DECISION PROBLEMS OF FINITE AUTOMATA DESIGN AND RELATED ARITHMETICS[1]

BY
CALVIN C. ELGOT

CHAPTER I. BACKGROUND

1. **Motivation.** Many variants of the notion of automaton have appeared in the literature. We find it convenient here to adopt the notion of E. F. Moore [7]. Inasmuch as Rabin-Scott [9] adopt this notion, too, it is convenient to refer to [9] for various results presumed here. In particular, Kleene's theorem [5, Theorems 3, 5] is used in the form in which it appears in [9]. It is often perspicacious to view regular expressions, and this notion is used in the sense of [3].

In general, we are concerned with the problems of automatically designing an automaton from a specification of a relation which is to hold between the automaton's input sequences and determined output sequences. These "design requirements" are given via a formula of some kind. The problems with which we are concerned have been described in [1]. With respect to particular formalisms for expressing "design requirements" as well as the notion of automaton itself, the problems are briefly and informally these: (1) to produce an algorithm which when it operates on an automaton and a design requirement produces the correct answer to the question "Does this automaton satisfy this design requirement?", or else show no such algorithm exists; (2) to produce an algorithm which operates on a design requirement and produces the correct answer to the question "Does there exist an automaton which satisfies this design requirement?", or else show no such algorithm exists; (3) to produce an algorithm which operates on a design requirement and terminates with an automaton which satisfies the requirement when one exists and otherwise fails to terminate, or else show no such algorithm exists.

Interrelationships among problems (1), (2), (3) will appear in the paper [1]. This paper will also indicate the close connection between problem (1) and decision problems for truth of sentences of certain arithmetics. The paper [1] will also make use of certain results concerning weak arithmetics already obtained in the literature to obtain answers to problems (1) and (3). Thus

Presented to the Society, January 21, 1959, under the title *Weak second order arithmetics of finite automata.* Preliminary report. I, II; received by the editors June 17, 1959.

[1] I wish to thank Drs. J. B. Wright and J. R. Büchi for stimulating and helpful discussions, my wife for typing and editing the manuscript of this thesis, and the following Federal agencies for financial support: National Science Foundation, Office of Naval Research, Office Ordnance Research, and the Signal Corps.

[1], in part, concerns applications of logic to automata theory. In the following pages, we shall give some applications of automata theory to logic. More particularly, we shall use automata theory to produce decision procedures for the truth of sentences of certain weak arithmetics.

Theorem 5.3 provides a uniform and surprisingly powerful technique for proving that various operations on sets of finite sequences preserve regularity.

2. Some basic notions.

Definition. (a) An I-automaton is a quadruple $\mathfrak{N}=\langle S, f, d, D\rangle$ where I is a finite nonempty set (the *input states* or the alphabet), S is a finite nonempty set (the *internal states*), f is a function, $f\colon I\times S\rightarrow S$ (the *transition function*), $d\in S$ (the *initial internal state*), and $D\subseteq S$ (D may be called the *output* of $\mathfrak{N}$).

(b) $T(\mathfrak{N})$ is the set of all sequences $(i_0, i_1, \cdots, i_{n-1})$, $n\geqq 0$, such that there is a sequence $(s_0, s_1, \cdots, s_n)$ satisfying:

$$f(i_k, s_k) = s_{k+1}, \quad 0 \leqq k \leqq n-1, s_k \in S, i_k \in I, \tag{1}$$

$$s_n \in D, \tag{2}$$

$$s_0 = d. \tag{3}$$

$T(\mathfrak{N})$ is the *set of tapes* [9] *accepted* by $\mathfrak{N}$ or the *behavior* of $\mathfrak{N}$. The null sequence $\Lambda\in T(\mathfrak{N})$ if and only if $d\in D$.

(c) $T(\mathfrak{N})$ may also be described as the set of all functions $i\colon \{0, 1, 2, \cdots, n-1\}\rightarrow I$, $n\geqq 0$ (the empty function is included) satisfying the formula: $\bigvee_s [s(0)=d\wedge s(n)\in D\wedge\bigwedge_{x<n} [(i(x), s(x))=c_1\supset s(x+1)=f(c_1)] \wedge[(i(x); s(x))=c_2\supset s(x+1)=f(c_2)]\wedge \cdots \wedge[(i(x), s(x))=c_m\supset s(x+1)=f(c_m)]]$ where $c_1, c_2, \cdots, c_m$ is an enumeration of all the elements of $I\times S$ (the *complete states* of the automaton).

3. Two characterizations of automata behavior.

Let V_I be the set of all finite sequences of elements of I (including the null sequence Λ). If $\alpha, \beta\subseteq V_I$, then $\alpha\cdot\beta$ is the subset of V_I obtained by concatenating a sequence from α with a sequence from β; $\alpha^*=\{\Lambda\}\cup\alpha\cup\alpha\cdot\alpha\cup\alpha\cdot\alpha\cdot\alpha\cup\cdots$. A subset of V_I is *I-regular* if and only if it is obtainable from $\varnothing$ and the unit sets, $\{a\}$, $a\in I$, by a finite number of applications of $\cup$, $\cdot$, $*$. Otherwise stated: The class of I-regular sets is the smallest class containing $\varnothing$, $\{a\}$, $a\in I$, and closed under $\cup$, $\cdot$, $*$. An I-regular expression is constructed out of symbols denoting each $\{a\}$, $a\in I$, $\varnothing$ (the empty set), and $\cup$, $\cdot$, $*$. [Note that $\varnothing^*=\{\Lambda\}$.] A set is *regular* if it is I-regular for some I. (Cf. [3, p. 182] and [9, p. 17].)

3.1. **Kleene's theorem.** If $\mathfrak{N}$ is an I-automaton, then $T(\mathfrak{N})$ is I-regular and an I-regular expression denoting $T(\mathfrak{N})$ may effectively be obtained. Conversely, if α is I-regular, then there exists an I-automaton such that $T(\mathfrak{N})=\alpha$ and, furthermore, $\mathfrak{N}$ may be effectively obtained from an I-regular expression denoting α.

The following statement is immediate from the definition of I-regular.

3.2. If α is I-regular and if $I\subseteq J$, then α is also J-regular.

3.3. The class of I-regular sets is closed with respect to union, intersection, complementation (with respect to V_I) (cf. [9, p. 17]).

3.4. The class of regular sets is closed with respect to symmetric difference, intersection. This follows from 3.2 and 3.3.

Let p be a mapping of I onto J. There is a unique homomorphism from the free semi-group F_I on I onto the free semi-group F_J on J which extends p. This homomorphism in turn induces a mapping $\hat{p}$ on subsets of F_I onto subsets of F_J. If α is a set of I-sequences, then $\hat{f}(\alpha)$ is a set of J-sequences, $\hat{f}$ is a *projection*, and $\hat{f}(\alpha)$ is a projection of α.

3.5. If α is regular and $\hat{p}$ is a projection, then $\hat{p}(\alpha)$ is regular.

Proof. Suppose α is I-regular and p: $I\rightarrow J$. If $a\in I$, then $\hat{p}\{a\} = \{p(a)\}$ is J-regular. Since $\hat{p}(\alpha\cdot\beta)=\hat{p}(\alpha)\cdot\hat{p}(\beta)$ and $\hat{p}(\alpha^*)=(\hat{p}(\alpha))^*$, the result follows.

(Medvedev [6, p. 13] gives a construction which, given an I-automaton $\mathfrak{M}$ and a p: $I\rightarrow J$, yields a J-automaton $\mathfrak{M}_p$ such that $T(\mathfrak{M}_p)=\hat{p}(T(\mathfrak{M}))$.)

From the point of view of regular expressions: the projection of a regular set is obtained by replacing each symbol $\mathbf{a}$ (denoting $\{a\}$) by $p(\mathbf{a})$ (denoting $\{p(a)\}$).

The following theorem strengthens a result of Medvedev [6, p. 11, Theorem 2].

3.6. Theorem. (1) *Every regular set is obtainable from a finite number of sets of the types*:

(a) V_A: *the set of all finite A-sequences* (*including the null sequence*) *where A is any finite set* (*nonempty*),

(b) $E_B(a, b)$: *the set of all sequences uabv where $a, b\in B$ and $u, v\in V_B$ and where B is any finite* (*nonempty*) *set, by a finite number of applications of symmetric difference, intersection, and projection.*

(2) *Each V_A, $E_B(a, b)$ is regular.*

Otherwise stated: *Given a regular set α there is a Boolean ring polynomial* (*in* $+$, $\cap$), *an assignment of sets chosen from* (a), (b), *and a projection $\hat{p}$ such that if* $+$, $\cap$ *are interpreted as symmetric difference and intersection respectively and if β is the set denoted by this polynomial under this assignment, then $\hat{p}(\beta)=\alpha$.*

Furthermore, if a regular expression is given which denotes α, then the polynomial, the assignment, and the projection may all effectively be determined.

Proof. (1) (i) If $A\cap B=\varnothing$, then $V_A\cap V_B=\{\Lambda\}$.

(ii) $V_A+\bigcup_{(a,b)\in A\times A} E_A(a, b)=\{\Lambda, a_1, a_2, \cdots, a_r\}$ where $\{a_1, a_2, \cdots, a_r\}=A$ and $\bigcup_{(a,b)\in A\times A} E_A(a, b)$ is equivalent to a polynomial in $+$, $\cap$ and the basic sets V_A, $E_A(a, b)$.

(iii) If $A\cap B=\{a\}$, then there is a polynomial in the basic sets equal to $\{a\}$.

(iv) If R is a binary relation over a finite set A, then a sequence $a_1a_2\cdots a_n$

is an *R-sequence* if and only if for each $i<n$, $(a_i, a_{i+1})\in R$. (Thus the sequences of length less than or equal to one are R-sequences.) The set of all R-sequences is equal to

$$V_A - [E_A(a_1, b_1) \cup E_A(a_2, b_2) \cup \cdots \cup E_A(a_r, b_r)]$$

where $\{(a_1, b_1), (a_2, b_2), \cdots, (a_r, b_r)\} = \overline{R} = (A \times A) - R$.

(v) Let $S_A(a) = \{au \mid a\in A \wedge u\in V_A\}$. Let R be a binary relation on $A \cup \{b\}, b \notin A$, viz., $[(x,y) \in R] \Leftrightarrow [(x = b \wedge y \in A) \vee (x \in A \wedge y \in A)]$ $\Leftrightarrow [y\in A \wedge (x=b \vee x\in A)]$. Then the set of R-sequences intersected with

$$\{b\} \cup \bigcup_{a\in A} E_{A\cup\{b\}}(a, b)$$

is the set M of R-sequences (of length >0) beginning with the letter "b." Now if $p: A\cup\{b\}\rightarrow A$ takes b into a and is the identity on A, then

$$\bar{p}(M) = S_A(a).$$

(vi) Let $T_A(a) = \{ua \mid a\in A \wedge u\in V_A\}$. Then $T_A(a)$ is expressible as the projection of a polynomial in the basic sets. The argument is analogous to (v).

Now let $\mathfrak{N} = \langle S, f, d, D\rangle$ be an I-automaton. Let R hold between complete states (i_1, s_1), (i_2, s_2) if and only if $f(i_2, s_1) = s_2$. Then the set of R-sequences beginning with (i, s) where $i\in I$ and $s = f(i, d)$ and terminating with an (i, s) such that $s\in D$ when projected by $\bar{p}$, where $p(i, s) = i$ for all $(i, s)\in I\times S$, yields $T(\mathfrak{N}) - \{\Lambda\}$. (Cf. the definition of $T(\mathfrak{N})$.)

Result (1) now follows from (i) through (vi).

(2) $V_A = A^*$; $E_B(a, b) = B^*\cdot\{a\}\cdot\{b\}\cdot B^*$ which shows V_A and $E_B(a, b)$ are regular. (Alternatively one may directly construct automata which accept tapes V_A, $E_B(a, b)$.)

Corollary. *If R is a binary relation over a set A, then the set of all R-sequences is regular.*

Proof. Follows from (iv), (2).

3.7. Theorem. *The class of all $T(\mathfrak{N})$, $\mathfrak{N}$ an automaton, is the smallest class of sets containing V_A, $E_B(a, b)$ (for every A, B, a, $b\in B$) and closed under symmetric difference, intersection, and projection.*

Proof. Immediate from 3.4, 3.5, 3.6.

3.8. Theorem. *Every set obtainable from the sets*

$$V_{A_1}, E_{A_2}(a, b), S_{A_3}(a), T_{A_4}(a)$$

by a finite number of applications of Boolean ring operations and projections is obtainable from the same sets by Boolean ring operations followed by a single projection (and these sets are exactly the regular sets).

Proof. Same as proof of 3.6.

CHAPTER II. TRUTH ALGORITHMS FOR CERTAIN ARITHMETICS

4. Truncation lemma.

DEFINITION. If u is a finite sequence, b is a letter, and, for some n, $u = vb^{(n)}$, (n iterations of b), $n \geqq 0$, and v does not terminate with b, then $u^b = v$. This is called *right truncation* of u by b. If α is a set of finite sequences, then $\alpha^b = \{u^b \mid u \in \alpha\}$ (right truncation of α by b). The meaning of *left truncation* is analogous.

Notice that $\Lambda \in \alpha^b$ if and only if $\{b\}^* \cap \alpha \neq \emptyset$.

4.1. LEMMA. (a) $(\alpha \cdot \beta)^b = \alpha \cdot (\beta^b - \{\Lambda\}) \cup \alpha^b \cdot (\beta^b - (\beta^b - \{\Lambda\}))$.
(b) $(\alpha^*)^b = \alpha^* \cdot (\alpha^b - \{\Lambda\}) \cup \{\Lambda\}$.

