DECIDABILITY OF THE EXISTENTIAL THEORY OF THE SET OF NATURAL NUMBERS WITH ORDER, DIVISIBILITY, POWER FUNCTIONS, POWER PREDICATES, AND CONSTANTS

VERONIQUE TERRIER

(Communicated by Andreas R. Blass)

ABSTRACT. We construct an algorithm to test if a system of conditions of the types $\mu < \eta$, μ/η , $\mu = \eta^a$, $P_a(\mu)$, $\neg(\mu < \eta)$, $\neg(\mu/\eta)$, $\neg(\mu = \eta^a)$, and $\neg(P_a(\mu))$ has a solution in natural numbers. ($a \in N$, and P_a denotes the set $\{n^a: n \in N\}$.)

INTRODUCTION

In this paper we give an algorithm that tests whether a system of conditions of the forms $\mu < \eta$, μ/η , $\mu = \eta^a$, $P_a(\mu)$, $\neg(\mu < \eta)$, $\neg(\mu/\eta)$, $\neg(\mu = \eta^a)$, and $\neg(P_a(\mu))$ (where P_a denotes the set $\{n^a: n \in N\}$; μ, η are variables (to vary over N) or natural numbers (called parameters), and a is a natural number) has a solution in natural numbers.

Since the language $\{<, /\} \cup \{P_a: a \in N\} \cup \{x \rightarrow x^a: a \in N\} \cup \{a: a \in N\}$ contains no binary function, every atomic formula or negation of an atomic formula is equivalent to a system of conditions of the above type.

Using the disjunctive normal form of formulas, we see that our result proves the decidability of the existential theory of N structured by the above language (hence, also the universal theory).

Bel'tyukov [B] and Lipshitz [L] have independently proved the decidability of the existential theory of N with addition and divisibility. Before, Kosovskii [Kos] showed that there exists no algorithm to test whether a system of conditions $\mu + \eta = \gamma$, μ/η , $P_2(\mu)$ has a solution in natural numbers. Then M. Davis, Y. Matiyasevich, and J. Robinson [DMR] wondered whether there exists an algorithm that tests whether a system of conditions $\mu < \eta$, μ/η , $P_2(\mu)$ has a solution in natural numbers. In 1979 Koppel [Kop] proved that there exists such an algorithm for systems of conditions $\mu < \eta$, μ/η , $P_a(\mu)$. Our result extends Koppel's algorithm: the system of conditions is allowed to contain negative conditions and terms constructed from functions in $\{x \rightarrow x^a: a \in N\}$.

In part A we transform, in an effective way, any system of conditions into an equivalent (in logical sense: i.e. the systems are both satisfiable or both not)

Received by the editors May 29, 1990 and, in revised form, October 3, 1990.

1980 *Mathematics Subject Classification* (1985 Revision). Primary 03F30.

Key words and phrases. Decision problems in arithmetic, decidability.

© 1992 American Mathematical Society
0002-9939/92 \$1.00 + \$.25 per page

disjunction of subsystems where some forms of conditions are eliminated or reinforced.

In part B we rewrite any subsystem by adding to it the conditions inherited by transitivity of the natural order and the divisibility.

In part C, if no contradictory condition appears in the rewriting of the subsystem, we construct a solution.

A

1. Elimination of negative forms of comparison and equality. We replace them by positive formulas according to the following equivalences:

$$\begin{aligned}\neg(n < x) &\leftrightarrow x < n + 1; \\ \neg(x < n) &\leftrightarrow n - 1 < x; \\ \neg(x < y) &\leftrightarrow x = y \vee y < x; \\ \neg(\mu = \eta^a) &\leftrightarrow \mu < \eta^a \vee \eta^a < \mu.\end{aligned}$$

2. Elimination of the positive forms of predicates P_a . We introduce new variables in the system: $P_a(\mu) \leftrightarrow \exists x (\mu = x^a)$.

3. Elimination of the positive forms of $x^a = y^b$. $x^a = y^b \leftrightarrow x^{a/(a,b)} = y^{b/(a,b)}$, where (a, b) denotes the greatest common divisor of a and b . $x^a = y^b \leftrightarrow \exists z (x = z^{b/(a,b)} \wedge y = z^{a/(a,b)})$. Thus, we introduce a new variable z , and replace all occurrences of the variable x by $z^{b/(a,b)}$ and all occurrences of the variable y by $z^{a/(a,b)}$.

