T H E U N I V E R S I T Y O F M I C H I G A N

COLLEGE OF LITERATURE, SCIENCE, AND THE ARTS
Logic of Computers Group

Technical Report

WEAK SECOND-ORDER ARITHMETIC AND FINITE AUTOMATA

J. Richard Büchi

administered by:

THE UNIVERSITY OF MICHIGAN RESEARCH INSTITUTE ANN ARBOR

September 1959

The work reported and discussed in this paper has been carried on under the listed grant and contracts with the following agencies:

National Science Foundation
Washington, D.C.
NSF Grant - G-4790

Office of Naval Research
Washington, D.C.
Contract NONR-1224(21), Project NR 049-114

U.S. Army
Office of Ordnance Research
through Detroit Ordnance District
Detroit, Michigan
Contract DA-20-018-ORD-16971

U.S. Army Signal Supply Agency
Laboratory Procurement Support Office
Fort Monmouth, New Jersey
Contract DA-36-039-sc-78057

INTRODUCTION*

The formalism of regular expressions was introduced by S. C. Kleene [6] to obtain the following basic theorems.

Synthesis: To every regular expression $\underline{\underline{E}}$ one can effectively obtain a finite automata $\underline{\underline{A}}$ with binary output $\underline{U}$ such that $\underline{\underline{E}}$ denotes the behavior of $\langle \underline{\underline{A}}, \underline{U} \rangle$.

Analysis: To every finite automaton $\underline{\underline{A}}$ with binary output $\underline{U}$ one can effectively construct a regular expression $\underline{\underline{E}}$ such that the behavior of $\langle \underline{\underline{A}}, \underline{U} \rangle$ is denoted by $\underline{\underline{E}}$.

For simplified expositions of Kleene's theory see Copi-Elgot-Wright [4], Rabin-Scott [13], and Myhill [8].

It will be shown here that a more conventional formalism, a weak second-order arithmetic, can be used in place of the formalism of regular expressions. Our theorems 1, 2 section 4 are equivalent to Kleene's synthesis and analysis theorems. This result is of interest for automata theory because formulas of weak second-order arithmetic seem to be more convenient than regular expressions for formalizing conditions on the behavior of automata. In addition, our synthesis and analysis theorems yield rather complete information on the strength of weak second-order arithmetic (see Section 5), thus providing an example of applying automata theory to logic.

*The author wishes to thank Dr. J. B. Wright for many stimulating discussions. Some of the results were announced in the Notices, American Mathematical Society. ("Decision Problems of Weak Second-Order Arithmetics and Finite Automata. Prelim. Report, Part I," Vol. 5, No. 7, December 1958).

1. NOTATIONS AND TERMINOLOGY

The following letters (possibly with subscripts) will be used as syntactic variables with range as indicated,

x, y, z, t	denote individual variables
X, Y, Z	denote propositional variables
i, j, r, s, u	denote monadic predicate variables
A, B, C, D,...	denote formulas of propositional calculus
$\underline{\underline{A}}$, $\underline{\underline{B}}$, $\underline{\underline{C}}$, $\underline{\underline{D}}$	denote formulas.

Besides the already mentioned (countable) lists of variables our formalism contains the primitive symbols $\barwedge$, $\barvee$, $\wedge$, $\vee$, $\sim$, $\supset$, $\equiv$, [,], $\forall$, $\exists$, (,) , o, ' . The formulas of propositional calculus (p.f.'s) are obtained in the conventional manner from $\barwedge$, $\barvee$ and propositional variables by means of the connectives and [,]. Examples of atomic formulas are i(o"), i(x), $r_2(t''')$. Matrices are obtained by replacing all propositional variables in a p.f. A by atomic formulas.

Formulas (of restricted, i.e. monadic, second-order-predicate calculus) are obtained in the conventional manner from matrices by applying individual—and predicate—quantifiers, and propositional connectives. A sentence is a formula without free variables.

A method for indicating occurrences of free variables is explained by the following examples. "D[X,Y,Z]" denotes a p.f. in which the indicated propositional variables but no others may occur. "D[i(o"), i(x), s(t')]" denotes the matrix obtained by making the obvious substitutions in D[X,Y,Z], and may be ab-

breviated as "D(o,x,t)". "$\underline{\underline{C}}(i_1,i_2,t)$" denotes a formula in which the variables i_1,i_2,t but no others may have free occurrences. We will also abbreviate "[~A]" by "$\tilde{A}$", and "[A$\wedge$B]" by "AB".

We will often deal with n-tuples of objects. The symbol "$\frown$" denotes concatenation of n-tuples. Thus for example "$H_1 \frown H_2 \frown H_1$" and "$i_1 \frown i_2 \frown i_3 \frown i_4$" denote respectively a 3-tuple of matrices and a 4-tuple of propositional variables. The second component of the 3-tuple $a \frown b \frown c$ is b. The n-tuple $2 \frown 2 \frown 2 \ldots \frown 2$ will also be denoted by "$\underline{n}$". We next explain the use of a vector-notation which will considerably condense the presentation and make it more comprehensible.

$\underline{X}^n$, $\underline{Y}^n$, $\underline{Z}^n$	denote n-tuples of propositional variables
$\underline{i}^n$, $\underline{j}^n$, $\underline{r}^n$, $\underline{s}^n$	denote n-tuples of monadic predicate variables
$\underline{A}^n$, $\underline{B}^n$, ...	denote n-tuples of propositional formulas

For example, "$\underline{r}^m(t') \equiv \underline{H}^m[r^m(t), i^n(t)]$" stands for the m-tuples of matrices whose components are $r_1(t') \equiv H_1[r_1(t),\ldots r_m(t), i_1(t),\ldots i_n(t)],\ldots,r_m(t') \equiv H_m[r_1(t),\ldots,r_m(t), i_1(t'),\ldots,i_n(t')]$. "$\underline{X}^n \frown Y$" stand for the (n+1)-tuple $X_1 \frown X_2 \frown \ldots \frown X_n \frown Y$. At some places a notation for an n-tuple of propositional formulas is used ambiguously to denote the conjunction of the p.f.'s occurring in the n-tuple. Furthermore the superscripts on notation for n-tuples are often omitted; in such cases it is clear from the context how they are to be restored.

Interpretation: We will not make use of any deductive structure on the syntactic frame. However, propositional formulas and formulas will be interpreted. Because the interpretations are quite conventional we will not state rigorous definitions. Furthermore, we will make ambiguous use of the syntactic notations, using them at times also for reference to the interpretation. The following list

will explain additional notations and terminology.

Λ, V	truth values false, true
$\underline{\Lambda}^n$	the n-tuple $\Lambda \frown \ldots \frown \Lambda$
predicate	function from natural numbers to $\{\Lambda, V\}$ (set of natural numbers)
special predicate	predicate which is ultimately false (finite set of natural numbers)
n-predicate	n-tuple of predicates
special n-predicates	n-predicate with special components (n-predicate which is ultimately $\underline{\Lambda}^n$)

Further notations are introduced in the various sections.

2. WEAK SECOND-ORDER ARITHMETIC

We now consider the following interpretation of the primitive symbols of the restricted second-order system described in 1.

Λ, V	true, false
$\wedge, \vee, \sim, \supset, \equiv$	the usual truth functions
o, '	the natural number zero, the successor-function on natural numbers
individual variables	range over natural numbers
predicate variables	range over special predicates (finite sets of natural numbers)
$(\exists x), (\forall x)$	there is a n.n.x, for all n.n.'s x
$(\exists i), (\forall i)$	there is a special predicate i, for all special predicates i.

This leads in a conventional manner to a definition of satisfaction for formulas, and truth for sentences. The resulting interpreted system will be called weak second-order arithmetic (W.2.A). The notation "$\hat{\underline{i}}\ \underline{\underline{C}}(\underline{i})$" will be used for the set of all special predicates i on natural numbers which satisfy the formula $\underline{\underline{C}}(\underline{i})$. The notations "$\hat{x}\ \underline{\underline{C}}(x)$", "$\hat{\underline{i}}\ \underline{\underline{C}}(\underline{i}^n)$" are used similarly. The formula $\underline{\underline{C}}(\underline{i})$ defines the set $\hat{\underline{i}}\ \underline{\underline{C}}(\underline{i})$ in W.2.A. $\underline{\underline{C}}(\underline{i},x)$ is equivalent to $\underline{\underline{B}}(\underline{i},x)$ if $\hat{\underline{i}}\hat{x}\underline{\underline{C}}(\underline{i},x) = \hat{\underline{i}}\hat{x}\underline{\underline{C}}(\underline{i},x)$, i.e., if $(\forall \underline{i})\ (\forall x)$. $\underline{\underline{C}}(\underline{i},x) \equiv \underline{\underline{B}}(\underline{i},x)$ holds in W.2.A.

Lemma 1: In W.2.A., to every formula $\underline{\underline{C}}(\underline{i}^n)$ one can effectively construct a formula $\underline{\underline{C}}^*(\underline{i}^n)$ such that $\hat{\underline{i}}\ \underline{\underline{C}}^*(\underline{i}^n) = \hat{\underline{i}}\ \underline{\underline{C}}(\underline{i}^n)$ and $\underline{\underline{C}}^*(\underline{i}^n)$ is of the form

$(\underline{j}) \cdot K[\underline{j}(o)] \wedge (\forall t)\ B[\underline{i}(t),\underline{j}(t),\underline{j}(t')]$, whereby $\underline{j}$ is a r-tuple $j_1 \frown \ldots \frown j_r$ of predicate variables and $(\underline{j})$ is a prefix of quantifiers $(\exists j_\nu)$ and $(\forall j_\nu)$.

Proof: It is clear that one can construct a formula $\underline{\underline{Z}}(x)$ such that o is the only number satisfying $\underline{\underline{Z}}(x)$. Now if o occurs in $\underline{\underline{C}}(\underline{i})$ and $\underline{\underline{D}}(\underline{i},x)$ is obtained by substituting x for o in $\underline{\underline{C}}(\underline{i})$, then $\underline{\underline{C}}(\underline{i}) \cdot\equiv\cdot (\exists x)\ [\underline{\underline{Z}}(x) \wedge \underline{\underline{D}}(\underline{i},x)]$ holds for $\underline{i}$. Thus we have obtained a formula $\underline{\underline{C}}_1(\underline{i})$ equivalent to $\underline{\underline{C}}(\underline{i})$ in which o does not occur. The next step is to construct from $\underline{\underline{C}}_1(\underline{i})$ an equivalent formula $\underline{\underline{C}}_2(\underline{i})$ in which no iterations of ' occur and no ' occurs in argument places of $\underline{i}$. This is easily accomplished by introduction of new predicate variables which are appropriately quantified. Then $\underline{\underline{C}}_3(\underline{i})$ is obtained by passing to prenex form.

Next we repeatedly apply to $\underline{\underline{C}}_3(\underline{i})$ identities of the form (prefix 1) $(\exists x)$ (prefix 2) $A(x,\ldots) \cdot\equiv\cdot$ (prefix 1) $(\exists j)\ (\forall x)$ (prefix 2) $(\exists y)\ [j(y) \wedge j(x) \supset A(x,\ldots)]$ and their duals, to obtain a formula $\underline{\underline{C}}_4(\underline{i})$ equivalent to $\underline{\underline{C}}(\underline{i})$ which is of the form $\underline{\underline{C}}_4(\underline{i})$: (predicate prefix) (individual prefix) [Matrix]. Because the matrices are constructed from monadic predicate variables only we can make

use of Behmann's [1] device of moving individual quantifiers into the matrix of $\underline{\underline{C}}_4(\underline{i})$. The result is a formula $\underline{\underline{C}}_5(\underline{i})$ equivalent to $\underline{\underline{C}}(\underline{i})$, and of form $\underline{\underline{C}}_5(\underline{i})$: (predicate prefix) $\Updownarrow [(\exists t)D_\nu(t) \vee (\forall t)E_{\nu,1}(t) \vee \ldots\ldots \vee (\forall t)E_{\nu,n}(t)]$. Now we note that predicate quantification is over special predicates, and therefore identities of the form $(\forall t)E(t) \mathrel{..\equiv..} (\forall j) \cdot \tilde{j}(o) \vee (\exists t)[j(t)\ \tilde{j}(t')E(t)]$ hold in W.2.A. If we accordingly replace each constituent $(\exists t)E_{\nu,\mu}(t)$ in $\underline{\underline{C}}_5(\underline{i})$, making use of different j's, and then move the newly introduced predicate-quantifiers into the prefix, the result is a formula $\underline{\underline{C}}_6(\underline{i})$ equivalent to $\underline{\underline{C}}(\underline{i})$ and of the form, $\underline{\underline{C}}_6(\underline{i})$: (predicate prefix) $\Updownarrow [A_\nu(o) \vee (\exists t)B_\nu(t)]$. Now we remark again that predicate quantification is over special predicates, and therefore identities of the form $A(o) \vee (\exists t)B(t) \mathrel{..\equiv..} (\exists j) \cdot [\tilde{A}(o) \supset j(o)] \wedge (\forall t)[j(t) \wedge \tilde{j}(t') \supset B(t)]$ hold in W.2.A. Accordingly we replace each $A_\nu(o) \vee (\exists t)B_\nu(t)$ in $C_6(\underline{i})$, making use of different j's, and then move the new predicate quantifiers into the prefix. The result is a formula $\underline{\underline{C}}^*(\underline{i})$ equivalent to $\underline{\underline{C}}(\underline{i})$ and of the form required in lemma 1.

