

Arithmetic Theories for Computational Complexity Problems

STEVE HOMER*

Department of Computer Science, Boston University, Boston, Massachusetts 02215

AND

JOHN REIF†

Aiken Computation Laboratory, Harvard University, Cambridge, Massachusetts 02138

This paper considers a number of arithmetic theories and shows how the strength of these theories relates to certain open problems in complexity theory concerning the polynomial-time hierarchy. These results are proved quite generally and hold for a wide class of subrecursive hierarchies. They can be used to characterize certain properties of functions provable in these theories.

INTRODUCTION

Over the past several years there has been a flurry of interest in studying particular theories as they relate to some of the major open problems of complexity theory. This interest was kindled by the observations of Hartmanis and Hopcroft (1976) concerning the independence of the relativized $P = NP$ question and by the results of Kirby and Paris (1976), Harrington and Paris (1978), and Paris (1978) concerning a natural number-theoretic question independent of Peano arithmetic. The hope was raised that similar methods could be developed to yield interesting independence and consistency results for other naturally arising theories. While this idea has not been completely successful (see O'Donnell (1979) for a notable exception), related considerations have yielded a number of results relating open problems in computer science and various theories which arise naturally in their study. Significant work in this area can be found in Leivant (1982), Lipton and DeMillo (1979, 1980), Lipton (1978),

* This work was partially supported by NSF Grant MCS82-18383.

† This work was supported in part by NSF Grant MCS79-21024 and the Office of Naval Research Contract N00014-80-C-0647.

Joseph and Young (1980), Joseph (1983), and the recent work of Buss (1985).

These results have taken two major directions. One has been a discussion of whether particular theories are adequate for computer science. That is, one wants to base computer science on a theory which is sufficiently strong to settle the important questions in the field while at the same time not so strong as to mask the effective and computational nature of computer science. See Lipton (1978) and Joseph and Young (1980) for a detailed discussion of these ideas.

A second aspect of this approach has been to consider the central open problems of complexity theory and to show how these problems relate to the strength of various theories, generally Peano arithmetic or similar arithmetical theories. The main logical tools used here are model-theoretic and in general consist of the construction and study of non-standard models of the theory. Such results can be found in DeMillo and Lipton (1979, 1980), Leivant (1982), and Paris and Dimitracopoulos (1979).

This second approach is continued here. We are interested in classifying a number of these open problems by finding arithmetic theories of corresponding strength and sentences whose provability in these theories is equivalent to the original problem. Thus we provide a "translation" of these problems into logical problems where different techniques can be brought to bear.

This paper extends and generalizes the results of DeMillo and Lipton (1979). In (DeMillo and Lipton, 1979) they considered a first order quantified logic PT whose function and predicate symbols are restricted to polynomial time and whose axioms are all true Σ_2 sentences of this logic. They construct a formula ϕ_S for each $S \in NP \cap co-NP$ such that $S \in P$ iff $PT \vdash \phi_S$. Thus $P = NP$ is related to the strength of PT . This paper considers a general class of first order theories of bounded complexity with a restricted interpretation of the function and predicate symbols.

The main theorem presents the construction of DeMillo and Lipton in this more general setting. The proof, which is essentially that of (DeMillo and Lipton, 1979), is carried out in greater detail and with an eye to its applications. It is these applications which are the major contribution of the paper.

We show that provability of certain formulas is equivalent to properties of corresponding complexity-theoretic hierarchies. Several of these yield connections with the polynomial-time hierarchy of Stockmeyer (1976). Most notably they imply under certain circumstances, the collapsing of the hierarchy at certain levels as well as provability of certain properties of functions in this hierarchy. Another application is to the hierarchy of Δ_0^N sets of integers. Finally, an application to provably total functions is noted.

PRELIMINARIES

We will be dealing with models of arithmetic. Let N be the standard model and F a collection of functions on N closed under finite composition and containing all the 0-ary constant functions. A collection of predicates R on N is said to be *adequate* if

1. the polynomial-time predicates $P \subseteq R$,
2. R is closed under finite union and complementation, and
3. R is closed under F -substitution. That is, if $A(x_1, x_2, \dots, x_n) \in R$ and $t(y_1, y_2, \dots, y_n)$ is an m -ary term composed from elements of F then $A(t(y_1, y_2, \dots, y_n), x_2, x_3, \dots, x_n)$ is a relation in R . (Similarly with t substituted for other variables of R .)

