Proceedings of the International Congress of Mathematicians
Vancouver, 1974

The Inherent Computational Complexity of Theories of Ordered Sets*

Albert R. Meyer

The significance of the theoretical distinctions between problems which are effectively decidable and those which are not can be challenged by objections of at least two kinds:

(1) Only a *finite* collection of sentences about arithmetic, for example, are of human concern, so the undecidability of the infinite collection of true sentences of arithmetic is immaterial.

(2) An *efficient* decision procedure for the monadic predicate calculus, for example, would have important practical applications, but the mere fact that it is effectively decidable is immaterial.

We first consider the second objection. Clearly more time and effort are required to prove the truth or validity of long sentences simply because it may require a long time to read them. The "efficiency" of a decision procedure must thus be measured relative to the size of the sentences to which the procedure is applied. A hint that many decision problems in logic cannot have efficient decision procedures follows from the observation that short sentences can define relatively large sets.

For example, consider the pure predicate calculus with monadic (i.e., one argument) predicate letters $P_1, P_2, \cdots, P_n$. If we choose some interpretation of $P_1, P_2, \cdots, P_n$ as predicates on some domain, then any element x in the domain can be identified with the vector of truth-values $\langle P_1(x), P_2(x), \cdots, P_n(x)\rangle$. Then the formula

$$D_i(x, y) := (P_i(x) \equiv \neg P_i(y)) \wedge \bigwedge_{j\neq i} (P_j(x) \equiv P_j(y))$$

means that x and y differ precisely in their ith component. Hence, the sentence

*This research was supported by the National Science Foundation under research grant GJ-43634X.

$$S := \forall x\left(\bigwedge_{i=1}^{n} \exists y D_i(x, y)\right)$$

means that for every vector x and every component of x, there is another vector y which differs from x precisely at that component. Clearly S is satisfied only by interpretations in which each of the 2^n vectors occurs in the domain. Notice, however, that S, even with the abbreviated conjunctions fully expanded, contains only proportional to n^2 connectives and is of length proportional to $n^2 \cdot \log n$. (By the length of S we mean the number of occurrences of all symbols including connectives, variables, predicate letters and parentheses. The factor $\log n$ appears because the alphabet of symbols is assumed to be fixed and $n \cdot \log n$ subscript digits are then required to represent the n distinct predicate letters $P_1, \cdots, P_n$.)

The following theorem implies that any decision procedure for satisfiability of sentences of monadic predicate calculus with n predicate letters requires essentially the same effort as exhaustively testing all possible interpretations on domains of size up to 2^n. (The usual proofs of the decidability of monadic predicate calculus imply that testing domains up to this size is sufficient.)

THEOREM (MEYER [MR75]). *Any Turing machine which, given any sentence of monadic predicate calculus, decides whether the sentence is satisfiable, requires a number of steps exceeding* $2^{\varepsilon \cdot \text{length}(S)/\log(\text{length}(S))}$ *for some* $\varepsilon > 0$ *and infinitely many sentences* S.

It should be apparent that if a Turing machine requires an exponentially growing number of steps, then so will any other reasonable model of a computer. Moreover, the lower bound of the theorem applies even to nondeterministic Turing machines, which implies that the shortest *proofs* of satisfiability or validity of such sentences will also be exponential (cf. [FR74] for further discussion of proof-length).

The preceding theorem and others to follow can in retrospect be seen as a natural extension of Gödel's first incompleteness theorem and Turing's and Church's proofs of undecidability: One "arithmetizes" or codes the computations of Turing machines into a domain and constructs sentences which assert that the coded computation halts in an accepting state. The technical flavor of the proofs differs from undecidability proofs in that emphasis rests on efficiently (relative to the size of the Turing machine) constructing short sentences which describe computations which eventually halt after a long time. We shall not attempt to describe the proofs further.

The first proof that a decidable theory, namely the weak monadic second-order theory of the successor function on the nonnegative integers (WS1S), was discovered in May, 1972 [Me72], [Me73]. Since then reasonably close upper and lower bounds on the inherent computational complexity of most of the classical examples of decidable theories have been obtained.

