Department of Computer Science Technical Reports

Department of Computer Science

1967

Definability in the Monadic Second-Order Theory of Successor

J. Richard Buchi

Lawrence H. Landweber

Report Number:
67-015

Definability in the Monadic Second-Order Theory of Successor

J. Richard Büchi and Lawrence H. Landweber

September 1967

CSD TR 15

DEFINABILITY IN THE MONADIC SECOND-ORDER THEORY OF SUCCESSOR*

By J. Richard Büchi and Lawrence H. Landweber**
Purdue University, Lafayette, Indiana

1. INTRODUCTION. Let $\underline{D} = \langle D, P_1, P_2, \ldots \rangle$ be a relational system whereby D is a non-empty set and P_i is an m_i-ary relation on D. With $\underline{D}$ we associate the (weak) monadic second-order theory (W)MT[$\underline{D}$] consisting of: the first-order predicate calculus with individual variables ranging over D; monadic predicate variables ranging over (finite) subsets of D; predicate quantifiers; and constants corresponding to $P_1, P_2, \ldots$. We will often use (W)MT[$\underline{D}$] ambiguously to mean also the set of true sentences of (W)MT[$\underline{D}$].

In this note we study variants of the structure $\langle N, ' \rangle$ where N is the set of natural numbers and ' is the successor function on N. Our results are a consequence of McNaughton's [7] work on the ω-behavior of finite automata and the decision procedure for MT [N,'] given in [1]. The former is essential as we have been unable to obtain proofs which utilize only [1]'s characterization of ω-behavior. In [2] we discuss related results.

Section 2 studies definability in MT[N,']. For every formula C(X) of MT[N,'] where X is a vector of unary predicate variables,

*This research was supported by the National Science Foundation (Contract 4730-50-595).

**Presently at the University of Wisconsin, Madison, Wisconsin.

the relation $C(X)$ is arithmetic and, in fact, is in the Boolean algebra over Π_2. In section 3, we investigate the existence of decision procedures for (W)MT[N,',Q] where Q is a subset of N. Such theories were previously studied by Elgot and Rabin [4]. For any recursive Q, the decision problem for MT[N,',Q] is in $\Sigma_3 \cap \Pi_3$. We also define a recursive Q for which (W)MT[N,',Q] is undecidable. This provides a rather natural example of an undecidable theory which is still arithmetic.

2. DEFINABILITY IN MT[N,'].

In this section we study definability in MT[N,'] with respect to the arithmetic and classical Borel hierarchies. In particular we are interested in those relations definable by formulas $C(X)$, X a vector of free set variables, of MT[N,']. The main result is that every such relation is in the Boolean algebra over Π_2 (G_δ) of the arithmetic (Borel) hierarchy where Π_0 (G) are the recursive (open) sets and $C(X) \in \Pi_2$ (G_δ) if it is representable as $(\forall x)(\exists y)M(x,y,X)$, M recursive (a denumerable intersection of open sets). In fact Lemma 1 below also gives this result for a wider class of $C(X)$ than are definable in MT[N,']. In the following $x,y,z,\ldots$ are individual variables ranging over N.

A recursive operator (RO) $Z = A(X)$ is an operator mapping ω-sequences over a finite set I into ω-sequences over a finite set S which can be presented in the form

(1) $$Zt = \Phi(\overline{X}\ \phi(t))$$

whereby $\overline{X}t = X0,..,Xt$ and Φ and ϕ are recursive functions from I^* into S and N into N respectively. Sup Z is the set of members of S appearing infinitely often in the ω-sequence $Z = Z0, Z1, \ldots$.

LEMMA 1. Let $Z = \Lambda(X)$ be a RO and $U \subseteq 2^S$. Then the relation $F(X)$ given by

(2) $$(\exists Z)\ [Z=\Lambda(X) \wedge \sup Z \in U]$$

is in the Boolean algebra over Π_2 of the arithmetic hierarchy.