3. FINITE AUTOMATA

We will now define automata as syntactic entities. We refer to Section 6 for motivation. In Section 6, our concept also is compared with other definitions of "finite automaton."

Definition 1. A (finite n/m-automaton with input X^n and transit $\underline{Y}^m$ is a 2m-tuple $\underline{E}^m \frown \underline{H}^m[\underline{Y}^m, \underline{X}^n]$ of propositional formulas. (Note that no propositional variables occur in $\underline{E}^m$). A (binary) output of a n/m-automaton with transit $\underline{Y}^m$ is a propositional formula $U[\underline{Y}^m]$.

The transition-recursion of an automaton $\underline{E}^m \frown \underline{H}^m$ is the 2m-tuple of matrices

$$\underline{r}^m(o) \equiv \underline{E}^m$$

$$\underline{r}^m(t') \equiv \underline{H}^m[\underline{r}^m(t), \underline{i}^n(t)] \ ,$$

it defines recursively a functional which will be denoted by $\underline{r} = \zeta(\underline{E},\underline{H},\underline{i})$.

The output-recursion of an automaton with output $\underline{E}^m \frown \underline{H}^m \frown U$, is obtained by adding the matrix $u(t) \equiv U[\underline{r}\ (t)]$ to the transition-recursion. It defines recursively a functional which will be denoted by $u = \psi(\underline{E},\underline{H},U,\underline{i})$.

The "input to output" functional $u = \psi(\underline{E},\underline{H},U,\underline{i})$ might be defined to be the behavior of the automaton with output. However, this is inconvenient for establishing relations to W.2.A., because in general $u = \psi(\underline{i})$ will not be special even for special $\underline{i}$. We therefore will deal with a special sort of output only. It will be seen in Section 6 that this is not essentially a restriction.

Definition 2. $U[\underline{Y}^m]$ is a special output of the automaton $\underline{E}^m \frown \underline{H}^m$ if $U[\underline{Y}] \equiv U[\underline{H}[\underline{Y},\underline{\Lambda}]]$.

It is easy to see that in case U is special the output recursion defines an operator ψ such that $\psi(\underline{i})$ or $\sim\psi(\underline{i})$ is special whenever $\underline{i}$ is special. This makes the operator definition of behavior manageable in W.2.A. However, it is more convenient to work with the set β consisting of all special $\underline{i}$ for which $\sim\psi(\underline{i})$ is special, rather than with ψ directly. This leads to the following definition of behavior, which is closely related to Kleene's [6] (see Section 7).

Definition 3. The behavior $\beta(\underline{E}^m,\underline{H}^m,U)$ of a $\underline{n}/\underline{m}$-automaton with special output is the set of all special n-predicates $\underline{i}^n$ for which the predicate $u = \psi(\underline{E},\underline{H},U,\underline{i})$,

determined by the output-recursion, is ultimately true, i.e., $(\exists x)\ (\forall t)_x^{\infty} u(t)$.

By the length of a special n-predicate $\underline{i}^n$ we mean the smallest number x such that $\underline{i}^n(t) \equiv \underline{\Lambda}^n$ for $t > x$. By definitions 2,3 one easily proves,

(*) If U is a special output of the automaton $\underline{E}^m \frown \underline{H}^m$, and if $\underline{i}^n$ is a n-predicate of length γ, then $\underline{i} \in \beta(\underline{E},\underline{H},U)$.≡. $U[\underline{r}(\gamma+1)]$ whereby $\underline{r} = \underline{\zeta}(\underline{E},\underline{H})$ is given by the transition-recursion of $\underline{E} \frown \underline{H}$.

Lemma 2: If U is a special output of the n/m-automaton $\underline{E}^m \frown \underline{H}^m$ then so is ~U. Furthermore the behaviors $\beta(\underline{E},\underline{H},U)$ and $\beta(\underline{E},\underline{H},\sim U)$ are complementary subsets of the set of all special n-predicates.

Proof: That ~U again is special follows directly by definition 2. That the behaviors of U and ~U are complementary is best seen by referring to (*).

Definition 4: An n/m-automaton with output, $\underline{E}^m \frown \underline{H}^m \frown U$, is in expanded form if $\underline{H}^m$ and U are of the form

$$\underline{H}^m[Y_1,\ldots,Y_m,\underline{X}^n] \ : \ Y_1\underline{K}_1^m[\underline{X}^n] \vee \ldots\ldots\ldots \vee Y_m\underline{K}_m^m[\underline{X}^n]$$

$$U\,[Y_1,\ldots,Y_m] \ : \ Y_1 \vee Y_2 \vee \ldots\ldots\ldots \vee Y_k$$

Lemma 3: To every n/m-automaton $\underline{E}^m \frown \underline{H}^m \frown U$ one can construct a n/k-automaton $\underline{G}^k \frown \underline{L}^k \frown W$ which is in expanded form, and such that if U is special output of $\underline{E}^m \frown \underline{H}^m$ then W is special output of $\underline{G}^k \frown \underline{L}^k$ and the behavior $\beta(\underline{G},\underline{L},W)$ is equal to $\beta(\underline{E},\underline{H},U)$.

Proof: We indicate the construction of $\underline{G}$, $\underline{L}$, W in case $\underline{m}=2 \frown 2$, and $U[Y_1,Y_2] \equiv Y_1$. The given automaton then consists of p.f's E_1, E_2, $H_1[Y_1,Y_2,\underline{X}^n]$, $H_2[Y_1,Y_2,\underline{X}^n]$.

The first step in the construction is to obtain disjunctive forms for H_1,H_2, and U. Let this be,

$$H_1[Y_1,Y_2,\underline{X}] \;.\equiv.\; Y_1Y_2A_{11}[\underline{X}] \vee Y_1\tilde{Y}_2A_{12}[\underline{X}] \vee \tilde{Y}_1Y_2A_{13}[\underline{X}] \vee \tilde{Y}_1\tilde{Y}_2A_{14}[\underline{X}]$$

(1)

$$H_2[Y_1,Y_2,\underline{X}] \;.\equiv.\; Y_1Y_2A_{21}[\underline{X}] \vee Y_1\tilde{Y}_2A_{22}[\underline{X}] \vee \tilde{Y}_1Y_2A_{23}[\underline{X}] \vee \tilde{Y}_1\tilde{Y}_2A_{24}[\underline{X}]$$

(2) $$U[Y_1,Y_2] \;.\equiv.\; Y_1Y_2 \vee Y_1\tilde{Y}_2$$

Now we let $\underline{k} = 2\frown 2\frown 2\frown 2$ and construct $\underline{G}^k$, $\underline{H}^k$, W as follows,

(3)
$$G_1 : E_1E_2 \qquad G_3 : \tilde{E}_1E_2$$
$$G_2 : E_1\tilde{E}_2 \qquad G_4 : \tilde{E}_1\tilde{E}_2$$

(4)
$$L_1[Z_1,Z_2,Z_3,Z_4,\underline{X}] : Z_1A_{11}[\underline{X}]A_{21}[\underline{X}] \vee Z_2A_{12}[\underline{X}]A_{22}[\underline{X}] \vee Z_3A_{13}[\underline{X}]A_{23}[\underline{X}] \vee Z_4A_{14}[\underline{X}]A_{24}[\underline{X}]$$
$$L_2[Z_1,Z_2,Z_3,Z_4,\underline{X}] : Z_1A_{11}[\underline{X}]\tilde{A}_{21}[\underline{X}] \vee Z_2A_{12}[\underline{X}]\tilde{A}_{22}[\underline{X}] \vee Z_3A_{13}[\underline{X}]\tilde{A}_{23}[\underline{X}] \vee Z_4A_{14}[\underline{X}]\tilde{A}_{24}[\underline{X}]$$
$$L_3[Z_1,Z_2,Z_3,Z_4,\underline{X}] : Z_1\tilde{A}_{11}[\underline{X}]A_{21}[\underline{X}] \vee Z_2\tilde{A}_{12}[\underline{X}]A_{22}[\underline{X}] \vee Z_3\tilde{A}_{13}[\underline{X}]A_{23}[\underline{X}] \vee Z_4\tilde{A}_{14}[\underline{X}]A_{24}[\underline{X}]$$
$$L_4[Z_1,Z_2,Z_3,Z_4,\underline{X}] : Z_1\tilde{A}_{11}[\underline{X}]\tilde{A}_{21}[\underline{X}] \vee Z_2A_{12}[\underline{X}]\tilde{A}_{22}[\underline{X}] \vee Z_3\tilde{A}_{13}[\underline{X}]\tilde{A}_{23}[\underline{X}] \vee Z_4\tilde{A}_{14}[\underline{X}]\tilde{A}_{24}[\underline{X}]$$

(5) $$W[Z_1,Z_2,Z_3,Z_4] \;:\; Z_1 \vee Z_2$$

By definition 4, and (3), (4), (5) it is clear that $\underline{G}\frown\underline{L}\frown W$ is in expanded form. Next we obtain from (1) the identities $\tilde{H}_\nu[Y_1,Y_2,\underline{X}] \;.\equiv.\; Y_1Y_2\tilde{A}_{\nu 1}[\underline{X}] \vee Y_1\tilde{Y}_2\tilde{A}_{\nu 2}[\underline{X}] \vee Y_1\tilde{Y}_2\tilde{A}_{\nu 3}[\underline{X}] \vee \tilde{Y}_1\tilde{Y}_2\tilde{A}_{\nu 4}[\underline{X}]$. Together with (1) and (4) this yields,

(6)
$$L_1[Y_1Y_2,\; Y_1\tilde{Y}_2,\; \tilde{Y}_1Y_2,\; \tilde{Y}_1\tilde{Y}_2,\; \underline{X}] \;.\equiv.\; H_1[Y_1,Y_2,\underline{X}]\; H_2[Y_1,Y_2,\underline{X}]$$
$$L_2[Y_1Y_2,\; Y_1\tilde{Y}_2,\; \tilde{Y}_1Y_2,\; \tilde{Y}_1\tilde{Y}_2,\; \underline{X}] \;.\equiv.\; H_1[Y_1,Y_2,\underline{X}]\; \tilde{H}_2[Y_1,Y_2,\underline{X}]$$
$$L_3[Y_1Y_2,\; Y_1\tilde{Y}_2,\; \tilde{Y}_1Y_2,\; \tilde{Y}_1\tilde{Y}_2,\; \underline{X}] \;.\equiv.\; \tilde{H}_1[Y_1,Y_2,\underline{X}]\; H_2[Y_1,Y_2,\underline{X}]$$
$$L_4[Y_1Y_2,\; Y_1\tilde{Y}_2,\; \tilde{Y}_1Y_2,\; \tilde{Y}_1\tilde{Y}_2,\; \underline{X}] \;.\equiv.\; \tilde{H}_1[Y_1,Y_2,\underline{X}]\; \tilde{H}_2[Y_1,Y_2,\underline{X}]$$

and from (2) and (5) we get,

(7) $$W[Y_1Y_2,\; Y_1\tilde{Y}_2,\; \tilde{Y}_1Y_2,\; \tilde{Y}_1\tilde{Y}_2] \;.\equiv.\; U[Y_1Y_2] \;.$$

Now assume that U is a special output of $\underline{E}\frown\underline{H}$. Let $\underline{C}[Y_1,Y_2]$ stand for $Y_1Y_2\frown Y_1\tilde{Y}_2\frown\tilde{Y}_1Y_2\frown\tilde{Y}_1\tilde{Y}_2$. Then using in order (7), definition 2, (7), (6) one obtains $W[\underline{C}[Y_1,Y_2]] \equiv W[\underline{L}[\underline{C}[Y_1Y_2],\Lambda]]$. This means that $W[\underline{Z}] \equiv W[\underline{L}[\underline{Z},\Lambda]]$ holds for the values $\overbrace{\vee\Lambda\Lambda\Lambda}$, $\overbrace{\Lambda\vee\Lambda\Lambda}$, $\overbrace{\Lambda\Lambda\vee\Lambda}$, and $\overbrace{\Lambda\Lambda\Lambda\vee}$ of $\underline{Z}$. Because of the particular form (5) of W the restriction of the range of $\underline{Z}$ can be omitted, which by definition 2 means that W is special output of $\underline{G}\frown\underline{L}$.

