The Journal of Symbolic Logic
Volume 31, Number 2, June 1966

DECIDABILITY AND UNDECIDABILITY OF EXTENSIONS OF SECOND (FIRST) ORDER THEORY OF (GENERALIZED) SUCCESSOR[1]

CALVIN C. ELGOT[2] AND MICHAEL O. RABIN[3]

Introduction. We study certain first and second order theories which are semantically defined as the sets of all sentences true in certain given structures. Let $\mathfrak{M} = \langle A, P_\alpha \rangle_{\alpha<\lambda}$ be a *structure* where A is a non-empty set, λ is an ordinal, and P_α is an $n(\alpha)$-ary relation or function[4] on A. With $\mathfrak{M}$ we associate a language L appropriate for $\mathfrak{M}$ which may be a first or higher order calculus. L has an $n(\alpha)$-place predicate or function constant $\mathbf{P}$ for each $\alpha < \lambda$. We shall study three types of languages: (1) first-order calculi with equality; (2) second-order monadic calculi which contain monadic predicate (set) variables ranging over subsets of A; (3) restricted (weak) second-order calculi which contain monadic predicate variables ranging over *finite* subsets of A. With a given structure and an appropriate language L we associate the theory $T = T(\mathfrak{M}, L)$ which is, by definition, the set of all sentences of L true in $\mathfrak{M}$. The theory T constructed in this manner will be referred to as *the theory of the structure* $\mathfrak{M}$, or sometimes *the theory of the relations and functions* P_α, $\alpha < \lambda$. The adjective *second-order* or *weak second-order* will be added when the language L is of that respective kind.

Of prime interest are extensions of theories which are obtained in the following manner. Let P be an n-ary relation or function on A and let be a n-place predicate or constant. Form the structure $\mathfrak{M}' = \langle A, P_\alpha, P \rangle_{\alpha<\lambda}$ and the language L' obtained by adding $\mathbf{P}$ to the formalism of L. The theory $T' = T(\mathfrak{M}', L')$ will be called the extension of T by P. We shall sometimes use the abbreviation $T + P$ to denote the extension T' of T by P.

Let $R(x, y)$ be a relation over A. R is said to be *definable* in $T = T(\mathfrak{M}, L)$ if there exists a formula $F(\mathrm{x}, \mathrm{y})$ of L such that for all $x, y \in A$, $R(x, y)$ holds iff $F(x, y)$ is true in $\mathfrak{M}$. Two extensions $T + P$ and $T + Q$ of T are

Received January 13, 1965.

[1] Presented to the American Mathematical Society in January, 1963 under the titles "Decision Problems of Extensions of Second Order Theory of Successor" and "On the First Order Theory of Generalized Successor".

[2] Sponsored in part by Air Force Contract AF 30 (602)–3340, Rome Air Development Center.

[3] Sponsored in part by Air Force Grant AF EOAR 63–70 and by Navy contract N 62558–4695.

[4] If P is a relation on A then its order is the number n such that $P \subseteq A^n$. In particular if $n = 1$ then P is a subset of A. If P is a function then its order n is the number of argument places. Here we do *not* consider functions as special relations on A.

called *equivalent* if P is definable in $T + Q$, and Q is definable in $T + P$. The notation for equivalence of extensions of T will be $(T + P)$ *eq*$(T + Q)$. If $(T + P)$ *eq* $(T + Q)$, then, of course, every relation definable in $T + P$ is definable in $T + Q$ and vice versa.

Specifically we shall study the second-order (SS) and weak second-order (WSS) theories of the successor function $S(x) = x + 1$ over the domain N of non-negative integers. These theories have been proved decidable [1, 2, 4]. We obtain a number of results showing that under very general conditions, extensions (in the above explained sense) of SS or WSS are undecidable. Thus, for example, *if we add to WSS a function* $f : N \to N$ *such that* $f^{-1}(n)$ *is infinite for every* $n \in N$, *then the resulting theory is undecidable.* On the other hand, it is possible to add to WSS or SS some relations or functions which are not definable in these theories, e.g. the relation (set) $P = \{i! \mid i \in N\}$, and obtain decidable extensions.

These last positive results employ methods of the theory of automata. We run, in fact, into a new kind of decision problem in automata theory. For a fixed *infinite* sequence x over the input alphabet, to find an effective procedure of deciding for every given automaton $\mathfrak{A}$ whether it accepts x or not (or to prove that such a procedure does not exist).

In Section 3 we study the first-order theory of generalized successor (GS). Let B be the set of all words on $\{0, 1\}$ and r_0, r_1 be the functions from B to B such that $r_0(x) = x0$ (i.e. the sequence x followed by 0) and $r_1(x) = x1$. Let $E(u, v)$ and $u \leqslant v$ be the relations on B defined in § 3. GS is the theory of the structure $\langle B, r_0, r_1, \leqslant, E\rangle$. GS was first considered by J. C. Shepherdson who proved that it is decidable (unpublished). This applied calculus is useful in the study of finite automata but these connections are not explored in the present article. We establish natural and, in a sense, dual interpretations of GS in WSS and vice versa.

These interpretations enable us to carry over results about decidability and undecidability of extensions of WSS to corresponding results about extensions of GS. In particular, under very general conditions, extensions of GS will be undecidable, but some extensions are decidable.

Our study of the first-order theory GS motivates a problem concerning the existence of so called *maximally decidable theories* which is posed following Theorem 11.

The authors wish to thank J. B. Wright for stimulating discussions and J. B. Wright and J. W. Thatcher for improvements in the manuscript.

1. Undecidability results for *WSS* and *SS*. The (monadic) second-order theory of successor, SS, is the set of true sentences of the following interpreted calculus. Logical constants of SS include equality, the usual propositional connectives, and the quantifiers $\exists$ and $\forall$.Non-logical constants are $\mathbf{0}$ and a singularly function constant $\mathbf{S}$. There are individual variables

$\mathsf{u}, \mathsf{v}, \mathsf{x}, \mathsf{y}, \mathsf{z}, \ldots$, and monadic predicate (set) variables $\mathsf{A}, \mathsf{B}, \mathsf{C}, \ldots$. Quantification is possible over predicate as well as over individual variables. Let $\langle N, 0, S\rangle$ be the structure where N is the set of non-negative integers, 0 is zero and S is the successor function $S(x) = x + 1$. In the interpretation $\mathbf{0}$ will denote 0, $\mathbf{S}$ will be interpreted as S. The individual variables will range over elements of N and the predicate variables will range over arbitrary subsets of N.

