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


(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.

21
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 $\mathfrak{A} = (S, f, d, D)$ 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, $f: I \times S \rightarrow S$ (the transition function), $d \in S$ (the initial internal state), and $D \subseteq S$ ($D$ may be called the output of $\mathfrak{A}$).

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

1. $f(i_k, s_k) = s_{k+1}$, $0 \leq k \leq n - 1$, $s_k \in S$, $i_k \in I$,
2. $s_n \in D$,
3. $s_0 = d$.

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

(c) $\mathfrak{T}(\mathfrak{A})$ may also be described as the set of all functions $i: \{0, 1, 2, \ldots, n-1\} \rightarrow I$, $n \geq 0$ (the empty function is included) satisfying the formula:

\[
\forall s, \exists \alpha \in I \times S, \exists u \in S, f(s) = s_{k+1} = f(i_{k+1}) = f(c_k) \cap [(i(x), s(x)) = c_k \cap (s(x) = f(c_k)) \cap \cdots \cap [(i(x), s(x)) = c_m \cap (s(x) = f(c_m))]
\]

where $c_1, c_2, \ldots, c_m$ is an enumeration of all 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 $\Lambda$). If $\alpha, \beta \subseteq V_I$, then $\alpha \cdot \beta$ is the subset of $V_I$ obtained by concatenating a sequence from $\alpha$ with a sequence from $\beta$; $\alpha^* = \{\Lambda\} \cup \alpha \cup \alpha \cdot \alpha \cup \alpha \cdot \alpha \cdot \alpha \cup \cdots$. A subset of $V_I$ is $I$-regular if and only if it is obtainable from $\emptyset$ and the unit sets, $\{a\}, a \in I$, by a finite number of applications of $\cup$, ·, *.

Otherwise stated: The class of $I$-regular sets is the smallest class containing $\emptyset$, $\{a\}, a \in I$, and closed under $\cup$, ·, *. An $I$-regular expression is constructed out of symbols denoting each $\{a\}, a \in I$, $\emptyset$ (the empty set), and $\cup$, ·, *.

[Note that $\emptyset^* = \{\Lambda\}$.] 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 $\mathfrak{A}$ is an $I$-automaton, then $\mathfrak{T}(\mathfrak{A})$ is $I$-regular and an $I$-regular expression denoting $\mathfrak{T}(\mathfrak{A})$ may effectively be obtained. Conversely, if $\alpha$ is $I$-regular, then there exists an $I$-automaton such that $\mathfrak{T}(\mathfrak{A}) = \alpha$ and, furthermore, $\mathfrak{A}$ may be effectively obtained from an $I$-regular expression denoting $\alpha$. 
The following statement is immediate from the definition of $I$-regular.

3.2. If $\alpha$ is $I$-regular and if $I \subset J$, then $\alpha$ 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 $\hat{p}$ 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 $\hat{p}$. This homomorphism in turn induces a mapping $\hat{p}$ on subsets of $F_I$ onto subsets of $F_J$. If $\alpha$ 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 $\alpha$.

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

**Proof.** Suppose $\alpha$ is $I$-regular and $\hat{p}: I \rightarrow J$. If $a \in I$, then $\hat{p}\{a\} = \{\hat{p}(a)\}$ 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 $\mathcal{A}$ and a $p: I \rightarrow J$, yields a $J$-automaton $\mathcal{B}$ such that $T(\mathcal{B}) = \hat{p}(T(\mathcal{A})))$.)

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

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 $\alpha$ 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 $\beta$ is the set denoted by this polynomial under this assignment, then $\hat{p}(\beta) = \alpha$.

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

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

(ii) $V_A + U(a, b)_{a \in A \times A} E_A(a, b) = \{A, a_1, a_2, \cdots, a_n\}$ where $\{a_1, a_2, \cdots, a_n\} = A$ and $U(a, b)_{a \in A \times A} E_A(a, b)$ 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

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

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

(v) Let $S_A(a) = \{au | a \in A \land u \in V_A\}$. Let $R$ be a binary relation on $A \cup \{b\}, b \in A$, viz., $[(x, y) \in R] \Leftrightarrow [(x = b \land y \in A) \lor (x \in A \land y \in A)] \Leftrightarrow [y \in A \land (x = b \lor x \in A)]$. 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 $p : A \cup \{b\} \to A$ takes $b$ into $a$ and is the identity on $A$, then

$$p(M) = S_A(a).$$

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

Now let $\mathfrak{M} = (S, f, d, D)$ 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 $p$, where $p(i, s) = i$ for all $(i, s) \in I \times S$, yields $T(\mathfrak{M}) - \{A\}$. (Cf. the definition of $T(\mathfrak{M})$.)

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 $T(\mathfrak{M})$, $\mathfrak{M}$ 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

$V_A, E_A(a, b), S_A(a), T_A(a)$

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 \( n \), \( u = v b^{(n)} \), \( (n \) iterations of \( b) \), \( n \geq 0 \), and \( v \) does not terminate with \( b \), then \( u^b = v \). This is called right truncation of \( u \) by \( b \). If \( \alpha \) is a set of finite sequences, then \( \alpha^b = \{ u^b | u \in \alpha \} \) (right truncation of \( \alpha \) 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 \( b \).

\[ u \in (\alpha \cdot \beta)^b \iff \forall n \left[ u b^{(n)} \in \alpha \cdot \beta \land n \geq 0 \land \sim p_b(u) \right] \]

\[ \iff \forall \left[ u_1 u_2 = u b^{(n)} \land n \geq 0 \land u_1 \in \alpha \land u_2 \in \beta \land \sim p_b(u) \right] \]

\[ \iff \forall \left[ u_1 u_2 = u b^{(n)} \land n \geq 0 \land u_1 \in \alpha \land u_2 \in \beta \right] \]

\[ \lor l(u_2) > n \]

\[ \lor (u_1 u_2 = u b^{(n)} \land n \geq 0 \land u_1 \in \alpha \land u_2 \in \beta \land \sim p_b(u) \land l(u_2) \leq n) \]

\[ \iff \forall \left[ (u_1 \cdot u_2 = u \land u_2 \neq \Lambda \land u_1 \in \alpha \land u_2 \in \beta) \right] \]

\[ \lor (u = u_1 \land u_2 = \Lambda \land u_1 \in \alpha \land u_2 \in \beta) \]

\[ \iff \forall \left[ (u = u_1 \cdot u_2 \in \alpha \land u_2 \in \beta \land u_2 \in \beta \land \{ \Lambda \}) \land u_1 \in \alpha \land u_2 \in \beta \right] \).

(b) \( u \neq \Lambda \land u \in (\alpha^*)^b \)

\[ \iff \forall \left[ u b^{(n)} \in \alpha^* \land n \geq 0 \land \sim p_b(u) \land u \neq \Lambda \right] \]

\[ \iff \forall \left[ n \geq 0 \land r > 0 \land u_1 u_2 \cdots u_r \right] \]

\[ = u b^{(n)} \land \land u_i \in \alpha \land \sim p_b(u) \land u \neq \Lambda \]

\[ \iff \forall \left[ m > 0 \land u = u_1 u_2 \cdots u_{m-1} u_m^b \land u_m \neq \Lambda \land \land u_i \in \alpha \right] \]

\[ \iff u \in \alpha^* \cdot (\alpha^b - \{ \Lambda \}) \).
4.2. Lemma. The class of regular sets is closed under right truncation. Moreover, from a regular expression denoting $\alpha$ one can obtain effectively a regular expression denoting $\alpha^*$. Analogous statements hold for left truncation.