4. $\neg(P_a(x^b)) \leftrightarrow \neg(P_{a/(a,b)}(x))$. If $\neg(P_a(x^b))$ occurs in the system, either $a = (a, b)$ is true and the system has no solution, or $a/(a, b) > 1$ and we can substitute $\neg(P_{a/(a,b)}(x))$ for $\neg(P_a(x^b))$ in the system.

5. Since for any formula Φ , we have

$$\Phi(x) \leftrightarrow (\Phi(x) \wedge x = 0) \vee (\Phi(x) \wedge x = 1) \vee (\Phi(x) \wedge x > 1).$$

We can assume that each variable x strictly greater than 1.

6. Reinforcement by the natural order of the conditions of the forms $\neg(\mu/n)$ and μ/η according to the following equivalences:

$$\begin{aligned}\neg(\mu/n) &\leftrightarrow n < \mu \vee (\neg(\mu/n) \wedge \mu < n), \\ \mu/\eta &\leftrightarrow \mu = \eta \vee (\mu/\eta \wedge \mu < \eta) \quad (\text{each variable is strictly greater than 1}).\end{aligned}$$

We reduce the system to a disjunction of subsystems such that if $\neg(\mu/n)$, or μ/η occurs then $\mu < n$ also does occur. If new positive forms $x^a = y^b$ are introduced, we once again apply 3.

7. Elimination of the conditions that bound the variables, i.e. the conditions of the forms $x^a = n$, $x^a < n$, x^a/n , and according to 6, $\neg(x^a/n) \wedge x^a < n$. When some of these conditions occur in a system, we replace this system by a disjunction of subsystems where the natural numbers that satisfy the condition take the place of x . (There is a finite number of such integers and when no natural number satisfies the condition, the system has no solution.) If necessary, this process is applied several times.

8. Elimination of the conditions where only natural numbers occur. On account of the decidability of such conditions, we can determine if they are satisfied and then we eliminate them, otherwise the system has no solution.

To sum up, applying the previous algorithms on any system of conditions, either we show that it has no solution, or we transform it into an equivalent (in

logical sense) disjunction of subsystems of conditions of the form:

$$n < x^a, \quad n/x^a, \quad \neg(n/x^a), \quad x^a/y^b, \quad x^a < y^b, \quad \neg(x^a/y^b), \quad \neg(P_a(x)).$$

Thus, the problem is reduced to these subsystems.

Notation. We express the condition x^u/y^v by x^α/y with $\alpha = u/v \in \mathbf{Q}_+$,
the condition $x^u < y^v$ by $x^\beta < y$ with $\beta = u/v \in \mathbf{Q}_+$,
the condition $\neg(x^u/y^v)$ by $\neg(x^\gamma/y)$ with $\gamma = u/v \in \mathbf{Q}_+$.

For each pair of variables, we reduce the whole set of conditions of divisibility involving these two variables to one only, according to the following equivalence:

$$\bigwedge x_i^{\alpha_{ij}^t}/x_j \leftrightarrow x_i^{\alpha_{ij}}/x_j \quad \text{where } \alpha_{ij} = \max_t \{\alpha_{ij}^t\};$$

Idem for comparison and nondivisibility conditions:

$$\begin{aligned} \bigwedge x_i^{\beta_{ij}^t} < x_j &\leftrightarrow x_i^{\beta_{ij}} < x_j \quad \text{where } \beta_{ij} = \max_t \{\beta_{ij}^t\}; \\ \bigwedge \neg(x_i^{\gamma_{ij}^t}/x_j) &\leftrightarrow \neg(x_i^{\gamma_{ij}}/x_j) \quad \text{where } \gamma_{ij} = \min_t \{\gamma_{ij}^t\}. \end{aligned}$$

B

Now we care about the conditions implied by transitivity of the divisibility and the natural order. These conditions would be said to be inherited. If $x_i^{\alpha_{ij}}/x_j$ and $x_j^{\alpha_{jk}}/x_k$ occur in the system, we would like a condition of divisibility on (x_i, x_k) at least as strong as the inherited condition $x_i^{\alpha_{ij} \cdot \alpha_{jk}}/x_k$ to occur in the system. Idem for the comparison conditions. We would also like that if p^u/x_i and $x_i^{\alpha_{ij}}/x_j$ occur in the system (where p is prime), then a condition at least as strong as the inherited condition $p^{\lceil u\alpha_{ij} \rceil}/x_j$ also occur in the system ($\lceil \cdot \rceil$ denotes the ceiling).

