

16

GEORGIA INSTITUTE OF TECHNOLOGY
OFFICE OF CONTRACT ADMINISTRATION
SPONSORED PROJECT INITIATION

Date: April 3, 1979

Project Title: *Model Theory for Algorithmic Logics*

Project No: *G-36-635* *Green card*

Project Director: *Dr. Richard A. DeMillo*

Sponsor: *National Science Foundation, Washington, D. C. 20550*

Agreement Period: From 3/1/79 Until 8/31/80*
*Includes 6 month flexibility period

Type Agreement: *Grant No. MCS-7807379*

Amount: *\$41,292 NSF Funds (G-36-635)*
2,046 GIT Contribution (G-36-330)
\$43,338 *Total*

Reports Required: *Annual Progress Reports; Final Project Report*

Sponsor Contact Person (s):

Technical Matters

*Dr. George I. Davida, Director - Theoretical
Computer Science Program
Division of Mathematical and
Computer Sciences
1800 G Street, N. W.
Washington, D. C. 20550

Phone: (202) 632-5744*

Contractual Matters
(thru OCA)

*Ms. Mary Frances O'Connell
Grants Specialist - Area 4
National Science Foundation
1800 G Street, N. W.
Washington, D. C. 20550

Phone: (202) 632-2858*

Defense Priority Rating: *N/A*

Assigned to: *Information & Computer Sciences* (School/Laboratory)

COPIES TO:

Project Director
Division Chief (EES)
School/Laboratory Director
Dean/Director-EES
Accounting Office
Procurement Office
Security Coordinator (OCA)
Reports Coordinator (OCA)

Library, Technical Reports Section
EES Information Office
EES Reports & Procedures
Project File (OCA)
Project Code (GTRI)
Other _____

GEORGIA INSTITUTE OF TECHNOLOGY
OFFICE OF CONTRACT ADMINISTRATION
SPONSORED PROJECT TERMINATION

Date: 6/15/81

Project Title: Model Theory ^{of} ~~for~~ Algorithmic Logics

Project No: G-36-635

Project Director: Dr. R. A. DeMillo

Sponsor: National Science Foundation

Effective Termination Date: 8/31/80

Clearance of Accounting Charges: 8/31/80

Grant/Contract Closeout Actions Remaining:

- ☐ Final Invoice and Closing Documents
- ☒ Final Fiscal Report (FTCR)
- ☒ Final Report of Inventions (IF POSITIVE)
- ☐ Govt. Property Inventory & Related Certificate
- ☐ Classified Material Certificate
- ☐ Other _____

Assigned to: Information & Computer Sciences (School/Laboratory)

COPIES TO:

Administrative Coordinator
Research Property Management
Accounting Office
Procurement Office/EES Supply Services
Research Security Services
✓ Reports Coordinator (OCA)
Suspense

Legal Services (OCA)
Library, Technical Reports
EES Research Public Relations (2)
Project File (OCA)
Other: _____

FINAL REPORT
PROJECT NO. G36-635

MODEL THEORY OF ALGORITHMIC LOGICS

By
Richard A. DeMillo

Prepared for
NATIONAL SCIENCE FOUNDATION
Washington, D.C.

Under
NSF Award Number MCS 7807379

Contract period covered
1 March 1979 through 31 August 1980

3 June 1981

GEORGIA INSTITUTE OF TECHNOLOGY
SCHOOL OF INFORMATION AND COMPUTER SCIENCE
ATLANTA, GEORGIA 30332

1981



NATIONAL SCIENCE FOUNDATION
Washington, D.C. 20550

FINAL PROJECT REPORT
NSF FORM 98A

PLEASE READ INSTRUCTIONS ON REVERSE BEFORE COMPLETING

PART I-PROJECT IDENTIFICATION INFORMATION

1. Institution and Address	2. NSF Program	3. NSF Award Number
School of Information & Computer Sci.	Theoretical Computer Sci.	MCS 7807379
Georgia Institute of Technology	4. Award Period	5. Cumulative Award Amount
Atlanta, Georgia 30332	From 3/1/79 To 8/31/80	\$41,292

6. Project Title

Model Theory of Algorithmic Logics

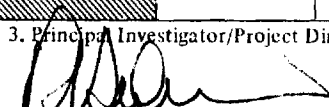
PART II-SUMMARY OF COMPLETED PROJECT (FOR PUBLIC USE)

The two papers which comprise this report were presented at the 1979 and 1980 Symposia on the Theory of Computing. They represent, in large measure, the initial stages of a more extensive investigation into applications of mathematical logic, specifically, model theory - in theoretical computer science. The goal of these investigations has been to use the powerful tools of model theory to shed light on the "P=NP" problem of complexity theory. Two directions are possible. First, it is conceivable that by a suitable paraphrase of certain lower bound problems that they fall to classical attacks. The second, and more promising direction, is that classical techniques insight into the fundamental problems of computation will be gained. The results contained in these reports are not sufficient to lend credence to either hypothesis, but the results are clearly suggestions of what might be obtained in a more thorough study of classical reformulation of the "P=NP" problem.

The contents of these papers may be roughly characterized as follows. In "Connections Between Mathematical Logic and Complexity Theory", Lipton and I show that the problem of determining lower bounds for NP-like problems is formally equivalent to a model theoretic problem: finding a particular nonstandard model of a fragment of arithmetic. Thanks to a result of Robert Solovay (whose proof appears for the first time in this paper) we know that any such model must be noneffective, providing with interesting speculation on the nature of the mathematical tools which can be used to resolve "P=NP".

The principle results of "The Consistency of 'P=NP' and Related Problems" and "Fragments of Number Theory" concern the construction of explicit nonstandard models. First, we show how to build nonstandard models in which "P=NP" is true; these are models of a large fragment of complete arithmetic. Second, we show the existence of models in which "P ≠ coNP" is true. Besides the obvious interesting implications for independence from Peano arithmetic, both constructions carry some independent

PART III-TECHNICAL INFORMATION (FOR PROGRAM MANAGEMENT USES)

1. ITEM (Check appropriate blocks)	NONE	ATTACHED	PREVIOUSLY FURNISHED	TO BE FURNISHED SEPARATELY TO	
				Check (✓)	App
a. Abstracts of Theses	X				
b. Publication Citations		X			
c. Data on Scientific Collaborators		X			
d. Information on Inventions	X				
e. Technical Description of Project and Results		X			
f. Other (specify)					
2. Principal Investigator/Project Director Name (Typed)	3. Principal Investigator/Project Director Signature			4. Date	
Richard A. DeMillo				6-	

Part II - SUMMARY OF COMPLETED PROJECT (continued)Data on Scientific Collaborators

Co-Investigators:

Richard J. Lipton, Professor of Computer Science, Princeton University

Michael Merritt, Graduate Research Assistant, Georgia Institute of Technology

Gregory L. Moore, Graduate Research Assistant, Georgia Institute of Technology

Akihiko Tanaka, Graduate Research Assistant, Georgia Institute of Technology

Two Papers on Model Theoretic Methods
in Computer Science: FINAL REPORT
For NSF Grant MCS-78-07379

Richard A. DeMillo
Richard J. Lipton

January 1981

SOME CONNECTIONS BETWEEN MATHEMATICAL LOGIC AND COMPLEXITY THEORY[†]

Richard A. DeMillo
School of Information and Computer Science
Georgia Institute of Technology
Atlanta, GA 30332

Richard J. Lipton
Computer Science Division
University of California, Berkeley
Berkeley, CA 94720

and

Department of Computer Science
Yale University
New Haven, CT 06520

[†]This work was supported in part by the US Army Research Office Grant No. DAAG29-76-C-0024 and by National Science Foundation Grants No. MCS-78-81486 and No. MCS-78-07379. Our work was also facilitated by the use of Theory Net, NSF Grant No. MCS-78-01689

I. Introduction

However difficult the fundamental problems of theoretical computer science may seem, there is very little to suggest that they are anything more than knotty combinatorial problems. So, when we look for reasons for our inability to resolve $P = NP$ and related questions, we most likely find them dealing with a lack of understanding of particular computational problems and their lower bounds. This is the sense of Hopcroft's prediction: "...within the next five years, nobody will prove that any of these problems takes more than let's say n^2 time. I think that's a reasonably safe conjecture and it also illustrates how little we know about lower bounds." [MT]. Hopcroft's guess is uncanny in its accuracy -- after six years and considerable effort by many researchers, his conjecture remains unchallenged.

The results in this paper offer a possible explanation for our failure to resolve these problems. Roughly, the main result of the sequel links lower bounds and a branch of mathematical logic known as model theory. In particular, we prove that the existence of nonpolynomial lower bounds is equivalent to the existence of nonstandard models of a sizable fragment of arithmetic. Since these are deep logical issues and there are very few techniques for handling them, and since the nonstandard models in question are non-effective, it seems plausible that this linking of complexity theory and logic explains our failure to obtain nontrivial lower bounds.

One of the aims of mathematical logic is to clarify the relation between mathematical theories and their interpretations -- or models. In logic, a theory is simply a collection of statements and all of their logical consequences, that is, a collection of (nonlogical) axioms closed under the relation " \vdash ".

Models are the structures in which theories are interpreted.

Plane geometry is such a mathematical theory. In antiquity, the relation between Euclidean geometry and its models was considered obvious, and this relationship was even further clarified by the arithmetization of geometry. It was therefore a shock to the mathematical world when, in 1868, Beltrami announced that geometry can have more than one model -- a very strange one at that since in his model the parallel postulate is false. Since the parallel postulate is certainly true in the standard model of geometry, its negation is not provable -- the parallel postulate is consistent with Euclidean geometry. On the other hand, since the negation of the parallel postulate is also true in a (nonstandard) model, its negation (i.e., the parallel postulate itself) is not provable. More recently, Cohen [Co] proved that both the axiom of choice and generalized continuum hypothesis cannot be proved from the remaining axioms of set theory -- Cohen introduced a radically new concept called forcing to construct nonstandard models with prescribed properties. The first such result for formal arithmetic was obtained by Paris and Harrington [PH]. They proved that a modest generalization of the finite Ramsey theorem of combinatorics is not decided by Peano arithmetic. Sheperdson [Sh] discusses the unprovability of induction schemes and such statements as Fermat's Last Theorem, for the case $n = 3$, from weak fragments of arithmetic.

This property of statements of a theory is called independence: a statement is independent from a theory T if the statement cannot be proved or disproved within T . Of course, Godel proved that every sufficiently powerful theory must leave infinitely many statements unresolved in this way. In current terminology, however, a qualitative distinction is usually drawn between formal undecidability and interesting independence theorems. In the

"Gödel-style formal undecidability theorems, one explicitly formulates a diagonalizing statement and using the properties of the axiom system in question, encodes that statement as a formal statement of the theory. In independence results whatever diagonalization is present in the proof, is well-hidden. One begins with a fixed (true) formal statement -- whose formalization has not been obtained with a knowledge of the axioms to be used -- and using model theoretic techniques, shows an interpretation in which the statement fails to hold (cf. [DL] for a survey of these results). Therefore, independence results seem to exhibit the following characteristics.

- (1) There is no direct diagonalization. That is, the statements whose independence is to be proved do not refer explicitly to, say, halting computations.
- (2) The independent statements are interesting in their own right. In set theory, for instance, independent statements often represent useful infinitary combinatorial principles.
- (3) The independence of a statement is sensitive to the underlying theory. In formal undecidability results one can add additional axioms to the theory, encode the independent statement for the new theory and retain its undecidability. In interesting independent theorems, however, the independence of the statement from a set of axioms characterizes the power of the axioms; changing the underlying theory by adding more axioms decides the statement in the expanded theory.