Next let $\underline{i}$ be any n-predicate and let $r_1\frown r_2 = \underline{\zeta}(\underline{E},\underline{H},\underline{i})$, $s_1\frown s_2\frown s_3\frown s_4 = \underline{\zeta}(\underline{G},\underline{L},\underline{i})$, so that

$$(8)\qquad \begin{aligned} \underline{r}(o) &\equiv \underline{E} \\ \underline{r}(t') &\equiv \underline{H}[\underline{r}(t),\underline{i}(t)] \end{aligned} \qquad\qquad (9)\qquad \begin{aligned} \underline{s}(o) &\equiv \underline{G} \\ \underline{s}(t') &\equiv \underline{L}[\underline{s}(t),\underline{i}(t)] \end{aligned}$$

Using (3), (6), (8), (9) one shows by an induction on t that $s_1(t) \equiv r_1(t)\ r_2(t)$, $s_2(t) \equiv r_1(t)\ \tilde{r}_2(t)$, $s_3(t) \equiv \tilde{r}_1(t)\ r_2(t)$, $s_4(t) \equiv \tilde{r}_1(t)\ \tilde{r}_2(t)$ hold for all t. Because of (7) this yields, $(\forall t)\cdot W[\underline{s}(t)] \equiv U[\underline{r}(t)]$. By definition 3 it follows that $\beta(\underline{G},\underline{L},W) = \beta(\underline{K},\underline{H},U)$.

Lemma 4. Let $\underline{E}^m\frown\underline{H}^m$ be an $\underline{n}\frown 2/\underline{m}$-automaton in expanded form and let $\underline{L}^m$ be defined by, $\underline{L}^m[\underline{Y}^m, \underline{X}^n] \ :\ \underline{H}^m[\underline{Y}^m, \underline{X}^n\frown\vee] \vee \underline{H}^m[\underline{Y}^m, \underline{X}^n\frown\Lambda]$.

(a) If $\underline{i}^n\frown j$ is any $\underline{n}\frown 2$-predicate and if $\underline{r}^m = \underline{\zeta}(\underline{E},\underline{H},\underline{i}^m\frown j)$, and $\underline{s}^m = \underline{\zeta}(\underline{E},\underline{L},\underline{i}^n)$, then (t) $[\underline{r}(t) \supset \underline{s}(t)]$.

(b) If $\underline{i}^n$ is any $\underline{n}$-predicate, and $\underline{s}^m = \underline{\zeta}(\underline{E},\underline{L},\underline{i}^n)$, and $s_\nu(x') \equiv \vee$, then there exists a special predicate j of length $\leq x$ such that also $r_\nu(x') \equiv \vee$, in case $\underline{r}^m = \underline{\zeta}(\underline{E},\underline{H},\underline{i}^n\frown j)$.

Proof: By assumption $\underline{H}^n$ is of form

(1) $\underline{H}^m[\underline{Y}^m, \underline{X}^n\frown Z] \ :\ Y_1\underline{K}^m[\underline{X}^n\frown Z] \vee \ldots\ldots \vee Y_m\underline{K}^m_m[\underline{X}^n\frown Z]$.

Now let $\underline{i}\frown\underline{j}$ be any $\underline{n}\frown 2$-predicate and let $\underline{r} = \underline{\zeta}(\underline{E},\underline{H},\underline{i}\frown\underline{j})$, $\underline{s} = \underline{\zeta}(\underline{E},\underline{L},\underline{i})$. Then by definition 3 and the construction of $\underline{L}$,

$$(2)\qquad \begin{aligned} \underline{r}(o) &\equiv \underline{E} \\ \underline{r}(t') &\equiv \underline{H}[\underline{r}(t),\underline{i}(t)\frown\underline{j}(t)] \end{aligned}$$

$$(3)\qquad \begin{aligned} \underline{s}(o) &\equiv \underline{E} \\ \underline{s}(t') &\equiv \underline{H}[\underline{s}(t),\underline{i}(t)\frown\mathsf{V}] \vee \underline{H}[\underline{s}(t),\underline{i}(t)\frown\Lambda] \end{aligned}$$

hold for all t. Making use of (1), (2), (3) it follows by induction on t that $(\forall t)[\underline{r}(t)\supset\underline{s}(t)]$. Thus part (a) of the lemma is established.

Next let $\underline{i}$ be any $\underline{n}$-predicate, let $\underline{s} = \underline{\zeta}(\underline{E},\underline{L},\underline{i})$, and suppose that $s_\nu(x') \equiv \mathsf{V}$. Then by definition 3 the predicates $\underline{i}$ and $\underline{s}$ satisfy (3) for all t, so that by (1) we obtain

$$(4)\qquad \begin{aligned} s_\rho(o) &\equiv E_\rho && ,\rho = 1,\ldots,m \\ s_\rho(t') &\equiv \bigvee_{\substack{\nu=1,\ldots,m \\ Y=\Lambda,\mathsf{V}}} s_\nu(t)K_{\rho,\nu}[\underline{i}(t')\frown Y] && ,\rho = 1,\ldots,m \end{aligned}$$

Now we stepwise choose a sequence of truth values $j(x),\ldots,j(o)$ and a sequence of indices $\nu_{x+1},\ldots,\nu_o$ according to the following specifications. I. Let ν_{x+1} be ν. II. If ν_{y+1} has already been obtained choose $\nu_y, j(y)$ such that $s_{\nu_y}(y)$ and $K_{\nu_{y+1},\nu_y}[\underline{i}^n(y)\frown j(y)]$ hold. That these choices are possible clearly follows by the assumption $s_\nu(x) \equiv \mathsf{V}$ and (4). Let now the values $\underline{r}(o),\ldots,\underline{r}(x')$ be defined from $\underline{i}(o),\ldots,\underline{i}(x)$, $j(o),\ldots,j(x)$ by the recursions (2), so that by (1), $r_\rho(o) \equiv E_\rho$; $r_\rho(t') \equiv \bigvee_{\mu=1,\ldots,m} r_\mu(t)K_{\rho,\mu}[\underline{i}(t)\frown j(t)]$ for $t \leq x$. Then by using II one stepwise obtains $r_{\nu_o}(o)$, $K_{\nu_1,\nu_o}[\underline{i}(o)\frown j(o)],\ldots,r_{\nu_x}(x)$, $K_{\nu_{x+1},\nu_x}[\underline{i}(x)\frown j(x)]$, $r_{\nu_{x+1}}(x+1)$. Therefore by I, $r_\nu(x') \equiv \mathsf{V}$. Thus by extend-

ing the sequence $j(o),\ldots,j(x)$ letting $j(t) \equiv \Lambda$ for $t > x$, we obtain a special predicate j such that j is of length $\leq x$, and $r_\nu(x') \equiv \mathrm{V}$ in case $\underline{r} = \zeta(\underline{E},\underline{H},\underline{i}^n)$. Therefore also part (b) of the lemma is established.

Lemma 5. For every $\underline{n}/\underline{m}$-automaton with output $\underline{E}^{m\frown}\underline{H}^{m\frown}\underline{U}$ one can construct a number h and an output W such that

(a) $U[\underline{Y}] \supset W[\underline{Y}]$

(b) $\underline{Z}_1 \equiv \underline{Y} \wedge \underline{Z}_2 \equiv \underline{H}[\underline{Z}_1,\underline{\Lambda}] \wedge \ldots \wedge \underline{Z}_h \equiv \underline{H}[\underline{Z}_{h-1},\underline{\Lambda}] \;.\supset.\; U[\underline{Z}_1] \vee \ldots \vee U[\underline{Z}_h]$

(c) If $U[\underline{Y}] \supset U[\underline{H}[\underline{Y},\underline{\Lambda}]]$ then W is special output of $\underline{E}^{\frown}\underline{H}$.

Proof: The construction of h and $W[\underline{Y}^m]$ from $\underline{H}^m[\underline{Y}^m,\underline{X}^m]$ and $U[\underline{Y}\ ]$ proceeds by the following rules,

I. Let $U_o[\underline{Y}]$ be V, let $U_1[\underline{Y}]$ be $U[\underline{Y}]$.

II. If $U_k[\underline{Y}] \equiv U_{k+1}[\underline{Y}]$ is not tautologous, let $U_{k+2}[\underline{Y}]$ be $U_{k+1}[\underline{Y}] \vee U_{k+1}[\underline{H}[\underline{Y},\underline{\Lambda}]]$

III. If $U_k[\underline{Y}] \equiv U_{k+1}[\underline{Y}]$ is tautologous, let h be k, let W be U_k, and stop.

From this construction it is clear that $U_o[\underline{Y}] \supset U_1[\underline{Y}]$, $U_1[\underline{Y}] \supset U_2[\underline{Y}]$, ... Because there are only $a=2^{(2^m)}$ truth-functions on m arguments the construction must reach a stage $k \leq a$ such that U_k and U_{k+1} denote the same truth function, i.e., such that $U_k[\underline{Y}] \equiv U_{k+1}[\underline{Y}]$. The next step in the construction then clearly must use the stoprule III. Thus the construction always ends in $k \leq a$ steps, yielding an h and a W.

Suppose now for example that h turns out to be 3, so that W is U_3 and $U_3 \equiv U_4$. Letting $\underline{K}[\underline{Y}]$ stand for $\underline{H}[\underline{Y},\underline{\Lambda}]$ it follows from the construction, (1) $U_2[\underline{Y}] \equiv. U[\underline{Y}] \vee U[\underline{K}[\underline{Y}]]$, and (2) $U_3[\underline{Y}] \equiv. U_2[\underline{Y}] \vee U_2[\underline{K}[\underline{Y}]]$, and (3) $U_4[\underline{Y}] \equiv U_3[\underline{Y}] \vee U_3[\underline{K}[\underline{Y}]]$.

By (1), $U[\underline{Y}] \supset U_2[\underline{Y}]$ and by (2), $U_2[\underline{Y}] \supset U_3[\underline{Y}]$. Therefore $U[\underline{Y}] \supset U_3[\underline{Y}]$. Because W is U_3 this established part (a) of the lemma.

Next suppose $\underline{Z}_1 \equiv \underline{Y}_1$, $\underline{Z}_2 \equiv \underline{K}[\underline{Z}_1]$, $\underline{Z}_3 \equiv \underline{K}[\underline{Z}_2]$, and $U_3[\underline{Y}_1]$. Then by (2), $U_2[\underline{Z}_1] \vee U_2[\underline{Z}_2]$. This yields by (1), $U[\underline{Z}_1] \vee U[\underline{Z}_2] \vee U[\underline{Z}_3]$. Because U_3 is W and $\underline{K}[\cdot]$ is $H[\cdot, \underline{\Lambda}]$ this established part (b) of the lemma.

Now suppose $U[\underline{Y}] \supset U[\underline{K}[\underline{Y}]]$. Then by (1), $U_2[\underline{Y}] \supset U[\underline{K}[\underline{Y}]]$, and also by (1), $U[\underline{K}[\underline{Y}]] \supset U_2[\underline{K}[\underline{Y}]]$. Therefore $U_2[\underline{Y}] \supset U_2[\underline{K}[\underline{Y}]]$. From this, by using (2), $U_3[\underline{Y}] \supset U_3[\underline{K}[\underline{Y}]]$ is similarly obtained. But also $U_3[\underline{K}[\underline{Y}]] \supset U_3[\underline{Y}]$, because of (3) and $U_3 \equiv U_4$. Thus, $U_3[\underline{Y}] \equiv U_3[\underline{K}[\underline{Y}]]$. Because U_3 is W and $K[\underline{Y}]$ is $H[\underline{Y}, \underline{\Lambda}]$ this means that W is a special output of $\underline{E} \frown \underline{H}$. This establishes part (c) of the lemma.

