ON EASILY INFINITE SETS AND ON A STATEMENT OF R. LIPTON

by

Daniel Leivant

TR79-390

Department of Computer Science
Cornell University
Ithaca, New York 14853

On Easily Infinite Sets and on a Statement of R. Lipton

Daniel Leivant

Department of Computer Science
Cornell University
Ithaca, N.Y.
14853

First draft, August 9, 1979

Abstract

For a complexity measure κ, a set is κ-infinite if it contains a κ-decidable infinite subset. For a time-based κ, we prove that there is a recursive S s.t. both S and its complements, $\bar{S}$, are infinite but not κ-infinite.

Lipton[6] states that the existence of a recursive set S s.t. neither S nor $\bar{S}$ is polynomially infinite is not a purely logical consequence of Π_2^0 theorems of Peano's Arithmetic PA. His proof uses a construction of an algorithm within a non-standard model of Arithmetic, in which the existence of infinite descending chains in such models is overlooked. We give a proof of a stronger statement to the effect that the existence of a recursive set S s.t. neither S nor $\bar{S}$ is linearly infinite is not a tautological consequence of all true Π_2^0 assertions.

We comment on other aspects of [6], and show (§2) that a tautological consequence of true Π_2^0 assertions may not be equivalent (in PA, say) to a Π_2^0 sentence. The three sections of this paper use techniques of Recursion Theory, Proof Theory and Model Theory, respectively.

1. κ-infinite sets, for a complexity class κ.

1.1. κ-enumerations. Let κ be a set of recursive functions with a given time-based calculation complexity; e.g., the functions calculated (a.e.) in polynomial time. A function $f \in \kappa$ is a κ-enumeration if $f(x) \neq f(y)$ for $x \neq y$. $X \subseteq \mathbb{N}$ is κ-enumerable if it is the range of a κ-enumeration. If we drop the injectiveness clause, then any r.e. set becomes linearly enumerable, devoiding the notion of interest. On the other hand, any r.e. set enumerated by a function majorizing all $f \in \kappa$ is not κ-enumerable. We show that this does not imply that a κ-enumerable set must have a simple structure. Assume given some (primrec.) coding of sequences of naturals, and let $(x)_i$ denote the i'th element of the sequence coded by x (:=0 if no such element exists).

1.2. Proposition. There is a many-one complete linearly enumerable set

Proof. Let K = (the domain of ϕ_e) be a many-one complete r.e. set. Define a recursive function f as follows. For input x perform $(x)_0$ steps in calculating $\phi_e((x)_1)$. If this yields a result only at the last step, then set $f(x) := 2(x)_1$. Otherwise $f(x) := 2x + 1$. The function f is clearly a linear-time enumeration and, for any z, $z \in K$ iff $2z \in \mathrm{range}(f)$. $\boxtimes$

1.3. κ-listing. The example of 1.2. shows that the non-monotonicity of a κ-enumeration may offset much of the restriction implied by injectiveness. Define a function $f \in \kappa$ to be a κ-listing if it is strictly increasing. A set $X \subseteq \mathbb{N}$ is κ-listable if it is the range of a κ-listing. $X \subseteq \mathbb{N}$ is κ-recursive if its characteristic function χ_X is in κ. Clearly, a κ-listable set is κ-recursive, so there are κ-enumerable sets that are not κ-listable. On the other hand, a κ-recursive set may fail to be κ-listable. Let f be a recursive function majorizing all functions in κ, and let $\ell(x)$ be the run-time of $f(x)$; define $g(x) := \langle x, f(x), \ell(x)\rangle$, $X :=$ range(g). Clearly, X is not κ-listable; but $z \in X$ can be decided by performing $(z)_2$ steps in the calculation of $f((z)_0)$, and comparing the result with $(z)_1$. So X is linearly recursive.

1.4. <u>κ-immune sets</u>. A set $X \subseteq \mathbb{N}$ is <u>κ-infinite</u> if it contains an infinite κ-recursive subset. X is <u>strongly κ-infinite</u> if it contains an infinite κ-listable subset. In the example in **1.3.**, X is κ-infinite but not strongly κ-infinite.

