PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 96, Number 2, February 1986

A COMPLETENESS THEOREM FOR TRIGONOMETRIC IDENTITIES AND VARIOUS RESULTS ON EXPONENTIAL FUNCTIONS

LOU VAN DEN DRIES[1]

ABSTRACT. All valid identities in terms of variables, real constants, the arithmetic operations of addition and multiplication, and the trigonometric operations of sine and cosine are shown to be consequences of a few familiar identities and numerical facts. We also indicate how to decide whether f eventually dominates g, for f and g from a certain class of exponential functions. Finally, we correct a statement from an earlier paper.

Introduction. Consider the familiar identities:
(1) $\cos(x+y) = \cos x \cdot \cos y - \sin x \cdot \sin y$,
(2) $\sin(x+y) = \cos x \cdot \sin y + \sin x \cdot \cos y$,
(3) $\cos(-x) = \cos x$, $\sin(-x) = -\sin x$.

From these identities and numerical facts like $\cos 0 = 1$ we can derive other identities like $\cos^2 x + \sin^2 x = 1$. The question came up (cf. [**HR**, p. 31]) whether all valid identities formulated in terms of variables, individual real numbers, the functions cos and sin, and the ring operations $+$, $-$, $\cdot$ can be derived from the identities (1)–(3) above, plus the identities defining commutative rings with unit 1, plus the "true numerical facts", these being the valid identities not containing variables. (We allow terms like $\sin(\cos x)$.)

In §1 we shall answer this question affirmatively.[2]

In [**L**, p. 219] H. Levitz asked whether "eventual dominance" for a certain class of exponential functions could be effectively decided. We now indicate a larger class of exponential functions for which we found a decision method. To describe this class of functions let us define a *Skolem monomial* to be a formal product

$$M = P_0 \cdot P_1^{Q_1} \cdot \cdots \cdot P_k^{Q_k},$$

where $P_0, P_1, \ldots, P_k$ are rational functions in X over $\mathbf{Q}$, such that $P_1(x), \ldots, P_k(x)$ are > 0 for all sufficiently large real x, and $Q_1, \ldots, Q_k$ are polynomials in X over $\mathbf{Q}$. (So $M(x)$ is a well-defined real number for sufficiently large x.)

If $M_1, \ldots, M_s$ are Skolem monomials, then either $M_1(x) + \cdots + M_s(x) > 0$ for all sufficiently large x, or $M_1(x) + \cdots + M_s(x) = 0$ for all sufficiently large x, or $M_1(x) + \cdots + M_s(x) < 0$ for all sufficiently large x.

This fact follows from the main theorem in Hardy's book [**H**], but the proof there does not lead to a decision procedure.

Received by the editors January 21, 1985.
1980 *Mathematics Subject Classification*. Primary 03B25, 03D40, 26A09, 26A12; Secondary 03C05, 08A50, 08B05.
[1]Supported by the NSF.

[2]In a discussion with W. Henson we found that the addition law for the cosine and the symmetry law for the cosine ($\cos(-x) = \cos x$) are derivable from the other identities, but that one cannot also leave out $\sin(-x) = -\sin x$, as was inadvertently done in [**HR**, Corollary 5.3].

In §2 we show how to decide for any given Skolem monomials $M_1, \dots, M_s$ which of the three alternatives holds. The proof depends on unique factorization and the fact that e is transcendental.

In §3 we point out a false statement in the author's article [**VdD**], and substitute a correct statement. I thank E. Bouscaren for casting doubt on the statement in [**VdD**].

1. A completeness theorem for trigonometric identities.

(1.1) Let $L = \{0, 1, +, -, \cdot\}$ be the usual language of rings with unit 1 and $L_{\mathbf{R}} = L$ augmented by a constant symbol (name) for each real number. Further let c and s be two extra 1-place function symbols and define $\mathrm{Tr}(\mathbf{R})$ (for trigonometry over $\mathbf{R}$) to be the equational theory in the language $L_{\mathbf{R}} \cup \{c, s\}$ axiomatized by the following identities:

(1) the L-identities defining commutative rings with 1;

(2) the trigonometric identities: $c(x+y) = c(x)c(y) - s(x)s(y)$, $s(x+y) = c(x)s(y) + s(x)c(y)$, $c(-x) = c(x)$, $s(-x) = -s(x)$;

(3) the true numerical facts: all sentences $\tau = 0$ true in $\mathbf{R}$, where τ is an $L_{\mathbf{R}} \cup \{c, s\}$-term not containing variables; the symbols c and s are to be interpreted as cos and sin respectively.