Lemma 6: To every $\underline{n} \frown 2/\underline{m}$-automaton with special output $\underline{E}^{\underline{m}} \frown \underline{H}^{\underline{m}} \frown U$ in expanded form one can construct a $\underline{n}/\underline{m}$-automaton with special output $\underline{E}^{\underline{m}} \frown \underline{L}^{\underline{m}} \frown W$ such that for every special $\underline{n}$-predicate $\underline{i}^{\underline{n}}$, $\underline{i} \epsilon \beta(\underline{G}, \underline{L}, W) \equiv (\exists j)[\underline{i} \frown j \epsilon \beta(\underline{E}, \underline{H}, U)]$ and $\underline{E} \frown \underline{L} \frown \underline{W}$ is again in expanded form.

Proof: The construction of $\underline{L}^{\underline{m}}$, W is as follows,

(1) $\underline{L}[\underline{Y}, \underline{X}] \ : \ \underline{H}[\underline{Y}, \underline{X} \frown \vee] \vee \underline{H}[\underline{Y}, \underline{X} \frown \Lambda]$

(2) $h, W[\underline{Y}] \ :$ apply construction of lemma 4 to $\underline{E} \frown \underline{L} \frown U$.

Assume now that $\underline{E}$ $\underline{H}$ U is in expanded form and U is special. Then by definitions 2, 4,

(3) $U[\underline{Y}] \ : \ Y_1 \vee Y_2 \vee \ldots \vee Y_k$

(4) $U[\underline{Y}] \equiv U[\underline{H}[\underline{Y}, \underline{\Lambda} \frown \Lambda]]$

By using (4), (3), (1), (3) in this order one shows $U[\underline{Y}] \supset U[\underline{L}, [\underline{Y}, \underline{\Lambda}]]$. Therefore, by (2) and lemma 5 (c), W is a special output of $\underline{E} \frown \underline{L}$.

Next assume $\underline{i} \frown j \epsilon \beta(\underline{E}, \underline{H}, U)$, and let $\underline{r} = \underline{\zeta}(\underline{E}, \underline{H}, \underline{i} \frown j)$ and $\underline{s} = \underline{\zeta}(\underline{E}, \underline{L}, \underline{i})$. Then by definition 3, $(\exists x)\ (\forall t)_x^{\infty}\ U[\underline{r}(t)]$, and by (1), lemma 4(a), $(\forall t)\ [\underline{r}(t) \supset \underline{s}(t)]$.

Therefore it follows by (3) that $(\exists x)\ (\forall t)^{\infty}_{x}\ U[\underline{s}(t)]$. By (2) and lemma 5(a) this yields $(\exists x)\ (\forall t)^{\infty}_{x}\ W[\underline{s}(t)]$. Therefore, by definition 3, $\underline{i}\epsilon\beta(\underline{E},\underline{L},W)$. Thus we have shown that $(\exists j)[\underline{i}\frown j\epsilon\beta(\underline{E},\underline{H},U)] \supset \underline{i}\epsilon\beta(E,L,W)$.

Assume now that $\underline{i}\epsilon\beta(\underline{E},\underline{L},W)$, and let $\underline{s} = \underline{\zeta}(\underline{E},\underline{L},\underline{i})$. Then if γ is the length of $\underline{i}$ it follows by (*) that $W[\underline{s}(\gamma+1)]$. Because of (3) and lemma 5(b) this implies that $U[s(\gamma+1)]\vee.....\vee U[s(\gamma+h+1)]$, and by (3), there are $\nu,p \leq h$ such that $s_{\nu}(\gamma+p+1) \equiv \Upsilon$. Because $\underline{E}\frown\underline{H}$ is in expanded form and because of (1) we therefore can apply lemma 4(b) to conclude that there is a j of length $\leq 1+p$ such that $r_{\nu}(\gamma+p+1) \equiv \Upsilon$, for $\underline{r} = \underline{\zeta}(\underline{E},\underline{H},\underline{i}\frown j)$. Using (3) we obtain $U[\underline{r}(\gamma+p+1)]$. Now observe that $\underline{i}(t) \equiv \underline{\Lambda}$, and $j(t) \equiv \Lambda$, for $t>1+p$. Because U is special output of $\underline{E}\frown\underline{H}$ it therefore follows that $(\forall t)^{\infty}_{\gamma+p+1}\ U[\underline{r}(t)]$. By definition 3 this means that $\underline{i}^{n}\frown j\epsilon\beta(\underline{E},\underline{H},U)$. Thus we have concluded the proof of lemma 6 by showing that $\underline{i}\epsilon\beta(\underline{E},\underline{L},W) \supset (\exists j)[\underline{i}\frown j\epsilon\beta(\underline{E},\underline{H},U)]$.

4. ANALYSIS AND SYNTHESIS

We begin by establishing a synthesis result for formulas of W.2.A. which do not contain predicate-quantifiers. Using the lemmas of Sections 2 and 3 one then easily extends the result.

Lemma 7: To every formula $\underline{\underline{C}}(\underline{i}^{n})$ of the form $K[\underline{i}(o)]\wedge(\forall t)B[\underline{i}(t),\underline{i}(t')]$ one can construct a $\underline{n}/\underline{m}$-automaton $\underline{E}^{m}\frown\underline{H}^{m}$ and a special output $U[\underline{Y}^{m}]$ such that $\beta(E,H,U) = \hat{\underline{i}}\underline{\underline{C}}(\underline{i})$.

Proof: We first determine whether or not $B[\underline{\Lambda},\underline{\Lambda}]$. In case $\tilde{B}[\underline{\Lambda},\underline{\Lambda}]$, we take for $\underline{E}\frown\underline{H}$ any automaton and for U the output Λ. Then clearly U is special out-

put and $\beta(\underline{E},\underline{H},U) = \hat{\underline{i}}\underline{C}(\underline{i})$ are both empty. Thus in this case Lemma 7 is established.

Let us next consider the case $B[\underline{\Lambda},\underline{\Lambda}]$. Then we take m to be n+2, and E^m to be $\underline{\mathcal{V}}^m$. $\underline{H}^m$ we define as follows.

$$H_\nu[\underline{Y}^n \frown Z_1 \frown Z_2, \underline{X}^n] \ : \ X_\nu \qquad \text{for } \nu = 1,\ldots,n$$

$$H_{n+1}[\underline{Y}^n \frown Z_1 \frown Z_2, \underline{X}^n] \ : \ \Lambda$$

$$H_{n+2}[\underline{Y}^n \frown Z_1 \frown Z_2, \underline{X}^n] \ : \ Z_1K[\underline{X}^n] \vee \tilde{Z}_1Z_2B[\underline{Y}^n,\underline{X}^n].$$

As output we choose the formula

$$U[\underline{Y}^n \frown Z_1 \frown Z_2] \ : \ Z_1K[\underline{\Lambda}^n] \vee \tilde{Z}_1Z_2B[\underline{Y}^n,\underline{\Lambda}^n].$$

Noting that $B[\underline{\Lambda},\underline{\Lambda}]$, and using definition 2, one easily checks that U is a special output of $\underline{E} \frown \underline{H}$. Furthermore, the transition-recursion of $\underline{E} \frown \underline{H}$ is clearly equivalent to the recursion

$$r_\nu(o) \equiv \mathcal{V} \qquad , \nu = 1,\ldots,n+2$$

$$r_{n+2}(1) \equiv K[\underline{i}(o)]$$

$$r_\nu(t') \equiv i_\nu(t) \qquad , \nu = 1,\ldots,n$$

$$r_{n+1}(t') \equiv \Lambda$$

$$r_{n+2}(t'') \equiv r_{n+2}(t')\ B[\underline{i}(t),\underline{i}(t')]$$

and therefore the operator $\underline{r}^m = \zeta(\underline{E},\underline{H},\underline{i}^n)$ can also be defined by

$$r_\nu(o) \equiv \mathcal{V} \qquad , \nu = 1,\ldots,n+2$$

$$r(t') \equiv i_\nu(t) \qquad , \nu = 1,\ldots,n$$

$$r_{n+1}(t') \equiv \Lambda$$

$$r_{n+2}(t') \equiv K[\underline{i}(o)] \wedge (\forall x)_o^{t-1}\ B[\underline{i}(x),\underline{i}(x')]$$

Consequently, the output-operator $u = \psi(\underline{E},\underline{H},U)$ is defined by

$$u(o) \equiv K[\underline{\Lambda}]$$

$$u(t') \equiv K[\underline{i}(o)] \wedge (\forall x)_o^{t-1}\ B[\underline{i}(x),\underline{i}(x')] \wedge B[\underline{i}(t),\underline{\Lambda}].$$

Because B[$\underline{\Lambda},\underline{\Lambda}$] it follows that for any special $\underline{i}$, $u = \underline{\psi}(\underline{E},\underline{H},U)$ is ultimately $\underline{\vee}$ just in case $K[\underline{i}(o)] \wedge (\forall t)B[\underline{i}(t),\underline{i}(t')]$. I.e., by definition 3, $\beta(\underline{E},\underline{H},U) = \hat{\underline{\underline{i}}}\underline{\underline{C}}(\underline{i})$.

Theorem 1: (synthesis) For every formula $\underline{\underline{C}}(\underline{i}^n)$ of W.2.A. one can construct a $\underline{n}/\underline{m}$-automaton $\underline{E}^m \frown \underline{H}^m$ with special output $U[\underline{Y}^m]$ such that $\beta(\underline{E},\underline{H},U) = \hat{\underline{\underline{i}}}\underline{\underline{C}}(\underline{i})$, i.e., such that the behavior of $\underline{E} \frown \underline{H} \frown U$ is just the set of special $\underline{n}$-predicates which satisfy $\underline{\underline{C}}(\underline{i})$.

Proof: Using Lemma 1 we first construct the formula $\underline{\underline{C}}^*(\underline{i})$ equivalent to $\underline{\underline{C}}(\underline{i})$. Let us for example assume that $\underline{\underline{C}}^*(\underline{i})$ is as follows, $\underline{\underline{C}}^*(\underline{i})$: $(\forall \underline{r})\ (\exists\, \underline{s})\ \cdot$ $K[\underline{r}(o),\underline{s}(o)] \wedge (\forall t)\ B[\underline{i}(t),\underline{r}(t),\underline{s}(t),\underline{r}(t'),\underline{s}(t')]$. Next we use the construction of Lemma 7 to obtain an automaton $\underline{E}_1 \frown \underline{H}_1$ with special output U_1 such that for special $\underline{i}$, $\underline{r}$, $\underline{s}$,

(1) $$\underline{i} \frown \underline{r} \frown \underline{s}\ \epsilon\beta(\underline{E}_1,\underline{H}_1,U)\ \ .\equiv.\ \ K(o) \wedge (\forall t)B(t).$$

Using Lemma 3 we next construct $\underline{E}_2 \frown \underline{H}_2 \frown U_2$ in expanded form and such that

(2) $$\beta(\underline{E}_2,\underline{H}_2,U_2) = \beta(\underline{E}_1,\underline{H}_1,U_1).$$

By repeated application of the construction of Lemma 6 starting with $\underline{E}_2 \frown \underline{H}_2 \frown U$ one obtains $\underline{E}_3 \frown \underline{H}_3 \frown U_3$ such that for special $\underline{i}$, $\underline{r}$, $\underline{i} \frown \underline{r}\ \epsilon\beta(\underline{E}_3,\underline{H}_3,U_3)\ .\equiv.$ $(\exists\, \underline{s})[\underline{i} \frown \underline{r} \frown \underline{s}\ \epsilon\beta(\underline{E}_2,\underline{H}_2,U_2]$ and therefore by Lemma 2,

(3) $$\underline{i} \frown \underline{r}\ \epsilon\beta(\underline{E}_3,\underline{H}_3,\tilde{U}_3)\ .\equiv.\ (\exists s)[\underline{i} \frown \underline{r} \frown \underline{s}\ \epsilon\beta(\underline{E}_2,\underline{H}_2,U_2)]$$

Because the complementation destroys the expanded form we are forced to use Lemma 3 again to obtain $\underline{E}_4 \frown \underline{H}_4 \frown U_4$ in expanded form and such that

(4) $$\beta(\underline{E}_4,\underline{H}_4,U_4) = \beta(\underline{E}_3,\underline{H}_3,\tilde{U}_3).$$

By repeatedly applying Lemma 6 we next construct $\underline{E}_5 \frown \underline{H}_5 \frown U_5$ such that for every

special $\underline{i}$, $\underline{i} \in \beta(\underline{E}_5,\underline{H}_5,U_5)$ $.\equiv.$ $(\exists \underline{r}).\underline{i}^\frown \underline{r} \in \beta(\underline{E}_4,\underline{H}_4,U_4)$ and therefore by Lemma 2,

(5) $$\underline{i} \in \beta(\underline{E}_5,\underline{H}_5,\tilde{U}_5) .\equiv. \sim (\exists \underline{r})\ \underline{i}^\frown \underline{r} \in \beta(\underline{E}_4,\underline{H}_4,U_4)$$

From (1),.....,(5) it clearly follows that $\underline{i} \in \beta(\underline{E}_5,\underline{H}_5,U_5)$ $.\equiv.$ $\underline{\underline{C}}^*(\underline{i})$. Because $\underline{\underline{C}}^*$ is equivalent to $\underline{\underline{C}}$ this shows that the behavior of $\underline{E}_5^\frown \underline{H}_5^\frown U_5$ is $\hat{\underline{i}}\underline{\underline{C}}(\underline{i})$.