Proof. If $x$ is a letter, then $\{x\}^* \neq \{x\}$ if $b \neq x$ and $\{x\}^* = \{A\}$ 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

\[(a) \quad x_i \in F_j, \quad x_i' \in F_j, \ldots, \quad x_i^{(r)} \in F_j, \ldots;
(b) \quad x = y, \quad x < y,
\]

by means of propositional connectives and quantifiers $\forall x_i, \forall F_j$. 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 $L_1^r$. If $A \{F_1, F_2, \ldots, F_r\}, \ r \geq 0,$ is a formula in which at most the variables $F_1, F_2, \ldots, F_r$ (the first $r$ set variables in the alphabet of $L_1$) occur free, then associated with $A$ is the class of $r$-tuples $(F_1, F_2, \ldots, F_r)$ of finite sets for which $A \{F_1, F_2, \ldots, F_r\}$ 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:

\[
f(n) = \begin{cases} a_1 \\ \vdots \\ a_r \\ \vdots \\ \end{cases} & \text{if and only if } n \in F_i \equiv a_i = 1.
\]

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 $\sigma_r$ be the restriction of $f$ to the domain $\{0, 1, 2, \ldots, x\}$; $\sigma_r$ may be identified with the $r \times (x+1)$ matrix whose $i$th column is $f(i)$. Moreover $\sigma_r$ 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, $s \geq 0$, 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 $L_1^r$ is associated a set $T_r(A)$ of admissible $r \times s$ matrices, $s \geq 0$, 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 $T_r(A) = \{A\}$ if $A$ is true and $T_r(A) = \emptyset$ if $A$ is false.] Let $U_r$ be the set of all $r$-tuples of zeros and ones, $s \geq 0$; let $U_r = U_r - \{0_r\}$ where $0_r$ is the all zero $r$-tuple. [If $r = 0$, let $U_r = \{0\}, \ U_r = \emptyset$. Recall that $V_0 = \emptyset^* = \{A\}$.]
5.2. Notice that in $L_1$:

\[ x = y \iff \bigwedge_{F} \left( x \in F \equiv y \in F \right), \]
\[ x = 0 \iff \bigwedge_{F} \sim y' = x, \]
\[ x < y \iff \bigvee_{F} \left[ \bigwedge_{F} \left( z' \in F \implies z \in F \right) \land x \in F \land y \in F \right]. \]

5.3. Theorem. (a) If $A[F_1, F_2, \ldots, F_r]$ is a formula of $L_1$, 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 $\alpha \subseteq U_r$ of admissible sequences there is a formula $E(A)$ of $L_1$ 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 $\alpha$ be an arbitrary $I$-regular set. Let $p$ be a 1-1 mapping of $I$ into $U_0^0$. Then $p(\alpha)$ is a $U_0^0$-regular set ("isomorphic" to $\alpha$, i.e., the set is $\alpha$ in coded form) and so there is a formula $A$ of $L_1^1$ such that $T_r(A) = p(\alpha)$.

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 natural numbers and range an element of $U_r$ and satisfying $(f(x)) = 1 \iff x \in F_i$ as well as the property $\bigvee z f(x) = 0_r \land \bigwedge_{y} (y > x \implies f(y) = 0_r)$, 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 $(F_1, F_2, \ldots, F_r)$, then $V_f$ abbreviates $V_{F_1} V_{F_2} \cdots V_{F_r}$.

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

Proof. Observe that

\[ V \land C = V \land \bigwedge_{G,F} \left[ (G(x) \supset C) \land V G(z) \right] \]

(1)

and

\[ \land V C = \land V \bigwedge_{G,F} \left[ V G(z) \supset G(x) \land C \right] \]

(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 \( V_s[A] \) is the right-most 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

\[
\forall \left[ x^{(m_0)} \eta F_{k_0} \land x^{(m_1)} \eta F_{k_1} \land \cdots \land x^{(m_r)} \eta F_{k_r} \right],
\]

where each occurrence of \( \eta \) is independently \( \subseteq \) or \( \in \), will be called a principal formula where \( 0 \leq m_0 < m_1 < \cdots < m_r \).

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 \( L_1 \) is equivalent to a formula of \( L_1 \) 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 \( V_s A \). \( V_s \) distributes over the disjuncts of \( A \). Let \( D \) be a disjunct of the form \( D_1(x) \land D_2 \) where \( x \) does not occur free in \( D_2 \) and no variable other than \( x \) occurs free in \( D_1 \). Then \( V_s D = D_2 \lor V_s D_1(x) \).

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 \( V_u \) is \( U^* \cdot U^0 \cup \{A\} \) and is, therefore, regular.

5.6. Proof of 5.3 (a). Consider a formula of \( L_1 \) 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
\[ T_r(A \land B) = T_r(A) \cap T_r(B), \]
\[ T_r(A \lor B) = T_r(A) \cup T_r(B), \]
\[ T_r(\neg A) = \text{compl} \ T_r(A) \]

[complementation is with respect to the set of all admissible sequences in \( V_{ur} \) (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 \( A = A \left[F_1, F_2, \ldots, F_r\right], r > 1 \), then \( T_{r-1}(V_{fr}, A) \) is the set obtainable from \( T_r(A) \) by deleting the \( r \)-th row followed by right truncation of the all zero \((r-1)\)-tuple, i.e., if \( r > 1 \)
\[ T_{r-1} \left( \bigvee_{F_r} A \right) = (p_r(T_r(A)))^b \]
where \( p_r \) maps an \( r \)-tuple of zeros and ones onto the \((r-1)\)-tuple obtained by deleting the \( r \)-th component and \( b \) is the all zero \((r-1)\)-tuple. Hence \( T_{r-1}(V_{fr}, A) \) is regular and from a regular expression for \( T_r(A) \) one may effectively obtain one for \( T_{r-1}(V_{fr}, A) \).

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
\[
\bigvee_{\eta} \bigwedge_{z \in \text{sig}_r} (x_\eta F_i \land x'\eta F_i),
\]
where each occurrence of \( \eta \) is independently \( \in \text{or} \in \). This follows from the fact that (assuming \( m > 1 \))
\[
x^{(m)} \eta F \iff y_1 = x' \land y_2 = y'_1 \land \cdots \land y_{m-1} = y'_{m-2} \land y'_{m-1} \eta F \equiv \bigwedge_{\eta} \left[ y_1 \in G \iff x' \in G \land y_2 \in G \equiv y'_1 \in G \land \cdots \land y_{m-1} \in G \equiv y'_{m-2} \in G \land y'_{m-1} \eta F \right]
\]
and
\[
x \eta F \iff (x \eta F \land x' \in F) \lor (x \eta F \land x' \notin F),
x' \eta F \iff (x \in F \land x' \eta F) \lor (x \notin F \land x' \eta F).
\]

Let \( A \) be \( V_r \left[f(x) = a \land f(x') = b\right] \) (cf. Remark 5.3).

CASE I. \( a \in U_r \) and \( b \in U_r^0 \). Then
\[ T_r(A) = U_r^* \cdot \{a\} \cdot \{b\} \cdot ((U_r^* \cdot U_r^0) \lor \{A\}). \]

CASE II. \( a \in U_r^0 \) and \( b = 0_r \). Then
\[ T_r(A) = (U_r^* \cdot \{a\}) \cup (U_r^* \cdot \{a\} \cdot \{b\} \cdot U_r^* \cdot U_r^0). \]
Case III. \(a = 0_r = b\). Then

\[ T_r(A) = (U_r^* \cdot U_r^0) \cup \{A\}. \]

5.7. Proof of 5.3 (b). Let \(\alpha \subseteq V_r\) be a regular set of admissible sequences. Then \(\alpha - \{A\}\) is regular and is a projection of a regular set \(\beta \subseteq V_{r+s},\ s > 0\). Specifically: there exists a \(U_r\)-automaton \(\mathfrak{N} = (S, f, d, D)\) such that \(\alpha = T(\mathfrak{N})\). Without loss of generality, let \(S\) be a subset of \(U_r^0\) for a suitable \(s > 0\). The complete states \(U_r \times S\) of \(\mathfrak{N}\) may be identified with a subset of \(U_{r+s}\) as follows:

\(\langle x, y \rangle \in U_r \times S\) is identified with the \((r+s)\)-tuple whose \(i\)th member, \(1 \leq i \leq r\), is the \(i\)th member of \(x\) and whose \((r+j)\)th member, \(1 \leq j \leq s\), is the \(j\)th member of \(y\). Let \(B \subseteq U_r^0\), be the set \(\{\langle x, f(x, d) \rangle | x \in U_r\}\). Let \(E = U_r^0 \times D\). Define \(R \subseteq U_{r+s}^0 \times U_{r+s}^0\) 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 \(\beta\) is the set of finite \(R\)-sequences beginning with an element of \(B\) and ending with an element of \(E\) and \(\alpha = \beta(\beta)\) where \(\beta\) is the mapping which takes \(\langle x, y \rangle \in U_r \times S\) into \(x\).

