PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 94, Number 1, May 1985

EQUATIONAL THEORY OF POSITIVE NUMBERS WITH EXPONENTIATION

R. GUREVIČ

ABSTRACT. A. Tarski asked if all true identities involving 1, addition, multiplication, and exponentiation can be derived from certain so-called "high-school" identities (and a number of related questions). I prove that equational theory of $(\mathbf{N}, 1, +, \cdot, \uparrow)$ is decidable ($a \uparrow b$ means a^b for positive a, b) and that entailment relation in this theory is decidable (and present a similar result for inequalities). A. J. Wilkie found an identity not derivable from Tarski's axioms with a difficult proof-theoretic argument of nonderivability. I present a model of Tarski's axioms consisting of 59 elements in which Wilkie's identity fails.

1. This note is related to "Tarski's high school algebra problem" and a number of other model-theoretic questions concerning exponentiation of positive real numbers and positive integers (see e.g. [**1**]). Let $a \uparrow b = a^b$ for positive a, b, and $L =$ the set of terms in signature $(1, +, \cdot, \uparrow)$. As always, $\mathbf{R}^+$ is the set of positive reals. We give proofs of decidability for two problems about identities, and we also present a 59-element model in which Tarski's "high school algebra" identities are true, while Wilkie's identity is false.

Our first result gives a new proof of a theorem of A. Macintyre [**3**] (proved for terms in one variable by Richardson [**4**]).

THEOREM 1. *Let X be any subset of $\mathbf{R}_+$ containing* 1 *and closed under addition, multiplication, and exponentiation. Then the set of valid equalities $T = \{t_1 = t_2 \mid t_1, t_2 \in L, X \models t_1 = t_2\}$ is decidable and does not depend on X.*

The proof is based on the following lemma, which is proved in §§2 and 3.

LEMMA 1. *There is a recursive function M: $L \times L \to \mathbf{N}$ such that, for any $t_1(\vec{r}, s), t_2(\vec{r}, s) \in L$, for any positive real (values of) $\vec{r}$ if*

$$\operatorname{card}\{s \in \mathbf{R}_+ \mid t_1(\vec{r}, s) = t_2(\vec{r}, s)\} \geqslant M(t_1, t_2)$$

then $\forall s \in \mathbf{R}_+$: $t_1(\vec{r}, s) = t_2(\vec{r}, s)$.

PROOF OF THEOREM 1. Proceed by induction on the number of variables: $\forall s \in X$: $t_1(\vec{r}, s) = t_2(\vec{r}, s)$ is equivalent to $\&_{k=1}^{M} t_1(\vec{r}, k) = t_2(\vec{r}, k)$, where $M = M(t_1, t_2)$.

Received by the editors February 4, 1983 and, in revised form, April 2, 1984.

1980 *Mathematics Subject Classification*. Primary 03B25, 03C05, 03C13.

Key words and phrases. Exponentiation of positive reals, exponentiation of positive integers, Tarski's high school algebra problem, decidability of equational theory, decidability of entailment relation, differential ring, finite model of Tarski's axioms.

THEOREM 2. *Let S = the set of finite subsets of T. Then the set*

$$\{(s, t_1, t_2) \in S \times L \times L \mid 1^x = 1, x^1 = 1x = x1 = x, s \vdash t_1 = t_2\}$$

is decidable.

The proof follows immediately from the next lemma, which is proved in §4.

LEMMA 2. *There is a recursive function B: $L \times L \to \mathbf{N}$ such that, for any $t_1, t_2 \in L$ and any set s of valid equalities, we have $1^x = 1$, $x^1 = 1x = x1 = x$, $s \nvdash t_1 = t_2$ if and only if $\nvDash t_1 = t_2$ in a model of $1^x = 1$, $x^1 = 1x = x1 = x$, s of cardinality $\leqslant B(t_1, t_2)$.*

This research was provoked by **[5]**, which provided an axiom system adequate for equational theory of $(\mathbf{N}, 1, +, \cdot, \uparrow)$. The idea to bound the number of real solutions of some transcendental equations via chains of first order differential equations is due to A. G. Khovanski. I learned it from O. Viro, who partly reproduced for me talks given by A. G. Khovanski and V. I. Arnold; **[2]** is related to, but not used in, this paper.