Proof. (a) Let $l(u)$ be the length of the finite sequence u. Let $p_b(u)$ mean u terminates with the letter b.

$$
\begin{aligned}
u \in (\alpha \cdot \beta)^b \Leftrightarrow & \bigvee_{n} [ub^{(n)} \in \alpha \cdot \beta \wedge n \geqq 0 \wedge \sim p_b(u)] \\
\Leftrightarrow & \bigvee_{n,u_1,u_2} [u_1u_2 = ub^{(n)} \wedge n \geqq 0 \wedge u_1 \in \alpha \wedge u_2 \in \beta \wedge \sim p_b(u)] \\
\Leftrightarrow & \bigvee_{n,u_1,u_2} [(u_1u_2 = ub^{(n)} \wedge n \geqq 0 \wedge u_1 \in \alpha \wedge u_2 \in \beta \\
& \wedge \sim p_b(u) \wedge l(u_2) > n) \\
& \vee (u_1u_2 = ub^{(n)} \wedge n \geqq 0 \wedge u_1 \in \alpha \wedge u_2 \in \beta \wedge \sim p_b(u) \\
& \wedge l(u_2) \leqq n)] \\
\Leftrightarrow & \bigvee_{u_1,u_2} [(u_1 \cdot \overset{b}{u_2} = u \wedge \overset{b}{u_2} \neq \Lambda \wedge u_1 \in \alpha \wedge u_2 \in \beta) \\
& \vee (u = \overset{b}{u_1} \wedge \overset{b}{u_2} = \Lambda \wedge u_1 \in \alpha \wedge u_2 \in \beta)] \\
\Leftrightarrow & \bigvee_{u_1,u_2} [(u = u_1 \cdot \overset{b}{u_2} \wedge u_1 \in \alpha \wedge u_2 \in \beta \wedge \overset{b}{u_2} \in \beta^{b} - \{\Lambda\}) \\
& \vee (u = \overset{b}{u_1} \wedge \overset{b}{u_2} \in (\beta^{b} - (\beta^{b} - \{\Lambda\})) \wedge u_1 \in \alpha \wedge u_2 \in \beta)].
\end{aligned}
$$

(b) $u \neq \Lambda \wedge u \in (\alpha^*)^b$

$$
\begin{aligned}
& \Leftrightarrow \bigvee_{n} [ub^{(n)} \in \alpha^* \wedge n \geqq 0 \wedge \sim p_b(u) \wedge u \neq \Lambda] \\
& \Leftrightarrow \bigvee_{n,r,u_1,u_2,\cdots,u_r} [n \geqq 0 \wedge r > 0 \wedge u_1u_2 \cdots u_r \\
& = ub^{(n)} \wedge \bigwedge_{1 \leqq i \leqq r} u_i \in \alpha \wedge \sim p_b(u) \wedge u \neq \Lambda] \\
& \Leftrightarrow \bigvee_{m,u_1,u_2,\cdots,u_m} \left[m > 0 \wedge u = u_1u_2 \cdots u_{m-1} \cdot \overset{b}{u_m} \wedge \overset{b}{u_m} \neq \Lambda \wedge \bigwedge_{1 \leqq i \leqq r} u_i \in \alpha \right] \\
& \Leftrightarrow u \in \alpha^* \cdot (\alpha^b - \{\Lambda\}).
\end{aligned}
$$

4.2. LEMMA. *The class of regular sets is closed under right truncation. Moreover, from a regular expression denoting α one can obtain effectively a regular expression denoting α^b. Analogous statements hold for left truncation.*

Proof. If x is a letter, then $\{x\}^b=\{x\}$ if $b\neq x$ and $\{x\}^b=\{\Lambda\}$ if $b=x$. The result for right truncation now follows by 4.1. The result for left truncation follows from this and the fact that the class of regular sets is closed under conversion (reversing the order of the sequences) (cf. [9, p. 17]).

5. **Characterization of automata behavior via a formal arithmetic.** Let L_1 be the class of formulas constructed out of

$$\text{(a)} \qquad x_i \in F_j,\ x_i' \in F_j,\ \cdots,\ x_i^{(r)} \in F_j,\ \cdots; \qquad i, j = 1, 2, 3, \cdots,$$

$$\text{(b)} \qquad x = y,\ x < y,$$

by means of propositional connectives and quantifiers $\bigvee_{x_i}$, $\bigvee_{F_j}$. The x_i are individual variables, the F_j set variables, and x_i' is interpreted as the successor of x_i.

5.1. Let the individual variables of L_1 range over the natural numbers and the set variables range over finite sets of natural numbers. Call the system consisting of the class of formulas L_1 and this interpretation L_1^1. If $A[F_1, F_2, \cdots, F_r]$, $r\geqq 0$, is a formula in which at most the variables $F_1, F_2, \cdots, F_r$ (the first r set variables in the alphabet of L_1) occur free, then associated with A is the class of r-tuples $(F_1, F_2, \cdots, F_r)$ of finite sets for which $A[F_1, F_2, \cdots, F_r]$ is true. Alternatively we may associate with such a formula a function f on the natural numbers with values which are (column) r-tuples of zeros and ones (i.e., an $r\times\infty$ matrix) as follows:

$$f(n) = \begin{pmatrix} a_1 \\ \cdot \\ \cdot \\ \cdot \\ a_r \end{pmatrix} \text{ if and only if } n \in F_i \equiv a_i = 1.$$

If $x=\max(F_1\cup F_2\cup \cdots \cup F_r)$ and $y>x$, then $f(y)$ is the r-tuple of all zeros. Let σ_r be the restriction of f to the domain $\{0, 1, 2, \cdots, x\}$; σ_r may be identified with the $r\times(x+1)$ matrix whose ith column is $f(i)$. Moreover σ_r is a 1-1 correspondence between all $r\times\infty$ matrices of zeros and ones whose columns are ultimately zero and remain zero and all those $r\times s$ matrices of zeros and ones, $s\geqq 0$, whose last (rightmost) column is not the all zero r-tuple. Call these $r\times s$ matrices *admissible*. (The matrix with zero columns is admissible.) Thus with each formula A of L_1^1 is associated a set $T_r(A)$ of admissible $r\times s$ matrices, $s\geqq 0$, where A is a formula without free individual variables and the number of free set variables is less than or equal to r. [If $r=0$, let $T_r(A)=\{\Lambda\}$ if A is true and $T_r(A)=\varnothing$ if A is false.] Let U_r be the set of all r-tuples of zeros and ones, $r\geqq 0$; let $U_r^0=U_r-\{0_r\}$ where 0_r is the all zero r-tuple. [If $r=0$, let $U_r=\{0\}$, $U_r^0=\varnothing$. Recall that $V_\phi=\varnothing^*=\{\Lambda\}$.]

5.2. Notice that in L_1^1:

$$x = y \Leftrightarrow \bigwedge_F (x \in F \equiv y \in F),$$

$$x = 0 \Leftrightarrow \bigwedge_y \sim y' = x,$$

$$x < y \Leftrightarrow \bigvee_F \left[\bigwedge_z (z' \in F \supset z \in F) \wedge x \in F \wedge y \notin F \right].$$

5.3. Theorem. (a) *If $A[F_1, F_2, \cdots, F_r]$ is a formula of L_1^1, then $T_r(A)$ is U_r-regular and one can effectively find a regular expression which denotes $T_r(A)$.*

(b) *For every regular set $\alpha \subseteq V_{U_r}$ of admissible sequences there is a formula $E(A)$ of L_1^1 such that $T_r(E(A)) = \alpha$, where E is a string of existential set quantifiers, A is free of set quantifiers, and the only terms in A are of the form x, x'.*

Corollary. *Let α be an arbitrary I-regular set. Let p be a* 1-1 *mapping of I into U_r^0. Then $\hat{p}(\alpha)$ is a U_r^0-regular set ("isomorphic" to α, i.e., the set is α in coded form) and so there is a formula A of L_1^1 such that $T_r(A) = \hat{p}(\alpha)$.*

Remark. It will be convenient to abbreviate formulas of L_1^1 by replacing an r-tuple of finite set variables by a function variable interpreted as having as its domain the naturel numbers and range an element of U_r and satisfying $(f(x))_i = 1 \Leftrightarrow x \in F_i$ as well as the property $\bigvee_x f(x) = 0_r \wedge \bigwedge_y (y > x \supset f(y) = 0_r)$, where 0_r is the r-tuple of all zeros, so that any such function is associated with a finite sequence of elements of U_r.

If f abbreviates $(F_1, F_2, \cdots, F_r)$, then $\bigvee_f$ abbreviates $\bigvee_{F_1} \bigvee_{F_2} \cdots \bigvee_{F_r}$.

5.4. Lemma[2]. *Every formula $A[F_1, F_2, \cdots, F_r]$ of L_1^1 is equivalent to a formula $B[F_1, \cdots, F_r]$ of L_1^1 in prenex form and such that every individual quantifier occurs to the right of every set quantifier.*

Proof. Observe that

$$\begin{aligned} \bigvee_x \bigwedge_F C &\equiv \bigvee_G \bigwedge_F \bigwedge_x \left[(G(x) \supset C) \wedge \bigvee_z G(z) \right] \\ &\equiv \bigvee_G \bigwedge_F \bigwedge_x C_1 \end{aligned} \tag{1}$$

and

$$\begin{aligned} \bigwedge_x \bigvee_F C &\equiv \bigwedge_G \bigvee_F \bigvee_x \left[\bigvee_z G(z) \supset G(x) \wedge C \right] \\ &\equiv \bigwedge_G \bigvee_F \bigvee_x C_1, \end{aligned} \tag{2}$$

[2] This was pointed out to me by J. R. Büchi.

where G is a set variable not occurring free in C.

Assume $A[F_1, F_2, \cdots, F_r]$ has the property that every set quantifier has as its scope the entire formula to the right of it.

Notice that in applying (1) or (2) to A the number of set quantifiers to the right of the x-quantifier is reduced by one. Thus, if $\bigvee_x$ $[\bigwedge_x]$ is the rightmost individual quantifier which has set quantifiers to the right of it, by iterating (1) and (2) a finite number of times one obtains a formula A' in which the x-quantifier appears to the right of all set quantifiers. Moreover, the number of individual quantifiers with set quantifiers to the right is one less in A' than in A. Thus one ultimately obtains a formula B equivalent to A and having the desired properties.

5.5. A formula of the form

$$\bigvee_x [x^{(m_0)}\eta F_{k_0} \wedge x^{(m_1)}\eta F_{k_1} \wedge \cdots \wedge x^{(m_r)}\eta F_{k_r}],$$

where each occurrence of η is independently $\in$ or $\notin$, will be called a ***principal formula*** where $0 \leqq m_0 < m_1 < \cdots < m_r$.

Call a formula ***normal*** if it is a disjunction of conjunctions of (1) principal formulas, (2) atomic formulas, (3) negations of (1) or (2).

LEMMA 1. *Every formula of L_1^1 is equivalent to a formula of L_1^1 of the form $Q[M]$ where Q is a string of set quantifiers and M is a disjunction of conjunctions of principal formulas and negations of principal formulas. [By appropriately permuting $F_1, F_2, \cdots, F_r$ in the given formula, the variables in Q may be assumed to appear in alphabetical order terminating with F_r.]*

Proof. In view of 5.2, it may be assumed that the given formula contains atomic parts 5(a) only. Suppose A is normal.

(a) Then $\sim A$ is equivalent to a normal formula (with the same free variables).

(b) Consider $\bigvee_x A$. $\bigvee_x$ distributes over the disjuncts of A. Let D be a disjunct of the form $D_1(x) \wedge D_2$ where x does not occur free in D_2 and no variable other than x occurs free in D_1. Then $\bigvee_x D \equiv D_2 \wedge \bigvee_x D_1(x)$.

Starting with a formula $B[F_1, F_2, \cdots, F_r]$ of Lemma 5.4 one makes use of (a) and (b) until all the individual quantifiers are "moved in." This yields a formula of the desired form.

LEMMA 2. *The set of all admissible sequences in V_{U_r} is $U_r^* \cdot U_r^0 \cup \{\Lambda\}$ and is, therefore, regular.*

5.6. **Proof of** 5.3 (a). Consider a formula of L_1^1 of the form $Q[M]$ of Lemma 1 of 5.5 with free set variables $F_1, F_2, \cdots, F_r$. Assume that it is known that if A is a principal formula then $T_r(A)$ is regular, and that from A, a regular expression denoting $T_r(A)$ may be effectively obtained. Then since

$$\begin{aligned} T_r(A \wedge B) &= T_r(A) \cap T_r(B), \\ T_r(A \vee B) &= T_r(A) \cup T_r(B), \\ T_r(\sim A) &= \text{compl } T_r(A) \end{aligned}$$

[complementation is with respect to the set of all admissible sequences in V_{U_r} (which is regular)] for A and B any formulas of L_1 without free individual variables, it follows then $T_r(M)$ is regular and a regular expression denoting it is effectively obtainable.

Now if $A = A[F_1, F_2, \cdots, F_r]$, $r > 1$, then $T_{r-1}(\bigvee_{F_r} A)$ is the set obtainable from $T_r(A)$ by deleting the rth row followed by right truncation of the all zero $(r-1)$-tuple, i.e., if $r > 1$

$$T_{r-1}\left(\bigvee_{F_r} A\right) = (\hat{p}_r(T_r(A)))^b$$

where p_r maps an r-tuple of zeros and ones onto the $(r-1)$-tuple obtained by deleting the rth component and b is the all zero $(r-1)$-tuple. Hence $T_{r-1}(\bigvee_{F_r} A)$ is regular and from a regular expression for $T_r(A)$ one may effectively obtain one for $T_{r-1}(\bigvee_{F_r} A)$.