\(\beta\) is the intersection of the three following sets.

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

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

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

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

a) Let \(B = \{b_1, b_2, \ldots, b_n\}\). \(b_k\) is the \(k\)th component of \(b_i\). For each \(b_i\) the formula \(A^i: A_{1 < k < r+s} x_{\eta_i} F_k,\) where \(\eta_i\) is \(\in\) if \(b_i^k = 1\) and \(\notin\) otherwise, corresponds to \(S_{U_{r+s}}(b_i)\), so that (a) corresponds to \(A^1 \lor A^2 \lor \cdots \lor A^n\). Then \(A^1 \lor A^2 \lor \cdots \lor A^n\) is an abbreviation of a formula \(A\) of \(L_1\) and

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

b) Let \(E = \{e_1, e_2, \ldots, e_n\}\). With each \(e_i\) associate the formula

\[ A^i: \bigvee_{\eta} \bigwedge_{x_{\eta}} F_k \land \bigwedge_{y} (y > x \supset (y \in F_1 \land y \in F_2 \land \cdots \land y \in F_{r+s})), \]

where \(\eta\) is \(\in\) if \(e_i^k = 1\) and otherwise \(\notin\). Then \(A^1 \lor A^2 \lor \cdots \lor A^n\) is an abbreviation of a formula \(A\) of \(L_1\) 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 \(\{e_1, f_1\}, \{e_2, f_2\}, \ldots, \{e_n, f_n\}\) \(= H\). With each \(e_i\) associate \(A(e_i): A_{1 < k < r+s} x_{\eta_i} F_k\) where \(\eta_i\) is \(\in\) or \(\notin\) depending on whether \(e_i^k = 1\) or not. With each \(f_i\) associate \(B(f_i): A_{1 < k < r+s} x_{\eta_i} F_k\) where \(\eta_i\) is \(\in\) or \(\notin\) depending on whether \(f_i^k = 1\) or not. Then if \(A\) is the formula abbreviated by \(\bigwedge_{x} V_{1 < k < n} A(e_i) \land B(f_i)\), then \(T_{r+s}(A)\) is the set (c).
If \( \mathcal{F} \) is the conjunction of the formulas a), b), c), then \( T_{r+1}(\mathcal{F}) = \beta \) and 
\[ T_{r}(\bigvee_{\mathcal{F}+1} \bigvee_{\mathcal{F}+2} \cdots \bigvee_{\mathcal{F}+r} \mathcal{F}) = \alpha. \]
Note that \( \{ \Delta \} = T_{r}(\bigvee_{x \in \mathcal{F}} x). \)


The set of true sentences of \( L_{1} \) is effective.

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

(a) \[ \bigvee_{\mathcal{F}} A[F] \]
or

(b) \[ \sim \bigvee_{\mathcal{F}} A[F] \]

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 \( \mathcal{A} = (S, f, d, D) \) 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 \( T_{0}(\mathcal{A}) \) 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 \( r(F) = \sum_{x \in F} 2^x \). Then \( r \) is a 1-1 correspondence between the class of all finite subsets of the natural numbers and the natural numbers.

\[ r(G) = r(F_1) + r(F_2) \iff \bigvee_{C} \bigwedge_{x} (x' \in C \iff (x \in F_1 \land x \in F_2) \lor (x \in F_1 \land x \in C) \land (x \in F_2 \land x \in C) \land (x \in F_1 \land x \in F_2 \land x \in C)) \]

where \( \Delta \) represents "exclusive or". Thus:

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

(4*) 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 \(n, m \geq 1\), consider the \(2^{2n} n\)-place predicates

\[
\forall x \left[ x \in F_1 \land x \in F_2 \land \cdots \land x \in F_n \land x' \in F_1 \land x' \in F_2 \land \cdots \land x' \in F_n \right]
\]

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

**Corollary.** The first order arithmetic theory based upon \(\tau \mathcal{O}\) 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 \(\tau \mathcal{O}\), not every predicate in \(\tau \mathcal{O}\) is definable in the first order theory of addition.

**Proof.** \(\forall x \left[ x \in F \land x' \in F \land y \in F \right] \left( y = x \lor y = x' \right) \right)\) is the set \(3, 6, 12, 24, \ldots\), 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 \(\cap, \cup, \ominus\) (symmetric difference), \(\emptyset\), =, and the unary operation \(F \mapsto F^*\) defined by

\[
x \in F^* \text{ if and only if } \forall y \left[ x \leq y \land y \in F \right]
\]

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 \(\cap, \cup, \ominus\), and the relations \(F = G\) and \(F = \emptyset\) are definable in \(L_1^1\). The principal formula \(\forall x \left[ x \in G_1 \land x' \in G_1 \land x \notin G_2 \land x' \in G_2 \right]\) 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):

\[
\forall F_1, F_2, F_3 \left[ F_1 = F_1^* \land F_2 = F_2^* \land F_3 = F_3^* \land F_1 \subseteq F_2 \subseteq F_3 \right]
\]

\[
\land \left[ (G - G^* \land F_1 \subseteq G \land F_2 \subseteq G) \land (G = G^* \land F_2 \subseteq G \land F_2 \subseteq G) \right]
\]

\[
\land F_2 \ominus F_1 \subseteq G_1 \land F_3 \ominus F_2 \subseteq G_2 \land (F_2 \ominus F_1) \cap G_2 = \emptyset \right].
\]
Similarly for other principal formulas.

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

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

\[
\tau(\cap) y = z \iff \tau^{-1} x \cap \tau^{-1} y = \tau^{-1} z,
\]

\[
\tau(\oplus) y = z \iff \tau^{-1} x \oplus \tau^{-1} y = \tau^{-1} z.
\]

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

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 $L_2^*$ 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 $A[F_1, F_2, \ldots, F_r]$ of $L_2^*$ and for each integer $l$, $A[F_1, F_2, \ldots, F_r] = A[F_1', F_2', \ldots, F_r']$ where $x \in F_1 \iff x - l \in F_1$, i.e., the class of $r$-tuples of finite sets defined by a formula of $L_2^*$ is closed under translation (cf. 5.13).

**Lemma 1** of 5.5 is valid for $L_2^*$. 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 $A[F_1, F_2, \ldots, F_r]$ or in $\sim A[F_1, F_2, \ldots, F_r]$ 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 $A[F_1, F_2, \ldots, F_r]$ of $L_1^*$ a set $T^2_\tau(A[F_1, F_2, \ldots, F_r])$ 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 $A[F_1, F_2, \ldots, F_r]$ is a formula of $L_2^*$, then $T^2_\tau(A)$ is $U_r$-regular and one can effectively find a regular expression which denotes $T^2_\tau(A)$.

(b) For every regular set $\alpha$ of admissible-2 $U_r$-sequences there is a formula $E(A)$ of $L_2^*$ such that $T^2_\tau(E(A)) = \alpha$ 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 $L_2^*$.