We next obtain a rather strong converse to Theorem 1.

Theorem 2: (analysis) To every $\underline{n}/\underline{m}$-automaton with special output $\underline{E}^{m\frown} \underline{H}^{m\frown} U$ one can construct a formula $\underline{\underline{C}}(\underline{i}^n)$ of W.2.A. such that $\underline{i}\underline{\underline{C}}(\underline{i}) = \beta(\underline{E},\underline{H},U)$, and such that furthermore $\underline{\underline{C}}(\underline{i})$ is of the form $(\exists \underline{j}^p).K[\underline{j}(o)] \wedge (\forall t)B[\underline{i}(t),\underline{j}(t),\underline{j}(t')]$.

Proof: By definition 3 it is clear that for every special $\underline{i}$, $\underline{i} \in \beta(\underline{E},\underline{H},U)$ $.\equiv.$ $(\exists \underline{r})[\underline{r}(o)\equiv\underline{E} \wedge (\forall t)[\underline{r}(t')\equiv\underline{H}[\underline{r}(t),\underline{i}(t)]] \wedge (\exists x)(\forall t)_x^\infty U[r(t)]]$. However, the range of $(\exists \underline{r})$ in this formula may not be restricted to special predicates. On the other hand, because U is assumed to be special, the formula may be slightly modified so that the range of $(\exists r)$ can be restricted to special predicates. Namely, it is clear that for any special $\underline{i}$,

(1) $\underline{i} \in (\underline{E},\underline{H},U)..\equiv..(\exists \underline{r})(\exists x)\ .\ \underline{r}(o)\equiv\underline{E}\ \ (\forall t)_o^x[\underline{r}(t')\equiv\underline{H}(t)] \wedge (\forall t)_x^\infty[\underline{i}(t)\equiv \underline{\wedge}$

$\wedge U\ \underline{r}(t)]]$.

It remains to change this definition of β in W.2.A. to one of the simple form required in Theorem 2. This is accomplished by using the following device for changing the individual quantification $(\exists x)$ to a quantification $(\exists j)$ over restricted predicates,

(2) $\underline{i} \in \beta(\underline{E},\underline{H},U)..\equiv..(\exists \underline{r})(\exists j)\ .\ (\forall t)[j(t') \supset j(t)] \wedge \underline{r}(o)\equiv\underline{E} \wedge (\forall t)\ j(t) \supset$

$[\underline{r}(t')\equiv\underline{H}(t)]] \wedge (\forall t)[\tilde{j}(t) \supset [\underline{i}(t)\equiv \underline{\wedge}\wedge U[\underline{r}(t)]]]$.

To see that (2) is correct in case $(\exists \underline{r})(\exists j)$ is interpreted as ranging over special predicates we observe that the right sides of (1) and (2) are equivalent

because of an obvious one-to-one relationship between numbers x and restricted predicates j satisfying $(\forall t)[j(t') \supset j(t)]$.

Thus the right side of (2) is a formula $\underline{\underline{C}}(\underline{i})$ as required in Theorem 2.

5. DEFINABILITY IN W.2.A.

We will use the notation "[0, x+1, $\exists_0 i$]" to denote W.2.A. This is intended to indicate that we are dealing with an interpreted system which besides first-order quantification over natural numbers contains 0, the function x+1, and quantification over special predicates. Similar notations for other interpreted systems, all containing first-order quantification over natural numbers, are used below. "$\exists_0 \zeta$" indicates quantification over eventually constant monadic functions from natural numbers to natural numbers.

The following systems are known to be very strong in the sense that all recursively enumerable predicates are definable in each.

[0, =, x+1, $\exists_0 \zeta$] Gödel [5]

[0, =, x+y, x.y] Gödel [5]

[0, x+1, 2x, $\exists_0 i$] Robinson [14]

(In fact these systems are equivalent in the sense that the same predicates on natural numbers can be defined in each.) In contrast we will now show that [0, x+1, $\exists_0 i$] is much weaker, in particular the only monadic predicates on natural numbers definable in W.2.A. are those which are ultimately periodic.

Definition 5: A formula of W.2.A is said to be in normal form if it is of the following type, $\underline{\underline{C}}(\underline{i}^m, x_1, \ldots, x_p)$: $(\exists\, \underline{j}^m)[K[\underline{j}(o)] \wedge (\forall t)B[\underline{i}(t), \underline{j}(t), \underline{j}(t')] \wedge A_1[\underline{j}(x_1)] \wedge \ldots \wedge A_p[\underline{j}(x_p)]$

Theorem 3: For every formula $\underline{\underline{C}}(\underline{i}^n, x_1,\ldots,x_p)$ of W.2.A. one can construct an equivalent formula $\underline{\underline{C}}^*(\underline{i}^n, x_1,\ldots,x_p)$ which is in normal form, i.e., every predicate on numbers and special predicates definable in W.2.A. is definable by a formula in normal form.

Proof: Suppose first that $\underline{\underline{A}}(\underline{i}^n)$ is a formula without free individual variables. Then by Theorem 1 one can construct an automaton $\underline{E}^{\frown}\underline{H}$ with special output U such that $\beta(\underline{E},\underline{H},U) = \hat{\underline{\underline{i}}}\underline{\underline{A}}(i)$. Next, by Theorem 2 one can construct a formula $\underline{\underline{A}}^*(\underline{i})$ in normal form such that $\hat{\underline{\underline{i}}}\underline{\underline{A}}^*(\underline{i}) = \beta(\underline{E},\underline{H},U)$. It follows, $\hat{\underline{\underline{i}}}\underline{\underline{A}}(\underline{i}) = \hat{\underline{\underline{i}}}\underline{\underline{A}}^*(i)$. Thus,

(1) If $\underline{\underline{A}}(\underline{i})$ does not contain free individual variables one can construct a normal $\underline{\underline{A}}^*(\underline{i})$ equivalent to $\underline{\underline{A}}(\underline{i})$.

Let us next start with a formula $\underline{\underline{C}}$ which contains free individual variables, say for example $\underline{\underline{C}}(\underline{i},x_1,x_2)$. Let $\underline{\underline{A}}$ be defined thus, $\underline{\underline{A}}(\underline{i},s_1,s_2)$: $s_1(o) \wedge s_2(o) \wedge (\forall t)[s_1(t') \supset s_1(t)] \wedge (\forall t)[s_2(t') \supset s_2(t)] \wedge (\forall t_1 t_2)[s_1(t_1)\tilde{s}_1(t_1')s_2(t_2)\tilde{s}_2(t_2') \supset \underline{\underline{C}}(\underline{i},t_1,t_2)]$. It is then easy to see that $\underline{\underline{A}}(\underline{i},s_1,s_2)\ \underline{\underline{C}}(\underline{i},x_1,x_2)$, in case x_1+1, x_2+1 are respectively the length of the special predicates s_1,s_2. Re-stating this we obtain $\underline{\underline{C}}(\underline{i},x_1,x_2) \ .\equiv. \ (\exists s_1 s_2)[\underline{\underline{A}}(\underline{i},s_1,s_2) \wedge s_1(x_1)\tilde{s}_1(x_1') \wedge s_2(x_2)\tilde{s}_2(x_2')]$, and therefore,

(2) $\underline{\underline{C}}(\underline{i},x_1,x_2) \ ..\equiv.. \ (\exists s_1 s_2 r_1 r_2).\underline{\underline{A}}(\underline{i},s_1,s_2) \wedge (\forall t)[r_1(t)\equiv s_1(t')] \wedge (\forall t)[r_2(t)\equiv s_2(t')] \wedge s_1(x_1)\tilde{r}_1(x_1) \wedge s_2(x_2)\tilde{r}_2(x_2)$.

Finally we use (1) to obtain a $\underline{\underline{A}}^*(\underline{i},s_1,s_2)$ in normal form and equivalent to $\underline{\underline{A}}$. Replacing in the right side of (2) $\underline{\underline{A}}$ by $\underline{\underline{A}}^*$ and performing some obvious shifts of quantifiers will then yield a $\underline{\underline{C}}^*$ equivalent to $\underline{\underline{C}}$ such that $\underline{\underline{C}}^*$ is in normal form.

Corollary 1: There is a procedure for deciding whether or not a sentence of W.2.A. is true.[2]

Proof: Because of Theorem 3 it is sufficient to indicate a procedure which decides the truth of sentences $\underline{\underline{C}}$ of form $(\exists \underline{j}) \cdot K[\underline{j}(o)] \wedge (\forall t)\, B[\underline{j}(t), \underline{j}(t')]$. We may furthermore assume that $B[\underline{\Lambda},\underline{\Lambda}]$, because otherwise the sentence $\underline{\underline{C}}$ is clearly false in W.2.A. $\underline{\underline{C}}$ then is equivalent to the assertion,

(1) There is an x and a sequence of states $\underline{Y}_o,\ldots,\underline{Y}_x$ such that $K[\underline{Y}_o]$, $B[\underline{Y}_o,\underline{Y}_1],\ldots$ $\ldots$, $B[\underline{Y}_{x-1},\underline{Y}_x]$, $\underline{Y}_x \equiv \underline{\Lambda}$.

Note that in case $x \geq k$ = number of states of $\underline{j}$ there must occur a repetition in the sequence $\underline{Y}_o, \underline{Y}_1,\ldots,\underline{Y}_x$, say $\underline{Y}_y \equiv \underline{Y}_z$ for some $0 \leq y < z \leq x$. Then if $\underline{Y}_o,\ldots,\underline{Y}_y,\ldots,\underline{Y}_z,\ldots,\underline{Y}_x$ is a B-sequence, the shorter sequence $\underline{Y}_o,\ldots,\underline{Y}_y$, $\underline{Y}_{z+1},\ldots,\underline{Y}_x$ is still a B-sequence. Consequently the assertion (1) is equivalent to,

(2) There is an $x \leq k$ = number of states of $\underline{j}$, and there is a sequence of states $\underline{Y}_o,\ldots,\underline{Y}_x$ such that $K[\underline{Y}_o]$, $B[\underline{Y}_o,\underline{Y}_1],\ldots,$ $B[\underline{Y}_{x-1},\underline{Y}_x]$, $\underline{Y}_x \equiv \underline{\Lambda}$.

Because there are only a finite number of sequences $\underline{Y}_o,\ldots,\underline{Y}_x$, $x \leq k$, it is clear that one can effectively check whether or not (2) holds. Because $\underline{\underline{C}}$ is equivalent to (1), and (1) is equivalent to (2), this establishes Corollary 1.

Corollary 2: Every formula $\underline{\underline{C}}(x)$ of W.2.A. defines an ultimately periodic set $\hat{x}\underline{\underline{C}}(x)$ of natural numbers, i.e., there are numbers $\underline{\gamma}$ (phase) and p (period) such that $(\forall t)[\underline{\underline{C}}(\underline{\gamma}+t+p) \equiv \underline{\underline{C}}(\underline{\gamma}+t)$.

2. As R. L. Vaught remarks, this result can be obtained from a theorem of A. Ehrenfeucht; see Robinson [14].

Every ultimately periodic set of natural numbers is definable in W.2.A. by a formula $\underline{\underline{C}}(x)$.