Except for the discussion of Hopcroft and Hartmanis [HH] and the results of Lipton [Li], we are aware of no other results that relate the basic issues of complexity theory to independence or nonstandard models. The impact of

our results is that proving lower bounds on certain computational problems is as hard as showing that a certain true sentence is independent from a powerful theory. In particular, we show that for certain S , $S \notin P$ (i.e., S is intractible) exactly when a particular true sentence Δ_S related to S must be false in a nonstandard model of arithmetic. Furthermore, this model must be noneffective. The various proofs of this result yield existential proof techniques for showing that problems are solvable in polynomial time. An interesting aspect of this result is that it apparently does not generalize much beyond polynomial time computation. That is, it does not relativize in any obvious way, nor is it possible to formally substitute many other time classes for P in the statement of the theorem.

II. Definitions

The definitions from complexity theory are standard [BL]. P denotes the set of problems solvable in deterministic polynomial time. NP denotes the problems solvable in nondeterministic polynomial time, and $coNP$ denotes the set of problems whose complements lie within NP . The inclusions

$$P \subseteq NP \cap coNP \subseteq NP$$

are obvious. Although it is widely believed that both inclusions are strict, the results to be quoted below are interesting even if, say, $P = NP \cap coNP$. We will return to this point later.

Our logical notation is standard (see [Ba]). Our language is any acceptable first order language with arithmetical symbols and equality. We use \forall for universal quantification and \exists for existential quantification. Among other symbols, x, y, z are used for variables, and the infix symbols

$+$ and \times and \div are used for addition and multiplication and subtraction, succ and pred for the successor and predecessor functions, and 0 for the constant zero.

Let T be a set of formulas, then $T \vdash \phi$ indicates that ϕ is a logical consequence of T . A theory is simply the set of formulas which are logical consequences of T . Since the set of theorems of the theory is uniquely characterized by T , we identify the two. A theory is consistent if $0=1$ is not among its theorems. A formula ϕ is independent of the theory if neither ϕ nor $\neg\phi$ is a theorem. If T is a theory, $T+\phi$ denotes the result of adjoining ϕ as an axiom. Thus ϕ is independent of T if both $T+\phi$ and $T+\neg\phi$ are consistent. A model of a theory T is an interpretation of the individuals, functions and relations of the underlying language such that each $\phi \in T$ is true. A set of formulas has a model if and only if it is consistent. In addition to this basic fact, we will use the

Compactness Theorem [BS]: Let T be a set of formulas. T has a model iff every finite subset of T has a model.

We will deal with a subtheory of (complete) arithmetic. Of course the standard model of this theory is the integers $N = \{0,1,2,\dots\}$ with the remaining symbols interpreted in the obvious way. Any model $*N$ (with $+$ interpreted as $*+$, etc.) which is not isomorphic to N is said to be nonstandard. Since $*N$ may be uncountable it is not surprising that nonstandard models of arithmetic can exist. Skolem [SK], however, showed that countable nonstandard models are possible. We will discuss these more fully in Section IV. For now it will be sufficient to note that if $*N$ is a countable nonstandard model of arithmetic $*N-N$ consists of nonstandard objects which are infinite relative to N ; i.e., if $a \in *N-N$, $a > n$, for each $M \in N$. Henceforth

*N (or $*N_0, *N_1$) always denotes such a model.

We will now define a particular theory PT. The language for PT includes symbols for all the functions and predicates which are countable in polynomial time. The axioms of PT are all true sentences of the form

$$(\exists x)(\forall y)A(x,y),$$

where A is quantifier-free (as usual x and y may denote several occurrences of bound variables). A formula with such a quantifier is called an EA formula. Similarly an AE formula contains the quantifier prefix $\forall\exists$. The theory PT is quite powerful. It includes the theory studied by Skolem [Sk1] -- which he felt represented an important part of constructive number theory. Hilbert, Herbrand, Kreisel and Scott [Sc] have also studied systems much weaker than PT [Sh]. Perhaps more relevant to our discussion, the PV system of Cook [Ck1, Ck2] is also weaker than PT. The axioms of PT include all the recursive equations that define the functions and predicates included in PT. Moreover, PT contains the induction axiom

$$A(0) \wedge (\forall x)[A(x) \rightarrow A(x+1)] \rightarrow (\forall y)A(y). \quad (*)$$

where A is a quantifier-free. To see this just note that (*) is equivalent to

$$(\exists x)(\forall y)[\neg A(0) \vee (A(x) \wedge \neg A(x+1)) \vee A(y)].$$

For model-theoretic purposes the axioms PT can be replaced by their universal members without changing the degree of the theory: both axiomatizations are equivalent. The theory which Skolem studied can be formed by (*) and the recursive definitions of the functions successor, addition, multiplication, subtraction and integer division. Cook's PV theory is related to PT, but notice that PT is not even recursively enumerable (inclusion of an axiom depends upon its truth), so that PT is a vastly more powerful theory. Indeed

it is not obvious how to deal with independence from PT using other than model-theoretic techniques -- since PT is not recursively enumerable, it is not clear how diagonalization can work at all!

III. Main Result

Our main result is that the intractability of any $S \in \text{NP} \cap \text{coNP}$ is equivalent to the existence of a nonstandard model for PT in which a certain sentence Δ_S , related to S , fails; i.e., $\text{PT} + \neg \Delta_S$ is a consistent theory.

Let S be fixed and let $A(x,y)$, $B(x,y)$ be defined as follows:

$$(\exists y)A(x,y) \text{ iff } x \in S,$$

and

$$(\exists y)B(x,y) \text{ iff } x \notin S.$$

Now form $\Delta_S(A,B)$:

$$\Delta_S(A,B) = (\forall x)[(\exists y)A(x,y) \vee (\exists z)B(x,z)]$$

Notice that, when interpreted in N , $N \models \Delta_S(A,B)$ since in N

$$\Delta_S(A,B) \leftrightarrow (\forall x)(x \in S \vee x \notin S).$$

Theorem. Let $S \in \text{NP} \cap \text{coNP}$. Then the following statements are equivalent:

- (1) $S \in P$.
- (2) $\text{PT} \vdash \Delta_S(A,B)$, for some A,B in the language of PT.

Proof of (1) \Rightarrow (2): If $S \in P$, there are polynomial time predicates A,B so that $x \in S$ iff $A(x)$ and $x \notin S$ iff $B(x)$.

Hence

$$(\forall x)[(\exists y)A(x) \vee (\exists z)B(x)]$$

is an axiom of PT.

□

Proof of (2) \Rightarrow (1):

We will present three proofs of the converse. What is needed in all three cases is to pass from $PT \vdash \Delta_S(A,B)$ to a true formula

$$(\forall x) \left(\bigvee_{i=1}^n A(x, f_i(x)) \vee \bigvee_{i=1}^m B(x, g_i(x)) \right)$$

where the terms f_i, g_i are in the language of PT. Hence $x \in S$ is decided by checking

$$\bigvee_{i=1}^n A(x, f_i(x)) \quad (3)$$

and

$$\bigvee_{i=1}^m B(x, g_i(x)) \quad (4)$$

If (3) is true $x \in S$ and if (4) is true $x \notin S$, and since all terms and predicates are polynomial time computable, $S \in P$.

Proof A:

Let $(\forall x)(\exists y)\Gamma(x,y)$ denote $\Delta_S(A,B)$, so that $PT \vdash (\forall x)(\exists y)\Gamma(x,y)$,

and suppose that

$$PT \not\vdash (\forall x) \left(\bigvee_{i=1}^n \Gamma(x, f_i(x)) \right), \quad n=1,2,\dots$$

where f_1, f_2, \dots are terms of PT. Define the theory T^* by

$$T^* = PT + \neg\Gamma(c, f_1(c)) + \dots + \neg\Gamma(c, f_n(c)) + \dots$$

where c is a new constant, not appearing in PT. We first claim that T^* is consistent, for if not

$$PT + \neg\Gamma(c, f_1(c)) + \dots + \neg\Gamma(c, f_m(c)) \vdash 0=1$$

by compactness and hence

$$PT \vdash \bigvee_{i=1}^n \Gamma(c, f_i(c))$$

which implies

$$PT \vdash (\forall x) \bigvee_{i=1}^m \Gamma(x, f_i(x)),$$

establishing the claim. Choose any model M for T^* and let M_c be the submodel generated by c . Since PT is open, $M_c \models PT$ and thus $M_c \models (\exists y)\Gamma(c, y)$. But by our choice of c , $M_c \models (\forall y)\neg\Gamma(c, y)$. $S \in P$ now follows as described above. \square

Proof B:

We need to recall the following fact, often called the Kleene-Herbrand-Gentzen Theorem [K1].

Lemma If T is a consistent collection of EA formulas and $T \vdash (\forall x)(\exists y)\phi(x, y)$ where ϕ is open, then for some terms over the terms of T , their compositions and definition by cases, say f_1, \dots, f_m ,

$$\bigvee_{i=1}^m \phi(x, f_i(x))$$

is true.

Roughly speaking, this allows us to make the existential quantifiers explicit in a quite constructive fashion. Without the restriction on T the lemma is easily seen to be false. Since PT satisfies the hypothesis for T and $\Delta_S(A, B)$ is AE , $S \in P$ follows by (3), (4) as described above.

□

Proof C:

The application of the Kleene-Herbrand-Gentzen Theorem can be replaced by an application of the "pure" Herbrand Theorem [St1] as in Proof B to conclude $PT \vdash "S \in P"$.

□

Notice that Proof A is nonconstructive and involves compactness arguments. The provability of $\Delta_S(A, B)$ in this setting constitutes a "pure" existence proof for polynomial time algorithms. The provability of $\Delta_S(A, B)$ in the setting of Proofs B and C constitutes a constructive existence proof for polynomial time algorithms. (The apparent simplicity of Proof B compared to Proof A lies in the great power of Herbrand's Theorem, which has played a basic role in various consistency proofs in logic. The proof of Herbrand's Theorem is based on a very careful analysis of how T can prove $(\forall x)(\exists y)\phi(x, y)$). However, the running times of polynomial time algorithms produced in this way may be very bad indeed. In fact, the best known bound is of order

$$n^{2^{2^{\dots^2}}} \quad (5)$$

where the depth of nesting of the stack of 2's is bounded by the number of inferences in the shortest proof of $\Delta_S(A,B)$ in PT. These upper bounds are the best known to logicians, although the lower bound literature is very sparse (Statman has obtained this polynomial as a lower bound [St] although for a theory much less relevant to complexity theorists). It has been often noticed that, although there are problems with very large polynomial running times, the only naturally occurring problems in P have "small" polynomial complexity. This gap has helped to sustain a certain feeling that membership in P is sufficient for computational tractability. If indeed the polynomial bounds (5) cannot be locally reduced, this is compelling evidence that P is much too extensive

This theorem above does not apply to arbitrary complexity classes. It is apparently rather highly specialized for polynomial-like complexity classes. At concrete levels, the theorem can be made to work for the following complexity classes:

$$2^{\text{poly-log}}$$

$$\text{linear}$$

$$n^{1+\epsilon}$$

$$\bigcup_k n \log^{(k)} n$$

How about those problems for which lower bound proofs have already been supplied?[†] The theorem does not hold for any elementary lower bound (functions which consist of bounded nestings of exponentials do not have the

[†]This issue was raised by R. E. Tarjan.

closure properties required by Herbrand's Theorem). On the other hand, the Δ_1 sentence for those sets which have provable nonelementary lower bounds [MS] are false in the standard model of T , and so the issue of independence does not even arise for those problems. In short, the theorem cannot apply to a class of lower bounds F if the functions in F are not closed under composition and definition by cases, or if determinism and nondeterminism are not distinguished at complexity F .

By identical arguments we can show that PT is also related to " $P = NP$." Let us say that a theory T can verify that NP is closed under complements if for $S \in NP$

$$T \vdash "S \in coNP."$$

Corollary. PT can verify that NP is closed under complements iff $P = NP$.