A set $X \subseteq \mathbb{N}$ is <u>κ-immune</u> if it is infinite but not κ-infinite. X is <u>weakly κ-immune</u> if it is infinite but not strongly κ-infinite. When the restriction to a complexity class κ is lifted, one gets the sets extensively studied under the name immune (cf. Rogers [9] p. 107). for κ = [all recursive functions] the distinction between the attributes κ-infinite and strongly κ-infinite disappears. It is easy to show that there are $2^{\aleph_0}$ sets X s.t. both X and its complement, $\bar{X}$, are immune (Rogers [9] p. 108). The existence of infinite recursive sets that are κ-immune was demonstrated by R. Constable [11].

1.5. <u>Recursive sets that are κ-immune and co-κ-immune</u>. Post [7] proved that there are r.e. sets with an immune complement (cf. Rogers [9] p. 106; such sets are called simple). We give a construction akin to Post's, in which we make sure that our set is recursive, not just r.e. or κ-enumerable.

<u>Theorem I</u>. Given a complexity class κ, there is a recursive set S s.t. both S and $\bar{S}$ are κ-immune.

<u>Proof</u>. We assume that the κ-functions may be listed effectively, $(\psi_i)_i$. This holds true for all usual measures κ. Let $X_j :=$ domain

We define simultaneously, by recursion, functions $f(n)$, $g(n)$ and finite sets K_n, J_n $(n \geq 0)$. We shall have $K_n \subseteq K_{n+1}$, $J_n \subseteq J_{n+1}$, $K_n \subseteq J_n$, and for $S :=$ range(f), $T :=$ range(g) we shall have $S \cap T = \emptyset$. Having $j \in J_n$ will guarantee that $X_j \cap S \neq \emptyset$, and $j \in K_n$--that $X_j \cap T \neq \emptyset$. The function f (as well as g) will be strictly increasing, so S will be recursive.

Order all pairs (x,y) so that (x_1,y) comes before (x_2,y) for $x_1 < x_2$, and (x,y_1) before (x,y_2) for $y_1 < y_2$. E.g., $(0,0)$; $(0,1)$, $(1,0)$, $(1,1)$; $(0,2)$, $(1,2)$, $(2,0)$, $(2,1)$, $(2,2)$; ...; $(0,r)$, $(1,r)$, ..., $(r-1,r)$, $(r,0)$, $(r,1)$, ..., (r,r); ....

Set $f(0)$, $g(0) := 0$, and J_0, $K_0 := \emptyset$. To define $f(n+1)$, $g(n+1)$, J_{n+1}, K_{n+1}, calculate successively, following the ordering above on (x,y), the values of $\psi_x(y)$ for $x \notin K_n$ and $y > f(n)$, $g(n)$. Let (x_0,y_0) be the first pair s.t. $\psi_{x_0}(y_0) > 0$. If $x_0 \notin J_n$, set $f(n+1) := y_0$, $g(n+1) := g(n)$, $J_{n+1} := J_n \cup \{x_0\}$, $K_{n+1} := K_n$. Otherwise, set $f(n+1) := f(n)$, $g(n+1) := y_0$, $J_{n+1} := J_n$, $K_{n+1} = K_n \cup \{x_0\}$. Since f is non-decreasing, $S :=$ range(f) is recursive. Also, $S \cap T = \emptyset$ is obvious.

We conclude the proof by using induction to prove that if X_n is infinite, the $f(p_n)$, $g(q_n) \in X_n$ for sufficiently large p_n, q_n. Let $I_n := \{j < n \mid X_j \text{ infinite}\}$, $F_n := \{j < n \mid X_j \text{ finite}\}$. For $j \in I_n$ there exists, by ind. hyp., some q_j s.t. $g(q_j) \in X_j$; let q be larger than all q_j, $j \in I_n$. Then $I_n \subseteq K_q \subseteq J_q$. If $n \in K_q$, then $g(q_n) = n$ for some $q_n < q$, and $f(p_n) = n$ for some $p_n < q_n$, and we are done. Assume $n \notin K_q$; then the calculation of $f(r)$, $g(r)$ for $r \geq q$ uses values of ψ_n but not of ψ_j, $j \;\; I_n$. Now let k be the number of elements in $\bigcup_{j<n} F_j$, and let $a_1 \ldots, a_{2k+2}$ be the first $2k+2$ elements of x_n larger than all $f(p_j)$, $g(q_j)$, $j \in I_n$ (so $\psi_n(a_i) > 0$ for $i = 1, \ldots, 2k+2$).