From this point on R denotes an adequate collection of predicates. Note that P , $PSPACE$, and the classes $\Sigma_k^P \cap \Pi_k^P$ in the polynomial-time hierarchy are all adequate classes, where in each case F = the functions in the respective class. The language $L(R, F)$ is a first-order language which contains function symbols for every element of F , a predicate symbol for every element of R as well as the usual propositional connectives, first-order quantifiers, arithmetical symbols and equality.

The theory $T(R, F)$ is the collection of all true (in the standard model) sentences of $L(R, F)$ of the form $\exists \forall \theta$, where \exists is a string of existential quantifiers, \forall a string of universal quantifiers, and θ a quantifier free matrix whose functions and predicate symbols are restricted to the classes F and R . We will sometimes abuse notation and use the same symbol for a relation or function on N and for the symbol in our language which represents that relation or function. Note that $T(R, F)$ is not recursively enumerable and that, since Kleene's T predicate is in P (see Rogers, 1967), $T(R, F)$ contains all true Σ_2^0 facts about the integers.

We assume the reader is familiar with the polynomial-time hierarchy of Meyer and Stockmeyer (1976). We let P denote the polynomial-time predicates and P^F the polynomial-time computable functions. A second hierarchy we will consider is that of the Δ_0^N subsets of integers. A set $X \subseteq N$ is in the class Δ_0^N if X can be written as

$$\{m \in N \mid N \models Q_1 x_1 \leq m Q_2 x_2 \leq m \cdots Q_n x_n \leq m \theta(x_1 \cdots x_n, m)\}$$

where Q_1, \dots, Q_n is an alternating series of quantifiers and θ is a quantifier-free formula containing only the standard number-theoretic symbols (the usual logical symbols and symbols $+$, \cdot , S (successor) and 0).

The Δ_0^N sets can be broken up as follows:

$\Sigma_0^D = \Pi_0^D =$ sets definable over N by quantifier free formulas

$\Sigma_k^D =$ sets definable over N by a formula of the form

$$\exists \mathbf{x}_1 \leq m \forall \mathbf{x}_2 \leq m \cdots Q \mathbf{x}_k \leq m \theta(\mathbf{x}_1 \cdots \mathbf{x}_k, m),$$

where \mathbf{x}_i is a finite sequence of variables.

$\Pi_k^D =$ sets whose complements are in Σ_k^D .

Clearly $\bigcup_k \Sigma_k^D = \mathcal{A}_0^N$. The \mathcal{A}_0^N sets form an ‘‘alternating linear time’’ hierarchy and for all k , $\Sigma_k^D \subseteq \Sigma_k^P$ and $\Pi_k^D \subseteq \Pi_k^P$ (Σ_k^P and Π_k^P are the corresponding levels of the polynomial hierarchy.) Many of the basic properties of the \mathcal{A}_0^N hierarchy are unresolved. Resolution of these properties would have important consequences in number theory as well as complexity theory. This hierarchy has been studied by Dimitracopoulos and Paris (1979). In Paris and Dimitracopoulos (1979) they show that settling the question of whether the \mathcal{A}_0^N hierarchy collapses is equivalent to answering certain definability questions concerning nonstandard models of Peano arithmetic. Similar results are shown there for the polynomial-time hierarchy. These two hierarchies are closely related and the model theory of these hierarchies has significant consequences for complexity theory.

THE MAIN THEOREM

Our main interest here is the logical strength of the various open problems of complexity theory. Putting these problems in a logical setting enables one to bring to bear several different approaches and additional methods. It may be possible to achieve a new measure of the difficulty of these problems in terms of the complexity of corresponding logical statements. It opens the possibility that other concepts and methods from logic can be applied to these complexity-theoretic problems. Even considerations as to the independence of these problems may be explored.

We study here the strengths of the theory $T(R, F)$. The theorem in this section relates the question of whether a recursive set S belongs to the class R to the provability of a sentence θ^S from the theory $T(R, F)$. Our goal is to relate the strength of the theories $T(R, F)$ (for various R and F) to open problems in complexity theory and to this end R and F will be defined in terms of complexity classes. We will get such results as corollaries to the next theorem. Our theorem is a generalization of the main result of DeMillo and Lipton (1979) and follows from the general method used there. We have recast this proof into the general setting described above. This enables us to use the theorem in the next section to prove a number of corollaries. Previously only the connections to the $P = ?NP$ problem was considered and the question arose in DeMillo and Lipton (1979) as to whether these methods applied to other problems as well.