5.13. In $L_1^*$:
\[ x = y \iff \bigwedge_{F} (x \in F \iff y \in F), \]
\[ x < y \iff \bigwedge_{F, z} [(z \in F \land z \neq x \cup z' \in F) \cup y \in F]. \]

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 \( A = \cup r \) for appropriate \( r \). There is a formula \( \exists \mathcal{F}[f] \) such that \( T_{\mathcal{F}} = \alpha \). It is sufficient to prove the theorem for \( A = b \). Then \( f(x) = 0 \iff x > 0 \). Let \( g[g] \) be the formula:

\[ \forall_{f} \wedge \left\{ \exists \mathcal{F}[f] \land f(y') = 0 \iff f(y) \neq 0, \exists_{z} \left[ f(y) \neq b \cup \bigwedge_{z} f(z) = g(x) \right] \right\} \]
\[ \wedge \left[ f(y) = b \cup \bigwedge_{z} \left[ f(x) = b \iff \left( \forall_{z'} f(z') = x \cup f(z) \neq b \right) \right] \right) \]
\[ \wedge \left( \bigwedge_{z} x \cdot f(x) = b \lor f(z) = 0 \iff \bigwedge_{w} g(w) = f(w) \right) \]
\[ \wedge \left( \forall_{w} g(w) = 0 \right) \].

Then \( T_{\mathcal{F}} = \alpha \cdot b \). 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 \( L_1^8 \) 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 \( F_1, F_2, \ldots, F_r \) be quasi-finite sets. Let \( c_k(n) = 1 \iff n \in F_k \). Let
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 $\Lambda_y y > x \supset c(y) = c(x)$. The function $c$ restricted to the first $x$ such that this property holds is an element $\sigma^r_1(F_1, F_2, \ldots, F_r)$ of $V_{U_r}$.

Moreover, $c$ is 1-1. Briefly: $\sigma^r_1(F_1, F_2, \ldots, F_r) = f$ where domain $f = \{x | x \leq y\}$ and $y = (\mu z) \Lambda_i [\Lambda_z z \geq x \supset x \in F_i \cdot \vee \cdot \Lambda_z z \geq y \supset f(y) = f(z)]$. The image of $\sigma^r_1$ is the set of all admissible-3 elements of $V_{U_r}$. If $A [F_1, F_2, \ldots, F_r]$ is a formula of $L_3^r$, then $T_{\sigma^r_1}(A)$ is the set of all $\sigma^r_1(F_1, F_2, \ldots, F_r)$ such that $A [F_1, F_2, \ldots, F_r]$ holds.

Notice that 5.2 holds in $L_3^r$.

**Theorem.** (a) If $A [F_1, F_2, \ldots, F_r]$ is a formula of $L_3^r$, then $T_{\sigma^r_1}(A)$ 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 $L_3^r$ such that $T_{\sigma^r_1}(E(A)) = \alpha$ 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 “$L_3^r$” in place of “$L_3^r$”. If $A, B$ are formulas of $L_3^r$ with at most $F_1, F_2, \ldots, F_r$ free, then

$$T_{\sigma^r_1}(A \land B) = T_{\sigma^r_1}(A) \cap T_{\sigma^r_1}(B),$$

$$T_{\sigma^r_1}(A \lor B) = T_{\sigma^r_1}(A) \cup T_{\sigma^r_1}(B),$$

$$T_{\sigma^r_1}(\neg A) = \text{compl } T_{\sigma^r_1}(A)$$

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

If $\alpha = T_{\sigma^r_1}(A)$, then $T_{\sigma^r_{r-1}}(V_{F_r}(A)) = (\cdots (((p(\alpha) \cdot a) \cdot b) \cdots)$ where $p$ maps an element of $U_r$ into the element obtained by deleting the $r$th 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 $T_{\sigma^r_{r-1}}(V_{F_r}(A))$ is regular.

It remains only to show that if $A$ is $V_s [f(x) = a / f(x') = b]$, then $T_{\sigma^r_1}(A)$ is regular, where $f$ abbreviates $(F_1, F_2, \ldots, F_r)$ (cf. 5.3). Let

$$\beta = \bigcup_{\Delta \in U_r, \Delta \supset \{a\}} (U_r \cdot \{a\} \cdot \{b\} \cdot U_r \cdot \{c\} \cdot \{d\}) \cup \bigcup_{\Delta \in U_r, \Delta \supset \{c\}} U_r \cdot \{a\} \cdot \{b\} \cdot \{c\}.$$
Then $\beta$ is regular. If $a \neq b$, then $T^3_\alpha(A) = \beta \cup (U^* \cdot \{a\} \cdot \{b\})$ while if $a = b$, then $T^3_\alpha(A) = \beta \cup (U^* \cdot U_r - \{a\} \cdot \{a\}) \cup \{a\}$. Then $T^3_\alpha(A)$ is regular and the proof is completed.

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

Define $R$ and $R^+$ as follows:

$$(a, c)R(b, d) \iff aRb \land c = 1 = d;$$
$$(a, c)R^+(b, d) \iff (a, c)R(b, d) \land \exists a = b \land (c = 1 \lor c = 0) \land d = 0,$$

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

Observation. Every finite non-null $R$-sequence has a unique extension to an infinite $R^+$-sequence in which $\langle a, 0 \rangle$ occurs for some $a \in U_{r+i}$, and every infinite $R^+$-sequence in which $\langle a, 0 \rangle$ appears for some $a \in U_{r+i}$ is an extension of some finite non-null $R$-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 $F_1, F_2, \ldots, F_{r+i}$. Let $3\alpha = \bigwedge_{x, y \in R^+} [f(x) = a \land f(x') = b] \land \bigvee_{x, y \in F_{r+i+1}}$. Then sequences in $T^3_{r+i+1}(3\alpha)$ 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 $\langle a, 1 \rangle(\alpha, 0)$;
(3) if it is of length greater than two, then its last three members are of the form $\langle b, 1 \rangle(a, 1)(\alpha, 0)$, where $a, b \in U_{r+i}$ and $a \neq b$. It follows that $T^3_{r+i}(\bigvee F_{r+i+1}(3\alpha))$ is the set of all $R$-sequences.

Let $\exists\![g]$ be $\bigvee F_{r+i+1}(3\alpha)$. Let $3\alpha\![g]$ be:

$$\exists\! [g] \land g(0) \subseteq B \land \bigvee_{x, y \in U_r \times D} (y > x \supset g(y) = g(x)).$$

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

$$T^3_r\left( \bigvee_{F_{r+i}} \bigvee_{F_{r+i+2}} \cdots \bigvee_{F_{r+i}} 3\alpha \right) = \alpha.$$
Proof. Similar to 5.11.

5.16. Let $L^*_i$ be the system consisting of the formulas $L_i$ 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 $L^*_i$.

Proof. If $F_1, F_2, \ldots, F_r$ satisfies a formula of $L^*_i$, then any translate (cf. 5.12) of this $r$-tuple satisfies the formula. The function $f: N \rightarrow U_r$ such that $(f(x))_i = 1 \iff x \in F_i$ has the property that for $x, y, a \in \mathbb{Z}$, $\bigwedge_{z \leq x, a} f(z) = a$ and $x \leq y$ because of the quasi-finite character of the $F_i$. If $f$ is not constant, let

$$x_0 = (\max x) \lor \bigwedge_{a} \{ z \leq x \cup f(z) = a \},$$

$$y_0 = (\min y) \lor \bigwedge_{a} \{ z \geq y \cup f(z) = a \}.$$ 

Then the finite sequence $g = \sigma^*_i(F_1, F_2, \ldots, F_r)$ if domain $g = \{ x \mid x \leq y_0 - x_0 \}$ and $\bigwedge_{a} \{ f(x) = a \}$, if $f$ is constant and equal to $b$, then let domain $g = \{ 0 \}$ and $g(0) = b$. The mapping $\sigma^*_i$ 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 $\sigma^*_i(F_1, F_2, \ldots, F_r) = g$ and domain $g = \{ x \mid x \leq y \}$ and $y > 0$, then $y > 1$ and $g(0) = g(y), g(0) \neq g(1), g(y - 1) \neq g(y)$.