The weak (monadic) second-order theory of successor, *WSS*, is similar to *SS* except that instead of the predicate variables $\mathsf{A}, \mathsf{B}, \mathsf{C}, \ldots$, there are (monadic) predicate variables $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}, \ldots$, which range over the set $\mathscr{F}$ of *finite* subsets of N.

The formula

$$(1)\quad \forall \mathsf{A}[\mathsf{A}(\mathsf{y}) \wedge \forall \mathsf{z}[\mathsf{A}(\mathbf{S}(\mathsf{z})) \rightarrow \mathsf{A}(\mathsf{z})] \rightarrow \mathsf{A}(\mathsf{x})] \quad .$$

is satisfied by $x, y \in N$ if and only if $x \leqq y$. We shall abbreviate (1) by $\mathsf{x} \leqq \mathsf{y}$. If we replace in (1) the set variable A by the variable $\boldsymbol{\alpha}$ of *WSS* then the resulting formula defines $\leqq$ in *WSS*. The formula $Fn(\mathsf{A})$

$$Fn(\mathsf{A}) = \exists \mathsf{y} \forall \mathsf{x}[\mathsf{A}(\mathsf{x}) \rightarrow \mathsf{x} \leqq \mathsf{y}]$$

is satisfied by $A \subseteq N$ if and only if A is finite. Using Fn to relativize quantification over predicate variables, we can interpret *WSS* in *SS*. Thus every undecidability result concerning extensions of *WSS* yields an undecidability result concerning the corresponding extensions of *SS*. Every decidability result concerning extensions of *SS* yields a corresponding result for *WSS*.

We shall consider extensions of the theories *WSS* and *SS* which are obtained by adding to the structure $\langle N, 0, S\rangle$ a fixed function $f : N \rightarrow N$ or a fixed set $P \subseteq N$ and adding to the formalism a function constant $\mathbf{f}$ or a predicate constant $\mathbf{P}$ to denote it. It turns out that under rather weak assumptions the resulting theory will be undecidable.

We remark, first of all, that if in an extension T of *WSS* there is a formula $F(\alpha, \mathsf{x}, \mathsf{y})$ such that for every finite binary relation $R \subseteq N \times N$ there exists a finite set α such that $F(\alpha, x, y)$ holds if and only if $\langle x, y\rangle \in R$, then T is undecidable.

This is proved by showing that addition and multiplication of integers are definable in T. Define

$$Fnc(\boldsymbol{\alpha}, \mathsf{z}) = \forall \mathsf{x}[\mathsf{x} \leqq \mathsf{z} \rightarrow \exists ! \mathsf{y} F(\boldsymbol{\alpha}, \mathsf{x}, \mathsf{y})].$$

We use $\exists ! y$ to mean *there exists a single y*. *Fnc* is satisfied by $\alpha \subseteq N$ and $z \in N$ if and only if the relation $F(\alpha, x, y)$ is a single valued function in the interval $0 \leqq x \leqq z$. The formula

$$\exists \boldsymbol{\alpha}[Fnc(\boldsymbol{\alpha},\mathsf{y}) \wedge F(\boldsymbol{\alpha},\mathbf{0},\mathsf{x}) \wedge \forall \mathsf{u} \forall \mathsf{v}[\mathsf{u} < \mathsf{y} \wedge F(\boldsymbol{\alpha},\mathsf{u},\mathsf{v}) \rightarrow F(\boldsymbol{\alpha},\mathbf{S}(\mathsf{u}),\mathbf{S}(\mathsf{v})] \wedge F(\boldsymbol{\alpha},\mathsf{y},\mathsf{z})]$$

clearly defines the relation $x + y = z$ in T. Using this definition we can define $x \cdot y = z$ in a similar way.

THEOREM 1. *Let $f : N \to N$ be such that $f^{-1}(n)$ is infinite for every $n \in N$. The theory T resulting from WSS by adjoining f is undecidable.*

PROOF. The proof is accomplished by construction of a formula $F(\alpha, \mathrm{x}, \mathrm{y})$ which reproduces in T, in the sense explained above, every finite binary relation.

Let $Nxt(\alpha, \mathrm{x}, \mathrm{y})$ denote the formula

$$\alpha(\mathrm{x}) \wedge \alpha(\mathrm{y}) \wedge \mathrm{x} < \mathrm{y} \wedge \forall \mathrm{z}[\mathrm{x} < \mathrm{z} < \mathrm{y} \to \sim\alpha(\mathrm{z})].$$

If $\alpha = \{n_1, \ldots, n_k\}$, $n_1 < n_2 < \ldots < n_k$, then α, x, y, satisfy Nxt if and only if $x = n_i$, $y = n_{i+1}$, for some i, $1 \leqq i \leqq k$. Let $Od(\alpha, \mathrm{x})$ denote the formula

$$\alpha(\mathrm{x}) \wedge \forall\beta\{\beta \subseteq \alpha \wedge \forall \mathrm{y}[\alpha(\mathrm{y}) \wedge \forall \mathrm{z} \sim Nxt(\alpha, \mathrm{z}, \mathrm{y}) \to \beta(\mathrm{y})] \wedge$$
$$\forall\mathrm{y}\forall\mathrm{z}\forall\mathrm{u}[\beta(\mathrm{y}) \wedge Nxt(\alpha, \mathrm{y}, \mathrm{u}) \wedge Nxt(\alpha, \mathrm{u}, \mathrm{z}) \to \beta(\mathrm{z})] \to \beta(\mathrm{x})\}.$$

With α as above, α, x satisfy Od if and only if $x = n_{2i+1}$ for some i, $1 \leqq 2i + 1 \leqq k$.