By "checking" the theorem against the well-known problems which lie in $NP \cap coNP$ (e.g., Primes, Linear Programming, Breaking Public Key Cryptosystem [Ri]), a great deal of information can be obtained about the nonstandard models whose existence is so intimately connected to lower bounds. We have the corollaries:

Corollary. If Primes is not in P , then there is a nonstandard model of PT in which primes need not have primitive roots [Pr].

Corollary. If Linear Programming is not in P , then there is a nonstandard model of PT in which for some point y and some point-set X whose convex hull does not contain y , there is no separating hyperplane through y [Do].

Since both of these corollaries negate properties which hold in the standard integers, it is difficult to imagine the models in which they fail.

Moreover, the classical techniques for constructing nonstandard models do not work at the simple level of $\Delta_1^1(A, B)$. For example, forcing is a technique that can be applied to formulas very high in the analytical hierarchy [Bu]. It is generally acknowledged by logicians that there are few techniques for constructing such nonstandard models, yet the theorem cited above asserts that a byproduct of any lower bound proof is an existence proof for such nonstandard models.

Finally, we note that although we are unable to extend these results to Peano Arithmetic, we can extend the theory PT slightly to include theories with the property that all terms which grow slowly are easy to compute. Thus we have corresponding independence results for theories of $+$, \times and polynomially honest functions. For instance, suitable theories are theories of

$$+, \times, x! \quad \text{and} \quad +, \times, x^{y+1}$$

IV. Nonstandard Models

In this section we will describe a result, due to R. Solovay, showing that from the standpoint of constructing nonstandard models the theory PT is almost as strong as Peano Arithmetic (PA, for short). We begin with a digression on the nature of nonstandard models of PA and fragments of arithmetic.

The classical observation of Skolem was that a countable nonstandard model of PA could be obtained simply by applying compactness to the set of formulas

$$PA + (a > 0) + (a > 1) + (a > 2) + \dots$$

It is consistent to assume, then, that there exists a "nonstandard object" a which is greater than all standard integers. Such a model *N contains N as an initial segment and has an ordering ${}^*\leq$ extending \leq to ${}^*N - N$. The global

structure of ${}^*\mathbb{N}$ is remarkable. Define for $x, y \in {}^*\mathbb{N}$ $x \equiv y$ to mean that x and y differ by a standard integer, i.e., for some $n \in \mathbb{N}$:

$$x^*-y = n \quad \text{or} \quad y^*-x = n.$$

${}^*\mathbb{N}/\equiv$ is a set of equivalence classes called blocks (each is order isomorphic to \mathbb{N}). \mathbb{N} is a block. Also ${}^*\leq$ totally orders blocks like the rationals (i.e., blocks are densely ordered). Nonstandard integers cannot be described by formulas of PA and any formula true of infinitely many integers must also hold at some $b \in {}^*\mathbb{N}-\mathbb{N}$.

Nonstandard models for fragments of arithmetic also contain infinite, nonstandard objects but may have vastly simpler structure. Consider the (infinite) axiom system: for all $n, m \in \mathbb{N}$,

$$\text{suc}^m(0)+0 = \text{suc}^m(0),$$

$$\text{suc}^m(0)+\text{suc}(\text{suc}^m(0)) = \text{suc}(\text{suc}^{m+n}(0)),$$

$$\text{suc}^n(0) \times 0 = 0,$$

$$\text{suc}^n(0) \times \text{suc}(\text{suc}^m(0)) = \text{suc}^n(0) \times \text{suc}^m(0) + \text{suc}^n(0),$$

$$\text{suc}^n(0) \neq \text{suc}^m(0), \text{ for } m \neq n,$$

$$(\forall x)(x \leq \text{suc}^m(0) \leftrightarrow \bigvee_{0 \leq i \leq m} x = \text{suc}^i(0)),$$

$$(\forall x)(x \leq \text{suc}^m(0) \vee \text{suc}^m(0) \leq x).$$

A nonstandard model for this theory is

$${}^*\mathbb{N} = \mathbb{N} \cup \{\omega\}, \omega \notin \mathbb{N} \text{ with } {}^*\text{suc}(\omega) = 0,$$

$${}^*\text{suc}(m) = \text{suc}(m) \text{ for all } m \in \mathbb{N} \text{ and } {}^*+, {}^*\times \text{ defined by the following tables}$$

difficult as independence proofs. This in itself leads to interesting speculations, but we feel the real force of these results lies in the link they create between the relatively new (and rather concrete) problems of computer science and some classical questions at the foundations of mathematics. We will mention just a few possibilities which ensue from such a link.

- (1) It is possible that the methods of mathematical logic may help us resolve such questions as whether or not $P = NP$.
- (2) Since lower bound proofs are equivalent to independence proofs, it is possible that the lower bound statements themselves are independent from PA or similar theorems. We make the following conjecture: " $P = NP$ " is independent of PT.
- (3) Following the measuring of (2), a viable approach to lower bounds might be to look for consistency with theories such as PA and PT.
- (4) It is possible that a nontrivial lower bound will be proved, providing an entirely new method of building nonstandard models for arithmetic.
- (5) It is possible that $T \vdash \Delta_S(A,B)$ implying the existence of a polynomial but quite useless algorithm for S.
- (6) The main result of Section III together with Solovay's result comes very close to explaining the difficulty in obtaining lower bounds: any such proof must implicitly construct a noneffective system. This makes it seem far less likely that the finite combinatorial methods of the sort which have been applied in extant lower bound proofs will be able to prove nontrivial lower bounds are NP-complete problems.

ACKNOWLEDGEMENTS

We would like to thank Manuel Blum, David Dobkin, Stephen Kleene, Larry Landweber, Nancy Lynch, and Rick Statman for helpful conversations. A special thanks is due to Robert Solovay for sharing with us the main result of Section IV.

REFERENCES

- [Ba] J. Barwise, Handbook of Mathematical Logic, North Holland, 1978.
- [BL] W. Brainerd and L. Landweber, The Theory of Computation, Wiley, 1974.
- [BS] J. Bell and J. Slomson, Models and Ultraproducts, North-Holland, 1970.
- [Bu] J. P. Burgess, "Forcing", in [Ba], pp. 403-542.
- [Co] P. J. Cohen, Set Theory and the Continuum Hypothesis, Benjamin, 1966.
- [Ck1] S. Cook, "Feasibly Constructive Proofs and the Propositional Calculus", Proceedings Seventh ACM Symposium on the Theory of Computing, 1975.
- [Ck2] S. Cook and R. Rehow, "On the Lengths of Proofs in the Propositional Calculus", Proceedings Sixth ACM Symposium on the Theory of Computing, 1974, pp. 135-148.
- [DL] R. DeMillo and R. Lipton, "Independence", SIGACT News (to appear).
- [Do] D. Dobkin and S. Reiss, "The Complexity of Linear Programming", Yale University Technical Report, No. 69, June 1978.
- [EK] A. Ehrenfeucht and G. Kreisel, "Strong Models of Arithmetic", Mathematics and Logic, 1966.
- [HH] J. Hartmanis and J. Hopcroft, "Independence Results in Computer Science", SIGACT News, Vol. 8, No. 4, 1976, pp. 13-23.
- [K1] S. Kleene, Introduction to Metamathematics, VanNostrand, 1953.
- [Li] R. Lipton, "Model Theoretic Aspects of Computational Complexity", Proceedings 19th FOCS, 1978, pp. 193-200.
- [MS] A. Meyer and L. Stockmeyer, "Nonelementary Word Problems in Automata Theory and Logic", Proceedings AMS Symposium on Complexity of Computation, 1973.
- [MT] R. Miller and J. Thatcher, Complexity of Computer Computations, Plenum, 1972.

- [PH] J. Paris and L. Harrington, "A Mathematical Incompleteness in Peano Arithmetic", in [Ba], pp. 1133-1142.
- [Pr] V. Pratt, "Every Prime Has a Succinct Certificate", SIAM J. Computing, 1975.
- [Ri] R. Rivest, private communication.
- [Sc] D. S. Scott, "On Constructing Models for Arithmetic", Infinitistic Methods, Warsaw, 1959 (Oxford, 1961), pp. 235-255.
- [Sh] J. Shepherdson, "Nonstandard Models of Fragments of Arithmetic", Model Theory, (J. Addison, ed.), North-Holland, 1963, pp. 342-358.
- [Sk] Th. Skolem, "Über die Nicht-charakterisierbarkeit der Zahlenreihe Mittels endlich oder abzählbar unendlich vieler Aussagen mit Ausschliesslich Zahlenvariablen", Fund. Math. 23, pp. 150-161, 1934.
- [Sk1] Th. Skolem, "Peano's Axioms and Models of Arithmetic", Mathematical Interpretations of Formal Systems, Amsterdam, 1955, pp. 1-14.
- [St] R. Statman, private communication.
- [St1] R. Statman, "Herbrand's Theorem and Gentzen's Notion of Direct Proof", in [Ba], pp. 897-912.

THE CONSISTENCY OF "P = NP" AND RELATED PROBLEMS WITH FRAGMENTS OF NUMBER THEORY*

Richard A. DeMillo
School of Information and Computer Science
Georgia Institute of Technology
Atlanta, Georgia 30332

Richard J. Lipton
Dept. Electrical Engineering & Computer Science
University of California, Berkeley
Berkeley, California 94720

1. Introduction

The main results of this paper demonstrate the consistency of "P = NP" and a variant of "NP ≠ coNP" with certain natural fragments of number theory to be defined precisely in the sequel.[†] Consistency results represent an approach to the lower bound problems of complexity theory which points to a number of interesting lines of inquiry. Our ultimate goal is to make precise the difficulty of proving certain nontrivial lower bounds. Among the possibilities which follow from this approach are:

- (1) that logical techniques may help us resolve the P = NP question,
- (2) that showing why certain arguments must fail may lead to mathematical tools capable of resolving the problems, and
- (3) that the special character of model theoretic methods in complexity theory may lead to new results which are of purely logical interest.

We will address these possibilities below.

Roughly speaking, a statement ϕ is consistent with a mathematical theory T (usually written " $T + \phi$ is consistent") if the addition of ϕ as an

*This work was supported in part by the US Army Research Office, Grant No. DAAG29-76-C-0024 and by the National Science Foundation Grants MCS-78-81486 and MCS-78-07379. Our work was facilitated by the use of Theory Net, NSF Grant MCS-78-01689.

[†]We have tried to keep the logical background self contained -- when we fail in this, a good reference is the encyclopedic [2].

axiom of T does not lead to a contradiction. We will write $\Sigma \vdash \psi$ to mean that the statement ψ is a logical consequence of the collection Σ of statements -- of course, we always assume a formalization in an appropriate system of first order logic. $T + \phi$ is consistent if

$$T + \phi \not\vdash 0 = 1;$$

alternatively, $T + \phi$ is said to be consistent if it is possible to find an interpretation of $T + \phi$ in which the statements in $T \cup \{\phi\}$ are simultaneously true, i.e., a model of $T + \phi$. If $T + \phi$ is consistent, there are two additional possibilities:

- (1) $T \vdash \phi$: that is, not only is there a model of $T + \phi$, but every model of T is also a model of ϕ , so T can totally resolve ϕ .
- (2) $T + \neg \phi$ is consistent: that is, neither $T \vdash \phi$ nor $T \vdash \neg \phi$, so no argument involving only T can resolve ϕ -- in this case ϕ is said to be independent of T.

Consistency and independence have come to be topical issues in computer science, combinatorics and related fields. The impetus perhaps derives from the discovery by Paris [3] that certain natural combinatorial principles cannot be proved or disproved in Peano Arithmetic. Hartmanis and Hopcroft [4] suggested that relativized P = NP questions may be formally undecidable. This theme was more fully developed in [5]. Lipton [6] was the first to use model theoretic techniques to prove the consistency of a complexity - theoretic statement with an interesting fragment of arithmetic. A formal connection between independence and lower bound problems was announced in [1].

