On Exponentiation - A Solution to Tarski's High School Algebra Problem

A. J. Wilkie

1

To explain the problem in the title we introduce the first-order language L, which contains a constant symbol 1 (one), and three binary function symbols $+$ (addition), $\cdot$ (multiplication) and E (exponentiation). We usually write a^b for $E(a, b)$.

We denote by $\mathbb{Z}, \omega, \mathbb{N}, \mathbb{R}$ and $\mathbb{R}^+$ the sets of integers, non-negative integers, positive integers, real numbers and positive real numbers respectively. We shall also use $\mathbb{N}$ and $\mathbb{R}^+$ to denote the L-structures with these domains and the usual interpretations of the symbols of L.

The simplest case of Tarski's problem is: given terms f, g of L such that $\mathbb{N} \models f = g$, is it true that the equation $f = g$ can be proved from the usual laws of addition, multiplication and exponentiation?

By "the usual laws ..." I assume the following equational theory, which we denote by EXP, is meant:-

1.1 (i) $x + y = y + x$, (ii) $x \cdot y = y \cdot x$.

1.2 (i) $x + (y + z) = (x + y) + z$, (ii) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

1.3 $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

1.4 $1 \cdot x = x$.

1.5 (i) $x^1 = x$, (ii) $1^x = 1$.

1.6 $(x \cdot y)^z = x^z \cdot y^z$.

1.7 $x^{(y+z)} = x^y \cdot x^z$.

1.8 $(x^y)^z = x^{(y.z)}$.

Tarski's problem thus becomes:- Does $\mathbb{N} \models f = g$ imply EXP $\vdash f = g$? We shall show later that the answer to this question is no and in order to motivate the modification of EXP that we shall be making shortly, we reveal our counterexample now.

Let $A = (x + 1)$, $B = (x^2 + x + 1)$, $C = (x^3 + 1)$, $D = (x^4 + x^2 + 1)$. (Since we shall always be working in a theory at least as strong as EXP, we may make the usual conventions concerning omitting of brackets, etc., when writing down terms of L.)

Let $f_0 = (A^x + B^x)^y (C^y + D^y)^x$ and $g_0 = (A^y + B^y)^x (C^x + D^x)^y$. Then $\mathbb{N} \models f_0 = g_0$ but EXP $\not\vdash f_0 = g_0$. That $\mathbb{N} \models f_0 = g_0$ can be seen by noting that $C = A \cdot (x^2 - x + 1)$ and $D = B \cdot (x^2 - x + 1)$, and then factoring the "term" $(x^2 - x + 1)^{x \cdot y}$ from both f_0 and g_0. Of course, the fact that $(x^2 - x + 1)^{x \cdot y}$ is *not* a term of L turns out to be the reason that EXP $\not\vdash f_0 = g_0$.

We shall show that this is essentially the only way in which EXP is inadequate. More precisely, we modify EXP as follows.

Let $\rho = \rho(x_1, ..., x_n)$ be a polynomial with integer coefficients in the variables shown. We call ρ *positive* if $\rho(r_1, ..., r_n) \in \mathbb{R}^+$ whenever $r_1, ..., r_n \in \mathbb{R}^+$. Let $\mathcal{P}_n$ denote the set of positive polynomials with n variables. For each $\rho \in \mathcal{P}_n$ let t_ρ be a new n-place function symbol, and let L^* be the language obtained by adding all the t_ρ (for all $\rho \in \bigcup\limits_{n \in \omega} \mathcal{P}_n$) to L. Notice that $\mathbb{N}$ and $\mathbb{R}^+$ can be expanded to L^* structures (also denoted $\mathbb{N}, \mathbb{R}^+$) by interpreting t_ρ as ρ.

We define EXP* to be the equational theory obtained by adding to EXP all equations $(f = g)$, where f, g are terms of L^* *not involving exponentiation*, such that $\mathbb{N} \models (f = g)$ (or, obviously equivalently, such that $\mathbb{R}^+ \models (f = g)$).

We shall prove later the following theorem, which seems to be, in the light of the above counterexample, the best possible positive solution to Tarski's problem.

1.9 **Theorem**.

Let f, g be terms of L such that $\mathbb{N} \models f = g$. Then EXP$^* \vdash f = g$.

Remarks: (i) Notice that f, g are terms of L, and not of L^*. I do not know if 1.9 can be strengthened to allow f, g to be terms of L^*.

(ii) It might have seemed simpler to modify EXP by just adding axioms for $-$ (negation). However, there would be great difficulties of interpretation if we did this.

2

Fix $n \in \mathbb{N}$. We assume L contains the variables $y_1, ..., y_n, x_1, x_2, ..., x_k, ... (k \in \mathbb{N})$.

Let P_m denote the set of irreducible (over $\mathbb{Z}$) members of $\mathcal{P}_m$ *other than* 1 or a single variable (i.e. a projection function). Let M_m denote the set of monomials of $\mathcal{P}_m$ (with coefficient 1) other than 1.

Since no factor of a positive polynomial can have a zero in the positive real quandrant, it follows that

2.1 every element of $\mathcal{P}_m$ (other than 1) factors uniquely (apart from order) as a product of an element of M_m and elements of P_m.

We now fix an enumeration $\langle p_1, q_1 \rangle, \langle p_2, q_2 \rangle, ..., \langle p_k, q_k \rangle, ... (k \in \mathbb{N})$ of terms, not involving exponentiation, of L^* with the following properties:-

2.2 $\forall\, k \in \omega$, $p_{k+1} = t_\rho(y_1, ..., y_n, x_1, ..., x_{k'})$ or $p_{k+1} = y_i$ for some $i \in \mathbb{N}$, $i \leq n$, $q_{k+1} = t_\mu(y_1, ..., y_n, x_1, ..., x_{k''})$ for some $k', k'' \in \omega$, $k', k'' \leq k$, $\rho \in P_{n+k'}$ and $\mu \in M_{n+k''}$.

2.3 $\forall\, k, k' \in \omega\ \forall\, \rho \in P_{n+k}\ \forall\, \mu \in M_{n+k'}$ there is some $l \in \mathbb{N}$ such that EXP$^* \vdash p_l = t_\rho(y_1, ..., y_n, x_1, ..., x_k)$ and EXP$^* \vdash q_l = t_\mu(y_1, ..., y_n, x_1, ..., x_{k'})$.

2.4 $\forall\, k \in \mathbb{N}, \forall\, i \in \mathbb{N}, i \leq n, \forall\, \mu \in M_{n+k}$, there is some $l \in \mathbb{N}$ such that $\mathrm{EXP}^* \vdash p_l = y_i$ and $\mathrm{EXP}^* \vdash q_l = t_\mu(y_1, ..., y_n, x_1, ..., x_k)$.

2.5 $\forall\, k, l \in \mathbb{N},\ k \leq l$, if $\mathrm{EXP}^* \vdash \forall\, y_1, ..., y_n, x_1, ..., x_{l-1}(p_k = p_l \wedge q_k = q_l)$ (or equivalently, if this sentence holds in $\mathbb{N}$, or in $\mathbb{R}^+$), then $k = l$.

It is clearly easy to construct such an enumeration.

We now define sequences of terms of L^*, $\langle u_i \rangle_{i \in \mathbb{N}}$, $\langle s_i \rangle_{i \in \mathbb{N}}$, $\langle \tau_i \rangle_{i \in \mathbb{N}}$ as follows:-

2.6 $u_1 = p_1,\ s_1 = q_1,\ \tau_1 = p_1^{q_1}$.

