MIT/LCS/TM-42

ON THE COMPLEXITY OF THE THEORIES OF WEAK DIRECT PRODUCTS

Charles Rackoff

January 1974

TM-42

ON THE COMPLEXITY OF THE THEORIES OF WEAK DIRECT PRODUCTS†

by

Charles Rackoff

Massachusetts Institute of Technology

January, 1974

†This research was supported by the National Science Foundation under research grant GJ-34671.

ABSTRACT

Let N be the set of nonnegative integers and let $<N^*,+>$ be the weak direct product of $<N,+>$ with itself. Mostowski[9] shows that the theory of $<N^*,+>$ is decidable, but his decision procedure isn't elementary recursive. We present here a more efficient procedure which operates within space $2^{2^{2^{cn}}}$. As corollaries we obtain the same upper bound for the theory of finite abelian groups, the theory of finitely generated abelian groups, and the theory of the structure $<N^+,\cdot>$ of positive integers under multiplication. Fischer and Rabin have shown that the theory of $<N^*,+>$ requires time $2^{2^{2^{dn}}}$ on nondeterministic Turing machines [5].

We also obtain some very general results about the nature of the theory of the weak direct product of a structure with itself.

Section 1: Introduction

The significance of the distinction between decidable and undecidable theories has been blurred by recent results of Meyer and Stockmeyer [7,8,14] and Fischer and Rabin[5] who have shown that most of the decidable theories known to logicians cannot be decided by any algorithm whose computational complexity grows less than exponentially with the size of sentences to be decided. In many cases even larger lower bounds have been established. In this paper we develop some decision procedures whose computational complexity roughly meets the lower bounds. Part of this development includes a treatment of the relationship between the theory of a structure and the theory of its weak direct product which may be of independent interest.

Let N be the set of non-negative integers. Whether a sentence of the first order theory of N under addition is true is decidable according to a theorem of Presburger[12]. A more efficient decision procedure given by Cooper[2] has been proved by Oppen[10] to require only

$$2^{2^{2^{cn}}}$$

steps for sentences of length n, where c is some constant. This result is strengthened by Ferrante and Rackoff[4], who show that <u>space</u>

$$2^{2^{cn}}$$

is sufficient; this latter theorem will also appear in this paper as a corollary of some more general results.

Let N^* be the set of functions from N to N of finite support, i.e., $N^* = \{f: N \to N \mid f(i)=0$ for all but finitely many $i \in N\}$. The structure $< N^+, \cdot >$ positive integers under multiplication is isomorphic to the structure $< N^*, + >$ where addition is defined component wise and the first order theory of this structure is known to be decidable by a theorem of Mostowski[9]. Mostowski's procedure, however, is not elementary recursive in the sense of the following definition:

Defintion: An elementary recursive function (on strings or integers) is one which can be computed by some Turing machine within time bounded by a fixed composition of exponential functions of the length of the input. (This is shown by Cobham[1] and Ritchie[13] to be equivalent to Kalmar's definition [cf. 11].)

In this paper we use the technique of Ehrenfeucht games[3] to derive a new procedure for deciding whether sentences are true over $< N^*, + >$. Our procedure can be implemented on a Turing machine which uses at most

$$2^{2^{2^{cn}}}$$

tape squares (and hence

$$2^{2^{2^{2^{c'n}}}}$$

steps) on sentences of length n. As a corollary we obtain the same upper bound on decision procedures for the first order theory of finite abelian groups and of finitely generated abelian groups. Recent results of Fischer and Rabin[5] show that for some constant $c'' > 0$, any decision procedure for the first order theory of $< N^*, + >$ requires time

$$2^{2^{2^{c''n}}}$$

even on nondeterministic Turing machines. Thus, the worst case behavior of our procedure for $< N^*, + >$ is nearly optimal in its computational requirements.†

In section 2 we derive some very general results about theories of structures and their weak direct products. In section 3 we apply some of these results to the theories of $< N,+ >$, $< N^*, + >$ and abelian groups. (Most of the results on abelian groups are due to Mike Fischer.)

† If t is a function of n, let DTIME(t) (NTIME(t)) be the class of functions, each of which can be computed by some deterministic (nondeterministic) Turing machine within time t as a function of the length of input. It is easy to see that $\mathrm{NTIME}(t) \subseteq \bigcup_{c>0} \mathrm{DTIME}(c^t)$. It is conjectured that $\mathrm{NTIME}(t) - \mathrm{DTIME}(2^t) \neq \emptyset$.

Section 2: Some General Development

For this section, let $\mathcal{L}$ be the language of the first order predicate calculus with no function symbols, with finitely many relational symbols $\underline{\mathcal{R}}_1, \underline{\mathcal{R}}_2, \ldots, \underline{\mathcal{R}}_\ell$ such that $\underline{\mathcal{R}}_i$ is a t_i-place formal predicate for $1 \le i \le \ell$, and a constant symbol $\underline{e}$. We will denote the formal variables of $\mathcal{L}$ by $x, x_1, x_2, \ldots$. When we write $F(x_1, x_2, \ldots, x_k)$ we will mean that F is a formula of $\mathcal{L}$ free in at most $x_1, x_2, \ldots, x_k$.

For the rest of this section, let $\mathcal{S}$ be a fixed structure for $\mathcal{L}$; $\mathcal{S} = \langle S, \mathcal{R}_1, \ldots, \mathcal{R}_\ell, e \rangle$ where S is a nonempty set, $\mathcal{R}_i \subseteq S^{t_i}$ for $1 \le i \le \ell$, and $e \in S$. We will assume that we have a norm on S, by which we mean a function $\| \ \| : S \to N$, and we will denote the norm of $a \in S$ by $\|a\|$. If $i \in N$, then we will write $a \preceq i$ to mean $\|a\| \le i$.

For convenience we will use $\vec{a}_k$ to denote the k-tuple $(a_1, a_2, \ldots, a_k)$ when $k > 0$, and similarly for $\vec{b}_k, \vec{x}_k$, etc. $(\vec{a}_k, a)$ will denote the k+1-tuple $(a_1, a_2, \ldots, a_k, a)$, etc. When k=0, $\vec{a}_k$ and $\vec{x}_k$ simply denote the unique 0-tuple, i.e., the empty sequence.

Definition: Let F be a formula of $\mathcal{L}$. Then by the quantifier-depth of F, or q-depth(F), we will mean the depth of the deepest nesting of quantifiers in F. Formally, if F is an atomic formula then q-depth(F)=0; otherwise q-depth($F_1 \vee F_2$)=Max{q-depth(F_1),q-depth(F_2)}, q-depth(~F)=q-depth(F), and q-depth($\exists x$ F)=1+q-depth(F).

Definition: For all $n, k \in N$ and all $\vec{a}_k, \vec{b}_k \in S^k$, define $\vec{a}_k \equiv_n \vec{b}_k$ iff for every formula $F(\vec{x}_k)$ of q-depth $\le n$, $F(\vec{a}_k)$ and $F(\vec{b}_k)$ are either both true or both false.

Remark: For each $n,k \in N$, $\underset{n}{\equiv}$ is an equivalence relation on S^k.

Lemma 1: Let $n,k \in N$ and $\vec{a}_k, \vec{b}_k \in S^k$ such that

1) For each $a_{k+1} \in S$ there exists some $b_{k+1} \in S$ such that $\vec{a}_{k+1} \underset{n}{\equiv} \vec{b}_{k+1}$.

and 2) For each $b_{k+1} \in S$ there exists some $a_{k+1} \in S$ such that $\vec{a}_{k+1} \underset{n}{\equiv} \vec{b}_{k+1}$.

Then $\vec{a}_k \underset{n+1}{\equiv} \vec{b}_k$.

Proof: Say that 1) and 2) hold. Since every formula is a boolean combnation of formulas each of which begins with an existential quantifier, it is sufficient to prove, for $F(\vec{x}_k)$ of the form $\exists x_{k+1} G(\vec{x}_{k+1})$ where q-depth$(G) \le n$, that $F(\vec{a}_k) \Leftrightarrow F(\vec{b}_k)$.

