RAIRO. INFORMATIQUE THÉORIQUE ET APPLICATIONS

PIERPAOLO DEGANO
PATRIZIA GIANNI

A normal form for restricted exponential functions

RAIRO. Informatique théorique et applications, tome 23, n° 2 (1989), p. 217-231

<http://www.numdam.org/item?id=ITA_1989__23_2_217_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 23, n° 2, 1989, p. 217 à 231)

A NORMAL FORM FOR RESTRICTED EXPONENTIAL FUNCTIONS (*)

by Pierpaolo DEGANO (1) and Patrizia GIANNI (2)

Communicated by G. LONGO

Abstract. – *A first order theory* **G** *is defined, the terms of which, roughly speaking, can be built as linear combination of "towers of simple exponentiations" with polynomial coefficients. A term rewriting system* $\mathfrak{R}$ *is introduced, which converts every term of* **G** *to its normal form* $\mathfrak{R}$ *can be run as it is on a computer in order to solve the identity problem for a subsystem of* $E=\langle N_+, +, \times, \exp, 1\rangle$. *This is done by showing that two terms in* **G** *are identical if and only if they have the same normal form with respect to* $\mathfrak{R}$.

Résumé. – *On définit une théorie du premier ordre* **G**, *dont les termes, de façon informelle, peuvent être construits comme combinaison linéaire de « tours de simples exponentielles » à coefficients polynomiaux. On introduit un système de réécriture de termes* $\mathfrak{R}$ *qui transforme chaque terme de* **G** *dans sa forme normale. On peut implanter* $\mathfrak{R}$ *sur un ordinateur pour résoudre le problème de l'identité pour un sous-système de* $E=\langle N_+, +, \times, \exp, 1\rangle$. *Pour cela on montre que deux termes de* **G** *sont identiques si et seulement si ont la même forme normale par rapport à* $\mathfrak{R}$.

1. INTRODUCTION

In what follows we assume the reader is familiar with the basic notions and results of equational theories and term rewriting systems, referring to Huet and Oppen (1980) and to Tarski (1968) for detailed surveys.

By the *equational theory* of the system $E=\langle N_+, +, \times, \exp, 1\rangle$ we understand the set **T** of all equations which are identically satisfied in **E**. More precisely, if σ and τ are terms in a first order theory of E, we say that σ and τ are *identical* ($\sigma \equiv \tau$) if and only if σ and τ have the same value in E, for every substitution of values in N_+ for all the variables occuring in them.

(*) Received May 1985, accepted February 1988.
(1) Dipartimento di Informatica, Università di Pisa, Italy.
(2) Dipartimento di Matematica, Università di Pisa, Italy.

Informatique théorique et Applications/Theoretical Informatics and Applications
0296-1598 89/02 217 15/$3.50/

The set of identities of **T** has been proved to be recursive by Macintyre (1981).

Tarski (1968) raised the question whether or not the following finite set of axioms stating identities in $\boldsymbol{E}$:

$$\Delta = \{ (x+y=y+x),\ (x \times y = y \times x),\ (x+(y+z)=(x+y)+z),$$
$$(x \times (y \times z)=(x \times y) \times z),\ (x \times (y+z)=x \times y + x \times z),$$
$$(x \exp (y+z)=(x \exp y) \times (x \exp z)),$$
$$((x \exp y) \exp z = x \exp (y \times z)),$$
$$((x \times y) \exp z=(x \exp z) \times (y \exp z)),$$
$$(x \times 1 = x),\ (x \exp 1 = x),\ (1 \exp x = 1)\}$$

is a *base* for **T**, *i.e.* if all and only the identities of **T** can be derived from Δ (needless to say, the symbols in Δ have the standard interpretation in $\boldsymbol{E}$).

Wilkie (1984), within proof theory, has shown that Δ is not a base for **T**; a further negative result, due to Martin (1973), is that there is no finite base for the equatorial theory of $\langle N, +, \times, \exp \rangle$.

However, it is possible to obtain from Δ bases for the equatorial theory of the polynomials with integer coefficients, for the equatorial theory of $\langle N, \times, \exp \rangle$ and for that of $\langle N, \exp \rangle$ (Martin, 1973).

In this paper we define a subtheory **V** of **T**, the terms of which belong to the first order theory **G**. Roughly speaking, the elements of **G** are those terms that can be built as linear combination with polynomial coefficients of "towers of simple exponentiations". In other words, we do not allow in **G** any term to have polynomials involved in the operation of exponentiation.

The identity problem for **V** is solved by deriving from Δ a term rewriting system $\mathfrak{R}$ which converts every term σ of **G** to a *unique* term $\sigma\hat{}$ (*normal form*) such that $\sigma \equiv \sigma\hat{}$. The identity problem for **V** is reduced to show that, for every pair of terms $\sigma, \tau \in \mathbf{G}$, $\sigma \equiv \tau$ if and only if they have the same normal form ($\sigma\hat{} = \tau\hat{}$). While solving the identity problem for **V** in this framework, we also construct an effective simplification procedure to compute the normal form of every term of **G**.