Via $\sigma^*_i$, with each formula $\bar{F}[F_1, F_2, \ldots, F_r]$ of $L^*_i$ is associated a set of finite sequences $T^*_i(\bar{F})$ 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 $i$th member of $[u, v]$ is the $i$th member of $u$ and whose second member is the $i$th member of $v$ and $[u, v]$ is an initial segment of $[u', v']$. Similarly the $i$th 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 $i$th member of $u$, of $v$ and of $w$. A sequence $[u, v] \subseteq \sigma$ is $A$-extendable in $\sigma$ if and only if $\bigwedge_{a \in A} \bigvee_{b \in B} [u, v] | a, b \subseteq \sigma$. A sequence in $\sigma$ is strongly $A$-extendable in $\sigma$ if and only if every initial segment of the sequence is in $\sigma$ and is $A$-extendable in $\sigma$. The set $\sigma$ is strongly $A$-extendable if and only if every sequence in $\sigma$ is strongly $A$-extendable in $\sigma$. If $\sigma$ is strongly $A$-extendable, every initial segment of an element in $\sigma$ is in $\sigma$.

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

(1) $\gamma_A$ is regular,
(2) $\gamma_A$ is strongly $A$-extendable,
(3) if $\beta \subseteq \gamma$ and $\beta$ is strongly $A$-extendable, then $\beta \subseteq \gamma_A$. Furthermore, from an automaton $C$ such that $T(C) = \gamma$ one can effectively construct (by the method given in proof) an automaton $C_A$ such that $T(C_A) = \gamma_A$.

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

\[
\langle a_1, b_1, c_1 \rangle \in M_{n+1} \Rightarrow \langle a_1, b_1, c_1 \rangle \in M_n \land \bigvee_{a \in A} (a, c) \in B \times D
\]

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

\[
\langle a_1, b_1, c_1 \rangle \in M_A \Leftrightarrow \bigvee_{a \in A} (a, c) \in B \times D
\]

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

(1) $\gamma_A$ is regular since it is a projection of a regular set $\sigma$.
(2) We shall show $\gamma_A$ 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 $w_1, w_2 \in V_B$ 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

\[
\bigwedge_{a \in A} \bigvee_{b, c \in B \times D} | u_1, v_1, w_1 | \ | \ a, b, c | \in \sigma
\]

so that

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

(3) Suppose $\beta$ 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 $C$ (i.e., if $| u, v | = a_0a_1 \cdots a_n \in A \times B$, then
w is $s_0s_1 \cdots s_n$ where $f(a_0, d) = s_0$ and, for $0 < r \leq n, f(a_r, s_{r-1}) = s_r$, then every initial segment of $|u, v, w|$ is an element of $\delta$. Thus, every member of the sequence $|u, v, w|$ is an element of $M_0$ and $|u, v, w|$ is $\Lambda$ or is an $R_0$-sequence beginning with an element of $E$. Consider an arbitrary initial segment

$$|u_0, v_0, w_0| \mid a_0, b_0, c_0|$$

of $|u, v, w|$. Hence

$$\wedge \vee (a_0, b_0, c_0) \in \emptyset.$$
and 0, is the all zero \( r \)-tuple. Note that \( h \leq g \) means that the element of \( V_{U^0_r} \) represented by \( h \) is an initial segment of the element of \( V_{U^0_r} \) 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 \( \alpha \cap \) of all open sets containing a given regular set \( \alpha \) is regular (and open).

Proof. Let \( \alpha \subseteq V_{U^0} \) be regular. The intersection of all open sets containing \( \alpha \) is simply the set of all initial segments of elements in \( \alpha \). Thus if \( T, \bar{s} [f] = \alpha \) and if \( \bar{s}[g] \) is defined as follows:

\[
\forall x : \bar{s} [f] \land \bigwedge g(x) \neq 0 \cup g(x) = f(x),
\]

the desired set is \( T, \bar{s}[g] \).

6.4. Lemma. Let \( \alpha \subseteq V_{A \times \{0,1\}} \) be regular. Suppose \( \Lambda \in \alpha \). Let \( K_i(\alpha) \), \( i = 0, 1 \), be the set of sequences \( a_0, a_1, \ldots, a_n, a \in A \), such that there exists \( b_0, b_1, \ldots, b_n \) satisfying

\[
\begin{align*}
(1) & \quad b_j \in \{0, 1\}, \\
(2) & \quad |a_0, b_0|, |a_1, b_1|, \ldots, |a_n, b_n| \in \alpha, \\
(3) & \quad b_n = i.
\end{align*}
\]

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

\[
|a_0, b_0|, |a_1, b_1|, \ldots, |a_n, b_n| \in \alpha
\]

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

6.5. Lemma. Let \( \beta \subseteq V_{A \times \{0,1\}} \) be regular. Let \( \preceq \) be the lexicographical ordering of \( V_B \) induced by a given fixed ordering \( (\prec) \) of \( B \). Define \( \alpha = \Lambda \leq (\beta) \) as follows:

\[
|u, v| \in \alpha \iff |u, v| \in \beta \land \bigwedge \wedge u, v| \in \beta \supset v \leq w.
\]

Then \( \alpha \) 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 \( A \subseteq U^0_r \), \( B \subseteq U^0_s \) for appropriate \( r, s \). Suppose that

\[
T_{r+s} \bar{s}[f_1, f_2] = \beta \quad \text{for an appropriate formula } \bar{s} \text{ of } L^1.
\]

Define \( \bar{s}[g_1, g_2] \) as follows:
\[ \mathcal{F}[g_1, g_2] \land \mathcal{F}[g_1, f_2] \land f_2(x) \neq g_2(x) \land \bigwedge_y (y < x \supset f_2(y) = g_2(y)) \]
\[ \supset \cdot g_2(x) \leq f_2(x), \]
where \( g_1 \) abbreviates \( F_1, \ldots, F_r \), \( g_2 \) abbreviates \( F_{r+1}, \ldots, F_{r+s} \), and \( f_2 \) abbreviates \( F_{r+s+1}, \ldots, F_{r+2s} \), and \( g_2(x) \leq f_2(x) \) abbreviates a conjunction of conditionals of the form
\[ g_2(x) = b \cdot \supset f_2(x) = b_1 \lor f_2(x) = b_2 \lor \cdots \lor f_2(x) = b_m \]
where \( \{ b_1, \ldots, b_n \} \) is the set of all elements \( b_i \) in \( B \) such that \( b < b_i \).

Then \( T_{r+s} \supset = a \), and \( a \) is regular (cf. Theorem 5.3 and remark).

7. Characterizations of \( A/B \)-automata behavior. An \( A/B \)-automaton is a quadruple \( \mathfrak{A} = (S, f, d, g) \) where \( f: A \times S \rightarrow S \) and \( g: S \rightarrow B \). The finite behavior \( \mathfrak{B}(\mathfrak{A}) \) of \( \mathfrak{A} \) is defined as follows:
\[ \mathfrak{B}(\mathfrak{A}) = \{ (u, v) \in V_{A \times B} \mid (u, v) \neq \Lambda \} \]
and
\[ \bigvee_{v} \left[ w \in V_{S} \land u = a_0 a_1 \cdots a_n \land v = b_0 b_1 \cdots b_n \land w = s_0 s_1 \cdots s_n \supset \cdot s_0 = f(a_0, d) \land \bigwedge_{0 \leq m \leq n} f(a_m, s_{m-1}) = s_r \land \bigwedge_{0 \leq m \leq n} g(s_m) = b_m \right]. \]

7.1. Theorem. A set \( a \subseteq V_{A \times B} \) is the behavior of an \( A/B \)-automaton if and only if
(1) \( a \) is regular,
(2) \( a \) is open,
(3) \( \{ (u, v) \mid (u, v) \in a \} \) is a function,
(4) \( \{ u \mid (u, v) \in a \} = V_{\Lambda} \).