So assume that $F(\vec{a}_k)$ holds. Then let $a_{k+1} \in S$ be such that $G(\vec{a}_{k+1})$ holds. By 1), let $b_{k+1} \in S$ be such that $\vec{a}_{k+1} \underset{n}{\equiv} \vec{b}_{k+1}$. Since $G(\vec{a}_{k+1})$ is true, $G(\vec{b}_{k+1})$ is true (by definition of $\underset{n}{\equiv}$), so $F(\vec{b}_k)$ is true. By symmetry, $F(\vec{a}_k)$ holds if $F(\vec{b}_k)$ holds. □

Definition: Let $M(n,k)$ be the number of equivalence classes of $\underset{n}{\equiv}$ restricted to S^k.

Lemma 2: Let $n,k \in N$. Then $M(n,k)$ is finite and for all $\vec{a}_k \in S^k$ there is a Formula $F(\vec{x}_k)$ of q-depth n such that for all $\vec{b}_k \in S^k$, $F(\vec{b}_k) \Leftrightarrow \vec{b}_k \underset{n}{\equiv} \vec{a}_k$ (i.e., F defines the $\underset{n}{\equiv}$ equivalence class of $\vec{a}_k$).

Proof (by induction on n): If $n=0$ and $\vec{a}_k \in S^k$, we can clearly take $F(\vec{x}_k)$ to be a conjunction of atomic formulas and negations of atomic formulas. The number of atomic formulas free in at most $x_1, x_2, \ldots, x_k$ is $\sum_{i=1}^{\ell}(k+1)^{t_i}$.

So $M(0,k) \le 2^{\sum_{i=1}^{\ell}(k+1)^{t_i}}$.

So assume the Lemma true for n (and all k). We shall prove it for n+1 (and k). Let $F_1(\vec{x}_{k+1}), F_2(\vec{x}_{k+1}), \ldots, F_{M(n,k+1)}(\vec{x}_{k+1})$ be a sequence of formulas of q-depth n such that for each $\vec{a}_{k+1} \in S^{k+1}$ there exists an i, $1 \le i \le M(n,k+1)$, such that F_i defines the $\underset{n}{\equiv}$ equivalence class of $\vec{a}_{k+1}$.

For each $\vec{c}_k \in S^k$ define

$W(\vec{c}_k) = \{ i \mid 1 \le i \le M(n,k+1) \text{ and } \exists x_{k+1} F_i(\vec{c}_k, x_{k+1}) \text{ is true } \}$. We shall show that for all $\vec{b}_k, \vec{c}_k \in S^k$, $\vec{b}_k \underset{n+1}{\equiv} \vec{c}_k \Leftrightarrow W(\vec{b}_k) = W(\vec{c}_k)$. Thus the formula $F(\vec{x}_k) =$

$$\left(\bigwedge_{i \in W(\vec{c}_k)} \exists x_{k+1} F_i(\vec{x}_{k+1}) \right) \wedge \left(\bigwedge_{\substack{i \notin W(\vec{c}_k) \\ 1 \le i \le M(n,k+1)}} \sim\exists x_{k+1} F_i(\vec{x}_{k+1}) \right)$$

defines the $\underset{n+1}{\equiv}$ equivalence class of $\vec{c}_k$.

Clearly if $\vec{b}_k \underset{n+1}{\equiv} \vec{c}_k$, then $W(\vec{b}_k) = W(\vec{c}_k)$ by definition since each formula $\exists x_{k+1} F_i(\vec{x}_{k+1})$ is of q-depth n+1. To prove the converse we first prove the following:

<u>Lemma 2.1</u>: If $W(\vec{b}_k) = W(\vec{c}_k)$, then for each $c_{k+1} \in S$ there exists some $b_{k+1} \in S$ such that $\vec{c}_{k+1} \underset{n}{\equiv} \vec{b}_{k+1}$ (and by symmetry, for each $b_{k+1} \in S$ there exists some $c_{k+1} \in S$ such that $\vec{c}_{k+1} \underset{n}{\equiv} \vec{b}_{k+1}$).

<u>Proof of Lemma 2.1</u>: Say that $W(\vec{b}_k) = W(\vec{c}_k)$ and $c_{k+1} \in S$. Let i, $1 \le i \le M(n,k+1)$, be such that $F_i(\vec{x}_{k+1})$ defines the $\underset{n}{\equiv}$ equivalence class of $\vec{c}_{k+1}$. $F_i(\vec{c}_{k+1})$ is true, so $\exists x_{k+1} F_i(\vec{c}_k, x_{k+1})$ is true, so $i \in W(\vec{c}_k)$. So $i \in W(\vec{b}_k)$. This means that $\exists x_{k+1} F_i(\vec{b}_k, x_{k+1})$ is true, and therefore we can find $\vec{b}_{k+1}$ such that $F_i(\vec{b}_{k+1})$. Since F_i defines the $\underset{n}{\equiv}$ equivalence class of $\vec{c}_{k+1}$, we must have $\vec{c}_{k+1} \underset{n}{\equiv} \vec{b}_{k+1}$.

By Lemmas 2.1 and 1, $W(\vec{b}_k) = W(\vec{c}_k) \Rightarrow \vec{b}_k \underset{n+1}{\equiv} \vec{c}_k$. Note that the $\underset{n+1}{\equiv}$ equivalence class of $\vec{c}_k$ is determined by $W(\vec{c}_k)$ which is a subset of $\{1, 2, \ldots, M(n,k+1)\}$. So $M(n+1,k) \le 2^{M(n,k+1)}$. This and the bound on $M(0,k)$ imply that

$$M(n,k) \le 2^{2^{2^{\cdot^{\cdot^{\cdot^{2^{(n+k)^c}}}}}}} \Big\} \text{height } n+1$$ for some constant c. □

Remark: There are structures $\mathcal{S}$ such that

$$M(n,k) \ge 2^{2^{2^{\cdot^{\cdot^{\cdot^{2^{n+k}}}}}}} \Big\} \text{height } \epsilon n$$ (for some constant ϵ), so $M(n,k)$ is not in general bounded above by an elementary recursive function. For many structures, however, $M(n,k)$ grows considerably more slowly.

Definition: Let $H:N^3 \to N$. Then $\mathcal{S}$ is H-bounded iff for all $n,k \in N$ and all $F(\vec{x}_{k+1})$ of q-depth $\le n$ and all $\vec{a}_k \in S^k$, if $\exists x_{k+1} F(\vec{a}_k, x_{k+1})$ is true in $\mathcal{S}$ then $[\exists x_{k+1} \le H(n,k,\underset{1\le i\le k}{\mathrm{Max}}\{||a_i||\})]F(\vec{a}_k,x_{k+1})$ is true in $\mathcal{S}$. (We take $\mathrm{Max}\ \emptyset$ to be 0.)

For the rest of this section, let $H:N^3 \to N$ be a fixed function such that $\mathcal{S}$ is H-bounded; we will also assume that H is nondecreasing in each argument. H-boundedness of a structure guarantees that quantifiers ranging over all of S in a sentence can be replaced by quantifiers ranging over elements of S whose norms are bounded by a function determined by H. This is made precise in the following lemma.

Lemma 3: Let $n,k \in N$ and let $Q_1x_1 Q_2x_2 \ldots Q_kx_kF(\vec{x}_k)$ be a sentence of $\mathcal{L}$ ($Q_i = \forall$ or $\exists$ for each i, $1 \le i \le k$) with q-depth $\le n+k$, i.e., q-depth$(F) \le n$. Let $\vec{m}_k \in N^k$ be a sequence such that $m_i \ge H(n+k-i, i-1, \underset{1\le j<i}{\mathrm{Max}}\{m_j\})$ for $1 \le i \le k$. Then $Q_1x_1 Q_2x_2 \ldots Q_kx_kF(\vec{x}_k)$ is true $\Leftrightarrow$ $(Q_1x_1 \le m_1)(Q_2x_2 \le m_2)\ldots(Q_kx_k \le m_k)F(\vec{x}_k)$ is true.