We remark that our equational theory **V** is contained in the subtheory of **T** defined by Henson and Rubel (1984), which state the existence of a formal proof of the equality $\sigma = \tau$ from Δ and $\sigma \equiv \tau$. In spite of the loss of generality, we claim that our use of rewriting system techniques makes identity checking much simpler and more easily manageable by a computer. Indeed, it is not evident how to transform a set of equalities, as presented by Henson and

Rubel (1984), into a program. We construct a term rewriting system $\mathfrak{R}$ which is in fact a program that can be run on a computer, provided that a commutative-associative matching procedure is available (Peterson and Stickel, 1981).

As a final remark, we note that the class of terms to which our method is applicable could be extended by defining a sort of "pre-processing" that reduces a term to a product of terms in **G** following the guidelines of Henson and Rubel (1984). In general, however, this pre-processing cannot be handled by rewriting techniques alone.

NOTATION

We will use the following notations:

- N(N_+ resp.) denote the non-negative (positive resp.) integers;
- m stands for the term $\underbrace{((\ldots((1+1)+1)\ldots)+1)}_{m \text{ times}}$;
- $\# S$ stands for the cardinality of set S;
- let $I=(i_1, \ldots, i_n)\in N^n$, then $I>0$ if there exists a k, $1\leqq k\leqq n$, such that $i_k>0$;
- let $\{x_i\}$ be a set of variable symbols, $j\in N$ and $I=(i_1, \ldots, i_n)\in N^n$, then
  - $x_i x_j$ denotes as usual $x_i \times x_j$;
  - $x_i^j=\underbrace{x_i \ldots x_i}_{j \text{ times}}$ if $j>0$, and $x_1^j=1$ if $j=0$;
  - $x_i^{x_j}$ denotes x_i exp x_j;
  - $X=(x_1, \ldots, x_n)$;
  - $X^I=x_1^{i_1}\ldots x_n^{i_n}$;
- $A(n)$ denotes the set of analytic functions depending on n variables;
- $N_+[X]=\{\Sigma_I a_I X^I \mid a_I\in N_+,\ I\in N^n\}$ denotes the polynomials in n variables;
- given a term rewriting system defining a relation $\rightarrow$,
  - $\rightarrow^*$ denotes the reflexive, transitive closure of $\rightarrow$;
  - $\sigma\hat{}$ denotes the normal form of σ;
- formal terms in theories will be written in Roman, objects in systems in *Italic* style; formal equality will be rendered as $=$, identity by $\equiv$.

2. A CLASS OF RESTRICTED EXPONENTIALS

In order to define the set **G** containing the formal terms of the equational theory **V**, we need the following preliminary definitions.

DEFINITION 2.1: An element $p \in A(n)$ satisfies condition G if either condition holds

(1) either $p \in N_+$, or p is written as X^I, $I \geqq 0$, or

(2) p is written as b^m, where b satisfies (1) and m satisfies G.

Let $\mathbf{P} = \bigcup_{n \in N} \{ p \in A(n) \setminus N_+ \mid p \text{ satifies } G \} \cup \{1\}$.

Example 2.1:

$$3^{(xy^2)^{7z^5}},\ 3^{2^x}$$

are elements of **P**, while

$$3^{(x+y)^z},\ 3^x 3^x,\ (x^x y)^x$$

are not elements of **P**.

DEFINITION 2.2: Let $\mathbf{G} = \{ \sum_i a_i p_i \mid a_i \in N_+[x_1, \ldots, x_n] \text{ and } p_i \in \mathbf{P} \}$.

Example 2.2:

$$(x+2y+z^2)+3^{(xy^2)^{7z^5}}+(xyz^2+4)3^{2^x}+11$$

is in **G**.

We can now introduce the term rewriting system $\mathfrak{R}$ giving normal forms to **G**, up to commutativity and associativity. $\mathfrak{R}$ consists of two sets: the first contains the equations which formally express the commutativity and associativity of addition and multiplication (represented by $+$ and $\times$, respectively) and define the decidable congruence **ca**; the second set consists of the rewrite rules modulo **ca**.

EQUATIONS OF $\mathfrak{R}$

$$E_1.\ \sigma+\tau=\tau+\sigma, \qquad E_2.\ \sigma\times\tau=\tau\times\sigma$$
$$E_3.\ (\sigma+\tau)+\rho=\sigma+(\tau+\rho), \qquad E_4.\ (\sigma\times\tau)\times\rho=\sigma\times(\tau+\rho).$$