Proof: By theorem 3 we may assume that $\underline{\underline{C}}(x)$ is of the form $\underline{\underline{C}}(x)$: $(\exists\, \underline{j}).K[\underline{j}(o)] \wedge (\forall t)B[j(t), \underline{j}(t')] \wedge A[\underline{j}(x)]$. Now, let $\underline{Y}_1,\ldots,\underline{Y}_a$ be those states $\underline{Y}$ of $\underline{j}$ for which $A[\underline{Y}]$, and for $\nu = 1,\ldots,a$ let, $\underline{\underline{C}}_\nu(x)$ stand for $(\exists \underline{j})[K(o) \wedge (\forall t)B(t) \wedge \underline{j}(x) \equiv \underline{Y}_\nu]$. Then clearly, $\underline{\underline{C}}(x) \equiv \underline{\underline{C}}_1(x) \vee \ldots \vee \underline{\underline{C}}_a(x)$, $\underline{\underline{C}}_\nu(x) \equiv (\exists j)[K(o) \wedge (\forall t)_o^x B(t) \wedge \underline{j}(x) \equiv \underline{Y}_\nu] \wedge (\exists j)[\underline{j}(o) \equiv \underline{Y}_\nu \wedge (\forall t)B(t)]$ hold in W.2.A. Therefore, if $\underline{Y}_1,\ldots,\underline{Y}_b$ $(b \leq a)$ are those states among $\underline{Y}_1,\ldots,\underline{Y}_a$ for which $(\exists \underline{j})[\underline{j}(o) \equiv \underline{Y} \wedge (\forall t)B(t)]$, then $\underline{\underline{C}}(x) \equiv (\exists j).K(o) \wedge (\forall t)_o^x B(t) \wedge [\underline{j}(x) \equiv \underline{Y}_1 \vee \ldots \vee \underline{j}(x) \equiv \underline{Y}_b]$ holds in W.2.A.

Next let k = number of states of $\underline{j}$, and let $\underline{Y}_1,\ldots,\underline{Y}_b,\ldots,\underline{Y}_k$ be the states of $\underline{j}$, and let $r_1,\ldots,r_k$ be defined by the recursion

$$(1)\qquad \begin{aligned} r_\nu(o) &\equiv K[\underline{Y}_\nu] && ,\nu=1,\ldots, k \\ r_\nu(t') &\equiv r_1(t)B[\underline{Y}_1,\underline{Y}_\nu] \vee \ldots \vee r_k(t)B[\underline{Y}_k,\underline{Y}_\nu] && ,\nu=1,\ldots, k \end{aligned}$$

One then easily shows that $(\exists \underline{j})\ [K(o) \wedge (\forall t)_o^x B(t) \wedge [\underline{j}(x) \equiv Y_1 \vee \ldots \vee \underline{j}(x) \equiv \underline{Y}_b]]$ holds if and only if $[r_1(x) \vee \ldots \vee r_b(x)]$. Consequently, $\hat{x}\underline{\underline{C}}(x) = \hat{x}[r_1(x) \vee \ldots \vee r_b(x)]$. Now $\underline{r}$ has 2^k states, therefore a repetition must occur in $\underline{r}(o),\ldots,\underline{r}(2^k)$, say $r(\underline{\ell}) \equiv r(\underline{\ell}+p)$ whereby $\underline{\ell}+p \leq 2^k$ and $0 < p$. By (1) it then follows that $r(\underline{\ell}+t) \equiv r(\underline{\ell}+p+t)$, for all t, so that $\hat{x}[r_1(x) \vee \ldots \vee r_b(x)] = \hat{x}\underline{\underline{C}}(x)$ is ultimately periodic with phase $\underline{\ell}$ and period p.

The second part of Corollary 2 is best shown by first obtaining definitions in W.2.A. of the relations $x=y$, $x<y$, $x \equiv y \pmod p$, for fixed p.

Note also that the selection of $\underline{Y}_1,\ldots,\underline{Y}_b$ from $\underline{Y}_1,\ldots,Y_a$ in the proof of Corollary 2 can be effectively made (by Corollary 1). As a result one can ef-

fectively find the phase and period of the set $\hat{x}\underline{\underline{C}}(x)$.

By using similar methods to those employed in the proof of Corollary 2 one shows that every relation $R(x,y)$ definable in W.2.A. must be of the form $R(x,y) \equiv \bigvee_{\nu=1,\ldots,a} [x \leq y \wedge A_\nu(x) \wedge B_\nu(y-x)] \vee \bigvee_{\nu=1,\ldots,c} [y \leq x \wedge C_\nu(y) \wedge D_\nu(x-y)]$ whereby A_ν, B_ν, C_ν, are ultimately periodic. In particular $y = f(x)$ is definable in W.2.A. if and only if it is ultimately periodic, i.e., satisfies $f(\gamma+x+p) = f(\gamma+x) + q$, for some γ,p,q (compare this with Robinson's [14] result on $[0,x+1,2x,\exists_0 i]$). However, the following result seems more informative.

Corollary 3: If $R(x,y)$ well-orders a subset of natural numbers and is definable by a formula $\underline{\underline{C}}(x,y)$ of W.2.A., then the type α of R is less than ω^2. Conversely, if α is an ordinal less than ω^2 one can find a formula $\underline{\underline{C}}(x,y)$ of W.2.A. such that $\hat{x}\hat{y}\underline{\underline{C}}(x,y)$ is an α-well-ordering of all natural numbers.

Proof: Suppose $R(x,y)$ is a well-ordering of natural numbers of type α, and for $\eta \leq \alpha$ let $A\eta$ be the initial segment relative to R of type η. Then from a definition $\underline{\underline{C}}(x,y)$ of R in W.2.A. one can easily obtain definitions of the sets $A\eta$, for $\eta < \omega^2$; so that by Corollary 2 the sets $A\eta, \eta < \omega^2$ are ultimately periodic. Now it is easy to see that there is no strictly increasing $\omega 2$-sequence of ultimately periodic sets of natural numbers. Consequently if $R(x,y)$ is definable in W.2.A. then its type α must be less than ω^2. To indicate a proof of the second part of Corollary 3, let us consider the case $\alpha = \omega 3 + 2$. Because one can define $x \equiv y \pmod 3$ and $x<y$, and $x=y$ in W.2.A., it is clear that one can also define a relation $R(x,y)$ which well-orders the natural numbers in sequence,

$6,9,12,\ldots\ldots,1,4,7,\ldots\ldots,2,5,8,\ldots\ldots,0,3.$

It seems clear that one could use Theorem 3 also to investigate the nature of sets $\hat{i}\underline{\underline{C}}(i)$ definable in W.2.A. by formulas with free predicate variables. However, a rather concrete characterization of these sets of finite sets is given by Theorems 1 and 2, namely

Corollary 4: The sets of n-tuples of finite sets definable in W.2.A. are exactly the behaviors of special outputs of finite automata with n-ary input.

We will terminate this section with the presentation of a first-order theory which is equivalent to W.2.A. in a very strong sense. For this purpose note that

$$f(i) = \sum_{i(x)} (2^x)$$

defines a one-to-one mapping f from all special predicates (finite sets) of natural numbers onto all natural numbers. $f(i) = y$ simply means that for ℓ = length of i, $i(o)i(1) \ldots i(\ell)$ is the binary expansion of y. This mapping f induces a natural one-to-one correspondence between relations on special predicates and relations on natural numbers, let us say that $R(i_1,\ldots,i_n)$ and $S(x_1,\ldots,x_n)$ are adjoined to each other in case $R(i_1,\ldots,i_n) \equiv S(f(i_1),\ldots, f(i_n))$, for all special $i_1,\ldots,i_n$. Let furthermore "$Pw_2(x)$" stand for "x is a power of 2."

Theorem 4: The first-order theory $[=, +, Pw_2]$ is equivalent to the weak second-order theory $[0, ', \exists_0 i]$ in the sense that a relation $S(x_1,\ldots,x_n)$ on natural numbers is definable in $[=, +, Pw_2]$ if and only if its adjoined relation $R(i_1,\ldots,i_n)$ is definable in $[0, ', \exists_0 i]$. Moreover, from a definition $\underline{\underline{C}}(x_1,\ldots,x_n)$ of S one can effectively obtain a definition $\underline{\underline{D}}(i_1,\ldots,i_n)$ of R,

and conversely.

Proof: Let S(i, j, s) be the adjoined to x+y=z, i.e., "S(i, j, s)" stand for "f(i) + f(j) = f(s)." Then by formalizing the procedure of adding natural numbers in binary expansion one obtains the following definition of S in the weak second-order theory $[0, ', \exists_0 i]$,

$$S(i, j, s) : (\exists r).\tilde{r}(o) \wedge (\forall t)[r(t') \equiv [r(t)i(t) \vee r(t)j(t) \vee i(t)j(t)]] \wedge (\forall t)[s(t) \equiv [r(t) \nabla i(t) \nabla j(t)]]$$

whereby "$X \nabla Y$" stands for "$X\tilde{Y} \vee Y\tilde{X}$." Furthermore, if U(i) is the adjoined to $Pw_2(x)$; then $U(i) : (\exists x)(\forall t)[i(t) \equiv (t=x)]$ is a definition of U in $[o, ', \exists_0 i]$. To prove Theorem 4 in one direction it therefore is sufficient to indicate a translation of formulas $\underline{\underline{C}}$ of $[=, +, Pw_2]$ into formulas $\underline{\underline{C}}^*$ of $[o, ', U, S, \exists_0 i]$ such that $\underline{\underline{C}}^*(i_1,\ldots,i_n)$ and $\underline{\underline{C}}(x_1,\ldots,x_n)$ define adjoined relations. Because every formula $\underline{\underline{C}}$ of $[=, +, Pw_2]$ is easily changed to an equivalent one in which no iteration of + occurs, the following specifications yield the required translation.. 1. $[x_\nu+x_\mu=x_\rho]^*$ is $S(i_\nu,i_\mu,i_\rho)$, 2. $[Pw_2(x_\nu)]^*$ is $U(i_\nu)$, 3. $[\underline{\underline{C}} \wedge \underline{\underline{D}}]^*$ is $\underline{\underline{C}}^* \wedge \underline{\underline{D}}^*$, 4. $[\sim\underline{\underline{C}}]^*$ is $\sim\underline{\underline{C}}^*$, 5. $[(\exists x_\nu)\underline{\underline{C}}]^*$ is $(\exists i_\nu)\underline{\underline{C}}^*$.

To prove Theorem 4 in the other direction we note that $E(x,y) : Pw_2(x) \wedge (\exists uv)[(y = u+x+v) \wedge (u<v) \wedge [v=o \vee 2x \leq v]]$ is a definition in $[=, +, Pw_2]$ of "x is a power of 2, and x occurs in the representation of y as a sum of powers of 2." It therefore is sufficient to indicate a translation of formulas $\underline{\underline{C}}$ of $[o, ', \exists_0 i]$ into formulas $\underline{\underline{C}}^o$ of $[=, +, Pw_2, E]$ such that $\underline{\underline{C}}^o)x_1,\ldots,x_n)$ and $\underline{\underline{C}}(i_1,\ldots,i_n)$ define adjoined relations. If one notes that i(x) means the same as E(x,f(i)), and that every formula $\underline{\underline{C}}(i_1,\ldots,i_n)$ can be changed to an equivalent one in which o does not occur and ' only occurs in parts

of form $(\forall t)[j(t) \equiv i(t')]$, then it is clear that the following specifications yield such a translation. We single out the individual variable t and divide the remaining ones in $x_1,x_2,\ldots;y_1,y_2,\ldots$. In [o, ' , $\exists_o$i] we make use of $Y_1,Y_2,\ldots$, and t only (while it is intended that in [=, + , Pw_2, E] the range of the y's is restricted to Pw_2). 1. $[i_\nu(y_\mu)]^o$ is $E(y_\mu,x_\nu)$, 2. $[(\forall t)[i_\mu(t) \equiv i_\nu(t')]^o$ is $[x_\nu = x_\mu + x_\mu \vee x_\nu = x_\mu + x_\mu + 1]$, 3. $[\underline{\underline{C}} \wedge \underline{\underline{D}}]^o$ is $\underline{\underline{C}}^o \wedge \underline{\underline{D}}^o$, 4. $[\sim \underline{\underline{C}}]^o$ is $\sim \underline{\underline{C}}^o$, 5. $[(\exists i_\nu)\ \underline{\underline{C}}]^o$ is $(\exists x_\nu)\ \underline{\underline{C}}^o$, 6. $[(\exists y_\nu)\ \underline{\underline{C}}]^o$ is $(\exists y_\nu)[Pw_2(y_\nu) \wedge \underline{\underline{C}}^o]$.