Further, if \( a \) satisfies the conditions, the proof gives an effective procedure for producing an \( \mathfrak{A} \) such that \( \mathfrak{B}(\mathfrak{A}) = a \).

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

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

\(^{(1)}\) This was pointed out to me by J. B. Wright.
(cf. 6.4). Let \( \mathfrak{A} = (S, f, d, g) \) be an \( A/B \)-automaton where \( B = U_r, S = S_1 \times S_2 \times \cdots \times S_r, (f(s))_i = f_i(s_i), 1 \leq i \leq r, \) where \( s \in S \) and the subscript \( "i" \) indicates the \( i \)th component of an \( r \)-tuple, and \( d = (d_1, d_2, \cdots, d_r) \) and 
\[
(g(s))_i = 1 \iff s_i \in D_i.
\]

Because of condition (3), for all \( i, 1 \leq i \leq r, K_1(\alpha_i) \cap K_2(\alpha_i) = \emptyset \) and because of (4), \( K_1(\alpha_i) \cup K_2(\alpha_i) = V_A \). Now, \( \mathfrak{A} \) 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 \( \nu_1 \) is the unique element of \( V_B \) such that \( |u, \nu_1| \in \alpha \) and \( \nu_2 \) is the unique element of \( V_B \) such that \( |u, \nu_2| \in \mathfrak{A} \), then \( \nu_1 = \nu_2 \).

It is obvious that \( \Lambda \in \alpha \cap \mathfrak{A} \). Suppose \( |u, \nu| \in \alpha \cap \mathfrak{A} \) and \( |u, w| \cdot |a, b| \in \alpha \). Because \( \alpha \) is open, \( |u, w| \in \alpha \), and so by (3), \( w = v \). Let \( b_i \) be the \( i \)th component of \( b \) and let \( \nu_i \) be the sequence of \( i \)th components of its members. Now,
\[
|u, \nu| \cdot |a, b| \in \alpha \iff \bigwedge_{1 \leq i \leq r} |u, \nu_i| \cdot |a, b_i| \in \alpha \iff |b_i = 1 \iff u, a \in K_1(\alpha_i)|.
\]

Note that \( |u, \nu| \cdot |a, c| \in \mathfrak{A} \iff |u, \nu| \cdot |a, c, s| \) satisfies conditions given in 7 above, for some (unique) \( ws \in V_B \). In particular, \( g(s) = c \). For this \( s, g(s) = c \iff \bigwedge_i [c_i = 1 \iff s_i \in D_i] \) and since (for this \( s \)) \( \bigwedge_i [s_i \in D_i \iff u, a \in K_1(\alpha_i)] \), it follows that \( \bigwedge_i [c_i = 1 \iff u, a \in K_1(\alpha_i)] \), so that \( b = c \).

Remark. Suppose \( T_{r+s}\mathfrak{A} = \alpha \subseteq V_A \times B, A \subseteq U_r, B \subseteq U_s \) for appropriate \( r, s, \) and \( \mathfrak{A} \) is a formula of \( L_1 \). One can effectively decide whether \( \alpha \) is the behavior of an \( A/B \)-automaton as follows:

(1) \( \alpha \) is open if and only if \( "\bigwedge_{r+s} \mathfrak{A}[f] \land g \subseteq f \cdot \neg \mathfrak{A}[g]" \) is true, where \( f \) abbreviates \((r+s)\) set variables, cf. 6.2;

(2) 7.1 (4) holds if and only if \( "\bigwedge_{r+s} \mathfrak{A}[f_1, f_2] \" \) is true;

(3) 7.1 (3) holds if and only if \( "\bigwedge_{r+s} \mathfrak{A}[f_1, f_2] \land \mathfrak{A}[f_1, f_2] \neg f_2 = g_2" \) 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 \( \alpha \):
\[
\begin{pmatrix}
1 \\
0
\end{pmatrix}^* \cdot \begin{pmatrix}
1 \\
1
\end{pmatrix} \cup \{A\}.
\]

Since \( 0^* \cdot 1 \cup \{A\} \) denotes this set if \( "0" \) denotes \( \{1, 0\} \) and \( "1" \) denotes \( \{1, 1\} \), \( \alpha \) 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 \( A, B, \alpha \) be as in 7.2.1. Then \( \alpha^c \) (cf. 6.3) satisfies (1), (2), (4) but not (3).

7.2.3. Let \( A = \{0, 1\}, B = \{1\}, \) and let \( \alpha \) be the set:
\[
\begin{pmatrix}
1 \\
1
\end{pmatrix}^*.
\]

then \( \alpha \) satisfies (1), (2), (3), but not (4).
7.2.4. Let $A = \{a, b\}$ and let $B = \{0, 1\}$. Let $\beta$ be the set:

$$a^{(n)}b^{(n)}, \quad n \geq 0.$$ 

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

$$|u, v| \in \alpha \Rightarrow \bigvee_{u_1, v_1, u_2, v_2} |u, v| = |u_1, v_1| |u_2, v_2| \land v_1 \in V_1 \land v_2 \in V_0.$$ 

Now $\alpha$ satisfies 7.1 (2), (3), (4). We wish to show $\alpha$ is not regular. If $\alpha$ were regular, then $y = \alpha|\forall xM$ is regular. Further, $y$ is isomorphic to $\beta^L$. Hence to show $\alpha$ is not regular, it is sufficient to show $\beta^L$ is not regular.

Suppose $\beta^L$ were regular; then, assuming $a, b \in U^0_2$, for some formula $\phi[f]$ of $L^1_2$:

$$\phi[f] = \beta^L.$$ 

Let $\phi[g]$ be the formula:

$$\phi[g] \land \bigwedge_j : g \leq f \land \phi[f] \land g = f$$

(cf. 6.2).

Then $T_2(\phi) = \beta^L$ is regular. Contradiction. Thus $\alpha$ 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 $a \in A$, then $a \in \lim a^{\infty}$, where $\beta^L$, for $\beta \subseteq A^N$, means the set of all finite initial segments of elements in $\beta$.

**Theorem.** If $\alpha \subseteq (A \times B)^N$, then there exists an $A/B$-automaton such that

$$\lim 3(\alpha^N) = \alpha$$

if and only if

1. $\alpha^L$ is regular,
2. $|f_1, g_1| \in \alpha \land |f_2, g_2| \in \alpha \land f_1 \uparrow n = f_2 \uparrow n \cdots g_1 \uparrow n = g_2 \uparrow n$ where $f \uparrow n$ 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 $\alpha^L$; 7.1 (2) is obvious from the definition of $\alpha^L$; and 7.1 (4) follows from condition (3). Hence, there exists an $A/B$-automaton $\mathfrak{N}$ such that $3(\mathfrak{N}) = \alpha^L$.

**Claim:** $\lim \alpha^L = \alpha$. If $|f, g| \in \alpha$, then $\{ \{f, g\} \subseteq \alpha^L \}$ 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 $n$, $|f, g| \uparrow n = |f', g'| \uparrow n$ for some $|f', g'| \in \alpha$. Since $f \uparrow n = f' \uparrow n$, it follows that $h \uparrow n = g' \uparrow n = g \uparrow n$ (using condition (2)). Thus, $g = h$ and our claim is established (based only upon conditions (2) and (3)).