RULES OF $\mathfrak{R}$

$$R_1.\ [1\times\tau]_{ca}\to[\tau]_{ca}$$
$$R_2.\ [1\ \exp\ \tau]_{ca}\to[1]_{ca}$$
$$R_3.\ [\tau\ \exp\ 1]_{ca}\to[\tau]_{ca}$$
$$R_4.\ [\sigma\times(\tau+\rho)]_{ca}\to[(\sigma\times\tau)+(\sigma\times\rho)]_{ca}$$
$$R_5.\ [(\tau\ \exp\ \sigma)\times(\rho\ \exp\ \sigma)]_{ca}\to[(\tau\times\rho)\ \exp\ \sigma]_{ca}$$
$$R_6.\ [(\tau\ \exp\ \sigma)\ \exp\ \rho]_{ca}\to[\tau\ \exp\ (\sigma\times\rho)]_{ca}.$$

The equations and rules of $\mathfrak{R}$ can be directly obtained from the equations of Δ, and we will prove that they provide a *sum-of-products-of-exponentials* normal form to the terms of **G**. Before giving the main result, we need to ensure that all the terms of **G** have an irreducible form (*i.e.* they cannot be further rewritten by any rule in $\mathfrak{R}$), and to relate the set of these irreducible forms to **G** itself.

LEMMA 2.1: $\mathfrak{R}$ *is noetherian.*

Proof: This proof is based on a refinement of a well-founded ordering on terms given in Lankford (1979). We define a mapping W from the set of terms to a set that is well-ordered by a relation $\geqslant$, and we prove that, for any substitution of terms for variables:

(*a*) of each equation $\sigma=\tau$ of $\mathfrak{R}$, we have $W(\sigma)=W(\tau)$;

(*b*) of each rule $\sigma\to\tau$ of $\mathfrak{R}$, we have $W(\sigma)\geqslant W(\tau)$.

Definition of W: Let

$F=\{\ \mathbf{f}:(N_+\setminus\{1\})^n\to N_+\setminus\{1\}\mid n\in N_+$ and **f** is construted by using the functions of addition, multiplication and exponentiation $\}$.

We first define an ordering on F as follows:

$\mathbf{f}(X)>\mathbf{g}(X)$ if and only if $\mathbf{f}(N)>\mathbf{g}(N)$, for every $N\in(N_+\setminus\{1\})^n$;

$\mathbf{f}(X)=\mathbf{g}(X)$ if and only if $\mathbf{f}(N)=\mathbf{g}(N)$, for every $N\in(N_+\setminus\{1\})^n$.

where $>$ and $=$ stand for the standard *less-than* and *equal-to* relations on N.

Then, the ordering $\gg$ on $F \times F$ in defined as the extension of $>$, by using the lexicographical ordering on $N \times N$.

Let W be the following mapping from the set $\mathbf{G}$ of formal terms except the variables to the set $\mathbf{F} \times \mathbf{F}$.

$W(\sigma) = \langle \mathbf{f}(\sigma), \mathbf{g}(\sigma) \rangle$, where $\mathbf{f}$ and $\mathbf{g}$ are recursively defined as follows:

(i) $\mathbf{f}(1) = \lambda x.2, \quad \mathbf{g}(1) = \lambda x.2$

(ii) $\mathbf{f}(+) = \lambda xy.x+y+1, \quad \mathbf{g}(+) = \lambda xy.x+y+1$

(iii) $\mathbf{f}(\times) = \lambda xy.xy, \quad \mathbf{g}(\times) = \lambda xy.xy$

(iv) $\mathbf{f}(\exp) = \lambda xy.x^y, \quad \mathbf{g}(\exp) = \lambda xy.xy+y$

The proof of items (*a*) and (*b*) above is now straigthforward. We only show two examples.

If we take E_1, we have

$W(\sigma+\tau) = W(\tau+\sigma)$, since

$$\langle \mathbf{f}(\sigma+\tau), \mathbf{g}(\sigma+\tau) \rangle = \langle \mathbf{f}(\tau+\sigma), \mathbf{g}(\tau+\sigma) \rangle$$

$$\langle \mathbf{f}(\sigma)+\mathbf{f}(\tau)+1, \mathbf{g}(\sigma)+\mathbf{g}(\tau)+1 \rangle = \langle \mathbf{f}(\tau)+\mathbf{f}(\sigma)+1, \mathbf{g}(\tau)+\mathbf{g}(\sigma)+1 \rangle$$

which holds for every value $\mathbf{f}(\sigma)$, $\mathbf{f}(\tau)$, $\mathbf{g}(\sigma)$ and $\mathbf{g}(\tau)$ can take on $N_+ \setminus \{1\}$.

If we consider R_1 instead, we have

$W(1 \times \tau) \gg W(\tau)$, being

$$\mathbf{f}(1 \times \tau) = \mathbf{f}(1) \times \mathbf{f}(\tau) = 2 \times \mathbf{f}(\tau) > \mathbf{f}(\tau).$$

Note that the use of function $\mathbf{g}$ is crucial in proving noetherianity of rules R_5 and R_6 only.

Q.E.D.

We want to focus our attention at the set of normal forms of the elements in $\mathbf{G}$. This set is contained in $A(n)$, but ve will show that $\mathbf{G}$ is closed with respect to the relation $\rightarrow^*$.