It remains only to show that $T_r(A)$ is regular for A a principal formula. To simplify the exposition we point out that the principal formulas can, without loss of generality, be taken to be of the form

$$\bigvee_x \bigwedge_{1 \leq i \leq r} (x\eta F_i \wedge x'\eta F_i), \tag{1}$$

where each occurrence of η is independently $\in$ or $\notin$. This follows from the fact that (assuming $m > 1$)

$$\begin{aligned} x^{(m)}\eta F &\Leftrightarrow y_1 = x' \wedge y_2 = y_1' \wedge \cdots \wedge y_{m-1} = y_{m-2}' \wedge y'_{m-1}\eta F \\ &\Leftrightarrow \bigwedge_G [y_1 \in G \equiv x' \in G \wedge y_2 \in G \equiv y_1' \in G \wedge \cdots \\ &\qquad \wedge y_{m-1} \in G \equiv y_{m-2}' \in G \wedge y_{m-1}'\eta F] \end{aligned}$$

and

$$\begin{aligned} x\eta F &\Leftrightarrow (x\eta F \wedge x' \in F) \vee (x\eta F \wedge x' \notin F), \\ x'\eta F &\Leftrightarrow (x \in F \wedge x'\eta F) \vee (x \notin F \wedge x'\eta F). \end{aligned}$$

Let A be $\bigvee_x [f(x) = a \wedge f(x') = b]$ (cf. Remark 5.3).

CASE I. $a \in U_r$ and $b \in U_r^0$. Then

$$T_r(A) = U_r^* \cdot \{a\} \cdot \{b\} \cdot ((U_r^* \cdot \overset{0}{U_r}) \vee \{\Lambda\}).$$

CASE II. $a \in U_r^0$ and $b = 0_r$. Then

$$T_r(A) = (U_r^* \cdot \{a\}) \cup (U_r^* \cdot \{a\} \cdot \{b\} \cdot U_r^* \cdot \overset{0}{U_r}).$$

Case III. $a=0_r=b$. Then

$$T_r(A) = (U_r^*\cdot \overset{0}{U_r}) \vee \{\Lambda\}.$$

5.7. **Proof of** 5.3 (b). Let $\alpha\subseteq V_{U_r}$ be a regular set of admissible sequences. Then $\alpha-\{\Lambda\}$ is regular and is a projection of a regular set $\beta\subseteq V_{U^0_{r+s}}$, $s>0$. Specifically: there exists a U_r-automaton $\mathfrak{N}=\langle S, f, d, D\rangle$ such that $\alpha=T(\mathfrak{N})$. Without loss of generality, let S be a subset of U^0_s for a suitable $s>0$. The complete states $U_r\times S$ of $\mathfrak{N}$ may be identified with a subset of U^0_{r+s} as follows: $\langle x, y\rangle\in U_r\times S$ is identified with the $(r+s)$-tuple whose ith member, $1\leqq i\leqq r$, is the ith member of x and whose $(r+j)$th member, $1\leqq j\leqq s$, is the jth member of y. Let $B\subseteq U^0_{r+s}$ be the set $\{\langle x, f(x, d)\rangle \mid x\in U_r\}$. Let $E=U^0_r\times D$. Define $R\subseteq U^0_{r+s}\times U^0_{r+s}$ as follows: $\langle\langle x_1, y_1\rangle, \langle x_2, y_2\rangle\rangle\in R$ if and only if $f(x_2, y_1)=y_2$. Then β is the set of finite R-sequences beginning with an element of B and ending with an element of E and $\alpha=\hat{p}(\beta)$ where p is the mapping which takes $\langle x, y\rangle\in U_r\times S$ into x.

β is the intersection of the three following sets.

(a) $\bigcup_{a\in B} S_{U_{r+s}}(a)$, $B\subseteq U^0_{r+s}$ (those elements of $V_{U_{r+s}}$ beginning with an element of B).

(b) $\bigcup_{a\in E} W_{U_{r+s}}(a)$, $E=U^0_r\times D$ (those elements of $V_{U_{r+s}}$ terminating with an element of E).

(c) The set of all R-sequences, $R\subseteq U^0_{r+s}\times U^0_{r+s}$.

We now obtain formulas "corresponding" to (a), (b), (c).

a) Let $B=\{b^1, b^2, \cdots, b^n\}$. b^i_k is the kth component of b^i. For each b^i the formula A^i: $\bigwedge_{1\leq k\leq r+s} 0\eta_k F_k$, where η_k is $\in$ if $b^i_k=1$ and η_k is $\notin$ otherwise, corresponds to $S_{U_{r+s}}(b^i)$, so that (a) corresponds to $A^1\vee A^2\vee\cdots\vee A^n$. Then $A^1\vee A^2\vee\cdots\vee A^n$ is an abbreviation of a formula A of L^1_1 and

$$T_{r+s}(A) = \bigcup_{a\in B} S_{U_{r+s}}(a).$$

b) Let $E=\{e^1, e^2, \cdots, e^n\}$. With each e^i associate the formula

$$A^i\colon\ \bigvee_x \left[\bigwedge_{1\leq k\leq r+s} x\eta_k F_k \wedge \bigwedge_y (y > x \supset (y\notin F_1 \wedge y\notin F_2 \wedge \cdots \wedge y\notin F_{r+s}))\right]$$

where η_k is $\in$ if $e^i_k=1$ and otherwise η is $\notin$. Then $A^1\vee A^2\vee\cdots\vee A^n$ is an abbreviation of a formula A of L^1_1 and

$$T_{r+s}(A) = \bigcup_{a\in E} W_{U_{r+s}}(a).$$

c) Let $H=R\cup(U_{r+s}\times\{z\})$ where z is the all zero $(r+s)$-tuple. Let $\{(e^1,f^1), (e^2,f^2), \cdots, (e^n,f^n)\}=H$. With each e^i associate $A(e^i)\colon \bigwedge_{1\leq k\leq r+s} x\eta_k F_k$ where η_k is $\in$ or $\notin$ depending on whether $e^i_k=1$ or not. With each f^i associate $B(f^i)\colon \bigwedge_{1\leq k\leq r+s} x'\eta_k F_k$ where η_k is $\in$ or $\notin$ depending on whether $f^i_k=1$ or not. Then if A is the formula abbreviated by $\bigwedge_x \bigvee_{1\leq i\leq n} A(e^i)\wedge B(f^i)$, then $T_{r+s}(A)$ is the set (c).

If $\mathfrak{F}$ is the conjunction of the formulas a), b), c), then $T_{r+s}(\mathfrak{F})=\beta$ and $T_r(\bigvee_{F_{r+1}} \bigvee_{F_{r+2}} \cdots \bigvee_{F_{r+s}} \mathfrak{F})=\alpha$.

Note that $\{\Lambda\}=T_1(\bigwedge_x x\notin F)$.

5.8. Corollary to 5.3 (a)[3]. Ehrenfeucht's theorem (*unpublished*). *The set of true sentences of L_1^1 is effective.*

Proof. It may be assumed (5.4) that the given sentence is of the form

$$\text{(a)} \qquad \bigvee_F A[F]$$

or

$$\text{(b)} \qquad \sim \bigvee_F A[F]$$

where A is a formula in which at most the set variable F occurs free. Then (a) is true if and only if $T_1(A[F])$ is nonempty, and (b) is true if and only if $T_1(A[F])$ is empty. $T_1(A[F])$ is empty if and only if $T_0(\bigvee_F A[F])$ is empty.

Thus, one can effectively find an automaton $\mathfrak{N}=\langle S, f, d, D\rangle$ with one input state (sometimes called an input-free automaton or autonomous automaton) which represents (a) (or (b)).

If the automaton has n internal states, then the (unique) input sequence of length n will determine a sequence of internal states starting with d of length $n+1$. At least one internal state must occur more than once in this sequence so that $T_0(\mathfrak{N})$ is nonempty if and only if an $s\in D$ occurs in this sequence.

5.9. For each finite set F of natural numbers let $\tau(F)=\sum_{x\in F} 2^x$. Then τ is a 1-1 correspondence between the class of all finite subsets of the natural numbers and the natural numbers.

$$\begin{aligned}\tau(G) = \tau(F_1) + \tau(F_2) \Leftrightarrow \bigvee_C \, [0 \notin C \wedge (0 \in G \equiv 0 \in F_1 \triangle 0 \in F_2) \\ \wedge \bigwedge_x (x' \in C \equiv (x \in F_1 \wedge x \in F_2) \vee (x \in F_1 \wedge x \in C) \\ \vee (x \in F_2 \wedge x \in C) \cdot \triangle \cdot x' \in G \\ \equiv (x \in F_1 \triangle x \in F_2 \triangle x \in C))]\end{aligned}$$

where $\triangle$ represents "exclusive or". Thus:

Corollary[4]. (1) *The first order theory of addition of natural numbers is decidable.* (2) *Furthermore, for any relation $A[x_1, x_2, \cdots, x_r]$ in the first order theory of natural numbers there is a formula $B[F_1, F_2, \cdots, F_r]$ such that $A[x_1, x_2, \cdots, x_r]\Leftrightarrow B[\tau^{-1}x_1, \tau^{-1}x_2, \cdots, \tau^{-1}x_r]$.*

[3] This result has been obtained independently by J. R. Büchi.

[4] This was suggested by J. R. Büchi.

Statement (1) with "natural numbers" replaced by "integers" was established by Presburger; statement (1) itself was established by Hilbert and Bernays. The proof of (1) indicated here appears to be simpler than either of the two proofs mentioned, both of which make use of the theory of congruences.

5.10. For each n, $n \geqq 1$, consider the 2^{2n} n-place predicates

$$\bigvee_x [x\eta F_1 \wedge x\eta F_2 \wedge \cdots \wedge x\eta F_n \wedge x'\eta F_1 \wedge x'\eta F_2 \wedge \cdots \wedge x'\eta F_n]$$

where each occurrence of η is independently replaced by $\in$ or $\notin$. Call the class of all these predicates $\mathcal{P}$. Then every first order formula in $\mathcal{P}$ is equivalent to one in L_1^1 (without free individual variables) and vice versa. Let $\tau\mathcal{P}$ be the class of predicates $A[\tau F_1, \tau F_2, \cdots, \tau F_r]$ defined to hold if and only if $A[F_1, F_2, \cdots, F_r]$ holds and $A[F_1, F_2, \cdots, F_r]$ is a predicate of $\mathcal{P}$. Then:

Corollary. *The first order arithmetic theory based upon $\tau\mathcal{P}$ is decidable and this theory strictly contains the elementary theory of addition of natural numbers in the sense that while addition is definable in the theory of $\tau\mathcal{P}$, not every predicate in $\tau\mathcal{P}$ is definable in the first order theory of addition.*

Proof. $\tau\{\bigvee_x [x\in F \wedge x'\in F \wedge \bigwedge_y y\in F \supset (y=x \vee y=x')]\}$ is the set 3, 6, 12, 24, $\cdots$, i.e., the set $\{3\times 2^n\}_{n\geq 0}$. This set is not definable in the first order theory based upon $+$ because the sets definable in this latter theory are exactly those whose characteristic function is ultimately periodic while the set $\{3\times 2^n\}_{n\geq 0}$ does not have this property. (Cf. [4, last paragraph, §3].) The rest of the argument is contained in 5.9.

5.11. Corollary 1. *The first order theory of finite sets of natural numbers based upon $\cap$, $\oplus$ (symmetric difference), $\varnothing$, $=$, and the unary operation $F \rightarrow F^s$ defined by*

$$x \in F^s \text{ if and only if } \bigvee_y x \leqq y \wedge y \in F$$

is decidable. Furthermore, the relations on finite sets definable in L_1^1 are exactly the same as those definable in this theory.

Proof. The operation $\cap$, $\oplus$, ^{s} and the relations $F=G$ and $F=\varnothing$ are definable in L_1^1.

The principal formula $\bigvee_x [x\in G_1 \wedge x'\in G_1 \wedge x\notin G_2 \wedge x'\in G_2]$ has as its counterpart in this new theory the formula (i.e., the set of ordered pairs of finite sets defined by this formula is the same as that given by the formula below):

$$\begin{aligned}\bigvee_{F_1,F_2,F_3} \{F_1 = F_1^s \wedge F_2 = F_2^s \wedge F_3 = F_3^s \wedge F_1 \subset F_2 \subset F_3 \\ \wedge \bigwedge_{G_3} [(G - G^s \wedge F_1 \subset G \cdot\supset\cdot F_2 \subseteq G) \wedge (G = G^s \wedge F_2 \subset G \cdot\supset\cdot F_3 \subseteq G)] \\ \wedge F_3 \oplus F_1 \subseteq G_1 \wedge F_3 \oplus F_2 \subseteq G_2 \wedge (F_2 \oplus F_1) \cap G_2 = \varnothing\}.\end{aligned}$$

Similarly for other principal formulas.

The unary operation $F \rightarrow F^s$ may be replaced by the property $F = F^s$ without changing the strength of the system.

COROLLARY 2. *The first order theory of natural numbers based upon* $\tau(\cap)$, $\tau(\oplus)$, $=$, $+$, *and the property* $P(n)$ *of being of a power of* 2 *is decidable where*

$$x\tau(\cap)y = z \Leftrightarrow \tau^{-1}x \cap \tau^{-1}y = \tau^{-1}z,$$

$$x\tau(\oplus)y = z \Leftrightarrow \tau^{-1}x \oplus \tau^{-1}y = \tau^{-1}z.$$

Notice that $P(n) \Leftrightarrow \tau^{-1}n$ is a unit set and the property of being a unit set is definable in L_1^1.

Note, too, that we have, in particular, a proper strengthening of Presburger's result, viz., the first order theory of natural numbers based upon addition and the property of being a power of two is decidable and the property of being a power of two is not definable in the Presburger system.