The desired formula $F(\alpha, \mathrm{x}, \mathrm{y})$ will be

$$F(\alpha,\mathrm{x},\mathrm{y}) = \exists\mathrm{u}\exists\mathrm{v}[\alpha(\mathrm{u}) \wedge \alpha(\mathrm{v}) \wedge Od(\alpha, \mathrm{u}) \wedge Nxt(\alpha, \mathrm{u}, \mathrm{v}) \wedge \mathbf{f}(\mathrm{u}) = \mathrm{x} \wedge \mathbf{f}(\mathrm{v}) = \mathrm{y}].$$

To see this, let $R = \{\langle x_1, y_1\rangle, \ldots, \langle x_k, y_k\rangle\}$ be an arbitrary finite relation, $R \subseteq N \times N$. Choose n_1 such that $f(n_1) = x_1$. Choose $n_2 > n_1$ such that $f(n_2) = y_1$; this is possible since $f^{-1}(y_1)$ is infinite. Choose $n_3 > n_2$ such that $f(n_3) = x_2$, and so on up to n_{2k}. Let $\alpha = \{n_1, \ldots, n_{2k}\}$ then α, x, y satisfy $F(\alpha, \mathrm{x}, \mathrm{y})$ if and only if $\langle x, y\rangle \in R$. Thus T is undecidable.

COROLLARY 1. *The theory resulting from WSS by adjunction of the square excess function (introduced in* [7]*) is undecidable.*

THEOREM 2. *The extension T of WSS by a function $g : N \to N$ such that*

(2) $x < y$ *implies* $1 < g(y) - g(x)$

is undecidable.

PROOF. Condition (2) implies that $g^{-1}(g(n) + 1)$ is *never* defined.

Let

$$f(x) = \begin{cases} n \text{ if } x = g^m(g(n) + 1) \text{ for some } n, m \in N \\ 0 \text{ otherwise.} \end{cases}$$

The function f is well-defined and the set

$$f^{-1}(n) = \{x \mid x = g^m(g(n) + 1), m = 0, 1, \ldots\}$$

is infinite for every $n \in N$.

We claim that f is definable in T. Let $G(\mathrm{x}, \mathrm{y})$ be the formula

$$\forall\alpha[\alpha(\mathrm{x}) \wedge \forall\mathrm{z}[\alpha(\mathbf{g}(\mathrm{z})) \to \alpha(\mathrm{z})] \to \alpha(\mathbf{S}(\mathbf{g}(\mathrm{y})))].$$

The formula

$$G(\mathsf{x}, \mathsf{y}) \vee [\forall \mathsf{u} \sim G(\mathsf{x}, \mathsf{u}) \wedge \mathsf{y} = \mathbf{0}]$$

is satisfied by $x, y \in N$ if and only if $f(x) = y$.

The theory T is now undecidable by the previous theorem.

COROLLARY 2. *The function $g(x) = 2x$ satisfies the condition of Theorem 2. Hence adding this function to WSS results in an undecidable theory.*

This result is due to R. M. Robinson [8]. The function $g^m(g(n) + 1)$ is a generalization of the function $2^m(2n + 1)$ used by Robinson in his proof. In a similar way adding each of $g(x) = x^2$, $g(x) = x^3$, $g(x) = [e^x]$ to WSS yields undecidable theories. These are, of course, just samples of the possible applications of our theorem.

2. Decidability results for *SS* and *WSS*. In this section we shall prove that it is possible to add to SS certain sets or functions not definable in SS and retain decidability. By a previous remark it then follows that similar results hold for WSS. These investigations combine the interesting methods and results of Büchi [3] with a new operation of *contraction* of a set of integers.

Let $\mathfrak{A} = \langle S, M, S_0, F\rangle$ be a finite non-deterministic automaton over the alphabet $\Sigma = \{0, 1\}$ (see [6]). Let $x = (\sigma_i)$, $0 \leqq i < \infty$, $\sigma_i \in \Sigma$. A sequence $(s_i)_{0 \leqq i < \infty}$, $s_i \in S$, of elements of S is called *compatible* with x if $s_{i+1} \in M(s_i, \sigma_i)$, $0 \leqq i < \infty$. Compatibility of a finite sequence $(s_i)_{0 \leqq i < m}$ with a finite sequence $(\sigma_i)_{0 \leqq i < m}$ is defined in a similar way. The infinite sequence x is *accepted by* $\mathfrak{A}$ if there exists a sequence $(s_i)_{0 \leqq i < \infty}$ compatible with x such that $s_0 \in S_0$ and the set $\{i \mid s_i \in F\}$ is infinite. The set of all sequences accepted by $\mathfrak{A}$ will be denoted by $T(\mathfrak{A})$.

We shall use Σ^* to denote the set of all finite sequences on Σ. If $n \in N$ then 0^n (1^n) will denote the sequence consisting of n letters 0 (1). If $P \subseteq N$ is a set of natural numbers, define $x_P = (\sigma_i)_{0 \leqq i < \infty}$ where $\sigma_i = 1$ if $i \in P$ and $\sigma_i = 0$ if $i \notin P$.

The following important result was proved by Büchi [3]. Let $F(\mathsf{A})$ be a formula of SS containing only the free set variable A. We can effectively correlate with $F(\mathsf{A})$ a finite automaton $\mathfrak{A}_F$ such that for every $A \subseteq N$, A satisfies $F(\mathsf{A})$ if and only if $x_A \in T(\mathfrak{A}_F)$. In particular we can effectively calculate the number $n(F)$ of states of the automaton $\mathfrak{A}_F$.

For $\lambda = (s_i)_{0 \leqq i \leqq m+1}$ define $S(\lambda) = \{s_0, \ldots, s_{m+1}\}$.