Let S be a recursive set such that for some predicate symbols ϕ, ψ in $L(R, F)$ we have

$$x \in S \leftrightarrow N \models \exists y \phi(x, y)$$

$$x \notin S \leftrightarrow N \models \exists y \psi(x, y).$$

Given the above, define $\theta_{\phi, \psi}^S = \forall x \exists y (\phi(x, y) \vee \psi(x, y))$. Our theorem now allows us to characterize recursive elements of R in terms of the strength of the theory $T(R, F)$.

THEOREM. *For any recursive set S , $S \in R \leftrightarrow T(R, F) \vdash \theta_{\phi, \psi}^S$ for some ϕ, ψ as above.*

To prove the theorem we will need

LEMMA. *If $M \models T(R, F)$ and M' is a submodel of M then $M' \models T(R, F)$.*

Proof of Lemma. Let $\exists x \forall y \theta(x, y)$ be an element of $T(R, F)$, so $N \models \exists x \forall y \theta(x, y)$. Hence for some $k \in N$, $N \models \forall y \theta(\bar{k}, y)$. (Here \bar{k} is the numeral representing k in the language of $T(R, F)$.) As $M \models T(R, F)$, $M \models \forall y \theta(\bar{k}, y)$ and so $M' \models \forall y \theta(\bar{k}, y)$, since M' is a submodel of M and the formula is universal. Hence we have $M' \models \exists x \forall y \theta(x, y)$ as desired. ■

Proof of Theorem. (\Rightarrow) If $S \in R$, as R is closed under complement, $x \in S \leftrightarrow \phi(x)$ and $x \notin S \leftrightarrow \psi(x)$ for some predicates ϕ, ψ representing elements of R . Then $N \models \forall x (\phi(x) \vee \psi(x))$ so this formula is an axiom of $T(R, F)$ and so $\vdash \forall x \exists y (\phi(x) \vee \psi(x))$.

(\Leftarrow) Assume $T(R, F) \vdash \forall x \exists y (\phi(x, y) \vee \psi(x, y))$. Let t_1, t_2, t_3, \dots be an enumeration of the terms of $L(R, F)$ which have at most one free variable.

The next claim is an essential application of the compactness theorem. It tells us that the “witnesses” y for the formula $\phi(x, y) \vee \psi(x, y)$ can be bounded for all x by a fixed integer n . This fact is a consequence of the simple nature of the theory $T(R, F)$.

CLAIM. *There exists an n , dependent on ϕ and ψ , such that*

$$N \models \forall x \bigvee_{i=1}^n (\phi(x, t_i(x)) \vee \psi(x, t_i(x))).$$

Proof of Claim. Let T' be the theory

$$T(R, F) \cup \{ \neg (\phi(c, t_i(c)) \vee \psi(c, t_i(c))) \}_{i=1,2,3,\dots}$$

with c a new constant symbol not in $L(R, F)$. Assume the claim is false. Then T' is consistent, since otherwise, by the compactness theorem,

$$T(R, F) \cup \{\neg(\phi(c, t_i(c)) \vee \psi(c, t_i(c)))\}_{i=1,2,\dots,n}$$

for some fixed n , yields a contradiction. So we would have

$$T(R, F) \vdash \forall x \bigvee_{i=1}^n (\phi(x, t_i(x)) \vee \psi(x, t_i(x)))$$

contrary to the assumption.

Let $M \models T'$ and let M_c be the submodel of M generated by c . By the Lemma $M_c \models T(R, F)$. Hence as $T(R, F) \vdash \forall x \exists y (\phi(x, y) \vee \psi(x, y))$ we have $M_c \models \exists y (\phi(c, y) \vee \psi(c, y))$. But by the definition of T' , $M \models \forall y \neg (\phi(c, y) \vee \psi(c, y))$ and hence $M_c \models \forall y \neg (\phi(c, y) \vee \psi(c, y))$. This contradiction proves the claim.