THEOREM. *Any Turing machine which decides membership in the set* $\mathscr{A}$ *requires a number of steps exceeding*

$$\left.2^{2^{\cdot^{\cdot^{2^{\text{length}(S)}}}}}\right\} \varepsilon \cdot \log(\text{length}(S))$$

for some $\varepsilon > 0$ *and infinitely many* $S \in \mathscr{A}$, *where* $\mathscr{A}$ *is any of the following*:

1. *WS1S* (*Meyer* [**Me73**]),
2. *star-free expressions (from automata theory) for the empty set* (*Stockmeyer* [**St74**], [**SM75**]),
3. *the theory of linear orders* (*Meyer* [**St74**], [**SM75**]),
4. *the theory of any nonempty family of infinite linear orders with a single monadic predicate* (*Stockmeyer* [**St74**], [**SM75**]),
5. *the theory of two successors and prefix* (*Meyer and Stockmeyer* [**St74**], [**SM75**]),
6. *the theory of a single unary function* (*M. Fischer and Meyer* [**FM75**]),
7. *the theory of pure finite types* (*M. Fischer and Meyer* [**FM75**]),
8. *the theory of addition on the nonnegative integers with the predicate "x is a power of* 2 *and x divides y"* (*Meyer* [**Me73**]),
9. *the theory of any nonempty family of pairing functions* (*Rackoff* [**Rac74b**]).

For each of these examples, decision procedures are known which require at most

$$\left.2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}\right\} n$$

Turing machine steps on inputs of length n. It is a curious empirical observation that all natural decision problems known to be decidable require at most this many steps. (Of course it is not hard to contrive examples of decidable theories which are not even primitive recursive (cf. [**Rac74b**]).)

An exponential lower bound for the computational complexity of the theory of essentially any algebraic structure follows from the following theorem. A family of semigroups is of *unbounded order* if for every $k > 0$ there is a semigroup in the family and an element s in the semigroup such that $s^i \neq s^j$ for all $1 \leqq i < j \leqq k$.

THEOREM (M. FISCHER [**FR74**]). *The first order theory of any family of semigroups of unbounded order requires time* $2^{\varepsilon \cdot \mathrm{length}(S)}$.

An immediate corollary is that exponentially many steps are required to decide sentences in the theory of the real numbers under addition, and, a fortiori, efficient implementations of Tarski's celebrated decision procedure for the real field do not exist. Decision procedures for sentences of length n in the first order theory of the real field which require at most $2^{2^{kn}}$ steps for some constant k have recently been announced by Collins [**Co174**] and independently by Monk [**Mo74**]and Solovay [**So74**].

The decision problem for Presburger's arithmetic (i.e., the first order theory of addition of integers) which admits a very simple proof of decidability compared to real closed fields is computationally more difficult.

THEOREM (M. FISCHER-RABIN [**FR74**]). *Presburger's arithmetic requires time* $2^{2^{\varepsilon \cdot \mathrm{length}(S)}}$

THEOREM (OPPEN [**Op73**], FERRANTE-RACKOFF [**FeRa75**], [**Rac74**]). *Moreover time* $2^{2^{\varepsilon \cdot \mathrm{length}(S)}}$ *is sufficient.*

Fischer-Rabin [**FR74**] also have shown that *three* exponentials of steps are required to decide the theory of multiplication of positive integers, and Rackoff **[Rac74a, b]** has developed a general theorem relating the complexity of theories of structures to theories of powers of structures (the positive integers under multiplication being the weak direct power of the nonnegative integers under addition) which yields an upper bound of *four* exponentials for the theory of integer multiplication.

We note that since the lower bounds apply to nondeterministic as well as deterministic Turing machines, while the upper bounds are always deterministic, upper and lower bounds which differ by only one exponential are well matched (cf. **[St74]** for further explanation of this remark).

Apparently similar theories may have quite different complexities.

