A NOTE ON HILBERT'S TENTH PROBLEM

Z.A. Melzak

(received August 10, 1959)

1. The tenth problem on Hilbert's well known list [1] is the following.

(H 10) For an arbitrary polynomial $P = P(x_1, x_2, \ldots, x_n)$ with integer coefficients to determine whether or not the equation $P = 0$ has a solution in integers.

By 'integers' we always mean 'rational integers'. The problem (H 10) is still unsolved but it appears likely that no decision procedure exists; in this connection see [2]. It will be shown here that (H 10) is equivalent to deciding whether or not every member of a certain given countable set of rational functions of a single variable x is absolutely monotonic. We recall that $f(x)$ is absolutely monotonic in I if $f(x)$ possesses non-negative derivatives of all orders at every $x \epsilon I$.

2. We show first that in (H 10) it suffices to be able to determine the existence (or non-existence) of solutions in positive integers. First, following Davis [2], this is shown for non-negative integers. The reduction to non-negative integers is a direct consequence of two observations.

1) $P(x_1, x_2, \ldots, x_n) = 0$ has a solution in integers if and only if one of the 2^n equations $P(\pm x_1, \pm x_2, \ldots, \pm x_n) = 0$ has a solution in non-negative integers;

2) $P(x_1, x_2, \ldots, x_n) = 0$ has a solution in non-negative integers if and only if

$$P(p_1^2 + q_1^2 + r_1^2 + s_1^2,\ p_2^2 + q_2^2 + r_2^2 + s_2^2, \ldots,\ p_n^2 + q_n^2 + r_n^2 + s_n^2) = 0$$

has a solution in integers. Finally, $P(x_1, x_2, \ldots, x_n) = 0$ has a solution in positive integers if and only if

$$P(x_1 + 1, x_2 + 1, \ldots, x_n + 1) = 0$$

has a solution in non-negative integers.

https://doi.org/10.4153/CMB-1960-019-9 Published online by Cambridge University Press

3. In this section we collect a few necessary lemmas.

LEMMA 1. Let $k_1, k_2, \ldots, k_n$ be any n non-negative integers. Then there exist positive integers $N, a_1, a_2, \ldots, a_n$, such that the only solution of

$$(1) \qquad \sum_{j=1}^{n} a_j x_j = N$$

in non-negative integers is $x_j = k_j$, $(j = 1, 2, \ldots, n)$.

Proof. Let $K = \max(k_1, k_2, \ldots, k_n)$ and let $p_1, p_2, \ldots, p_n$ be n primes, such that $K < p_1 < p_2 < \cdots < p_n$. Let

$$(2) \qquad P = \prod_{j=1}^{n} p_j, \quad P_j = P/p_j.$$

Take $a_j = P_j$, $(j = 1, 2, \ldots, n)$ in (1) and let $N = \sum_{j=1}^{n} P_j k_j$. Now consider the equation

$$(3) \qquad \sum_{j=1}^{n} P_j(x_j - k_j) = 0.$$

Suppose, if possible, that $x_j = b_j$ $(j = 1, 2, \ldots, n)$ is a solution of (3) in non-negative integers and with $b_j \neq k_j$ for some index j. Then $b_i < k_i$ for some i. By (2) we have

$$p_i = \text{g.c.d.}(P_1, P_2, \ldots, P_{i-1}, P_{i+1}, \ldots, P_n)$$

and therefore $p_i \mid |b_i - k_i|$. Since $0 \leq b_i < k_i < p_i$, we have a contradiction and the lemma is proved.

LEMMA 2. Let

$$(4) \qquad \sum_{m=0}^{\infty} (m+1)^n x^m = A_n(x)/(1-x)^{n+1}.$$

Then $A_0(x) = 1$,

$$(5) \qquad A_{n+1}(x) = x(1-x) A_n'(x) + (nx+1)A_n(x),$$

and, for $n \geq 1$, $A_n(x)$ is a polynomial of degree $n - 1$ with positive integer coefficients.

Proof. $A_0(x) = 1$ by direct verification. Multiplying both sides of (4) by x, differentiating and simplifying yields (5). The rest follows by an easy induction on n in (5).

Let $P(u_1, u_2, \ldots, u_n)$ be a polynomial. In the next lemma it is assumed that every variable u_j occurs in every term of P. For instance, $u_1^2 - u_1u_2u_3 + 3u_2u_3^3$ would be written as

https://doi.org/10.4153/CMB-1960-019-9 Published online by Cambridge University Press

$u_1^2u_2^0u_3^0 - u_1u_2u_3 + 3\, u_1^0u_2u_3^3$.