Now by the claim we have

$$T(R, F) \vdash \forall x \bigvee_{i=1}^n (\phi(x, t_i(x)) \vee \psi(x, t_i(x)))$$

and so

$$x \in S \leftrightarrow \bigvee_{i=1}^n \phi(x, t_i(x)).$$

Hence $S \in R$ since R is closed under finite union and F -substitution. ■

APPLICATIONS OF THE MAIN THEOREM

The main theorem can now be directly applied to get results for a number of subrecursive hierarchies of interest in complexity theory and logic. We first consider applications to the polynomial-time hierarchy as this hierarchy was the original motivation for looking at these theories. These corollaries characterize sets in various levels of the hierarchy in terms of the strength of theories gotten from these same classes together with polynomial-time functions. When applied to complete sets for these classes the correspondence is to the collapse of the hierarchy at particular levels. The first corollary is essentially the main result in DeMillo and Lipton (1979). As usual let Σ_k^P , Π_k^P denote the k th levels of the polynomial-time hierarchy.

COROLLARY 1. *For any recursive set S ,*

$$S \in P \text{ iff } T(P, P^F) \vdash \theta_{\phi, \psi}^S \quad \text{for some } \phi, \psi \text{ in our language.}$$

Proof. This is just a restatement of the main theorem in this setting. Note that using the same theory we can characterize the $P = NP$ problem by the following: For any NP -complete set S ,

$$P = NP \text{ iff } T(P, P^F) \vdash \theta_{\phi, \psi}^S \quad \text{for some } \phi, \psi.$$

These same results are generalized to other levels of the polynomial hierarchy by the following corollaries:

COROLLARY 2. For any recursive S , any $k \geq 1$,

$$S \in \Sigma_k^P \cap \Pi_k^P \leftrightarrow T(\Sigma_k^P \cap \Pi_k^P, P^F) \vdash \theta_{\phi, \psi}^S \quad \text{for some } \phi, \psi.$$

Thus, for $k \geq 1$, if S is Σ_k^P -complete then

$$\Sigma_k^P = \Pi_k^P \leftrightarrow T(\Sigma_k^P \cap \Pi_k^P, P^F) \vdash \theta_{\phi, \psi}^S \quad \text{for some } \phi, \psi.$$

Proof. $\Sigma_k^P = \Pi_k^P \leftrightarrow S \in \Pi_k^P \leftrightarrow S \in \Sigma_k^P \cap \Pi_k^P$.

Remark. Note that Kleene's T -predicate (Rogers, 1967) is easily seen to be in P . Hence by Kleene's normal form theorem for recursively enumerable sets, any recursive set S has the property that

$$x \in S \leftrightarrow N \models \exists y \phi(x, y)$$

$$x \notin S \leftrightarrow N \models \exists y \psi(x, y)$$

where ϕ and ψ are predicate symbols representing polynomial time predicates. Hence for any recursive S not in $\Sigma_k^P \cap \Pi_k^P$ we have

$$T(\Sigma_k^P \cap \Pi_k^P, \text{polynomial-time functions}) \not\vdash \theta_{\phi, \psi}^S.$$

In this respect the theories we are considering are quite weak.

Similarly for PSPACE we have,

COROLLARY 3. For any S which is PSPACE-complete,

$$P = PSPACE \leftrightarrow T(P, P^F) \vdash \theta_{\phi, \psi}^S \quad \text{for some } \phi, \psi.$$

Analogous corollaries can be drawn concerning the Δ_0^N hierarchy. This hierarchy is a natural recursion-theoretic hierarchy based on linear-time sets. It has been studied by Wrathall (1978) and Paris and Dimitracopoulos (1979) among others and has applications in many areas of logic and computer science including nonstandard models of arithmetic. A corollary which follows immediately from the main theorem is

COROLLARY 4. For any $S \in \Delta_0^N$ and $k \geq 1$,

$$S \in \Sigma_k^D \cap \Pi_k^D \leftrightarrow T(\Sigma_k^D \cap \Pi_k^D, \Delta_0^D - \text{computable functions}) \vdash \theta_{\phi, \psi}^S \text{ for some } \phi, \psi.$$

The Δ_0^N hierarchy admits a natural reducibility similar to polynomial reducibility in some respects. For any sets A and B we say $A \leq_{\Delta} B$ if there is a function f Σ_0^D -definable over N such that, $x \in A \leftrightarrow f(x) \in B$. This definition satisfies the usual properties of a reducibility (e.g., it is transitive). Any two Σ_0^D sets (except the empty set and N) are \leq_{Δ} equivalent. A set C is Σ_k^D -complete if

- (i) $C \in \Sigma_k^D$
- (ii) $\forall D \in \Sigma_k^D, D \leq_{\Delta} C$.