5.12. Let L_1^2 be the system consisting of the formulas L_1 with individual variables interpreted as ranging over integers rather than natural numbers and set variables ranging over finite sets of integers.

LEMMA. *For each formula* $A[F_1, F_2, \cdots, F_r]$ *of* L_1^2 *and for each integer* l, $A[F_1, F_2, \cdots, F_r] \equiv A[F_1^l, F_2^l, \cdots, F_r^l]$ *where* $x \in F_i^l \Leftrightarrow x - l \in F_i$, *i.e., the class of r-tuples of finite sets defined by a formula of* L_1^2 *is closed under translation* (*cf.* 5.13).

Lemma 1 of 5.5 is valid for L_1^2. Let R_r be the relation between two r-tuples of finite sets that one is a translate of the other. Each R_r-equivalence class is included in $A[F_1, F_2, \cdots, F_r]$ or in $\sim A[F_1, F_2, \cdots, F_r]$ for every formula A for this is true for principal formulas and is preserved by the Boolean operations and projection.

Analogous to 5.1 and in view of the lemma one may associate with $A[F_1, F_2, \cdots, F_r]$ of L_1^2 a set $T_r^2(A[F_1, F_2, \cdots, F_r])$ of admissible-2 matrices, an admissible-2 matrix being a finite sequence of r-tuples of zeros and ones which neither begins nor terminates with the all zero r-tuple. Analogous to the proof of 5.3 one may establish the following theorem.

THEOREM. (a) *If* $A[F_1, F_2, \cdots, F_r]$ *is a formula of* L_1^2, *then* $T_r^2(A)$ *is* U_r-*regular and one can effectively find a regular expression which denotes* $T_r^2(A)$.

(b) *For every regular set* α *of admissible*-2 U_r-*sequences there is a formula* $E(A)$ *of* L_1^2 *such that* $T_r^2(E(A)) = \alpha$ *where* E *is a string of existential set quantifiers and the only terms in* A *are of the form* x, x'.

COROLLARY TO (a). *There is a decision procedure for the truth of sentences of* L_1^2.

5.13. In L_1^2:

$$x = y \Leftrightarrow \bigwedge_{F} (x \in F \equiv y \in F),$$

$$x < y \Leftrightarrow \bigwedge_{F,z} [(z \in F \wedge z \neq x \cdot \supset \cdot z' \in F) \supset y \notin F].$$

However, $x=0$ is not definable in L_1^2 by virtue of the lemma of 5.12. Compare with 5.2.

5.14. Let A be an arbitrary finite set. A sequence of V_A is *admissible-3* if and only if (1) it is of length one or (2) it is of length greater than one and the last two elements of the sequence are distinct.

LEMMA 1. *The set of all admissible-3 sequences in V_A is A-regular.*

Proof. Identify elements of A with sequences of length one. The set of all admissible-3 sequences is:

$$A \cup \bigcup_{b \in A} V_A \cdot (A - \{b\}) \cdot b.$$

DEFINITION. If $\alpha \subseteq V_A$ and $b \in A$, then $\alpha^{\cdot b}$ (modified truncation by b) is defined as follows: $v \in \alpha^{\cdot b}$ if and only if

(1) $v \in \alpha$ and v does not terminate with b, or

(2) there exists $u \in \alpha$ which terminates with b and if $wbb \cdots b = u$ and w does not terminate with b, then $v = wb$.

LEMMA 2. *If $\alpha \subseteq V_A$ is A-regular and $b \in A$, then $\alpha^{\cdot b}$ is A-regular.*

Proof. Cf. Corollary 5.3 and remark. Without loss of generality assume that $A = U_r^0$ for appropriate r. There is a formula $\mathfrak{F}[f]$ such that $T_r\mathfrak{F} = \alpha$. It is sufficient to prove the theorem for $\Lambda \notin \alpha$. Then $f(x) = 0_r \supset x > 0$. Let $\mathfrak{G}[g]$ be the formula:

$$\bigvee_{f} \bigwedge_{y} \Big\{ \mathfrak{F}[f] \wedge f(y') = 0_r \wedge f(y) \neq 0_r : \supset : \Big[f(y) \neq b \supset \bigwedge_{x} f(x) = g(x) \Big]$$
$$\wedge \Big[f(y) = b \supset \bigwedge_{x} \Big[f(x) = b \wedge \Big(\bigvee_{z} z' = x \supset f(z) \neq b \Big) \Big)$$
$$\wedge \Big(\bigwedge_{z} z \geqq x \cdot \supset \cdot f(x) = b \vee f(z) = 0_r \Big) \cdot \supset \cdot \bigwedge_{w \leqq x} (g(w) = f(w)) \wedge \bigwedge_{w > x} g(w) = 0 \Big] \Big] \Big\}.$$

Then $T_r\mathfrak{G} = \alpha^{\cdot b}$. By Theorem 5.3 (a), $\alpha^{\cdot b}$ is regular.

5.15. By a *quasi-finite* set of natural numbers (integers) is meant a set which is finite or whose complement is finite. Let L_1^3 be the system consisting of the set of formulas L_1 with individual variables interpreted over the natural numbers and set variables interpreted over quasi-finite sets of natural numbers. Let $F_1, F_2, \cdots, F_r$ be quasi-finite sets. Let $c_k(n) = 1 \Leftrightarrow n \in F_k$. Let

$$c(n) = \begin{Bmatrix} c_1(n) \\ c_2(n) \\ \cdot \\ \cdot \\ \cdot \\ c_r(n) \end{Bmatrix}.$$

Thus, with each r-tuple of finite sets of natural numbers is associated $c \in U_r^N$ (N is the set of non-negative integers). Because the F_k are quasi-finite, there exists $x \in N$ such that $\bigwedge_y y > x \supset c(y) = c(x)$. The function c restricted to the first x such that this property holds is an element $\sigma_r^3(F_1, F_2, \cdots, F_r)$ of V_{U_r}. Moreover, c is 1-1. Briefly: $\sigma_r^3(F_1, F_2, \cdots, F_r) = f$ where domain $f = \{x \mid x \leqq y\}$ and $y = (\mu z) \bigwedge_i [\bigwedge_x x \geqq z \supset x \in F_i \cdot \vee \cdot \bigwedge_x x \geqq z \supset x \notin F_i]$ and if $x \leqq y$ then $(f(x))_i = 1 \Leftrightarrow x \in F_i$ and $\bigvee_z z > y \supset f(y) = f(z)$. The image of σ_r^3 is the set of all admissible-3 elements of V_{U_r}. If $A[F_1, F_2, \cdots, F_r]$ is a formula of L_1^3, then $T_r^3(A)$ is the set of all $\sigma_r^3(F_1, F_2, \cdots, F_r)$ such that $A[F_1, F_2, \cdots, F_r]$ holds.

Notice that 5.2 holds in L_1^3.

THEOREM. (a) *If $A[F_1, F_2, \cdots, F_r]$ is a formula of L_1^3, then $T_r^3(A)$ is U_r-regular and one can effectively find a regular expression which denotes it.*

(b) *For every regular set $\alpha \subseteq V_{U_r}$ of admissible-3 sequences there is a formula $E(A)$ of L_1^3 such that $T_r^3(E(A)) = \alpha$ where E is a string of existential set quantifiers, A is free of set quantifiers, and the only terms in A are of the form x, x'.*

Proof. (a) The proof is analogous to 5.6. Lemma 1 of 5.5 holds with "L_1^{3}" in place of "L_1^1". If A, B are formulas of L_1^3 with at most $F_1, F_2, \cdots, F_r$ free, then

$$T_r^3(A \wedge B) = T_r^3(A) \cap T_r^3(B),$$

$$T_r^3(A \vee B) = T_r^3(A) \cup T_r^3(B),$$

$$T_r^3(\sim A) = \text{compl } T_r^3(A)$$

where complementation is with respect to the set of all admissible-3 sequences of V_{U_r} (cf. 5.14, Lemma 1).

If $\alpha = T_r^3(A)$, then $T_{r-1}^3(\bigvee_{F_r}(A)) = (\cdots(((\hat{p}(\alpha))^{\cdot a})^{\cdot b})\cdots)$ where p maps an element of U_r into the element obtained by deleting the rth component and $a, b, \cdots$ is an enumeration of the elements of U_{r-1}. Since regularity is preserved by projection and modified right truncation (Lemma 2, 5.14) it follows that $T_{r-1}^3(\bigvee_{F_r} A)$ is regular.

It remains only to show that if A is $\bigvee_x [f(x) = a \wedge f(x') = b]$, then $T_r^3(A)$ is regular, where f abbreviates $(F_1, F_2, \cdots, F_r)$ (cf. 5.3). Let

$$\beta = \bigcup_{c \neq d;\, c,d \in U_r} (U_r^* \cdot \{a\} \cdot \{b\} \cdot U_r^* \cdot \{c\} \cdot \{d\}) \cup \bigcup_{c \neq b;\, c \in U_r} U_r^* \cdot \{a\} \cdot \{b\} \cdot \{c\}.$$

Then β is regular. If $a \neq b$, then $T_r^3(A) = \beta \cup (U_r^* \cdot \{a\} \cdot \{b\})$ while if $a = b$, then $T_r^3(A) = \beta \cup (U_r^* \cdot U_r - \{a\} \cdot \{a\}) \cup \{a\}$. Then $T_r^3(A)$ is regular and the proof is completed.

(b) Let $\alpha \subseteq U_r^*$ be a regular set of admissible-3 sequences. Thus $\alpha = T(\mathfrak{N})$ for some automaton $\mathfrak{N} = \langle S, f, d, D \rangle$. We may take S as a subset of U_s for some $s > 0$. Identify $U_r \times U_s$ with U_{r+s}, the complete states of $\mathfrak{N}$. Then α is a projection of a set $\beta \subseteq U_{r+s}^*$ and β is the set of all R-sequences $[R \subseteq U_{r+s} \times U_{r+s}]$ beginning with an element of $B = \{\langle a, f(a, d) \rangle \mid a \in U_r\}$ and terminating with an element of $U_r \times D$ where $\langle u_1, v_1 \rangle R \langle u_2, v_2 \rangle$ if and only if $u_1, u_2 \in U_r$, $v_1, v_2 \in U_s$ and $f(u_2, v_1) = v_2$. Notice that the elements of β are admissible-3.

Define $\dot{R}$ and R^+ as follows:

$$\langle a, c \rangle \dot{R} \langle b, d \rangle \Leftrightarrow aRb \wedge c = 1 = d;$$

$$\langle a, c \rangle R^+ \langle b, d \rangle \Leftrightarrow \langle a, c \rangle \dot{R} \langle b, d \rangle \cdot \vee \cdot a = b \wedge (c = 1 \vee c = 0) \wedge d = 0,$$

for all $a, b \in U_{r+s}$.

Observation. Every finite non-null $\dot{R}$-sequence has a unique extension to an infinite R^+-sequence in which $\langle a, 0 \rangle$ occurs for some $a \in U_{r+s}$, and every infinite R^+-sequence in which $\langle a, 0 \rangle$ appears for some $a \in U_{r+s}$ is an extension of some finite non-null $\dot{R}$-sequence. If g is an infinite R^+-sequence such that $g(x) = \langle a, 0 \rangle$, then for all $y > x$, $g(y) = \langle a, 0 \rangle$.

Let f abbreviate $F_1, F_2, \cdots, F_{r+s+1}$. Let $\mathfrak{F} = \bigwedge_x \bigvee_{\langle a,b \rangle \in R^+} [f(x) = a \wedge f(x') = b] \wedge \bigvee_y y \notin F_{r+s+1}$. Then sequences in $T_{r+s+1}^3(\mathfrak{F})$ have the property:

(1) if it is of length one, it is of the form $\langle a, 0 \rangle$;

(2) if it is of length two, it is of the form $\langle a, 1 \rangle \langle a, 0 \rangle$;

(3) if it is of length greater than two, then its last three members are of the form $\langle b, 1 \rangle \langle a, 1 \rangle \langle a, 0 \rangle$, where $a, b \in U_{r+s}$ and $a \neq b$. It follows that $T_{r+s}^3(\bigvee_{F_{r+s+1}} (\mathfrak{F}))$ is the set of all R-sequences.

Let $\mathcal{G}[g]$ be $\bigvee_{F_{r+s+1}} (\mathfrak{F})$. Let $\mathcal{H}[g]$ be:

$$\mathcal{G}[g] \wedge g(0) \in B \wedge \bigvee_x g(x) \in U_r \times D \wedge \bigwedge_y (y > x \supset g(y) = g(x)).$$

(The second and third conjuncts are abbreviations of disjunctions.) Then

$$T_r^3\left(\bigvee_{F_{r+1}} \bigvee_{F_{r+2}} \cdots \bigvee_{F_{r+s}} \mathcal{H} \right) = \alpha.$$

Corollary 1. *There is a decision procedure for the truth of sentences of* L_1^3 (*and one such procedure is given by the proof of Theorem* 5.15 (a) *together with the last paragraph of* 5.8).

Corollary 2. *The first order theory* L^3 *of the Boolean algebra of all quasi-finite sets of natural numbers* (*based, say, upon* $\cup$, $\cap$, $^-$) *with operator* F^s (*cf.* 5.11) *is decidable. More generally, the relations on quasi-finite sets definable in* L^3 *are exactly the same as those definable in* L_1^3.

Proof. Similar to 5.11.

5.16. Let L_1^4 be the system consisting of the formulas L_1 with individual variables ranging over all the integers and set variables ranging over quasi-finite sets of integers.

THEOREM. *There is a decision procedure for the truth of sentences of* L_1^4.