By the ordering we chose for pairs (x,y), each term $\psi_n(a_i)$ is considered in our algorithm before $\psi_r(a_i)$ for $r > n$. Hence, the only cases where neither of $f(z)$, $g(z)$ for $z \geq q$ will yield a_i are when $\psi_j(a_i)$ is considered for some $j \in F_n$, and $\psi_j(a_i) > 0$. This may happen at most twice for each $j \in F_n$, $a_i \in X_j$ (since, if $g(r) = a_i$, then $a_i \in K_{r'}$ for $r' \geq r$), so altogether at most $2k$ times. Hence, we must have $g(r) = a_i$ for some $i \in \{1, \ldots, 2k+2\}$ and $r \geq q$, and so $f(s) \in X_n$ for some $s < r$ ($f(s) = a_h$ for some $h < i$ with $s \geq q$ if $n \in J_q$, $s < q$ otherwise). $\boxtimes$

1.6. <u>Weakly κ-immune recursive sets</u>. The proof of theorem I is non-constructive in that the values of $a_n \in S \cap X_n$, $b_n \in T \cap X_n$ depend on evaluating the size of the finite X_j, $j < n$. We shall prove in §3 below that this non-constructive feature is essential.

However, the proof of theorem I may be amended to yield a constructive proof of the following weaker result.

<u>Proposition</u>. There is a recursive set S s.t. both S and $\overline{S}$ are weakly κ-immune.

Proof. Let $(\chi_i)_i$ be an effective enumeration of all κ-listings. Now replace throughout the proof of theorem I $\psi_{\ldots}$ by $\chi_{\ldots}$. We have then $F_n = \emptyset$ trivially. In the closing argument, q is obtained effectively (and uniformly) from n. If a_1, a_2 are the first elements of X_n larger than $f(p_j), g(q_j)$ fc $j < n$, then: $f(q) = a_1$, $g(q+1) = a_2$, if $n \notin J_q$; $g(q) = a_2$, $f(s) \in X_n$ for some $s < q$, if $n \in J_q - K_q$. $\boxtimes$

Related to this proposition is a theorem of Rabin [8], to the effect that, for any κ, there is a recursive set S s.t. neither S nor $\bar{S}$ is κ-recursive. Rabin's proof is also fully constructive (though the result is not recursive in κ, as shown by Hartmanis and Stearns [2]).

2. The theory of true Π_2^0 statements.

Let TA_k stand for the first-order theory in the language of PA, whose axioms are all the true Π_k^0 sentences. I.e., TA_k consists of the tautological consequences of true Π_k^0 sentences. We shall be especially interested in TA_2.

2.1. The scope of TA_2. Among the axioms of TA_2 one may find most of the open problems in Number Theory. E.g., Fermat's "Last Theorem," Goldbach's Conjecture and the (by now proven) Four-Colors Theorem are Π_1^0; the existence of infinitely many twin primes, and of infinitely many perfect numbers is Π_2^0, etc. Certain theorems and conjectures in Analysis turn out to be equivalent to Π_2^0 sentences. An example is Riemann's Hypothesis (cf. [1] p. 335). In Metamathematics, all theorems on consistency and relative consistency of formal theories may be codified as Π_1^0 sentences.