We will proceed as follows. Two theories, ET and PT, will be defined. Intuitively, these theories correspond to constructive components of the first order theories of exponential time and polynomial time, respectively. It was shown in [1] that in a certain sense PT is the characterizing theory of P = NP type problems by showing that P = NP exactly when a certain true sentence Δ_S , where S is NP-complete, is provable in PT. So, in particular, proving nonpolynomial lower bounds is equivalent to constructing certain nonstandard models of PT. (Nonstandard models of PT are discussed in Section 3.) There are two ways to interpret such a result. If $T \vdash \phi$ is equivalent

to, say, $P = NP$, then a way of showing that $P \neq NP$ is to prove that $T + \neg \phi$ is consistent. On the other hand, if $P = NP$, then $T + "P \neq NP"$ could still be consistent. A new understanding of polynomial time computation may result by looking at nonstandard interpretations of the notion of efficiency, that is, by showing that $T + "P = NP"$ is consistent. In either case, the crucial step is a consistency proof. In Sections 4 and 5 we prove that $ET + "P = NP"$ is a consistent theory, pointing either toward an independence result or the unlikely alternative: $P = NP$. The corresponding result for $NP \neq coNP$ and PT is proved in Sections 6 and 7. This result carries some interest due to the recent announcement of a polynomial time algorithm for linear programming [7], which has cast doubt on some widely held opinions concerning the complexity of problems in $NP \neq coNP$. The proof employed in Section 7 introduces a quantifier elimination technique that may prove useful for constructing other models. The final section compares the independence techniques most widely used for independence proofs in number theory with the techniques most likely to yield progress in complexity theory, concluding that technical breakthroughs may be required.

2. Preliminaries

Our logical notation is standard (see, e.g., [2]). Our underlying language is any acceptable first order language with arithmetic symbols and equality. We use the symbols $x+y$, $x-y$, xy , c^x ($c > 2$ a constant), $\min(x,y)$, $\max(x,y)$, all with the usual intended interpretation. We use x, y, z for variables and a, b, c , and sometimes α , for constants.

A theory T is simply a set of formulas closed under \vdash . We usually identify T with a set of axioms T_A :

$$T = \{\phi \mid T_A \vdash \phi\}$$

If $T_A \vdash \phi$, then ϕ is a theorem of T . T is said to be consistent if $0 = 1$ is not among the theorems of T . There is a unique inconsistent theory: it contains all formulas. $T + \phi$ denotes the theory resulting from $T_A \cup \{\phi\}$. A formula ϕ is independent of T if $T + \phi$ and $T + \neg \phi$ are consistent.

A model of a theory T is an interpretation (in ordinary mathematics) of the individuals, functions, and relations** such that each $\phi \in T$ is true. More precisely, let (M, F, R) be a system of individuals, M , functions on M , F , and relations on M , R . We denote such a system simply by M when no confusion results. Let $\phi(\vec{x})$ be an atomic

* $x-y$ is defined to be $x-y$ if $x > y$, and 0 otherwise.

** When necessary we denote the interpretation of a symbol in an interpretation M by appending M as a superscript.

formula with free variables \vec{x} , and let \vec{a} be a vector of elements of M , $|\vec{x}| = |\vec{a}|$. Then ϕ is satisfied by \vec{a} in M , written

$$M \models \phi[\vec{a}],$$

if ϕ^M is true in M when x_1 is interpreted as a_1 , x_2 as a_2 , etc. For remaining ϕ , $M \models \phi[\vec{a}]$ is defined by induction:

(i) if $\phi = \phi_0 \vee \phi_1$ then $M \models \phi[\vec{a}]$ iff

$$M \models \phi_0[\vec{a}] \vee M \models \phi_1[\vec{a}];$$

(ii) if $\phi = \neg \phi_0$, then $M \models \phi[\vec{a}]$ iff

$$M \not\models \phi_0[\vec{a}];$$

and

(iii) if $\phi = (\forall x_i) \phi_0$, then $M \models \phi[\vec{a}]$ iff

for all $m \in M$

$$M \models \phi_0[a_1, \dots, a_{i-1}, m, a_{i+1}, \dots].$$

If $M \models \phi[\vec{a}]$ for all \vec{a} , then ϕ is true in M and $M \models \phi$. (M is said to be a model of ϕ). Obviously if ϕ is a sentence, then $M \models \phi$ if $M \models \phi[\vec{a}]$ for any \vec{a} . A set of formulas Σ has a model M if for every $\phi \in \Sigma$, ϕ is true in M . There are three essentially equivalent formulations of the relationship between \models and \vdash . Let Σ be a collection of formulas:

Deduction Theorem. Σ is consistent iff each finite subset of Σ has a model.

Completeness Theorem. Σ is consistent iff Σ has a model.

Compactness Theorem. Σ has a model iff each finite subset of Σ has a model.

Basic to our development is a number theory; that is, a theory of the system $N = \{0, 1, 2, \dots\}$. The most celebrated theory of the natural numbers is Peano Arithmetic (PA), i.e., the usual recursive definition of N , $+$, \times together with mathematical induction. A related but immensely more powerful number theory is complete arithmetic (CA):

$$CA = \{\phi \mid N \models \phi\}.$$

Important subtheories of PA can be obtained by constraining the prefix of a prenex formula. A quantifier Q is said to be bounded if it is equivalent to writing $Q(x < t) \phi(x)$, where t is a term not containing x ; a bounded formula contains only bounded quantifiers. If ϕ is a bounded formula, then $\exists x \phi$ and $\forall x \phi$ are respectively Σ_1 and Π_1 formulas. The following table defines Σ_2, Π_2, \dots .

	Σ_n	Π_n
\exists	Σ_n	Σ_{n+1}
\forall	Π_{n+1}	Π_n

We usually reserve the notation Π_n, Σ_n for the
 $\{\phi \in \Sigma_n \mid PA \vdash \phi\}$ and $\{\phi \in \Pi_n \mid PA \vdash \phi\}$.

We will deal with other subtheories of CA. The first such theory is PT, the open theory of polynomial time [1]. The language of PT includes symbols for all the functions and predicates computable in polynomial time. The axioms of PT are all true sentences of the form

$$(\exists \vec{x})(\forall \vec{y}) A(\vec{x}, \vec{y}), *$$

when A is quantifier-free and \vec{x}, \vec{y} may denote several occurrences of the bound variables.

A theory similar to PT but weaker in a certain sense is the open theory of exponential time, ET. The language of ET is comprised of the predicates of PT and the functions $x+y, x \cdot y, x \cdot y, c^x (c \geq 2)$, $\min(x, y)$, and $\max(x, y)$. The axioms of ET are all true sentences

$$\forall \vec{x} A(\vec{x}),$$

where A is quantifier-free. For instance, if Fermat's last theorem is true, then ET contains the axioms

$$\vdash x^n + y^n = z^n \rightarrow x \times y \times z = 0, n = 3, 4, 5, \dots$$

$N = \{0, 1, 2, \dots\}$ is called the standard model of CA (and also PA). Any model $*N$ of CA (with + interpreted as *, etc.) which is not isomorphic to N is said to be nonstandard. By the Löwenheim-Skolem Theorem there are infinitely many nonstandard models of CA, but countable nonstandard models are also possible. We will discuss nonstandard models more fully in Section 3.

3. PT and Nonstandard Models

The main result of [1] establishes a relationship between lower bound problems in complexity theory and independence problems in the foundations of mathematics. In particular, the existence of non-polynomial lower bounds for certain combinatorial problems is equivalent to the existence of certain nonstandard models of PT: for any $S \in NP \cap coNP$ there is a fixed true sentence Δ_S , related to S, so that S is intractable exactly

* A formula with such a quantifier prefix is called an EA formula. Similarly, an AE formula contains the quantifier prefix $\forall \exists$. Note that the axioms of PT can be replaced by their universal members without changing the theory.

when there exists a nonstandard model of PT in which Δ_S fails -- i.e., when $PT + \neg \Delta_S$ is a consistent theory.

More precisely, let S be fixed and let $A(x, y), B(x, y)$ be defined as follows:

$$(1) (\exists y)A(x, y) \text{ iff } x \in S,$$

and

$$(2) (\exists y)B(x, y) \text{ iff } x \notin S.$$

Now, form $\Delta_S(A, B)$:

$$\Delta_S(A, B) = (\forall x)((\exists y)A(x, y) \vee (\exists z)B(x, z)).$$

Notice that

$$N \models \Delta_S(A, B),$$

since in N

$$\models \Delta_S(A, B) \leftrightarrow (\forall x)(x \in S \vee x \notin S)$$

Theorem 3.1 [1]. Let $S \in NP \cap coNP$. Then the following statements are equivalent.

$$(1) S \in P.$$

$$(2) PT \vdash \Delta_S(A, B), \text{ for some } A, B \text{ in the language of PT.}$$

By a similar result it can be shown that PT is also related to "P = NP." Let us say that a theory T can verify that NP is closed under complement if for $S \in NP$

$$T \vdash "S \in coNP."$$

Theorem 3.2. PT can verify that NP is closed under complements iff $P = NP$.

Skolem [1B] is credited with the classical observation that nonstandard models of arithmetic exist. Of course, in one sense one obtains nonstandard models quite easily. Just apply the Löwenheim-Skolem Theorem to PA to get uncountable models which cannot be isomorphic to N. Skolem's method is to get a countable nonstandard model of PA by simply applying the Compactness Theorem to the set of formulas

$$PA + \{\alpha > 0\} + \{\alpha > 1\} + \dots$$

So it is consistent to assume that there exist "nonstandard objects", each greater than all of the standard integers. Every such model $*N$ contains N as an initial segment and has an ordering $*\leq$ extending $<$ to $*N$. The global structure of $*N$ is quite remarkable. Define, for $x, y \in *N$, $x \equiv y$ to mean that x and y differ by a standard integer:

$$|x - y| \leq n, \text{ for some } n \in N.$$

$*N/\equiv$ is a set of equivalence classes called blocks. N is a block. Each block $\neq N$ is order isomorphic to the (positive and negative) integers. By

extension, $\ast <$ also total orders blocks. Furthermore, the blocks are densely ordered. In summary, the order type of $\ast N$ is

$$\omega + \eta (\ast \omega + \omega),$$

(see, e.g., [19]).

An important logical property of $\ast N$ is that the standard objects cannot be characterized.

Lemma 3.3 (Robinson's Overspill Lemma). Let $\ast N$ be any nonstandard model of PA. Then for all formulas $\phi(x)$:

- (i) $N \neq \{a \mid \ast N \models \phi(x)[a]\}$, and
- (ii) if $\ast N \models \phi(x)[n]$ for infinitely many $n \in N$, then for some $a \in \ast N - N$, $\ast N \models \phi(x)[a]$.

Proof. Part (ii) follows easily from (i). To see why (i) holds, suppose that such a ϕ exists. Then $\phi(0)$, and for all $n \in N$, $\phi(n)$ but for $y \notin N$, $\neg \phi(y)$; hence $\ast N \models \phi(0) \wedge (\forall x)(\phi(x) \rightarrow \phi(x+1))$. But then $\ast N \models (\forall x)\phi(x)$, a contradiction. \square

This result is much stronger than it appears at first glance. There is a precise sense in which no formal system can define N . (cf. [20]).