Proof: Consider the formula $Q_2x_2 Q_3x_3 \ldots Q_kx_xF(\vec{x}_k)$. Because $\mathcal{S}$ is H-bounded, if $m_1 \geq H(n+k-1,0,0)$ then $Q_1x_1(Q_2x_2 \ldots Q_kx_kF(\vec{x}_k))$ is equivalent to $(Q_1x_1 \leq m_1)(Q_2x_2 \ldots Q_kx_kF(\vec{x}_k))$.

Now for each $a \in S$ such that $||a|| \leq m_1$, consider the formula $Q_3x_3\, Q_4x_4 \ldots Q_kx_kF(a,x_2,x_3,\ldots,x_k)$. Because $\mathcal{S}$ is H-bounded, if $m_2 \geq H(n+k-2,1,m_1)$ then $Q_2x_2(Q_3x_3 \ldots Q_kx_kF(a,x_2,x_3,\ldots,x_k))$ is equivalent to $(Q_2x_2 \leq m_2)(Q_3x_3 \ldots Q_kx_kF(a,x_2,x_3,\ldots,x_k))$. Hence, $(Q_1x_1 \leq m_1)Q_2x_2 \ldots Q_kx_kF(\vec{x}_k)$ is equivalent to $(Q_1x_1 \leq m_1)(Q_2x_2 \leq m_2)Q_3x_3\, Q_4x_4 \ldots Q_kx_kF(\vec{x}_k)$.

By k-2 additional applications of the H-boundedness of $\mathcal{S}$, we arrive at Lemma 3. □

Remark: The reason the concepts of norm and H-boundedness for $\mathcal{S}$ were introduced is because they have relevance in particular cases towards achieving efficient and easily described decision prodedures for the theories of $\mathcal{S}$ and the weak direct product of $\mathcal{S}$ with itself. Many of our lemmas and theorems (such as Lemma 1), however, either don't involve these concepts at all or have simpler versions which don't involve them. So even if all mention of norm or H-boundedness is ignored, this section implicitly contains important results about the nature of the weak direct product of $\mathcal{S}$ with itself.

Lemma 4: Let $n,k \in N$ and let $\vec{m}_k \in N^k$ be a sequence such that $m_i \geq H(n+k-i, i-1, \underset{1 \leq j < i}{\mathrm{Max}}\{m_j\})$ for $1 \leq i \leq k$. Then for each $\vec{a}_k \in S^k$ there is some $\vec{b}_k \in S^k$ such that $\vec{a}_k \equiv_n \vec{b}_k$ and $||b_i|| \leq m_i$ for $1 \leq i \leq k$.

Proof: Let $n, k, \vec{m}_k$, and $\vec{a}_k$ be as in the statment of the Lemma. By Lemma 2 there is a formula $F(\vec{x}_k)$ of q-depth n which defines the $\equiv_n$ equivalence class of $\vec{a}_k$. Since $F(\vec{a}_k)$ is true, $\exists x_1 \exists x_2 \ldots \exists x_k F(\vec{x}_k)$ is true. So by Lemma 3, $(\exists x_1 \leq m_1)(\exists x_2 \leq m_2)\ldots(\exists x_k \leq m_k)F(\vec{x}_k)$ is true. This means that for some $\vec{b}_k \in S^k$, $F(\vec{b}_k)$ is true and $||b_i|| \leq m_i$ for $1 \leq i \leq k$. □

<u>Lemma</u> <u>5</u>: Let $n,k \in N$ and let $\vec{a}_k,\vec{b}_k \in S^k$. If $\vec{a}_k \underset{n+1}{\equiv} \vec{b}_k$ then for each $a_{k+1} \in S$ there exists some $b_{k+1} \in S$ such that $\vec{a}_{k+1} \underset{n}{\equiv} \vec{b}_{k+1}$ and $||b_{k+1}|| \leq H(n,k,\underset{1\leq i\leq k}{\mathrm{Max}}\{||b_i||\})$.

<u>Proof</u>: Let $\vec{a}_k,\vec{b}_k \in S^k$ such that $\vec{a}_k \underset{n+1}{\equiv} \vec{b}_k$. Let $a_{k+1} \in S$. By Lemma 2 there is a formula $F(\vec{x}_{k+1})$ of q-depth n defining the $\underset{n}{\equiv}$ equivalence class of $\vec{a}_{k+1}$. Since $\exists x_{k+1}F(\vec{a}_k,x_{k+1})$ is true and $\vec{a}_k \underset{n+1}{\equiv} \vec{b}_k$, $\exists x_{k+1}F(\vec{b}_k,x_{k+1})$ is true. Since $\mathbb{S}$ is H-bounded, we can choose $b_{k+1} \in S$ such that $F(\vec{b}_{k+1})$ and $||b_{k+1}|| \leq H(n,k,\underset{1\leq i\leq k}{\mathrm{Max}}\{||b_i||\})$. But $F(\vec{b}_{k+1})$ implies $\vec{b}_{k+1} \underset{n}{\equiv} \vec{a}_{k+1}$. □

<u>Lemma</u> <u>6</u>: Let $n,k \in N$ and $\vec{a}_k,\vec{b}_k \in S^k$. Then $\vec{a}_k \underset{n+1}{\equiv} \vec{b}_k \Leftrightarrow$

1) For each $a_{k+1} \in S$ there exists some $b_{k+1} \in S$ such that $\vec{a}_{k+1} \underset{n}{\equiv} \vec{b}_{k+1}$.

and 2) For each $b_{k+1} \in S$ there exists some $a_{k+1} \in S$ such that $\vec{a}_{k+1} \underset{n}{\equiv} \vec{b}_{k+1}$.

<u>Proof</u>: Immediate from Lemmas 1 and 5. □

<u>Lemma</u> <u>7</u>: Let $n,k \in N$. Then there exists a formula $F_{n,k}(\vec{x}_k,\vec{y}_k)$ with exactly 6n quantifiers such that for all $\vec{a}_k,\vec{b}_k \in S^k$, $F_{n,k}(\vec{a}_k,\vec{b}_k) \Leftrightarrow \vec{a}_k \underset{n}{\equiv} \vec{b}_k$.

<u>Proof</u>: The Lemma is clearly true if n=0. So assume it is true for n; we will prove it for n+1. By Lemma 6, we can define $F_{n+1,k}$ as follows:

$$\forall x_{k+1}\exists y_{k+1}\forall y'_{k+1}\exists x'_{k+1}\forall x\forall y([(x=x_{k+1} \wedge y=y_{k+1}) \vee (x=x'_{k+1} \wedge y=y'_{k+1})] \rightarrow F_{n,k+1}(\vec{x}_k,x,\vec{y}_k,y)).$$

$F_{n+1,k}$ clearly has 6 more quantifiers than $F_{n,k+1}$. □

Definition: Define the structure $\mathcal{S}^*=\langle S^*,\mathcal{R}_1^*,\mathcal{R}_2^*,\ldots,\mathcal{R}_\ell^*,e^*\rangle$:
$S^*=\{f:N\to S \mid f(i)\neq e$ for only finitely many $i\in N\}$;
for $1\le j\le \ell$, if $\vec{f}_{t_j}\in (S^*)^{t_j}$, then $\vec{f}_{t_j}\in \mathcal{R}_j^*$ iff $\vec{f}_{t_j}(i)\in\mathcal{R}_j$ for all $i\in N$
(where $\vec{f}_{t_j}(i)$ abbreviates $(f_1(i),f_2(i),\ldots,f_{t_j}(i))$);
$e^*(i)=e$ for all $i\in N$. (That is, $\mathcal{S}^*$ is the weak direct product of $\mathcal{S}$ with itself.)

For a norm on $\mathcal{S}^*$ we define, for $f\in S^*$,
$||f||=\mathrm{Max}\{\ \{i\in N \mid f(i)\neq e\}\cup\{||f(i)|| \ \ |i\in N\}\ \}$. By $f\preceq m$ we will mean $||f||\le m$.

