ALFRED J. VAN DER POORTEN

Arithmetic implications of the distribution of integral zeros of exponential polynomials


<http://www.numdam.org/item?id=SDPP_1974-1975__16_1_A7_0>
I will be discussing certain ideas of MAHLER ([7], [8], [9]) dating from the period 1928-30. Recently LOXTON and VAN DER POORTEN ([4], [5], [6]) have presented these results in a somewhat more generalised setting. There are a number of open questions mentioned by MAHLER in [11]. One of these questions can be transformed into a question concerning the distribution of zeros of exponential polynomials in several variables, thus partly justifying the title of this lecture. At the time of nominating this title, I believed I had proved a very general result concerning the integral zeros of such exponential polynomials; in the event, I am left with a conjecture and some remarks which hopefully will prove to be of interest.


1.1. A 1-variable example.

Let $T : \mathbb{C} \rightarrow \mathbb{C}$ be the map given by $z \mapsto z^f$, where $f$ is a positive integer $\geq 2$. It is easily seen that the function $f(z) = \sum_{u=0}^{\infty} z^{f^u}$ is a transcendental function (the unit circle is a natural boundary) and that it is a solution of the functional equation

$$f(Tz) = f(z) - z.$$  

THEOREM (MAHLER [7]). - If $0 < |\alpha| < 1$ and $\alpha$ is algebraic, then $f(\alpha)$ is transcendental.

Proof. - Suppose both $\alpha$, $f(\alpha)$ belong to an algebraic number field $K$. For $\beta \in K$, write

$$||\beta|| = \sup_{\sigma} (\text{den } \beta, |\sigma \beta|)$$

where $\text{den } \beta$ is a denominator for $\beta$ and $\sigma$ runs through the embeddings of $K$ in $\mathbb{C}$. If $[K : \mathbb{Q}] = d$ and $\beta \neq 0$, it is well-known that

$$\log |\beta| \geq - 2d \log ||\beta|| \quad (\text{see, say, WALDSCHMIDT [13], p. 6}).$$

In the following $c_1$, $c_2$, ... will denote positive constants independent of the parameters $\rho$, $k$ to be introduced below.

For each positive integer $\rho$ there are $\rho + 1$ polynomials $p_0(z), \ldots, p_{\rho}(z)$ with degree at most $\rho$ and with coefficients integers in $K$ (indeed in $\mathbb{Z}$), such that the auxiliary function

$$E_\rho(z) = \sum_{j=0}^{\rho} p_j(z) f(z)^j = \sum_{\mu} b_\mu z^\mu$$
is not identically zero, but all coefficients \( b_\mu \) with \( \mu \leq \rho^2 \) vanish. To see
this observe that the \((\rho + 1)^2\) coefficients of the \( p_j(z)\) are being asked to sa-

1.2. 1-variable generalisations.

The same argument as just employed can deal with the following more general si-
tuation. Let \( f \) be a function which in some neighbourhood of the origin has a
Taylor expansion

where the \( A_\mu \) all in some fixed algebraic number field. W

Suppose further that \( f \) satisfies a functional equation of the shape

One can now show that \( \alpha \neq 0 \) and \( f(\alpha) \) cannot both be algebraic subject to
certain conditions on \( T : z \mapsto z^\ell\) and \( \alpha \). These conditions are that, firstly,
\( \ell > s \); this is required to establish the inequality (6). Secondly, of course, the
series (7) must converge for \( z = \alpha \), and then automatically for \( z = T^k \alpha \),
k = 1, 2, \ldots; this leads to the requirement that \( T^k \alpha \rightarrow 0 \) as \( k \rightarrow \infty \).
Thirdly one wishes that (8) defines \( f(T^k \alpha) \), \( k = 1, 2, \ldots \) given \( f(\alpha) \); if \( \Delta(z) \) denotes the resultant of the two forms \( \sum a_j(z) u^j v^{s-j}, \sum b_j(z) u^j v^{s-j} \), then the condition turns out to be \( \Delta(T^k \alpha) \neq 0 \) for \( k = 0, 1, 2, \ldots \).

I do not know of interesting examples with \( s > 1 \). Some examples to which the theorem applies include

\[
\prod_{\mu=0}^{\infty} (1 - z^\mu), \sum_{\mu=0}^{\infty} z^\mu/(1 - z^\mu), \ldots
\]

1.3. Generalisation to functions of several variables.

Henceforth let \( n \) be a fixed integer and let \( z \) denote the \( n \)-tuple

\[ z = (z_1, \ldots, z_n). \]

If \( \mu = (\mu_1, \ldots, \mu_n) \) denotes a \( n \)-tuple, we denote by \( z^\mu \) the monomial \( z_1^{\mu_1} z_2^{\mu_2} \ldots z_n^{\mu_n} \). A point \( \alpha \in \mathbb{C}^n \) is algebraic if \( \alpha_1, \ldots, \alpha_n \) are algebraic.