DEFINITION. Let $\mathfrak{A}$ be as before and let $x = (\sigma_i)_{0 \leqq i < m}$, $\sigma_i \in \Sigma$. Define the *type* $Tp(x)$ of x by

$$Tp(x) = \{\langle s_0, s_{m+1}, S(\lambda)\rangle \mid \lambda = (s_i)_{0 \leqq i \leqq m+1} \text{ compatible with } x\}.$$

The type $Tp(x)$ depends, of course, not only on the sequence x but also on $\mathfrak{A}$. However, since the automaton $\mathfrak{A}$ remains fixed during the discussion, we omit reference to $\mathfrak{A}$ in the notation $Tp(x)$. The relation $Tp(x) = Tp(y)$

is an equivalence relation and if $\mathfrak{A}$ has n states then the number of equivalence classes is at most $d = 2^{n^2 2^n}$. It can be verified that if $Tp(x) = Tp(y)$ then $Tp(xz) = Tp(yz)$ for $z \in \Sigma^*$.

Lemma 1. *Let $\mathfrak{A}$ have n states, $d = 2^{n^2 2^n}$. If $d < r$, $d < s$, and $r \equiv s \bmod d!$ then $Tp(0^r) = Tp(0^s)$.*

Proof. Assume $r < s$. Consider the r sequences 0^i, $1 \leqq i \leqq r$. Since $d < r$ there must be two numbers i, $i + k$ such that $1 \leqq i < i + k \leqq r$, $k < d$, and $Tp(0^i) = Tp(0^{i+k})$. Hence $Tp(0^r) = Tp(0^i 0^{r-i}) = Tp(0^{i+k} 0^{r-i}) = Tp(0^{r+k})$. By repeated application we have $Tp(0^r) = Tp(0^{r+mk})$, $0 \leqq m < \infty$. Now $k < d$, thus $r \equiv s \bmod d!$ implies $r \equiv s \bmod k$. Hence $Tp(0^r) = Tp(0^s)$.

It follows from the lemma that with r and s as above, $Tp(0^r 1) = Tp(0^s 1)$.

Definition. Let $x = 0^{p_1} 10^{p_2} 1 \dots$ ($p_1 = 0$ is possible) and let d be an integer. Define $q_i = p_i$ if $p_i \leqq d$; define $q_i \equiv p_i \bmod d!$, $d < q_i \leqq d + d!$, if $d < p_i$. The *contraction* x^d of x by d is the sequence $x^d = 0^{q_1} 10^{q_2} 1 \dots$.

Theorem 3. *Let $\mathfrak{A} = \langle S, M, S_0, F \rangle$ be an automaton with n states, $d = 2^{n^2 2^n}$. Let x and x^d be as above, then $x \in T(\mathfrak{A})$ if and only if $x^d \in T(\mathfrak{A})$.*

Proof. The corresponding parts $0^{p_i} 1 = x_i$ and $0^{q_i} 1 = y_i$ satisfy, by the corollary to Lemma 1, $Tp(x_i) = Tp(y_i)$. Assume $x \in T(\mathfrak{A})$ and let λ be an infinite sequence of states compatible with x such that infinitely many of the states in λ are in F. Let λ_i be the subsequence of λ corresponding to the subsequence x_i of x. There exists a sequence of states μ_i compatible with y_i which has the same first and last members as λ_i and such that $S(\mu_i) = S(\lambda_i)$. Putting the μ_i together we get an infinite sequence μ of states which is compatible with x^d and which contains elements of F infinitely often. Thus $x^d \in T(\mathfrak{A})$. Since only $Tp(x_i) = Tp(y_i)$ was used in the proof, the fact that $x^d \in T(\mathfrak{A})$ implies $x \in T(\mathfrak{A})$ follows in a similar way.

Corollary 3. *Let $F(\mathsf{A})$ be a formula of SS and $n(F)$ be the number of states of the automaton $\mathfrak{A}_F$ such that $A \subseteq N$ satisfies $F(\mathsf{A})$ if and only if $x_A \in T(\mathfrak{A}_F)$. Let $d_1 = n^2(F)\, 2^{n(F)}$, $d = 2^{d_1}$. A set $A \subseteq N$ satisfies $F(\mathsf{A})$ if and only if the set $B \subseteq N$ such that $x_B = (x_A)^d$ satisfies $F(\mathsf{A})$.*

A set $A \subseteq N$ is called *eventually periodic* if it is the union of a finite set with a finite number of arithmetical progressions; thus

$$(3) \quad A = \{k_1, \dots, k_p\} \cup \bigcup_{1 \leqq i \leqq q} \{a_i + nd_i \mid n \in N\}.$$

If a description (3) of an eventually periodic set is given, we can effectively construct a formula $D(\mathsf{A})$ of SS such that A is the *only* set satisfying it.

For $A \subseteq N$ we shall call the set B such that $x_B = (x_A)^d$ the set obtained from A by *contraction by d*, and denote it by A^d. The effect of contracting a set $A = \{n_1, n_2, \dots\}$, $n_1 < n_2 < \dots$, by $d > 0$ may be described as follows. If $A^d = \{m_1, m_2, \dots\}$, $m_1 < m_2 < \dots$, then for all i, $m_{i+1} - m_i = n_{i+1} - n_i$ if $n_{i+1} - n_i \leqq d + 1$, and $d + 1 < m_{i+1} - m_i \leqq d + 1 + d!$, $m_{i+1} - m_i \equiv n_{i+1} - n_i \bmod d!$, if $d + 1 < n_{i+1} - n_i$.

THEOREM 4. *For each of the following sets* (1) $P = \{i! \mid i \in N\}$, (2) $Q = \{r^i \mid i \in N\}$, *r a fixed integer,* (3) $R = \{i^r \mid i \in N\}$, *r a fixed integer, the set obtained by contraction by an integer $d > 0$ is eventually periodic and a description of the form* (3) *of the contracted set can be effectively obtained.*

PROOF. (1) Assume that $P^d = \{m_1, m_2, \ldots\}$, $m_1 < m_2 < \ldots.$ We can effectively determine the smallest integer k such that for $i \geqq k$ we have $d + 1 < (i + 1)! - i!$ and $i! \equiv 0 \bmod d!$. For $i \geqq k$ we then have $m_{i+1} - m_i = d!$. Thus P^d is $\{m_1, \ldots, m_{k-1}\} \cup \{m_k + nd! \mid n \in N\}$. The numbers $m_1, \ldots, m_k$ can be effectively calculated.