Definition: Define the function $\mu:N^2\to N$ by setting $\mu(0,k)=1$ and $\mu(n+1,k)=M(n,k+1)\cdot\mu(n,k+1)$. So $\mu(n,k)=\prod_{i=1}^{n}M(n-i,k+i)$.

Definition: Define $H^*:N^3\to N$ by $H^*(n,k,m)=\mathrm{Max}\{H(n,k,m),m+\mu(n+1,k),||e||\}$.

The major theorem of this section will be

Theorem 1: $\mathcal{S}^*$ is H^*-bounded.

Definition: Let A and B be sets, let $n\in N$. Then $A \underset{n}{\sim} B$ iff either

1) card(A)=card(B) (where card abbreviates cardinality)

or 2) card(A) $\ge n$ and card(B) $\ge n$.

Clearly $\underset{n}{\sim}$ is an equivalence relation on the class of sets.

We now prove a combinatorial lemma:

Lemma 8: Let N_1 and N_2 be sets and let $n,m\in N$ such that $n\neq 0$ and $N_1 \underset{n\cdot m}{\sim} N_2$. Let $A_1,A_2,\ldots,A_n$ be a sequence of (possibly empty) pairwise disjoint subsets of N_1 such that $\bigcup_{i=1}^{n} A_i = N_1$.

Then there exists a sequence $B_1,B_2,\ldots,B_n$ of pairwise disjoint subsets of N_2 such that $\bigcup_{i=1}^{n} B_i = N_2$ and such that $A_i \underset{m}{\sim} B_i$ for $1\le i\le n$.

Proof: If $card(N_1)=card(N_2)$ then the Lemma is obvious. So assume $card(N_1) \geq n\cdot m$ and $card(N_2) \geq n\cdot m$. For some i, $1 \leq i \leq n$, we must have $card(A_i) \geq m$, so assume without loss of generality that $card(A_1) \geq m$.

Define numbers $p_2, p_3, \ldots, p_n \in N$ by

$$p_i = \begin{cases} card(A_i) & \text{if } card(A_i) < m \\ m & \text{if } card(A_i) \geq m \end{cases} \quad \text{for } 2 \leq i \leq n.$$

Clearly $\sum_{i=2}^{n} p_i \leq (n-1)\cdot m$. Since $card(N_2) \geq n\cdot m$, there exists a sequence of pairwise disjoint subsets of N_2, namely $B_2, B_3, \ldots, B_n$, such that $card(B_i)=p_i$ for $2 \leq i \leq n$. So $A_i \underset{m}{\sim} B_i$ for $2 \leq i \leq n$. Let $B_1=N_2-\bigcup_{i=2}^{n} B_i$. $card(N_2) \geq n\cdot m$ and $card(\bigcup_{i=2}^{n} B_i) \leq n\cdot m - m$, so $card(B_1) \geq m$. Since $card(A_1) \geq m$, $A_1 \underset{m}{\sim} B_1$. □

Definition: Let $n,k \in N$ and $\vec{f}_k, \vec{g}_k \in (S^*)^k$. Then we say $\vec{f}_k \; E_n \; \vec{g}_k$ iff for all $\vec{a}_k \in S^k$, $\{i \in N \mid \vec{f}_k(i) \underset{n}{\equiv} \vec{a}_k\} \underset{\mu(n,k)}{\sim} \{i \in N \mid \vec{g}_k(i) \underset{n}{\equiv} \vec{a}_k\}$.

Remark: E_n is an equivalence relation on $(S^*)^k$. We will show that if $\vec{f}_k \; E_n \; \vec{g}_k$ and if $F(\vec{x}_k)$ has q-depth $\leq n$, then $F(\vec{f}_k)$ and $F(\vec{g}_k)$ are either both true or both false in $\mathcal{S}^*$.

Lemma 9: For all $k \in N$ and $\vec{f}_k, \vec{g}_k \in (S^*)^k$, if $\vec{f}_k \; E_0 \vec{g}_k$ and if $F(\vec{x}_k)$ is a quantifier free formula (q-depth(F)=0), then $F(\vec{f}_k)$ is true in $\mathcal{S}^*$ if and only if $F(\vec{g}_k)$ is true in $\mathcal{S}^*$.

Proof: Clearly it is sufficient to prove the Lemma for the case where F is atomic. So say that $\vec{f}_k \; E_0 \; \vec{g}_k$ and $F(\vec{x}_k)$ is an atomic formula. By symmetry, it is sufficient to show that $F(\vec{f}_k)$ false in $\mathcal{S}^* \Rightarrow F(\vec{g}_k)$ false in $\mathcal{S}^*$.

So assume that $F(\vec{f}_k)$ is false in $\mathcal{S}^*$. By definition of the relations of $\mathbb{S}^*$ we can choose $i_0 \in N$ such that $F(\vec{f}_k(i_0))$ is false in $\mathbb{S}$. Since $\vec{f}_k\ E_0\ \vec{g}_k$, $\{i \in N \mid \vec{f}_k(i) \underset{0}{\equiv} \vec{f}_k(i_0)\} \underset{\mu(0,k)}{\sim} \{i \in N \mid \vec{g}_k(i) \underset{0}{\equiv} \vec{f}_k(i_0)\}$. Since $\mu(0,k)=1$, we have $\mathrm{card}(\{i \in N \mid \vec{g}_k(i) \underset{0}{\equiv} \vec{f}_k(i_0)\}) \geq 1$. So let $i_1 \in N$ be such that $\vec{g}_k(i_1) \underset{0}{\equiv} \vec{f}_k(i_0)$. By definition of $\underset{0}{\equiv}$, $F(\vec{f}_k(i_0))$ false in $\mathbb{S} \Rightarrow F(\vec{g}_k(i_1))$ false in $\mathbb{S}$. So $F(\vec{g}_k)$ is false in $\mathbb{S}^*$. □

<u>Lemma 10</u>: Let $n,k \in N$ and $\vec{f}_k,\vec{g}_k \in (S^*)^k$ such that $\vec{f}_k\ E_{n+1}\ \vec{g}_k$. Then for each $f_{k+1} \in S^*$ there exists some $g_{k+1} \in S^*$ such that

1) $\vec{f}_{k+1}\ E_n\ \vec{g}_{k+1}$

and 2) $||g_{k+1}|| \leq H^*(n,k,\underset{1\leq i\leq k}{\mathrm{Max}}\{||g_i||\})$.

<u>Proof</u>: Let $\vec{f}_k,\vec{g}_k \in (S^*)^k$ be such that $\vec{f}_k\ E_{n+1}\ \vec{g}_k$. Let $m=\underset{1\leq i\leq k}{\mathrm{Max}}\{||g_i||\}$ and let $f_{k+1} \in S^*$. Let $\vec{b}^1_{k+1},\vec{b}^2_{k+2},\ldots,\vec{b}^{M(n,k+1)}_{k+1}$ be a sequence of representatives of all the $\underset{n}{\equiv}$ equivalence classes on S^{k+1}. Our goal is to find $g_{k+1} \in S^*$ such that if $1 \leq j \leq M(n,k+1)$, then $\{i \in N \mid \vec{f}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\} \underset{\mu(n,k+1)}{\sim} \{i \in N \mid \vec{g}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\}$; we also want $||g_{k+1}|| \leq H^*(n,k,m)$. Instead of defining g_{k+1} simultaneously on all of N, we will define it separately on various pieces of N.

For each $\vec{a}_k \in S^k$ define $N_1(\vec{a}_k)=\{i \in N \mid \vec{f}_k(i) \underset{n+1}{\equiv} \vec{a}_k\}$ and $N_2(\vec{a}_k)=\{i \in N \mid \vec{g}_k(i) \underset{n+1}{\equiv} \vec{a}_k\}$. We claim it is sufficient to define g_{k+1} on each $N_2(\vec{a}_k)$ such that

I) $\{i \in N_1(\vec{a}_k) \mid \vec{f}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\} \underset{\mu(n,k+1)}{\sim} \{i \in N_2(\vec{a}_k) \mid \vec{g}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\}$

for all j, $1 \leq j \leq M(n,k+1)$.