Let \( T = (t_{ij}) \) denote a \( n \times n \) integer matrix. We define a transformation \( (\mathbb{C}^n)^n \rightarrow (\mathbb{C}^n)^n \), also denoted by \( T \), by the rule \( Tz = w \) where

\[
w_i = \prod_{j=1}^{n} t_{ij}^{z_j}, \quad i = 1, 2, \ldots, n.
\]

One easily sees that \( (Tz)^\mu = z^{\mu T} \) where \( \mu T \) is the usual product of the row-vector \( \mu \) and the matrix \( T \). It follows that \( T^k z = T(z^{k-1} z), \quad k = 1, 2, \ldots \).

Now denote by \( \lambda \) the spectral radius of the matrix \( T \), that is, the maximum of the absolute value of the eigenvalues of \( T \). With the appropriate \( n \)-variable reinterpretations of the notation we can apply the proof of section 1.1 to apply to functions \( f \) of \( z = (z_1, \ldots, z_n) \), where \( f \) satisfies (7) and (8). A trivial change is required, in particular in (5), \( \rho^2 \) is replaced by \( \rho^{1+\frac{s}{k}} \).

Of course certain conditions must be satisfied by the matrix \( T \) and the point \( \alpha \). In order to establish the analogue of (4), we will require that

\[
\log |(T^k \alpha)|^\mu | \leq -c_6 \lambda^k \langle u, \mu \rangle, \quad k \geq c_7
\]

where the constant \( c \) depends only on \( T \), \( \langle \cdot, \cdot \rangle \) denotes the inner product of \( n \)-tuples, the \( n \)-tuple \( u \) depends only on \( T \) and \( \alpha \), and \( u_1, \ldots, u_n > 0 \).

Secondly we need to know that

\[
E_p (T^k \alpha) \neq 0 \quad \text{for infinitely many} \quad k.
\]

Surprisingly it is this condition which presents the greatest difficulties and which motivates section 2.

Furthermore, but these conditions apply also in the 1-variable case, we need \( \alpha_1 \alpha_2 \ldots \alpha_n \neq 0 \) and \( T^k \alpha \rightarrow 0 \) as \( k \rightarrow \infty \), so that given (7), \( f(\alpha) \) automatically is defined when \( T \) is non-singular provided also that \( \Delta(T^k \alpha) \neq 0 \), \( k = 0, 1, \ldots \).

Finally we observe that we obtain the inequality (6) provided that \( \lambda > s \).
Since certainly $s \geq 1$ we cannot allow all the eigenvalues of $T$ to be roots of unity.

We shall not go into detail concerning the condition on $T$ that implies (9) but refer the reader to GANTMACHER ([2], pages 65-94, or to [5]).

We conclude with some examples: Let $\{a_h\}$ be the sequence of Fibonacci numbers $\{0, 1, 1, \ldots\}$ satisfying $a_{h+1} = a_h + a_{h-1}$, $h = 1, 2, \ldots$ The function

$$f(z) = f(z_1, z_2) = \sum_{h=0}^{\infty} a_h z_1^h z_2^{h+1}$$

satisfies

$$f(z_2, z_1, z_2) = f(z_1, z_2) - z_2,$$

here $T = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. It follows that if $\alpha_1 \neq 0$, $\alpha_1$, $\alpha_2$ are algebraic, and $f(\alpha_1, \alpha_2)$ is defined, then $f(\alpha_1, \alpha_2)$ is transcendental. In particular,

$$f(\alpha, 1) = \sum_{h=0}^{\infty} \alpha_h$$

is transcendental for $\alpha$ algebraic, $0 < |\alpha| < 1$. A sufficient condition in order that $f(\alpha_1, 1), f(\alpha_2, 1), \ldots, f(\alpha_m, 1)$ be linearly independent over the field $\mathbb{A}$ of all algebraic numbers is that the numbers $|\alpha_1|, \ldots, |\alpha_m|$ be multiplicatively independent, as we shall see later.

Let $f(z) = \sum_{h=0}^{\infty} z^h$ and let $\beta_1, \ldots, \beta_n$ be algebraic numbers, not all of which are zero. Then the function

$$F(z_1, \ldots, z_n) = \sum_{h=0}^{n} \beta_h f(z_h)$$

satisfies $F(z_1, \ldots, z_n) = F(z_1, \ldots, z_n) - (\beta_1 z_1 + \ldots + \beta_n z_n)$.