DEFINITION 2.3: Let

$$\mathbf{G}^* = \{ p \in \mathbf{G} \mid p \text{ is irreducible} \}$$

$$\bar{\mathbf{G}}^* = \{ p \in A(n) \mid p \text{ is irreducible and there exists a } q \in \mathbf{G} \text{ such that } q \rightarrow {}^*p \}.$$

Note that $\bar{\mathbf{G}}^*$ is the set of normal forms in $A(n)$ for elements of **G** and that it does contain the set of normal forms in **G**. It does not, *a priori*, contain *only* normal forms which are elements of **G**. However, this is the case, as proved by Proposition 2.1. below.

Remark 2.1:

(i) $\mathbf{P} \subset \mathbf{G}^*$;

(ii) $p \in \mathbf{G}^*$ if and only if $p = \sum_j X^{I_j} p_j + m$, where $p_j \in \mathbf{P}$ and $I_j \geqq 0$ for all j, $m \in N$.

PROPOSITION 2.1: **G** is closed under the relation $\rightarrow^*$ induced by $\mathfrak{R}$.

Proof: Let $q \in \mathbf{G}$, by Definition 2.2 we have $q = \sum_i a_i b_i^{m_i}$, with $a_i \in N_+[x_1, \ldots, x_n]$. Every element of **P** is irreducible, hence we could apply $\mathbf{R}_1$ and $\mathbf{R}_4$ only, and obviously these rules are such that $\mathbf{G} \rightarrow^* \mathbf{G}$.

Q.E.D.

COROLLARY 2.1: $\mathbf{G}^* = \bar{\mathbf{G}}^*$.

The theorem stating that the identity problem for **V** is solvable through the rewriting system $\mathfrak{R}$ follows.

THEOREM: *For all terms* $\sigma, \tau \in \mathbf{G}$, $\sigma \equiv \tau$ *if and only if* $\sigma\hat{} = \tau\hat{}$.

Proof: The proof of the if-part is obvious, since $\mathfrak{R}$ preserves identity.

Lemma 2.1 ensures that the irreducible form of any term of **G** exists, and Corollary 2.1 that these irreducible forms are still in **G**. The proof that a term admits a unique irreducible (thus normal) form (up to the **ca** congruence) is given in the next section. It is organized as follows: first a total order is introduced on the univariate terms in order to establish the theorem in this case. Then we define suitable specializations to carry the univariate result over the multivariate one. Q.E.D.

3. PROOF OF THE THEOREM

The proof that two terms are identical only if they have the same normal form requires some preliminary definitions and results.

In what follows let $\mathbf{P}_1 = \{p \in \mathbf{P} \mid p \text{ depending on } x_1 \text{ only}\}$. For simplicity we denote x_1 by x.

We remark that $\boldsymbol{P}_1$ is contained in the class $\mathscr{L}(N)$ studied by Levitz (1975) and that Hardy (1910) defined a well-ordering on this class. In our case, the

proof of this result is much simpler and we present it to make the paper self-contained. The reader wishing to accept these results may skip to Definition 3.2.

DEFINITION 3.1: Let $p \in \mathbf{P}_1$, we call *depth* (p) the integer defined as follows:

- depth $(1) = -1$;
- depth $(x^k) = 0$, for all $k \in N_+$;
- depth $(b^m) =$ depth $(m) + 1$.

Moreover, let $\mathbf{P}^i = \{ p \in \mathbf{P}_1 \mid \text{depth}(p) = i \}$, for all $i \geqq -1$.
Note that we have $\mathbf{P}_1 = \bigcup_{i \geqq -1} \mathbf{P}^i$.

Example:

$$\text{depth}(3^{(xy^2)^{7^{z^5}}}) = 3.$$

PROPOSITION 3.1: *Let* $p \in \mathbf{P}^i$. *If* $q \in \mathbf{P}^j$ *and* $j > i$, *then* $\lim_{x \to \infty} p/q$ *exists yielding* 0.

Proof: By induction on i.

The claim is obvious when i is either -1 or 0.

Let $i > 0$, we assume $p = b^u$ and $q = c^v$, where $b, c \in N[x] \setminus \{1\}$, $u \in \mathbf{P}^{i-1}$ and $v \in \mathbf{P}^{j-1}$. Since $j > i$, by using the inductive hypothesis we have

$$\begin{aligned} \lim_{x \to \infty} \log p/q &= \lim_{x \to \infty} (u(\log b) - v(\log c)) \\ &= \lim_{x \to \infty} v((u/v)(\log b) - \log c) \\ &= -\infty. \end{aligned}$$

Q.E.D.

PROPOSITION 3.2: *Let* $p, q \in \mathbf{P}^i$, $i \geqq -1$, *then* $\lim_{x \to \infty} p/q$ *exists yielding either*

(i) $\lim_{x \to \infty} p/q = 0$ or

(ii) $\lim_{x \to \infty} p/q = 1$ or

(ii) $\lim_{x \to \infty} p/q = \infty$.