2. A differential algebraic construction. Recall that $D[X]$ = the ring of polynomials in variables $\in X$ with coefficients in D, $D(X)$ = the field of rational functions in variables $\in X$ with coefficients in D for any commutative ring D without zero divisors, denote also $D[\varnothing] = D$, $D(\varnothing)$ = the field of quotients of D.

Let $\{X_n\}_n$ be disjoint sets and $K = \mathbf{Z}(\bigcup_n X_n)$. Let $\leqslant$ be a linear order on $\bigcup_n X_n$ such that $u \leqslant v$ for $u \in X_n$, $v \in X_{n+1}$. Define a relation $\triangleleft$ on K as follows. Let $t_1, t_2 \in K$, $t_2 \notin \mathbf{Q}$ and y be the last variable of t_2, $y \in X_n$. Put $t_1 \triangleleft t_2$ if all variables of t_1 are $\leqslant y$, each $x \in X_n$ occurring in t_1 occurs in t_2, and either

(1) $t_1 \in \mathbf{Z}(\{x \mid x < y\})[y] \not\ni t_2$,

(2) $t_1, t_2 \in \mathbf{Z}(\{x \mid x < y\})[y]$ and $\deg_y(t_1) < \deg_y(t_2)$, or

(3) $t_1 = p_m y^m + \cdots + p_0$, $t_2 = q_m y^m + \cdots + q_0$, with y not occurring in p_j's and q_j's and $p_m \triangleleft q_m$.

It is easy to see that $\triangleleft$ is well-founded.

Let a, b, c be functions $\bigcup_n X_n \to \mathbf{Z}[\bigcup_n X_n]$ such that $\forall x$: $a_x \neq 0$ (I will use a_x, b_x, c_x as alternatives for $a(x), b(x), c(x)$, respectively) and $a(X_n) \cup b(X_n) \cup c(X_n) \subseteq \mathbf{Z}[\bigcup_{k<n} X_k]$ for any n. (In particular, $a_x, b_x, c_x \triangleleft x$ for any x and $a(X_0) \cup b(X_0) \cup c(X_0) \subseteq \mathbf{Z}$.) Define a differentiation on K, putting $x' = b_x \cdot x/a_x + c_x/a_x$ for $x \in \bigcup_n X_n$.

PROPOSITION. *For any $t \in K - \mathbf{Q}$ there are $A_t, B_t, C_t \triangleleft t$, $A_t \neq 0$, such that $A_t \cdot t' = B_t \cdot t + C_t$. Moreover, let W be a subset of $\mathbf{Z}[\bigcup_n X_n]$ closed under multiplication, $1 \in W$, $W \cap \mathbf{Z}[\{x \mid x \leqslant y\}] \subseteq (W \cap \mathbf{Z}[\{x \mid x < y\}])[y]$ for any y, and $W \supseteq a(\bigcup_n X_n)$, and let $R = \{u/v \mid u \in \mathbf{Z}[\bigcup_n X_n], v \in W\} \subseteq K$. Then one can choose $A_t \in W$ and $B_t, C_t \in R$ for $t \in R$.*

PROOF. Let y be the last variable of t. Let $t \notin \mathbf{Z}(\{x \mid x < y\})[y]$, $t = P/Q$, where P, Q are polynomials, $\deg_y(Q) > 0$, and $Q \in W$ for $t \in R$. Then put $A_t = Q^2$, $B_t = 0$, $C_t = P' \cdot Q - P \cdot Q'$. For other cases, proceed by induction on $\triangleleft$. Let $t = py^n + Q$, $\deg_y(Q)$. If $p \notin \mathbf{Q}$ take A_p, B_p, C_p according to inductive assumption and put $A_t = A_p$, $B_t = B_p + nA_p b_y/a_y$, and $C_t = C_p y^n + (npA_p c_y/a_y)y^n + A_p \cdot Q' - (B_p + nA_p B_y/a_y)Q$. If $p \notin \mathbf{Q}$ put $A_p = 1$, $B_p = C_p = 0$ in the above formulae.