(2) Assume that $Q^d = \{m_1, m_2, \ldots\}$, $m_1 < m_2 < \ldots.$ Let $(d!, r) = k$ and $d! = kq$. The numbers r and q are relatively prime. Thus $r^{\varphi(q)} \equiv 1 \bmod q$ where φ is Euler's function. Since $k \mid r$ we have for $i > 0$, $r^{i+\varphi(q)} - r^i = r^i(r^{\varphi(q)} - 1) \equiv 0 \bmod d!$ Let i_0 be the smallest positive integer such that for $i \geqq i_0$, $r^{i+1} - r^i > d + 1$. The previous congruence implies that for $i > i_0$, $m_{i+\varphi(q)+1} - m_{i+\varphi(q)} = m_{i+1} - m_i$. This implies that Q^d is an eventually periodic set. By calculating i_0 and $m_{i+1} - m_i$ for $i_0 < i \leqq i_{0+\varphi(q)}$ we obtain a description (3) of Q^d

(3) We have $(i + d!)^r - i^r \equiv 0 \bmod d!$. The proof proceeds now as in (2).

THEOREM 5. *For each of the sets P, Q, R of Theorem 4, the theory T resulting from SS by adjoining this set is decidable.*

PROOF. We shall prove the assertion for the set P, the proofs for Q and R are identical. The sentences of T which do not contain the constant $\mathbf{P}$ are sentences of SS and their validity can be tested by Büchi's decision procedure for SS.

If a sentence σ of SS contains $\mathbf{P}$ then it has the form $F(\mathbf{P})$ where $F(\mathsf{A})$ is a formula of SS. With d as in Corollary 3 we have that P satisfies $F(\mathsf{A})$ (i.e. $F(\mathbf{P})$ is a valid sentence of T) if and only if P^d satisfies F. Let $D(\mathsf{A})$ be a definition of the eventually periodic set P^d in SS; such a formula $D(\mathsf{A})$ can be effectively found. Thus P^d satisfies $F(\mathsf{A})$ if and only if the sentence $\exists \mathsf{A}[D(\mathsf{A}) \wedge F(\mathsf{A})]$ of SS is true. This can again be decided by Büchi's procedure.

Given an infinite set A, let $\theta_A(x) = y$ if y is the largest number in A such that $y \leqq x$. Let $\theta_A(x) = 0$ for $x < \min A$.

COROLLARY 4. *Each of the theories obtained by adjoining to SS the functions θ_P, θ_Q, θ_R respectively is decidable.*

PROOF. The relation $\theta_A(x) = y$ is definable in the theory obtained by augmenting SS with A.

3. Mutual interpretability of extensions of *GS* and *WSS*. *The theory of generalized successor* (*GS*) is the first-order interpreted calculus with equality having individual variables ranging over elements of the set B of all finite words on the alphabet $\{0, 1\}$ and having non-logical constants $\boldsymbol{\Lambda}$, $\mathbf{r}_0$, $\mathbf{r}_1$, $\mathbf{E}$, $\preccurlyeq$ which are respectively interpreted as the empty word Λ, the functions $r_0 : B \rightarrow B$ and $r_1 : B \rightarrow B$ such that $r_0(u) = u0$ and $r_1(u) = u1$, the relation $E(u, v)$ which holds between words u, v iff they have the same length and the relation $u \preccurlyeq v$, u is a prefix (initial segment) of v.[5]

We construct interpretations of extensions of GS in extensions of WSS which are based upon the observation that the mapping θ which takes u into $\{l(v) \mid v1 \preccurlyeq u\} \cup \{l(u)\}$, where $l(u)$ is the length of u, is a *1–1* mapping of B onto all *non-empty* finite subsets of the set N of non-negative integers. For example $\theta(110) = 0110 = \{0, 1, 3\}$ and $\theta\Lambda = \{0\}$.

Let R be a binary relation over B and let R^* be the binary relation over $\mathscr{F} - \{\phi\}$, ($\mathscr{F}$ is the set of all finite sets of integers) such that

$$(4) \quad R^*(\theta u, \theta v) \leftrightarrow R(u, v).$$

THEOREM 6. *Given any wff* $F(\mathsf{u}, \mathsf{v}, \ldots)$ *of* $GS + R$ *(for this notation see Introduction) one may effectively find a wff* $F^*(\alpha, \beta, \ldots)$ *of* $WSS + R^*$ *such that*

$$(5) \quad F^*(\theta u, \theta v, \ldots) \leftrightarrow F(u, v, \ldots).$$

In particular, if F is a sentence then so is F^*; in this case F is true iff F^* is true.

PROOF. We note first that every wff of $GS + R$ is logically equivalent to a *reduced* wff of $GS + R$ in which no iterates of function symbols appear. A reduced wff is, by definition, constructed from variants of the *atomic* formulas

$$(6) \quad \mathbf{R}(\mathsf{u}, \mathsf{v}), [\mathsf{u} \preccurlyeq \mathsf{v}], \mathbf{E}(\mathsf{u}, \mathsf{v}), [\mathsf{u} = \mathbf{r}_0(\mathsf{v})], [\mathsf{u} = \mathbf{r}_1(\mathsf{v})]$$

by means of propositional connectives and quantifiers. It is therefore sufficient to construct F^* for reduced formulas F. We shall utilize the following abbreviations: $L(\mathsf{x}, \alpha)$ for $[\alpha(\mathsf{x}) \wedge \forall \mathsf{z}[\alpha(\mathsf{z}) \rightarrow \mathsf{z} \leqq \mathsf{x}]]$, $\alpha \neq \phi$ for $\exists \mathsf{z}\alpha(\mathsf{z})$.