B1. Inheritance of conditions of divisibility by a variable

Lemma 1. Let S be some system of conditions of the form $x_i^{\alpha_{ij}}/x_j$

$$S: \bigwedge_{(ij) \in A} x_i^{\alpha_{ij}}/x_j.$$

Then

- either we can construct effectively a system S' equivalent to the system S (in recursive sense: i.e. the solution sets of the systems are in 1-1 recursive correspondence) such that (1) If $x_i^{\alpha_{ij}}/x_j$ and $x_j^{\alpha_{jk}}/x_k$ occur in S' , then a condition $x_i^{\alpha_{ik}}/x_k$ occurs in S' where $\alpha_{ik} \geq \alpha_{ij} \cdot \alpha_{jk}$; (2) If $x_i^{\alpha_{ij}}/x_j$ and $x_j^{\alpha_{ji}}/x_i$ occur in S' , then $\alpha_{ij} \cdot \alpha_{ji} \leq 1$.
- or we can show that the system has no solution.

Proof. Let A' be the transitive closure of A (i.e. $A' = \{(i, j): \text{there exist } i_1, i_2, \dots, i_n \text{ such that } (i, i_1), (i_1, i_2), \dots, (i_n, i) \in A\}$). For each i such that $(i, i) \in A'$, let:

$$m_i = \max(\alpha_{ii_1} \cdot \alpha_{i_1 i_2} \cdot \dots \cdot \alpha_{i_n i}) \quad \text{where } (i, i_1), (i_1, i_2), \dots, (i_n, i) \in A \\ \text{and } i, i_1, i_2, \dots, i_n \text{ are distinct.}$$

If some m_i is such that $m_i > 1$, then the system has no solution: the condition $x_i^{m_i}/x_i$ is inherited, and cannot be satisfied.

If all m_i satisfy $m_i \leq 1$, then for all $(i, j) \in A'$ let

$$\alpha'_{ij} = \max(\alpha_{ii_1} \cdot \alpha_{i_1 i_2} \cdot \dots \cdot \alpha_{i_n j}) \quad \text{where } (i, i_1), (i_1, i_2), \dots, (i_n, j) \in A \\ \text{and } i, i_1, i_2, \dots, i_n, j \text{ are distinct.}$$

The system S' obtained from S by substituting $x_i^{\alpha'_{ij}}/x_j$ for $x_i^{\alpha_{ij}}/x_j$ is equivalent to S since the α'_{ij} 's express inherited conditions.

We show that S' satisfies conditions (1) and (2). Condition (2) is insured by the inequalities $m_i \leq 1$. As for condition (1), we have

$$\alpha'_{ij} \cdot \alpha'_{jk} = \alpha_{it_1} \cdot \dots \cdot \alpha_{t_n j} \cdot \alpha_{js_1} \cdot \dots \cdot \alpha_{s_m k} \quad \text{for some suffixes } t_u, s_v.$$

Case 1. $i, t_1, \dots, t_n, j, s_1, \dots, s_m, k$ are distinct. Then by definition of α'_{ik} , we have the desired property: $\alpha'_{ik} \geq \alpha'_{ij} \cdot \alpha'_{jk}$.

Case 2. At least two suffixes are identical: let $t_u = s_v$ where $[u, v]$ is the largest possible such interval. Since $m_{t_u} \leq 1$, we have $\alpha_{t_u t_{u+1}} \cdot \dots \cdot \alpha_{t_n j} \cdot \alpha_{js_1} \cdot \dots \cdot \alpha_{s_{v-1} s_v} \leq 1$. So $\alpha'_{ij} \cdot \alpha'_{jk} \leq \alpha_{it_1} \cdot \dots \cdot \alpha_{t_{u-1} t_u} \cdot \alpha_{t_u s_{v+1}} \cdot \dots \cdot \alpha_{s_m k}$, where $i, t_1, \dots, t_{u-1}, t_u, s_{v+1}, \dots, s_m, k$ are distinct. Then we have that: $\alpha'_{ik} \geq \alpha'_{ij} \cdot \alpha'_{jk}$.