2.7 For $i \in \mathbb{N}$, $u_{i+1} = p_{i+1}(y_1, ..., y_n, \tau_1, ..., \tau_i)$ (i.e. u_{i+1} is the result of substituting τ_1 for $x_1, ..., \tau_i$ for x_i in p_{i+1}), $s_{i+1} = q_{i+1}(y_1, ..., y_n, \tau_1, ..., \tau_i)$, $\tau_{i+1} = u_{i+1}^{s_{i+1}}$.

Clearly the variables occurring in u_i, s_i, τ_i (for $i \in \mathbb{N}$) are amongst $y_1, ..., y_n$.

Let us call a polynomial $\rho \in \mathcal{P}_m$ (for $m \in \mathbb{N}$) *strictly positive* if all its coefficients are positive.

(The reader might like to consult the beginning of section 7 now, where an example of 2.2–2.7 and 2.8, is calculated in detail.)

2.8 **Theorem.**

Let f be a term of L with the variables occurring in f amongst $y_1, ..., y_n$. Then there is a strictly positive polynomial $\rho_f \in \mathcal{P}_{n+m}$ (for some $m \in \omega$) such that $\mathrm{EXP}^* \vdash f = t_{\rho_f}(y_1, ..., y_n, \tau_1, ..., \tau_m)$, i.e. ρ_f *represents* f.

Proof.

By induction on f. Clearly the theorem is true if f is the term 1 or the term y_i (for some $i \in \mathbb{N}$, $i \leq n$). Also, if ρ_f represents f and ρ_g represents g then the positive polynomials $(\rho_f + \rho_g), (\rho_f \cdot \rho_g)$ clearly represent the terms $(f + g), (f \cdot g)$ respectively. (Recall that all exponential-free equations that are valid in $\mathbb{N}$ are in EXP^*.) We therefore only need to find a positive polynomial representing f^g.

Now by 2.1 and the fact that every positive polynomial (other than 1) can be written uniquely (apart from order) as the sum of monomials, it suffices to show that if $\rho \in \mathcal{P}_{n+m_0}$ (for some $m_0 \in \mathbb{N}$) is irreducible and $\mu \in \mathcal{P}_{n+m_1}$ (for some $m_1 \in \mathbb{N}$) is a non-constant monomial, then for some strictly positive $\alpha \in \mathcal{P}_{n+m_2}$ (for some $m_2 \in \mathbb{N}$),

$$(*) \ldots\ \mathrm{EXP}^* \vdash t_\alpha(y_1, ..., y_n, \tau_1, ..., \tau_{m_2}) = t_\rho(y_1, ..., y_0, \tau_1, ..., \tau_{m_0}) t_\mu(y_1, ..., y_n, \tau_1, ..., \tau_{m_1}).$$

(For using 1.6 and 1.7 and 1.5(i), $t_{\rho_f}^{t_{\rho_g}}$ is provably, in EXP^*, equal to a product of terms of the same form as those appearing on the right here together with a (constant) power of t_{ρ_g}, and, by the inductive hypothesis, we have $\mathrm{EXP}^* \vdash f^g = t_{\rho_f}(\ldots)^{t_{\rho_g}(\cdots)}$.)

The proof of (*) splits into cases. If either $\rho \in P_{n+m_0}$ or $\rho(y_1, ..., y_n, x_1, ..., x_{m_0})$ is identically equal to y_i, for $i \in \mathbb{N}$, $i \leq n$, then by 2.3 and 2.4 respectively, there is $l \in \mathbb{N}$ such that $\mathrm{EXP}^* \vdash p_l = t_\rho(y_1, ..., y_n, x_1, ..., x_{m_0})$ and $\mathrm{EXP}^* \models q_l = t_\mu(y_1, ..., y_n, x_1, ..., x_{m_1})$. Hence we may take $\alpha \in \rho_{n+l}$ where $\alpha(y_0, ..., y_n, x_1, ..., x_l)$ is identically equal to x_l. (*) holds by 2.6 (if $l = 1$) or 2.7.

If ρ is identically 1, then we may take α identically 1, so that (*) holds by 1.5(ii).

If $\rho(y_1,...,y_n,x_1,...,x_{m_0})$ is identically equal to x_j for some $j \in \mathbb{N}$, $j \leq m_0$, then $\mathrm{EXP}^* \vdash t_\rho(y_1,...,y_n,\tau_1,...,\tau_{m_0}) = \tau_j$. Also $\mathrm{EXP}^* \vdash \tau_j = t_{\rho'}(y_1,...,y_n,\tau_1,...,\tau_{k'})^{t_{\mu'}(y_1,...,y_n,\tau_1,...,\tau_{k'})}$ for some $k', k'' \in \omega$, $k', k'' \leq j-1$ and $\rho' \in P_{n+k'}$, $\mu' \in M_{n+k''}$ (by 2.6 (if $j=1$) or 2.7, and 2.2). Hence this case reduces to the first case (replacing ρ by ρ' and μ by $\mu\mu'$) by 1.8.

We have now exhausted the possibilities for ρ, so the proof of 2.8 is complete. □

If f is a term of L^* with variables occurring amongst $y_1,...,y_n$, we denote by $\overline{\overline{f}}$ the interpretation of this term in $\mathbb{N}$, or in $\mathbb{R}^+$. There can be no confusion here since $\mathbb{N}$ is an L^*-substructure of $\mathbb{R}^+$ and further, the function interpreting f in $\mathbb{R}^+$ is totally determined by the function interpreting f in $\mathbb{N}$, in the sense that if $\mathbb{N} \models f = g$ (for g a term of L^*) then $\mathbb{R}^+ \models f = g$. (See [1].)

Our aim now is to show that the functions $\overline{\overline{y}}_1,...,\overline{\overline{y}}_n, \overline{\overline{\tau}}_1, \overline{\overline{\tau}}_2, ...$ are algebraically independent over $\mathbb{R}$ (considered as functions $(\mathbb{R}^+)^n \to \mathbb{R}^+$). Clearly this, with 2.8, will suffice to establish 1.9. We first require some results from differential algebra.

3

The proofs of the following propositions can easily be extracted from the proof of theorem in [2] (due to M. Singer). Presumably they also appear in more conventional texts on differential algebra although I've never found them.

All fields are assumed to have characteristic 0.

3.1 **Proposition**

Suppose F, G are differential fields (with derivative $'$), $F \subseteq G$, and F and G have the same fields of constants. Suppose $\alpha \in G$ is transcendental over F. Then

(i) If $\beta \in F$ and $\alpha' = \beta'\alpha$ (in G), then $F(\alpha)$ is closed under $'$ and if $X, Y \in F(\alpha)$ satisfy $X' = Y'X$ then $X = \alpha^m u$ and $Y = m\beta + v$, for some $m \in \mathbb{Z}$ and $u, v \in F$ such that $u' = v'u$.

(ii) If $\beta \in F \smallsetminus \{0\}$ and $\alpha' = \frac{\beta'}{\beta}$ (in G), then $F(\alpha)$ is closed under $'$ and if $X, Y \in F(\alpha)$ are such that $X' = Y'X$ then $X = \beta^m u$ and $Y = m\alpha + v$, for some $m \in \mathbb{Z}$ and $u, v \in F$ such that $u' = v'u$.

3.2 **Proposition**

Suppse that F, G are differential rings (with derivative $'$) with F a field, $F \subseteq G$, and that F and G have the same fields of constants. Suppose $\alpha \in G$ and α is algebraic over F. Then

(i) If $\beta \in F$ and $\alpha' = \beta'\alpha$, then $\alpha^m = u$ and $m\beta = v$ for some $m \in \mathbb{Z} \smallsetminus \{0\}$ and $u, v \in F$ such that $u' = v'u$.

(ii) If $\beta \in F \smallsetminus \{0\}$ and $\alpha' = \frac{\beta'}{\beta}$, then $\alpha \in F$.