We shall start by constructing a formula $F^*(\alpha, \beta)$ for each of the five formulas $F(\mathsf{u}, \mathsf{v})$ listed in (6). $\mathbf{R}(\mathsf{u}, \mathsf{v})$ is $\mathbf{R}^*(\alpha, \beta)$. $[\mathsf{u} \preccurlyeq \mathsf{v}]^*$ is

$$\exists \mathsf{x} \exists \mathsf{y}[L(\mathsf{x}, \alpha) \wedge L(\mathsf{y}, \beta) \wedge [\mathsf{x} \leqq \mathsf{y}] \wedge \forall \mathsf{z}[\mathsf{z} < \mathsf{x} \rightarrow [\alpha(\mathsf{z}) \leftrightarrow \beta(\mathsf{z})]]$$

$\mathbf{E}(\mathsf{u}, \mathsf{v})^*$ is $\exists \mathsf{x} \exists \mathsf{y}[L(\mathsf{x}, \alpha) \wedge L(\mathsf{y}, \beta) \wedge [\mathsf{x} = \mathsf{y}]$.

$[\mathsf{u} = \mathbf{r}_0(\mathsf{v})]^*$ is

$$\exists \mathsf{x} \exists \mathsf{y}[L(\mathsf{x}, \alpha) \wedge L(\mathsf{y}, \beta) \wedge [\mathsf{x} = \mathbf{S}(\mathsf{y})] \wedge \forall \mathsf{z}[\mathsf{z} < \mathsf{y} \rightarrow [\alpha(\mathsf{z}) \leftrightarrow \beta(\mathsf{z})]] \wedge \sim\alpha(\mathsf{y})].$$

$[\mathsf{u} = \mathbf{r}_1(\mathsf{v})]^*$ is similar to the above formula except that the last conjunct is $\alpha(\mathsf{y})$.

It is easy to check that for each of the above formulas $F^*(\alpha, \beta)$ condition (5) is satisfied.

[5] Actually, Λ and one of the two successor functions are definable from the other primitives.

If F is $G \vee H$ or $\sim G$ and G^*, H^*, satisfy (5) then F^* can be taken as $G^* \vee H^*$ or $\sim G^*$, respectively. Finally if F is $\exists \mathsf{u} G(\mathsf{u}, \mathsf{v}, \ldots)$ and $G^*(\boldsymbol{\alpha}, \boldsymbol{\beta}, \ldots)$ is a formula of $GS + R^*$ such that (5) is satisfied (for G and G^*) then F^* can be taken as $\exists \boldsymbol{\alpha}[\boldsymbol{\alpha} \neq \phi \wedge G^*(\boldsymbol{\alpha}, \boldsymbol{\beta}, \ldots)]$. Since all reduced formulas are constructed from variants of the atomic formulas (6) by means of propositional connectives and quantifiers, the theorem follows by induction on formulas.

We shall now construct interpretations of extensions of WSS in extensions of GS which are based upon the 1–1 mapping ρ defined over $N \cup \mathscr{F}$, whose values are elements of B and which satisfies: (1) if $x \in N$ then $\rho x = 0^{x+1}$, (2) if $\alpha \in \mathscr{F}$ then $\rho\alpha$ is the shortest word u such that for any x,

$$\exists v[[x = l(v)] \wedge [v1 \preccurlyeq u]] \leftrightarrow x \in \alpha.$$

For example, $\rho 0 = 0$, $\rho 3 = 0000$, $\rho\{0, 2, 3\} = 1011$, $\rho\phi = \Lambda$.

Rather than treat the most general extensions of WSS, we shall restrict ourselves to a special but typical case and show how to interpret an extension $WSS + Q$ where $Q \subseteq N \times \mathscr{F}$ (i.e. Q is a relation between integers and finite sets of integers), in an appropriate extension $GS + Q^\dagger$ of GS. Let $Q^\dagger \subseteq B \times B$ be the smallest relation such that $Q^\dagger(\rho x, \rho\alpha) \leftrightarrow Q(x, \alpha)$.

Theorem 7. *Given any wff $F(\mathsf{x}, \boldsymbol{\alpha}, \ldots)$ of $WSS + Q$, one may effectively find a wff $F^\dagger(\mathsf{u}, \mathsf{v}, \ldots)$ of $GS + Q^\dagger$ such that*

(7) $F^\dagger(\rho x, \rho\alpha, \ldots) \leftrightarrow F(x, \alpha, \ldots)$.

In particular, if F is a sentence then so is $F^\dagger$; in this case F is true iff $F^\dagger$ is true.

Proof. We note first that every wff of $WSS + Q$ is equivalent to a *reduced* wff of $WSS + Q$ which, by definition, is constructed from variants of the atomic formulas

(8) $\mathbf{Q}(\mathsf{x}, \boldsymbol{\alpha}), \boldsymbol{\alpha}(\mathsf{x}), [\mathsf{y} = \mathsf{x}], [\mathsf{y} = \mathbf{S}(\mathsf{x})]$

by means of propositional connectives and quantifiers. It is therefore sufficient to construct $F^\dagger$ for reduced formulas F. Before proceeding with the construction, we introduce two abbreviations. Let $\tau(\mathsf{u})$ be an abbreviation for the following formula of GS: $[\mathsf{u} \neq \boldsymbol{\Lambda}] \wedge \forall \mathsf{w}[\mathsf{w} \prec \mathsf{u} \rightarrow \mathbf{r}_0(\mathsf{w}) \preccurlyeq \mathsf{u}]$. If $\tau(u)$ holds, u is called a *tally*. Let $T(u)$ be an abbreviation for the following formula of GS: $[[\mathsf{u} = \boldsymbol{\Lambda}] \vee \exists \mathsf{v}[\mathsf{u} = \mathbf{r}_1(\mathsf{v})]]$. The image of ρ is $\{u \mid \tau(u) \vee T(u)\}$.

As in the proof of Theorem 6, we shall prove the assertion by first constructing a formula $F^\dagger(\mathsf{u}, \mathsf{v})$ for each of the four formulas listed in (8) and then treating the propositional connectives and the quantifiers.

$\mathbf{Q}(\mathsf{x}, \boldsymbol{\alpha})^\dagger$ is simply $\mathbf{Q}^\dagger(\mathsf{u}, \mathsf{v})$. $\boldsymbol{\alpha}(\mathsf{x})^\dagger$ is

$$\exists \mathsf{w}[[\mathbf{r}_1(\mathsf{w}) \preccurlyeq \mathsf{v}] \wedge \mathbf{E}(\mathsf{u}, \mathbf{r}_1(\mathsf{w}))] \wedge \tau(\mathsf{u}) \wedge T(\mathsf{v}).$$

$[\mathsf{y} = \mathsf{x}]^{\dagger}$ is $[\mathsf{u} = \mathsf{v}] \wedge \tau(\mathsf{u}) \wedge \tau(\mathsf{v})$.