Proof. If $F_1, F_2, \cdots, F_r$ satisfies a formula of L_1^4, then any translate (cf. 5.12) of this r-tuple satisfies the formula. The function $f: N \to U_r$ such that $(f(x))_i = 1 \Leftrightarrow x \in F_i$ has the property that $\bigvee_{x,y,a} [\bigwedge_{z \leqq x} f(z) = a \wedge \bigwedge_{z \geqq y} f(z) = a$ and $x \leqq y]$ because of the quasi-finite character of the F_i. If f is not constant, let

$$x_0 = (\max x) \bigvee_a \bigwedge_z [z \leqq x \supset f(z) = a],$$

$$y_0 = (\min y) \bigvee_a \bigwedge_z [z \geqq y \supset f(z) = a].$$

Then the finite sequence $g = \sigma_r^4(F_1, F_2, \cdots, F_r)$ if domain $g = \{x \mid x \leqq y_0 - x_0\}$ and $\bigwedge_x [g(x) = f(x + x_0)]$. If f is constant and equal to b, then let domain $g = \{0\}$ and $g(0) = b$. The mapping σ_r^4 takes all members of a translation equivalence class into the same element of U_r and distinct equivalence classes go into distinct elements. Moreover, if $\sigma_r^4(F_1, F_2, \cdots, F_r) = g$ and domain $g = \{x \mid x \leqq y\}$ and $y > 0$, then $y > 1$ and $g(0) = g(y)$, $g(0) \neq g(1)$, $g(y-1) \neq g(y)$.

Via σ_r^4, with each formula $\mathfrak{F}[F_1, F_2, \cdots, F_r]$ of L_1^4 is associated a set of finite sequences $T_r^4(\mathfrak{F})$ which may be shown to be regular and a regular expression may effectively be obtained as in the proof of 5.15, Theorem (a). This, together with the last paragraph of 5.8, yields a decision procedure for truth.

CHAPTER III. SOLVABILITY ALGORITHMS

6. **Some operations which preserve regularity.** Let $\sigma \subseteq V_{A \times B}$. A sequence in $A \times B$ will sometimes be indicated thus: $|u, v|$, where $u \in V_A$ and $v \in V_B$ and u and v have the same length. Thus, the ith member of $|u, v|$ is the ordered pair whose first member is the ith member of u and whose second member is the ith member of v and $|u, v|$ is an initial segment of $|u, v|\ |u', v'|$. Similarly the ith member of $|u, v, w|$, where u, v, w all have the same length, is the ordered triple whose first, second and third members are respectively, the ith member of u, of v and of w. A sequence $|u, v| \in \sigma$ is *A-extendable in σ* if and only if $\bigwedge_{a \in A} \bigvee_{b \in B} |u, v|\ |a, b| \in \sigma$. A sequence in σ is *strongly A-extendable* in σ if and only if every initial segment of the sequence is in σ and is A-extendable in σ. The set σ is *strongly A-extendable* if and only if every sequence in σ is strongly A-extendable in σ. If σ is strongly A-extendable, every initial segment of an element in σ is in σ.

6.1. LEMMA. *If* $\gamma \subseteq V_{A \times B}$ *is regular, then there is a* $\gamma_A \subseteq \gamma$ *such that*

(1) γ_A *is regular,*

(2) γ_A *is strongly* A*-extendable,*

(3) *if* $\beta\subseteq\gamma$ *and* β *is strongly* A*-extendable, then* $\beta\subseteq\gamma_A$. *Furthermore, from an automaton* $\mathfrak{C}$ *such that* $T(\mathfrak{C})=\gamma$ *one can effectively construct (by the method given in proof) an automaton* $\mathfrak{C}_A$ *such that* $T(\mathfrak{C}_A)=\gamma_A$.

Proof. Let $\mathfrak{C}$ be the $A\times B$-automaton $\langle S, f, d, D\rangle$. Then γ is $p(\delta)$, where δ is the union of $\{\Lambda\}$ and the set of all R-sequences beginning with an element of $E=\{\langle a, f(a, b, d)\rangle \mid \langle a, b\rangle\in A\times B\}$ and terminating with an element of $(A\times B)\times D$, and R holds between $\langle\langle a_1, b_1\rangle, s_1\rangle$ and $\langle\langle a_2, b_2\rangle, s_2\rangle$ if and only if $f(\langle a_2, b_2\rangle, s_1)=s_2$ and $p(\langle a, b\rangle, s)=\langle a, b\rangle$. Let R_0 be the restriction of R to $A\times B\times D=M_0$, i.e., $R_0=R\cap(M_0\times M_0)$. For $n\geqq 0$ let R_{n+1} be the restriction of R_n to M_{n+1} where

$$\langle a_1, b_1, c_1\rangle\in M_{n+1}\Rightarrow\langle a_1, b_1, c_1\rangle\in M_n\wedge\bigwedge_{a\in A}\ \bigvee_{\langle b,c\rangle\in B\times D}\langle a_1, b_1, c_1\rangle R_n\langle a, b, c\rangle.$$

Inasmuch as M_0 is finite, there exists m such that $R_m=R_{m+1}=R_{m+2}=\cdots$. Define R_A to be R_m for this m and M_A to be M_m for this m. Then

$$\langle a_1, b_1, c_1\rangle\in M_A\Leftrightarrow\bigwedge_{a\in A}\ \bigvee_{\langle b,c\rangle\in B\times D}\langle a_1, b_1, c_1\rangle R_A\langle a, b, c\rangle.$$

[Of course, M_A may be empty.] Let σ be the set of all R_A-sequences beginning with an element of E, i.e., beginning with an element of $E\cap\mathfrak{D}R_A$ ($\mathfrak{D}R_A$ is the domain of the binary relation R_A). Let $\gamma_A=p\sigma$.

(1) γ_A is regular since it is a projection of a regular set σ.

(2) We shall show γ_A is strongly A-extendable. Let

$$|u_1, v_1|\ |u_2, v_2|\in\gamma_A$$

where $u_1, u_2\in V_A$ and $v_1, v_2\in V_B$; then there exists $w_1, w_2\in V_S$ such that

$$|u_1, v_1, w_1|\ |u_2, v_2, w_2|\in\sigma.$$

Then

$$|u_1, v_1, w_1|\in\sigma\quad\text{and}\quad|u_1, v_1|\in\gamma_A.$$

Since the elements in the sequence $|u_1, v_1, w_1|$ are in M_A, and, in particular, the last element of this sequence is in M_A, it follows that

$$\bigwedge_{a\in A}\ \bigvee_{\langle b,c\rangle\in B\times D}|u_1, v_1, w_1|\ |a, b, c|\in\sigma$$

so that

$$\bigwedge_{a\in A}\ \bigvee_{b\in B}|u_1, v_1|\ |a, b|\in\gamma_A.$$

(3) Suppose β is strongly A-extendable and $\beta\subseteq\gamma$. Let $|u, v|\in\beta$; then every initial segment of $|u, v|\in\beta$ so that if w is the sequence of internal states determined by the automaton $\mathfrak{C}$ (i.e., if $|u, v|$ is $a_0a_1\cdots a_n\in A\times B$, then

w is $s_0 s_1 \cdots s_n$ where $f(a_0, d) = s_0$ and, for $0 < r \leqq n, f(a_r, s_{r-1}) = s_r$), then every initial segment of $|u, v, w|$ is an element of δ. Thus, every member of the sequence $|u, v, w|$ is an element of M_0 and $|u, v, w|$ is Λ or is an R_0-sequence beginning with an element of E. Consider an arbitrary initial segment

$$|u_0, v_0, w_0|\;|a_0, b_0, c_0| \quad \text{of} \quad |u, v, w|$$

where $a_0 \in A$, $b_0 \in B$, $c_0 \in D$, i.e., $\langle a_0, b_0, c_0\rangle \in M_0$. Since

$$|u_0, v_0|\;|a_0, b_0| \in \beta,$$

$$\bigwedge_{a_1 \in A} \bigvee_{b_1 \in B} |u_0, v_0|\;|a_0, b_0|\;|a_1, b_1| \in \beta \subseteq \gamma.$$

Hence

$$\bigwedge_{a_1 \in A} \bigvee_{\langle b_1, c_1\rangle \in B \times D} [|u_0, v_0, w_0|\;|a_0, b_0, c_0|\;|a_1, b_1, c_1| \in \delta \wedge \langle a_1, b_1, c_1\rangle \in M_0].$$

It follows that $\langle a_0, b_0, c_0\rangle \in M_1$. Similarly

$$\bigwedge_{a_1 \in A} \bigvee_{\langle b_1, c_1\rangle \in B \times D} \bigwedge_{a_2 \in A} \bigvee_{\langle b_2, c_2\rangle \in B \times D} [|u_0, v_0, w_0|\;|a_0, b_0, c_0|\;|a_1, b_1, c_1|\;|a_2, b_2, c_2|$$
$$\in \delta \wedge \langle a_2, b_2, c_2\rangle \in M_0 \wedge \langle a_1, b_1, c_1\rangle \in M_1].$$

It follows that $\langle a_0, b_0, c_0\rangle \in M_2$. It should now be clear that $\langle a_0, b_0, c_0\rangle \in M_A$ so that $|u, v, w|$ is Λ or is a R_A-sequence beginning with an element of E. Thus $|u, v, w| \in \sigma$ and $|u, v| \in \gamma_A$. We have shown that: if $\beta \subseteq \gamma$ and β is strongly A-extendable, then $\beta \subseteq \gamma_A$.

6.2. If $\alpha \subseteq V_A$, define the *interior* of α (Int α) to be the set of sequences $u \in \alpha$ such that every initial segment of u is in α. A set α is *open* if and only if $\alpha = \text{Int}\ \alpha$. We note incidentally that it is immediate from the definition that arbitrary unions and arbitrary intersections of open sets are open so that the class of open sets constitute a topology in the usual sense for V_A. Notice that if α is open, then $\alpha \neq \emptyset \Leftrightarrow \Lambda \in \alpha$. Medvedev [6, p. 11, Theorem 2] proves that if α is regular, then Int α is regular by direct construction of an automaton. The result is established below by means of 5.3.

Lemma. *If α is regular, then* Int α *is regular.*

Proof. Assume $A \subseteq U_r^0$ for an appropriate r. Suppose that $T_r\mathfrak{F}[f] = \alpha$ for an appropriate formula $\mathfrak{F}$ of L_1^1. Define $\mathfrak{G}[g]$ as follows:

$$\bigwedge_h : h \leqq g \cdot \supset \cdot \mathfrak{F}[h]$$

where $h \leqq g$ abbreviates

$$\bigwedge_x (h(x) \neq 0_r \supset h(x) = g(x))$$

and 0_r is the all zero r-tuple. Note that $h \leqq g$ means that the element of $V_{U_r^0}$ represented by h is an initial segment of the element of $V_{U_r^0}$ represented by g. [Each of the r set variables abbreviated by h are distinct from each of the r set variables abbreviated by g.]

6.3. Lemma. *The intersection α^L of all open sets containing a given regular set α is regular (and open).*

Proof. Let $\alpha \subseteq V_{U_r^0}$ be regular. The intersection of all open sets containing α is simply the set of all initial segments of elements in α. Thus if $T_r\mathfrak{F}[f] = \alpha$ and if $\mathcal{G}[g]$ is defined as follows:

$$\bigvee_f : \mathfrak{F}[f] \wedge \bigwedge_x \cdot g(x) \neq 0_r \supset g(x) = f(x),$$

the desired set is $T_r\mathcal{G}[g]$.

6.4. Lemma. *Let $\alpha \subseteq V_{A \times \{0,1\}}$ be regular. Suppose $\Lambda \notin \alpha$. Let $K_i(\alpha)$, $i = 0, 1$, be the set of sequences $a_0a_1 \cdots a_n$, $a_j \in A$, such that there exists $b_0, b_1, \cdots, b_n$ satisfying*

$$b_j \in \{0, 1\}, \tag{1}$$

$$|a_0, b_0,| \; |a_1, b_1| \cdots |a_n, b_n| \in \alpha, \tag{2}$$

$$b_n = i. \tag{3}$$

Then $K_i(\alpha)$ is regular. If $\Lambda \in \alpha$, let $K_i(\alpha) = K_i(\alpha - \{\Lambda\}) \cup \{\Lambda\}$; then $K_i(\alpha)$ is regular.

Proof. Let $\mathfrak{N} = \langle S, f, d, D \rangle$ be an $A \times \{0, 1\}$ automaton and suppose $T(\mathfrak{N}) = \alpha$. Let $\mathcal{B} = \langle S, f, d, D \cap A \times \{i\} \rangle$. Let $\beta = T(\mathcal{B})$. Then β is the set of all sequences

$$|a_0, b_0| \; |a_1, b_1| \cdots |a_n, b_n| \in \alpha$$

such that $b_n = i$. If $p(a, b) = a$, where $a \in A$, $b \in \{0, 1\}$, then $K_i(\alpha) = \hat{p}(\beta)$.

6.5. Lemma. *Let $\beta \subseteq V_{A \times B}$ be regular. Let $\underline{\preceq}$ be the lexicographical ordering of V_B induced by a given fixed ordering ($\preceq$) of B. Define $\alpha = \mathfrak{L}_{\preceq}(\beta)$ as follows:*

$$|u, v| \in \alpha \Leftrightarrow |u, v| \in \beta \wedge \bigwedge_w |u, v| \in \beta \supset v \,\underline{\preceq}\, w.$$

Then α is regular (and the set of ordered pairs $\langle u, v \rangle$ of sequences such that $|u, v| \in \alpha$ is a function).