4

We now associate to the sequence $\tau_1, \tau_2, ...$ of terms a sequence $F_0, F_1, ...$ of fields of functions with domains subsets of $\mathbb{R}^+$.

First, for $i = 1, ..., n$, let $Y_i = Y_i(r)$ be functions $\mathbb{R}^+ \to \mathbb{R}^+$ which are real analytic and differentially independent over $\mathbb{R}$, i.e. the functions $Y_i^{(j)}$ (= the j'th derivative of Y_i) for $i = 1, ..., n$, $j \in \omega$, are algebraically independent over $\mathbb{R}$.

4.1 Now let us note that if $f_1, f_2, ...$ are any functions $\mathbb{R}^+ \to \mathbb{R}$ which are real analytic and algebraiclly independent, and if the domain $\mathbb{R}[f_1, f_2, ...]$ is closed under differentiation, then the field $\mathbb{R}(f_1, f_2, ...)$ is naturally a differential field of functions with domains certain open subsets of $\mathbb{R}^+$. This is because if $\alpha, \beta \in \mathbb{R}[f_1, f_2, ...]$ and β is not identically zero, then the function α/β is infinitely differentiable on the (open-co-countable) set $D_\beta = \{r \in \mathbb{R}^+ : \beta(r) \neq 0\}$, and the collection of all sets D_β (for $\beta \in \mathbb{R}[f_1, f_2, ...]$) clearly generates a proper filter of subsets of $\mathbb{R}^+$. Thus we may henceforth speak of "the differential field $\mathbb{R}(f_1, f_2, ...)$" (whenever $f_1, f_2, ...$ satisfy the above conditions) and operate formally with the derivative (which we always denote by $'$) without worrying about the domains of definition of functions in $\mathbb{R}(f_1, f_2, ...)$. (For example, we write $f' = g$, for $f, g \in \mathbb{R}(f_1, f_2, ...)$ to mean $f'(r) = g(r)$ $\forall r \in A$, where A is some set in the filter mentioned above.)

To return to the matter at hand, let F_{-1} be the differential field $\mathbb{R}(Y_i^{(j)} : i = 1, ..., n, j \in \omega)$, generated over $\mathbb{R}$ by the $Y_i^{(j)}$s. Consider the function $\log Y_1$ ($= r \mapsto \log Y_1(r)$ $(r \in \mathbb{R}^+)$. Note that $Y_1(r) \in \mathbb{R}^+$ for $r \in \mathbb{R}^+$, so $\log Y_1$ is a well-defined, real analytic function $\mathbb{R}^+ \to \mathbb{R}$). Since $(\log Y_1)' = \frac{Y_1'}{Y_1} \in F_{-1}$, it follows that the ring $F_{-1}[\log Y_1]$ is closed under differentiation, and hence, if $\log Y_1$ were algebraic over F_1 we would have, by 3.2(ii), $\log Y_1 \in F_{-1}$. However, this would clearly give rise to a non-trivial differential dependence amongst the $Y_i^{(j)}$'s. Thus $\log Y_1$ is transcendental over F_{-1}, and further, by 3.1(ii), if X, Y are elements of the differential field $F_{-1}(\log Y_1)$ such that $X' = Y'X$ then $X = cY_1^m$ for some $m \in \mathbb{Z}$ and $c \in \mathbb{R}$ (since there are only constant solutions to this equation in F_{-1}).

Clearly we can successively repeat this argument with $\log Y_2, ..., \log Y_n$ to obtain the differential field $F_{-1}(\log Y_1, ..., \log Y_n)$, which we denote by F_0, so that

4.2 F_0 is a differential field generated (as a field) by the algebraically independent set of functions $\{Y_i^{(j)}, \log Y_i : i \in \mathbb{N},\ 1 \leq i \leq n,\ j \in \omega\}$. Further, if $X, Y \in F_0$ and $X' = Y'X$ then

$$X = c \prod_{i=1}^{n} Y_i^{m_i} \quad \text{for some} \quad c \in \mathbb{R}, \quad m_i \in \mathbb{Z} \quad (i = 1, ..., n).$$

Now if $h = h(y_1, ..., y_n)$ is any term of L^* with free variables amongst $y_1, ..., y_n$, we denote by $\bar{h}$ the function $\mathbb{R}^+ \to \mathbb{R}^+$ defined by $\bar{h}(r) = \overline{\overline{h}}(Y_1(r), ..., Y_n(r))$. (Recall that $\overline{\overline{h}}$ is the function $(\mathbb{R}^+)^n \to \mathbb{R}^+$ interpreting h in the structure $\mathbb{R}^+$.)

Our aim is to use the propositions of section 4 to show that the functions $\bar{\tau}_1, \bar{\tau}_2, ...$ (see 2.6, 2.7) are algebraically independent over F_0. Unfortunately the rings $F_0[\bar{\tau}_1], F_0[\bar{\tau}_1, \bar{\tau}_2], ...$

are not closed under differentiation so we cannot apply these results (or remark 4.1) directly — we must clearly also consider the functions $\log \bar{u}_1, \log \bar{u}_2, \ldots$ (see 2.6, 2.7). We first define subsets V_0, V_1, V_2 of $\mathbb{N}$, which distinguish certain technically important properties of the p_i's (see section 2, especially 2.2–2.5), as follows:

$$\begin{aligned} V_0 &= \{i \in \mathbb{N} : \overline{\overline{p}}_i \ \text{ is constant}\}. \\ V_1 &= \{i \in \mathbb{N} : \exists j \in \mathbb{N},\ j \leq n,\ \text{EXP}^* \vdash p_i = y_j\}. \\ V_2 &= \{i \in \mathbb{N} \setminus (V_0 \cup V_1) : \ \text{ for no } \ j < i,\ j \in \mathbb{N}, \ \text{ do we have } \ \text{EXP}^* \vdash p_i = p_j\}. \end{aligned}$$

4.3 (a) Note that since each $\overline{\overline{p}}_i$ is an irreducible positive polynomial and is not 1 (by 2.2), if $i \in V_0$, then the constant value of $\overline{\overline{p}}_i$ (hence of $\bar{u}_i$) must be a positive prime integer. (b) Note also that $\forall j \in \mathbb{N} \setminus (V_0 \cup V_1)$ there is $j_0 \in V_2$ such that $j_0 \leq j_1$ and $\text{EXP}^* \vdash p_j = p_{j_0}$, in particular $\bar{u}_j = \bar{u}_{j_0}$.

4.4 **Theorem**

Suppose $i \in \omega$. Then

(I)$_i$ (a) The functions $\{\bar{\tau}_j : j \in \mathbb{N},\ j \leq i\} \cup \{\log \bar{u}_j : j \in V_2,\ j \leq i\}$ are algebraically independent over F_0, and (b) the ring they generate over F_0 is closed under differentiation.

(II)$_i$ Let F_i denote the differential field $F_0(\bar{\tau}_1, \ldots, \bar{\tau}_i, \log \bar{u}_j : j \in V_2,\ j \leq i)$, generated (as a field) by the functions in (I)$_i$ (see 4.1) and suppose $X, Y \in F_i$ and $X' = Y'X$. Then

$$X = c \prod_{j=1}^{n} Y_j^{m_j} \prod_{j=1}^{i} \bar{\tau}_j^{l_j} \prod_{\substack{j \leq i \\ j \in V_2}} \bar{u}_j^{k_j},$$

for some integers $m_1, \ldots, m_n, l_1, \ldots, l_i,\ k_j,\ (j \leq n, j \in V_2)$, and some $c \in \mathbb{R}$.

Proof

By induction on i. The case $i = 0$ reduces to 4.2, so suppose the theorem is true for some $i \geq 0$.

Case 1. $i + 1 \in V_2$.