$[\mathsf{y} = \mathbf{S}(\mathsf{x})]^{\dagger}$ is $[\mathsf{v} = \mathbf{r}_0(\mathsf{u})] \wedge \tau(\mathsf{u})$.

If G and H are formulas of $WSS + Q$ and $G^{\dagger}$, $H^{\dagger}$ satisfy (7), then $[G \vee H]^{\dagger}$ is $G^{\dagger} \vee H^{\dagger}$, $[\sim G]^{\dagger}$ is $\sim G^{\dagger}$, $[\exists x G]^{\dagger}$ is $\exists u[\tau(u) \wedge G^{\dagger}]$, $[\exists \alpha G]^{\dagger}$ is $\exists \mathsf{v}[T(\mathsf{v}) \wedge G^{\dagger}]$.

Theorem 8. *The theories $GS + R$ and $GS + R^{*\dagger}$ are equivalent (for the notion of equivalence see Introduction) and consequently R is definable in $GS + R^{*\dagger}$ and $R^{*\dagger}$ is definable in $GS + R$.*

The proof depends upon the observation that $\rho\theta(u) = u1$ and consequently R is definable in $GS + R^{*\dagger}$ and $R^{*\dagger}$ is definable in $GS + R$. The proof of the following corollary is straightforward.

Corollary 5. *$GS + R$ is decidable iff $WSS + R^{*}$ is decidable.*

Theorem 9. *The theories $WSS + Q$ and $WSS + Q^{\dagger *}$ are equivalent.*

Proof. We note that $\theta\rho(x) = \{x + 1\}$ and $\theta\rho(\alpha) = \alpha \cup \{1 + \max \alpha\}$. The proof now follows readily from the fact that there are formulas $F(x, \alpha)$, $G(\alpha, \beta)$ of WSS such that $F(x, \alpha) \leftrightarrow \theta\rho(x) = \alpha$ and $G(\alpha, \beta) \leftrightarrow \theta\rho(\alpha) = \beta$.

Corollary 6. *$WSS + Q$ is decidable iff $GS + Q^{\dagger}$ is decidable.*

4. Decidability and undecidability of extensions of *GS*.

The results concerning decidability and undecidability of extensions of WSS will now be combined with the interpretation of extensions $WSS + Q$ in the extensions $GS + Q^{\dagger}$ of GS and by using Corollary 6 we shall infer results concerning decidability and undecidability of extensions of GS.

Let $f : N \to N$ be a function. The graph G_f of f is the binary relation such that $\langle x, y\rangle \in G_f$ if and only if $y = f(x)$.

Theorem 10. *Let $f : N \to N$ be a function such that* (1) *$f^{-1}(x)$ is infinite for every $x \in N$,* or (2) *$x < y$ implies $1 < f(y) - f(x)$, then $GS + G_f^{\dagger}$ is undecidable.*

Proof. The extension $WSS + G_f$ is undecidable by Theorems 1 and 2. The result now follows from Corollary 6.

Corollary 7. *Let H be the predicate (set) $\{0^n 1\, 0^n \mid n \in N\}$; the theory $GS + H$ is undecidable.*

Proof. Let $f : N \to N$ be the function $f(x) = 2x$. $G_f^{\dagger}$ is the binary relation $\{\langle 0^{n+1}, 0^{2n+1}\rangle \mid n \in N\}$. The extension $GS + G_f^{\dagger}$ is undecidable. Hence it suffices to show that $G_f^{\dagger}$ is definable in $GS + H$. Indeed

$$G_f^{\dagger}(u, v) \leftrightarrow \tau(u) \wedge \tau(v) \wedge \exists w[H(w) \wedge [r_1(u) \leqslant w] \wedge E(r_0(r_0(v)), w)].$$

Let F be the set $\{0^n 1\, 0^n 1 \mid n \in N\}$ then $GS + F$ is clearly also undecidable. Similarly for $G = \{0^n 1\, 1\, 0^n \mid n \in N\}$.

Corollary 8. *The extensions of GS obtained by adjoining each of the following predicates is undecidable. Let u^c denote the word u written in reverse order.*

(a) $\{u \mid u = u^c\}$ (*i.e., u is a symmetric word*).

(b) $\{u \mid \exists v[u = vv]\}$ (*u is a square in the free semigroup B*).

(c) $\{u \mid \exists v[u = v^c v]\}$.

(d) $db = \{\langle u, v\rangle \mid l(v) = 2l(u)\}$.

(e) $Part = \{\langle u, v\rangle \mid \exists s \exists t[v = sut]$.

(f) $Suffix = \{\langle u, v\rangle \mid \exists s[v = su]\}$.

PROOF. In most cases we show directly that one of the predicates F, G, H is definable in the extension in question. To simplify notations we shall write the mathematical formulas defining the relation in terms of the relations of GS and the additional relation. Let

$$J = \{0^n\, 1\, 0^m\, 1 \mid n, m \in N\}, \qquad K = \{0^n\, 1\, 1\, 0^m \mid n, m \in N\},$$
$$L = \{0^n\, 1\, 0^m \mid n, m \in N\}, \qquad M = \{\langle 0^n\, 1, 1\, 0^n\rangle \mid n \in N\};$$

J, K, L, M are all definable in GS.

(a) $u \in H \leftrightarrow u = u^c \wedge L(u)$.

(b) $u \in F \leftrightarrow \exists v[u = vv] \wedge J(u)$.

(c) $u \in G \leftrightarrow \exists v[u = v^c v] \wedge K(u)$.

(d) Let $f(x) = 2x$. Then
$G_f^\dagger(u, v) \leftrightarrow \exists w \exists x[\tau(w) \wedge \tau(x) \wedge db(w, x) \wedge u = r_0(w) \wedge v = r_0(x)]$.