2.2. TA$_2$ in relation to PA. Infinitely many of the axioms of TA$_2$ are not theorems of PA, since the set of true Π_2^0 sentences is not r.e. On the other hand, there are infinitely many instances of induction that are not theorems of TA$_2$. Induction, here, is the schema

$$\mathrm{Ind}(\phi): \phi(0) \;\&\; \forall x(\phi(x) \to \phi(x+1)) \to \forall x\phi(x).$$

For a Σ_1^0 formula $\phi(x)$ with x as the only free variable, Ind(ϕ) is tautologically equivalent to a true Σ_3^0 sentence, and hence derived from a true Π_2^0 instance thereof. Similarly, for a Π_1^0 $\phi(x)$, Ind(ϕ) is Σ_2^0, and hence-derived from a Π_1^0 sentence. However, the consistency of TA$_2$ can be proved in TA$_2$ plus induction over Σ_1^0 formulas with parameters, so already such instances of induction exceed TA$_2$, by Gödel's Second Incompleteness Theorem.

2.3. The constructive contents of TA$_2$. All axioms of TA$_2$ are "constructively true": if $\forall x\exists y\phi(x,y)$ (ϕ quantifier-free), then $\forall x\phi(x,f(x))$ for the total recursive function $f(x) := \mu y\ \phi(x,y)$. Also, any prenex formula that is constructively true, in that sense, is a theorem of TA$_2$: assume that $\forall x_1\exists y_1 \ldots \forall x_k\exists y_k\ \phi(x_1,\ldots,x_k; y_1,\ldots,y_k)$ (ϕ quantifier-free) is constructively true, in that there exist recursive functions that yield each y_i from $x_1 \ldots x_i$ ($i = 1, \ldots, k$). This is codified by

$$\forall x_1 \ldots x_k \exists v_1 \ldots v_k \,[\, \mathop{\&}_{1\le i\le k} T(\bar{e}_i, \langle x_1,\ldots,x_i\rangle, v_i)$$
$$\& \;\phi(x_1,\ldots,x_k; U(v_1), \ldots, U(v_k))],$$

where T and U are Kleene's calculation-relation and result-extracting function, respectively (both are primitive-recursive), and $e_1, \ldots, e_k$ are codes for the algorithms in question.

In spite of the points raised above, it seems confusing and misleading to baptise TA_2 as "Constructive Arithmetic" (cf. [6]). There is a general concensus that at least the elementary part of constructive arithmetical reasoning is correctly represented by Heyting' Arithmetic HA (the intuitionistic variant of PA, in which the Law of Excluded Third, $\phi \vee \neg\phi$, is dropped from the underlying logic). It is true that prenex theorems of HA are tautological consequences of Π^0_2 theorems of HA; but there are (classically) Π^0_3 theorems of HA that are underivable in TA_2; e.g., the consistency of TA_2. On the other hand, there are (classically) Π^0_2 classical tautologies, so certainly theorems of TA_2, that are underivable in HA; e.g., $\phi \vee \neg\phi$ where ϕ is a Π^0_1 sentence canonically expressing the consistency of HA.

2.4. <u>Theorems of TA_2 that are not Π^0_2</u>. Any tautology ϕ (in the language of PA) is a theorem of TA_2; but, regardless of its complexity, ϕ is then tautologically equivalent to a quantifier-free sentence like $0 = 0 \rightarrow 0 = 0$. Are there any theorems of TA_2 that are not tautologically equivalent to a Π^0_2 sentence? We answer this positively, and actually establish the sharpest possible result.

Theorem II. There is a (tautologically) Δ_2^0 theorem ϕ of TA_2 that is not equivalent to any Π_2^0 sentence even in $PT_1 := PA + TA_1$. Moreover, ϕ is derived from an axiom of TA_2, using a propositional inference only.

Proof. Let Pr_1 be a cononical Σ_2^0 provability predicate for PT_1, and let Con_1 and Con_1Con_1 be Π_2^0 sentences expressing the consistency of PT_1 and of $PT_1 + Con_1$, respectively; so $Con_1 :\equiv \neg Pr_1(\ulcorner \overline{0} = \overline{1} \urcorner)$. Let $\phi :\equiv Con_1 \rightarrow Con_1Con_1$. Con_1Con_1 is true, so $TA_2 \vdash \phi$ (by a single instance of implication-introduction).

Assume (1) $PT_1 \vdash \phi \longleftrightarrow \psi$ for some Π_2^0 sentence ψ.