Let $\mathfrak{N}$ be an $A/B$-automaton. It is obvious that $\lim 3(\mathfrak{N})$ satisfies (2) and (3). Hence, the "claim" of the previous argument establishes that $\lim 3(\mathfrak{N}) = 3(\mathfrak{N})^L$ 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 $\gamma \subseteq V_{AB}$. There exists an $A/B$-automaton $\mathfrak{R}$ such that $3(\mathfrak{R}) \subseteq \gamma$ if and only if $\gamma_A$ (cf. 6.1) is nonempty. If $\gamma_A$ is nonempty, then one may effectively obtain an automaton $\mathfrak{R}$ such that $3(\mathfrak{R}) = \mathcal{L}(\gamma_A)$ where $\leq$ is an arbitrary ordering of $B$ (cf. 6.5.).

Proof. Suppose $3(\mathfrak{R}) \subseteq \gamma$ for some $\mathfrak{R}$. Then, since $3(\mathfrak{R})$ is strongly $A$-extendable, $3(\mathfrak{R}) \subseteq \gamma_A$ and $\gamma_A \neq \emptyset$.

If $\gamma_A \neq \emptyset$, then because it is open, $\Delta \in \gamma_A$ and because it is $A$-extendable, the set $\{u : |u, v| \in \gamma_A\} = V_A$. By Lemma 6.1, $\gamma_A$ is regular. Let $\mathcal{L}(\gamma_A) = \alpha$. From the definition of $\mathcal{L}(\gamma)$, 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, $\alpha$ is regular. It remains only to show that $\alpha$ 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 $|u_1, v_1| = |u_1, v|$, it follows $v \leq v_1$. Because $|u_1, v| = A$-extendable in $\gamma_A$, $|u_1, v_1| = |u_2, w| = \gamma_A$, for some $w \in V_B$. Thus $v_1w_2 \leq v_2w_2$, so that $v_1 \leq v_2$ (since $\leq$ is a lexicographical ordering). It follows that $v = v_1$ and $\alpha$ 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: $3(\mathfrak{R}_1) \subseteq \gamma$ and $3(\mathfrak{R}_2) \subseteq \gamma$ implies $3(\mathfrak{R}_1) = 3(\mathfrak{R}_2)$.

Proof. If $\gamma_A = \emptyset$, then the condition is vacuously satisfied (cf. 8.1). Suppose $\gamma_A \neq \emptyset$. If $\mathfrak{R}_1$ is the automaton picked out by 8.1 and $3(\mathfrak{R}_1) \subseteq \gamma$ and $3(\mathfrak{R}_1) \neq 3(\mathfrak{R}_2)$, then there exists $|u, v| \in 3(\mathfrak{R}_1)$, $|u, w| \in 3(\mathfrak{R}_2)$, and $v < w$. Hence, if $\mathfrak{R}_2$ is the automaton picked out by 8.1 when the ordering of $B$ is reversed, $3(\mathfrak{R}_1) \neq 3(\mathfrak{R}_2)$.

Thus, the conditional of the corollary holds if and only if (1) $\gamma_A = \emptyset$ or (2) $\gamma_A \neq \emptyset$ and if $\mathfrak{R}_1$ is the automaton picked out via 8.1 by an ordering $\leq$ of $B$ and $\mathfrak{R}_2$ is the automaton picked out via 8.1 by the reverse ordering $\leq$ of $B$, then the symmetric difference of $3(\mathfrak{R}_1)$ and $3(\mathfrak{R}_2)$ is $\emptyset$.

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

$$\mathfrak{I}[a, b] = \forall t \neq 0 \exists s(0) = f(a(0), d) \land \bigwedge_{s < t} (s(x') = f(a(x'), s(x)) \land b(x) = g(s(x)) \land \bigwedge_{a(x) = 0_m} b(x) = 0_m,$$

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 \( T_{m+m}(\mathfrak{A}) = 3(\mathfrak{A}) \). Thus the formula above may be identified with \( \mathfrak{A} \). Given an arbitrary formula \( \mathcal{F}[a, b] \) of \( L \), let \( T_{m+m}(\mathcal{F}) = \gamma \subseteq V_A \times B \). Then \( \mathfrak{A}(\mathcal{F}) = \mathfrak{A}(\mathcal{F}) \subseteq V_A \times B \).

8.4. If \( p \) maps the finite set \( A \) onto \( B \), \( p \) 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 \( p \). If \( f \in A^N \), then \( (pf)(n) = p(f(n)) \). If \( \alpha \subseteq A^N \), then \( p\alpha = \{ pf : f \in \alpha \} \).

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

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

**Proof.** Let \( f \in \lim \alpha \). For all \( n \geq 0, f \upharpoonright n \in \alpha \) and \( f(f \upharpoonright n) \in \alpha \). Now \( \hat{p} \subseteq \hat{p} \lim \alpha \) and \( \{ \hat{p}f \}^n = \{ \hat{p}(f \upharpoonright n) : n \geq 0 \} \). Hence \( \hat{p}f \in \lim(\hat{p}\alpha) \). Thus, \( \hat{p}(\lim \alpha) \subseteq \lim(\hat{p}\alpha) \).

We shall now show \( \lim(\hat{p}\alpha) \subseteq p(\lim \alpha) \). Suppose \( g \in \lim(\hat{p}\alpha) \). Let \( \alpha' = \alpha \cap \bigcup_{n \geq 0} p^{-1}(g \upharpoonright n) \). Note that \( \alpha' \) is open because \( \alpha \) is. Then \( \alpha' \) contains an infinite number of elements. For \( u \in \alpha' \), let \( \rho_u(u) \) be the number of elements in \( \alpha' \) of which \( u \) is an initial segment. Now \( \Delta(\alpha') \cap \rho_u(\Delta) = \infty \). We define \( \alpha_u \subseteq \alpha' \) inductively. Let \( \Lambda(\alpha_u) \subseteq \alpha_u \) as well as every initial segment of \( \alpha_u \) and suppose \( \rho_u(u) = \infty \). Let \( a_1, a_2, \ldots, a_n \) be an enumeration of the elements of \( A \). If \( u \) is an initial segment of \( v \) but \( u \neq v \), then, because \( \alpha' \) is open, \( v \) is an initial segment of either \( ua_1, ua_2, \ldots, ua_n \). Since \( \rho_u(u) = \infty \), for some \( i, \rho_u(ua_i) = \infty \). Let \( \beta \) be the first such \( i \) and place \( ua_i \) in \( \alpha_u \). Thus \( \alpha_u \subseteq V_A \) is an infinite set simply ordered by the relation “initial segment of”. It is thus unambiguous to define \( f(n) = u(n) \), where \( u \in \alpha_u \) has \( n \) in its domain. It follows, for all \( m, f \upharpoonright m \in \alpha_u \subseteq \alpha \) and \( \hat{p}(f \upharpoonright m) = g \upharpoonright m \). 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 \( \text{Int} \).

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

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

(2) \( u \in (\hat{p}\beta) \iff \forall_{\beta,m} g \in \beta \wedge ((\hat{p}g) \upharpoonright m) = u \iff \forall_{\beta,m} g \in \beta \wedge \hat{p}(g \upharpoonright m) = u \iff u \in \hat{p}(\beta) \).

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

(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 \( \text{compl} \cup_{w \in R} K(w) \) is regular and is the set of all \( R \)-sequences. The set \( E^L \) is regular, as is any finite set. The set \( \beta^L \) is: \( \text{compl} \cup_{w \in R} K(w) \cap E^L \) and is, therefore, regular. Since projection preserves regularity, \( \beta^L \) is regular.

8.6. Let \( L^L \) be the system consisting of the formulas of \( L_s \), with individual variables interpreted over natural numbers and the set variables interpreted over arbitrary sets of natural numbers. With a formula \( \mathcal{F} \{F_1, F_2, \cdots, F_r\} \) of \( L^L \) we associate a set \( T^* \mathcal{E} \) defined as follows:

\[
\mathcal{F} \in T^* \mathcal{E} \text{ if and only if } \mathcal{F} \in U^R \text{ and } (f(x))_i = f_i(x), 1 \leq i \leq r, \text{ where } f_i \text{ is the characteristic function of } F_i \text{ and } \mathcal{F} \{F_1, F_2, \cdots, F_r\} \text{ holds.} \]

Abbreviations introduced for \( L^L \) in Remark 5.3 will be used in \( L^L \) as well.