B2. Inheritance of comparison conditions

Lemma 2. Let S be some system of conditions of the form $x_i^{\beta_{ij}} < x_j$

$$S: \bigwedge_{(i,j) \in B} x_i^{\beta_{ij}} < x_j.$$

Then

- either we can construct effectively a system S' equivalent (in recursive sense) to the system S such that (1) If $x_i^{\beta_{ij}} < x_j$ and $x_j^{\beta_{jk}} < x_k$ occur in S' , then a condition $x_i^{\beta_{ik}} < x_k$ occurs in S' where $\beta_{ik} \geq \beta_{ij} \cdot \beta_{jk}$; (2) If $x_i^{\beta_{ij}} < x_j$ and $x_j^{\beta_{ji}} < x_i$ occur in S' , then $\beta_{ij} \cdot \beta_{ji} < 1$.

- or we can show that S has no solution.

Proof. The only difference with Lemma 1 is that the condition $x_i^{m_i} < x_i$ is satisfied only if $m_i < 1$ (strict inequality), so it is necessary that $\beta_{ij} \cdot \beta_{ji} < 1$.

Remark. According to 5, 6, and 8 of part A, we have (*)

$$(i, j) \in A \Rightarrow (i, j) \in B \quad \text{and} \quad \alpha_{ij} \leq \beta_{ij}.$$

Since

$$\beta'_{ij} = \max(\beta_{ii_1} \cdot \beta_{i_1 i_2} \cdot \dots \cdot \beta_{i_n j}) \quad \text{where } (i, i_1), (i_1, i_2), \dots, (i_n, j) \in B \\ \text{and } i, i_1, i_2, \dots, i_n, j \text{ are distinct;} \\ \beta'_{ij} \geq \max(\alpha_{ii_1} \cdot \alpha_{i_1 i_2} \cdot \dots \cdot \alpha_{i_n j}) \quad \text{where } (i, i_1), (i_1, i_2), \dots, (i_n, j) \in A \subset B \\ \text{and } i, i_1, i_2, \dots, i_n, j \text{ are distinct;} \\ \beta'_{ij} \geq \alpha'_{ij};$$

We see that (*) is still valid after the processes of Lemmas 1 and 2 have been applied. Note that, in fact, $\alpha_{ij} \alpha_{ji} \leq \beta_{ij} \beta_{ji} < 1$.

B3. Inheritance of conditions of divisibility by a parameter. (a) We come down to conditions of divisibility by a prime power.

$$\begin{aligned} n/x^u &\leftrightarrow \bigwedge_j p_j^{i_j}/x^u \quad \text{if } n = p_1^{i_1} \cdots p_k^{i_k} \text{ where the } p_i\text{'s are prime.} \\ &\leftrightarrow \bigwedge_j p_j^{\lceil i_j/u \rceil}/x. \end{aligned}$$

(b) Inheritance of conditions of divisibility by a prime power. Let

$$S: \bigwedge_i p^{t_i}/x_i \wedge \bigwedge_{(i,j) \in A} x_i^{\alpha_{ij}}/x_j \quad \text{where } \alpha_{ij} \geq \alpha_{ik}\alpha_{kj} \text{ and } \alpha_{ij}\alpha_{ji} < 1.$$

We look for k_i 's such that $S': \bigwedge_i p^{k_i}/x_i \wedge \bigwedge_{(i,j) \in A} x_i^{\alpha_{ij}}/x_j$ is equivalent (in recursive sense) to S and the inherited conditions explicitly belong to S' .

As for the inherited conditions of divisibility by a variable, the k_i 's have to satisfy $k_i\alpha_{ij} \leq k_j$; in addition, they have to be integers. In short, the k_i 's will be the smallest natural numbers such that $k_i \geq t_i$ and $k_i\alpha_{ij} \leq k_j$ for all $(i, j) \in A$ (for the existence look at C1a, Fact 1, below).

(c) We reduce all the conditions which involve divisibilities of some variable by a parameter to a unique one, according to the equivalence: $\bigwedge_i a_i/x \leftrightarrow \text{lcm}(a_i)/x$.

C

Lemma. *Let S be any system and let S' be the result of applying to S the successive algorithms defined in part B. If any one of the following three conditions is satisfied, then S has no solution.*

- (c1) *Applying an algorithm in part B, the system S has been seen to have no solution.*
- (c2) *There do occur two conditions $x_i^{\alpha_{ij}}/x_j$ and $\neg(x_i^{\gamma_{ij}}/x_j)$, where $\alpha_{ij} \geq \gamma_{ij}$.*
- (c3) *There do occur two conditions n/x and $\neg(m/x^u)$, where m/n^u .*

We can test in an effective way, whether these three conditions are satisfied. Now we assume that none of (c1), (c2), (c3) is satisfied and show that the system has a solution, which we do construct. Hence we show the problem to be decidable.