Claim A. $PT_1 \nvdash \psi$. Assume $PT_1 \vdash \psi$; then $PT_1 \vdash Con_1 \rightarrow Con_1Con_1$ by (1), i.e.: The theory $PT_1 + Con_1$ proves its own consistency, contradicting Gödel's Second Incompleteness Theorem.

Claim B. If (2) $PT_1 \vdash \neg\psi \rightarrow Con_1$, then $PT_1 \vdash \psi$. (This is due to Kreisel [5]). We use the elementary derivability conditions of Hilbert-Bernays [3] for PT_1 and Pr_1 (cf. [10] p. 827). The sentence $\neg\psi$ is Σ_2^0, so (3) $PT_1 \vdash \neg\psi \rightarrow Pr_1(\ulcorner \neg\psi \urcorner)$ (second derivability condition). Assuming (2) yields
(4) $PT_1 \vdash Pr_1(\ulcorner \neg\psi \urcorner) \rightarrow Pr_1(\ulcorner Con_1 \urcorner)$ (first and third conditions). Finally, by Rosser's refinement to Gödel's Second Incompleteness Theorem ([10] 2.2.3, p. 828), (5) $PT_1 \vdash Pr_1(\ulcorner Con_1 \urcorner) \rightarrow \neg Con_1$. Putting (3), (4) and (5) together yields (6) $PT_1 \vdash \neg\psi \rightarrow \neg Con_1$. Combined with (2), (6) implied $PT_1 \vdash \psi$. This proves claim B.

To conclude the proof, observe that (1) implies $PT_1 \vdash \neg\psi \rightarrow Con_1$, which yields $PT_1 \vdash \psi$ by claim B, contradicting claim A. $\boxtimes$

3. Underivability of theorem I in TA_2.

3.1. In [6] R. Lipton states that theorem I above is not a tautological consequence of the Π_2^0 theorems of PA. In that paper, Lipton pioneers a novel field of research, by indicating the potential application of Model Theory to independence result in Complexity Theory. Unfortunately, the proof in [6] is, at best, vague and misleading on a major issue. A non-standard model M_0 is constructed, for the Π_2^0 theorems of PA; then ([6], end of §3), an attempt is made to construct an algorithm within M_0, without paying attention (at least not explicitly) to the fact that M_0 is not well-founded. Indeed, standard informal algorithm-descriptions become inapplicable in non-standard models, where, e.g., the sequence $[\log^k x]$, $k = 1,2, \ldots,$ does not terminate whenever x is non-standard.

We feel that clarifying this point is of some interest, since most future applications of Model Theory to independence results in Computer Science would probably depend on a correct handling of algorithms in non-standard models of Arithmetic.

Our correction depends on avoiding algorithmic constructions within non-standard models. Instead, those properties of the algorithm one has in mind should be arithmetized, and proven true in a series of standard models. When evoking the Compactness Theorem to yield a non-standard model, the properties considered remain true. The object realizing them is, however, a non-standard number, which "codes an algorithm" in the sense of the model.

In 3.6.2. below we mention ways in which our theorem III improves on Lipton's statement.

3.2. Theorem III. Theorem I is not derivable in TA_2. Actually, more is true: it is not a theorem of TA_2 that there is a recursive set S s.t. both S and $\bar{S}$ are linear-time immune.

Corollary. Let $(\psi_i)_i$ be an effective enumeration of κ. There are no recursive set S and recursive functions α, β s.t. $\alpha(i)$ and $\beta(i)$ are defined whenever $X_i := \{x \mid \psi_i(x) > 0\}$ is infinite, and $\alpha(i) \in X_i \cap S$, $\beta(i) \in X_i \cap \bar{S}$.

Proof of the corollary. If there were such S, α, β, then theorem I would have a constructive form codified as a Π_2^0 sentence, as in 2.3 above, making it an axiom of TA_2, in contradiction to theorem III. $\boxtimes$

3.3. Proof of theorem III. We shall use the notations and conventions of Kleene [4] for coding sequences, algorithms and calculations. Also, it will be convenient to assume that the language of PA contains a symbol $\dagger$ for exponentiation (though this is not directly relevant, we note that PA with defining axioms for $\dagger$ is a conservative extention of PA).