(1.2) THEOREM. *Let $\tau(\overline{x})$, $\overline{x} = (x_1, \dots, x_n)$, be an $L_{\mathbf{R}} \cup \{c, s\}$-term such that $\tau(\overline{r}) = 0$ for each $\overline{r} = (r_1, \dots, r_n) \in \mathbf{R}^n$. Then* $\mathrm{Tr}(\mathbf{R}) \vdash \forall \overline{x}(\tau(\overline{x}) = 0)$.

(1.3) The proof is somewhat indirect, and we first derive a completeness result for identities which may also involve the exponential function $\exp(x) = e^x$.

So let e be a new 1-place function symbol and define $T_{(e,c,s)}$ as the equational theory in the language $L_{(e,c,s)} = L \cup \{1/2, e, c, s\}$ axiomatized by:

(a) the identities for commutative rings with 1, plus the identity $\frac{1}{2} + \frac{1}{2} = 1$,

(b) $e(x+y) = e(x) \cdot e(y)$, $e(0) = 1$,

(c) the trigonometric identities as in (2) above,

(d) all sentences $\tau = 0$ which are true on $\mathbf{R}$, where τ is an $L_{(e,c,s)}$-term not containing variables. (Here e, c, s are interpreted as exp, cos and sin on $\mathbf{R}$.)

(1.4) THEOREM. *Let $\tau(\overline{x})$, $\overline{x} = (x_1, \dots, x_n)$, be an $L_{(e,c,s)}$-term such that $\tau(\overline{r}) = 0$ for all $\overline{r} = (r_1, \dots, r_n) \in \mathbf{R}^n$. Then*

$$T_{(e,c,s)} \vdash \forall \overline{x}(\tau(\overline{x}) = 0).$$

(1.5) First we have a simple lemma. Let i be a new constant symbol and define *Euler* as the equational $L_{e,c,s}(i)$-theory axiomatized by Euler's identities

$$c(x) = (1/2) \cdot (e(ix) + e(-ix)), \qquad s(x) = (-1/2)i \cdot (e(ix) - e(-ix)).$$

These identities can be used to eliminate the symbols c and s at the expense of introducing the new symbol i, in other words, we have

(1.6) LEMMA. *For each $L_{(e,c,s)}$-term $\tau(\overline{x})$, $\overline{x} = (x_1, \dots, x_n)$, there is an $L \cup \{1/2, i, e\}$-term $\tau_e(\overline{x})$ such that Euler $\vdash \tau(\overline{x}) = \tau_e(\overline{x})$.*

(1.7) PROOF OF THEOREM (1.4). By model theory it suffices to show that, given any model $\underline{R}$ of $T_{(e,c,s)}$, we have $\underline{R} \models \forall \overline{x}(\tau(\overline{x}) = 0)$. Let A be the smallest subset of $\mathbf{R}$ containing 0, 1/2, 1 and closed under $+$, $-$, $\cdot$, exp, cos and sin. Clearly

A is the underlying set of a $T_{(e,c,s)}$-model $\underline{A}$. Let $\Phi\colon \underline{A} \to \underline{R}$ be the unique $L_{(e,c,s)}$-morphism. We consider $\underline{R}$ as an $\underline{A}$-algebra via Φ. The subring $\underline{A}[i] = \underline{A} + \underline{A} \cdot i$ of $\mathbf{C}$ is also closed under exp, cos and sin, since $\exp(a+bi) = \exp a \cdot (\cos b + i \sin b)$.