By Theorem 4, Corollary 1, Corollary 4 one clearly obtains,

Corollary 5: The first-order theory [= , + , Pw_2] is decidable. A relation $R(x_1,\ldots,x_n)$ is definable in this theory if and only if its adjoined $S(i_1,\ldots,i_n)$ is the behavior of a finite automaton with special output.

One might attempt to prove Corollary 5 directly by extending Presburger's [10] method for [=, +]. Corollary 1 would then follow by Theorem 4.

Let $Q_2(x)$ stand for "x is a square." Then by Putnam [11], the first-order theory [=, + , Q_2] is undecidable. It is interesting to compare this with Corollary 5, and one easily extends the results as follows,

Theorem 5: The first-order theory [=, + , P] is

(a) undecidable in case P(x) is ultimately a hyper-arithmetic-progression, i.e., in case P ultimately consists of the values of a polynomial of degree ≥ 2.

(b) decidable in case P(x) is ultimately a geometric progression.

To better understand the jump in strength from [=, +] to [=, + , .] it would be interesting to know whether there is a recursive predicate P(x) such that [=, + , P] is undecidable without admitting definitions for all recursive predicates.

6. OTHER CONCEPTS OF FINITE AUTOMATA

Clearly our concept of finite automata is very closely related to that of Church [3]. What we have callled the transition-recursion and output-recursion of an automaton (with output) are restricted recursions in his sense. While Church allows instantaneous action (the input at time t directly affects the transit and output at the same time t), it is just a matter of convenience that we have presented our theory in terms of automata with delayed action only; also our restriction to special outputs is inessential (see Section 7). The behavior-concept used implicitly by Church is that of the operator $u = \psi(\underline{i})$ defined by the output-recursion. We hope to show elsewhere how his synthesis procedure (Case II) can be extended to condition-formulas containing predicate-quantifiers.

Recursions like our output-recursions were first used by Burks and Wright [2]. Their concept of well-formed logical net is equivalent to our finite automata, except that instantaneous action occurs in logical nets.

In the following discussion it is intended that a $\underline{n}/\underline{m}$-automaton (whose input has n binary components) represents in coded form a $2^n/2^m$-automaton (whose input has one 2^n-ary component. Let $\Sigma_2 = \{\wedge, \vee\}$, $\Sigma_{\underline{n}} = \Sigma_2 \times \ldots \times \Sigma_2$ (n factors). Under the conventional interpretation of propositional formulas $\underline{E}^m$ denote an element $\sigma \in \Sigma_{\underline{m}}$, while $\underline{H}^m[\underline{Y}^m, \underline{X}^n]$ may be interpreted to denote a function τ: $\Sigma_{\underline{m}} \times \Sigma_{\underline{n}} \rightarrow \Sigma_{\underline{m}}$. Thus, with an $\underline{n}/\underline{m}$-automaton $\underline{E}^m$ $\underline{H}^m[\underline{Y}^m, \underline{X}^n]$ is associated a system $< \Sigma_n, \Sigma_m, \sigma, \tau >$ called its transition system. The elements of $\Sigma_{\underline{n}}$ and $\Sigma_{\underline{m}}$ are respectively called input states and transit-states, σ is the initial-state and τ the transit-function of the automaton. An output $U[\underline{Y}^m]$ may be interpreted to denote a subset of transit-states. These re-

marks are intended to indicate how our notion of finite automata (with output) is related to those used by Moore [9], Myhill [8], Rabin and Scott [13], and others. While our notion is syntactic these authors take automata to be what we called transition systems (with output set). The latter definition is not correct if the mathematical concept "finite automaton" is to correspond to physical structures. Two physical systems (two syntactic systems) can be quite different structurally (syntactically) and still display the same transition-system. Also from a purely mathematical point of view it is not advisable to identify automata with their transition-structure, as it then becomes impossible to rigorously state existence of algorithms as, for example, in our Theorems 1 and 2. The point is that an algorithm is better thought of as applying to and yielding syntactic entities.

We will now indicate how our theory of behavior can be extended to automata with many inputs, each of which may have any number of binary components. For this purpose it is convenient to extend propositional calculus so as to contain ω lists, each list consisting of ω propositional variables. A notation like "$H[\underline{X}^n; \underline{Y}^k; \underline{Z}^h]$" will be used to stand for a formula of (extended) propositional calculus in which the variables $\underline{X}$, $\underline{Y}$, $\underline{Z}$ and only these may occur, and furthermore the variables $\underline{X}$ belong to a first list, which precedes a second list to which the variables $\underline{Y}$ belong, which precedes a third list to which the variables $\underline{Z}$ belong.

Definition 1'. A (finite) $\underline{n_1};\ldots;\underline{n_k}/\underline{m}$-automaton with inputs $\underline{X}^{n_1},\ldots,\underline{X}_k^{n_k}$ and transit $\underline{Y}^m$ is a 2m-tuple $\underline{E}^m \frown \underline{H}^m[\underline{Y}^m; \underline{X}_1^{n_1};\ldots;\underline{X}_k^{n_k}]$ of propositional formulas (no variables occur in $\underline{E}^m$).

A (binary) output of such an automaton is a propositional formula $U[\underline{Y}^m]$, where $\underline{Y}^m$ is the transit of the automaton.

It is clear how one extends the notion of transition (output)-recursion, introduced in Section 3, to $\underline{n}_1;\ldots;\underline{n}_k/\underline{m}$-automata (with output). Also for the extension of the concept of special output we refer to Definition 2 in Section 3.

Definition 3'. The behavior $\beta(\underline{E}^m, \underline{H}^m, U)$ of a $\underline{n}_1;\ldots;\underline{n}_k/\underline{m}$-automaton with special output is the k-ary relation which holds for the special $\underline{n}_1$-predicate $\underline{i}_1$,...,$\underline{n}_k$-predicate $\underline{i}_k$, just in case $(\exists x)\ (\forall t)_x^\infty\ U[\underline{r}(t)]$, whereby $\underline{r}^m = \underline{\zeta}(\underline{E}, \underline{H}, \underline{i}_1;\ldots;\underline{i}_k)$ is obtained by the transition-recursion of $\underline{E}\frown\underline{H}$.

To obtain an extension of the analysis and synthesis Theorems 1 and 2, we extend W.2.A. to contain ω lists, each list containing ω predicate variables. A notation like "C(i;j)" will be used to denote a formula of (extended) W.2.A. in which the variables $\underline{i}$, $\underline{j}$ and only these may have free occurrences, and such that the variables $\underline{i}$ all belong to the same list which precedes a list containing all the variables $\underline{j}$. A formula $\underline{\underline{C}}(\underline{i}_1^{n_1}; \underline{i}_2^{n_2}; \underline{i}_3^{n_3})$ of W.2.A. defines a ternary relation $\hat{\underline{i}}_1, \hat{\underline{i}}_2, \hat{\underline{i}}_3\ \underline{\underline{C}}(i_1; \underline{i}_2; \underline{i}_3)$ on special $\underline{n}_1$-predicates, $\underline{n}_2$-predicates, $\underline{n}_3$-predicates.

Theorem 1'. (synthesis) To every formula $\underline{\underline{C}}(\underline{i}_1^{n_1};\ldots;\underline{i}_k^{n_k})$ of (extended) W.2.A. one can construct a $\underline{n}_1;\ldots;\underline{n}_k/\underline{m}$-automaton $\underline{E}^m\frown\underline{H}^m$ with special output U such that the behavior $\beta(\underline{E}, \underline{H}, U)$ is the k-ary relation $\hat{\underline{i}}_1;\ldots;\hat{\underline{i}}_k\ \underline{\underline{C}}(\underline{i}_1;\ldots;\underline{i}_k)$.

Theorem 2'. (analysis) To every $\underline{n}_1;\ldots;\underline{n}_k/\underline{m}$-automaton $\underline{E}^m\frown\underline{H}^m$ with special output U one can construct a formula $\underline{\underline{C}}(\underline{i}_1^{n_1};\ldots;\underline{i}_k^{n_k})$ of W.2.A. such that the k-ary relation $\hat{\underline{i}}_1\ldots\hat{\underline{i}}_k\ \underline{\underline{C}}(\underline{i}_1;\ldots;\underline{i}_k)$ is the behavior $\beta(\underline{E}, \underline{H}, U)$.

To prove Theorem 1' one at first simply disregards the grouping of the $q = n_1, n_2 \cdot \ldots \cdot n_k$ variables in the formula $\underline{C}(\underline{i}^{n_1}; \ldots; \underline{i}^{n_k})$ and constructs the $q/\underline{m}$-automaton with special output according to Theorem 1. By properly grouping the q components of the input of this automaton one obtains a $\underline{n}_1;\ldots;\underline{n}_k/\underline{m}$-automaton with special output as required in Theorem 1'. Similarly one proves Theorem 2'.

It thus appears that the theory of behavior for automata with many inputs does not present any additional difficulties, in case one works with special predicates rather than finite strings of input states. The reason for this is that a k-tuple $(\underline{i}_1^{n_1};\ldots;\underline{i}_k^{n_k})$ of special $\underline{n}$-predicates may be reinterpreted as one special $n_1,n_2\ldots n_k$-predicate. In contrast a k-tuple $(\underline{\underline{x}}_1;\ldots;\underline{\underline{x}}_k)$ of finite strings of input states can not readily be reinterpreted as one finite string of states. This seems to be the reason that no theory of behavior of automata with many inputs occurs in the literature.

Our concept of finite $\underline{n}_1;\ldots;\underline{n}_k/\underline{m}$-automaton still is somewhat specialized in that the components of each input and the transit are binary (i.e., can take values in $\Sigma_2 = \{ \wedge, \vee \}$ only). Because we allow many components to occur in an input (transit) there is of course the possibility of indirectly dealing with automata whose sets of input states (transit states) have any finite cardinality, by way of binary coding. However, to obtain an entirely satisfactory theory of $n_1;\ldots;n_k/m$-automata (for any numbers $n_1,\ldots,n_k$, m one would have to replace Σ_2 by $\Sigma_2,\Sigma_3,\ldots$ (Σ_k being a set of k elements), and one would have to set up a calculus PC_ω to replace propositional-calculus (PC_2), such that PC_ω contains variables X_k ranging over Σ_k and provides names $H_k[X_{k_1},\ldots,X_{k_a}]$

for all functions τ: $\Sigma_{n_1} \times \ldots \times \Sigma_{k_a} \rightarrow \Sigma_{k_a}$. To generalize the results obtained in Section 4 one would extend W.2.A. to contain variables i_k ranging over monadic functions from natural numbers to Σ_k which ultimately take the fixed value $\Lambda_k \in \Sigma_k$. It seems clear that this program could be carried out, and moreover the form of the presentation in Section 4 would remain essentially unchanged. We did not present our results in this general version because no calculus PC_ω is available in the literature.

7. FINITE STRINGS VERSUS SPECIAL PREDICATES; REGULAR RELATIONS

According to our definition the behavior β of an $\underline{n}/\underline{m}$-automaton with special output is a set of special $\underline{n}$-predicates (infinite strings of input-states which are ultimately $\underline{\Lambda}^n$). Simplifying Kleene's [6] theory of regularity, Myhill [8], Rabin and Scott [13], and Copi, Elgot and Wright [4] work instead with the set β_{sg} consisting of all finite strings of input states which turn on the output. In this approach the restriction to special outputs is not needed, so that it may seem at first that our concept of behavior is too specialized. However we will see in this section that on the contrary our theory of behavior is more general in that it yields a rather natural extension of the concept of regular set of finite strings to regular relation on finite strings.