By the Compactness Theorem, it suffices to show that for any recursive set S and any finite list

$$\phi_i = \forall x \exists y \psi_i(x,y) \quad (i = 1, \ldots, m)$$

of true Π_2^0 sentences, there is a model M_0 satisfying $\phi_1, \ldots, \phi_m$ and in which either S or $\bar{S}$ contains a subset that is linear-time infinite in the sense of M_0.

Define

$$f_0(x) := x\#x$$
$$f_i(x) := \mu y.\ \psi_i(x,y) \quad (i = 1, \ldots, m).$$

Since ϕ_i is true, f_i is total $(i = 1, \ldots, m)$. Let $g(x)$ be a total recursive function majorizing $f_0, \ldots, f_m$, with running-time function $\ell(x)$. Then the function $h(x) := \langle g(x), \ell(x)\rangle$ majorizes $f_0, \ldots, f_m$ and $h(x)$ is calculable in time $\leq p \cdot h(x)$ for a suitable p.

Let $\sigma(x)$, $\pi(x)$ be Σ_1^0 and Π_1^0 formulas, respectively, s.t. $x \in S$ iff $\sigma(x)$ iff $\pi(x)$; let $\eta(x,y)$, $\eta'(x,y)$ be Σ_1^0, Π_1^0 formulas, respectively, s.t. $h(x) = y$ iff $\eta(x,y)$ iff $\eta'(x,y)$.

Consider the following algorithm $\mathcal{A}$ for calculating a function $k(x,z,c)$. Let $z_0 := z$, and generate $z_{i+1} := h(z_i)$ $(i = 0,1,\ldots)$ until $z_j \geq x$, or until $p \cdot x$ steps are performed in the calculation of some $h(z_j)$, whichever comes first. If $z_j \geq x$ is reached, $z_j = x$ and $(c)_j = 1$, then set $k(x,z,c) := 1$; $:= 0$ otherwise. The length of this calculation is bounded by $\alpha := pz_1 + pz_2 + \ldots + pz_{j-1} + px + t$, where t is the time to calculate $(c)_j$. But $j < x$, and t is linear in c, i.e. $t \leq p \cdot c$ (provided p is suitably large, which we may assume w.l.o.g). So, $\alpha < 2p(z_1 - z_0) + \ldots + 2p(z_{j-1} - z_{j-2}) + px \leq 3px + pc \leq 4px_1$, where $x_1 := \max[x,c]$. Let e be the code of (a Herbrand-Gödel version of) the algorithm $\mathcal{A}$. Clearly, the calculation of $k(x,z,c)$ itself is bounded by $x_1\#s$ for a suitably large s.

Let $\mathscr{L}$ be the language of PA extended with new constants $\underline{c}$, $\underline{q}$, $\underline{a}_0$, $\underline{a}_1$, $\underline{a}_2$ .... Consider the following formulas of $\mathscr{L}$.

$$
\left.
\begin{array}{ll}
(1) & \underline{c} < \underline{a}_0 \ \& \ \underline{q} = 4\cdot\bar{p}\cdot\underline{a}_0 \\
(2)_i & \eta'(\underline{a}_i, \underline{a}_{i+1}) \\
(3)_i & \forall x < \underline{a}_i \exists v < (\underline{a}_i \# \bar{s}) [T^3(\bar{e}, x, \underline{a}_0, \underline{c}, v) \\
 & \quad .\&. \quad U(v) = 1 \rightarrow \pi(x) \\
 & \quad .\&. \quad \sigma(x) \rightarrow U(v) = 1 \\
 & \quad .\&. \quad \ell th(v) \le \underline{q}\cdot x]
\end{array}
\right\} \ i \ge 0
$$