A useful construction in model theory for building nonstandard models of arithmetic is the ultraproduct construction. We sketch here the Boolean-valued treatment suggested by Scott (See [20] for detailed development). Let I be an arbitrary index set and let

$$M = \prod_{i \in I} M_i$$

denote the infinite product of the structures M_i , $i \in I$. If the sets M_i , I , are infinite, then the elements of M , its relations and functions are infinite vectors. The central notion of the ultraproduct construction involves reducing the product M by identifying those $\vec{x}, \vec{y} \in M$ which differ only on a set of measure zero. First assign a Boolean-value[†] $\llbracket \phi \rrbracket$ to each formula ϕ of the language of M as follows.

- (i) $\llbracket A(a,b) \rrbracket = \{i \in I \mid A^i(a^i, b^i)\}$
- (ii) $\llbracket a=b \rrbracket = \{i \in I \mid a^i = b^i\}$
- (iii) $\llbracket \neg \phi \rrbracket = I - \llbracket \phi \rrbracket$

[†]Boolean values are always in the complete Boolean algebra $2^I = \{S \mid S \subseteq I\}$. See [2] for relevant definitions. For notational convenience, we assume that our underlying language contains a constant symbol for each element of M . Free variables are handled similarly.

$$(iv) \llbracket \phi_0 \vee \phi_1 \rrbracket = \llbracket \phi_0 \rrbracket \cup \llbracket \phi_1 \rrbracket$$

$$(v) \llbracket (\exists x)\phi(x) \rrbracket = \bigcup_a \llbracket \phi(a) \rrbracket.$$

It is an easy consequence of (i)-(v) that for any $a_0^M, \dots, a_n^M \in M$

$$\llbracket \phi(a_0, \dots, a_n) \rrbracket = \{i \mid M_i \models \phi[a_0^M(i), \dots, a_n^M(i)]\}$$

Since each formula is thus assigned a Boolean value in 2^I , we now need only consistently assign "true" to those Boolean values that represent truth i.e., by a homomorphism $H: 2^I \rightarrow \{0,1\}$ which defines the ultrafilter $F = \{S \mid H(S) = 1\}$. We then form the quotient structure M/\sim_F , where \sim_F is the equivalence defined by

$$x^m \sim_F y^m \text{ iff } \llbracket x=y \rrbracket \in F.$$

(\sim_F must also be extended to functions and relations). For simplicity the reduced structure is denoted by M/F . This is the ultraproduct of $\{M_i\}_{i \in I}$ modulo F . The following result is basic.

Los' Theorem. Let ϕ be a formula with free variables x_0, \dots, x_n , and let

$$a_i = x_i^{M/F}, \quad i = 0, \dots, n.$$

Then

$$M/F \models \phi[a_0, \dots, a_n] \text{ iff } \llbracket \phi(x_0, \dots, x_n) \rrbracket \in F.$$

To obtain a nonstandard model of PA, let $I = \omega$, $M_i = N$ (all $i \in I$) and let F be any non-principal ultrafilter (i.e., $F \neq \{K \subseteq \omega \mid x \in K\}$ for any $x \in \omega$). See [20] for a proof of this fact.

In [1], we discussed examples of nonstandard models of fragments of arithmetic. If a subtheory T of CA is weak enough, T may have nonstandard models with very simple structure, e.g., $\ast N$ may result by simply adjoining a single nonstandard point to N and extending $+$, \times to $N \cup \{\omega\}$. Since there are constructive definitions of such extended models, a problem which is equivalent to the existence of such a $\ast N$ may be resolved by entirely constructive means. PT, on the other hand, has only nonstandard models which are non-effective in the sense that at least one of $\ast +$ and $\ast \times$ must be nonrecursive. This result is due to Solovay.

Theorem 3.4.[1]. If $PT \models M$ and $+^M, \times^M$ are both recursive functions with respect to an effective enumeration of M , then $M = \{0,1,2,\dots\}$, that is, M is (isomorphic to) the standard model.

Notice that Theorems 3.1 and 3.4 together do not quite imply that proving a nonpolynomial lower bound requires nonconstructive arguments. On the other hand, any such proof necessarily implies the existence of certain noneffective functions.

4. Consistency of ET + "P = NP"

Recall that ET is the theory of true sentences

$$\forall \vec{x} \phi(\vec{x})$$

where ϕ is quantifier free and contains only terms formed from $+$, $-$, \times , \exp , \min , \max , and polynomial time computable predicates. For convenience in this section and in the remaining sections, we let α denote a special fixed constant which does not otherwise appear in ET, or in PT.

When it is convenient, we will confuse a term of ET with the function it denotes in N. We will also require a few preliminary facts about terms in ET.

Lemma 4.1. Let $f(x)$, $g(x)$ be terms of ET. Then for sufficiently large x either $f(x)$ is a constant or $f(x) \rightarrow \infty$ and is monotone (more precisely, $f(x) \geq \log^{(k)} x$).[†] Further, for all $x > x_0$ either $f(x) \geq g(x)$ or $f(x) < g(x)$.^{††}

Proof. This is essentially a result due to Hardy [24]. Let us say that an elementary function (what Hardy called a logarithmico-exponential function) is one which can be obtained

from $+$, $-$, \times , and c^x for any constant $c \geq 2$. Hardy proved that

- (i) beyond some point every elementary function is monotone and tends to a definite limit (including possibly $\pm \infty$);
- (ii) if $f(x) \rightarrow \infty$ is elementary then for some k , $f(x) \geq \log^k(x)$, when $x > x_0$.

The lemma follows from (i) and (ii) provided only that for each term $f_1(x)$ there is an elementary $f_2(x)$ so that $f_1(x) = f_2(x)$ for all sufficiently large x . But this is equivalent to showing that $+$, \min , \max do not lead outside the class of elementary functions. Let f_1 and f_2 be elementary. Then

$$h(x) = f_1(x) - f_2(x)$$

is elementary and so either $h(x) < 0$ or $h(x) \geq 0$, for $x > x_0$. If $h(x) \leq 0$ then $f_1(x) \leq f_2(x) = 0$.

If $h(x) \geq 0$ then $f_1(x) \div f_2(x) = h(x)$.

In both cases $f_1(x) \div f_2(x)$ is eventually defined by an elementary function.

The arguments for \min , \max are similar. \square

[†] $F^{(k)}(x)$ denotes $\underbrace{F(F \dots F(x) \dots)}_{k\text{-times}}$.

^{††} The asymptotic behavior of a function $F : N \rightarrow N$ is always phrased in terms of $F(x)$ for all x greater than some $x_0 \in N$. The choice of x_0 is implicit in the definition of the property and x_0 will always be used in this way without further explanation.

We will call any term $f(x) \rightarrow \infty$ of ET nontrivial; otherwise it is trivial. Also, for any term $f(x)$, $k \in N$, and finite $A \subseteq N$ we write $\langle f, k, A \rangle$ when for all $x > x_0$ the value of $f(x) \bmod k$ can be computed from

$$\{x \bmod \ell \mid \ell \in A\}.$$

In particular, if $\langle f, k, A \rangle$ and $x \equiv y \bmod \ell$ for all $\ell \in A$, then $f(x) \equiv f(y) \bmod k$ provided x is large enough.

Lemma 4.2. For any term $f(x)$ and $k \in N$, there is a set A such that $\langle f, k, A \rangle$.

Proof. First notice that if $(k_1, k_2) = 1$ and $\langle f, k_1, A_1 \rangle$, $\langle f, k_2, A_2 \rangle$ then $\langle f, k_1 k_2, A_1 \cup A_2 \rangle$. Therefore, we can assume that $k = p^n$, p a prime. We proceed by induction on the structure of the term $f(x)$

- (1) $f(x)$ is 1 or x . Then $A = \{p^n\}$ suffices.
- (2) $f(x)$ is $g(x) + h(x)$. Then $\langle g, p^n, A_1 \rangle$ and $\langle h, p^n, A_2 \rangle$ and so, $\langle f, p^n, A_1 \cup A_2 \rangle$.
- (3) $f(x)$ is $g(x) \times h(x)$. This follows as in case (2).
- (4) $f(x)$ is $g(x) \div h(x)$. By Lemma 4.1, $f(x)$ eventually becomes either 0 or $g(x) - h(x)$. Both cases follow as above.
- (5) $f(x)$ is $\min(g(x), h(x))$ or $\max(g(x), h(x))$. This is similar to case (4).
- (6) $f(x)$ is $c^{g(x)}$ ($c \geq 2$). By Lemma 4.1 either $g(x) \rightarrow \infty$ monotonically or it is constant, in which case there is nothing to do. If $p \mid c$ then $f(x) \bmod p^n$ is 0 for all x sufficiently large. If on the other hand $p \nmid c$, then $f(x) \bmod p^n$ is determined by $g(x) \bmod \phi(p^n)$, where ϕ is Euler's phi function. But since there is an A such that $\langle g, \phi(p^n), A \rangle$, it follows that $\langle f, p^n, A \rangle$. \square

Lemma 4.3. If $f(x)$ is nontrivial and $A \subseteq N$ is an arithmetic progression (a.p.), then there is an a.p. $A_0 \subseteq A$ and $k \in N$ such that for all $x \in A_0$, $f(x) \not\equiv 0 \bmod k$.

Proof. Let $A = \{cm + d \mid m > 0\}$, $c > 0$, $d > 0$. Also, let $g(x) = f(cx + d)$. Since g is nontrivial, $g(x_0) \neq 0$ for some x_0 , so let $g(x_0) \not\equiv 0 \bmod k$.

By Lemma 4.2 there is a $B \subseteq N$ such that $\langle g, k, B \rangle$. All $x \in B$ are > 0 so define b as the product of all elements of B ,

$$b = \prod B.$$

By the definition of B , $x \equiv x_0 \pmod{b}$ implies $g(x) \equiv g(x_0) \pmod{k}$, provided x is large. Choose

$$A_0 = \{c(bm + x_0) + d \mid m \geq m_0\}, \quad m_0 \in \mathbb{N}.$$

Clearly $A_0 \subset A$. Moreover

$$\begin{aligned} f(c(bm + x_0) + d) &\equiv g(bm + x_0) \pmod{k} \\ &\equiv g(x_0) \pmod{k} \\ &\equiv 0 \pmod{k}. \quad \square \end{aligned}$$

We define a class of formulas, P : P is the smallest class of ET formulas such that

- (i) every ET predicate is contained in P ,
- (ii) P is closed under Boolean operations,
- (iii) if $\phi(x) \in P$, then $(\exists x < \alpha)(\phi(x)) \in P$.

Intuitively, P corresponds to predicates in P , since all quantifiers involved in the definition of P may be thought of as "finite" searches through P -time predicates.

We are now ready to state the main result of this section.

Theorem 4.4. Let A be a predicate so that

$$\{x \mid (\exists y)(A(x, y))\}$$

is NP-complete. Then for some $\phi(x) \in P$

$$ET + (\forall x)((\exists y)A(x, y) \leftrightarrow \phi(x))$$

is consistent.

Proof. We will construct a nonstandard model in a sequence of lemmas.

Lemma 4.5. There is a model M of ET with α^M non-standard such that:

- (i) $M = \{f(\alpha) \mid f(x) \text{ is a term of ET}\}$
- (ii) if $f(x)$ is trivial, then $M \models f(\alpha) = 0$; otherwise, for some $k \in \mathbb{N}$, $M \models f(\alpha) \not\equiv 0 \pmod{k}$.
- (iii) $\{\phi(\alpha) \mid \phi(\alpha) \text{ is a quantifier-free sentence and } M \models \phi(\alpha)\}$ is arithmetically definable.

Proof. We construct M in stages. Let $T_0 = ET$ and $A_0 = \mathbb{N}$. At each stage i , T_i is a theory and A_i is an a.p. We assume that the terms of ET have been arranged into an RE listing

$$f_1(x), f_2(x), \dots$$

Assuming stage $i-1$ is completed, proceed with stage i as follows. If $f_i(x)$ is trivial, then define

$$T_i = T_{i-1} + "f_i(\alpha) = 0" + "\alpha \geq i",$$

and let $A_i = A_{i-1}$. If $f_i(x)$ is nontrivial then by Lemma 4.3 there is an a.p. $A_i \subseteq A_{i-1}$ and an

integer k so that $f_i(x) \not\equiv 0 \pmod{k}$, for all $x \in A_i$.