In particular, item (ii) occurs if and only if $p = q$.

Proof: By induction on i.

The claim is obvious when i is either -1 or 0.

If $i>0$, then $p=b^u$ and $q=c^v$, where $b, c \in \mathbf{N}[x] \setminus \{1\}$ and $u, v \in \mathbf{P}^{i-1}$. By inductive hypothesis, three cases may arise.

(1) $\lim_{x \to \infty} u/v=0$

(2) $\lim_{x \to \infty} u/v=1$ (*i.e.* $u=v$)

(3) $\lim_{x \to \infty} u/v=\infty$.

If (1) holds, we have

$$\lim_{x \to \infty} \log p/q = \lim_{x \to \infty} v((u/v)(\log b)-\log c)=-\infty$$

thus (i) is proved.

If (2) holds, let us consider b and c:

- if $b<c$ then (i) holds
- if $b=c$ then (ii) holds
- if $b>c$ then (iii) holds,

where $b<c$ means $\lim_{x \to \infty} b/c=0$ when $b, c \in \mathbf{N}_+$.

Case (3) is symmetric to (1).

Q.E.D.

DEFINITION 3.2: *Let $p \in \mathbf{P}^i$ and $q \in \mathbf{P}^j$, we define $p \leqq q$ if and only if either*

- *$i<j$, or*
- *$i=j=0$ and, if $p=x^k$, $q=x^h$, $k \leqq h$, or*
- *$i=j>0$ and, if $p=b^u$, $q=c^v$, either*
  - *$u<v$, or*
  - *$b \leqq c$ if $u=v$.*

We understand $p=q$ if and only if $p \leqq q$ and $q \leqq p$, and $p<q$ if and only if $p \leqq q$ and not $q \leqq p$.

Note that $p \leqq q$ if and only if $\lim_{x \to \infty} p/q$ is finite.

COROLLARY 3.1: *P_1 is totally ordered by $\leqq$.*

Now we extend the ordering $\leqq$ to irreducible terms which are products of elements of $\mathbf{P}_1$. We remark that these elements do not belong to the set $\mathbf{G}^*$, but we will need this extension later on (*see* Definition 3.5).

PROPOSITION 3.3: *Let* $p=\prod_i p_i$, $q=\prod_j q_j$, $p_i, q_j \in \mathbf{P}_1$, *p and q irreducible.*

Then $\lim_{x \to \infty} p/q$ *always exists yielding either*

(i) $\lim_{x \to \infty} p/q = 0$ *or*

(ii) $\lim_{x \to \infty} p/q = 1$ *or*

(iii) $\lim_{x \to \infty} p/q = \infty$.

We define $p \leqq q$ if and only if cases (i) or (ii) arise.

Proof: Let us consider the sets $\{p_i\}$ and $\{q_j\}$. Remark that there are no indexes k and m such that $p_k = p_m$ (resp. $q_k = q_m$) because if this were the case rule R_5 would apply contradicting the irreducibility hypothesis.

Furthermore, if we simpllify both p and q (by dividing them by the same terms) we can suppose that the sets of p_i's are either both equal to $\{1\}$, or disjoint. In the first case, obviously $p=q$ [case (ii)]. Otherwise, let us order these sets and let us call p_1 and q_1 their maxima. We define $p \leqq q$ if and only if $p_1 \leqq q_1$.

We will now prove that if $p \leqq q$ and not $q \leqq p$, then $\lim_{x \to \infty} p/q = 0$ [case (iii) is symmetric]. If $p_1 = b_1^{u_1} < c_1^{v_1} = q_1$, we have

$$\lim_{x \to \infty} \log p/q = \lim_{x \to \infty} \left(\sum_i u_i (\log b_i) - \sum_j v_j (\log c_j)\right)$$

$$= \lim_{x \to \infty} v_1 \left(\sum_i (u_i/v_1)(\log b_i) - \sum_{j>1} (v_j/v_1)(\log c_j) - \log c_1\right)$$

$$= -\infty.$$

This happens because p and q are irreducible, hence $v_j < v_1$, if $j \geqq 2$. For the same reason we can have at most $u_1 = v_1$, otherwise $b_1^{u_1} \times b_2^{u_1}$ will be reduced to $(b_1 b_2)^{u_1}$ by applying R_5. But in this case $b_1 < c_1$.

Not other case except for (i)-(iii) is possible by definition of $\leqq$.

Q.E.D.

COROLLARY 3.3: *Let* $p, q \in \{r = \sum_i \prod_k p_{ik} + n \mid r$ *is irreducible,* $p_{ik} \in \mathbf{P}_1\}$, *then we have* $p \equiv q$ *if and only if* $p = q$.

Proof (only-if pary): Because of the definition of $\mathbf{G}^*$ we can assume $p = \sum_i \prod_k p'_{ik} + n = \sum_i p_i + n$, and $q = \sum_j \prod_h q'_{jh} + m = \sum_j q_j + m$, where $m, n \in N$ and $p'_{ik}, q'_{jh} \in \mathbf{P}_1$.