PROOF. $F(X)$ can be written as

$$\bigvee_{B\in U} . (\exists x)(\forall y)[y \geq x \supset \Phi(\overline{X}\phi(y)) \in B] \wedge \bigwedge_{s\in B} (\forall x)(\exists y)[y \geq x \wedge \Phi(\overline{X}\phi(y)) = s]$$

The relations given by $[y \geq x \wedge \Phi(\overline{X}\phi(y))=s]$ and $[y \geq x \supset \Phi(\overline{X}\phi(y)) \in B]$ are recursive because Φ and ϕ are recursive. Hence $F(X)$ is a Boolean combination of formulas of the form $(\forall y)(\exists x)\ M(X,x,y)$ where M is recursive so $F(X)$ is in the Boolean algebra over Π_2. Q.E.D.

A finite automata operator (FAO) is a RO $Z = \Lambda(X)$ which can be presented in the form

$$Z0 = c$$
(3)
$$Zt' = H[Xt,Zt]$$

whereby $H: I\times S \to S$ and $c \in S$. Let $C(X)$ be a formula of $MT[N,']$ where X is an n-tuple of free set variables. The main definability results of [1] and [7] (see [2] for more details) state that from C we can effectively construct a presentation of a FAO $Z=E(X)$ as in (3) (i.e., obtain H, S, and c) and a $U \subseteq 2^S$ such that

$$C(X) \;.\equiv.\; (\exists Z)\ [Z=E(X) \wedge \sup Z \in U]$$

whereby $I = \{T,F\}^n$. Hence by Lemma 1 we have

Theorem 1. Every relation between subsets of N which is definable in $MT[N,']$ is arithmetical, and in fact occurs in the Boolean algebra over Π_2. Furthermore, given a formula $C(X_1,\ldots,X_n)$ of $MT[N,']$ one can construct an index of the relation C in the Boolean algebra over Π_2.

In contrast, all relations $R(y_1,\ldots,y_m,X_1,\ldots,X_n)$ appearing in the function-quantifier hierarchy over recursive relations are definable in $MT[N,',2x]$ (see [8]).

We can also consider $C(X)$ as defining a subset of the Cantor space of ω-sequences over I, namely the set of ω-sequences over I which satisfy C. The open and closed sets of the usual totally disconnected topology on this space are of the form $U_{w_1} \cup \cdots \cup U_{w_n}$ whereby $w_i \in I^*$ = all words over I and $U_w = \{X | (\exists t)[\overline{X}t = w]\}$. If C is recursive, there is an effective procedure which decides whether $C(X)$ or $\sim C(X)$ is true after being given some finite portion $\overline{X}t = X0 \ldots Xt$ of X. Hence, if X_0 is such that $\overline{X}_0 t = \overline{X}t$, then $C(X) \equiv C(X_0)$. This implies that every recursive set of X's is open and closed. But every $C(X)$ of $MT[N,']$ is a Boolean combination of expressions of the form $(\forall x)(\exists y)M(x,y,X)$ where for fixed x and y $\hat{X}\, M(x,y,X)$ is open and closed (since M is recursive). Thus by Theorem 1 we obtain,

COROLLARY 1. If $C(X)$ is a formula of $MT[N,']$, then the relation $C(X)$ is in the Boolean algebra over G_δ of the Borel hierarchy.

We conclude this section with an example of a $C(X)$ of $MT[N,']$ which is neither a G_δ nor an F_σ (and therefore neither a Σ_2 nor a Π_2). The following remark is observed in [3].

(1) A set $C(X)$ is a G_δ, if and only if, there is a set W of words over I such that $C(X)$ holds, if and only if, $w<X$ for infinitely many $w \in W$.

Here $w<X$ (w is initial segment of X) stands for $(\exists t)\, \overline{X}t = w$. Now define $C \subseteq \{T,F\}^N$ by,

(2) $$[X0 \wedge (\forall x)(\exists y)[x \leq y \wedge Xy]] \vee [\sim X0 \wedge (\exists x)(\forall y)[x \leq y \supset \sim Xy]]$$

Suppose C is a G_δ. Then, by (1), there exists a $W \subseteq I^*$ such that

(3) $C(X) \;.\!\equiv\!.\; W \cap \{w \mid w<X\}$ is infinite

Define the sequence $w_0, w_1, w_2, \ldots$ by

$$(4)\quad \begin{array}{l} w_0 = \text{shortest } v,\ v\varepsilon W \wedge v \text{ of form } FF^k \\ w_{n+1} = \text{shortest } v,\ v\varepsilon W \wedge v \text{ of form } w_n TFF^k \end{array}$$