C1. First, we come down to a system where the conditions of the forms $\neg(P_a(x))$ and $\neg(x_i^{\gamma_{ij}}/x_j)$ are replaced by stronger conditions of the forms n/x and $\neg(m/x^u)$.

C1a. *Conditions of the form $\neg(P_a(x))$.* Recall that $a > 1$, according to 4 of part A. Note that for some prime q and some $k \in \mathbb{N}$ such that a does not divide k , we have

$$(q^k/x \wedge \neg(q^{\lceil k/a \rceil a}/x)) \rightarrow \neg(P_a(x)).$$

We eventually adopt new conditions of the form p^k/x , and we put them in S .

The following fact prevents from adopting contradictory conditions.

Fact 1. *Consider $(\alpha_{ij})_{(i,j) \in \{1, \dots, n\} \times \{1, \dots, n\}}$ where $\alpha_{ij} = 0$ for $(i, j) \notin A$, $\alpha_{ij} \geq \alpha_{ii}\alpha_{ij}$, and $\alpha_{ij}\alpha_{ji} < 1$. Then whatever the natural number $a > 1$, there exist $k_1, \dots, k_n \in \mathbb{N}$ such that a does not divide k_1 and $k_i\alpha_{ij} \leq k_j$.*

Proof. Let k_1 be such that for each $i \leq n$, $k_1\alpha_{1i} \in \mathbb{N}$ and define $k_i = k_1\alpha_{1i}$. Note that $k_i\alpha_{ij} = k_1\alpha_{1i}\alpha_{ij} \leq k_1\alpha_{1j} = k_j$. If a does not divide k_1 , the fact is proved.

When a/k_1 : For all $K \in N^*$, we have $Kk_i\alpha_{ij} \leq Kk_j$; in particular:

$$Kk_i\alpha_{i1}\alpha_{1i} < Kk_1\alpha_{1i} = Kk_i \quad (\text{the inequality is strict since } \alpha_{i1}\alpha_{1i} < 1).$$

Then for large K we have: $Kk_i\alpha_{i1}\alpha_{1i} < (Kk_1 - 1)\alpha_{1i} \leq Kk_1\alpha_{1i} = Kk_i$. Then $(Kk_1 - 1), Kk_2, \dots, Kk_n$ satisfy the hypotheses of Fact 1.

If $\neg(P_a(x_t))$ occurs in S , we choose some prime q that is prime with all parameters occurring in S , and according to Fact 1 some $k_1, \dots, k_n$ such that a does not divide k_t and $k_i\alpha_{ij} \leq k_j$.

We obtain a new system S' by substituting $\bigwedge q^{k_i}/x_i \wedge \neg(q^{\lceil k_i/a \rceil a}/x_t)$ to $\neg(P_a(x_t))$ in S . This new system S' where the condition $\neg(P_a(x_t))$ has been replaced by stronger conditions, is such that its solutions are solutions of S . According to Fact 1, the inherited conditions occur explicitly. The condition (c3) is never satisfied (nor are the other ones), since the new parameters introduced are prime to the old ones, and a is greater than 1.

C1b. Conditions of the form $\neg(x_i^{\gamma_{ij}}/x_j)$. If $\neg(x_1^{\gamma_{12}}/x_2)$ occurs in S , we choose some prime q that is prime with all parameters occurring in S , and some k such that $k\gamma_{ij} \in N$, $k\alpha_{ij} \in N$.

We obtain a new system S' by substituting $q^k/x_1 \wedge \neg(q^{k\gamma_{12}}/x_2) \wedge \bigwedge q^{k\alpha_{1i}}/x_i$ for $\neg(x_1^{\gamma_{12}}/x_2)$ in S . This new system S' where the condition $\neg(x_1^{\gamma_{12}}/x_2)$ has been replaced by stronger conditions, is such that its solutions are solutions of S . As new conditions of the form p/x are introduced in S' , we again apply the process of B3. The inherited conditions are $\bigwedge q^{k\alpha_{1i}}/x_i$. As $\alpha_{12} < \gamma_{12}$ (condition (c2)), and q is prime with the other parameters, the condition (c3) is still never satisfied.