II) If $i \in N_2(\vec{a}_k)$ and $i > m+\mu(n+1,k)$, then $g_{k+1}(i)=e$.

and III) If $i \in N_2(\vec{a}_k)$ and $i \leq m+\mu(n+1,k)$, then $||g_{k+1}(i)|| \leq H(n,k,m)$.

An examination of the definitions of H^* and the norm on S^* will show that II) and III) together imply $||g_{k+1}|| \leq H^*(n,k,m)$. Since $\{N_1(\vec{a}_k) \mid \vec{a}_k \in S^k\}$ and $\{N_2(\vec{a}_k) \mid \vec{a}_k \in S^k\}$ are each a collection of disjoint sets, it is easy to see from I) and the definition of $\sim_{\mu(n,k+1)}$ that if $1 \leq j \leq M(n,k+1)$ then

$$\Big(\bigcup_{\vec{a}_k \in S^k} \{i \in N_1(\vec{a}_k) \mid \vec{f}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\}\Big) \sim_{\mu(n,k+1)} \Big(\bigcup_{\vec{a}_k \in S^k} \{i \in N_2(\vec{a}_k) \mid \vec{g}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\}\Big),$$

i.e., $\{i \in N \mid \vec{f}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\} \sim_{\mu(n,k+1)} \{i \in N \mid \vec{g}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\}$.

So now let $\vec{a}_k \in S^k$ be fixed for the rest of this proof. Abbreviate $N_1(\vec{a}_k)$ by N_1 and $N_2(\vec{a}_k)$ by N_2. Begin by defining $g_{k+1}(i)=e$ if $i \in N_2$ and $i > m+\mu(n+1,k)$; this guarentees II) above. It remains to define g_{k+1} on $N_3=\{i \in N_2 \mid i \leq m+\mu(n+1,k)\}$.

The definition of E_{n+1} implies that $N_1 \sim_{\mu(n+1,k)} N_2$. We wish however to demonstrate that $N_1 \sim_{\mu(n+1,k)} N_3$: If $\vec{a}_k \underset{n+1}{\equiv} \underbrace{(e,e,\ldots,e)}_{\text{length } k}$, then N_1 is an infinite set, and $\text{card}(N_3) \geq \mu(n+1,k)$ since $\vec{g}_k(i)=\underbrace{(e,e,\ldots,e)}_{\text{length } k}$ for $m < i \leq m+\mu(n+1,k)$; if $\vec{a}_k \underset{n+1}{\not\equiv} \underbrace{(e,e,\ldots,e)}_{\text{length } k}$, then $N_3=N_2$ (since $i > m+\mu(n+1,k) \Rightarrow \vec{g}_k(i)=\underbrace{(e,e,\ldots,e)}_{\text{length } k} \Rightarrow i \notin N_2$). So $N_1 \sim_{\mu(n+1,k)} N_3$.

Define, for $1 \leq j \leq M(n,k+1)$, $A_j=\{i \in N_1 \mid \vec{f}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\}$. $A_1, A_2, \ldots, A_{M(n,k+1)}$ form a sequence of pairwise disjoint sets whose union is N_1. Since $N_1 \sim_{\mu(n+1,k)} N_3$ and $\mu(n+1,k)=M(n,k+1)\cdot\mu(n,k+1)$, Lemma 8 tells us there exists a sequence $B_1, B_2, \ldots, B_{M(n,k+1)}$ of pairwise disjoint subsets of N_3 whose union is N_3 such that $A_j \sim_{\mu(n,k+1)} B_j$ if $1 \leq j \leq M(n,k+1)$.

Now let $i \in N_3$; we want to define g_{k+1} on i. Let j be such that $i \in B_j$. Since $B_j \neq \emptyset$, $A_j \neq \emptyset$. So let $i_0 \in A_j$. Since $i_0 \in N_1$ and $i \in N_2$, we have $\vec{f}_k(i_0) \underset{n+1}{\equiv} \vec{a}_k \underset{n+1}{\equiv} \vec{g}_k(i)$. By Lemma 5 we can define $g_{k+1}(i)$ such that $\vec{f}_{k+1}(i_0) \underset{n}{\equiv} \vec{g}_{k+1}(i)$ and

$||g_{k+1}(i)|| \le H(n,k,\text{Max}\{||g_1(i)||, ||g_2(i)||, \ldots, ||g_k(i)||\}) \le H(n,k,m)$.

Clearly III) above holds. Since $i_0 \in A_j$, $\vec{f}_{k+1}(i_0) \underset{n}{\equiv} \vec{b}^j_{k+1}$. So $\vec{g}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}$.

We have

$\{i \in N_3 \mid \vec{g}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\} = B_j \underset{\mu(n,k+1)}{\sim} A_j = \{i \in N_1 \mid \vec{f}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\}$ for $1 \le j \le M(n,k+1)$. To complete the proof of Lemma 10 we must show I), i.e., $\{i \in N_2 \mid \vec{g}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\} \underset{\mu(n,k+1)}{\sim} A_j$ when $1 \le j \le M(n,k+1)$.

So fix j, $1 \le j \le M(n,k+1)$. If $\{i \in N_2 \mid \vec{g}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\} = \{i \in N_3 \mid \vec{g}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\}$ we are done, so assume $\{i \in N_2 \mid \vec{g}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\} \ne \{i \in N_3 \mid \vec{g}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\}$. Since $N_3 = \{i \in N_2 \mid i \le m + \mu(n+1,k)\}$, there must exist some $i > m + \mu(n+1,k)$ such that $i \in N_2$ (hence $\vec{g}_k(i) \underset{n+1}{\equiv} \vec{a}_k$) and $\vec{g}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}$. But since $i > m + \mu(n+1,k)$ implies $\vec{g}_{k+1}(i) = \underbrace{(e,e,\ldots,e)}_{\text{length } k+1}$, this means that $\vec{a}_k \underset{n+1}{\equiv} \underbrace{(e,e,\ldots,e)}_{\text{length } k}$ and $\vec{b}^j_{k+1} \underset{n}{\equiv} \underbrace{(e,e,\ldots,e)}_{\text{length } k+1}$. Hence, both A_j and $\{i \in N_2 \mid \vec{g}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\}$ are infinite, so $\{i \in N_2 \mid \vec{g}_{k+1}(i) \underset{n}{\equiv} \vec{b}^j_{k+1}\} \underset{\mu(n,k+1)}{\sim} A_j$. □

<u>Lemma</u> <u>11</u>: Let $\vec{f}_k, \vec{g}_k \in (S^*)^k$ and let $F(\vec{x}_k)$ be a formula of q-depth $\le n$. If $\vec{f}_k \; E_n \; \vec{g}_k$, then $F(\vec{f}_k)$ is true in $\mathcal{S}^* \Leftrightarrow F(\vec{g}_k)$ is true in $\mathcal{S}^*$.

<u>Proof</u> (by induction on n): If n=0 then Lemma 11 follows from Lemma 9. So assume Lemma 11 true for n (and all k); we will prove it for n+1.

Let $\vec{f}_k, \vec{g}_k \in (S^*)^k$ such that $\vec{f}_k \; E_{n+1} \; \vec{g}_k$. By Lemma 10 (1), we have

a) For each $f_{k+1} \in S^*$ there exists some $g_{k+1} \in S^*$ such that $\vec{f}_{k+1}\ E_n\ \vec{g}_{k+1}$.

and b) For each $g_{k+1} \in S^*$ there exists some $f_{k+1} \in S^*$ such that $\vec{f}_{k+1}\ E_n\ \vec{g}_{k+1}$.