LEMMA 3. Let

$$P(u_1, u_2, \ldots, u_n) = \sum_{i_1, i_2, \ldots, i_n} a_{i_1 i_2 \ldots i_n} u_1^{i_1} u_2^{i_2} \ldots u_n^{i_n}$$

be any polynomial and put

$$F_P(x_1, x_2, \ldots, x_n)$$
$$= \sum_{i_1, i_2, \ldots, i_n} a_{i_1 i_2 \ldots i_n} \left\{ \prod_{r=1}^{n} A_{i_r}(x_r)/(1-x_r)^{i_r+1} \right\} .$$

Then F_P is a rational function of $x_1, x_2, \ldots, x_n$ with the power series expansion

$$(6) \sum_{m_1=0}^{\infty} \sum_{m_2=0}^{\infty} \cdots \sum_{m_n=0}^{\infty} P(m_1+1, m_2+1, \ldots, m_n+1) \times x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n} ,$$

valid for $|x_1| < 1$, $|x_2| < 1, \ldots,$ $|x_n| < 1$.

Proof. This follows at once from Lemma 2 by simple summation.

4. Given a polynomial $Q = Q(u_1, u_2, \ldots u_n)$ we shall say that the set of rational functions

$$\{F_Q(t^{a_1}, t^{a_2}, \ldots, t^{a_n})\}$$

is associated with Q. Here the exponents $a_1, a_2, \ldots, a_n$ range independently over positive integers.

THEOREM 1. Let $P(u_1, u_2, \ldots, u_n)$ be a polynomial with integer coefficients. The equation

$$(7) \qquad P(u_1, u_2, \ldots, u_n) = 0$$

has no solution in positive integers if and only if every function in the set

$$(8) \qquad \{F_{P^2-1}(t^{a_1}, t^{a_2}, \ldots, t^{a_n})\},$$

associated with the polynomial $P^2 - 1$, is absolutely monotonic over some interval $(0, \varepsilon)$, $\varepsilon > 0$.

Proof. It must be emphasized that the intervals of absolute monotoneity are not required to coincide. Suppose now that (7) does have a solution in positive integers:

https://doi.org/10.4153/CMB-1960-019-9 Published online by Cambridge University Press

$$P(k_1 + 1, k_2 + 1, \ldots, k_n + 1) = 0, \; k_j \geq 0, \; j = 1, 2, \ldots, n.$$

Then the power series of the form (6) with P replaced by $P^2 - 1$ has at least one coefficient equal to -1. Let $a_1, a_2, \ldots, a_n$ be a set of n positive integers. Then

$$F_{P^2-1}(t^{a_1}, t^{a_2}, \ldots, t^{a_n})$$
$$= \sum_{m_1=0}^{\infty} \sum_{m_2=0}^{\infty} \cdots \sum_{m_n=0}^{\infty} \{P^2(m_1+1, m_2+1, \ldots, m_n+1) - 1\} \times t^{a_1 m_1 + a_2 m_2 + \ldots + a_n m_n}$$
$$= \sum_{N=0}^{\infty} S(N) t^N ,$$

where

$$S(N) = \sum \{P^2(m_1 + 1, m_2 + 1, \ldots, m_n + 1) - 1\}$$

and the summation extends over all non-negative values $m_1, m_2, \ldots, m_n$ such that $\sum_{j=1}^{n} a_j m_j = N$. From lemma 1 we conclude that for some set $a_1, a_2, \ldots, a_n$ the rational function $F_{P^2-1}(t^{a_1}, t^{a_2}, \ldots, t^{a_n})$ has a negative coefficient in its power series. In fact, putting $N = \sum_{j=1}^{n} a_j k_j$, we see that the coefficient of t^N is -1. Therefore this function cannot be absolutely monotonic over any interval $(0, \varepsilon)$, $\varepsilon > 0$.

Suppose now that (7) has no solutions in positive integers. Then in the power series (6) for $P^2 - 1$ in place of P every coefficient is non-negative. The same is clearly true for the power series of any function $F(t)$ of the set associated with $P^2 - 1$. However, any rational function $F(t)$ regular at $t = 0$ and with non-negative power series coefficients, is absolutely monotonic over some interval $(0, \varepsilon)$, $\varepsilon > 0$. We can simply take ε to be the radius of convergence of the Taylor series of $F(t)$ at $t = 0$.

REFERENCES

1. D. Hilbert, Mathematical problems, Bull. Amer. Math. Soc. 8 (1901), 437-479.

2. M. Davis, Computability and Unsolvability, (New York, 1958).

McGill University

https://doi.org/10.4153/CMB-1960-019-9 Published online by Cambridge University Press