Proof. Suppose (without loss of generality) that $A \subseteq U_r^0$, $B \subseteq U_s^0$ for appropriate r, s. Suppose that

$$T_{r+s}\mathfrak{F}[f_1, f_2] = \beta \qquad \text{for an appropriate formula } \mathfrak{F} \text{ of } L_1^1.$$

Define $\mathcal{G}[g_1, g_2]$ as follows:

$$\mathfrak{F}[g_1, g_2] \wedge \bigwedge_{f_2,x} : \mathfrak{F}[g_1, f_2] \wedge f_2(x) \neq g_2(x) \wedge \bigwedge_{y} (y < x \supset f_2(y) = g_2(y))$$

$$\cdot\supset\cdot g_2(x) \leqq f_2(x),$$

where g_1 abbreviates $F_1, \cdots, F_r$, g_2 abbreviates $F_{r+1}, \cdots, F_{r+s}$, and f_2 abbreviates $F_{r+s+1}, \cdots, F_{r+2s}$, and $g_2(x) \leqq f_2(x)$ abbreviates a conjunction of conditionals of the form

$$g_2(x) = b \cdot\supset\cdot f_2(x) = b_1 \vee f_2(x) = b_2 \vee \cdots \vee f_n(x) = b_m$$

where $\{b_1, \cdots, b_n\}$ is the set of all elements b_i in B such that $b \prec b_i$.

Then $T_{r+s}\mathcal{G} = \alpha$, and α is regular (cf. Theorem 5.3 and remark).

7. **Characterizations of A/B-automata behavior.** An *A/B-automaton* is a quadruple $\mathfrak{N} = \langle S, f, d, g\rangle$ where $f: A \times S \rightarrow S$ and $g: S \rightarrow B$. The finite behavior $\mathfrak{I}(\mathfrak{N})$ of $\mathfrak{N}$ is defined as follows:

$$\left| u, v \right| \in \mathfrak{I}(\mathfrak{N}) \subseteq V_{A\times B} \Leftrightarrow (1) \ \left| u, v \right| = \Lambda \text{ or } (2) \ \left| u, v \right| \neq \Lambda$$

$$\text{and } \bigvee_{w} \Big[w \in V_S \wedge u = a_0a_1 \cdots a_n \wedge v = b_0b_1 \cdots b_n \wedge w = s_0s_1 \cdots s_n \cdot\supset\cdot s_0$$

$$= f(a_0, d) \wedge \bigwedge_{0<m\leq n} f(a_m, s_{m-1}) = s_r \wedge \bigwedge_{0\leqq m \leqq n} g(s_m) = b_m \Big].$$

7.1. THEOREM. *A set $\alpha \subseteq V_{A\times B}$ is the behavior of an A/B-automaton if and only if*

(1) *α is regular,*

(2) *α is open,*

(3) *$\{\langle u, v\rangle : |u, v| \in \alpha\}$ is a function,*

(4) *$\{u : |u, v| \in \alpha\} = V_A$.*

Further, if α satisfies the conditions, the proof gives an effective procedure for producing an $\mathfrak{N}$ such that $\mathfrak{I}(\mathfrak{N}) = \alpha$.

Proof. Assume $\alpha = \mathfrak{I}(\mathfrak{N})$ for some A/B-automaton $\mathfrak{N}$. Let $\mathfrak{N} = \langle S, f, d, g\rangle$. Define a binary relation R on $A \times B \times S$ as follows: $\langle a_1, b_1, s_1\rangle R \langle a_2, b_2, s_2\rangle$ if and only if $f(a_2, s_1) = s_2 \wedge g(s_1) = b_1 \wedge g(s_2) = b_2$. Let $u \in \beta$ if and only if $u = \Lambda$ or u is an R-sequence beginning with an element of $\{a, f(a, d), gf(a, d) : a \in A\}$. Let $p(a, b, s) = \langle a, b\rangle$ for $a \in A$, $b \in B$, $s \in S$. Then $\hat{p}\beta = \alpha$. (Cf. the definition of $\mathfrak{I}(\mathfrak{N})$.) Hence (1) is satisfied by α.[5]

Conversely, assume $\alpha \subseteq V_{A\times B}$ and α satisfies (1), (2), (3), (4). Without loss of generality assume $B \subseteq U_r$ for an appropriate r. Let $\alpha_i = \hat{p}_i(\alpha)$, $1 \leqq i \leqq r$, where $p_i\langle a, c_1, c_2, \cdots, c_i, \cdots, c_r\rangle = \langle a, c_i\rangle$, $a \in A$, and, for all j, $c_j \in \{0, 1\}$. Let $\mathfrak{N}_i = \langle S_i, f_i, d_i, D_i\rangle$, $1 \leqq i \leqq r$, be A-automata such that $T(\mathfrak{N}_i) = K_1(\alpha_i)$

[5] This was pointed out to me by J. B. Wright.

(cf. 6.4). Let $\mathfrak{N}=\langle S, f, d, g\rangle$ be an A/B-automaton where $B=U_r$, $S=S_1\times S_2\times\cdots\times S_r$, $(f(s))_i=f_i(s_i)$, $1\leqq i\leqq r$, where $s\in S$ and the subscript "i" indicates the ith component of an r-tuple, and $d=\langle d_1, d_2, \cdots, d_r\rangle$ and $(g(s))_i=1\Leftrightarrow s_i\in D_i$.

Because of condition (3), for all i, $1\leqq i\leqq r$, $K_1(\alpha_i)\cap K_2(\alpha_i)=\varnothing$ and because of (4), $K_1(\alpha_i)\cup K_2(\alpha_i)=V_A$. Now, $\mathfrak{J}(\mathfrak{N})$ satisfies (1), (2), (3), (4) by the first part of the theorem. Thus it is sufficient to show that for each $u\in V_A$, if v_1 is the unique element of V_B such that $|u, v_1|\in\alpha$ and v_2 is the unique element of V_B such that $|u, v_2|\in\mathfrak{J}(\mathfrak{N})$, then $v_1=v_2$.

It is obvious that $\Lambda\in\alpha\cap\mathfrak{J}(\mathfrak{N})$. Suppose $|u, v|\in\alpha\cap\mathfrak{J}(\mathfrak{N})$ and $|u,w|\cdot|a, b|\in\alpha$. Because α is open, $|u, w|\in\alpha$, and so by (3), $w=v$. Let b_i be the ith component of b and let w_i be the sequence of ith components of its members. Now,

$$|u,v|\ |a,b|\in\alpha\Leftrightarrow\bigwedge_{1\leq i\leq r}|u,v_i|\ |a,b_i|\in\alpha_i\Leftrightarrow\bigwedge_i\,[b_i=1\equiv ua\in K_1(\alpha_i)].$$

Note that $|u, v|\ |a, c|\in\mathfrak{J}(\mathfrak{N})\Leftrightarrow|u, v, w|\ |a, c, s|$ satisfies conditions given in 7 above, for some (unique) $ws\in V_S$. In particular, $g(s)=c$. For this s, $g(s)=c\Leftrightarrow\bigwedge_i[c_i=1\equiv s_i\in D_i]$ and since (for this s) $\bigwedge_i[s_i\in D_i\equiv ua\in K_1(\alpha_i)]$, it follows that $\bigwedge_i[c_i=1\equiv ua\in K_1(\alpha_i)]$, so that $b=c$.

REMARK. Suppose $T_{r+s}\mathfrak{F}[f_1, f_2]=\alpha\subseteq V_{A\times B}$, $A\subseteq U_r^0$, $B\subseteq U_s^0$ for appropriate r, s, and $\mathfrak{F}$ is a formula of L_1^1. One can effectively decide whether α is the behavior of an A/B-automaton as follows:

(1) α is open if and only if "$\bigwedge_{g,f}:\mathfrak{F}[f]\wedge g\leqq f\cdot\supset\cdot\mathfrak{F}[g]$" is true, where f abbreviates $(r+s)$ set variables, cf. 6.2;

(2) 7.1 (4) holds if and only if "$\bigwedge_{f_1}\bigvee_{f_2}[f_1, f_2]$" is true;

(3) 7.1 (3) holds if and only if "$\bigwedge_{f_1,f_2,g_2}:\mathfrak{F}[f_1, f_2]\wedge\mathfrak{F}[f_1, g_2]\cdot\supset\cdot f_2=g_2$" is true.

7.2. We wish to show that none of the conditions of 7.1 can be dropped without the statement becoming invalid.

7.2.1. Let $A=\{1\}$ and $B=\{0, 1\}$. Consider the set α:

$$\begin{pmatrix}1\\0\end{pmatrix}^*\cdot\begin{pmatrix}1\\1\end{pmatrix}\cup\{\Lambda\}.$$

Since $0^*\cdot 1\cup\{\Lambda\}$ denotes this set if "0" denotes $\{\langle 1, 0\rangle\}$ and "1" denotes $\{\langle 1, 1\rangle\}$, α is regular and 7.1 (1) is satisfied. It is obvious that 7.1 (3), (4) are satisfied and that 7.1 (2) is not satisfied.

7.2.2. Let A, B, α be as in 7.2.1. Then α^L (cf. 6.3) satisfies (1), (2), (4) but not (3).

7.2.3. Let $A=\{0, 1\}$, $B=\{1\}$, and let α be the set:

$$\begin{pmatrix}1\\1\end{pmatrix}^*;$$

then α satisfies (1), (2), (3), but not (4).

7.2.4. Let $A=\{a, b\}$ and let $B=\{0, 1\}$. Let β be the set:

$$a^{(n)}ba^{(n)}, \qquad n \geqq 0.$$

It is known (cf. [9]) that β is not regular. Let $|a_1, b_1|\ |a_2, b_2| \cdots |a_k, b_k| \cdots |a_n, b_n| \in\alpha\Leftrightarrow a_1a_2 \cdots a_k\in\beta^L\equiv b_k=1$. Since β^L is open, it follows that

$$|u, v| \in \alpha \Rightarrow \bigvee_{u_1,v_1,u_2,v_2} |u, v| = |u_1, v_1|\ |u_2, v_2| \wedge v_1 \in V_{\{1\}} \wedge v_2 \in V_{\{0\}}.$$

Now α satisfies 7.1 (2), (3), (4). We wish to show α is not regular. If α were regular, then $\gamma=\alpha\cap V_{A\times\{1\}}$ is regular. Further, γ is isomorphic to β^L. Hence to show α is not regular, it is sufficient to show β^L is not regular.

Suppose β^L were regular; then, assuming $a, b\in U_2^0$, for some formula $\mathfrak{F}[f]$ of L_1^1:

$$T_2(\mathfrak{F}) = \beta^L$$

Let $\mathfrak{G}[g]$ be the formula:

$$\mathfrak{F}[g] \wedge \bigwedge_f : g \leqq f \wedge \mathfrak{F}[f]\cdot\supset\cdot g = f \qquad \text{(cf. 6.2).}$$

Then $T_2(\mathfrak{G})=\beta$ is regular. Contradiction. Thus α is not regular.

7.3. If A is an arbitrary finite nonempty set, A^N is the set of all infinite sequences (functions on natural numbers) of elements of A. If $\alpha\subseteq V_A$, then $f\in\lim\alpha\Leftrightarrow\{f\}^L\subseteq\alpha$, where β^L, for $\beta\subseteq A^N$, means the set of all finite initial segments of elements in β.

THEOREM. *If $\alpha\subseteq(A\times B)^N$, then there exists an A/B-automaton such that* $\lim \mathfrak{J}(\mathfrak{M})=\alpha$ *if and only if*

(1) *α^L is regular,*

(2) *$|f_1, g_1|\in\alpha\wedge|f_2, g_2|\in\alpha\wedge f_1 \upharpoonright n=f_2 \upharpoonright n\cdot\supset\cdot g_1 \upharpoonright n=g_2 \upharpoonright n$ where $f \upharpoonright n$ is the restriction of f to the set of natural numbers $<n$,*

(3) *$\{f: |f, g|\in\alpha\}=A^N$.*

Proof. Assume (1), (2), (3) hold. From (2), it follows that 7.1 (3) holds for α^L; 7.1 (2) is obvious from the definition of α^L; and 7.1 (4) follows from condition (3). Hence, there exists an A/B-automaton $\mathfrak{M}$ such that $\mathfrak{J}(\mathfrak{M})=\alpha^L$. *Claim*: $\lim\alpha^L=\alpha$. If $|f, g|\in\alpha$, then $\{|f, g|\}^L\subseteq\alpha^L$ so that $|f, g|\in\lim\alpha^L$ and $\alpha\subseteq\lim\alpha^L$. Suppose $|f, g|\in\lim\alpha^L$. Because of (3), $|f, h|\in\alpha$ for some h. Consider an arbitrary n, $|f, g| \upharpoonright n=|f', g'| \upharpoonright n$ for some $|f', g'|\in\alpha$. Since $f \upharpoonright n=f' \upharpoonright n$, it follows that $h \upharpoonright n=g' \upharpoonright n=g \upharpoonright n$ (using condition (2)). Thus, $g=h$ and our claim is established (based only upon conditions (2) and (3)).

Let $\mathfrak{M}$ be an A/B-automaton. It is obvious that $\lim \mathfrak{J}(\mathfrak{M})$ satisfies (2) and (3). Hence, the "claim" of the previous argument establishes that $(\lim \mathfrak{J}(\mathfrak{M}))^L=\mathfrak{J}(\mathfrak{M})$ so that (1) is satisfied.

8. **Solvability-synthesis algorithms.** The fundamental solvability-synthesis theorem that we have obtained is given in 8.1. A reformulation is given

in 8.3. In 8.6 we obtain a result closely related to results obtained by A. Church [2].

