by (6), (9), and (10),

$$|p_{n0}(\alpha)| = |\sum_{h=s_n}^{\infty} f_h \alpha^h| \leqq |c_1 \alpha|^{s_n} c_6,$$

and it is also obvious that

$$|p_{n\lambda}(\alpha)| \leqq c_7 \qquad (\lambda = 1, 2, \cdots, l-1).$$

On combining these estimates it follows that

$$|p_n(\alpha)| \leqq c_0^l \cdot |c_1 \alpha|^{s_n} c_6 \cdot c_7^{l-1} < c_5^{-lr_n}$$

for all sufficiently large n, because by (1) and (8),

$$|c_1 \alpha| < 1, \qquad \lim_{n\to\infty} \frac{s_n}{r_n} = \infty.$$

Thus there exists an integer N_0 such that

$$p_n(\alpha) = 0 \text{ for all } n \geqq N_0.$$

This means that to every integer $n \geqq N_0$ there exists a suffix λ_n which has one of the values $0, 1, 2, \cdots, l-1$ such that

$$\sum_{h=0}^{r_n} f_h \alpha^h = \beta^{(\lambda_n)}.$$

Therefore also

$$\text{(13)} \qquad P_n(\alpha) = \sum_{h=0}^{r_{n+1}} f_h \alpha^h - \sum_{h=0}^{r_n} f_h \alpha^h = \beta^{(\lambda_{n+1})} - \beta^{(\lambda_n)} \quad \text{if} \quad n \geqq N_0.$$

Now $f(\alpha)$ is a convergent series, and hence

$$\lim_{n\to\infty} P_n(\alpha) = 0.$$

On the other hand, the l conjugate numbers (7) are all distinct. There is then an integer $N \geqq N_0$ with the property that

$$\lambda_{n+1} = \lambda_n \quad \text{if} \quad n \geqq N.$$

By (13), this implies that

$$P_n(\alpha) = 0 \quad \text{if} \quad n \geqq N,$$

giving the assertion.

4

Let Σ be a set of algebraic numbers, S a subset of Σ. For each element α of Σ denote by $A(\alpha)$ the set of all algebraic conjugates $\alpha, \alpha', \alpha'', \cdots$ of α that belong to Σ. We say that *the set S is complete relative to Σ* if

https://doi.org/10.1017/S1446788700025866 Published online by Cambridge University Press

$$\alpha \in S \text{ implies that also } A(\alpha) \in S.$$

Let again $f(z)$ be an admissible power series. Then denote by Σ_f the set of all algebraic numbers α satisfying $|\alpha| < R_f$ and by S_f the set of all $\alpha \in \Sigma_f$ for which $f(\alpha)$ is algebraic.

THEOREM 2. *If $f(z)$ is admissible, the set S_f is complete relative to Σ_f.*

PROOF. Let α be any element of S_f, and let $q(z)$ be the primitive irreducible polynomial with integral coefficients and positive highest coefficient for which $q(\alpha) = 0$. By Theorem 1,

$$P_n(\alpha) = 0 \quad \text{for} \quad n \geqq N,$$

and hence

$$P_n(z) \text{ is divisible by } q(z) \text{ for all suffixes } n \geqq N.$$

Hence, if α' is any conjugate of α, also

$$P_n(\alpha') = 0 \quad \text{for} \quad n \geqq N.$$

Assume, in particular, that $\alpha' \in \Sigma_f$, hence that $f(\alpha')$ converges. Then, by Theorem 1, $f(\alpha')$ is algebraic, and therefore also α' is in S_f.

5

The following result establishes all possible sets S_f in which an admissible power series can assume algebraic values.

THEOREM 3. *Let R be a positive constant not greater than* 1; *let Σ be the set of all algebraic numbers α satisfying $|\alpha| < R$; and let S be any subset of Σ which contains the element* 0 *and is complete relative to Σ. Then there exists an admissible power series $f(z)$ with the property that*

$$R_f = R \quad \textit{and} \quad S_f = S.$$

PROOF. As a set of algebraic numbers, S is countable. It is therefore possible to define an infinite sequence of polynomials

$$\{q_n(z)\} = \{q_0(z), q_1(z), q_2(z), \cdots\}$$

with the following properties.