By the induction hypothesis, $\vec{f}_{k+1}\ E_n\ \vec{g}_{k+1}$ implies that $\vec{f}_{k+1}$ and $\vec{g}_{k+1}$ satisfy the same depth n formulas in $\mathcal{S}^*$. We can therefore prove, exactly as in Lemma 1, that a) and b) together imply that $\vec{f}_k$ and $\vec{g}_k$ satisfy the same depth n+1 formulas. □

Theorem 1: $\mathcal{S}^*$ is H^*-bounded.

Proof: Let $F(\vec{x}_{k+1})$ be a formula of q-depth $\leq n$ and let $\vec{f}_k \in (S^*)^k$ be such that $\exists x_{k+1} F(\vec{f}_k, x_{k+1})$ is true in $\mathcal{S}^*$. Let $f_{k+1} \in S^*$ be such that $F(\vec{f}_{k+1})$ is true. Since $\vec{f}_k\ E_{n+1}\ \vec{f}_k$, Lemma 10 implies that for some $f'_{k+1} \in S^*$, $\vec{f}_{k+1}\ E_n\ (\vec{f}_k, f'_{k+1})$ and $||f'_{k+1}|| \leq H^*(n,k, \max_{1\leq i\leq k}\{||f_i||\})$. It is sufficient now to show that $F(\vec{f}_k, f'_{k+1})$ is true. But this is obvious from Lemma 11, since $F(\vec{f}_{k+1})$ is true and $\vec{f}_{k+1}\ E_n(\vec{f}_k, f'_{k+1})$ and q-depth(F) $\leq$ n. ■

Remarks: The complexity of $\mathcal{S}^*$ is related to the complexities of M(n,k) and $\mathcal{S}$ as follows:

Theorem 2: If the theory of $\mathcal{S}$ is elementary recursive and M(n,k) is bounded above by an elementary recursive function, then the theory of $\mathcal{S}^*$ is elementary recursive.

Theorem 2 follows either from a generalization of the results of this section or from a careful examination of Mostowski's decision procedure for $\mathcal{S}^*$ [9]; a proof will not be given here. It is interesting to note that in all cases we know of where the theory of $\mathcal{S}$ is proven to be elementary recursive, the proof essentially consists of giving an Ehrenfeucht game [3] decision procedure, which in turn shows that M(n,k) is elementary recursive. This suggests the following conjecture.

<u>Conjecture 1</u>: If the theory of $\mathcal{S}$ is elementary recursive, then M(n,k) is bounded above by an elementary recursive function.

The converses of both Theorem 2 and Conjecture 1 are false, as we will now indicate by an example. Let our language $\mathcal{L}$ consist of two relations, $x_1=x_2$ and $x_1 \approx x_2$ (x_1 equivalent to x_2), and the constant symbol 0. For every nonempty set A of integers greater than 1, let $\underset{A}{\approx}$ be an equivalence relation on N such that for every integer i

1) If $i \in A$ then there is exactly one $\underset{A}{\approx}$ equivalence class of size i.

and 2) If $i \notin A$ then there are no $\underset{A}{\approx}$ equivalence classes of size i.

Define the structure $\mathcal{S}_A = \langle N, =, \underset{A}{\approx}, 0 \rangle$.

Since for any integer i we can say in $\mathcal{L}$ that there exists an equivalence class of size i, by varying A we can make the theory of $\mathcal{S}_A$ arbitrarily hard to decide or arbitrarily nonrecursive. But it is easy to see that $\mathcal{S}_A^*$ is merely an infinite collection of infinite equivalence classes and hence has a simple theory; in fact, the theory of $\mathcal{S}_A^*$ can be decided in polynomial space. So the converse of Theorem 2 is false.

Now let A be a fixed set of positive integers and consider M(n,k) for $\mathcal{S}_A$; we will show that (no matter what A is) M(n,k) is bounded above by an elementary recursive function, contradicting the converse of Conjecture 1.

For each $\vec{a}_k, \vec{b}_k \in N^k$ define $\vec{a}_k \; R_n \; \vec{b}_k$ iff for all i,j such that $1 \le i,j \le k$,

I) $a_i \underset{A}{\approx} 0 \Leftrightarrow b_i \underset{A}{\approx} 0$, and $a_i=0 \Leftrightarrow b_i=0$.

II) $a_i \underset{A}{\approx} a_j \Leftrightarrow b_i \underset{A}{\approx} b_j$, and $a_i=a_j \Leftrightarrow b_i=b_j$.

and III) $\{a \in N \mid a \underset{A}{\approx} a_i\} \underset{n}{\sim} \{b \in N \mid b \underset{A}{\approx} b_i\}$.

It is not difficult to show that $\vec{a}_k \; R_n \; \vec{b}_k \Rightarrow \vec{a}_k \underset{n}{\equiv} \vec{b}_k$. Since the number of R_n equivalence classes on N^k is bounded above by an elementary recursive function (of n and k), so is M(n,k) for $\mathbb{S}_A$.

Remark: Although we have onlydealt here with the weak direct product of $\mathbb{S}$ with itself, a similar development can be carried out for the strong direct product of $\mathbb{S}$ with itself.

Section 3: Some Applications

Let $\mathcal{L}_1$ be the language of the first order predicate calculus with the predicates $x_1 \le x_2$ and $x_1+x_2=x_3$, and the constant symbol 0. Let Z be the set of integers and let I be the structure $< Z,\le,+,0 >$. Let $Z^*=\{f:N\to Z \mid f(i)\neq 0$ for only finitely many $i\in N\}$ and let I^* be the structure $< Z^*,\le,+,0^* >$ where $\le$ and $+$ are defined component-wise and 0^* is the identically 0 function. For $a\in Z$ let the norm of a be $|a|$, the absolute value of a. For $f\in Z^*$ let the norm of f, written $||f||$, be $\text{Max}\{ \{|f(i)| \mid i\in N\} \cup \{i\in N \mid f(i)\neq 0\} \}$ as in section 2. By $a\preceq m$ and $f\preceq m$ we will mean $|a|\le m$ and $||f||\le m$, respectively.

Lemma 12: There is a constant c such that for all $n,k\in N$ and all $\vec{a}_k\in Z^k$ and all formulas $F(\vec{x}_{k+1})$ of $\mathcal{L}_1$ with no more than n quantifiers, if $\exists x_{k+1}F(\vec{a}_k,x_{k+1})$ is true in I, then

$$[\exists x_{k+1}\preceq (1+\underset{1\le i\le k}{\text{Max}}\{|a_i|\})\cdot 2^{2^{2^{c(n+k)}}}]F(\vec{a}_k,x_{k+1}) \text{ is true in I.}$$

Proof: See Ferrante and Rackoff [4]. □

Lemma 13: There is a constant c_o such that I is H-bounded where $H(n,k,m)=(1+m)\cdot 2^{2^{2^{c_o(n+k)}}}$.

Proof: Let $n,k\in N$ and $\vec{a}_k\in Z^k$ and $F(\vec{x}_{k+1})$ be a formula of $\mathcal{L}_1$ such that $\exists x_{k+1}F(\vec{a}_k,x_{k+1})$ is true in I and q-depth(F) $\le$ n. Let $m=\underset{1\le i\le k}{\text{Max}}\{|a_i|\}$.

By Lemma 7, let $F_{n,k+1}(\vec{x}_{k+1},\vec{y}_{k+1})$ be a formula with exactly 6n quantifiers which defines the relation $\equiv_n$ on Z^{k+1}. Let $G(\vec{x}_k,x)$ be the formula $\forall x_{k+1}\exists x'_{k+1}(F_{n,k+1}(\vec{x}_k,x_{k+1},\vec{x}_k,x'_{k+1}) \wedge -x\le x'_{k+1}\le x)$.

Clearly G has $6n+2$ quantifiers and $\exists x\, G(\vec{a}_k, x)$ is true (in I). By Lemma 12 we can find $a \in Z$ such that $G(\vec{a}_k, a)$ is true and $|a| \le (1+m)\cdot 2^{2^{2^{c(6n+2+k)}}}$.