Σ_k^D -complete sets can be manufactured in the usual way. For example, $\{\langle \lceil \phi_i \rceil, x \rangle \mid N \models \exists y < x \phi_i(x, y)\}$ is Σ_1^D -complete, where ϕ_i is the i th Σ_0^D formula and $\lceil \phi_i \rceil$ is a Gödel number of ϕ_i in any standard Gödel numbering. We have, from the main theorem,

COROLLARY 5. Let S be Σ_k^D -complete. Then

$$\Sigma_k^D = \Pi_k^D \text{ iff } T(\Sigma_k^D \cap \Pi_k^D, \Sigma_0^D \text{ functions}) \vdash \theta_{\phi, \psi}^S \text{ for some } \phi, \psi.$$

Finally, a number of consequences can be drawn concerning provable properties of total functions. Provably total functions have played a central role in recent independence results in logic. The well-known independence theorem of Harrington and Paris (1978) can be recast and understood in terms of the provable totality of particular classes of functions. Generally, the functions provably total in a theory form a natural class and indicate the strength of the theory. We give results here for a hierarchy of functions derived from the polynomial hierarchy. Similar results can be gotten for other subrecursive hierarchies (i.e., Δ_0^N) whenever the main result applies.

DEFINITION. A function $f \in \Sigma_k^F(\Pi_k^F)$ iff f is total and graph $(f) \in \Sigma_k^P(\Pi_k^P)$.

Note. This definition gives a nonstandard notion of a function being in $P = \Sigma_0^P$. To be precise, any function computable in polynomial time (in the usual sense) is in Σ_0^F . However, the converse is not in general true. Consider for example the function $f(x) = 2^x$. This function is in Σ_0^F but not in P . On the other hand it is true that for 0–1 valued (or finite valued) functions that if the function is in Σ_0^F then it is computable in polynomial time.

The following proposition says that the classes Σ_k^F and $\Sigma_k^F \cap \Pi_k^F$ coincide.

It does not imply that this function hierarchy collapses, only that at each level the Σ and Π classes coincide.

PROPOSITION. *If $k \geq 1$ and $f \in \Sigma_k^F$ then $f \in \Pi_k^F$.*

Proof. Let $f \in \Sigma_k^F$. So

$$f(x) = y \leftrightarrow \exists z(|z| \leq |\langle x, y \rangle| \wedge Q(x, y, z)) \quad \text{with } Q \in \Pi_{k-1}^P.$$

Now since f is a total function we have

$$f(x) = y \leftrightarrow \forall z, z'(|z| \leq |\langle x, y \rangle| \wedge |z'| \leq |\langle x, y \rangle| \wedge Q(x, z', z) \rightarrow z' = y)$$

This formula is Π_k^P and so $f \in \Pi_k^F$.

COROLLARY 7. *Let f be a total recursive function and $k \geq 1$. Then $f \in \Sigma_k^F \leftrightarrow T(\Sigma_k^P \cap \Pi_k^P, P^F) \vdash \theta_{\phi, \psi}^f$, where $\theta_{\phi, \psi}^f$ is defined by*

$$f(x) = y \leftrightarrow \exists z \phi(x, y, z),$$

$$f(x) \neq y \leftrightarrow \exists z \psi(x, y, z),$$

and

$$\theta_{\phi, \psi}^f = \forall x, y \exists z (\phi(x, y, z) \vee \psi(x, y, z)).$$

Proof. The main theorem immediately gives that

$$f \in \Sigma_k^F \cap \Pi_k^F \leftrightarrow T(\Sigma_k^P \cap \Pi_k^P, P^F) \vdash \theta_{\phi, \psi}^f.$$

Hence the corollary follows from the proposition.