C2. In a first step we assign values to the variables so that the conditions of the forms n/x , $x_i^{\alpha_{ij}}/x_j$, $\neg(m/x^u)$ are satisfied. In a second step we change these values so as to satisfy also the conditions of the forms $m < x^u$, $x_i^{\beta_{ij}} < x_j$.

C2a. Conditions of the form n/x , $x_i^{\alpha_{ij}}/x_j$, $\neg(m/x^u)$. Let

$$a_i = \begin{cases} n & \text{if } n/x_i \text{ occurs in } S', \\ 1 & \text{otherwise.} \end{cases}$$

For $x_i = a_i$, $i = 1 \dots$, we have:

- the conditions n/x are obviously satisfied;
- the conditions $\neg(m/x^u)$ are satisfied according to condition (c3);
- the conditions $x_i^{\alpha_{ij}}/x_j$ are satisfied since according to B3, a_i is the lcm of all k such that $k\alpha_{ij}/a_j$.

C2b. Conditions of the form $m < x^u$, $x_i^{\beta_{ij}} < x_j$. Let $T > 1$ be an integer prime to all the parameters in S' and the previous a_i 's such that $T > m$ if $m < x$ occurs in S' , and $1/T \leq \min_{(ij) \in B} (a_i^{\beta_{ij}}/a_j)$. We choose integers u_i such that, letting $a'_i = T^{u_i}a_i$, the values $x_i = a'_i$ satisfy all conditions.

As T is prime to the parameters in S' and the a_i 's, the conditions of divisibility by a parameter and all conditions of non-divisibility are preserved.

For each $(i, j) \in B$, we let t_{ij} be the integer such that $T^{t_{ij}-1} \leq a_i^{\beta_{ij}}/a_j < T^{t_{ij}}$. We have $t_{ij} \geq 0$.

If we find u_i with the following property: for all $(i, j) \in B$, $u_j \geq t_{ij} + u_i\beta_{ij}$, then (1) the conditions of natural order are satisfied:

$$(a'_i)^{\beta_{ij}} = T^{u_i\beta_{ij}}a_i^{\beta_{ij}} < T^{t_{ij}+u_i\beta_{ij}}a_j \leq a'_j$$

and (2) the conditions of divisibility are satisfied:

$$(a'_i)^{\alpha_{ij}} = T^{u_i \alpha_{ij}} a_i^{\alpha_{ij}} / T^{u_i \alpha_{ij}} a_j$$

and from $\alpha_{ij} \leq \beta_{ij}$ and $t_{ij} \geq 0$, we have $u_i \alpha_{ij} \leq u_i \beta_{ij} + t_{ij} \leq u_j$ so $(a'_i)^{\alpha_{ij}} / T^{u_j} a_j$.

We still have to find u_i such that: for all $(i, j) \in B$, $u_j \geq t_{ij} + u_i \beta_{ij}$. First we choose u_i such that for all distinct $k_1, k_2, \dots, k_n \in N$ with $(i, k_n), \dots, (k_2, k_1), (k_1, i) \in B$, we have

$$u_i(1 - \beta_{ik_n} \cdots \beta_{k_2 k_1} \beta_{k_1 i}) \geq t_{k_1 i} + t_{k_2 k_1} \beta_{k_1 i} + \cdots + t_{ik_n} \beta_{k_n k_{n-1}} \cdots \beta_{k_1 i}.$$

(Recall that according to Lemma 2(2). $\beta_{ik_n} \cdots \beta_{k_2 k_1} \beta_{k_1 i} < 1$). Let

$$u'_i = \max(u_i, t_{k_1 i} + t_{k_2 k_1} \beta_{k_1 i} + \cdots + t_{ik_n} \beta_{k_n k_{n-1}} \cdots \beta_{k_1 i} + u_s t_{s k_n} \beta_{k_n k_{n-1}} \cdots \beta_{k_1 i})$$

with $(s, k_n), \dots, (k_2, k_1), (k_1, i) \in B$ and $i, s, k_1, \dots, k_n$ are distinct. Let us show that for all $(i, j) \in B$, $u'_j \geq t_{ij} + u'_i \beta_{ij}$.

Case 1. $u'_i = u_i$. Then by definition of u'_j , $u'_j \geq t_{ij} + u_i \beta_{ij}$.