Let us first show that $\log \bar{u}_{i+1}$ is transcendental over F_i. Now by 2.6, 2.7, $\bar{u}_{i+1} = \overline{\overline{p}}_{i+1}(Y_1, \ldots, Y_n, \bar{\tau}_1, \ldots, \bar{\tau}_i)$, and so $\bar{u}_{i+1} \in F_i$ (hence by (I)$_i$(b), $\bar{u}'_{i+1} \in F_i$). Since $(\log \bar{u}_{i+1})' = \frac{\bar{u}'_{i+1}}{\bar{u}_{i+1}}$, if $\log \bar{u}_{i+1}$ were algebraic over F_i we would have by 3.2(ii) (taking $G = F_i[\log \bar{x}_{i+1}]$) that $\log \bar{u}_{i+1} \in F_i$. But $\bar{u}'_{i+1} = (\log \bar{u}_{i+1})' \bar{u}_{i+1}$, so by (II)$_i$

$$\bar{u}_{i+1} = \overline{\overline{p}}_{i+1}(Y_1, \ldots, Y_n, \bar{\tau}_1, \ldots, \bar{\tau}_i) = c \prod_{j=1}^{n} Y_j^{m_j} \prod_{j=1}^{i} \bar{\tau}_j^{l_j} \prod_{\substack{j \leq i \\ j \in V_2}} (\bar{u}_j)^{k_j}.$$

for suitable m_j's, l_j's and k_j's $\in \mathbb{Z}$ and $c \in \mathbb{R}$. Using 2.6, 2.7 we obtain:

$$\overline{\overline{p}}_{i+1}(Y_1, ..., Y_n, \bar{\tau}_1, ..., \bar{\tau}_i) = c\prod_{j=1}^{n} Y_j^{m_j} \prod_{j=1}^{i} \bar{\tau}_j^{l_j} \prod_{\substack{j \le i \\ j \in V_2}} (\overline{\overline{p}}_j(Y_1, ..., Y_n, \bar{\tau}_1, ..., \bar{\tau}_{j-1}))^{k_j}.$$

Now by $(\mathrm{I})_i$(a), this equation may be regarded as a polynomial identity in the 'variables' $Y_1, ..., Y_n, \bar{\tau}_1, ..., \bar{\tau}_i$, so since $\overline{\overline{p}}_{i+1}$ is irreducible (by 2.2 and the definition of the sets P_m) we must have either (a) $\mathrm{EXP}^* \vdash p_{i+1} = y_j$ (for some $j \in \mathbb{N}$, $j \le n$), or (b) $\mathrm{EXP}^* \vdash p_{i+1} = x_j$ (for some $j \in \mathbb{N}$, $j \le i$) or (c) $\mathrm{EXP}^* \vdash p_{i+1} = p_j$ (for some $j \in \mathbb{N}$, $j \le n$) or (d) $\overline{\overline{p}}_{i+1}$ is constant.

However, (a),(c),(d) are impossible since $i + 1 \in V_2$, and (b) is impossible by 2.2 (recall P_m contains no projection functions — see the beginning of section 2).

Thus $\log \bar{u}_{i+1}$ is transcendental over F_i.

It now follows from 3.1(ii), $(\mathrm{II})_i$ and the fact that $F_i[\log \bar{u}_{i+1}]$ is closed under differentiation, that if X, Y are elements of the differential field (see 4.1) $F_i(\log \bar{u}_{i+1})$ and $X' = Y'X$ then

$$(\mathrm{II})_{i+\frac{1}{2}} \qquad X = c\prod_{j=1}^{n} Y_j^{m_j} \prod_{j=1}^{i} \bar{\tau}_j^{l_j} \prod_{\substack{j \le i+1 \\ j \in V_2}} \bar{u}_j^{k_j}$$

for suitable m_j's, l_j's and k_j's $\in \mathbb{Z}$ and $c \in \mathbb{R}$.

We now show that $\bar{\tau}_{i+1}$ is transcendental over $F_i(\log \bar{u}_{i+1})$. Now, by 2.6, 2.7:- (*) ... $(\bar{\tau}_{i+1})' = (\bar{u}_{i+1}^{\bar{s}_{i+1}})' = (\bar{s}_{i+1} \log \bar{u}_{i+1})' \bar{\tau}_{i+1}$, and $\bar{s}_{i+1} \log \bar{u}_{i+1} = \overline{\overline{q}}_{i+1}(Y_1, ..., Y_n, \bar{\tau}_1, ..., \bar{\tau}_i) \cdot \log \bar{u}_{i+1} \in F_i(\log \bar{u}_{i+1})$ ... (*). Hence if $\bar{\tau}_{i+1}$ were algebraic over $F_i(\log \bar{u}_{i+1})$ we would have, by 3.2(i) (taking $G = F_i(\log \bar{u}_{i+1})[\bar{\tau}_{i+1}]$) and by $(\mathrm{II})_{i+\frac{1}{2}}$

$$\bar{\tau}_{i+1}^{m} = c\prod_{j=1}^{n} Y_j^{m_j} \prod_{j=1}^{i} \bar{\tau}_j^{l_j} \prod_{\substack{j \le i+1 \\ j \in V_2}} \bar{u}_j^{k_j}$$

for some $m \in \mathbb{Z} \setminus \{0\}$, and suitable m_j's, l_j's and k_j's $\in \mathbb{Z}$ and $c \in \mathbb{R}$.

Now by taking logarithms here, using 2.6, 2.7, and equating coefficients of $\log \bar{u}_{i+1}$ (which is justified by the proven algebraic independence of the functions $\bar{\tau}_1, ..., \bar{\tau}_i$, $\log \bar{u}_j$ $(j \le i + 1, j \in V_2)$, $Y_1, ..., Y_n$ and $\log Y_1, ..., \log Y_n$) we obtain, (using also 4.3(b)):-

$$m\overline{\overline{q}}_{i+1}(Y_1, ..., Y_n, \bar{\tau}_1, ..., \bar{\tau}_i) = ck_{i+1}.$$

As usual, this implies that $\overline{\overline{q}}_{i+1}$ is a constant polynomial, and hence, since it is a monomial by 2.2, we have $\mathrm{EXP}^* \vdash q_{i+1} = 1$. But this contradicts 2.2 and the fact that M_r does not contain the monomial 1, for any $r \in \mathbb{N}$ (see the beginning of section 2).

We have now established $(\mathrm{I})_{i+1}(\mathrm{a})$ and, en route (see (*)), $(\mathrm{I})_{i+1}(\mathrm{b})$.

$(\mathrm{II})_{i+1}$ now follows easily from $(\mathrm{II})_{i+\frac{1}{2}}$, (*) and 3.1(i).

Case 2 $i+1 \notin V_2$.

Here we have either (a) $\overline{\overline{p}}_{i+1}$, and hence $\bar{u}_{i+1}$, is constant or (b) $i+1 \in V_1$, in which case $\bar{u}_{i+1} = Y_{j_0}$ for some $j_0 \in \mathbb{N}$, $j_0 \in n$ or (c) $i+1 \notin V_0 \cup V_1$, but $\mathrm{EXP}^* \vdash p_{i+1} = p_{j_0}$ for some $j_0 \leq i$, $j_0 \in \mathbb{N}$, and we may clearly take $j_0 \in V_2$, in which case $\bar{u}_{i+1} = \bar{u}_{j_0}$ (by 2.7).