(e) $u \in H \leftrightarrow L(u) \wedge \exists w \exists v[M(w, v) \wedge w \preccurlyeq u \wedge Part(v, u) \wedge$
$\forall s[s \prec u \rightarrow \sim Part(v, s)]]$.

(f) It is readily seen that *Part* is definable in $GS + Suffix$.

There are other consequences of Theorem 10 which, apparently, cannot be directly related to F, G, H. For example,

COROLLARY 9. *The theory resulting from GS by adjoining either of the following binary relations is undecidable.* (*a*) *$l(v)$ is the square* (*in the ordinary arithmetic sense*) *of $l(u)$.* (*b*) *square excess of $l(v)$ is $l(u)$.*

This follows at once from Corollaries 1 and 2 and Theorem 10.[6]

The great variety of extensions of GS which result in an undecidable theory might make one suspect that GS is *maximally decidable* in the sense that any relation not definable in GS when adjoined to GS results in an undecidable theory. However, this is not the case. Where P, Q, R are as in Theorem 4,

[6] Indeed one can establish the stronger result that concatenation is definable in the theory obtained by augmenting GS by (1) $G_f^\dagger$, where f is as in theorem 10, (2) H of corollary 7, (3) the predicates (a) through (f) of corollary 8 and (4) the predicates (a) and (b) of corollary 9. From a result of Quine [5], and the definability of concatenation in these theories, it follows that these theories are not even arithmetic and so, à fortiori, not recursively enumerable.

THEOREM 11. *Each of the theories obtained by adjoining to GS either the set $\{0^n \mid n \in P\}$ or $\{0^n \mid n \in Q\}$ or $\{0^n \mid n \in R\}$ is decidable.*

PROOF. By Theorem 5 and Corollary 6, $GS + \{0^{n+1} \mid n \in P\}$ is decidable from which the result quickly follows.

It has already been observed that P, Q, R are not definable in *WSS*. Hence the sets of Theorem 11 are not definable in *GS* (by Theorem 9).

At this point we wish to state in precise terms the problem concerning maximally decidable theories.

DEFINITION. Let $\mathfrak{M} = \langle N, f_1, \ldots, f_k\rangle$ be a structure where N is the set of non-negative integers and f_i, $1 \leqq i \leqq k$, are recursive functions of one or more variables. The first order theory $T = T(\mathfrak{M})$ is called *maximally* decidable if T is decidable but $T + P$ is undecidable for *every* predicate or function P on N which is not already definable in T.

PROBLEM. Does there exist any maximally undecidable theory T?

5. The EGS interpreted calculus.

It is natural to inquire whether there is a first order theory of infinite strings which is related to *SS* as *GS* is related to *WSS*. This led to the formulation of *EGS*. We do not, however, give a complete presentation analogous to section 4.

Let *EGS* be the first order interpreted calculus with equality having individual variables ranging over the set of all finite and one way infinite strings on the alphabet $\{0, 1\}$ and having non-logical constants $\mathbf{Eq}$, $\mathbf{R}_0$, $\mathbf{R}_1$, **Pref** which are interpreted as indicated below. The one way infinite strings may be identified with functions $f : N \to \{0, 1\}$.

(a) $\mathbf{Eq}(u, v)$ holds iff u and v are finite strings (words) of the same length.

(b) $\mathbf{R}_0(u, v)$ holds iff u and v are finite strings and $u = v0$.

(c) $\mathbf{R}_1(u, v)$ holds iff u and v are finite strings and $u = v1$.

(d) $\mathbf{Pref}(u, v)$ holds iff u is finite and for some w, $uw = v$.

Notice that *Pref* is anti-symmetric and transitive. Furthermore, $Pref(u, u)$ iff u is finite (iff $Eq(u, u)$) so that *GS* may be obtained from *EGS* by relativizing quantification with respect to $Pref(u, u)$. *SS* may be interpreted in *EGS* via the mapping which takes $x \in N$ into 0^x and a set M into $f_M : N \to \{0, 1\}$, where $f_M(x) = 1 \leftrightarrow x \in M$. *EGS* may be interpreted in *SS* via the mapping which takes a finite sequence u into $\{x + 1 \mid x \in \theta(u)\}$ and an infinite sequence $f : N \to \{0, 1\}$ into $\{x + 1 \mid f(x) = 1\} \cup \{0\}$. Using methods similar to those of section 4, one may prove for example:

THEOREM 12. *Each of the theories obtained by adjoining to EGS either the set $\{0^n \mid n \in P\}$ or $\{0^n \mid n \in Q\}$ or $\{0^n \mid n \in R\}$ is decidable.*

REFERENCES

[1] J. R. Büchi and C. C. Elgot, *Decision problems of weak second order arithmetics and finite automata, Part I,* (abstract), ***American Mathematical Society Notices,*** vol. 5 (1959), p. 834.

[2] J. R. Büchi, *Weak second order arithmetic and finite automata,* ***Zeitschrift für Mathematische Logik and Grundlagen der Mathematik,*** vol. 6 (1960), pp. 66–92.

[3] J. R. Büchi, *On a decision problem in restricted second order arithmetic,* ***Logic Methodology and Philosophy of Sciences, Proceedings of the 1960 International Congress,*** pp. 1–14.

[4] C. C. Elgot, *Decision problems of finite automata design and related arithmetics,* ***Transactions of the American Mathematical Society,*** vol. 98 (1961), pp. 21–51.

[5] Quine, W. V., *Concatenation as a basis of arithmetic,* this Journal, vol. 11 (1946) 105–114.

[6] M. O. Rabin and D. Scott, *Finite automata and their decision problems,* ***IBM Journal of Research and Development,*** vol. 3 (1959), pp. 114–125.

[7] J. Robinson, *General recursive functions,* ***Proceedings of the American Mathematical Society,*** vol. 1 (1950), pp. 703–718.

[8] R. M. Robinson, *Restricted set — theoretical definitions in arithmetic,* ***Proceedings of the American Mathematical Society,*** vol. 9 (1958), pp. 238–242.

IBM WATSON RESEARCH CENTER YORKTOWN HEIGHTS, NEW YORK
NEW YORK UNIVERSITY
HEBREW UNIVERSITY