THEOREM (FERRANTE **[Fe74]**). *The first order theory of $\mathscr{B}$ requires for sentences of length n time L(n) and can be decided in time U(n) where*

$\mathscr{B} =$	$L =$	$U =$
1. *Integers with successor*	?	$2^{\varepsilon \cdot n}$
2. *Integers with order*	?	$2^{\varepsilon \cdot n}$
3. *Integers with successor and a single monadic predicate*	$2^{2^{\varepsilon \cdot n}}$	$2^{2^{2^{\varepsilon \cdot n}}}$
4. *Integers with order and a single monadic predicate*	$\left.2^{2^{\cdot^{\cdot^{2}}}}\right\}\varepsilon \cdot n$	$\left.2^{2^{\cdot^{\cdot^{2}}}}\right\}n$

(The lower bound in the last line follows from the result of Stockmeyer cited earlier, and the upper bound is implicit in the decision procedures of Büchi-Elgot **[Bu60]**, **[El61]** and Rabin **[Rab69]**.)

Thus the second objection raised in the first paragraph seems cogent. Mere decidability of a problem cannot be taken even to suggest that the problem admits feasible, practical decision procedures. Indeed nearly all the known decidability results of logic are inherently impractical in that exponential or more time is required by any possible decision procedure. (A notable exception is the decision problem for the propositional calculus. No subexponential time procedure is known, but neither have any nontrivial lower bounds been proved. We regard the determination of the computational complexity of the decision problem for the propositional calculus as the most important open problem in the theory of computation. Cook **[Coo71]** and Karp **[Ka72]** show that dozens of classical problems of combinatorial optimization are computationally equivalent to the decision problem for the propositional calculus.)

To the first objection, however, the proofs of the above theorems as well as classical undecidability theorems provide an implicit answer; the theorems about infinite problems often contain information from which one can estimate the difficulty of finite problems.

Consider Boolean functions of *n* variables and programs (or logical networks) which compute them by successively applying binary Boolean operations to the variables and to previously computed results. For example, the sequence of operations

$$\begin{array}{ll} a_1 := x_1 \wedge x_2, & a_4 := a_1 \vee a_2, \\ a_2 := x_1 \wedge x_3, & a_5 := a_4 \vee a_3, \\ a_3 := x_2 \wedge x_3, & a_6 := \neg(a_1 \wedge x_3), \end{array}$$
$$a_7 := a_6 \wedge a_5,$$

comprises a program for the function

$$f(x_1, x_2, x_3) = [(x_1 \wedge x_2) \vee (x_1 \wedge x_3) \vee (x_2 \wedge x_3)] \wedge \neg(x_1 \wedge x_2 \wedge x_3).$$

Thus $f(x_1, x_2, x_3) = 1$ if and only if exactly two of the zero-one valued variables x_1, x_2, x_3 have the value one.

We choose sentences of length n in some formal theory and code the symbols in these sentences as binary sequences. In the particular example below, six binary digits are sufficient to code all the symbols required, so sentences of length n correspond to binary sequences of length $6n$. We then inquire about the minimum number of binary operations required in a network computing the function of $6n$ variables which equals one if and only if its $6n$ inputs are the code of a well-formed true sentence.

The previous proofs show that short sentences can describe large networks as well as large Turing machine computations, and from this one can deduce that the size of networks which decide sentences of length n must grow exponentially with n. (This was first proved in 1967 by Ehrenfeucht [Eh72] for the sentences of "bounded arithmetic" with explicit use of constants in exponential notation, e.g., 3^{29^7}, allowed in the sentences.) In particular,

THEOREM (STOCKMEYER-MEYER [St74], [SM75]). *If we choose sentences of length* 616 *in the decidable theory of WS1S and code these sentences into* $6 \times 616 = 3696$ *binary digits, then any logical network with* 3696 *inputs which decides truth of these sentences contains at least* 10^{123} *operations.*

We remind the reader that the radius of a proton is approximately 10^{-13} cm, and the radius of the known universe is approximately 10^{28} cm. Thus for sentences of length 616, a network whose atomic operations were performed by transistors the size of a proton connected by infinitely thin wires would densely fill the entire universe.