Notice that in all cases we have $\log \bar{u}_{i+1} \in F_i$. Hence, $\bar{s}_{i+1} \log \bar{u}_{i+1} = \overline{\overline{q}}_{i+1}(Y_1, ..., Y_n, \bar{\tau}_1, ..., \bar{\tau}_i) \cdot \log \bar{u}_{i+1} \in F_i$, and since $(\bar{\tau}_{i+1})' = (\bar{s}_{i+1} \log \bar{u}_{i+1})' \bar{\tau}_{i+1}$, both $(\mathrm{I})_{i+1}$ and $(\mathrm{II})_{i+1}$ will follow from $(\mathrm{I})_i$, $(\mathrm{II})_i$ and 3.1(i) if we can show that $\bar{\tau}_{i+1}$ is transcendental over F_i.

As above, if $\bar{\tau}_{i+1}$ were algebraic over F_i, we would have, by 3.2(i) and $(\mathrm{II})_i$

$$\bar{\tau}_{i+1}^m = c \prod_{j=1}^{n} Y_j^{m_j} \prod_{j=1}^{i} \bar{\tau}_j^{l_j} \prod_{\substack{j \leq i \\ j \in V_2}} \bar{u}_j^{k_j}$$

for suitable $m \in \mathbb{Z} \smallsetminus \{0\}$, m_j's, l_j's, k_j's $\in \mathbb{Z}$ and $c \in \mathbb{R}$.

Taking logarithms and using 2.6, 2.7 we obtain

$$m\bar{s}_{i+1} \log \bar{u}_{i+1} = \log c + \sum_{j=1}^{n} m_j \log Y_j + \sum_{j=1}^{i} l_j \bar{s}_j \log \bar{u}_j + \sum_{\substack{j \leq i \\ j \in V_2}} k_j \bar{u}_j \qquad \ldots \qquad (**)$$

(Clearly $c \in \mathbb{R}^+$.)

Let

$$\begin{aligned} V_1^j &= \{\nu \in V_1 : \nu \leq i \text{ and } \mathrm{EXP}^* \vdash p_\nu = y_j\} \text{ for } j = 1, ..., n, \\ V_2^j &= \{\nu \in \mathbb{N} : \nu \leq i \text{ and } \mathrm{EXP}^* \vdash p_\nu = p_j\} \text{ for } j \in V_2,\ j \leq i. \end{aligned}$$

Then we may rearrange the sum in (**) as follows:-

$$m\bar{s}_{i+1} \log \bar{u}_{i+1} = (\log c + \sum_{\substack{j \leq i \\ j \in V_0}} l_j \bar{s}_j \log \bar{u}_j) + \sum_{j=1}^{n} \left[(\log Y_j) \cdot (m_j + \sum_{\nu \in V_1^j} l_\nu \bar{s}_\nu) \right] +$$

$$+ \sum_{\substack{j \leq i \\ j \in V_2}} \left[(\log \bar{u}_j) \cdot (k_j + \sum_{\nu \in V_2^j} l_\nu \bar{s}_\nu) \right]. \qquad \ldots \qquad (***)$$

Now by 2.6, 2.7 each $\bar{s}_j$ (for $j \in \mathbb{N}$, $j \leq i+1$) can be written as a polynomial in $Y_1, ..., Y_n, \bar{\tau}_1, ..., \bar{\tau}_{j-1}$ and since the set $\mathcal{A} = \{Y_1, ..., Y_n, \log Y_1, ..., \log Y_n, \bar{\tau}_1, ..., \bar{\tau}_i, \bar{u}_j, \log \bar{u}_j$ $(j \leq i, j \in V_2)\}$ is algebraically independent (over $\mathbb{R}$) we are free to equate coefficients in (***).

Recall the three sub-cases:-

(a) $\bar{u}_{i+1}$ is a constant. Then (***) gives

$$m\bar{s}_{i+1}\log\bar{u}_{i+1} = \log c + \sum_{\substack{j\le i\\ j\in V_0}} l_j\bar{s}_j\log\bar{u}_j.$$

Now since each $\bar{s}_j$ appearing here is a non-constant *monomial* in $Y_1, ..., Y_n, \bar{\tau}_1, ..., \bar{\tau}_i$ (by 2.2), and each $\bar{u}_j$ is a positive prime integer (by 4.3(a)) and the logarithms of primes are linearly independent over $\mathbb{Z}$, the above equality can only hold if $\bar{s}_{i+1} = \bar{s}_j$ and $\bar{u}_{i+1} = \bar{u}_j$ for some $j \le i$ ($j \in V_0$). But then we would have (again using the algebraic independence of $\mathcal{A}$) EXP* $\vdash q_{i+1} = q_j \wedge p_{i+1} = p_j$ which is impossible by 2.5.

(b) $\bar{u}_{i+1} = Y_{j_0}$ for some $j_0 \in \mathbb{N}$, $j_0 \le i$. Then (***) gives

$$m\bar{s}_{i+1} = m_{j_0} + \sum_{\nu\in V_1^{j_0}} l_\nu\bar{s}_\nu.$$

As above, this easily implies $\bar{s}_{i+1} = \bar{s}_\nu$ for some $\nu \le i$ ($\nu \in V_1^{j_0}$), which is impossible (by 2.5) since $\bar{u}_{i+1} = \bar{u}_\nu$ ($= Y_{j_0}$ by definition of $V_1^{j_0}$).

(c) $\bar{u}_{i+1} = \bar{u}_{j_0}$ for some $j_0 \in V_2$, $j_0 \le i$. Then (***) gives

$$m\bar{s}_{i+1} = k_{j_0} + \sum_{\nu\in V_2^{j_0}} l_\nu\bar{s}_\nu.$$

Again, by a similar argument to the above this contradicts 2.5 (using the definition of $V_2^{j_0}$).

Thus we have shown that $\bar{\tau}_{i+1}$ is transcendental over F_i as required to complete the proof of theorem 4.4. □

5

We now complete the

5.1 **Proof of theorem 1.9**

Let f, g be terms of L, with variables amongst $y_1, ..., y_n$, say, such that $\mathbb{N} \models f = g$. Then, as already remarked at the end of section 2, we have $\mathbb{R}^+ \models f = g$. Let ρ_f, ρ_g be as given by theorem 2.8, i.e. EXP* $\vdash f = t_{\rho_f}(y_1, ..., y_n, \tau_1, ..., \tau_m)$ and EXP* $\vdash g = t_{\rho_g}(y_1, ..., y_n, \tau_1, ..., \tau_{m'})$ where $\rho_f \in \mathcal{P}_{n+m}$, $\rho_g \in \mathcal{P}_{n+m'}$ are strictly positive polynomials and $m, m' \in \omega$.

Since $\mathbb{R}^+ \models$ EXP* it follows that $\mathbb{R}^+ \models t_{\rho_f}(y_1, ..., y_n, \tau_1, ..., \tau_m) = t_{\rho_g}(y_1, ..., y_n, \tau_1, ..., \tau_{m'})$ and so, in particular, $\bar{\bar{t}}_{\rho_f}(Y_1, ..., Y_n, \bar{\tau}_1, ..., \bar{\tau}_m) = \bar{\bar{t}}_{\rho_g}(Y_1, ..., Y_n, \bar{\tau}_1, ..., \bar{\tau}_{m'})$. However, by theorem 4.4 (and the definition of F_0) $Y_1, ..., Y_n, \bar{\tau}_1, ..., \bar{\tau}_{m'}$ are algebraically independent (over $\mathbb{R}$) functions, so $\mathbb{R}^+ \models t_{\rho_f} = t_{\rho_g}$. Therefore EXP* $\vdash t_{\rho_f} = t_{\rho_g}$ (such an equation was included in EXP* as an axiom) and hence EXP* $\vdash t_{\rho_f}(y_1, ..., y_n, \tau_1, ..., \tau_m) = t_{\rho_g}(y_1, ..., y_n, \tau_1, ..., \tau_{m'})$, and therefore EXP* $\vdash f = g$ as required. □

6

We now show that we cannot replace EXP* by EXP in theorem 1.9 by showing that EXP $\nvdash f_0 = g_0$, where f_0, g_0 were introduced in section 1.