Now let $a_{k+1} \in Z$ be such that $F(\vec{a}_{k+1})$ is true. Since $G(\vec{a}_k, a)$ is true, we can find $a'_{k+1} \in Z$ such that $\vec{a}_{k+1} \equiv_n (\vec{a}_k, a'_{k+1})$ and $|a'_{k+1}| \le (1+m)\cdot 2^{2^{2^{c(6n+2+k)}}} \le (1+m)\cdot 2^{2^{2^{c_o(n+k)}}}$ for some constant c_o (unless n=k=0, a trivial case). Since $F(\vec{a}_{k+1})$ holds and q-depth(F) $\le n$, $F(\vec{a}_k, a'_{k+1})$ holds and the Lemma is proved. □

<u>Theorem</u> <u>3</u>: For some constant c_1, the theory of I can be decided in space $2^{2^{2^{c_1 n}}}$ (as a function of the length of sentences).

<u>Proof</u>: Let F be a sentence of $\mathcal{L}_1$ which in prenex normal form is $Q_1x_1\, Q_2x_2 \ldots Q_nx_n\, G(\vec{x}_n)$ where G is quantifier free. Let $m_i = 2^{2^{2^{c_o n+i}}}$ for $1 \le i \le n$. Applying Lemma 3 to I, we see that since $m_i \ge H(n-i, i-1, \underset{1\le j<i}{\mathrm{Max}}\{|m_j|\})$ for $1 \le i \le n$, F is equivalent to $(Q_1x_1 \le m_1)(Q_2x_2 \le m_2)\ldots(Q_nx_n \le m_n)\, G(\vec{x}_n)$.

F can be decided in I by setting aside for quantifier Q_i, $2^{2^{c_o n+i}} + 2$ tape squares; every integer $\le 2^{2^{2^{c_o n+i}}}$ in absolute value can be written in this space in binary. Then decide F by cycling through each quantifier space appropriately, all the time testing the truth of G on different n-tuples of integers. We let the reader convince himself that a Turing machine implementing this outlined procedure need use only $2^{2^{c_1 n}}$ tape squares for some constant c_1. ■

Lemma 14: For some constant c_2, I^* is $(1+m)\cdot 2^{2^{2^{c_2(n+k)}}}$-bounded.

Proof: We first calculate bounds for the function $M(n,k)$. Letting $m_i = 2^{2^{2^{c_0(n+k)+i}}}$ for $1 \le i \le k$, we see that $m_i \ge H(n+k-i, i-1, \operatorname{Max}_{1\le i<j}\{|m_j|\})$ for $1 \le i \le k$. So by Lemma 4, for each $\vec{a}_k \in Z^k$ there is some $\vec{b}_k \in Z^k$ such that $\vec{a}_k \equiv_n \vec{b}_k$ and $|b_i| \le m_i$ for $1 \le i \le k$. Hence

$M(n,k) \le (2\cdot 2^{2^{2^{c_0(n+k)+k}}} + 1)^k$. So $\mu(n,k) = \prod_{i=1}^{n} M(n-i, k+i) \le 2^{2^{2^{c_3(n+k)}}}$ for some constant c_3.

So for some constant c_2, $H^*(n,k,m) = \operatorname{Max}\{H(n,k,m), m+\mu(n+1,k), 0\} \le (1+m)\cdot 2^{2^{2^{c_2(n+k)}}}$. By Theorem 1, I^* is $(1+m)\cdot 2^{2^{2^{c_2(n+k)}}}$-bounded. □

Theorem 4: The theory of I^* can be decided in space $2^{2^{2^{c_4 n}}}$ for some constant c_4.

Proof: Let F in prenex normal form be the sentence $Q_1x_1 Q_2x_2 \ldots Q_nx_n G(\vec{x}_n)$ where G is quantifier free. Using the notion of $\preceq$ relevant to Z^* we see, exactly as in Theorem 3, that F is equivalent in I^* to

$$(Q_1x_1 \preceq 2^{2^{2^{c_2 n+1}}})(Q_2x_2 \preceq 2^{2^{2^{c_2 n+2}}})\ldots(Q_nx_n \preceq 2^{2^{2^{c_2 n+n}}})\, G(\vec{x}_n).$$

Now if $f \in Z^*$ and $f \preceq 2^{2^{2^{c_2 n+i}}}$, then $f(j)=0$ for $j > 2^{2^{2^{c_2 n+i}}}$ and

$|f(j)| \le 2^{2^{2^{c_2 n+i}}}$ for all $j \in N$, so the first $2^{2^{2^{c_2 n+i}}}$ successive values of f can be represented on a tape with roughly $(2^{2^{c_2 n+i}} + 2) \cdot 2^{2^{2^{c_2 n+i}}}$ tape squares. So a procedure like the one outlined in Theorem 3 would decide the theory of I^* in space $2^{2^{2^{c_4 n}}}$ for some constant c_4. ∎

<u>Definition</u>: Let $\mathfrak{N}^*$ be the structure $\langle N^*, \le, +, 0^* \rangle$, i.e., the weak direct product of the nonnegative integers with itself.

<u>Theorem 5</u>: The theory of $\mathfrak{N}^*$ can be decided in space $2^{2^{2^{c_5 n}}}$ for some constant c_5.

<u>Proof</u>: There exists an obvious procedure which operates in linear space and takes a sentence F to a sentence F' such that F is true in $\mathfrak{N}^*$ if and only if F' is true in I^*. So Theorem 4 implies Theorem 5. ∎

Our next goal is to efficiently embed the theory of finitely generated abelian groups into the theory of I^*. Recall that a finitely generated abelian group (henceforth abbreviated FGAG) can be thought of as a finite direct product of groups, each of which is either Z or a finite cyclic group [6]. Let Z_i denote the cyclic group $\{0,1,\ldots,i-1\}$ where addition is performed mod i. The basic idea of the embedding is to think of every nonzero $f \in Z^*$ as representing a FGAG, G_f. This is made precise in the following definition.

Definition: Let $f \in Z^*$, $f \neq 0^*$. Define $\ell_f = \text{card}\{i \in N \mid f(i) \neq 0\}$. Define $m_f : \{1,2,\ldots,\ell_f\} \to N$ by $m_f(j)$=the j^{th} smallest member of $\{i \in N \mid f(i) \neq 0\}$ for $1 \leq j \leq \ell_f$. Define the FGAG $G_f = G_1 \times G_2 \times \ldots \times G_{\ell_f}$ where

$$G_j = \begin{cases} Z \text{ if } f(m_f(j)) < 0 \\ Z_{f(m_f(j))} \text{ if } f(m_f(j)) > 0 \end{cases} \qquad \text{for } 1 \leq j \leq \ell_f.$$

Clearly every FGAG is isomorphic to G_f for some $f \in Z^*$, $f \neq 0^*$.

Definition: Let $f,g \in Z^*$, $f \neq 0^*$, such that for all $i \in N$

a) $f(i)=0 \Rightarrow g(i)=0$

and b) $f(i) > 0 \Rightarrow 0 \leq g(i) < f(i)$.

Then we say that g represents a member of G_f. In particular, g represents $<g(m_f(1)),g(m_f(2)),\ldots,g(m_f(\ell_f))>$ which can be verified to be a member of G_f. Clearly every member of G_f is represented by a unique $g \in Z^*$.

We now informally define some formulas of $\mathfrak{L}_1$ to be interpreted over I^*.

1) ONE(x). ONE(f) will mean that for some $i \in N$, $f(i)=1$ and for every $j \neq i$, $f(j)=0$. Define ONE(x) as follows:

$x \geq 0 \wedge x \neq 0 \wedge \forall x'(\ (0 \leq x' \wedge x' \leq x) \to (x'=0 \vee x'=x)\ )$.

2) NPOZ(x_1,x_2). NPOZ(f_1,f_2) will mean ONE(f_1) and $f_1(i)=1 \Rightarrow f_2(i) \leq 0$. Define NPOZ$(x_1,x_2)$ as follows:

ONE$(x_1) \wedge \exists x_3(x_3 \geq 0 \wedge x_3 + x_2 \geq 0 \wedge \sim(x_1 \leq x_3 + x_2)\ )$.