Consider now the $\underline{A}[i]$-algebra $\underline{R} \otimes_{\underline{A}} \underline{A}[i]$. The usual identifications give that $\underline{R} \otimes_{\underline{A}} \underline{A}[i] = \underline{R}[i]$, and $\underline{R}[i]$ is a free $\underline{R}$-module on the basis $1, i$. This allows us to extend the operations e, c, s on $\underline{R}$ to $\underline{R}[i]$: put $e(\lambda + \mu i) = e(\lambda) \cdot (c(\mu) + i \cdot s(\mu))$ for $\lambda, \mu \in \underline{R}$. It is easy to verify that the operation e on $\underline{R}[i]$ extends the operation e on $\underline{R}$ and is a morphism of the additive group of $\underline{R}[i]$ into the multiplicative group of units of $\underline{R}[i]$. We also put, for $z \in \underline{R}[i]$:

$$c(z) = (1/2) \cdot (e(iz) + e(-iz)), \qquad s(z) = (-1/2)i \cdot (e(iz) - e(-iz)),$$

and again c and s on $\underline{R}[i]$ extend c and s on $\underline{R}$. It is clear that the structural morphism $\underline{A}[i] \to \underline{R}[i]$ is also a morphism for the e-operation. From the assumption that $\tau(\overline{r}) = 0$ for all $\overline{r} \in \mathbf{R}^n$ we get by analytic continuation that $\tau(\overline{r}) = 0$ for all $\overline{r} \in \mathbf{C}^n$. Let $\tau_e(\overline{x})$ be an $L \cup \{1/2, i, e\}$-term such that $Euler \vdash \tau(\overline{x}) = \tau_e(\overline{x})$. (Such a term exists by the lemma.) Hence $\underline{A}[i] \models \forall \overline{x}(\tau_e(\overline{x}) = 0)$, and since the E-ring $\underline{A}[i]$ satisfies the hypotheses of [**VdD**, Proposition (4.1)] (with $r = 1$, $d_i = \partial/\partial x_i$), we get that $\forall \overline{x}(\tau_e(\overline{x}) = 0)$ is also true for every E-ring S for which there exists an E-ring morphism $\underline{A}[i] \to S$ (where $1/2, i$ are to be interpreted by their image in S under this morphism). In particular the sentence is true in $S = \underline{R}[i]$, and since $\underline{R}[i] \models Euler$, we get $\underline{R}[i] \models \forall \overline{x}(\tau(\overline{x}) = 0)$, hence $\underline{R} \models \forall \overline{x}(\tau(\overline{x}) = 0)$.

(1.8) For the proof of Theorem (1.2) we need the following relativization of (1.4). Let $L_{(e,c,s)}(\mathbf{R})$ be the language $L_{(e,c,s)}$ augmented by a constant symbol for each real number, and let $T_{(e,c,s)}(\mathbf{R})$ be the equational $L_{(e,c,s)}(\mathbf{R})$-theory which has the same axioms as $T_{(e,c,s)}$ except that in clause (d) we allow $L_{(e,c,s)}(\mathbf{R})$-terms (see (1.3)).

We now have the following result which is proved in the same way as Theorem (1.4).

Let $\tau(\overline{x})$, $\overline{x} = (x_1, \ldots, x_n)$, be an $L_{(e,c,s)}(\mathbf{R})$-term such that $\tau(\overline{r}) = 0$ for all $\overline{r} \in \mathbf{R}^n$. Then $T_{(e,c,s)}(\mathbf{R}) \vdash \forall \overline{x}(\tau(\overline{x}) = 0)$.

(1.9) We can now prove our trigonometric completeness result.

PROOF OF THEOREM (1.2). By model theory it suffices to show that, given any model R of $\mathrm{Tr}(\mathbf{R})$, we have $R \models \forall \overline{x}(\tau(\overline{x}) = 0)$. We may of course assume $R \neq \{0\}$. We have a canonical $L_{\mathbf{R}} \cup \{c, s\}$-morphism $\Phi\colon \mathbf{R} \to R$. Since $\mathbf{R}$ is a field and $R \neq \{0\}$, Φ is injective and $\Phi(\mathbf{R})$ is a direct summand of the $\mathbf{R}$-linear space R, say $R = \Phi(\mathbf{R}) \oplus B$. We equip R with an operation e by putting $e(\Phi(r) + b) = \Phi(\exp(r))$ $(r \in \mathbf{R}, b \in B)$. It is easy to see that then (R, e) is an E-ring and that Φ is also an E-ring morphism $(\mathbf{R}, \exp) \to (R, e)$. In other words: $(R, e) \models T_{(e,c,s)}(\mathbf{R})$ (see (1.8)), whence $(R, e) \models \forall \overline{x}(\tau(\overline{x}) = 0)$. But the symbol e does not occur in τ, therefore $R \models \forall \overline{x}(\tau(\overline{x}) = 0)$. $\square$

(1.10) Negative results on identity problems for elementary functions can be found in [**R1**].