By (2) F^ω belongs to C, therefore by (3) w_0 exists and $F \leq w_0$. Assume inductively that w_n exists and $F \leq w_n$. Then by (2) $w_n TF^\omega$ belongs to C, therefore by (3) w_{n+1} exists and $F \leq w_{n+1}$. Thus (4) really defines a sequence of words, and clearly $w_i \varepsilon W$, $F \leq w_0 < w_1 < w_2 \ldots$. Thus, by (3) and (2), the sequence Y having all w_i's as initial segments belong to C. But this is contradictory, as Y starts with F and has infinitely many initial segments in W. Thus $C \notin G_\delta$, and similarly one shows $\sim C \notin G_\delta$. But $x \leq y$ is definable in $MT[N,']$, and therefore C is. Consequently, (2) provides an example of a set C, definable in $MT[N,']$, but neither in G_δ nor F_σ.

3. DECISION PROBLEMS FOR EXTENSIONS OF MT[N,']

Elgot and Rabin [8] have studied the existence of decision procedures for extensions of $MT[N,']$. In particular they have shown that $MT[N,',Q]$ is decidable if Q is either of $\{x^k \mid x\varepsilon N\}$, $\{k^x \mid x\varepsilon N\}$ or $\{x! \mid x\varepsilon N\}$ where k is a fixed natural number. The results are obtained by reducing the decision problem for MT[N,',Q] to that for MT[N,'] and then applying the procedure given in [1]. If $Q = \{(x,2x) | x \varepsilon N\}$, then the corresponding weak monadic theory is undecidable [8].

Let Q be a subset of N. If WMT[N,',Q] is undecidable, then so is MT[N,',Q]. This follows from the definability of 'X is a finite set' in MT[N,'], by the formula $(\exists x)(\forall t)[t \geq x \supset \sim Xt]$ where $t \geq x$ is an abbreviation of $(\forall Y).\ Yt \wedge (\forall w)[Yw' \supset Yw] \supset Yx$.

If Q is not recursive, then WMT[N,',Q] is undecidable (e.g., $0^{'\cdots'} \varepsilon Q$ can not be effectively decided). If Q is recursive, the hierarchy result of section 2 can be applied to give an upper bound to the complexity of decision problems for MT[N,',Q].

Theorem 2: If Q is recursive then truth in MT[N,',Q] is in $\Sigma_3 \cap \Pi_3$.

Proof: Let $\Psi(e,Z)$ be a universal predicate for all predicates P(Z) in Π_2, which is itself in Π_2. By Theorem 1, there is a recursive function B which maps every formula $\Phi(Z)$ of MT[N,'] into a Boolean expression B_Φ, and a recursive function f which maps every formula $\Phi(Z)$ of MT[N,'] into a finite sequence $f_\Phi = \langle f_{\Phi,1}, \ldots, f_{\Phi,n} \rangle$ of numbers, such that for any $Z \subseteq N$,

(1) $\Phi(Z)$ holds in MT[N,'] $.\equiv.$ $B_\Phi[\Psi(f_{\Phi,1},Z), \ldots, \Psi(f_{\Phi,n},Z)]$

Let $X(e)$ stand for $\Psi(e,Q)$, and note that because $\Psi \varepsilon \Pi_2$ and Q is recursive it follows that $X \varepsilon \Pi_2$. Furthermore, (1) may be restated as,

(2) $\Phi(Q)$ holds in $MT[N,',Q]$ $.\equiv.$ $B_\Phi[X(f_{\Phi,1}),\ldots, X(f_{\phi,n})]$

Note that the functions B,f are recursive, and all sentences of $MT[N,',Q]$ are of form $\Phi(Q)$ where $\Phi(Z)$ is a formula of $MT[N,']$. It follows that (2) provides for a recursive reduction of $\{\Sigma|\Sigma$ true in $MT[N,',Q]\}$ to the set X (i.e. a Turing machine can be built which, given a sentence Σ of $MT[N,',Q]$ and an oracle for membership in X, decides whether or not Σ is true). Thus, truth in $MT[N,',Q]$ is reducible to some $X \in \Pi_2$. It follows, by a wellknown result, that truth in $MT[N,',Q]$ belongs to $\Sigma_3 \cap \Pi_3$. Q.E.D.