In this case, choose

$$T_i = T_{i-1} + "f_i(\alpha) \not\equiv 0 \pmod{k}" + "\alpha \geq i".$$

Notice that $N \models T_i$ for each i provided only that

$\alpha^N \geq i$ lies in the a.p. A_i . Therefore by the Deduction Theorem

$$T_\infty = T_0 + T_1 + \dots$$

is a consistent extension of ET.

Our next step is to suppose that all quantifier-free sentences $\phi(\alpha)$ are RE-listed ϕ_1, ϕ_2, \dots . Now, proceed in stages to extend T_∞ by adding at each stage ϕ_i or $\neg \phi_i$ according to whether the resulting theory is consistent. Let T denote the resulting theory. T is clearly consistent.

Let $M' \models T$ and define $M \subset M'$ to be $M = \{f_i(\alpha) \mid i \in \mathbb{N}\}$. Since T is an open theory, $M \models T$. M clearly satisfies restriction (i). Since $T \supset T_\infty$, $M \models T_\infty$ and so M satisfies restriction (ii). Finally, an examination of the construction above reveals that it is arithmetically definable, so restriction (iii) is also met. \square

M will henceforth denote the model constructed above. We now show that it is also the model required by the theorem.

Lemma 4.6.

- (i) The standard elements of M are defined by a formula in P .
- (ii) There is a formula $B(x) \in P$ so that $M \models \phi(\alpha) \leftrightarrow B(\ulcorner \phi(\alpha) \urcorner)$ for $\phi(\alpha)$ any quantifier-free sentence.

Proof.

Of Part (i). Let $R(x, y)$ denote $x \leq \log^* y$ and define

$$e_n(x) = \begin{cases} x, & \text{if } n = 0 \\ 2^{e_{n-1}(x)}, & \text{if } n > 0. \end{cases}$$

We claim that x is standard iff $M \models R(x, \alpha)$.

Suppose that $x = m \in \mathbb{N}$. It is easy to see that for some $n \in \mathbb{N}$

$$ET \vdash R(m, n)$$

and also that

$$ET \vdash R(x, y) \wedge z > y \rightarrow R(x, z)$$

But $M \models \alpha > n$ and thus $M \models R(m, \alpha)$. If x is standard $M \models R(x, \alpha)$. If x is nonstandard we cannot have $M \models R(x, \alpha)$. Suppose otherwise. By Lemma 4.5, $x = f(\alpha)$ for some nontrivial $f(x)$. So, by Lemma 4.1, there is a k such that

$f(w) \geq \log^{(k)} w$. It is easy to verify that

$$ET \vdash e_k(f(w)) \geq w$$

and for some n ,

$$ET \vdash R(x, z) \wedge e_k(x) > z \rightarrow z > n.$$

Let $\alpha \equiv \alpha$ we get the contradiction $M \models \alpha < n$.

Of Part (ii).

The truth of $\phi(\alpha)$ in M is definable by an arithmetical formula by Lemma 4.5. Since Part (i) establishes that the standards in M are definable, the arithmetical definition can be relativized to the standards in M . \square

We will now show that

$$M \models (\exists y)A(x, y) \leftrightarrow (\exists i)(\exists j) (E(x, i, \alpha) \wedge B(\ulcorner A(f_i(\alpha), f_j(\alpha)) \urcorner)), \quad (4.1)$$

where $i, j \in \mathbb{N}$ and $E(x, i, \alpha)$ is

$$(\forall k)(\forall \ell)(\ell \equiv x \bmod k \leftrightarrow B(\ulcorner \ell \equiv f_i(\alpha) \bmod k \urcorner))$$

where $k, \ell \in \mathbb{N}$. By Lemma 4.6, this will imply that for some $\phi \in P$,

$$M \models (\exists y)A(x, y) \leftrightarrow \phi(x).$$

The key to proving (4.1) is that for any $i \in \mathbb{N}$,

$$M \models x = f_i(\alpha) \leftrightarrow E(x, i, \alpha). \quad (4.2)$$

To see this, suppose that (4.2) is true. If

$M \models (\exists y)A(x, y)$, then, by Lemma 4.5,

$$M \models A(f_i(\alpha), f_j(\alpha)) \wedge x = f_i(\alpha),$$

for all i, j .

Then by Lemma 4.6,

$$M \models B(\ulcorner A(f_i(\alpha), f_j(\alpha)) \urcorner) \wedge E(x, i, \alpha),$$

establishing (4.1) in one direction. The opposite direction is similar.

Suppose first that $M \models x = f_i(\alpha)$. Then clearly for any standard k, ℓ

$$M \models \ell \equiv x \bmod k \leftrightarrow \ell \equiv f_i(\alpha) \bmod k.$$

From the definition of E and Lemma 4.6,

$M \models E(x, i, \alpha)$. On the other hand, suppose that

$M \models x \neq f_i(\alpha)$. We will show $M \not\models E(x, i, \alpha)$: suppose not. By Lemma 4.5 there is a j such that

$M \models x = f_j(\alpha)$. Lemma 4.1 allows us to assume

that eventually either $f_i(x) \geq f_j(x)$ or

$f_i(x) \leq f_j(x)$. The cases are essentially symmetric

so assume that $f_i(x) \geq f_j(x)$ for $x > x_0$. Let $f(x)$

be the term $f_i(x) \dot{-} f_j(x)$. Observe that $f(x)$ cannot be trivial. For suppose that $f(x)$ is trivial.

Lemma 4.5 shows that $M \models f(\alpha) = 0$.

We have

$$ET \vdash x \geq x_0 \rightarrow f_i(x) \geq f_j(x)$$

and

$$ET \vdash x \dot{-} y = 0 \wedge x \geq y \rightarrow x = y$$

Hence since α is nonstandard and $M \models ET$, it follows that $M \models f_i(\alpha) = f_j(\alpha)$.

But then $M \models f_i(\alpha) = x$, a contradiction.

Therefore, $f(x)$ is nontrivial. By Lemma 4.5, there is a k such that $M \models f(\alpha) \neq 0 \bmod k$. We have also

$$ET \vdash x \geq x_0 \rightarrow f_i(x) \geq f_j(x), \quad (4.3)$$

$$ET \vdash 0 \equiv x \bmod k \vee 1 \equiv x \bmod k \vee \dots \vee (k-1) \equiv x \bmod k, \quad (4.4)$$

and

$$ET \vdash y \geq z \wedge x \equiv y \bmod k \wedge z \equiv z \bmod k \rightarrow (y \dot{-} z) \equiv 0 \bmod k. \quad (4.5)$$

Since $M \models ET$, it follows that $M \models \ell \equiv f_i(\alpha) \bmod k$, for some ℓ . The definition of E ,

Lemma 4.6, and the assumption that $E(x, i, \alpha)$ is true in M together imply $M \models \ell \equiv x \bmod k$ or, equivalently, $M \models \ell \equiv f_j(\alpha) \bmod k$.

By the theorems of ET (4.3)-(4.5),

$$M \models (f_i(\alpha) \dot{-} f_j(\alpha)) \equiv (\ell \dot{-} \ell) \bmod k,$$

contradicting $M \models f(\alpha) \neq 0 \bmod k$. \square

5. Extending ET

The methods used in the proof of Theorem 4.4 can be used to obtain more general results. For instance, ET can be extended by the addition of any recursively enumerable list of recursive predicates; the resulting theory remains consistent with " $P = NP$ ".

The process of adding new functions to ET is much more delicate. The proof of Theorem 4.4 depends critically on the structure of the terms of ET. The chief difficulty in proving Theorem 4.4 is accounting for the fact that the terms of ET can grow very quickly; this forces us to test the truth of $x = f_i(\alpha)$ indirectly. Clearly, the procedure which evaluates $y = f_i(\alpha)$ and then checks $y = x$ does not necessarily run in polynomial time. Besides growth, the terms of ET are subject to another complexity: the presence of $\dot{-}$ in the terms of ET and the complex cancellation it allows. In order to underscore the problems $\dot{-}$ introduces, we will briefly study another theory T . This theory contains all those predicates computable in polynomial time; additional ones can be added as discussed above. A recursive function $\lambda(x)$ that tends to infinity monotonically but arbitrarily slowly (for example, $\lambda(x) = \log^* x$) is fixed. The terms of T are then built up from $+$ and \times (but not $\dot{-}$) and any recursively enumerable list of recursive functions that satisfy

- (*) if a term $f(x)$ is unbounded, then $f(x) > \lambda(x)$ for x sufficiently large;

(**) the predicate $f_i(x) = y$ (as a function of x, y, i) can be computed in time $e_m(y + i)$ for some constant m .

Before proceeding it is necessary to define a predicate " $x \in y$ " and a function " $r(x, y)$ ":

$x \in y$ if and only if $x = |y| + \ell$ and the ℓ^{th} bit of y as a binary number is a 1.

Defining $r(x, y)$ there are two cases to consider.

if $|x| \neq |y|$ then $r(x, y) = |x| + |y| + 1$;
second if $|x| = |y|$, then $r(x, y) = |x| + \ell$ where ℓ is the first bit position where x and y differ; if no such position then ℓ is $|y| + 1$.

Note that if $|x| = |y|$ and $x \neq y$ then there is a $y \leq 2^{|x|}$ such that

$$r(x, y) \in x \leftrightarrow r(x, y) \notin y$$

The reason for the unusual definitions used here is a technical one; the function $r(x, y)$ satisfies (*) and so we can assume that T contains it. $r(x, y)$ cannot be defined to be the first position where x and y differ without violating (*).

We are finally ready to state our theorem:

Theorem 5.1. $T + "P = NP"$ is a consistent theory.

Proof. The initial part of this proof follows closely that of Theorem 4.4. Let M be the model of T constructed as in Theorem 4.4. Thus in M the set of standards has a P definition -- this uses property (*) of T . Also $M \models B(\ulcorner \phi \urcorner) \leftrightarrow \phi$ for any quantifier free ϕ . The plan is to finish the proof as before, but with a new twist: we can no longer use the residue method to check $x = f_i(\alpha)$ quickly.

Our way around this difficulty is based on (**) and the function $r(x, y)$. Let $E_0(x, i, \alpha)$ denote the formula $x = f_i(\alpha)$; let $E_n(x, i, \alpha)$ denote the formula

$$\exists k (E_{n-1}(|x|, k, \alpha) \wedge B(\ulcorner f_k(\alpha) = f_i(\alpha) \urcorner) \wedge$$

$$(\forall \ell) (\forall y \leq 2^{|x|}) E_{n-1}(y, \ell, \alpha) \rightarrow$$

$$[y \in x \leftrightarrow B(\ulcorner f_\ell(\alpha) \in (f_i(\alpha)) \urcorner)])$$

where as before k and ℓ range over only standards. The theorem will follow once we have proved two claims: first, that $M \models E_n(x, i, \alpha) \leftrightarrow x = f_i(\alpha)$ for any fixed n ; second, that for n large enough $E_n(x, i, \alpha)$ is in P .

We will first show that $E_n(x, i, \alpha) \leftrightarrow x = f_i(\alpha)$ is true in M for any $n \geq 0$. For $n = 0$ this is obvious. Suppose therefore that $n > 0$ and that $M \models x = f_i(\alpha)$. Then an easy argument based on the inductive hypothesis and the definition of B establishes $M \models E_{n-1}(x, i, \alpha)$. On the other hand, suppose that $M \models x \neq f_i(\alpha)$ and $M \models E_n(x, i, \alpha)$. By assumption, there is a k so that $E_{n-1}(|x|, k, \alpha)$; hence, by induction $M \models |x| = f_k(\alpha)$.