One can easily generalize this proposition by taking any commutative differential ring without zero divisors instead of $\mathbf{Z}$ to obtain

COROLLARY. *Let $F \supseteq F_0$ be differential fields. Put $F_{n+1} = \{f \in F \mid \exists a, b, c \in F_n: f' = bf/a + c/a\}$. Then $\bigcup_n F_n$ is a differential subfield of F. If F is a function field closed under superposition and F_0 is the field of constants, then $\bigcup_n F_n$ is also closed under superposition.*

O. Viro attributed this result for a function field F to A. G. Khovanski.

Neither the generalizations of the Proposition nor the Corollary will be used.

3. Proof of Lemma 1. I am going to apply the Proposition of §2, so I will introduce notation corresponding to that of §2 (except Corollary).

Put $W =$ the set of $(1, +, \cdot, \uparrow)$-terms in variables $\vec{r}, s$. Define h: $W \to \mathbf{N}$ as follows: $h(u) = 0$ if u is a polynomial with respect to s; for other cases

$$h(u+v) = h(uv) = \max(h(u), h(v)), h(u \uparrow v) = 1 + \max(h(v), 1 + h(u)).$$

Put $X_0 = \{s\} \cup \{(1, +, \cdot, \uparrow)\}$-terms in variables $\vec{r}$ and $X_n =$ the set of expressions of the forms $u \uparrow v$ and $\ln(w)$, where $u, v, w \in W$ and $h(u \uparrow v) = n = 1 + h(w)$ for $n \neq 0$. Terms $\in W$ will be regarded as elements of $\mathbf{Z}[\bigcup_n X_n]$. Compare the situation with that of §2: We have disjoint $\{X_n\}_n$, $W \subseteq \mathbf{Z}[\bigcup_n X_n]$ is closed under multiplication, and it is quite easy to fix a linear order $\leqslant$ on $\bigcup_n X_n$ such that $x \leqslant y$ whenever $x \in X_n$, $y \in X_{n+1}$ for some n, and $W \cap \mathbf{Z}[\{x \mid x \leqslant y\}] \subseteq (W \cap \mathbf{Z}[\{x \mid x < y\}])[y]$ for any y. Put also $R = \{u/v \mid u \in \mathbf{Z}[\bigcup_n X_n], v \in W\} \subseteq K$, $K = \mathbf{Z}(\bigcup_n X_n)$. Elements of K can be regarded as real analytic functions in variables $\vec{r}, s$; then elements of R are defined for all positive $\vec{r}, s$.

Claim 1. There are a, b, c: $\bigcup_n X_n \to \mathbf{Z}[\bigcup_n X_n]$ such that $a(\bigcup_n X_n) \subseteq W$, $a(X_n) \cup b(X_n) \cup c(X_n) \subseteq \mathbf{Z}[\bigcup_{k<n} X_k]$ for any n, and $\partial x/\partial s = b_x \cdot x/a_x + c_x/a_x$ for any $x \in \bigcup_n X_n$.

PROOF. Proceed by induction on n, $x \in X_n$. If $n = 0$ then either $x = s$ with $a_x = 1, b_x = 0, c_x = 1$, or x does not depend on s, so $a_x = 1$, $b_x = c_x = 0$. Let $n \neq 0$. We have

$$\begin{aligned} &\frac{\partial}{\partial s}(u \uparrow v) = \frac{\partial}{\partial s} \exp(v \cdot \ln(u)) = (u \uparrow v) \cdot \left(\frac{\partial v}{\partial s} \cdot \ln(u) = \frac{v}{u} \cdot \frac{\partial u}{\partial s} \right) \quad \text{and} \\ &\frac{\partial}{\partial s} \ln(w) = \frac{1}{w} \cdot \frac{\partial w}{\partial s}. \end{aligned} \tag{4}$$

Since $u, v, w \in \mathbf{Z}[\bigcup_{k<n} X_n]$ we have

$$\frac{\partial u}{\partial s} = \sum_x \frac{\partial u}{\partial x} \cdot \frac{\partial x}{\partial s}, \quad \frac{\partial v}{\partial s} = \sum_x \frac{\partial v}{\partial x} \cdot \frac{\partial x}{\partial s}, \quad \frac{\partial w}{\partial s} = \sum_x \frac{\partial w}{\partial s} \cdot \frac{\partial x}{\partial s}, \tag{5}$$

where the x's are elements of $\bigcup_{k<n} X_k$ occurring in u, v, w and $\partial/\partial x$ are the usual derivations in the ring of polynomials. Since a, b, c are already defined for x's, $\partial x/\partial s = b_x \cdot x/a_x + c_x/a_x$, one can substitute this expression for $\partial x/\partial s$ in (5) and substitute obtained expressions for $\partial u/\partial s, \partial v/\partial s, \partial w/\partial s$ into (4); reducing fractions to common denominator one then obtains $a_{u \uparrow v}, b_{u \uparrow v}, c_{u \uparrow v} = 0$ and $a_{\ln(w)}, b_{\ln(w)} = 0, c_{\ln(w)}$.