2. A decision method for eventual dominance.

(2.1) In this section we solve a slightly generalized form of a decision problem posed by H. Levitz (see the Introduction). Another solution of Levitz's problem was found by R. Gurevic [**G**].

As is common in dealing with effectivity notions we abuse language to avoid unwieldy formulations. For instance, we assume tacitly that rings like $\mathbf{Q}$ and $\mathbf{Q}[X]$ are recursively presented. To give a concrete example, the precise formulation of Lemma (2.2) below is as follows:

There is an algorithm which, for any polynomials $f(X),\ g(X) \in \mathbf{Q}[X]$ *with* $g(X) \neq 0$, *computes a triple* $(a, i, e) \in \mathbf{Q} \times \mathbf{Z} \times \mathbf{N}$ *such that*

$$f(X)/g(X) = aX^i \cdot (1 + a_1X^{-1} + a_2X^{-2} + \cdots)$$

in the formal power series field $\mathbf{Q}((X^{-1}))$, *where* $a_1, a_2, a_3, \ldots$ *is a recursive sequence of rationals with index* e.

In the sequel we shall leave the translation of our statements into such pedantically precise language to the reader.

(2.2) LEMMA. *Given a rational function* $P(X) \in \mathbf{Q}(X)$ *one can compute a rational number* a, *an integer* i, *and a sequence of rationals* $a_1, a_2, a_3, \ldots$, *such that*

$$P(X) = aX^i \cdot (1 + a_1X^{-1} + a_2X^{-2} + \cdots).$$

PROOF. If P is a polynomial $a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ with $a_n \neq 0$, then

$$P = a_nX^n \cdot \left(1 + \frac{a_{n-1}}{a_n}X^{-1} + \cdots + \frac{a_0}{a_n}X^{-n} + 0\right);$$

also

$$\frac{1}{P} = a_n^{-1}X^{-n} \cdot \left(1 - \left(\frac{a_{n-1}}{a_n}X^{-1} + \cdots + \frac{a_0}{a_n}X^{-n}\right) + (\cdots)^2 \cdots\right),$$

and one computes easily successive rationals $b_1, b_2, b_3, \ldots$ such that this can be written as

$$a_n^{-1}X^{-n} \cdot (1 + b_1X^{-1} + b_2X^{-2} + \cdots).$$

The case of a quotient of polynomials can be reduced to the above cases and multiplication of power series in X^{-1} with given rational coefficients.

(2.3) LEMMA. *Given* (*the index of*) *a recursive sequence of rationals* $a_1, a_2, a_3, \ldots$ *one can compute a sequence of rationals* $b_1, b_2, b_3, \ldots$ *such that*

$$\log(1 + a_1X^{-1} + a_2X^{-2} + \cdots) = b_1X^{-1} + b_2X^{-2} + b_3X^{-3} + \cdots.$$

PROOF. The formal power series $\log(1+Y)$ is defined by: $\log(1+Y) = Y - Y^2/2 + Y^3/3 - \cdots$, and the result follows by substitution. □

(2.4) In the next lemmas we use expressions $E(X)$ containing the indeterminate X such that $E(x)$ is a well-defined real number for all sufficiently large x. Such an expression stands for the germ at ∞ of the real function it defines. So an identity $E_1(X) = E_2(X)$ means that $E_1(x) = E_2(x)$ for all $x > r$, for some $r \in \mathbf{R}$ such that $E_1(x)$ and $E_2(x)$ are defined for $x > r$.

For $P(X) \in \mathbf{Q}(X)$ we write $P(X) > 0$ if $P(x) > 0$ for all sufficiently large x. So $P(X) > 0$ if and only if $a > 0$, where a is as in Lemma (2.2).

Finally, we let $p_1 = 2, p_2 = 3, \ldots, p_n, \ldots$ be the successive prime numbers.