3.4. Lemma. For any $k \ge 1$ there is a model N of $\mathscr{L}$ satisfying (1), $(2)_i$, $(3)_i$ for $i \le k$.

Proof. Let the interpretation in N of the non-logical constants of PA be the same as in the standard model. For the new constants of $\mathscr{L}$, let

$$\underline{a}_0^N := \underbrace{\langle 1, \ldots, 1\rangle}_{k \text{ times}}$$

$$\underline{a}_{i+1}^N := g(\underline{a}_i^N) \qquad (i < k)$$

$$\underline{c}^N := \langle c_0, \ldots, c_k\rangle \text{ where } c_i := 1 \text{ if } \sigma(\underline{a}_i^N), \quad := 0 \text{ otherwise.}$$

$$\underline{q}^M := 4p\underline{a}_0^N \qquad (\text{i.e., if } \pi(\underline{a}_i^N)).$$

(1) and $(2)_i$ $(i \le k)$ are satisfied in N trivially. For $(3)_i$, the existence (and uniqueness) of v, and the bound $\underline{a}_i^N \# s$ follow by the definition of the algorithm $\mathscr{A}$ coded by e. We have $U(v) = 1$ iff $k(x, \underline{a}_0^N, \underline{c}^N) = 1$, which happens exactly when there is a "h-chain" $\underline{a}_0^N \xrightarrow{h} \underline{a}_1^N \xrightarrow{h} \underline{a}_2^N \ldots \xrightarrow{h} \underline{a}_j^N = x$, and $(\underline{c}^N)_j = 1$,

$x \in S$, $\pi(x)$, $\sigma(x)$.

To prove that $\ell th(V) < \underline{q}^N \cdot x$ consider two cases. If $x \le \underline{c}^N$ then $\ell th(V) \le \alpha \le 4p \cdot \max[x, \underline{c}^N] < 4p\underline{a}_0^N$. If $x > \underline{c}^N$ then $\ell th(V) \le \alpha \le 4px \le \underline{q}^N x$. This proves the lemma. $\boxtimes$

3.5. Proof of theorem III - concluded. Let Γ be the first order theory in $\mathscr{L}$ whose axioms are

(a) the quantifier-free axioms of PA (in particular--the defining equations for $+$, $\cdot$, $\#$).

(b) h majorizes $f_0, \dots f_m$, i.e. the sentence

$$\mu :\equiv \quad \forall x,y \quad [\quad \eta(x,y) \rightarrow . \; x\#x < y \;\&\; \mathop{\&}_{1 \le i \le n} \exists z < y \; \psi_i(x,z) \;]$$

(c) $\phi_1, \dots, \phi_m$

(d) all sentences (1), $(2)_i$, $(3)_i$ $(i \ge 1)$.

Groups (a)-(C) are true sentences in the language of PA, so they are satisfied by any model N as above. Hence, every finite $\Gamma_0 \subset \Gamma$ has a model, and, by the Compactness Theorem, Γ has a model $\langle M, <^M, 0^M, S^M, +^M, \cdot^M, \#^M, \underline{c}^M, \underline{q}^M, \underline{a}_0^M, \underline{a}_1^M, \dots\rangle$.

Let $M_0 = \{x \in M \mid x <^M \underline{a}_i^M$ for some $i \ge 0\}$. By $(2)_i$, $\eta(\underline{a}_i^M, \underline{a}_{i+1}^M)$, so by μ, M_0 is closed under $f_0^M = \lambda x \cdot x \#^M x$, and hence (by (a)), under $+^M$ and $\cdot^M$. Thus, taking the restriction to M_0 of $+^M$, $\cdot^M$, $\#^M$ we get a correctly defined model of $\mathscr{L}$. Since M_0 is a submodel of M, every Π_1^0 sentence true in M is true in M_0 too. We claim that M_0 is a model of Γ. This is immediate for the Π_1^0 axioms (a), (b) and (1), $(2)_i$. By

μ, the exponential bound in $(3)_i$ is realized in M_0, and $\phi_1 \ldots \phi_m$ are also true in M_0.

Now consider the set $A := \{i \mid \pi(\underline{a}_i^M)$ is true in $M_0\}$. If A is infinite, M_0 satisfies, in addition, also the statement $\forall z \exists x > z \exists v\, [T^3(\bar{e}, x, \underline{a}_0, \underline{c}, v)\ \&\ U(v) = \bar{1}]$. Otherwise, $\bar{A}$ is infinite, and M_0 satisfies the same, with 0 in place of $\bar{1}$.