Theorem 2 shows that for no recursive Q is it possible to prove $MT[N,',Q]$ undecidable by the standard method of showing that all recursive relations are definable.

If Q is the set of primes, then $(\forall x)(\exists y)[y>x \wedge Q(y) \wedge Q(y'')]$ states the twin prime problem in $MT[N,',Q]$. Indeed, this sentence is in the first order theory of $<N,',<,Q>$. Hence, the problem as to whether (W)MT[N,',primes] is decidable, would seem very difficult. Namely, a positive answer would settle the twin prime problem, while on the negative side, the standard methods of proving theories undecidable is not available.

Theorem 3. There is a recursive Q such that WMT[N,',Q] is undecidable.[1]

PROOF. Let R be a recursively enumerable set of primes which is not recursive. Let $r_1, r_2, \ldots$ be a recursive enumeration of R and let $Q_0 = \{r_i^2 p_i \mid i=1,2,\ldots\}$, whereby p_i is the ith prime. Q_0 is obviously recursive. To prove that WMT[N,',Q_0] is undecidable it is sufficient to show that the first order theory (FT) of $\langle N, M_1, M_2, \ldots, Q_0 \rangle$ is undecidable whereby M_k stands for the set of multiples of k. Just note that each M_k is definable in WMT[N,',Q_0] by the formula

$$M_k(w):\ (\forall X).\ Xw \wedge (\forall y)[X(y+k) \supset Xy] \supset X0).$$

From the definition of R and Q_0 we obtain

$$(*) \qquad R(k)\ .\equiv.\ k \neq 1 \wedge (\exists y)[M_{k^2}(y) \wedge Q_0(y)]$$

Let Σ_k be the sentence $k \neq 1 \wedge (\exists y)[M_{k^2}(y) \wedge Q_0(y)]$. By (*) Σ_k is true in FT[$N, M_1, M_2, \ldots, Q_0$] if and only if $k \in R$. But R is not recursive so there is no effective procedure for deciding truth in FT[$N, M_1, M_2, \ldots, Q_0$].

Q.E.D.

PROBLEM 1. Is there an 'interesting' recursive Q such that (W)MT[N,',Q] is undecidable? How about Q = primes?

[1]Michael O. Rabin has obtained a similar result (personal correspondence).

Although WMT[N,',Q_0] is undecidable, we have not classified its decision problem in the arithmetic hierarchy. This suggests,

PROBLEM 2. Is there a recursive Q such that the decision problem for (W)MT[N,',Q] is in $\Sigma_3 \cap \Pi_3$ but not in the Boolean algebra over Π_2?

Another interesting question is,

PROBLEM 3. Is there a recursive Q such that WMT[N,',Q] is decidable but MT[N,',Q] is undecidable?

A negative answer to Problem 3 whould imply the decidability of MT[N,'] as a consequence of the decidability of WMT[N,'] (Q=ϕ). Hence, a negative answer might be quite difficult.

BIBLIOGRAPHY

[1] J. R. Büchi, On a decision procedure in restricted second order arithmetic, Proc. Int. Cong. Logic, Method. and Philos. Sci. 1960, Stanford Univ. Press, Stanford, 1962.

[2] J. R. Büchi and L. H. Landweber, Solving sequential conditions by finite state operators, Purdue Report CSD TR 14.

[3] M. Davis, Infinite games of perfect information, Advances in Game Theory; Princeton Univ. Press, Princeton, 1964, 85-101.

[4] C. C. Elgot and M. O. Rabin, Decidability and undecidability of extensions of second (first) order theories of (generalized) successor, J. Symbolic Logic 31(1966), 169-181.

[5] S. C. Kleene, Introduction to metamathematics, New York, Van Nostrand, Amsterdam, North Holland and Groningem, Noordhoff, 1952.

[6] S. C. Kleene, Hierarchies of number theoretic predicates, Bull. Amer. Math. Soc. 61(1955), 193-213.

[7] R. McNaughton, Testing and generating infinite sequences by a finite automaton, Inf. and Control.9(1966), 521-530.

[8] R. M. Robinson, Restricted set theoretical definitions in arithmetic, Proc. Am. Math. Soc. 9(1958), 238-242.