Claim 2. For any $t \in R - \mathbf{Q}$ there is a finite sequence $t_0 \in \mathbf{Q}, t_1, \ldots, t_n = t$ of elements of R such that for any m, $1 \leqslant m \leqslant n$, $\partial t_m/\partial s = (\beta t_m + t_{m-1})/\alpha$ for some $\beta \in R, \alpha \in W$.

PROOF. Apply the Proposition of §2 with a, b, c of Claim 1; put $f_0 = t, f_{m+1} = C_{f_m}$. Since $\triangleleft$ is well-founded, there will be n such that $f_n \in \mathbf{Q}$. Put $t_m = f_{n-m}$. Then $\partial t_m/\partial s = (\beta_{t_m} \cdot t_m + t_{m-1})/A_{t_m}$.

Claim 3. Let $t_n, \ldots, t_0$ be a sequence of elements of R satisfying Claim 2. Then for any k, $0 \leqslant k \leqslant n$, either $t_k = 0$ or t_k has $\leqslant k$ zeros in $\mathbf{R}_+$ as a function of s when $\vec{r}$ assumes arbitrary positive real values.

PROOF. If $f' = pf + q$ on an interval $\subseteq \mathbf{R}$, then

$$f = \exp\left(\int p\right) \cdot \left(\mathrm{Const} + \int q \cdot \exp\left(-\int p\right)\right),$$

whence either $f = 0$ or f has no zeros (for $q = 0$), or $\mathrm{zeros}(f) \leqslant 1 + \mathrm{zeros}(q)$ by Rolle's theorem applied to Const $+ \int q \cdot \exp(-\int p)$. So either $t_k = 0$ or t_k has no zeros (for $t_{k-1} = 0$), or

$$\mathrm{zeros}(t_k) \leqslant 1 + \mathrm{zeros}(t_{k-1}/\alpha) = 1 + \mathrm{zeros}(t_{k-1}) \quad \text{one } R_+.$$

Now, in order to bound $\mathrm{card}\{s \in \mathbf{R}_+ | t_1(\vec{r}, s) = t_2(\vec{r}, s)\}$, put $t = t_1 - t_2$ and apply Claims 2 and 3.

Proof of Lemma 2. Define w: $L \to \mathbf{N}$ as follows: $w(1) = 1$, $w(\text{any variable}) = 2$, and $w(t_1 \square t_2) = w(t_1) \square w(t_2)$ for $\square = +, \cdot$, or $\uparrow$. Let $b_1(m) = 1$, $b_2(m) = m + 1$, and $b_{k+1}(m) = b_k(m) + 3 \cdot (b_k(m))^2$ for $k \geqslant 2$ and any m. I will show that $B(t_1, t_2) = b_k(m) + 1$, where $k = \max(w(t_1), w(t_2))$ and m is the total number of variables occurring in t_1, t_2, satisfies Lemma 2.

Let s be any subset of T and $E = s \cup \{1^x = 1, x^1 = x, 1 \cdot x = x, x \cdot 1 = x\}$. Let P be the set of $(1, +, \cdot, \uparrow)$-terms in variables $v_1, \ldots, v_m$ modulo equivalence of terms t_1, t_2 whenever $E \vdash t_1 = t_2$. Since the equalities in E are valid in $\mathbf{N}$, by assumption, we may regard w as a function $P \to \mathbf{N}$. It is easy to see that for every integer j, $\{p \in P | w(p) \leqslant j\}$ has $\leqslant b_j(m)$ members. (Each member of P is represented by a term which does not contain any 1; the functions $+, \cdot$ and $\uparrow$ are strictly increasing on arguments > 1.) Let t_1, t_2 be $(1, +, \cdot, \uparrow)$-terms in variables $v_1, \ldots, v_m$ such that $E \nvdash t_1 = t_2$. Then $t_1 \neq t_2$ in P. Let $K = \max(w(t_1), w(t_2))$ and define a congruence on P by $p_1 \equiv p_2$ iff $p_1 = p_2$ or $w(p_1), w(p_2) \geqslant K + 1$. Then $p/\equiv$ still satisfies $t_1 \neq t_2$ and has $\leqslant B(t_1, t_2) = b_k(m) + 1$ members.