We shall show later that it is sufficient that the non-zero algebraic numbers $\alpha_1, \ldots, \alpha_n$ be multiplicatively independent in order that, if also $|\alpha_h| < 1$, $h = 1, \ldots, n$, the number $F(\alpha_1, \ldots, \alpha_n)$ be transcendental. Thus with the given conditions on $\alpha_1, \ldots, \alpha_n$ the numbers $f(\alpha_1), \ldots, f(\alpha_n)$ are linearly independent over the field $\mathbb{A}$.

On the other hand, the theorem cannot deal with the following examples: Although

$$f(z, q) = \sum_{h=0}^{\infty} z^h q^{h(h-1)}$$

satisfies $f(zq, q) = z^{-1} f(z, q) - z^{-1}$, we have $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and both eigenvalues are $1$, so $k \neq 1$. For a different reason, we cannot deal with: let $j(\omega)$ be Weber's modular function of level 1. Then if

$$F(z) = j\left( \frac{\log z}{2\pi i} \right) - z^{-1},$$

there is a polynomial $P$ such that $F(z, F(z), F(z^k)) = 0$, $k$ an integer $\geq 2$. However we require that $F(z^k)$ be a rational function of $z$ and $F(z)$.

We conclude by remarking that all of the ideas of section 1 are due to MAHLER ([7], [8], [9], [11]). For the details which are omitted above, the reader is referred to these original papers, or to [5].
2. Integral zeros of exponential polynomials.

2.1. The vanishing of power series in certain sequences of points.

Let \( E(z) = \sum_{\mu} b_{\mu} z^{\mu} \) be a power series with coefficients \( b_{\mu} \) all of which lie in some fixed algebraic number field. Further let \( \alpha \in (\mathbb{C}^n)^n \) be an algebraic point, and \( T \) a \( n \times n \) integer matrix such that the condition

\[
\log |(T^k \alpha)^\mu| \leq - c_6 \langle u, \mu \rangle, \quad k \geq c_7
\]

is satisfied; here \( u_1, \ldots, u_n \) are all positive, and we remark that \( u \) is actually the projection of \((- \log |\alpha_1|, \ldots, - \log |\alpha_n|)\) onto the eigenspace of \( T \) spanned by eigenvectors whose eigenvalue has absolute value \( \lambda \). If the power series \( E(z) \) converges in a neighbourhood of the origin, then \( E(T^k \alpha) \) exists for \( k \geq c_8 \). We suppose \( E(z) \) is not identically zero. We can write

\[
E(z) = \sum_{R} E_R(z)
\]

where

\[
E_R(z) = \sum_{\langle \mu, u \rangle = R} b_{\mu} z^{\mu}.
\]

The notation is so chosen that none of the \( E_R(z) \) in (11) vanishes identically. Since \( u > 0 \), each \( E_R(z) \) is a polynomial, and the index \( R \) in (11) runs through a discrete series \( 0 < R_0 < R_1 < R_2 < \ldots \)

If \( E(T^k \alpha) = 0 \), \( k \geq c_9 \) it follows that one has for some \( \varepsilon > 0 \)

\[
E_{R_0}(T^k \alpha) = 0(\exp(- (R_0 + \varepsilon) \lambda^k)) \quad (k \to \infty).
\]

One sees however without undue difficulty, that as a consequence of a theorem of A. BAKER [1], we must have

\[
E_{R_0}(T^k \alpha) = 0 \quad k \geq c_{10}.
\]

Hence, in order to study conditions on \( \alpha \) such that \( E(T^k \alpha) = 0 \), \( k \geq c_9 \) it is sufficient to consider polynomials \( F(z) \) such that \( F(T^k \alpha) = 0 \), \( k \geq c_{10} \).

2.2. The vanishing of polynomials in certain sequences of points.

Let \( M \) be a finite set of \( n \)-tuples of non-negative integers, and denote by

\[
F(z) = \sum_{\mu \in M} b_{\mu} z^{\mu}
\]

a polynomial in \( \mathbb{Q}[z_1, \ldots, z_n] \). Suppose \( F(z) \) does not vanish identically but

\[
F(T^k \alpha) = 0, \quad k = 0, 1, 2, \ldots
\]

If the minimal polynomial of \( T \) has degree \( m \) write

\[
t^k = \lambda_{k_1} I + \lambda_{k_2} T + \cdots + \lambda_{k_m} T^{m-1}, \quad k = 0, 1, 2, \ldots
\]