3) ZERO(x_1,x_2). ZERO(f_1,f_2) will mean ONE(f_1) and $f_1(i)=1 \Rightarrow f_2(i)=0$.

Define $ZERO(x_1,x_2)$ as follows:

$NPOZ(x_1,x_2) \wedge NPOZ(x_1,-x_2)$.

4) $PICK(x_1,x_2,x_3)$. $PICK(f_1,f_2,f_3)$ will mean $ONE(f_1)$, and $f_1(i)=0 \Rightarrow f_2(i)=0$, and $f_1(i)=1 \Rightarrow f_2(i)=f_3(i)$. Define $PICK(x_1,x_2,x_3)$ as follows:

$ZERO(x_1,x_3-x_2) \wedge \forall x(\ (ONE(x) \wedge x \neq x_1) \rightarrow ZERO(x,x_2)\ )$.

5) $MEM(x_1,x_2)$. $MEM(f_1,f_2)$ will mean $f_1 \neq 0^*$ and f_2 represents a member of G_{f_1}. Define $MEM(x_1,x_2)$ as follows:

$x_1 \neq 0 \wedge \forall x \forall x_1' \forall x_2'(\ (PICK(x,x_1',x_1) \wedge PICK(x,x_2',x_2)) \rightarrow$
$((x_1'=0 \rightarrow x_2'=0) \wedge [(x_1' \geq 0 \wedge x_1' \neq 0) \rightarrow (0 \leq x_2' \leq x_1' \wedge x_2' \neq x_1')])\ )$.

6) $PLUS(x_1,x_2,x_3,x_4)$. $PLUS(f_1,f_2,f_3,f_4)$ will mean $f_1 \neq 0^*$ and f_2,f_3,f_4 represent members of G_{f_1} and the member represented by f_4 is the sum in G_{f_1} of the members represented by f_2 and f_3. Define $PLUS(x_1,x_2,x_3,x_4)$ as follows:

$MEM(x_1,x_2) \wedge MEM(x_1,x_3) \wedge MEM(x_1,x_4) \wedge \forall x \forall x_1' \forall x_2' \forall x_3' \forall x_4'\ ($
$[PICK(x,x_1',x_1) \wedge PICK(x,x_2',x_2) \wedge PICK(x,x_3',x_3) \wedge PICK(x,x_4',x_4)] \rightarrow$
$[x_2'+x_3'=x_4' \vee (x_1' \geq 0 \wedge x_2'+x_3'-x_1'=x_4')]\ )$.

<u>Theorem</u> <u>6</u>: The first order theory of FGAG can be decided in space $2^{2^{2^{cn}}}$ for some constant c.

<u>Proof</u>: Using the formulas MEM and PLUS and the fact that $f \in Z^*$ represents a FGAG if and only if $f \neq 0^*$, we obtain a procedure which operates in linear space and which takes a sentence F of the language of groups

to a sentence F' of $\mathcal{L}_1$ such that F is true of all FGAG if and only if F' is true in I^*. Applying Theorem 4, we arrive at Theorem 6. ∎

Theorem 7: The first order theory of finite abelian groups (abbreviated FAG) can be decided in space

$2^{2^{2^{cn}}}$ for some constant c.

Proof: Recall that a FAG can be thought of as a finite direct product of cyclic groups [6]. Hence, using MEM and PLUS we can do exactly the same embedding as in Theorem 6 except that now $f \in Z^*$ represents a FAG if and only if $f \neq 0^*$ and $f \geq 0^*$. ∎

Acknowledgments: I'd like to thank Albert Meyer for his numerous helpful suggestions about the content and format of this paper.

REFERENCES

1. Cobham, A. The intrinsic computational difficulty of functions, 1964 International Congress for Logic, Methedology, and Philosophy of Science, August, 1964, 24-30.

2. Cooper, C.D. Theorem-proving in arithmetic without multiplication, Computer and Logic Group Memorandum No. 16, U.C. of Swansea, April, 1972.

3. Ehrenfeucht, A. An application of games to the completeness problem for formalized theories, Fund. Math. 49, 1961, 129-141.

4. Ferrante, J. and C. Rackoff, A decision procedure for the first order theory of real addition with order, Project MAC Technical Memorandum 33, (May, 1973), 16pp., to appear SIAM Journ. for Computing.

5. Fischer, M. and M.O. Rabin, The complexity of theories of addition, to appear.

6. Maclane S. and G. Birkhoff, Algebra, Macmillan, 1968, 598pp.

7. Meyer, A.R. Weak monadic second order theory of successor is not elementary-recursive, 23pp., Boston University Logic Colloquium Proc., to appear 1974.

8. Meyer, A.R. and L. Stockmeyer, The equivalence problem for regular expressions with squaring requires exponential space, 13th Switching and Automata Theory Symp., IEEE, 1972, 125-129.

9. Mostowski, A. On direct powers of theories, Jour. Symb. Logic, 17, 1952, 1-31.

10. Oppen, D.C. Elementary bounds for Presburger arithmetic, 5th ACM Symp. on Theory of Computing, April, 1973, 34-37.

11. Péter, R. Recursive Functions, Academic Press, 1967, 300pp.

12. Presburger, M. Ueber die vollständigkeit eines gewissen systems der arithmetik ganzer zahlen in welchem die addition als einzige operation hervortritt, Comptes Rendus, I Congrès des Math. des Pays Slaves, Warsaw, 1929, 192-201, 395.

13. Ritchie, R.W. Classes of predictably computable functions, Trans. AMS, 106, 1963, 139-173.

14. Stockmeyer, L. and A.R. Meyer, Word problems requiring exponential time, 5th ACM Symp. on Theory of Computing, April, 1973, 1-9.

BIBLIOGRAPHIC DATA SHEET

1. Report No. NSF-OCA-GJ34671 - TM -42

2.

3. Recipient's Accession No.

4. Title and Subtitle

On the Complexity of the Theories of Weak Direct Products

5. Report Date : Issued January 1974

6.

7. Author(s)

Charles Rackoff

8. Performing Organization Rept. No. MAC TM-42

9. Performing Organization Name and Address

PROJECT MAC; MASSACHUSETTS INSTITUTE OF TECHNOLOGY:

545 Technology Square, Cambridge, Massachusetts 02139

10. Project/Task/Work Unit No.

11. Contract/Grant No.

GJ34671

12. Sponsoring Organization Name and Address

Associate Program Director
Office of Computing Activities
National Science Foundation
Washington, D. C. 20550

13. Type of Report & Period Covered: Interim Scientific Report

14.

15. Supplementary Notes

16. Abstracts : Let N be the set of nonnegative integers and let $\langle N^*, + \rangle$ be the weak direct product of $\langle N, + \rangle$ with itself. Mostowski [9] shows that the theory of $\langle N^*, + \rangle$ is decidable, but his decision procedure isn't elementary recursive. We present here a more efficient procedure which operates within space $2^{2^{2^{cn}}}$. As corollaries we obtain the same upper bound for the thoery of finite abelian groups, the theory of finitely generated abelian groups, and the theory of the structure $\langle N^+, \cdot \rangle$ of positive integers under multiplication. Fischer and Rabin have shown that the theory of $\langle N^*, + \rangle$ <u>requires</u> <u>time</u> $2^{2^{2^{dn}}}$ on nondeterministic Turing machines [5].

We also obtain some very general results about the nature of the theory of the weak direct product of a structure with itself.

17. Key Words and Document Analysis. 17a. Descriptors

Presburger Arithmetic

Decision Procedures

Direct Products

Weak Direct Products

Abelain Groups

17b. Identifiers/Open-Ended Terms

17c. COSATI Field/Group

18. Availability Statement

Unlimited Distribution

Write Project MAC Publications

19. Security Class (This Report) UNCLASSIFIED

20. Security Class (This Page) UNCLASSIFIED

21. No. of Pages 28

22. Price