8.1. Theorem. *Suppose $\gamma \subseteq V_{A \times B}$. There exists an A/B-automaton $\mathfrak{N}$ such that $\mathfrak{J}(\mathfrak{N}) \subseteq \gamma$ if and only if γ_A (cf. 6.1) is nonempty. If γ_A is nonempty, then one may effectively obtain an automaton $\mathfrak{N}$ such that $\mathfrak{J}(\mathfrak{N}) = \mathcal{L}_{\preceq}(\gamma_A)$ where $\preceq$ is an arbitrary ordering of B (cf. 6.5.).*

Proof. Suppose $\mathfrak{J}(\mathfrak{N}) \subseteq \gamma$ for some $\mathfrak{N}$. Then, since $\mathfrak{J}(\mathfrak{N})$ is strongly A-extendable, $\mathfrak{J}(\mathfrak{N}) \subseteq \gamma_A$ and $\gamma_A \neq \emptyset$.

If $\gamma_A \neq \emptyset$, then because it is open, $\Lambda \in \gamma_A$ and because it is A-extendable, the set $\{u: |u, v| \in \gamma_A\} = V_A$. By Lemma 6.1, γ_A is regular. Let $\mathcal{L}_{\preceq}(\gamma_A) = \alpha$. From the definition of $\mathcal{L}_{\preceq}$, it follows that $\{\langle u, v \rangle: |u, v| \in \alpha\}$ is a function and, since $\{u: |u,v| \in \gamma_A\} = V_A$, so, too, $\{u: |u, v| \in \alpha\} = V_A$. By Lemma 6.5, α is regular. It remains only to show that α is open and then the result follows from 7.1.

Suppose $|u_1, v_1|\ |u_2, v_2| \in \alpha$. For some v, $|u_1, v| \in \alpha$. Since $|u_1, v_1|\ |u_1, v|$ $\in \gamma_A$, it follows $v \preceq v_1$. Because $|u_1, v|$ is A-extendable in γ_A,

$$|u_1, v|\ |u_2, w| \in \gamma_A, \qquad \text{for some } w \in V_B.$$

Thus $v_1 v_2 \preceq vw$, so that $v_1 \preceq v$ (since $\preceq$ is a lexicographical ordering). It follows that $v = v_1$ and α is open, and the theorem is proved.

8.2. Corollary. *Given $\gamma \subseteq A \times B$, one can effectively decide (by the method indicated by the proof) whether: $\mathfrak{J}(\mathfrak{N}_1) \subseteq \gamma$ and $\mathfrak{J}(\mathfrak{N}_2) \subseteq \gamma$ implies $\mathfrak{J}(\mathfrak{N}_1) = \mathfrak{J}(\mathfrak{N}_2)$.*

Proof. If $\gamma_A = \emptyset$, then the condition is vacuously satisfied (cf. 8.1). Suppose $\gamma_A \neq \emptyset$. If $\mathfrak{N}_1$ is the automaton picked out by 8.1 and $\mathfrak{J}(\mathfrak{N}_2) \subseteq \gamma$ and $\mathfrak{J}(\mathfrak{N}_1) \neq \mathfrak{J}(\mathfrak{N}_2)$, then there exists $|u, v| \in \mathfrak{J}(\mathfrak{N}_1)$, $|u, w| \in \mathfrak{J}(\mathfrak{N}_2)$, and $v \prec w$. Hence, if $\mathfrak{N}$ is the automaton picked out by 8.1 when the ordering of B is reversed, $\mathfrak{J}(\mathfrak{N}_1) \neq \mathfrak{J}(\mathfrak{N})$.

Thus, the conditional of the corollary holds if and only if (1) $\gamma_A = \emptyset$ or (2) $\gamma_A \neq \emptyset$ and if $\mathfrak{N}_1$ is the automaton picked out via 8.1 by an ordering $\preceq$ of B and $\mathfrak{N}_2$ is the automaton picked out via 8.1 by the reverse ordering $\succeq$ of B, then the symmetric difference of $\mathfrak{J}(\mathfrak{N}_1)$ and $\mathfrak{J}(\mathfrak{N}_2)$ is $\emptyset$.

8.3. An A/B-automaton, $A \subseteq U_m^0$, $B \subseteq U_{m'}^0$, may be identified, it will be shown, with a formula of L_1^1 of a certain form. Let $\mathfrak{N} = \langle S, f, d, g \rangle$ be such an automaton. Consider the formula

$$\mathfrak{F}_{\mathfrak{N}}[a, b] \text{ of } L_1^1\colon \bigvee_{s,t} [t \neq 0 \supset s(0) = f(a(0), d) \wedge \bigwedge_{x<t} (s(x') = f(a(x'), s(x))$$
$$\wedge\, b(x) = gs(x) \wedge \bigwedge_{x \geq t} a(x) = 0_m \wedge b(x) = 0_{m'}],$$

where "a," "b" are function symbols interpreted as taking values respectively in A, B and, respectively, abbreviating finite sequences of set variables. It is obvious that $T_{m+m'}(\mathfrak{F})=\mathfrak{J}(\mathfrak{N})$. Thus the formula above may be identified with $\mathfrak{N}$. Given an arbitrary formula $\mathcal{G}[a, b]$ of L_1^1, let $T_{m+m'}(\mathcal{G})=\gamma\subseteq V_{A\times B}$. Then $\mathfrak{J}(\mathfrak{N})\subseteq\gamma\Leftrightarrow\bigwedge_{a,b}\cdot\mathfrak{F}[a, b]\supset\mathcal{G}[a, b]$.

8.4. If p maps the finite set A onto B, $\hat{p}$ maps elements (and sets of elements) of V_A onto elements (and sets of elements) of V_B. We wish to extend further the meaning of $\hat{p}$. If $f\in A^N$, then $(\hat{p}f)(n)=p(f(n))$. If $\alpha\subseteq A^N$, then $\hat{p}\alpha=\{\hat{p}f: f\in\alpha\}$.

Lemma. (1) *If* $\alpha\subseteq V_A$ *is open, then* $\lim(\hat{p}\alpha)=\hat{p}(\lim\alpha)$.

(2) *For arbitrary* $\beta\subseteq V_A$, $\lim\beta=\lim(\mathrm{Int}\,\beta)$.

Proof. Let $f\in\lim\alpha$. For all $n\geqq 0$, $f\restriction n\in\alpha$ and $\hat{p}(f\restriction n)\in\hat{p}\alpha$. Now $\hat{p}f\in\hat{p}\lim\alpha$ and $\{\hat{p}f\}^L=\{\hat{p}(f\restriction n): n\geqq 0\}$. Hence $\hat{p}f\in\lim(\hat{p}\alpha)$. Thus, $\hat{p}(\lim\alpha)\subseteq\lim(\hat{p}\alpha)$.

We shall now show $\lim(\hat{p}\alpha)\subseteq\hat{p}(\lim\alpha)$[6]. Suppose $g\in\lim(\hat{p}\alpha)$. Let $\alpha'=\alpha\cap\bigcup_{n\geqq 0}\hat{p}^{-1}(g\restriction n)$. Note that α' is open because α is. Then α' contains an infinite number of elements. For $u\in\alpha'$, let $\rho_{\alpha'}(u)$ be the number of elements in α' of which u is an initial segment. Now $\Lambda\in\alpha'\wedge\rho_{\alpha'}(\Lambda)=\infty$. We define $\alpha_g\subseteq\alpha'$ inductively. Let $\Lambda\in\alpha_g$. Suppose $u\in\alpha_g$ as well as every initial segment of u and suppose $\rho_{\alpha'}(u)=\infty$. Let $a_1, a_2, \cdots, a_n$ be an enumeration of the elements of A. If u is an initial segment of v but $u\neq v$, then, because α' is open, v is an initial segment of either $ua_1, ua_2, \cdots, ua_n$. Since $\rho_{\alpha'}(u)=\infty$, for some i, $\rho_{\alpha'}(ua_i)=\infty$. Let k be the first such i and place ua_k in α_g. Thus $\alpha_g\subseteq V_A$ is an infinite set simply ordered by the relation "initial segment of". It is thus unambiguous to define $f(n)=u(n)$, where $u\in\alpha_g$ has n in its domain. It follows, for all m, $f\restriction m\in\alpha_g\subseteq\alpha$ and $\hat{p}(f\restriction m)=g\restriction m$. Thus $f\in\lim\alpha$, $\hat{p}f=g$ and $g\in\hat{p}\lim\alpha$.

The proof of (2) is immediate from the definition of lim and Int.

8.5. Lemma. *Let* $\beta\subseteq A^N$ *be the set of all infinite R-sequences* f *such that* $f\restriction n$ *is an element of a given set* E *of sequences of length* n, *where* R *is an* n*-ary relation over* A. *Then* (1) $\lim(\beta^L)=\beta$, *and if* $\hat{p}$ *is a projection*, (2) $(\hat{p}\beta)^L=\hat{p}(\beta^L)$, (3) $\lim((\hat{p}\beta)^L)=\hat{p}\beta$, (4) β^L *and* $\hat{p}(\beta^L)$ *are regular sets and a regular expression denoting them may effectively be obtained.*

Proof. (1) Let $f\in\beta$. Then $\{f\}^L\subseteq\beta^L$. Hence $f\in\lim(\beta^L)$ and $\beta\subseteq\lim(\beta^L)$. Suppose $f\in\lim(\beta^L)$. Then $f\restriction n\in\{g\restriction n: g\in\beta\}\subseteq E$ and, for all m, $f\restriction m$ is an R-sequence. Hence f is an R-sequence and $f\in\beta$.

(2) $u\in(\hat{p}\beta)^L\Leftrightarrow\bigvee_{g,m}\ g\in\beta\wedge((\hat{p}g)\restriction m)=u\Leftrightarrow\bigvee_{g,m}\ g\in\beta\wedge\hat{p}(g\restriction m)=u$ $\Leftrightarrow u\in\hat{p}(\beta^L)$.

(3) $\lim((\hat{p}\beta)^L)=\lim(\hat{p}(\beta^L))$ by (2) and by 8.4, $\lim\ \hat{p}(\beta^L)=\hat{p}\lim(\beta^L)$, since β is open and by (1) the result follows.

[6] The proof is closely related to König's infinity lemma. *Theorie der endlichen und unendlichen Graphen*, Leipzig, Akademische Verlagsgesellschaft M. B. H., 1936, p. 81, Satz 6.

(4) $K(w)=A^*\cdot\{a_1\}\cdot\{a_2\}\cdots\{a_n\}\cdot A^*$, $a_i\in A$, is the set of sequences in V_A in which the sequence $w=a_1a_2\cdots a_n$ occurs and this set is regular. The set compl $\bigcup_{w\notin R} K(w)$ is regular and is the set of all R-sequences. The set E^L is regular, as is any finite set. The set β^L is: compl $\bigcup_{w\notin R} K(w)\cap E^L$ and is, therefore, regular. Since projection preserves regularity, $\hat{p}(\beta^L)$ is regular.

8.6. Let L_1^5 be the system consisting of the formulas of L_1, with individual variables interpreted over natural numbers and the set variables interpreted over arbitrary sets of natural numbers. With a formula $\mathfrak{F}[F_1, F_2, \cdots, F_r]$ of L_1^5 we associate a set $T_r^\infty\mathfrak{F}$ defined as follows:

$f\in T_r^\infty\mathfrak{F}$ if and only if $f\in U_r^N$ and $(f(x))_i=f_i(x)$, $1\leqq i\leqq r$, where f_i is the characteristic function of F_i and $\mathfrak{F}[F_1, F_2, \cdots, F_r]$ holds. Abbreviations introduced for L_1^1 in Remark 5.3 will be used in L_1^5 as well.

8.6.1. Let $\mathfrak{N}=\langle S, f, d, g\rangle$ be an A/B-automaton. The following formula $\mathfrak{G}_{\mathfrak{N}}[a, b]$ of L_1^5 (abbreviated) below may be identified with $\mathfrak{N}$:

$$\bigvee_s \left[s(0) = f(a(0), d) \wedge \bigwedge_x \cdot(s(x') = f(a(x'), s(x))) \wedge b(x) = gs(x)\right].$$

If $\alpha=T^\infty_{m+m'}(\mathfrak{G}_{\mathfrak{N}})$ (assuming range $a\subseteq U_m^0$ and range $b\subseteq U_{m'}^0$), then comparison with $\mathfrak{F}_{\mathfrak{N}}[a, b]$ shows that $\alpha^L=\mathfrak{J}(\mathfrak{N})=T_{m+m'}\mathfrak{F}_{\mathfrak{N}}$ (cf. 8.3) and by Lemma 8.5 (3), lim $\mathfrak{J}(\mathfrak{N})=\alpha$.

8.6.2. Consider arbitrary formulas of L_1^5 of the form $\bigvee_s \bigwedge_x M[a, b, s, x]$, where range $a\subseteq A$, range $b\subseteq B$, and where M: is free of quantifiers, contains only s, a, b, x free (a, b, s, respectively, abbreviate finite sequences of set variables), may contain numerals but not "$=$" nor "$<$". Assume M to be in disjunctive normal form and let n be the maximum of those m's such that $x^{(m)}$ or $0^{(m)}$ appears in M. Then $T^\infty_{m+m'+r}(\bigwedge_x M)$, range $s\subseteq S\subseteq U_r$, is the set of all $f\in(A\times B\times S)^N$ which are R-sequences, for some n-ary R, and such that $f\restriction n\in E$, for some finite set E (of elements of $V_{A\times B\times S}$ of length n). Both R and E are effectively, indeed readily, obtained from M in expanded disjunctive normal form. If $\beta=T^\infty_{m+m'+r}(\bigwedge_x M)$, then $\hat{p}\beta=T^\infty_{m+m'}(\bigvee_s \bigwedge_x M)$, where p maps an $(m+m'+r)$-tuple into the appropriate $(m+m')$-tuple.