References

[Bu60] J. R. Büchi, *Weak second-order arithmetic and finite automata*, Z. Math. Logik Grundlagen Math. **6** (1960), 66–92. MR **23** #A2317.

[Col74] G. E. Collins, *Quantifier eliminations for real closed fields by cylindrical algebraic decomposition*, preliminary report, Proc. EUROSAM 74, ACM SIGSAM Bull. **8** (1974), 80–90.

[Coo71] S. A. Cook, *The complexity of theorem proving procedures*, Proc. Third ACM Sympos. on Theory of Computing, 1971, pp. 151–158.

[Eh72] A. Ehrenfeucht, *Practical decidability*, Report CU-CS-008-72. Dept. of Computer Science, Univ. of Colorado, 1972.

[El61] C. C. Elgot, *Decision problems of finite automata design and related arithmetics*, Trans. Amer. Math. Soc. **98** (1961), 21–51. MR **25** #2962.

[Fe74] J. Ferrante, *Some upper and lower bounds on decision procedures in logic*, Doctoral Thesis, Dept. of Mathematics, M. I. T., Cambridge, Mass., 1974.

[FeRa73] J. Ferrante and C. Rackoff, *A decision procedure for the first order theory of real addition with order*, SIAM J. Computing **4** (1975), 69–76.

[FM75] M. J. Fischer and A. R. Meyer, (1975) (in preparation).

[FR74] M. J. Fischer and M. O. Rabin, *Super-exponential complexity of Presburger arithmetic*, Complexity of Computation, edited by R. Karp, SIAM-AMS Proc., vol. **7**, Amer. Math. Soc. (1974), 27–41.

[Ka72] R. M. Karp, *Reducibility among combinatorial problems*, Complexity of Computer Computations, edited by R. E. Miller and J. W. Thatcher, Plenum Press, New York, 1972, pp. 85–104.

[Me72] A. R. Meyer, *Weak* S1S *cannot be decided*, Notices Amer. Math. Soc. **19** (1972), A-598. Abstract #72T-E67.

[Me73] ———, *Weak monadic second order theory of successor is not elementary-recursive*, Boston Univ. Logic Colloq. Proc. 1975 (to appear); also: Project MAC Technical Memo 38, M.I.T., Cambridge, Mass., 1973.

[MR75] A. R. Meyer and C. Rackoff, (1975) (in preparation).

[Mo74] L. Monk, *An elementary-recursive decision procecure for* $TH(R, +, \cdot)$, Dept. of Math., Univ. of California, 1974 (manuscript).

[Op73] D. C. Oppen, *Elementary bounds for Presburger arithmetic*, Proc. Fifth ACM Sympos. on Theory of Computing, Austin, Texas, 1973, pp. 34–37.

[Rab69] M. O. Rabin, *Decidability of second-order theories and automata on infinite trees*, Trans. Amer. Math. Soc. **141** (1969), 1–35. MR **40** #30.

[Rac74a] C. Rackoff, *On the complexity of the theories of weak direct products*, Project MAC Technical Memo 42, M.I.T., Cambridge, Mass., 1974; J. Symbolic. Logic (to appear).

[Rac74b] ———, *Complexity of some logical theories*, Doctoral Thesis, Dept. of Electrical Engineering, M.I.T., Cambridge, Mass., 1974.

[So74] R. Solovay, Correspondence with A. R. Meyer, September 1974.

[St74] L. J. Stockmeyer, *The complexity of decision problems in automata theory and logic*, Doctoral Thesis, Dept. of Electrical Engineering, M.I.T., Cambridge, Mass., 1974; Project MAC Technical Report 133, M.I.T., Cambridge, Mass., 1974.

[SM75] L. J. Stockmeyer and A. R. Meyer, *Inherent computational complexity of decision problems in logic and automata theory*, Lecture Notes in Comp. Sci., Springer-Verlag, 1975 (to appear).

M. I. T. PROJECT MAC
CAMBRIDGE, MASSACHUSETTS 02139, U.S.A.