(2.5) LEMMA. *Given* $P(X) \in \mathbf{Q}(X)$ *and* $Q(X) \in \mathbf{Q}[X]$, *with* $P(X) > 0$, *one can compute a positive integer* n *and polynomials* $q(X), q_1(X), \ldots, q_n(X), q_\infty(X) \in \mathbf{Q}[X]$, *and a sequence of rationals* $c_1, c_2, c_3, \ldots$, *such that*

$$P(X)^{Q(X)} = e^{q(X)} \cdot 2^{q_1(X)} \cdot \ldots \cdot p_n^{q_n(X)} \cdot X^{q_\infty(X)} \cdot (1 + c_1X^{-1} + c_2X^{-2} + \cdots).$$

PROOF. Write $P(X) = aX^i \cdot (1 + a_1X^{-1} + a_2X^{-2} + \cdots)$ as in (2.2). Then

$$\begin{aligned} P(X)^{Q(X)} &= e^{Q(X)\cdot \log P(X)} \\ &= e^{Q(X)\cdot[\log a + i \log X + \log(1+a_1X^{-1}+\cdots)]} \quad \text{(using (2.3))} \\ &= e^{Q(X)\cdot(\log a + i\log X) + Q(X)\cdot[b_1X^{-1}+b_2X^{-2}+\cdots]} \\ &= e^{q(X)+q_l(X)\log a + q_\infty(X)\log X} \cdot e^{d_1X^{-1}+d_2X^{-2}+\cdots}, \end{aligned}$$

where $q(X), q_l(X), q_\infty(X) \in \mathbf{Q}[X]$, and the sequence of rationals $d_1, d_2, d_3, \ldots$ can be computed from $Q(X)$, i, and the sequence $b_1, b_2, b_3, \ldots$.

Now factor a as $a = 2^{k_1} \cdot 3^{k_2} \cdot \cdots \cdot p_n^{k_n}$ ($k_i \in \mathbf{Z}$), so we obtain $q_l(X)\log a = q_1(X)\log 2 + q_2(X)\log 3 + \cdots + q_n(X)\log p_n$ for polynomials $q_1, \ldots, q_n \in \mathbf{Q}[X]$. Furthermore, substituting $d_1X^{-1} + d_2X^{-2} + \cdots$ in the power series $e^Y = 1 + Y + Y^2/2! + \cdots$, we can compute rationals $c_1, c_2, c_3, \ldots$, such that

$$e^{d_1X^{-1}+d_2X^{-1}+\cdots} = 1 + c_1X^{-1} + c_2X^{-2} + \cdots.$$

The result is

$$P(X)^{Q(X)} = e^{q(X)} \cdot 2^{q_1(X)} \cdot \cdots \cdot p_n^{q_n(X)} \cdot X^{q_\infty(X)} \cdot (1 + c_1X^{-1} + c_2X^{-1} + \cdots). \quad \square$$

(2.6) LEMMA. *Given $P_1(X) > 0, \ldots, P_k(X) > 0$ in $\mathbf{Q}(X)$ and polynomials $Q_1(X), \ldots, Q_k(X) \in \mathbf{Q}[X]$ one can compute a positive integer n, polynomials $q(X), q_1(X), \ldots, q_n(X), q_\infty(X) \in \mathbf{Q}[X]$, and a sequence of rationals $c_1, c_2, c_3, \ldots$, such that*

$$\begin{aligned} &P_1(X)^{Q_1(X)} \cdot P_2(X)^{Q_2(X)} \cdot \cdots \cdot P_k(X)^{Q_k(X)} \\ &\quad = e^{q(X)} \cdot 2^{q_1(X)} \cdot 3^{q_2(X)} \cdot \cdots \cdot p_n^{q_n(X)} \cdot X^{q_\infty(X)} \cdot (1 + c_1X^{-1} + c_2X^{-2} + \cdots). \end{aligned}$$

PROOF. The proof is immediate from Lemma (2.5). Note that one can take the same n for all powers $P_i(X)^{Q_i(X)}$ by letting some exponents be equal to zero, if necessary. $\square$

(2.7) LEMMA. *If $r, r_1, \ldots, r_n \in \mathbf{Q}$, then $r + r_1\log 2 + r_2\log 3 + \cdots + r_n \log p_n = 0$ if and only if $r = r_1 = \cdots = r_n = 0$. For given $r, r_1, \ldots, r_n \in \mathbf{Q}$ one can determine effectively which of the three statements*

$$r + r_1\log 2 + \cdots + r_n \log p_n \begin{cases} = 0, \\ > 0, \\ < 0 \end{cases}$$

holds.