6.1 We first compute a representation for f_0 (as a "polynomial" in the τ_i's). To simplify matters we assume the sequence of p's and q's (as defined in section 2) begins as follows (we write x for y_1 and y for y_2— so we are in the case $n = 2$):-

$$\begin{aligned}
p_1 &= t_\rho(x) \ \ \text{(where } \rho \text{ is the positive polynomial } \ r \mapsto r^2 - r + 1),\\
q_1 &= y; \ \ p_2 = (x+1), \ q_2 = x; \ \ \rho_3 = (x^2+x+1), \ q_3 = x;\\
p_4 &= (x_2 + x_3), \ q_4 = y; \ \ p_5 = (x+1), \ q_5 = y; \ \ p_6 = (x^2+x+1), \ q_6 = y;\\
p_7 &= (x_5 + x_6), \ q_7 = x; \ \ p_8 = x_1, \ q_8 = x.
\end{aligned}$$

Clearly we can continue this sequence so that the conditions 2.2–2.5 are met.

Computing u's, s's and τ's we get:-

$$\begin{aligned}
u_1 &= t_\rho(x), \ s_1 = y, \ \tau_1 = t_\rho(x)^y; \ \ u_2 = (x+1), \ s_2 = x, \ \tau_2 = (x+1)^x\\
u_3 &= (x^2+x+1), \ s_3 = x, \ \tau_3 = (x^2+x+1)^x; \ \ u_4 = (\tau_2 + \tau_3) =\\
&= ((x+1)^x + (x^2+x+1)^x), \ s_4 = y, \ \tau_4 = ((x+1)^x + (x^2+x+1)^x)^y;\\
u_5 &= (x+1), \ s_5 = y, \ \tau_5 = (x+1)^y; \ \ u_6 = (x^2+x+1), \ s_6 = y,\\
\tau_6 &= (x^2+x+1)^y; \ \ u_7 = (\tau_5 + \tau_6) = ((x+1)^y + (x^2+x+1)^y), \ s_7 = x,\\
\tau_7 &= ((x+1)^y + (x^2+x+1)^y)^x; \ \ u_8 = \tau_1 = t_\rho(x)^y, \ s_8 = x,\\
\tau_8 &= (t_\rho(x)^y)^x.
\end{aligned}$$

Now

$$\begin{aligned}
f_0 &= ((x+1)^x + (x^2+x+1)^x)^y((x^3+1)^y + (x^4+x^2+1)^y)^x\\
&= \text{(in EXP}^*\text{)} \ \ ((x+1)^x + (x^2+x+1)^x)^y((x+1)^y + (x^2+x+1)^y)^x(t_\rho(x)^y)^x\\
&= \tau_4\tau_7\tau_8.
\end{aligned}$$

Thus the representing polynomial, ρ_{f_0} given by theorem 2.8 is the 10-variable ($= 2 + 8$) polynomial defined by $(r_1, r_2, ..., r_{10}) \mapsto r_6 r_9 r_{10}$ (and theorem 4.4 tells us that it is essentially unique).

6.2 It seems rather difficult to construct a model of EXP in which $f_0 = g_0$ is false, so we resort to proof theory.

Let EXP^- denote EXP without axiom 1.8, and for $k \in \mathbb{N}$, let $\mathbf{k}$ denote the term $(...\underbrace{((1+1)+1)+\cdots+1}_{k \ 1's})$.

6.3 **Lemma**

(i) If $m, r, k \in \mathbb{N}$ and $m = \mathbf{r}^k$, then EXP$^-$ $\vdash \mathbf{m} = \mathbf{r}^{\mathbf{k}}$.

(ii) If f is any term of L and $k \in \mathbb{N}$ and $\mathbb{N} \models f = \mathbf{k}$, then EXP$^-$ $\vdash f = \mathbf{k}$.

(iii) For f, g, h terms of L, and $k \in \mathbb{N}$, if either $\mathbb{N} \models f = \mathbf{k}$ or $\mathbb{N} \models g = \mathbf{k}$ or $\mathbb{N} \models h = 1$, then $\mathrm{EXP}^- \vdash (h^g)^f = h^{(g \cdot f)}$.

Proof

(i) By induction on k. For $k = 1$, $m = r$ and $\mathrm{EXP}^- \vdash \mathbf{r} = \mathbf{r}^{\mathbf{1}}$ by 1.5(i). Suppose $m = r^{(k+1)}$. Let $p = r^k$. Then, working in EXP^-

$$\begin{aligned} \mathbf{r}^{\mathbf{k+1}} &= \mathbf{r}^{\mathbf{k}} \cdot \mathbf{r}^{\mathbf{1}} \quad \text{(by 1.7)} \\ &= \mathbf{p} \cdot \mathbf{r} \quad \text{(by inductive hypothesis, and 1.5(i))} \\ &= \mathbf{m} \quad \text{(easily, using 1.1–1.4).} \end{aligned}$$

(ii) By induction on f. The result is trivial if $f = 1$ or a variable.

Suppose $\mathbb{N} \models (f \Box g) = \mathbf{k}$, where $\Box$ is $+$ or $\cdot$.

Then $\mathbb{N} \models f = \mathbf{m}$ and $\mathbb{N} \models g = \mathbf{r}$ for some $m, r \in \mathbb{N}$ s.th. $m \Box r = k$.

(This clearly follows from results in [ ].)

Therefore $\mathrm{EXP}^- \vdash f = \mathbf{m}$ and $\mathrm{EXP}^- \vdash g = \mathbf{r}$, by the inductive hypothesis.

Hence

$$\begin{aligned} \mathrm{EXP}^- \vdash (f \Box g) &= (\mathbf{m} \Box \mathbf{r}) \\ &= \mathbf{k} \quad \text{(using 1.1–1.4).} \end{aligned}$$

Suppose $\mathbb{N} \models f^g = \mathbf{k}$. Then either $\mathbb{N} \models f = \mathbf{r}$ and $\mathbb{N} \models g = \mathbf{m}$ for some $r, m \in \mathbb{N}$ s.th. $k = r^m$ (again by [ ]), in which case $\mathrm{EXP}^- \vdash f = \mathbf{r}$ and $\mathrm{EXP}^- \vdash g = \mathbf{m}$ (by the inductive hypothesis), so

$$\begin{aligned} \mathrm{EXP}^- \vdash f^q &= \mathbf{r}^{\mathbf{m}} \\ &= \mathbf{k} \text{ (by 1.5(ii)).} \end{aligned}$$

(iii) We do the case $\mathbb{N} \models g = \mathbf{k}$ and leave the others as exercises. The proof is by induction on k. If $k = 1$, then $\mathbb{N} \models g = 1$ so $\mathrm{EXP}^- \vdash g = 1$ (by (ii)). Thus, working in EXP^- we have $h^g = h^1 = h$ (by 1.5(i)), so $(h^g)^f = h^f$. Further $(g \cdot f) = (1 \cdot f) = f$ (by 1.4), so $h^{(g \cdot f)} = h^f$, as required.