Let us order the addends of p by the total ordering defined in Proposition 3.3, and let p_1 be their maximum. Furthermore, consider the following

$$\lim_{x \to \infty} \sum_j q_j/p_1 = \lim_{x \to \infty} \sum_i p_i/p_1$$

$$= \sum_{I_1} \lim_{x \to \infty} p_i/p_1 + \sum_{I_2} \lim_{x \to \infty} p_i/p_1$$

$$= \# I_1$$

where $I_1 = \{ i \in I \mid p_i = p_1 \}$ and $I_2 = I \setminus I_1$.

Hence we have that

– $q_j \leqq p_1$ for all j;

– there exists exactly $\# I_1$ indexes j_i's such that $q_{j_1} = \ldots = q_{jI_1} = p_1$.

We cross out these $\# I_1$ terms and, by iterating this process, we conclude the proof.

Q.E.D.

We now consider the general case with n variables.

DEFINITION 3.2: *Let* $p \in \mathbf{P}$, we say that $b \in N_+ \setminus \{1\}$ is a *base* for p if either condition holds

(i) $p = b^m$, $m \in \mathbf{P}$ or

(ii) $p = b_1^{m_1}$, $b_1 \neq b$ and b is a base for m_1.

Furthermore, we let

$$\boldsymbol{B}(p) = \{ b \in N_+ \mid b \text{ is a base for } p \} \text{ and}$$

$$\boldsymbol{D}(p) = \{ \lambda \in N_+ \mid \lambda \text{ is prime and } \lambda \nmid b \text{ for all } b \in \mathbf{B}(p) \}.$$

DEFINITION 3.3: Let $q \in \mathbf{G}^*$, $q = \sum_j X^{k_j} p_j$, $p_j \in \mathbf{P}$. We define

– $\text{depth}(q) = \max_j \text{depth}(p_j)$

– $\boldsymbol{D}(q) = \bigcap_j \boldsymbol{D}(p_j)$

where the definition of depth for elements of $\mathbf{P}$ is the obvious extension of Definition 3.1.

Example: Let

$$q = 3^{(xy^2)^{7z^5}} + 2^x$$

then $\boldsymbol{B}(q) = \{2, 3, 7\}$, $depth(q) = 3$, $\boldsymbol{D}(q) = \{ n \in N_+ \mid n \text{ is prime and } n \neq 2, 3, 7 \}$.

DEFINITION 3.4: Let

- $D \subset \{\alpha \in N_+ \mid \alpha \text{ is prime and } \alpha \neq 1\}$,
- $t \in N$.
- $\mathbf{G}^*(t, D) = \{p \in \mathbf{G}^* \mid D(p) = D \text{ and depth } (p) = t\}$.

Remark 3.1: We have the following

- $\mathbf{G}^* = \bigcup_{t, D} \mathbf{G}^*(t, \mathbf{D}) \cup \{1\}$;
- if $q_i \in \mathbf{G}^*(t_i, D(q_i))$, $i = 1, 2$, and either $t_1 \neq t_2$ or $D(q_1) \neq D(q_2)$ then $q_1 \not\equiv q_2$

(the second claim follows from the result for the univariate case when all the variables of q_i are specialized to x_1).

DEFINITION 3.5: Given an infinite set $D \subset \{\alpha \in N_+ \mid \alpha \text{ is prime and } \alpha \neq 1\}$ and a number $t \in N$, the mapping

$$\mathbf{h} = \mathbf{h}(t, D) : \mathbf{G}^*(t, D) \to \{r = \sum_i \prod_k p_{ik} + n \mid r \text{ is irreducible, } p_{ik} \in \mathbf{P}_1\}$$

is defined as follows.

If $D = \{\lambda_1, \ldots, \lambda_n, \ldots \mid \lambda_i < \lambda_j, i < j\}$, choose $\lambda_1 < \ldots < \lambda_{n-1}$ (recall that we are in the n-variable case) and then set

- $\mathbf{h}(q) = q$ for all $q \in \mathbf{G}^*(t, D) \cap \mathbf{P}_1$;
- $\mathbf{h}(q) = \sum_j \mathbf{h}(X^{I_j}) \mathbf{h}(p_j)$ if $q = \sum_j X^{I_j} p_j$, being $p_j \in \mathbf{P}$, where

$$\mathbf{h}(X^I) = x_1^{i_0} \times \delta_1^{\lambda_1 x_1} \cdot \cdot \cdot \times \ldots \times \delta_{n-1}^{\lambda_n x_1 - 1}$$
$$= x_1^{i_0} \times \delta_1^{\Lambda_1} \times \ldots \times \delta_{n-1}^{\Lambda_n - 1},$$

with $\delta_j = \lambda_j^1 j$ and depth $(\Lambda_j) = t + 1$.