If S consists of the single element 0, put $q_n(z) \equiv 1$ for all suffixes n. If S is a finite set, take for the first finitely many elements of $\{q_n(z)\}$ all distinct primitive irreducible polynomials with integral coefficients and positive highest coefficients that vanish in at least one point α of S, and put all remaining sequence elements equal to $q_n(z) \equiv 1$. If, finally, S is an infinite set, let $\{q_n(z)\}$ consist of all distinct primitive irreducible polynomials with integral coefficients and positive highest coefficients that vanish in at least one point α of S.

Further let

$$Q_n(z) = q_0(z)q_1(z)\cdots q_n(z) \qquad (n = 0, 1, 2, \cdots);$$

denote by d_n the degree of $Q_n(z)$; and put

$$H_n = H(Q_n) \qquad (n = 0, 1, 2, \cdots).$$

Next choose a sequence of integers $\{s_n\}$ where

$$0 = s_0 < s_1 < s_2 < \cdots$$

such that

$$\text{(14)} \qquad \lim_{n\to\infty} \frac{s_n}{d_n} = \infty, \quad \lim_{n\to\infty} \frac{s_{n+1}}{s_n} = \infty, \quad \lim_{n\to\infty} H_n^{1/s_n} = 1$$

and

$$s_{n+1} > s_n + d_n \qquad (n = 0, 1, 2, \cdots).$$

Hence, on putting

$$r_{n+1} = s_n + d_n \qquad (n = 0, 1, 2, \cdots),$$

the two sequences $\{r_n\}$ and $\{s_n\}$ have the property

$$\text{(1)} \qquad 0 = s_0 \leqq r_1 < s_1 \leqq r_2 < s_2 \leqq r_3 < s_3 \leqq \cdots, \quad \lim_{n\to\infty} \frac{s_n}{r_n} = \infty.$$

Finally denote by $\{K_n\}$ a sequence of positive integers satisfying

$$\text{(15)} \qquad \lim_{n\to\infty} K_n^{1/s_n} = \frac{1}{R}.$$

On putting

$$P_n(z) = K_n Q_n(z) z^{s_n}, = \sum_{h=s_n}^{r_{n+1}} f_h z^h \text{ say} \qquad (n = 0, 1, 2, \cdots),$$

and

$$\text{(4)} \qquad f(z) = \sum_{n=0}^{\infty} P_n(z) = \sum_{h=0}^{\infty} f_h z^h,$$

$f(z)$ is a lacunary power series of the kind defined in § 1.

Distinct polynomials $P_n(z)$ evidently involve different powers of z, so that the contributions to $f(z)$ from these polynomials do not overlap.

To prove that $f(z)$ is admissible we have to prove that the radius R_f of convergence of $f(z)$ is positive. In fact

$$\frac{1}{R_f} = \limsup_{h\to\infty} |f_h|^{1/h},$$

and this, by the formulae (1) and (14), is equal to

https://doi.org/10.1017/S1446788700025866 Published online by Cambridge University Press

$$\frac{1}{R_f} = \limsup_{\substack{s_n \leqq h \leqq r_{n+1} \\ n \to \infty}} |f_h|^{1/s_n}.$$

Further

$$|f_h| \leqq H_n K_n \quad \text{for} \quad s_n \leqq h \leqq r_{n+1},$$

with equality for at least one suffix h in this interval. Hence, by (14) and (15),

$$\frac{1}{R_f} = \limsup_{n \to \infty} (H_n K_n)^{1/s_n} = \frac{1}{R},$$

so that

$$R_f = R > 0.$$

The second assertion

$$S_f = S$$

is now an immediate consequence of Theorem 1 and the construction of the polynomials $P_n(z)$. For if α is any element of S, then evidently $P_n(z)$, for sufficiently large n, will be divisible by the polynomial $q_\nu(z)$ which has α as a root, and so $\alpha \in S_f$. On the other hand, if α is not an element of S, no polynomial $q_\nu(z)$ and hence also no polynomial $P_n(z)$ vanishes for $z = \alpha$.