An important set E of identities which are valid in $\mathbf{N}$ is the following set of "high school algebra" identities:

(T1) $1^x = 1, x^1 = 1x = x1 = x$,

(T2) $x + y = y + x, xy = yx$,

(T3) $x + (y + z) = (x + y) + z, x(yz) = (xy)z$,

(T4) $x(y + z) = xy + xz$,

(T5) $x^{y+z} = x^y \cdot x^z$,

(T6) $(xy)^z = x^z \cdot y^z$,

(T7) $(x^y)^z = x^{yz}$.

Tarski raised the question of whether or not every identity valid in **N** can be derived from this set. Wilkie answered this question negatively, by showing that the following identity is true in **N** but is not derivable from Tarski's axioms:

$$\text{(W)}\quad ((x+1)^x+(x^2+x+1)^x)^y\cdot((x^3+1)^y+(x^4+x^2+1)^y)^x$$
$$=((x+1)^y+(x^2+x+1)^y)^x\cdot((x^3+1)^x+(x^4+x^2+1)^x)^y.$$

Wilkie's proof of nonderivability was difficult and made use of proof theory. In the remainder of this paper I will present a model of Tarski's axioms which consists of 59 elements and in which Wilkie's identity does not hold.

Note that we are *not* applying Theorem 2; the model given here provides a separate verification that (W) cannot be derived from Tarski's identities. Note also that when $x = y = 2$, the value of the terms in (W) is about 10^9. The bound given in the proof of Theorem 2 for the size of a finite model in this situation is approximately $(3^2)^{10^9}$. In constructing the 59-element model presented below, we are guided by the same idea as in the proof of Theorem 2, but we set the variables equal to 1 instead of 2. This requires some intricate changes in the definition of the model, and the verification that it is a model of Tarski's identities becomes more difficult.

The 59 elements of the model consist of the constants $1, 2, \ldots, 26$ together with the two terms which appear on either side of Wilkie's identity (W) and the following thirty-one other terms:

$x^1, x^2, x^3, x^4, y;$

$1+x^1, 1+x^2, 1+x^3, 1+x^4, x^1+x^2, x^1+x^3, x^1+x^4, x^2+x^4;$

$(1+x)^x, (1+x)^y, (1+x^3)^x, (1+x^3)^y;$

$1+x+x^2, (1+x+x^2)^x, (1+x+x^2)^y, 1+x^2+x^4, (1+x^2+x^4)^x, (1+x^2+x^4)^y;$

$(1+x)^x+(1+x+x^2)^x, ((1+x)^x+(1+x+x^2)^x)^y;$

$(1+x^3)^x+(1+x^2+x^4)^x, ((1+x^3)^x+(1+x^2+x^4)^x)^y;$

$(1+x)^y+(1+x+x^2)^y, ((1+x)^y+(1+x+x^2)^y)^x;$

$(1+x^3)^y+(1+x^2+x^4)^y, ((1+x^3)^y+(1+x^2+x^4)^y)^x$

(Here, for readability, we have used the usual superscript notation for exponentiation.) Let f, g denote the terms in (W), so the identity has the form $f = g$.

The operations in the model will be defined so that if the expressions on either side of (W) are evaluated in the model, treating x and y as elements of the model, then the values will be the terms f and g. Since these are distinct in the model, it follows that (W) is false.

Now we proceed to define the operations in the model. For each element t of the model, let $|t|$ be the integer value which results from interpreting t in **N** with $x = y = 1$.

(I) If t, u, v are elements in the model, $\square$ is $+, \cdot,$ or $\uparrow$, and if $t\square u = v$ is a valid identity in **N**, then we define $t\square u$ to equal v in the model.