Now suppose $\mathbb{N} \models g = \mathbf{k+1}$. Then $\mathrm{EXP}^- \vdash g = \mathbf{k+1}$ by (ii), so working in EXP^- we have

$$\begin{aligned} H^g = h^{\mathbf{k+1}} &= h^{\mathbf{k}} \cdot h^{\mathbf{1}} \quad \text{(by 1.7)} \\ &= h^{\mathbf{k}} \cdot h \quad \text{(by 1.5 (i)).} \end{aligned}$$

Hence

$$\begin{aligned} (h^g)^f = (h^{\mathbf{k}} \cdot h)^f &= (h^{\mathbf{k}})^f \cdot h^f \quad \text{(by 1.6)} \\ &= h^{(\mathbf{k} \cdot f)} \cdot h^f \quad \text{(by the inductive hypothesis)} \\ &= h^{((\mathbf{k} \cdot f) + f)} \quad \text{(by 1.7)} \\ &= h^{((\mathbf{k}+1) \cdot f)} \quad \text{(using 1.1–1.4)} \\ &= h^{(g \cdot f)} \quad \text{as required.} \end{aligned}$$

□

6.4 We must now be more precise about formal proofs.

We regard a proof, $\mathcal{I}$, to be a finite tree (with unique minimum element) each node of which is labelled with an equation of L. Maximal nodes are labelled with instances of an axiom (of EXP or EXP$^-$, depending on the system under consideration) or an equation of the form $f = f$. The rules are as follows:-

$$(=C) \quad \begin{array}{c} f = g \\ | \\ g = f \end{array} \ , \quad (=T) \quad \begin{array}{c} f = g \quad g = h \\ \diagdown\!\diagup \\ f = h \end{array} \ , \quad (+I) \quad \begin{array}{c} f_1 = f_2 \qquad\qquad g_1 = g_2 \\ \diagdown\!\diagup \\ (f_1 + g_1) = (f_2 + g_2) \end{array} \ ,$$

$$(\cdot I) \quad \begin{array}{c} f_1 = f_2 \qquad\qquad g_1 = g_2 \\ \diagdown\!\diagup \\ (f_1 \cdot g_1) = (f_2 \cdot g_2) \end{array} \ , \quad (EI) \quad \begin{array}{c} f_1 = f_2 \qquad g_1 = g_2 \\ \diagdown\!\diagup \\ f_1^{g_1} = f_2^{g_2} \end{array} \ ,$$

We call a use of the rule EI above, *improper*, if $\mathbb{N} \models f_1 = 1$.

We call a maximal node (and its label) of a proof, $\mathcal{I}$, *proper* if no improper use of EI lies below it in $\mathcal{I}$.

If u, f are terms of L we define the notion u *occurs properly in* f by induction on f as follows:
u occurs properly in 1 iff $u = 1$; u occurs properly in a variable z iff $u = z$; u occurs properly in $(f \square g)$ (where $\square = +$ or $\cdot$) iff $u = (f \square g)$ or u occurs properly in f or u occurs properly in g; u occurs properly in f^g iff not $\mathbb{N} \models f = 1$ and $u = f^g$ or u occurs properly in f or u occurs properly in g.

The following lemma is easily established by induction on height of proof.

6.5 **Lemma**

Suppose $\mathcal{I}$ is a proof of the equation (of L) $f = g$. Suppose further that $e = h$ is the label of some proper maximal node of $\mathcal{I}$. Then there is a term f^* of L such that $\mathbb{N} \models f = f^*$ and either $\mathbb{N} \models e = 1$ or e occurs properly in f^*. $\square$

6.6 **Lemma**

Let $u = u(x, y)$, $f = f(x, y)$ be terms of L in two variables x, y (for simplicity - it's the only case we will need). Then

(i) $\forall m_1, m_2 \in \mathbb{N} \smallsetminus \{1\}$, $\overline{\overline{f}}(m_1, m_2) \geq 2$, provided not $\mathbb{N} \models f = 1$.

(ii) $\exists i \in \{1, 2\}$ such that $\forall m_1, m_2 \in \mathbb{N} \smallsetminus \{1\}$, $\overline{\overline{f}}(m_1, m_2) \geq m_i$, provided $\overline{\overline{f}}$ is not constant.

(iii) Suppose further that u occurs properly in f and $\overline{\overline{u}}$ is non-constant. Then either (a) $\exists i \in \{1, 2\}$ such that for all sufficiently large $m_1, m_2 \in \mathbb{N}$, $\overline{\overline{f}}(m_1, m_2) \geq \overline{\overline{u}}(m_1, m_2)^{\sqrt{m_i}}$ or (b) there are terms v, h such that either $\mathbb{N} \models f = (v \cdot u) + h$ or $\mathbb{N} \models f = v \cdot u$.

Proof

(i) and (ii) are easy by induction on f, so are left to the reader. (iii) is also proved by induction on f. Clearly (b) holds if $f = x$ or $f = y$ or $f = 1$.

If u occurs properly in $f \Box g$ ($\Box = +$ or $\cdot$), then either $u = f \Box g$, in which case (b) holds, or u occurs properly in f or in g, say, without loss of generality, that u occurs properly in f. But if either (a) or (b) holds for f, then clearly the same holds for $f \Box g$.

Now suppose u occurs properly in f^g. Then not $\mathbb{N} \models f = 1$. If $u = f^g$, then case (b) holds. Suppose u occurs properly in f. If (a) holds for f it clearly also holds for f^g. If (b) holds for f then it also holds for f^g if $\overline{\overline{g}}$ is constant; if $\overline{\overline{g}}$ is not constant then clearly (a) holds for f^g by (ii).

Suppose finally that u occurs properly in g. Since not $\mathbb{N} \models f = 1$ we have by (i), $\forall m_1, m_2 \in \mathbb{N} \smallsetminus \{1\}$, $\overline{\overline{f}}(m_1, m_2)^{\overline{\overline{g}}(m_1,m_2)} \geq 2^{\overline{\overline{g}}(m_1,m_2)}$, hence if (a) holds for g it also holds for f^g. If (b) holds for g, then $\forall m_1, m_2 \in \mathbb{N} \smallsetminus \{1\}$, $\overline{\overline{g}}(m_1, m_2) \geq \overline{\overline{u}}(m_1, m_2)$, hence $\overline{\overline{f^g}}(m_1, m_2) \geq 2^{\overline{\overline{u}}(m_1,m_2)}$ and $2^{\overline{\overline{u}}(m_1,m_2)} \geq \overline{\overline{u}}(m_1, m_2)^{\sqrt{m_i}}$ for some $i \in \{1, 2\}$ and sufficiently large $m_1, m_2 \in \mathbb{N}$ by (ii), since $\overline{\overline{u}}$ is not constant. □

6.7 **Lemma**

Suppose $f = f(x, y)$ is a term of L and $\overline{\overline{f}}(1, 2) = 1$. Then for some term g of L, $\mathbb{N} \models f = x^g$ or $\mathbb{N} \models f = 1$.

Proof

By induction on f. The lemma is clearly true for $f = 1$ or $f = x$, or $f = y$. The induction step is also clear since for any terms u, v, $(\overline{\overline{u \cdot v}})(1, 2) = 1$ implies $\overline{\overline{u}}(1, 2) = 1$ and $\overline{\overline{v}}(1, 2) = 1$, $(\overline{\overline{u + v}})(1, 2) \neq 1$ and $\overline{\overline{u^v}}(1, 2) = 1 \Rightarrow \overline{\overline{u}}(1, 2) = 1$. □

6.8 **Corollary**

For no term $f = f(x, y)$ of L do we have $\forall m_1, m_2 \in \mathbb{N}$, $\overline{\overline{f}}(m_1, m_2) = (m_1^2 - m_1 + 1)^{m_1 m_2}$.

Proof

If f were such a term then since $\overline{\overline{f}}(1, 2) = 1$, there would be a term g such that $\mathbb{N} \models f = x^g$ (by 6.7). But then $\overline{\overline{f}}(2, 1) = 2^{\overline{\overline{g}}(2,1)}$, and also $\overline{\overline{f}}(2, 1) = (2^2 - 2 + 1)^2 = 3^2$, which is impossible. □

6.9 **Lemma**

Suppose $\mathrm{EXP} \vdash f_0 = g_0$ (with f_0, g_0 as defined in section 1). Then $\mathrm{EXP}^- \vdash f_0 = g_0$.