For each \( \mu \in M \) define \( m \)-tuples \( \gamma_\mu \) by

\[
\gamma_\mu = (\langle \beta, \mu \rangle, \langle \beta, \mu T \rangle, \ldots, \langle \beta, \mu T^{m-1} \rangle)
\]
where $\beta$ is the $n$-tuple $\beta = (\log \alpha_1, \ldots, \log \alpha_n)$. Then the vanishing of the polynomial $F(z)$ in the sequence $z = t^k \alpha$, $k = 0, 1, 2, \ldots$ implies that the exponential polynomial

$$G(\xi) = \sum_{\mu \in M} b_\mu \exp(\gamma_\mu, \xi)$$

in the $m$-variables $\xi = (\xi_1, \ldots, \xi_m)$ vanishes at the points $\xi = \lambda_k$, $k = 0, 1, 2, \ldots$ as defined by (12). More explicitly if

$$T^m = a_1 I + a_2 T + \ldots + a_n T^{m-1}$$

then $G(\xi)$ vanishes on the sequence $\xi = \lambda_0 g^k$, $k = 0, 1, 2, \ldots$ where $\lambda_0 = (1, 0, \ldots, 0)$ and $3$ is the $m \times m$ matrix

$$3 = \begin{pmatrix}
0 & 1 & \cdots & 0 \\
1 & \ddots & \ddots & 1 \\
\vdots & \ddots & \ddots & \ddots \\
a_1 & a_2 & \cdots & a_n
\end{pmatrix}.$$

We digress to remark the following: given the condition (9) on $T$ and $\alpha$ one can conclude without difficulty, though non-trivially, since the argument requires a transcendence result of BAKER (see, for example, [13]) that if $|\alpha_1|, \ldots, |\alpha_n|$ are multiplicatively independent (that is, $\log |\alpha_1|, \ldots, \log |\alpha_n|$ are linearly independent over $\mathbb{Q}$) then $F(t^k \alpha) = 0$, $k = 0, 1, 2, \ldots$ implies $F(z) \equiv 0$. By a more elementary argument one similar sees that $F(z) \equiv 0$ is implied if the characteristic polynomial of $T$ is irreducible over $\mathbb{Q}$. So in both these circumstances one has the condition (10). The second assertion is already proved by MAHLER [7]. For details, see [5]. Neither of these two cases require the argument of sections 2.1 and 2.2.

2.3. The vanishing of exponential polynomials at integer points.

We shall suppose that in the foregoing construction, no eigenvalue of $T$ is a root of unity, and that the eigenvalues of $3$ have distinct absolute value (if necessary we replace $T$ by a power and then proceed as in 2.2; there is no loss of generality in our assumption, in that the condition (9) essentially places this condition on $T$); we also suppose that $T$ is invertible.

In an attempt to apply SKOLEM's method (see [12] and references below), we select a rational prime $p$ with respect to which $\det T$ is a unit, and then a positive integer $d$ such that $T^d \equiv I \pmod{p^d}$ where $d$ is sufficiently large so as to render the following valid. It is clear (but for details see, for example, LECH [3]) that there is a prime ideal $p$ containing $p$ so that the $p$-adic completion $K_p$ contains an isomorphic copy of the field generated over $\mathbb{Q}$ by the finitely many numbers $\mu$ and the components of the $\gamma_\mu$. The following then takes place in $K_p$ and the valuation is the $p$-adic valuation so normalised that $|p| = p^{-1}$. 


We write
\[ S = \log(1 + (3^d-1)) = (3^d-1)/1 - (3^d-1)^2/2 + (3^d-1)^3/3 - \ldots \]
(14)
\[ = \log 3^d \quad (p\text{-adic}) \]
which is well-defined because \(|3^d - 1| \leq p^{-\ell} \). Then we can expand
\[ \sum_{\mu \in M} b_{\mu} \exp(\gamma_{\mu} \lambda_{0}) \exp(\gamma_{\mu} \lambda_{0}(3^d - 1)) \]
(15)
as a \( p \)-adic power series convergent for all \( z \in \mathbb{Z}_p \) the \( p \)-adic integers. But the power series vanishes at the infinitely many points \( z = 0, 1, 2, \ldots \) in the compact set \( \mathbb{Z}_p \) and so vanishes identically on \( \mathbb{Z}_p \). Hence the coefficient of each power of \( z \) vanishes and we obtain infinitely many \( p \)-adic equations. Unfortunately these equations increase in complexity and do not seem to provide much useful insight. In the special case however, where \( \mathcal{J} \) is a \( 1 \times 1 \) matrix (so \( m = 1 \)), that is \( T = \lambda I \) these equations do "unravel" and one does obtain that for some \( \mu \neq \mu' \)
\[ \alpha_{\mu}^{p_{\mu} - \mu'} = 1. \]