PROOF. We may assume the r_i are integers. Then $r + r_1\log 2 + \cdots + r_n\log p_n = 0 \Leftrightarrow e^r = 2^{-r_1} \cdot \cdots \cdot p_n^{-r_n}$. Since e is transcendental, this can only happen when $r = 0$, which, by unique factorization, implies $r_1 = \cdots = r_n = 0$. The second statement follows from the first and from the fact that we can compute rational approximations to $\log p$ for p a given positive integer. $\square$

(2.8) In the following we consider tuples $\sigma = (q, q_1, \ldots, q_n, q_\infty)$ ($n \geq 0$) with each term in $X \cdot \mathbf{Q}[X]$, i.e., q, q_i ($1 \leq i \leq n$) and q_∞ are polynomials in X over $\mathbf{Q}$ with constant term 0.

To such a tuple σ we associate the formal product $F_\sigma = e^q \cdot 2^{q_1} \cdot \cdots \cdot p_n^{q_n} \cdot X^{q_\infty}$.

Note that, given any two tuples σ_1 and σ_2, one can determine a tuple τ such that $F_{\sigma_1}(x)/F_{\sigma_2}(x) = F_\tau(x)$ for all $x > 0$; by inserting dummy zeros if necessary we may assume that σ_1 and σ_2 are of the same length and then one obtains τ by $\tau = \sigma_1 - \sigma_2$.

(2.9) LEMMA. *For any tuple $\sigma \neq (0,0,\dots,0)$ there is a constant $c > 0$ such that either $F_\sigma(x) < e^{-cx}$ for all sufficiently large x, or $F_\sigma(x) > e^{cx}$ for all sufficiently large x.*

For any given tuple $\sigma \neq (0,0,\dots,0)$ one can determine effectively which of the two cases takes place.

PROOF. Let $\sigma = (q, q_1, \dots, q_n, q_\infty)$, and let k be the maximum of the degrees of the terms of σ. Then we can write

$$F_\sigma = \exp\left(\sum_{i=1}^{k} X^i(r_i + r_{i_1}\log 2 + \cdots + r_{i_n}\log p_n + r_{i_\infty}\log X)\right).$$

Here the r_i, r_{i_j} and r_{i_∞} are rational numbers which we can compute from σ. By definition of k one of the numbers $r_k, r_{k_j}, r_{k_\infty}$ is not zero. If $r_{k_\infty} < 0$, then $F_\sigma(x) < e^{-cx}$ for some $c > 0$ and all sufficiently large x.

Suppose $r_{k_\infty} = 0$. By Lemma (2.7) either $r_k + r_{k_1}\log 2 + \cdots + r_{k_n}\log p_n < 0$ or $r_k + r_{k_1}\log 2 + \cdots + r_{k_n}\log p_n > 0$. In the first case we have again $F_\sigma(x) < e^{-cx}$ for some $c > 0$ and all sufficiently large x, and in the second case $F_\sigma(x) > e^{cx}$ for some $c > 0$ and all sufficiently large x. □

(2.10) LEMMA. *Given $P_0(X) \in \mathbf{Q}(X)$, $P_1(X) > 0, \dots, P_k(X) > 0$ in $\mathbf{Q}(X)$ and polynomials $Q_1(X), \dots, Q_k(X) \in \mathbf{Q}[X]$ we can effectively determine a tuple σ, positive integers m and M, a rational number r, and a sequence of algebraic real numbers $d_{-m}, d_{-m+1}, \dots, d_0, d_1, d_2, \dots$ such that, with $f_i = d_i \cdot e^r$, we have*

$$\begin{aligned} &P_0 \cdot P_1^{Q_1} \cdot \dots \cdot P_k^{Q_k} \\ &\quad = F_\sigma \cdot \left(f_{-m}X^{m/M} + f_{-m+1}X^{(m-1)/M} + \cdots + f_0 + f_1X^{-1/M} + \cdots\right). \end{aligned}$$