8.6.3. Theorem. *Given a formula* $\bigvee_s \bigwedge_x M[a, b, s, x]$, *$M$ as in* 8.6.2, *of* L_1^5, *there exists an A/B-automaton $\mathfrak{N}$ such that* lim $\mathfrak{J}(\mathfrak{N})\subseteq\beta=T^\infty_{m+m'}(\bigvee_s \bigwedge_x M)$ *if and only if* $\gamma_A\neq\varnothing$ (*cf.* 8.1) *where* $\gamma=\beta^L$. *Whether or not* $\gamma_A=\varnothing$ *can be effectively decided* (*by the method given in proof*) *and if* $\gamma_A\neq\varnothing$, *one can effectively produce an automaton satisfying the condition* (*by the method below*).

Proof. From 8.6.1 and 8.6.2, it follows that

$$\lim \mathfrak{J}(\mathfrak{N}) \subseteq \beta \Leftrightarrow \mathfrak{J}(\mathfrak{N}) \subseteq \beta^L.$$

The set β^L may be effectively obtained (8.5 (4)). The problem is now reduced to 8.1.

8.6.4. In connection with 8.6.3, it should be noted that:

$$\lim \mathfrak{I}(\mathfrak{N}) \subseteq \beta \Leftrightarrow \bigwedge_{a,b} \cdot \mathcal{G}_{\mathfrak{N}}[a, b] \supset \bigvee_{s} \bigwedge_{x} M[a, b, s, x]$$

where $\mathcal{G}_{\mathfrak{N}}$, $\mathfrak{N}$ are as in 8.6.1.

9. Remark. We give a metamathematical proof that the set

$$\beta = \{a^{(n)}ba^{(n)} \mid n \geqq 0\}$$

is not regular. Let a, $b \in U_2^0$. If the set were regular, then there would be a formula $\mathfrak{F}[f]$ of L_1^1 such that $T_2\mathfrak{F} = \beta$. Then $y = 2x \Leftrightarrow \bigvee_f \cdot f(x) = b \wedge f(y) \neq 0 \wedge \bigwedge_z (z > y \supset f(z) = 0) \wedge \mathfrak{F}[f]$. Thus regularity of β implies that doubling is definable in L_1^1 and by results of R. M. Robinson [10] it would follow that the set of true sentences of L_1^1 is not effective, contradicting 5.8.

Chapter IV. Nonexistence of Certain Algorithms

10. Let L_2 be the class of well-formed formulas constructed out of individual variables and monadic predicate variables, by means of the successor operation ($'$), addition ($+$), $=$, propositional connectives, and first order quantification.

Let L_2^1 be the system consisting of L_2 with the individual variables ranging over natural numbers and the monadic predicates range over properties of natural numbers which are ultimately false and remain false (we could have used finite set variables instead, as in 5) and the unary and binary (nonlogical) operations interpreted as indicated and the logical operators and $=$ interpreted in standard fashion.

It will be convenient, as a device for abbreviation similar to 5.3 remark, to employ unary function symbols (we shall use "i") in formulas such as $i(x) = a$ where $a \in A$ and A is a finite set of symbols. By coding A, i.e., putting A into 1-1 correspondence with a set of r-tuples of zeros and ones, for appropriate r, the function symbol "i" may be replaced by a sequence of r distinct monadic predicate variables. To say i is free means that the associated r monadic predicate variables are free. If $\sigma = abc$ is a word (finite sequence), $a, b, c \in A$, then $i(x)i(x+1)i(x+2) = \sigma$will abbreviate $i(x) = a \wedge i(x+1) = b \wedge i(x+2) = c$.

Notice that in L_2^1:

$$x = 0 \Leftrightarrow x + x = x,$$
$$x < y \Leftrightarrow \bigvee_{u} x + u = y \wedge u \neq 0,$$

so that as further abbreviations, we shall employ 0, $<$.

Given a formula $G = G[i, m]$ in which only i, m occur free where i is a unary function (interpreted as a function on the natural numbers with values in a finite set B) and m is a monadic predicate. With each i, m such that

$G[i, m]$ is true and $m(0)$ holds associate the finite sequence $T_G(i, m)$ of words (in B) whose first n words are $i(1)i(2) \cdots i(x_1)$, $i(x_1+1)i(x_1+2) \cdots i(x_2)$, $\cdots$, $i(x_{n-1}+1)i(x_{n-1}+2) \cdots i(x_n)$ where $0<x_1<x_2< \cdots <x_n$ are the first $n+1$ numbers for which m holds. Let $T(G)$ be the set of all $T_G(i, m)$ such that $G[i, m]$ is true and $m(0)$ holds.

10.1. Lemma. *For every Post normal system P there is a formula $F=F(P)$ in L_2^1 such that $T(F)$ is the set of all proofs of P.*

Proof. Let $C_m(x, y)$ abbreviate:

$$m(x)m(y)(x < y) \bigwedge_z (x < z < y \supset {\sim}m(z)),$$

i.e.,

$$\begin{aligned} & m(x) \wedge m(y) \wedge \bigvee_u x + u = y \wedge {\sim} u + u = u \\ & \wedge \bigwedge_z \Big[\Big(\bigvee_u x + u = z \wedge {\sim} u + u = u \\ & \qquad\qquad \wedge \bigvee_u z + u = y \wedge {\sim} u + u = u\Big) \supset {\sim} m(z)\Big]. \end{aligned}$$

With each production of P

$$\overset{k}{(\sigma_1, \sigma_2)} : \overset{k}{\sigma}_1\beta \rightarrow \beta\overset{k}{\sigma}_2$$

associate the formula

$$\begin{aligned} S_{\overset{k}{\sigma}_1, \overset{k}{\sigma}_2}(w, x, y) &: i(w + 1)i(w + 2) \cdots i(w + l(\overset{k}{\sigma}_1)) = \overset{k}{\sigma}_1 \wedge \bigvee_u u + l(\overset{k}{\sigma}_2) = y \\ & \wedge i(u + 1)i(u + 2) \cdots i(u + l(\overset{k}{\sigma}_2)) = \overset{k}{\sigma}_2 \\ & \wedge \bigvee_z \Big[z + w + l(\overset{k}{\sigma}_1) = x \wedge z + x + l(\overset{k}{\sigma}_2) = y \\ & \wedge \bigwedge_u \Big({\sim} u + u = u \wedge \textstyle\bigvee_v u + v = z \supset i(w + l(\overset{k}{\sigma}_1) + u) = i(x + u)\Big)\Big] \end{aligned}$$

where $l(\sigma)$ represents the length of σ. This formula expresses the condition that $i(w+1)i(w+2) \cdots i(x) = \sigma_1^k\beta$ and $i(x+1)i(x+2) \cdots i(y) = \beta\sigma_2^k$ for some β. Let $(\sigma_1, \sigma_2)^1$, $(\sigma_1, \sigma_2)^2$, $\cdots$, $(\sigma_1, \sigma_2)^n$ be the productions of P and let α be the axiom of P and define

$$\begin{aligned} S^P(i, m) : \bigwedge_{w,x,y} & \Big[(C_m(w, x)C_m(x, y) \supset S_{\overset{1}{\sigma}_1, \overset{1}{\sigma}_2}(w, x, y) \vee \cdots \vee S_{\overset{n}{\sigma}_1, \overset{n}{\sigma}_2}(w, x, y)) \\ & \wedge (w = 0 \supset x = l(\alpha) \wedge i(1)i(2) \cdots i(l(\alpha)) = \alpha)\Big]. \end{aligned}$$

Then F is

$$\Big[S^P(i, m) \wedge m(0) \wedge \bigvee_{x,y} x \neq 0 \wedge y \neq 0 \wedge x \neq y \wedge m(x) \wedge m(y)\Big] \vee m(0)$$
$$\wedge \bigvee_x \Big[x \neq 0 \wedge m(x) \wedge \Big(\bigwedge_y y \neq 0 \wedge m(y) \supset y = x\Big) \supset x = l(\alpha)$$
$$\wedge\, i(1)i(2) \cdots i(l(\alpha)) = \alpha\Big].$$

10.2. Theorem. *The set of satisfiable formulas of L_2^1 is effectively enumerable but not effective. Indeed, the degree of unsolvability of this set is maximum among all effectively enumerable sets. If P is a Post normal system with* 2 *letters* (*see M. Davis, Computability and unsolvability, New York, McGraw-Hill,* 1958, p. 100, *Theorem* 5.3) *which generates the complete* (*Post,* 1944) *set of natural numbers and if $F_n = F(P) \wedge \bigvee_x C_m(x, x+n+1) \wedge i(x+1) = 1 \wedge i(x+2) = 1 \wedge \cdots \wedge i(x+n+1) = 1$, then every recursively enumerable set is recursive in the set of Gödel numbers of the satisfiable formulas F_n.*

Proof. $n \in S_p$ (see Davis, p. 85, Definition 1.ii) if and only if $\bigvee_{i,m} F_n$ is true, i.e., if and only if F_n is satisfiable.

The fact that the satisfiable formulas are effectively enumerable follows readily from the Presburger result.

10.3. It is clear that the results of 10.1 and 10.2 hold if the individual variables are interpreted over positive integers rather than non-negative integers. Hence, one obtains for either the non-negative integers or the positive integers:

Corollary. *If L_2^2 is the system consisting of the formulas L_2 but with the interpretation of the predicates unrestricted, then the set of satisfiable formulas of L_2^2 is not effective.*

Proof. The property of a predicate that it becomes ultimately false and remains so is definable in L_2^2.

This (for positive integers) is Putnam's Theorem 4 [8, p. 50]. Putnam's argument can, however, be adapted to give the stronger result: The set of satisfiable formulas of L_2^2 is not arithmetic.

10.4. Let L_2^3 be the system consisting of the class of formulas L_2 with individual variables interpreted as ranging over all the integers and with the predicates ranging over finite sets of integers.

Analogues of the lemma of 10.1 and the theorem of 10.2 hold for L_2^3. $T(G)$ is defined exactly as before.

Notice that in L_2^3:

$$x = 0 \Leftrightarrow \bigvee_x x + x = x, \quad x = 1 \Leftrightarrow \bigvee_y y = 0 \wedge y' = x,$$
$$x > 0 \Leftrightarrow \bigvee_p \bigwedge_y [p(y) \wedge y \neq 1 \supset p(y-1)] \wedge p(x)$$

and

$$p(y-1) \Leftrightarrow \bigvee_{z} z' = y \wedge p(z).$$

To establish the analogues for L_2^3, we show that "$\vee_p$" can be moved all the way to the left.

Let $D(p)$ stand for $\wedge_y\ [p(y) \wedge y \neq 1 \supset p(y-1)]$. Notice that $D(p)$ holds for p if and only if p is a consecutive set of positive integers beginning with 1.

Then $F = F(i, m)$ is modified by conjoining $\wedge_x\, m(x) \supset D(p) \wedge p(x)$ and prefixing the conjunction by $\vee_p$. In the formula F, wherever one wishes to express $x < y$, one writes $\vee_u\, x + u = y \wedge p(u)$.

10.5. Let L_2^4 be the system consisting of the class of formulas L_2 with individual variables interpreted over natural numbers and predicates interpreted over ultimately periodic sets (a set of natural numbers is ultimately periodic if its characteristic function is).

COROLLARY. *The set of satisfiable formulas of L_2^4 is effectively enumerable but not effective. The degree of unsolvability of this set is maximum among all recursively enumerable sets.*

Proof. That the set of satisfiable formulas is effectively enumerable follows from the Presburger result. The rest of the statement follows from the fact that the property of a predicate of being finite is definable in L_2^4 and from 10.2.

A similar result holds for "integers" in place of "natural numbers".

10.6. COROLLARY. *Given an input-free automaton $\mathfrak{N}$ and a formula B of L_2^4 in which the predicates are interpreted as outputs: the problem of deciding whether $\mathfrak{N}$ satisfies B is effectively decidable while the question "does there exist an $\mathfrak{N}$ such that $\mathfrak{N}$ satisfies B?" is undecidable.* See Büchi, Elgot and Wright [1] and Elgot and Wright [4, p. 68, last paragraph].

BIBLIOGRAPHY

1. J. R. Büchi, C. C. Elgot and J. B. Wright, *The non-existence of certain algorithms of finite automata theory* (Abstract), Notices Amer. Math. Soc. vol. 5 (1958) p. 98.

2. A. Church, *Application of recursive arithmetic in the theory of computers and automata*, Lecture Notes, Summer Conference, University of Michigan, June, 1958.

3. I. M. Copi, C. C. Elgot and J. B. Wright, *Realization of events by logical nets*, J. Assoc. Comput. Mach. vol. 5 (1958) pp. 181–196.

4. C. Elgot and J. Wright, *Quantifier elimination in a problem of logical design*, Michigan Math. J. vol. 6 (1959) pp. 65–69.

5. S. C. Kleene, *Representation of events in nerve nets and finite automata*, Automata Studies, Princeton University Press, 1956, pp. 3–41.

6. I. T. Medvedev, *On a class of events representable in a finite automaton* (translated from the Russian by J. Schorr-Kon), M.I.T. Lincoln Lab. Group Report, June 30, 1958, pp. 34–73.

7. E. F. Moore, *Gedanken-experiments on sequential machines*, Automata Studies, Princeton University Press, 1956, pp. 129–153.

8. H. Putnam, *Decidability and essential undecidability*, J. Symb. Logic vol. 22 (1957) pp. 39–54.

9. M. Rabin and D. Scott, *Finite automata and their decision problems*, Report, IBM Research Center, Lamb Estate, Yorktown, New York, 1958.

10. R. M. Robinson, *Restricted set-theoretical definitions in arithmetic*, Proc. Amer. Math. Soc. vol. 9 (1958) pp. 238–242.

University of Michigan, Research Institute,
Ann Arbor, Michigan