Putting everything together, M_0 is a model satisfying the sentence (in the language of PA)

$$
\begin{aligned}
(*)\quad \exists a, c, q \{\forall x \exists v [T^3(\bar{e}, x, a, c, v) \\
&.\&.\quad U(v) = 1 \rightarrow \pi(x) \\
&.\&.\quad \sigma(x) \rightarrow U(v) = 1 \\
&.\&.\quad \ell th(v) < qx] \\
\&\ [\forall z \exists x > z \exists v\ T^3(\bar{e}, x, a, c, v)\ \&\ U(v) = 1 \\
.v.\quad \forall z \exists x > z \exists v\ T^3(\bar{e}, x, a, c, v)\ \&\ U(v) = 0]\}.
\end{aligned}
$$

Decoded, this sentence says that the algorithm $\mathcal{A}$ may be supplemented with numbers a,c and become a linear-time algorithm for the characteristic function of either an infinite subset of $\{x \mid \sigma(x)\}$ or an infinite subset of $\{x \mid \neg\sigma(x)\}$. (Here we assume $\sigma(x) \leftrightarrow \pi(x)$).

This concludes the proof of the theorem. $\boxtimes$

3.6. <u>Some comments on [6]</u>.

3.6.1. In [6] Lipton states the independence of our theorem I, to which there is no reference. An erroneous assumption seems to have been made, namely; that this is a direct corollary of Rabin's theorem. Actually, Rabin's proof is fully constructive, and the statement of his theorem can consequently be strengthened to a Π_2^0 sentence. The first corollary on p. 197 in [6] seems therefore erroneous. The same remark would probably apply to the second corollary, as well as to the concluding paragraph of [6] §3.

3.6.2. Theorem III improves on the statement in [6] in two respects. Firstly, we show independence over all true Π_2^0 sentences, not just the Π_2^0 theorems of PA. Secondly, we refer to linear-time immune sets; the argument in [6], if corrected, would refer to κ-immune sets, where κ is the run-time-class for $\lambda n.an \cdot g^{-1}(n)$, g a fixed monotonous function majorizing the PA-provably recursive functions.

3.6.3. In the proof of lemma 4 in [6] it is assumed that every recursive predicate is provably-recursive in PA. This is false, as can be seen by considering the graph of a total recursive function majorizing all PA-provably recursive functions.

References

[1] M. Davis, Y. Matijasevic and J. Robinson: Hilbert's tenth problem and diophantial equations: positive aspects of a negative solution; AMS Proceeding of Symposia in Pure Mathematics 28, pp. 323-378, 1976.

[2] J. Hartmanis and R.E. Stearns: On the computational complexity of algorithms; Transactions of the American Mathematical Society 117 (1965), pp. 285-306.

[3] D. Hilbert and P. Bernays: Die Grundlagen der Mathematischen Wissenschaften II, Springer, Berlin, 1939.

[4] S.C. Kleene: Introduction to Metamathematics, Wolters-Noordhoff, Groningen, 1952.

[5] G. Kreisel: Review of Szabo(ed): The Collected Papers of Gerhard Gentzen; Journal of Philosophy, 1971.

[6] R.J. Lipton: Model theoretic aspects of computational complexity; Proceedings of the 19th FOCS, 1978, pp. 193-200.

[7] E. Post: Recursively enumerable sets of positive integers and their decision problems; Bull. of the American Mathematical Society 50 (1944) pp. 284-316.

[8] M.O. Rabin: Degree of difficulty of computing a function and a partial ordering of recursive sets; technical report, the Hebrew University, Jerusalem, 1960.

[9] H. Rogers Jr.: Theory of Recursive Functions and Effective Computability, McGraw-Hill, New York, 1967.

[10] C. Smoryński: The incompleteness theorems; in Barwise (ed.), Handbook of Mathematical Logic, North-Holland, Amsterdam, 1977.

[11] R. Constable: Two types of hierarchy theorems for axiomatic complexity classes; Courant Computer Science Symposium no. 7, Academic Press, New York, 1973, pp. 37-63.