Case 2. $u'_i = t_{k_1 i} + t_{k_2 k_1} \beta_{k_1 i} + \cdots + u_e t_{e k_n} \beta_{k_n k_{n-1}} \cdots \beta_{k_1 i}$. So $t_{ij} + u'_i \beta_{ij} = t_{ij} + t_{k_1 i} \beta_{ij} + t_{k_2 k_1} \beta_{k_1 i} \beta_{ij} + \cdots + u_e t_{e k_n} \beta_{k_n k_{n-1}} \cdots \beta_{k_1 i} \beta_{ij}$.

(2a) $j \neq e, k_1, \dots, k_n$. Then by definition of u'_j , $u'_j \geq t_{ij} + u'_i \beta_{ij}$.

(2b) $j = k_r$.

$$t_{ij} + u'_i \beta_{ij} = t_{ij} + \cdots + t_{jk_{r-1}} \beta_{k_{r-1} k_{r-2}} \cdots \beta_{k_1 i} \beta_{ij} + \beta_{jk_{r-1}} \cdots \beta_{k_1 i} \beta_{ij} (t_{k_{r+1} j} + \cdots + t_{ek_n} \beta_{k_n k_{n-1}} \cdots \beta_{k_{r+1} j} + u'_e \beta_{ek_n} \cdots \beta_{k_{r+1} j})$$

and by definition of u'_j ,

$$\begin{aligned} &\leq t_{ij} + \cdots + t_{jk_{r-1}} \beta_{k_{r-1} k_{r-2}} \cdots \beta_{k_1 i} \beta_{ij} + \beta_{jk_{r-1}} \cdots \beta_{k_1 i} \beta_{ij} u'_j \\ &\leq u'_j \quad \text{as } u'_j \geq u_j \text{ and by choice of } u_j. \end{aligned}$$

The case $j = e$ is proved similarly. Hence our claim is proved and the theorem follows.

Theorem. *The existential theory of N with order, divisibility, power functions, power predicates and constants is decidable.*

It seems that the method described above has some power. By similar method, we can prove the decidability of the existential theory of N with order, divisibility, and functions $\{x \rightarrow ax : a \in N\}$ [T] which is a simple consequence of [B] and [L]. A more general problem appears: "Is the existential theory of N with multiplication and natural order decidable?"

Recall some relative results:

(1) Skolem, [S] has shown the decidability of the full theory of N with multiplication;

(2) in [DMR] the existential theory of N with successor and multiplication is shown undecidable (this implies the undecidability of the full theory of N with multiplication and natural order).

ACKNOWLEDGMENT

I would like to thank Professor S. Grigorieff for encouragement and helpful discussions.

REFERENCES

- [B] A. P. Bel'tyukov, *Decidability of the universal theory of natural numbers with addition and divisibility*, Zapiski Nauch. Sem. Lenin. Otdeleniya Math. Inst. im. V. A. Steklova Akad. Nauk SSSR, vol. 60, 1976, pp. 15–28.
- [DMR] M. Davis, Ju. V. Matijasevic, and J. Robinson, *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution* (Proc. Sympos. on the Hilbert problems, DeKalb, Illinois, May 1974), vol. 28, Amer. Math. Soc., Providence, RI, 1976, pp. 323–378.
- [Kop] M. Koppel, *Some decidable diophantine problem: positive solution to a problem of Davis, Matijasevic and Robinson*, Proc. Amer. Math. Soc. **77** (1979), 319–323.
- [Kos] N. K. Kosovskii, *On solutions of systems consisting of both word equations and word length inequalities*, J. Soviet Math. **8** (1977), 262–265.
- [L] L. Lipshitz, *The diophantine problem for addition and divisibility*, Tran. Amer. Math. Soc. **235** (1978), 271–283.
- [S] T. Skolem, *Über einige Satzfunctionen in der Arithmetik*, Skrifte Vidensk. Kristiana I, no. 7, 1930, pp. 1–28.
- [T] V. Terrier, *Decidability of the existential theory of N with order, divisibility and functions $\{x \rightarrow ax : a \in N\}$* , preprint. (French)

LABORATOIRE DE L'INFORMATIQUE DU PARALLÉLISME, ECOLE NORMALE SUPÉRIEURE DE LYON,
46 ALLÉE D'ITALIE, 69364 LYON CEDEX 07-FRANCE