6

The two Theorems 1 and 3 together solve the problem of establishing all possible sets S_f in which an admissible function may be algebraic. In order to obtain further results, it becomes necessary to specialise $f(z)$.

Let us, in particular, consider those admissible power series

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

which are of the bounded type, i.e. to which there exists a positive constant c such that

$$(16) \qquad |f_h| \leqq c \quad \text{for all} \quad h \geqq 0.$$

For such series the set S_f is restricted as follows.

THEOREM 4. *If $f(z)$ is an admissible power series of the bounded type, then S_f may, or may not, be an infinite set. If*

$$S_f = \{\alpha_1, \alpha_2, \alpha_3, \cdots\}$$

is an infinite set, then

$$\lim_{k \to \infty} |\alpha_k| = R_f = 1.$$

PROOF. (i) It is obvious from Theorem 1 that there exist admissible power series of the bounded type for which S_f is a finite set, e.g. consists

https://doi.org/10.1017/S1446788700025866 Published online by Cambridge University Press

of the single point 0. The following construction, on the other hand, leads to such a series for which S_f is an infinite set.

We procede similarly as in the proof of Theorem 3, but take $R = 1$ and

$$q_n(z) = 1-z^{3^n}-z^{2\cdot 3^n}, \qquad K_n = 1 \qquad (n = 0, 1, 2, \cdots).$$

Then, in the former notation,

$$H_n = 1 \qquad (n = 0, 1, 2, \cdots),$$

because the Taylor coefficients of $Q_n(z) = q_0(z)q_1(z)\cdots q_n(z)$ all can only be equal to 0, $+1$, or -1. The construction leads therefore to an admissible power series $f(z)$ the Taylor coefficients of which likewise can only be equal to 0, $+1$, or -1. Furthermore, the corresponding set S_f consists of the infinitely many numbers

$$\sqrt[3^n]{\frac{\sqrt{5}-1}{2}} \qquad (n = 0, 1, 2, \cdots).$$

(ii). Next let $f(z)$ be an admissible power series of the bounded type, thus with the radius of convergence $R_f = 1$, and let r and R be any two constants satisfying

$$0 < r < R < 1.$$

Let $S_f(r)$ be the subset of those elements α of S_f for which

$$|\alpha| \leqq r.$$

We apply again the formulae (3) and (4) and put

$$P_n^*(z) = z^{-s_n}P_n(z) = \sum_{h=s_n}^{r_{n+1}} f_h z^{h-s_n} \qquad (n = 1, 2, 3, \cdots);$$

here, by (2),

$$P_n^*(0) = f_{s_n} \neq 0 \qquad (n = 1, 2, 3, \cdots).$$

Therefore, by Jensen's formula,

$$\sum_\alpha \log \frac{R}{|\alpha|} = \log \frac{1}{|f_{s_n}|} + \frac{1}{2\pi}\int_0^{2\pi} \log |P_n^*(Re^{\vartheta i})| d\vartheta,$$

where $\sum_\alpha$ extends over all zeros α of $P_n^*(z)$ for which $|\alpha| \leqq R$. Here, on the right-hand side,

$$\log \frac{1}{|f_{s_n}|} \leqq 0, \quad |P_n^*(Re^{\vartheta i})| \leqq c(1+R+R^2+\cdots) = \frac{c}{1-R} \text{ for real } \vartheta,$$

where c is the constant in (16).

Assnme, in particular, that $|\alpha| \leqq r$ and hence $\log R/|\alpha| \geqq \log R/r$. The inequality (17) shows then that $P_n^*(z)$ cannot have more than

$$\left(\log \frac{c}{1-R}\right) \Big/ \left(\log \frac{R}{r}\right)$$

zeros for which $|\alpha| \leqq r$. This estimate is independent on n. On allowing both R and r to tend to 1, the assertion follows immediately from Theorem 1.

Mathematics Department,
Institute of Advanced Studies,
Australian National University,
Canberra, A.C.T.
11th August, 1964