PROOF. The case $P_0 = 0$ being trivial, we may assume without loss of generality that $P_0 > 0$. Using Lemmas (2.2) and (2.6) we can write

$$P_0 \cdot P_1^{Q_1} \cdot \dots \cdot P_k^{Q_k} = F_\sigma \cdot (e^r \cdot 2^{r_1} \cdot \dots \cdot p_n^{r_n} \cdot X^{r_\infty}) \cdot (1 + c_1X^{-1} + \cdots)$$

for some tuple σ and rational numbers $r_0, r_1, \dots, r_n, r_\infty$, and a sequence of rationals $c_1, c_2, \dots$.

The last two factors on the right-hand side can be contracted in an obvious way to a fractional power series of the desired form. □

We can now prove the result stated in the Introduction.

(2.11) THEOREM. *Given any Skolem monomials $M_1, \dots, M_s$ one can determine effectively whether $M_1 + \cdots + M_s > 0$, or $M_1 + \cdots + M_s = 0$, or $M_1 + \cdots + M_s < 0$.*

PROOF. Write each M_i as

$$M_i = F_{\sigma(i)} \cdot (f_{-mi}X^{m/M} + F_{(-m+1)i}X^{(m-1)/M} + \cdots),$$

according to the previous lemma. We can do this in such a way that all tuples $\sigma(i)$ are of the same length and the numbers m, M are also independent of i. Using (2.8) and (2.9) we may also assume that, for some $t \in \{1, \dots, s\}$, we have

$\sigma(1) = \cdots = \sigma(t) = \sigma$, and $F_{\sigma(i)}(x)/F_\sigma(x) < e^{-cx}$ for $i = t+1, \ldots, s$, a constant $c > 0$, and all sufficiently large x.

This implies that $M_1 + \cdots + M_t$ dominates $M_{t+1} + \cdots + M_s$ in absolute value, provided $M_1 + \cdots + M_t \neq 0$. We can effectively verify whether or not $M_1 + \cdots + M_t = 0$ by [**R2** or **M**]. If $M_1 + \cdots + M_t = 0$ we have a reduction to a sum of fewer Skolem monomials.

Suppose that $M_1 + \cdots + M_t \neq 0$. Then we can effectively write

$$M_1 + \cdots + M_t = F_\sigma \cdot (g_{-m}X^{m/M} + g_{-m+1}X^{(m-1)/M} + \cdots + g_0 + g_1 X^{-1/M} + \cdots),$$

where each coefficient g_j is of the form $g_j = b_{ij}e^{r_{1j}} + \cdots + b_{tj}e^{r_{tj}}$, with the b_{ij} algebraic real numbers and the r_{ij} rational numbers.

Since e is transcendental we can find the first nonzero coefficient g_j and determine its sign. If the sign is 1, then $M_1 + \cdots + M_s > 0$, if the sign is -1, then $M_1 + \cdots + M_s < 0$. □

3. A correction.

(3.1) In this section we assume some familiarity with the author's article [**VdD**]. At the end of that paper I claim, without proof, two (equivalent, but false) statements, $(*)$ and $(**)$ (cf. [**VdD**, p. 65]).

Statement $(*)$ is as follows:

> "For each nonzero E-polynomial $p(X)$ over $(\mathbf{R}, e^x)$, all $a, b \in \mathbf{R}$ with $a < b$, and each ordered E-extension field F of $(\mathbf{R}, e^x)$ we have: all roots of $p(X)$ in F between a and b are in $\mathbf{R}$." (Here, and in the following, an ordered E-field F satisfies $E(x) \geq 1 + x$, in accordance with the convention of [**VdD**, p. 64].)

A counterexample to $(*)$ is implicit in [**DW**]: Take a positive infinitesimal α in some ordered field R extending $\mathbf{R}$. As in the proof of Corollary 27 in [**DW**] we see that $(1+\alpha/n)^n < 1 + \alpha + \alpha^2/2 < (1-\alpha/n)^n$ for all natural numbers n, and therefore, according to Theorem 26 of [**DW**] we have $E(\alpha) = 1 + \alpha + \alpha^2/2$ for a suitable ordered E-extension field F of $(\mathbf{R}, e^x)$. But $E(X) - (1 + X + X^2/2)$ is an example of an E-polynomial over $(\mathbf{R}, e^x)$ which has no real root strictly between 0 and 1, and we have a contradiction with $(*)$.