(II) If $t\square u$ is not defined by (I), then we define

$$t\square u = \min(26, |t|\square|u|),$$

except in the special cases listed below:

(i) special cases for addition:

$$1 + y = y + 1 = 1 + x^3; \quad x + y = y + x = x + x^3;$$

(ii) special cases for multiplication:

$$x^i \cdot x^j = x^4 \quad \text{when } 1 \leqslant i, j \leqslant 4 \text{ and } i + j > 4;$$
$$x^i \cdot y = y \cdot x^i = x^4 \quad \text{when } 1 \leqslant i \leqslant 4, y \cdot y = x^4;$$
$$x \cdot (1 + x^4) = (1 + x^4) \cdot x = x + x^4;$$
$$x \cdot (x + x^4) = (x + x^4) \cdot x = x^2 + x^4;$$
$$x^2 \cdot (1 + x^3) = (1 + x^3) \cdot x^2 = x^2 + x^4;$$
$$x^2 \cdot (1 + x^4) = (1 + x^4) \cdot x^2 = x^2 + x^4;$$

(iii) special cases for exponentiation (u is any element of the model):

$$(x^i)^u = x^{\min(4, i|u|)}, \quad \text{where } 1 \leqslant i \leqslant 4;$$
$$y^u = x^4 \quad \text{if } u \text{ is not } 1.$$

It remains to show that Tarski's axioms (T1)–(T7) are true in this model. This is done by direct verification, which will not be given here. There are not too many cases which require detailed analysis, since $t \square u$ is often merely $|t| \square |u|$.

Remark 1. Wilkie's identity contains two variables. Substituting for y a suitable term in x, one can obtain an identity in x which is only valid over **N** but cannot be derived from Tarski's axioms. Moreover, finite models for Tarski's axioms in which such identities are false can be obtained by modifying the 59-element model given here. For example, this can be done when y is replaced by x^x; the resulting model will again have 59 elements.

Remark 2. Applying ideas similar to those which are used to prove Theorem 2, one can prove

Theorem 3. *Let J be the set of inequalities of $(1, +, \cdot, \uparrow)$-terms, $j = \{t_1 \leqslant t_2 | t_1, t_2 \in L\}$ and $S(J)$ the set of finite subsets of J. There is a recursive function A: $S(J) \times L \times L \to \{yes, no\}$ such that if $s \in S(J)$ consists of valid inequalities then $A(s, t_1, t_2)$ is the answer to the question whether $s, x^1 = 1x = x1 = x, 1^x = 1 \vdash t_1 \leqslant t_2$. One can add, e.g., rules $x|y, p \leqslant q \vdash xp \leqslant yq$, and $x \leqslant y, p \leqslant q \vdash x + p \leqslant y + q$ to the usual (substitution and monoticity) rules—the result shall remain valid.*

Note that inequational theory of $(N; 1, +, \cdot, \uparrow, \leqslant)$ is undecidable.

Acknowledgement. Professor C. Ward Henson made a computer check of the original model presented by the author and found that it did not satisfy all of Tarski's axioms. He was able to modify the model (by adding the exceptional cases in the definition of $+$) to correct this problem. He has checked by computer that the model presented here does satisfy Tarski's axioms. Curiously this would also be true if $x + y$ were defined to be $x + x^4$ instead of $x + x^3$.

References

1. L. Henkin, *The logic of equality*, Amer. Math. Monthly **84** (1977) 597–612.

2. A. G. Hovanskii, *Ob odnom klasse sistem transcendentnykh uravnenii*, Dokl. Akad. Nauk SSSR **255** (1980), 804–807; English transl. in Soviet Math. Dokl. **22** (1980), 762–765.

3. A. Macintyre, *The laws of exponentiation*, Model Theory and Arithmetic Proc., Paris, 1979/80; (C. Berline, K. McAloon and J.-P. Ressayre, eds.), Lecture Notes in Math., vol. 890, Springer-Verlag, 1981, pp. 185–197.

4. D. Richardson, *Solution of the identity problem for integral exponential functions*, Z. Math. Logik Grundlag. Math. **15** (1969), 333–340.

5. A. J. Wilkie, *On exponentiation—A solution to Tarski's high school algebra problem*, Math. Inst. Oxford Univ., October 1981 (preprint).

Current address: Maurice Thorez, 33 Apt. 205, Leningrad 194223, USSR