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

\[
\forall \mathcal{F} \left[ s(0) = f(a(0), d) \land \bigwedge_{x} (s(x) = f(a(x'), s(x'))) \lor b(x) = g_s(x) \right].
\]

If \( \alpha = T_{m+m'}^n (\mathfrak{G} \{a, b\} \) (assuming range \( a \subseteq U^m \) and range \( b \subseteq U^{m'} \)), then comparison with \( \mathfrak{G} \{a, b\} \) shows that \( \alpha^L = \mathfrak{A} \to T_{m+m'}^n \mathcal{E} \mathfrak{G} \{a, b\} \) (cf. 8.3) and by Lemma 8.5 (3), \( \mathfrak{A} = \alpha \).

8.6.2. Consider arbitrary formulas of \( L^L \) of the form \( \forall s, \mathcal{F} \mathfrak{M} \mathcal{L} a, b, s, x \), where range \( a \subseteq A \), range \( b \subseteq B \), and where \( \mathfrak{M} \) : 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 \( \mathfrak{M} \) 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 \( \mathfrak{M} \). Then \( T_{m+m'+r}^n (\mathfrak{M} \mathcal{L} a, b, s, x \), range \( s \subseteq S \subseteq U_n \), 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 \( f \upharpoonright n \subseteq E \), 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 \( \mathfrak{A} \) in expanded disjunctive normal form. If \( \beta = T_{m+m'+r}^n (\mathfrak{M} \mathcal{L} a, b, s, x \), then \( \beta \mathfrak{G} = T_{m+m'}^n (\forall s, \mathcal{F} \mathfrak{M} \mathfrak{L} a, b, s, x \), \( \mathfrak{P} \) maps an \( (m+m'+r) \)-tuple into the appropriate \( (m+m') \)-tuple.

8.6.3. **Theorem.** Given a formula \( \forall s, \mathcal{F} \mathfrak{M} \mathcal{L} a, b, s, x \), \( \mathfrak{M} \) as in 8.6.2, of \( L^L \), there exists an \( A/B \)-automaton \( \mathfrak{A} \) such that \( \lim \mathfrak{A} (\mathfrak{A}) \subseteq \beta = T_{m+m'}^n (\forall s, \mathcal{F} \mathfrak{M} \mathfrak{L} a, b, s, x \), if and only if \( \gamma = \beta^L \) (cf. 8.1) where \( \gamma = \beta^L \). Whether or not \( \gamma = \beta^L \) can be effectively decided (by the method given in proof) and if \( \gamma = \beta^L \), 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

\[
\lim \mathfrak{A} (\mathfrak{A}) \subseteq \beta \iff \mathfrak{A} (\mathfrak{A}) \subseteq \beta^L.
\]

The set \( \beta^L \) 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:
\[
\lim \mathcal{A}(\mathcal{M}) \subseteq \beta \iff \mathcal{A}(a, b) \supseteq \bigvee_{s, x} M[a, b, s, x]
\]
where \( \mathcal{A}, \mathcal{M} \) are as in 8.6.1.

9. Remark. We give a metamathematical proof that the set
\[
\beta = \{ a^{(n)} b^{(n)} | n \geq 0 \}
\]
is not regular. Let \( a, b \in \mathcal{U} \). If the set were regular, then there would be a formula \( \mathcal{F}[f] \) of \( \mathcal{L} \) such that \( T_\mathcal{F} = \beta \). Then \( y = \exists x \forall y. f(x) = b \land f(y) \neq 0 \land \exists z. (x > y \lor f(z) = 0) \land \mathcal{F}[f] \). Thus regularity of \( \beta \) implies that doubling is definable in \( \mathcal{L} \) and by results of R. M. Robinson [10] it would follow that the set of true sentences of \( \mathcal{L} \) is not effective, contradicting 5.8.

Chapter IV. Nonexistence of Certain Algorithms

10. Let \( \mathcal{L}_2 \) 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 \( \mathcal{L}_1 \) be the system consisting of \( \mathcal{L}_2 \) 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 (non-logical) 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 \( i(x) = a \land i(x+1) = b \land i(x+2) = c \).

Notice that in \( \mathcal{L}_2 \):
\[
\begin{align*}
x = 0 & \iff x + x = x, \\
x < y & \iff \bigvee_{u} x + u = y \land u \neq 0,
\end{align*}
\]
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 $T_0(i, m)$ 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 $T_0(i, m)$ 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 $L^1$ such that $T(F)$ is the set of all proofs of $P$.

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

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

i.e.,

$m(x) \land m(y) \land \bigwedge_u x + u = y \land \sim u + u = u \land \bigwedge_z \bigwedge_u \left[ (\bigvee_z x + u = z \land \sim u + u = u \land \bigwedge_w z + u = y \land \sim u + u = u \supset \sim m(z) \right].$

With each production of $P$

$(\sigma_1, \sigma_2)^k : \sigma_1\beta \rightarrow \beta\sigma_2$

associate the formula

$S_{1,2}^k(w, x, y) : i(w + 1)i(w + 2) \cdots i(w + l(\sigma_1)) = \sigma_1^k \land \bigvee_u u + l(\sigma_2) = y \land i(u + 1)i(u + 2) \cdots i(u + l(\sigma_2)) = \sigma_2^k \land \bigvee_z z + w + l(\sigma_1) = x \land z + x + l(\sigma_2) = y \land \bigwedge_u \left( (\sim u + u = u \land \bigvee_v u + v = z \supset i(w + l(\sigma_1) + u) = i(x + u)) \right)$

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

$S^P(i, m) : \bigwedge_{w, x, y} \left[ (C_m(w, x)C_m(x, y) \supset S_{1,2}^k(w, x, y) \lor \cdots \lor S_{1,2}^n(w, x, y)) \land (w = 0 \supset x = l(\alpha) \land i(1)i(2) \cdots i(l(\alpha)) = \alpha) \right].$

Then $F$ is
10.2. Theorem. The set of satisfiable formulas of $L_1$ 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 $F_n = F(P) \land \forall x, n \land (x+n+1) = 1 \land i(x+1) = 1 \land \cdots \land i(x+n+1) = 1$, 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 I.ii) if and only if $\forall i, m F_n$ 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 $L_2$ is the system consisting of the formulas $L_1$ but with the interpretation of the predicates unrestricted, then the set of satisfiable formulas of $L_2$ is not effective.

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

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 $L_2$ is not arithmetic.

10.4. Let $L_3$ 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 $L_3$. $T(G)$ is defined exactly as before.

Notice that in $L_3$:

$x = 0 \iff \forall x + x = x$, $x = 1 \iff \forall y, y = 0 \land y' = x$,

$x > 0 \iff \forall y \land \exists y \neq 1 \lor p(y - 1) \land p(x)$
and

\[ p(y - 1) \iff \forall z' = y \land p(z'). \]

To establish the analogues for \( L^4 \), we show that \( \forall p \) can be moved all the way to the left.

Let \( D(p) \) stand for \( \forall y \neq 1 \supset p(y - 1) \). 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 \( \forall x \exists m \supset D(p) \land p(x) \) and prefixing the conjunction by \( \forall p \). In the formula \( F \), wherever one wishes to express \( x < y \), one writes \( \forall u \ x + u = y \land p(u) \).

10.5. Let \( L^4 \) 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 \( L^4 \) 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 \( L^4 \) and from 10.2.

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

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

**Bibliography**

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


UNIVERSITY OF MICHIGAN, RESEARCH INSTITUTE, 
ANN ARBOR, MICHIGAN