(3.2) The intention behind the (refuted) statement $(*)$ was to indicate *universal* axioms satisfied by $(\mathbf{R}, e^x)$ which, together with the axioms for E-fields and the diagram of $(\mathbf{R}, e^x)$, could prove every true instance of "$p(X)$ has exactly k zeros between a and b" ($p(X) \in \mathbf{R}[X]^E$, $k \in \mathbf{N}$, $a, b \in \mathbf{R}$). This intention can still be realized, but we need more than just the axiom $\forall x(E(x) \geq 1 + x)$.

Let us define a *nicely ordered E-field* to be an ordered E-field F such that

$$|E(x) - E_k(x)| \leq \frac{e^{|x|} \cdot |x|^{k+1}}{(k+1)!} \qquad \text{for all } x \in F,\ k \in \mathbf{N},$$

where $E_k(x) = \sum_{i=0}^{k} x^i/i!$.

Now we have the following result which comes in place of $(*)$.

(3.3) PROPOSITION. *Let F be a nicely ordered E-extension field of $(\mathbf{R}, e^x)$, and $p(X) \in \mathbf{R}[X]^E$, $p \neq 0$. Then each finite zero of $p(X)$ in F is in $\mathbf{R}$.*

PROOF. By induction on the complexity of $p(X)$ one shows first that for each $a \in \mathbf{R}$ and $k \in \mathbf{N}$ there is a positive real constant C such that

$$\left| p(a+x) - \sum_{i=0}^{k} \frac{p^{(i)}(a)}{i!} x^i \right| \leq C|x|^{k+1}$$

for all infinitesimals x in F.

Let $b \in F$ be a finite zero of $p(X)$ where $p \neq 0$. Then $b = a + x$ for some $a \in \mathbf{R}$ and infinitesimal x. Suppose now that $b \notin \mathbf{R}$. Then $x \neq 0$, and it will suffice to derive a contradiction from this. Since $p \neq 0$ we can take $k \in \mathbf{N}$ so large that the Taylor polynomial

$$f(X) = \sum_{i=0}^{k} \frac{p^{(i)}(a)}{i!} X^i$$

is nonzero. From $p(b) = 0$ it follows that $|f(x)| \leq C|x|^{k+1}$ for some positive real number c, and this contradicts $\deg f \leq k$. $\square$

REFERENCES

[**DW**] B. I. Dahn and H. Wolter, *On the theory of exponential fields*, Z. Math. Logik Grundlag. Math. **29** (1983), 465–480.

[**G**] R. Gurevic, *Transcendental numbers and eventual dominance of exponential functions*, preprint.

[**H**] G. H. Hardy, *Orders of infinity*, Cambridge Univ. Press, New York, 1910.

[**HR**] C. W. Henson and L. A. Rubel, *Some applications of Nevanlinna theory to mathematical logic: Identities of exponential functions*, Trans. Amer. Math. Soc. **282** (1984), 1–32.

[**L**] H. Levitz, *Calculation of an order type: An application of non-standard methods*, Z. Math. Logik Grundlag. Math. **28** (1982), 219–228.

[**M**] A. Macintyre, *The laws of exponentiation*, Model Theory and Arithmetic, Lecture Notes in Math., vol. 890, Springer-Verlag, Berlin and New York, 1981, pp. 185–197.

[**R1**] D. Richardson, *Some undecidable problems involving elementary functions of a real variable*, J. Symbolic Logic **33** (1968), 514–520.

[**R2**] ——, *Solution of the identity problem for integral exponential functions*, Z. Math. Logik Grundlag. Math. **15** (1969), 333–340.

[**VdD**] L. van den Dries, *Exponential rings, exponential polynomials and exponential functions*, Pacific J. Math. **113** (1984), 51–66.

DEPARTMENT OF MATHEMATICS, STANFORD UNIVERSITY, STANFORD, CALIFORNIA 94305

Current address: Max Planck Institute für Mathematik, Gottfried-Claren-Strasse 26, 5300 Bonn 3, Federal Republic of Germany