$M \models f_k(\alpha) = |f_i(\alpha)|$, and $M \models |x| = |f_i(\alpha)|$. As discussed above it then follows in M that there is a $y \leq 2^{|x|}$ such that $y = r(x, f_i(\alpha))$ and

$$y \in x \leftrightarrow y \notin f_i(\alpha).$$

By the construction of M there is a ℓ so that $y = f_\ell(\alpha)$. So by induction $M \models E_{n-1}(y, \ell, \alpha)$. But then in M ,

$$y \in x \leftrightarrow B(\ulcorner f_\ell(\alpha) \in f_i(\alpha) \urcorner)$$

$$\leftrightarrow f_\ell(\alpha) \in f_i(\alpha)$$

$$\leftrightarrow y \in f_i(\alpha),$$

which is a contradiction.

It remains only to prove the second claim: $E_n(x, i, \alpha)$ is in P for n large enough. By (**), $y = f_i(x)$ can be computed in time $e_m(y + 1)$ for some m . It is also easy to see that $E_n(x, i, \alpha)$ can be computed in polynomial time plus the time required for the $E_0(y, j, \alpha)$ used. But an inspection of these formulas shows that $E_0(y, j, \alpha)$ is used only when $y \leq \log^{(n)} x$. So let $E(x, y, j, \alpha)$ be $E_0(y, j, \alpha)$ if $y \leq \log^{(n)} x$ and false otherwise. Then $E(x, y, j, \alpha)$ can be computed in time polynomial in $e_m(y + j)$. Since j is a standard,

$$e_m(y + j) \leq e_m(2y) + e_m(\log^{(n)} \alpha)$$

(for if y is a nonstandard, $2y > y + j$; otherwise $\log^{(n)} \alpha > y + j$). Then for n large enough this is polynomial in $|x|$. Thus $E_n(x, i, \alpha)$ is in P for n large enough. \square

6. Model-Completeness

A good intuitive basis for understanding the $P = NP$ problem lies in quantifier elimination: if $(\exists y)B(x, y)$ defines an NP-complete set, $P = NP$ exactly when $(\forall x)(A(x) \leftrightarrow (\exists y)B(x, y))$. This is the essence of Theorem 3.1.

There is a well-developed model theory of quantifier-elimination. We will sketch the basic theory in this section -- the numbered theorems will be used in Section 7. For a more complete discussion, see MacIntyre's survey article in [2], or the more detailed treatment in [25].

Let T_0, T_1 be theories over the same language L . Then T_1 is said to be model-consistent relative to T_0 if for all models M_0 of T_0 there is a model M_1 of T_1 extending M_0 . Let M be a structure and denote by $LANG(M)$ the language of M ; i.e., the language obtained from L by adding constants for each element of M . Define the diagram of M , $DIAG(M)$, to be the set of all atomic formulas in $LANG(M)$ and their negations which hold in M .

Lemma 6.1 [25]

- (i) T_1 is model-consistent relative to T_0 iff for each model M of T_0 , $T_1 + \text{DIAG}(M)$ is a consistent theory.
- (ii) T_1 is model-consistent relative to T_0 iff for each universal sentence ϕ , $T_1 \vdash \phi$ implies $T_0 \vdash \phi$.

Notice that by Lemma 6.1 (ii) if the universal members of T_1 are contained in the universal members of T_0 , then every model of T_0 is embedded in a model of T_1 .

Let M_0, M_1 be structures for the same language with $M_0 < M_1$. M_1 is an elementary extension of M_0 , $M_0 < M_1$, if for all sentences ϕ defined in M_1 , $M_1 \models \phi$ iff $M_0 \models \phi$. The theory T is called model-complete if whenever M_0, M_1 are models of T and $M_0 < M_1$, then $M_0 < M_1$. The term "complete" is explained by the following characterization.

Lemma 6.2. [25] T is model-complete iff $M \models T$ implies $T + \text{DIAG}(M)$ is a complete theory.[†]

This should be compared with Lemma 6.1 (i).

More directly, the relationship with quantifier-elimination is via the concept of existential completeness. A substructure $M_0 < M_1$ is existentially complete in M_1 if every existential sentence ϕ defined in M_0 and such that $M_1 \models \phi$ is also true in M_0 . Existential completeness is the model theoretic generalization of algebraic closure of a field k (by, for instance, the Hilbert Nullenstatz): if $\{p_i\}, \{q_j\}$ are polynomials with coefficients in k and if in some extension L of k there are elements a'_1, a'_2, \dots, a'_n such that

$$p_i(a'_1, a'_2, \dots, a'_n) = 0, \quad \text{all } i$$

$$q_j(a'_1, a'_2, \dots, a'_n) \neq 0, \quad \text{all } j$$

then there are already $a_i \in k$ ($1 \leq i \leq n$) such that

$$p_i(a_1, \dots, a_n) = 0, \quad \text{all } i$$

$$q_j(a_1, \dots, a_n) \neq 0, \quad \text{all } j$$

Let $E(T)$ be the class of existentially complete models for T .

[†] That is, for any ϕ , either $\vdash \phi$ or $\vdash \neg \phi$.

In other words, $M_0 \in E(T)$ if

- (i) M_0 is a structure of the proper type,
- (ii) $M_1 \models T$ for some $M_1 > M_0$,

and

- (iii) for any model M_1 of T , if $M_1 > M_0$, then M_0 is existentially complete in M_1 .

Our claim that model-completeness implies a form of quantifier elimination is now provided by the following theorem, sometimes called Robinson's Test.

Theorem 6.3. [25] T is model-complete iff whenever M_0, M_1 are models of T and $M_0 < M_1$, then M_0 is existentially complete in M_1 .

A theory T_1 is said to be a model-companion of T_0 when

- (i) T_0 and T_1 are mutually model-consistent
- (ii) T_1 is model-complete.

Lemma 6.4. [25] If T_1 is a model-companion of T_0 , then $E(T_0) = \{M \mid M \models T_1\}$.

A collection of structures K is a generalized elementary class (EC_Δ) if for some set of sentences Σ

$$K = \{M \mid M \models \Sigma\};$$

i.e., if the property of being a structure in K is a first order property.

For example, the collection of all commutative fields of characteristic zero is EC_Δ .

Lemma 6.5 follows from Los's Theorem.

Lemma 6.5. [26] If $K \in EC_\Delta$, then K is closed under formation of ultraproducts.

Lemma 6.6. [25] T has a model companion iff $E(T) \in EC_\Delta$.

The final fact concerning existential completeness is due to Robinson.

Lemma 6.7. [27] There is a fixed sentence ϕ such that for all $M \in E(\Pi_2)$, $M \models \phi[m]$ if and only if m is nonstandard.

Lemma 6.7 has the corollary that no non-standard models of arithmetic can be existentially complete structures.

7. On the Consistency of PT + "NP ≠ coNP"

Let $\lambda(x) \rightarrow \infty$ as slowly as desired. As in Section 3, we let $\Delta_S(A, B)$ be a predicate so that

$$\Delta_S(A, B) \leftrightarrow [(\forall x)((\exists y)(|y| \leq |x|^{\lambda(|x|)} \wedge A(x, y)) \leftrightarrow (\exists z)(|z| \leq |x|^{\lambda(|x|)} \wedge B(x, z))].$$

First, note that even though PT contains no symbols for exponential formation the predicate $|y| \leq |x|^{\lambda(|x|)}$ can be expressed in PT. For instance, the following predicates express this relationship

$$(i) \log y \leq \lambda(\log x) \times \log x$$

$$(ii) |y|^{1/\lambda(|x|)} \leq |x|.$$

It is not necessary to be able to actually construct the exponential terms.

We use $\text{NTIME}(f(n))$ to denote the problems solved in nondeterministic $f(n)$ time. Similarly for $\text{coTIME}(f(n))$. Note that $\text{NTIME}(n^{\lambda(n)})$ majorizes NP as closely as desired. If $\text{PT} \vdash \text{"NTIME}(n^{\lambda(n)}) = \text{coTIME}(n^{\lambda(n)})\text{"}$ then for every model M of PT, it is the case that for each A

$$M \vdash \Delta_S(A, B)$$

for some B , and conversely.

Theorem 7.1. $\text{PT} + \text{"NTIME}(n^{\lambda(n)}) \neq \text{coTIME}(n^{\lambda(n)})$ is consistent.

Proof. We assume

$$\text{PT} \vdash \text{"NTIME}(t) = \text{coTIME}(t)\text{"},$$

where $t(n) = n^{\lambda(n)}$. Choose a constant α , not appearing in PT, and let BA_α be the axiom

$$(\forall x)(|x| \leq |\alpha|^{\lambda(|\alpha|)}),$$

bounding the individuals x .

Lemma 7.2. $\text{PT} + \text{BA}_\alpha$ and PT are mutually model-consistent.

Proof. Since any model of $\text{PT} + \text{BA}_\alpha$ is also a model of PT, it is sufficient to show that any model of PT can be extended to a model of $\text{PT} + \text{BA}_\alpha$. Let $M \models \text{PT}$ and let $M = \{m_0, m_1, \dots\}$.

Then

$$\text{PT} + \text{DIAG}(M) + \bigwedge_{i < k} \alpha > m_i$$

is consistent for each standard k . Thus by compactness

$$\text{PT} + \text{DIAG}(M) + \bigwedge_{m \in M} \alpha > m$$

is consistent, with model, say, M_0 . Let $M_\alpha \subset M_0$ be the substructure generated by $M \cup \{\alpha\}$. Since PT is open, $M_\alpha \models \text{PT}$. Since $\lambda \rightarrow \infty$ slowly, $\lambda(\alpha) \leq k \in \mathbb{N}$ implies $\alpha \leq \ell \in \mathbb{N}$, so $\lambda(\alpha)$ is non-

standard. Notice that M_α contains only elements of the form

$$x = h(\alpha, m_1, \dots, m_k),$$

for PT terms $h(x_1, \dots, x_{k+1})$, so that $|x| \leq |\alpha|^s$ for some $s \in \mathbb{N}$. Hence

$$M_\alpha \models (\forall x)(|x| \leq |\alpha|^{\lambda(|\alpha|)}).$$

Thus $\text{PT} + \text{BA}_\alpha$ is consistent. \square

Lemma 7.3 $\text{PT} + \text{BA}_\alpha$ is model-complete.

Proof. Choose $M_0 \subset M_1$ so that $M_0 \models \text{PT} + \text{BA}_\alpha$ and $M_1 \models \text{PT} + \text{BA}_\alpha$. Clearly, if ϕ is any existential sentence defined and true in M_0 , then $M_1 \models \phi$ since $M_0 \subset M_1$. We proceed by induction to apply Robinson's Test. Let $\phi(x, \alpha)$ be open and consider $(\forall x)\phi(x, \alpha)$ which by BA_α is equivalent in any model to

$$(\forall x)(|x| \leq |\alpha|^{\lambda(|\alpha|)} \rightarrow \phi(x, \alpha)),$$

which we abbreviate

$$(\forall |x| \leq |x|^{\lambda(|\alpha|)})\phi(x, \alpha).$$

Since ϕ is some A in PT and $\text{NTIME}(n^{\lambda(n)}) =$

$\text{coTIME}(n^{\lambda(n)})$, there is some B in PT such that

$$(\exists |x| \leq |\alpha|^{\lambda(|\alpha|)})B(x),$$

or

$$(\exists |x| \leq |\alpha|^{\lambda(|\alpha|)})\sigma(x, \alpha),$$

which is existential.