So necessarily the numbers \( \alpha_1, \ldots, \alpha_n \) are multiplicatively dependent; this is a much stronger result than the previously remarked upon condition that \( |\alpha_1|, \ldots, |\alpha_n| \) are necessarily multiplicatively dependent. The reader will notice that the result for the case \( T = \lambda I \) is actually a special case of a theorem of LECH [3] and MAHLER [10] concerning integer zeros of exponential polynomials in one variable. Actually, by a quite different method, the special case was already proved by MAHLER [8] and generalised to triangular matrices \( T \) by LOXTON and the author [5]; this last generalisation does not appear to be obtainable by the \( p \)-adic method outlined above.

Nevertheless, in view of these results, it seems reasonable to conjecture that if the exponential polynomial (13)
\[ G(\zeta) = \sum_{\mu \in M} b_{\mu} \exp(\gamma_{\mu} \zeta) \]
vanishes at all the points \( \zeta = \lambda_{0} 3^k, k = 0, 1, 2, \ldots \) then necessarily for some \( \mu \neq \mu' \) one has \( \gamma_{\mu} = \gamma_{\mu'} \), which is to say \( \langle \beta, \mu \zeta^k \rangle = \langle \beta, \mu' \zeta^k \rangle \), \( \zeta = 0, 1, \ldots, m - 1 \), and finally
\[ \alpha_{\mu}^{(\mu - \mu')} s = 1, \text{ for all } s \in \mathbb{Z}[T], \]
so a strong form of multiplicative dependence of the number \( \alpha_1, \ldots, \alpha_n \).

Incidentally, if the characteristic polynomial of \( \mathcal{J} \) (so the minimal polynomial of \( T \)) is irreducible over \( \mathbb{Q} \) and \( \mathcal{J} \) has an eigenvalue \( \lambda \) greater in absolute value than its other eigenvalues (as is implied by the condition (9)) then
\[ G(\lambda_{0} 3^k) = 0, \quad k = 0, 1, 2, \ldots, \]
implies that for some \( \mu \neq \mu' \)
\[ |\exp(\gamma_{\mu} - \gamma_{\mu'}, \nu)| = 1, \]
where the components of $v$ are algebraic numbers linearly independent over $\mathbb{Q}$. Since $\gamma_\mu, \gamma_{\mu'}$ have components which are logarithms of algebraic numbers (given $\alpha$ an algebraic point) one can conclude by a transcendence result of Baker that $|\exp(\beta, (\mu - \mu')^T)| = 1$ for $\ell = 0, 1, \ldots, m - 1$ and finally that $|\alpha^{(\mu - \mu')}^s| = 1$ for all $s \in \mathbb{Z}[T]$.

It is this argument which justifies the assertion in 1.3 that if $|\alpha_1|, \ldots, |\alpha_m|$ are multiplicatively independent, and $\{a_n\}$ is the sequence of Fibonacci numbers, then the numbers

$$f(\alpha_\ell, 1) = \sum_{n=0}^{\infty} a_n \alpha_\ell^n, \ \ell = 1, 2, \ldots, m,$$

are linearly independent over the field $\mathbb{Q}$.

2.4. A conjecture.

The theorem of Lech-Mahler which is referred to above shows that the integer zeros of an exponential polynomial in one variable consist of a finite number of arithmetic progressions (where an isolated point is deemed to be an arithmetic progression with common difference 0). One might ask whether there should be an analogous result for exponential polynomials in several variables.

It seems likely to me that the following should be the case: If $v_0, v_1, \ldots, v_m$ are elements of $\mathbb{Q}^n$ such that $v_1 - v_0, v_2 - v_0, \ldots, v_m - v_0$ are linearly independent over $\mathbb{Q}$ then define a $(m$-dimensional) $\mathbb{Z}$-manifold to be a set of the shape $\{n_0 v_0 + \ldots + n_m v_m : n_0, \ldots, n_m \in \mathbb{Z}, n_0 + \ldots + n_m = 1\}$. I then conjecture that:

The zeros in $\mathbb{Z}^n$ of an exponential polynomial in $n$ variables are the disjoint union of finitely many $\mathbb{Z}$-manifolds in $\mathbb{Q}^n$.

The only supporting evidence is that this is the case for $n = 1$ and that the general case can be reduced to finitely many cases not much more general than the situation briefly discussed in 2.3.

REFERENCES


(Texte reçu le 20 janvier 1975)

Alfred J. VAN DER POORTEN
School of Mathematics
The University of New South Wales
KENSINGTON (Sydney), NSW 2031
(Australie)