Note. The right-hand side of Corollary 7 essentially says that the function f is provably total. In Harrington and Paris (1978) and Paris (1978) it is shown that a certain function generated by a Ramsey-type partition relation on the integers is not provably total in Peano arithmetic. Corollary 7 above is a much simpler result which characterizes functions being provably total with respect to the weaker theories $T(\Sigma_k^P \cap \Pi_k^P, P^F)$. At present there is no known method to show that such simple, slow, growing functions are not provably total from Peano arithmetic.

CONCLUSIONS

This paper shows that for many subrecursive hierarchies there are theories whose strengths correspond to the various levels of these hierarchies. The results give an exact correspondence between lower bound

proofs and independence of particular true sentences from the fragments of arithmetic herein considered. They suggest several different directions for further research.

The model theory of Peano arithmetic, though far from being completely understood, has been an active area of mathematical logic in recent years. The results of this paper suggest that studying the model theory of weaker arithmetical theories might yield results in complexity theory. In particular, a study of the theory of true Σ_2 statements of arithmetic is of interest as many of the theories considered in the paper are theories of this strength.

Another task which could be undertaken is to try to extend the results of this paper to stronger theories. Some different theories have previously been considered by DeMillo and Lipton (1980).

One weakness of most of the work to date is that the theories discussed are not natural. It would be of interest to see similar results proved for more commonly considered theories. The eventual hope is that independent results could be shown for Peano arithmetic, or at least a large fragment of PA. While this goal is very far off, a significant connection between subrecursive hierarchies and non-standard models of PA has been found by Paris and Dimitracopoulos (1979) and by Buss (1985). Eventually results like those considered here might be achieved for fragments of Peano arithmetic using techniques developed in Paris and Dimitracopoulos (1979).

RECEIVED: April 22, 1983; REVISED: March 20, 1984

REFERENCES

- BUSS, S. R. (1985), The polynomial hierarchy and fragments of bounded arithmetic, in "Proc. 17th ACM Sympos. on Theory of Computing," pp. 285–290.
- DEMILLO, R. A., AND LIPTON, R. J. (1979), Some connections between mathematical logic and complexity theory, in "Proc. of the 11th Sympos. on the Theory of Computation."
- DEMILLO, R. A., AND LIPTON, R. J. (1980), The consistency of " $P=NP$ " and related problems with fragments of number theory, in "12th Sympos. on Theory of Computing," April.
- HARRINGTON, L., AND PARIS, J. (1978), A mathematical incompleteness in Peano arithmetic, in "Handbook of Mathematical Logic" (Barwise, Ed.), North-Holland, Amsterdam.
- HARTMANIS, J., AND HOPCROFT, J. E. (1976), Independence results in computer science, *SIGACT News* 8, No. 4.
- JOSEPH, D. (1983), Polynomial time computations in models of ET, *J. Comput. System Sci.* 26, 311–338.
- JOSEPH, D., AND YOUNG, P. (1980), Independence results in computer science, in "12th Sympos. on Theory of Computing," April.
- KIRBY, L., AND PARIS, J. (1976), Initial segments of models of Peano's axioms, in "Proceedings, Conf. Set Theory and Hierarchy Theory V," Lecture Notes in Math. Vol. 619, Springer-Verlag, New York/Berlin.
- LEIVANT, D. (1982), Unprovability of theorems of complexity theory in weak number theories, *Theoret. Comput. Sci.* 18, 259–268.

- LIPTON, R. J. (1978), Model theoretic aspects of complexity theory, in "Proceedings, 19th IEEE, Found. of Comput. Sci."
- O'DONNELL, M. (1979), A programming language theorem which is independent of Peano arithmetic, in "Proc. of the 11th Sympos. on the Theory of Computation."
- PARIS, J. B. (1978), Some independence results for Peano arithmetic, *J. Symbolic Logic* 43.
- PARIS, J. B., AND DIMITRACOPOULOS, C. (1979), Truth definitions for Δ_0 formulas, logic, and algorithmic, *Enseign. Math.* 30.
- ROGERS, H. (1967), "The Theory of Recursive Functions and Effective Computability," McGraw-Hill, New York.
- STOCKMEYER, L. J. (1976), The polynomial-time hierarchy, *Theoret. Comput. Sci.* 3.
- WRATHALL, C. (1978), Rudimentary predicates and relative computation, *SIAM J. Comput.* 7, No 2.