Proof

Let $\mathcal{I}$ be a proof of $f_0 = g_0$ from EXP. We modify $\mathcal{I}$, to get a proof $\mathcal{I}^*$, as follows.

(a) For each occurrence of an equation of the form $f_1^{g_1} = f_2^{g_2}$ with $\mathbb{N} \models f_1 = 1$, delete everything above this occurrence in $\mathcal{I}$ and replace it with a proof from EXP^- of $f_1^{g_1} = f_2^{g_2}$. This is clearly possible by 6.3(ii) (with $k = 1$) and uses of axiom 1.5(ii) and the rule EI.

(b) For each occurrence of an equation of the form $(f^g)^h = f^{g \cdot h)}$ appearing on a maximal node where either $\overline{\overline{g}}$ is constant, or $\overline{\overline{h}}$ is constant or $\overline{\overline{f}}$ is identically 1, precede this node with a proof of $(f^g)^h = f^{(g \cdot h)}$ from EXP$^-$. This is possible by 6.3(iii).

I now claim that no instance of 1.8 occurs on a maximal node (i.e. as an axiom) of $\mathcal{I}^*$ — which clearly establishes 6.9.

For suppose $(f^g)^h = f^{(g \cdot h)}$ is such an instance. By (a) the node on which this equation occurs is proper. Also, by (b), not $\mathbb{N} \models f = 1$, therefore not $\mathbb{N} \models (f^g)^h = 1$ and so, by 6.5, there is a term f^* such that $\mathbb{N} \models f^* = f_0$ and $(f^g)^h$ occurs properly in f^*. But by (b), neither g nor h are constant, and not $\mathbb{N} \models f = 1$. Therefore $\exists i, j \in \{1,2\}$, $\forall m_1, m_2 \in \mathbb{N} \setminus \{1\}$, $\overline{\overline{(f^g)^h}}(m_1, m_2) \geq 2^{m_i m_j}$ (by 6.6(i) and (ii)). Also

$$\begin{aligned} \overline{\overline{f}}^*(m_1, m_2) &= \overline{\overline{f}}_0(m_1, m_2) \\ &= ((m_1+1)^{m_1} + (m_1^2 + m_1 + 1)^{m_1})^{m_2}((m_1^3+1)^{m_2} + (m_1^4 + m_1^2 + 1)^{m_2})^{m_1} \\ &\leq (25m_1^4)^{m_1 m_2} \quad \forall m_1, m_2 \in \mathbb{N}, \end{aligned}$$

and for no $k \in \{1,2\}$ do we have $(25m_1^4)^{m_1 m_2} \geq 2^{m_1 m_j \sqrt{m_k}}$ holding for sufficiently large $m_1, m_2 \in \mathbb{N}$.

Thus, by 6.6(iii), there are terms v, h such that either $\mathbb{N} \models f^* = (v \cdot u) + h$ or $\mathbb{N} \models f^* = v \cdot u$, where $u = (f^g)^h$.

Now consider the polynomials in the τ_i's which represent v and h (as given by 2.8). Since $\mathbb{N} \models f^* = \tau_4 \tau_7 \tau_8$ (by the computation of 6.1) and the polynomial representing $(v \cdot u) + h$ cannot be a monomial with coefficient 1, $\mathbb{N} \models f^* = (v \cdot u) + h$ is impossible by 4.4(I)(a), and if $\mathbb{N} \models f^* = v \cdot u$, then by 6.8 we must have $\mathbb{N} \models u = \tau_4$ or $\mathbb{N} \models u = \tau_7$ or $\mathbb{N} \models u = \tau_4 \cdot \tau_8$ or $\mathbb{N} \models u = \tau_7 \cdot \tau_8$ or $\mathbb{N} \models u = \tau_4 \cdot \tau_7 \cdot \tau_8$, (since $\overline{\overline{\tau}}_8 \neq \overline{\overline{g}}$ for any term g of L).

However, $\overline{\overline{u}}(2,2) = \overline{\overline{(f^g)^h}}(2,2) = k^4$ for some $k \in \mathbb{N} \setminus \{1\}$, by 6.6 (i) Also $\overline{\overline{\tau}}_4(2,2) = 58^2$, $\overline{\overline{\tau}}_7(2,2) = 58^2$, $\overline{\overline{\tau_4 \cdot \tau_8}}(2,2) = 58^2 {\cdot} 3^4$, $\overline{\overline{\tau_7 \cdot \tau_8}}(2,2) = 58^2 {\cdot} 3^4$, none of which are fourth powers, so $\mathbb{N} \models (f^g)^h = f_0$. However $\overline{\overline{(f^g)^h}}(2,3)$ is also a fourth power (by the same argument), whereas $\overline{\overline{f}}_0(2,3) = 58^3 \cdot (370)^2 \cdot 3^6$ is not. This contradiction completes the proof. □

Remark: We have tacitly assumed above that all formulas mentioned have just the two variables x, y. This is justified since in any proof of $f_0 = g_0$ we can equate all other variables to 1. Further, all the results in this section could have been proved assuming L contained only these two variables.

We now come to the main result of this section.

6.10 **Theorem**

$$\text{EXP} \nvdash f_0 = g_0$$

Proof

By 6.9 it is sufficient to find a model $\mathcal{G}$ of EXP$^-$ such that $\mathcal{G} \models \exists x \exists y f_0(x,y) \neq g_0(x,y)$.

We let the domain of $\mathcal{G}$ be $\mathbb{N}[z]$ = all polynomials with coefficients in $\mathbb{N}$, in the one indeterminate z. Let $1, +, \cdot$ have their natural interpretation on $\mathbb{N}[z]$ (so that 1.1–1.4 are clearly satisfied), and we define exponentiation, as follows.

For $p(z) \in \mathbb{N}[z]$, $p(z)^m = \underbrace{p(z) \cdot p(z) \cdots p(z)}_{m \text{ times}}$ for $m \in \mathbb{N}$;

$$\begin{aligned}
p(z)^z &= \begin{cases} z^k & \text{if } k \in \mathbb{N} \text{ and } (z^2-z+1)^k | p(z), \quad (z^2-z+1)^{k+1} \nmid p(z), \\ 1 & \text{if no such } k \in \mathbb{N} \text{ exists} \end{cases} \\
p(z)^{z^2} &= \begin{cases} (z+1)^k & \text{if } k \in \mathbb{N} \text{ and } z^k | p(z), \quad z^{k+1} \nmid p(z), \\ 1 & \text{if no such } k \in \mathbb{N} \text{ exists} \end{cases} \\
p(z)^{z^m} &= 1 \text{ for } m \geq 2, \ m \in \mathbb{N}; \quad p(z)^{\sum_{i=0}^m a_i z^i} = \prod_{i=0}^m (p(z)^{z^i})^{a_i}
\end{aligned}$$

for $a_0, a_1, .., a_m \in \omega$, where we have made the convention here that $t^0 = 1$. Clearly (1.1)–(1.7) are satisfied with this definition of exponentiation, so $\mathcal{G} \models \mathrm{EXP}^-$. However, $f_0^{\mathcal{G}}[z, z^2] = 1$ and $g_0^{\mathcal{G}}[z, z^2] = z + 1$. □

References

1. A.J. Macintyre, The laws of exponentiation, in ‘Model theory and arithmetic’, ed. Berline, McAloon and Ressayre, Springer Lecture Notes 890 (1981), pp. 185–197.

2. M. Rosenlicht, Differential extension fields of exponential type, Pacific J. Math. Vol. 57, No. 1 (1975), pp. 289–300.

A.J. Wilkie
Mathematical Institute
24-29 St Giles’
Oxford OX1 3LB
UK
wilkie@maths.ox.ac.uk