$$\mathbf{h}(p) = \begin{cases} b^{\mathbf{h}(m)}, & \text{if } p = b^m, \quad b \in N_+ \\ ((x_1^{i_0})^{\mathbf{h}(m)} \times \delta_1^{\Lambda_1 \mathbf{h}(m)} \times \ldots \times \delta_{n-1}^{\Lambda_n - 1 \mathbf{h}(m)}, & \text{if } p = (X^I)^m. \end{cases}$$

Remark 5.2:

- $\mathbf{h}$ is the identity function in the univariante case;
- depth $(p) > t + 2$, if $p \in \mathbf{P} \setminus \mathbf{P}_1$;
- depth $(p) > t + 2$, if $p = b^m$, $m \in \mathbf{P}_1$.

Example: Let

$$p = y^{(xy^2)^z} + y^{z^x}$$

then $\mathbf{D} = \{2, 3, 5, \ldots\}$, depth $(p) = 2$. We chose

$$\lambda_1 = 2, \qquad \lambda_2 = 3, \qquad \Lambda_1 = 2^{2^{2^x}}, \qquad \Lambda_2 = 3^{3^{3^x}},$$

and

$$\begin{aligned}\mathbf{h}(p) &= 2^{(2^{2^{2^x}} \times \mathbf{h}((xy^2)^z))} + 2^{(2^{2^{2^x}} \times \mathbf{h}(z^x))} \\ &= 2^{(2^{2^{2^x}} \times x \times 4^{2^{2^{2^x}} \times \mathbf{h}(z)})} + 2^{(2^{2^{2^x}} \times 3^{(3^{3^{3^x}} \times \mathbf{h}(x))})} \\ &= 2^{(2^{2^{2^x}} \times x \times 4^{2^{2^{2^x}} \times 3^{3^{3^{3^x}}})} + 2^{(2^{2^{2^x}} \times 3^{(3^{3^{3^x}} \times x)})}\end{aligned}$$

PROPOSITION 3.4: *Given $t \in N$ and an infinite set $\mathbf{D}$ of prime numbers, the mapping*

$$\mathbf{h} = \mathbf{h}(t, \mathbf{D}) : \mathbf{G}^*(t, \mathbf{D}) \to \{ r = \sum_i \prod_k p_{ik} + n \mid r \text{ is irreducible, } p_{ik} \in \mathbf{P}_1 \}$$

is such that

(*a*) $\mathbf{h}(p)$ is irreducible for any $p \in \mathbf{G}^*(t, \mathbf{D})$;

(*b*) $\mathbf{h}$ is injective.

Proof: Let $q \in \mathbf{G}^*(t, \mathbf{D})$ and $p \in \mathbf{P}$. First we remark that $\mathbf{h}(p)$ is irreducible for every $p \in \mathbf{P}$ by definition of $\mathbf{h}$.

In order to prove (*a*), we can restrict ourselves to consider elements of the form $q = X^I \times p$, fpr $p \in \mathbf{P}$ with depth $(p) > 0$, *i.e.* we are left to prove that no rewrite rule of $\mathfrak{R}$ can be applied to the product. We have

$$\text{depth}(\mathbf{h}(X^I)) = t + 2 \qquad \text{if} \quad X^I \notin \mathbf{P}_1$$

$$\text{depth}(\mathbf{h}(p)) \begin{cases} < t+2 & \text{if} \quad p \in \mathbf{P}_1 \\ = t+2 & \text{if} \quad p = (X^I)^m,\ m \in \mathbf{P}_1 \\ > t+2 & \text{otherwise} \end{cases}$$

and in any case the claim is obvious (even rule R_5 does not apply).

In order to prove (*b*), we define a mapping

$$\mathbf{k} : \quad \mathbf{h}(\mathbf{G}^*(t, \mathbf{D})) \to \mathbf{G}^*(t, \mathbf{D})$$

such that $\mathbf{k} \circ \mathbf{h}$ is the identity function.

Note that any term in $\mathbf{h}(\mathbf{G}^*(t, \boldsymbol{D}))$ has either form:

(i) $x_1^{i_0} \times \delta_1^{\Lambda_1} \times \ldots \times \delta_{n-1}^{\Lambda_{n-1}} \times b^{\mathbf{h}(m)}$, $b \in \boldsymbol{N}_+$

(ii) $x_1^{i_0} \times \delta_1^{\Lambda_1} \times \ldots \times \delta_{n-1}^{\Lambda_{n-1}} \times x_1^{\mathbf{h}(m)} \times \varepsilon_1^{\Lambda_1 \mathbf{h}(m)} \times \ldots \times \varepsilon_{n-1}^{\Lambda_{n-1} \mathbf{h}(m)}$

where $\operatorname{depth}(\Lambda_j) = t+1$ and $\operatorname{depth}(\mathbf{h}(m)) \geqq t+1$.