At the induction step, consider $(\forall x)\phi(x, \alpha)$, which, by the construction above, is equivalent to

$$(\forall |x| \leq |\alpha|^{\lambda(|\alpha|)})(\exists |y| \leq |\alpha|^{\lambda(|\alpha|)})\sigma(x, y, \alpha),$$

which, since $\text{NTIME}(n^{\lambda(n)}) = \text{coTIME}(n^{\lambda(n)})$, is in turn equivalent to

$$(\forall |x| \leq |\alpha|^{\lambda(|\alpha|)})(\forall |y| \leq |\alpha|^{\lambda(|\alpha|)})\psi(x, y, \alpha),$$

and this is equivalent to an existential sentence. \square

The proof is now nearly complete. Since we have just shown that $\text{PT} + \text{BA}_\alpha$ is a model companion for PT, $E(\text{PT}) \in \text{EC}_\Delta$, by Lemma 6.6 and so by Lemma 6.5 is closed under function of ultra-products.

Lemma 7.4. $N \in E(\text{PT})$

Proof. Suppose otherwise, and let $M \models \text{PT}$ be an extension of N . Let $(\exists x)\phi(x)$ be defined in N with

$M \models (\exists x)\phi(x)$ and $N \not\models (\exists x)\phi(x)$.

But then, $N \models (\forall x) \rightarrow \phi(x)$, so $(\forall x) \rightarrow \phi(x)$ is an axiom of PT, contradicting our choice of ϕ . \square

Now, choose a nonprincipal ultrafilter F on 2^ω , so that $N^\omega/F \in E(PT)$. Since the universal members of Π_2 are also axioms of PT, $N^\omega/F \in E(\Pi_2)$ by Lemma 6.1. By Lemma 6.7 the nonstandards have a first order definition in any $M \in E(\Pi_2)$, but the overspill lemma holds in N^ω/F , which is a contradiction. \square

An analysis of the above proof suggests that it is not very sensitive to our choice of PT as the underlying theory. To make this apparent, let C be a class of functions defining time classes, and let $C_\lambda \supset C$ represent a class which majorizes C arbitrarily closely. For example, if $C = U \{x^k | k \geq 0\}$, $C_\lambda = x^{\lambda(x)}$ is a possible choice.

Theorem 7.5. Let T be any theory and $\text{NTIME}(C)$ be any nondeterministic time class such that

- (i) all predicates in T are computable in deterministic time C ,
- (ii) every term in T is eventually bounded by a function in C ,
- (iii) if ϕ is open, $N \models \phi$, then $T \vdash \phi$.

Then $T + \text{"NTIME}(C_\lambda) \neq \text{coTIME}(C_\lambda)"$ is consistent.

Proof. The proof parallels the proof of Theorem 7.1. \square

A major open problem left unresolved here is the relationship between

$$PT + \text{"NP} \neq \text{coNP"}$$

and

$$PT + \text{"NTIME}(n^{\lambda(n)}) \neq \text{coTIME}(n^{\lambda(n)})"$$

In general, we would like to know: is it possible that

$$T \vdash \text{NTIME}(C) = \text{coTIME}(C)$$

but

$$T \vdash \text{NTIME}(C_\lambda) \neq \text{coTIME}(C_\lambda)?$$

8. On Independence Theorems in Complexity Theory

Hartmanis and Hopcroft [4] have pointed out that it is quite easy to obtain independence results in complexity theory. Unfortunately, the methods of [4] do not seem to be well-adapted to our problems. First, we are not concerned with simple undecidability. That is, we cannot choose a theory and encode the undecidable statement into the theory. This rule also rules out relativization-style results as in [28]. Second, we must work with specific fragments of number theory,

e.g., Π_2 , ET, PT, or PA.

Until Paris' announcement [3] that a minor generalization of the finite Ramsey theorem is independent of PA, there were no natural examples of mathematical statements which are independent of PA whose undecidability did not follow from explicit encoding and diagonalization. This was especially surprising in view of the extant independence results for geometry and various set theories.

Following [3], O'Donnel [29] announced a "programming language theorem" which cannot be resolved in PA. We will have more to say about these proofs in a moment.

The only remaining methods available for constructing nonstandard models of PA do not lead to sharp independence results. Let us look very briefly at forcing. In 1963, Cohen [22] proved that ZFC, a standard set theory, is consistent with

$$2^{\aleph_0} > \aleph_1$$

To prove this, Cohen constructed a nonstandard model of ZF by proceeding roughly as follows. The standard countable model contains ω ; to get 2^ω to be larger than the continuum, it is only necessary to put into ω some subsets not in

\aleph_1 . Since the result may not be a model of ZFC any more, some closure operations must be carried out. The technique of forcing allows one to construct larger and larger such models without violating the essential properties of the model. Robinson [30] has adapted this process to model theoretic construction. Let T be fixed. Using recursion-theoretic arguments, one proceeds from a set of forcing conditions (finite fragments of diagrams of models of T) to construct approximations to the diagram of the original model. These are internal arguments which argue explicitly about the structures of a model. Unfortunately such methods require a certain technical complexity on the part of the statement which is to hold in the nonstandard model.

By contrast the independence results of [3] rely on a tradition in proof theory dating from Gentzen [31]. In his proof of the consistency of number theory, Gentzen provided a rate-of-growth characterization of provability. It is possible to associate ordinal numbers with proofs in PA that indicate the "complexity" of the proof. No provable formula of PA can implicitly or explicitly mention the ordinal of its proof. Therefore, properties of functions which grow more quickly than the ordinals assigned to the proofs of those properties cannot be decided in PA. This growth argument approach has been the principle tool in recent independence results.

Let M be a finite set of integers. Define $f(n)$ to be the size of the smallest M such that for every n -coloring of the complete hypergraph with vertices M and hyperedges of degree n , there is a monochromatic $H \subset M$ with $|H| \geq \min(H)$ and $|H| > n+1$. In [32] it is shown that for some m , $f(n) \leq f_m(n)$, where

$$f_i(x) = \begin{cases} x + 2, & \text{if } i = 0 \\ [f_{i-1}]^{(x)}(2), & \text{otherwise} \end{cases}$$

Theorem 8.1. [32] Let g be a recursive function.
 $\Pi_1 \vdash "fg"$ is total" if $g(n) < f(n)$ for all $n > n_0$.

Such results are also characterizations of provability of $\text{PA} + \Pi_1$.

Theorem 8.2. [32] Let $N \models (\forall x)(\exists y)A(x,y)$ where A is quantifier-free.

Then

$$\text{PA} + \Pi_1 \vdash (\forall x)(\exists y)A(x,y)$$

iff

$$N \models A(x, g(x))$$

implies $g(x) \leq f_n(x)$ for some $m \in N$.

This device is exploited by O'Donnell to show that

$$\text{PA} + \Pi_1 \nvdash \text{"All programs in } L \text{ terminate"},$$

by showing that the programming language L defines functions violating the bounds in 8.1, 8.2.

Theorem 8.2 has special relevance. We cannot hope to prove the independence result of Section 3 by the methods of [32] since we explicitly assume that the Skolem function $g(x)$ is polynomial in x .

Indeed there seems to be no source of independence results

$$\text{PA} \nvdash \phi("fg")$$

where ϕ is a property and g is of polynomial growth. If techniques can be developed to deal with slowly growing albeit very irregular Skolem functions, the result should be a new method of building nonstandard models. This would appear to require new technical breakthroughs.

References

1. R. DeMillo, R. Lipton, "Some Connections Between Computational Complexity Theory and Mathematical Logic", Proceedings 11th ACM Symposium on Theory of Computing, 1979, pp. 153-159.
2. J. Barwise, editor, Handbook of Mathematical Logic, North-Holland, 1978.
3. J. Paris and L. Harrington, "A Mathematical Incompleteness in Peano Arithmetic", in [2], pp. 1132-1142.
4. J. Hartmanis and J. Hopcroft, "Independence Results in Computer Science", SIGACT News, Vol. 8, No. 4, 1976, pp. 13-23.
5. J. Hartmanis, Feasible Computation, SIAM, 1978.
6. R. Lipton, "Model Theoretic Aspects of Computational Complexity", Proceedings 19th FOCS, 1978, pp. 193-200.
7. L.G. Khachiyan, "A Polynomial Algorithm for Linear Programming" (in Russian) Doklady Akad. Nauk USSR, Vol. 244, No. 5, 1979, pp. 1093-1096.
8. Th. Skolem, "Über die Nicht-charakterisierbarkeit der Zahlenreihe Mittels endlich oder abzählbar unendlich vieler Aussagen mit ausschliesslich Zahlenvariablen", Fund. Math. 23, 1934, pp. 150-161.
9. D.S. Scott, "On Constructing Models for Arithmetic", Infinitistic Methods, Warsaw, 1959 (Oxford, 1961), pp. 235-255.
10. S. Cook, Feasibility Constructive Proofs and the Propositional Calculus", Proceedings Seventh ACM Symposium on the Theory of Computing, 1975.
11. S. Kleene, Introduction to Metamathematics, VanNostrand, 1953.
12. R. Statman, "Herbrand's Theorem and Gentzen's Notion of Direct Proof", in [2], pp. 897-912.
13. R. Statman, "Lower Bounds on Herbrand's Theorem", Proceedings of the American Mathematical Society, Vol. 15, No. 1, June, 1979, pp. 104-107.
14. A. Meyer and L. Stockmeyer, "Nonelementary Word Problems in Automata Theory and Logic", Proceedings AMS Symposium on Complexity of Computation, 1973.
15. V. Pratt, "Every Prime Has a Succinct Certificate", SIAM J. Computing, 1975.
16. D. Dobkin and S. Reiss, "The Complexity of Linear Programming", Yale University Technical Report, No. 69, June 1978.
17. J.P. Burgess, "Forcing", in [2], pp. 403-542.
18. Th. Skolem, "Peano's Axioms and Models of Arithmetic", Mathematical Interpretations of Formal Systems, Amsterdam, 1955, pp. 1-14.
19. A. Fraenkel, Abstract Set Theory, North-Holland, 1976.
20. J. Bell and M. Machover, A Course in Mathematical Logic, North-Holland, 1976.
21. J. Shepherdson, "Nonstandard Models of Fragments of Arithmetic", Model Theory, (J. Addison, ed.), North-Holland, 1963, pp. 342-358.
22. P.J. Cohen, Set Theory and the Continuum Hypothesis, Benjamin, 1966.
23. A. Ehrenfeucht and G. Kreisel, "Strong Models of Arithmetic", Mathematics and Logic, 1966.
24. G.H. Hardy, "Properties at Logarithmico-Exponential Functions", Proceedings of the London Mathematical Society, 1912, Vol. 2, No. 10, pp. 54-90.

25. W. Wheeler and J. Hirschfeld, Forcing, Arithmetic and Division Rings, Springer Lecture Notes in Mathematics #454, 1975.
26. J. Bell and J. Slomson, Models and Ultra-products, North-Holland, 1970.
27. A. Robinson, Nonstandard Arithmetic and Generic Arithmetic, Proceedings 4th International Congress on Logic, Methodology and Philosophy of Science, 1971, North-Holland, 1973, pp. 137-154.
28. T. Baker, J. Gill and R. Solovay, "Relativizations of the $P=?NP$ Question.", SIAM Journal of Computing 4 (Dec. 1975), pp. 431-432.
29. M. O'Donnell, "A Programming Language Theorem Which is Independent of Peano Arithmetic", Proceedings 11th ACM Symposium on Theory of Computing, 1979, pp. 176-188.
30. A. Robinson, "Forcing in Model Theory", Symposia Mathematica, Vol. 5, 1971, pp. 69-82.
31. M.E. Szabo, editor, The Collected Papers of Gerhard Gentzen, North-Holland, 1969.
32. J. Paris, "Some Independence Results for Peano Arithmetic", Journal of Symbolic Logic, 1978.

Acknowledgement: We would like to thank Mike Merritt for his careful reading of this paper.