If $\xi_j \in \mathbf{h}(\mathbf{G}^*(t, \mathbf{D}))$, we define the mapping $\mathbf{k}$ by cases:

(i) $\mathbf{k}(x_1^{i_0} \times \delta_1^{\Lambda_1} \times \ldots \times \delta_{n-1}^{\Lambda_{n-1}} \times b^{\mathbf{h}(m)})$

$$= \mathbf{k}(x_1^{i_0} \times \delta_1^{\Lambda_1} \times \ldots \times \delta_{n-1\,\Lambda_{n-1}}) \ \mathbf{k}(b^{\mathbf{h}(m)}) = X^I b^{\mathbf{k}(\mathbf{h}(m))}$$

where $I = (i_0, \ldots, i_{n-1})$ is such that $\delta_j = \lambda_j^{i_j}$

(ii) $\mathbf{k}(x_1^{i_0} \times \delta_1^{\Lambda_1} \times \ldots \times \delta_{n-1}^{\Lambda_{n-1}} \times x_1^{\mathbf{h}(m)} \times \varepsilon_1^{\Lambda_1 \mathbf{h}(m)} \times \ldots \times \varepsilon_{n-1}^{\Lambda_{n-1} \mathbf{h}(m)})$

$$= X^I \times (X^J)^{\mathbf{k}(\mathbf{h}(m))}$$

where $I = (i_0, \ldots, i_{n-1})$ is such that $\delta_j = \lambda_j^{i_j}$
and $J = (j_0, \ldots, j_{n-1})$ is such that $\varepsilon_k = \lambda_k^{j_k}$.

We eventually define $\mathbf{k}(\sum_j \xi_j) = \sum_j (\mathbf{k}(\xi_j))$.

Now, it is easy to see that $\mathbf{k} \circ \mathbf{h}(q) = q$ for every $q \in \mathbf{G}^*(t, \boldsymbol{D})$.

Q.E.D.

THEOREM (only-if part): *Let* $q_1, q_2 \in \mathbf{G}^*$, *if* $q_1 \equiv q_2$ *then* $q_1 = q_2$.

Proof: Since $q_1 \equiv q_2$ we have

$$\boldsymbol{D} = \boldsymbol{D}(q_1) = \boldsymbol{D}(q_2) \qquad \text{and} \qquad t = \operatorname{depth}(q_1) = \operatorname{depth}(q_2)$$

by the second claim of Remark 3.1. Let us then consider $\mathbf{h}(t, \boldsymbol{D})(q_i)$, $i = 1, 2$. We have $\mathbf{h}(t, \boldsymbol{D})(q_1) \equiv \mathbf{h}(t, \boldsymbol{D})(q_2)$, hence $\mathbf{h}(q_1) = \mathbf{h}(q_2)$ by Corollary 3.3. The thesis follows immediately from the injectivity of $\mathbf{h}$.

Q.E.D.

REFERENCES

1. G. H. HARDY, *Orders of Infinity*, Cambridge Tracts in Math. Phys., 12, Cambridge University Press 1910, Reprint Hafner, New York.
2. C. W. HENSON and L. A. RUBEL, *Some Applications of Nevalinna Theory to Mathematical Logic: Identities of Exponential Functions, Trans. of the American Math. Soc.*, Vol. 282, No. 1, 1984, pp. 1-32.
3. G. HUET and D. C. OPPEN, Equations and Rewrite Rules: A Survey. In: *Formal Languages Theory: Perspectives and Open Problems*, R. BOOK Ed., Academic Press, New York, 1980, pp. 349-405.

4. D. LANKFORD, *On Proving Term Rewriting Systems are Noetherian*, Rep. MTP-3, Louisiana Tech. Univ., 1979.
5. H. LEVITZ, *An Ordered Set of Arithmetic Functions Representing the Least ε-Number*, Z. Math. Logik Grundlag. Math., Vol. 21, 1975, pp. 115-120.
6. A. MACINTYRE, The Laws of Exponentiation. In: *Model Theory and Arithmetic*, C. BERLINE, K. MCALOON and J.-P. RESSAYRE Eds., Lecture Notes in Mathematics, No. 890, Springer-Verlag, Berlin, 1981, pp. 185-197.
7. C. MARTIN, *Equational Theories of Natural Numbers and Transfinite Ordinals*, Ph. D. Thesis, Univ. of California, Berkley, 1973.
8. G. E. PETERSON and M. E. STICKEL, *Complete Sets of Reductions for Some Equational Theories*, J. of the A.C.M., Vol. 28, 1981, pp. 233-264.
9. A. TARSKI, Equational Logic and Equational Theories of Algebras. In: *Contributions to Mathematical Logic*, H. A. SCHMIDT, K. SHUTTE and H. J. THIELE Eds., North-Holland, Amsterdam, 1968, pp. 275-288.
10. A. J. WILKIE, *On Exponentiation — A Solution to Tarski's High School Algebra Problem*. Unpublished Manuscript, quoted in Assoc. of Automated Reasoning Newsletter, Vol. 3, 1984, p. 6.