We begin by observing that there is a one-to-one mapping f of all finite strings of elements of $\Sigma_{\underline{n}}$ onto all special $\underline{n}$-predicates $\underline{i}^n$ which have the property $\underline{i}(\ell) \equiv \underline{\nabla}^n$, if ℓ is the length of $\underline{i}$. Namely,

$$\underline{i} = f(\underline{Y}_o \frown \ldots \frown \underline{Y}_h) \;.\equiv.\; (\forall t)_{t<h}[\underline{i}(t) \equiv \underline{Y}_t] \wedge [\underline{i}(h') \equiv \underline{\nabla}] \wedge (\forall t)_{t>h'}[\underline{i}(t) \equiv \underline{\Lambda}].$$

In particular the empty string corresponds to the predicate $\underline{i}(o) \equiv \underline{\vee}$, $\underline{i}(t') \equiv \underline{\wedge}$. To simplify the presentation we will identify finite strings with the corresponding $\underline{n}$-predicate, i.e.,

(**) A finite $\underline{n}$-string of length γ is a special $\underline{n}$-predicate $\underline{i}^n$ of length $\gamma+1$ which takes the value $\underline{i}(\gamma') \equiv \underline{\vee}^n$.

The definition of finite string behavior which occurs in the literature can, in our notation, be formulated thus,

Definition 6. The sg-behavior of a $\underline{n}/\underline{m}$-automaton $\underline{E}\,\widehat{}\,\underline{H}$ with arbitrary output U is the set $\beta_{sg}(\underline{I}, \underline{H}, U)$ consisting of all $\underline{n}$-strings $\underline{i}$ such that $U[\underline{r}(\gamma+1)]$, if γ is the length of the string $\underline{i}$ and $\underline{r} = \zeta(\underline{I}, \underline{H}, \underline{i})$ is the $\underline{m}$-predicate determined by the transition-recursion of $\underline{E}\,\widehat{}\,\underline{H}$.

Theorem 6. A set β of $\underline{n}$-strings is the sg-behavior $\beta_{sg}(\underline{E}, \underline{H}, U)$ of some $\underline{n}/\underline{m}$-automaton with arbitrary output if and only if it is the behavior $\beta(\underline{I}, \underline{G}, W)$ of some $\underline{n}/q$-automaton with special output.

Proof. Suppose first that $\beta = \beta_{sg}(\underline{E}, \underline{H}, U)$, whereby U is an arbitrary output of the $\underline{n}/\underline{m}$-automaton $\underline{E}\,\widehat{}\,\underline{H}$. Let the $\underline{n}/\underline{m}\,\widehat{}\,2$-automaton $\underline{I}\,\widehat{}\,\underline{G}$ and its output W be defined by,

$$I_\nu \;::\; E_\nu \qquad G_\nu[\underline{Y}^m\,\widehat{}\,Z;\ \underline{X}^n] \;:\; H_\nu[\underline{Y}, \underline{X}] \qquad ,\nu = 1,\ldots,m$$

$$I_{m+1} \;:\; \underline{\wedge} \qquad G_{m+1}[\underline{Y}^m\,\widehat{}\,Z;\ \underline{X}\ ] \;:\; [\underline{X} \equiv \underline{\vee}]\ U[\underline{Y}] \vee [\underline{X} \equiv \underline{\wedge}]Z$$

$$W[\underline{Y}^m\,\widehat{}\,Z] \;:\; Z$$

Then clearly $G_{m+1}\ [\underline{Y}\,\widehat{}\,Z';\underline{\wedge}] \equiv Z$, and therefore $W[\underline{G}[\underline{Y}\,\widehat{}\,Z;\underline{\wedge}]] \equiv W[\underline{Y}\,\widehat{}\,Z]$, which by definition Z means that W is special output of $\underline{I}\,\widehat{}\,\underline{G}$. Furthermore note that the transition-recursions of the two automata are,

(1) $\underline{r}(o) \equiv \underline{E}$

$\underline{r}(t') \equiv \underline{H}[\underline{r}(t),\underline{i}(t)]$

(2) $\underline{r}(o) \equiv \underline{E}, \quad s(o) \equiv \underline{\wedge}$

$\underline{r}(t') \equiv \underline{H}[\underline{r}(t),\underline{i}(t)]$

$\underline{r}(t') \equiv [\underline{i}(t) \equiv \underline{\vee}]\, U[\underline{r}(t)] \vee [\underline{i}(t) \equiv \underline{\wedge}]s(t)$

Now let $\underline{i}$ be any special predicate of length γ. If $\underline{i} \epsilon \beta(\underline{I}, \underline{G}, W)$ then by (*) of Section 3 and (2), $W[r(\gamma+1)^{\frown} s(\gamma+1)]$, i.e., $s(\gamma+1)$. Therefore by (2), $[\underline{i}(\gamma) \equiv \underline{\vee}]\, U[\underline{r}(\gamma)] \vee [i(\gamma) \equiv \underline{\wedge}]s(\gamma)$. Because γ is the length of $\underline{i}$, $\underline{i}(\gamma) \equiv \underline{\wedge}$ is not the case, so that $[\underline{i}(\gamma) \equiv \underline{\vee}]U[\underline{r}(\gamma)]$. Consequently by definition 6, $\underline{i} \epsilon \beta_{sg}(\underline{E}, \underline{H}, U)$. These steps are reversible, so that also $\underline{i} \epsilon \beta_{sg}(\underline{E}, \underline{H}, U)$ implies $\underline{i} \epsilon \beta(I, \underline{G}, W)$. Thus we have constructed an automaton $\underline{I}^{\frown} \underline{G}$ with special output W such that also $\beta(\underline{I}, \underline{G}, W) = \beta$. This proves Theorem 6 in one direction.

Suppose next that $\beta = \beta(\underline{I}, \underline{H}, W)$, whereby $\underline{I}^{\frown} \underline{H}$ is an $\underline{n}/\underline{m}$-automaton with special output. Define $U[\underline{Y}^m] \; : \; W[\underline{H}[\underline{Y}^m, \underline{\vee}^n]]$. Noting that β consists of finite $\underline{n}$-strings only, and using Definition 6 and (*) of Section 3, one easily shows that $\beta_{sg}(\underline{I}, \underline{H}, U) = \beta(\underline{I}, \underline{H}, W) = \beta$. This establishes Theorem 6 in the other direction.

Theorem 6 shows that the restriction to special outputs in our analysis and synthesis Theorems 1 and 2 (Section 4) is not a limitation in generality, but rather a natural feature which appears when one works with special predicates instead of finite strings. In fact it now is easy to obtain synthesis and analysis theorems in terms of sg-behavior and without restriction on the outputs. For this purpose we remark that the set of all finite $\underline{n}$-strings can be defined by a formula $S_{g_n}(\underline{i}^n)$ of W.2.A.,

$S_{g_n}(\underline{i}^n) \; : \; (\exists j).j(o) \wedge (\forall t)[j(t') \supset j(t)][j(t)\tilde{j}(t') \supset \underline{i}(t) \equiv \underline{\vee}] \; [\tilde{j}(t) \supset \underline{i}(t) \equiv \underline{\wedge}]$

and we define a formula $\underline{\underline{C}}(\underline{i}^n)$ to be an <u>sg-formula</u> in case $(\forall \underline{i})\; \underline{\underline{C}}(\underline{i}) \supset S_{g_n}(\underline{i})$

holds in W.2.A. (by Corollary 1 one can effectively decide whether a formula of W.2.A. is a sg-formula).

Theorem 7. Analysis: To every $\underline{n}/\underline{m}$-automaton $\underline{E}^{\frown}\underline{H}$ with arbitrary output U one can construct a sg-formula $\underline{\underline{C}}(\underline{i}^n)$ of W.2.A. such that $\underline{\underline{C}}(\underline{i})$ defines the sg-behavior $\beta_{sg}(\underline{E}, \underline{H}, U)$.

Synthesis: To every sg-formula $\underline{\underline{C}}(\underline{i}^n)$ of W.2.A. one can construct a $\underline{n}/\underline{m}$-automaton $\underline{E}^{\frown}\underline{H}$ with output U such that $\beta_{sg}(\underline{E}, \underline{H}, U) = \hat{\underline{i}}\underline{\underline{C}}(\underline{i})$.

Proof: By Theorems 1, 2, and 6. Note that we actually established an effective version of Theorem 6.

In short form Theorem 7 states that the sg-behaviors of $\underline{n}/\underline{m}$-automata with arbitrary (binary) output are exactly the sets of finite $\underline{n}$-strings definable (by sg-formulas) in W.2.A. It has been shown that the sg-behaviors are the regular sets of finite strings (references at the beginning of this section). Thus,

Theorem 8. For any set β of finite $\underline{n}$-strings the following are equivalent conditions,

(1) β is the sg-behavior of an $\underline{n}/\underline{m}$-automaton with arbitrary output.

(2) β is the behavior of an $\underline{n}/\underline{m}$-automaton with special output.

(3) β is definable in W.2.A. (by a sg-formula).

(4) β is regular

In the literature sg-behavior has been studied only for automata with one input. Consequently the concept of regularity has been limited to sets. On the other hand we have seen in Section 6 that our theory of behavior can easily

be extended to automata with many inputs. On the basis of Theorems 1', 2' (Section 6) and Theorem 8 the following definition suggests itself as a natural extension of the concept of regularity.

A formula $\underline{\underline{C}}(\underline{i}_1^{n_1};.....;\underline{i}_k^{n_k})$ of (extended) W.2.A is called an sg-formula if $(\forall \underline{i}_1....\underline{i}_k).\underline{\underline{C}}(\underline{i}_1;.....;\underline{i}_k) \supset Sg_{n_1}(\underline{i}_1).....Sg_{n_k}(\underline{i}_k)$ holds in W.2.A.

Definition 7. A relation $R(\underline{i}_1^{n_1};.....;\underline{i}_k^{n_k})$ on special $\underline{n}_\nu$-predicates (finite $\underline{n}_\nu$-strings) is regular if it is definable by a formula (sg-formula) $\underline{\underline{C}}(\underline{i}_1;....;\underline{i}_k)$ of extended W.2.A.

Theorems 1' and 2' can now be restated in the following short form,

Theorem 8'. A relation $R(\underline{i}_1^{n_1};.....;\underline{i}_k^{n_k})$ on special n_ν-predicates (finite n_ν-strings) is the behavior $\beta(\underline{E}, \underline{H}, U)$ of a $\underline{n}_1;.....;\underline{n}_k/\underline{m}$-automaton with special output, if and only if R is regular.

In case one prefers to work with finite strings one could extend Definition 6 to a definition of sg-behavior of many-input-automata with arbitrary output, so as to obtain a corresponding extension of Theorem 6, and Theorem 7.

A binary relation on strings which naturally arises in connection with a $\underline{n}/\underline{m}$-automaton $\underline{E}^{\underline{m}}\frown\underline{H}^{\underline{m}}$ is its equi-response relation $\underline{i}^{\underline{n}} \backsim \underline{j}^{\underline{n}}$ (mod $\underline{E}\frown\underline{H}$). Two finite strings $\underline{i}$, $\underline{j}$ of input-states are in this relation if they produce the same transit-state, i.e., if $\underline{r}(\gamma') \equiv \underline{s}(h')$ in case $\underline{r} = \zeta(\underline{E}, \underline{H}, \underline{i})$, $\underline{s} = \zeta(\underline{E}, \underline{H}, \underline{j})$, γ = length of string $\underline{i}$, and h = lengths of string $\underline{j}$. It is easy to construct a $\underline{n};\underline{n}/q$-automaton with special output whose behavior is the relation $\underline{i}^{\underline{n}} \backsim \underline{j}^{\underline{n}}$ (mod $\underline{E}\frown\underline{H}$). Therefore, by Theorem 8', the equi-response relation of any $\underline{n}/\underline{m}$-automaton is a regular relation on finite $\underline{n}$-strings. In k-ary number theory

(i.e., the theory of finite strings on the alphabet $1_1,\ldots.1_k$) the equi-response relations module k/q-automata take the place of conventional congruence relations in ordinary (1-ary) number theory. Correspondingly the concept of regularity is the natural analogue in k-ary number theory to ultimate periodicity in ordinary number theory.

Another example of a regular relation on special predicates is the adjoined S(i,j,s) under binary expansion (see Section 5) to the relation x+y=z. Moreover Theorem 4 may be restated as follows. A relation $R(x_1,\ldots x_k)$ is definable in the first-order theory [=, + , Pw_2] if and only if it is the adjoined under binary expansion to a regular relation $S(i_1,\ldots,i_k)$ on special predicates.

In case one prefers to deal with finite strings the following modified concept of binary expansion is appropriate. If $a_o,\ldots,a_h$ are either 1 or 2 then $a_oa_1\ldots\ldots a_h$ represents $a_o2^o + a_12^1 + \ldots\ldots + a_h2^h$. In particular the empty string represents the number 0. It is easy to see that this yields a one-to-one mapping x = g(i) from all finite 2-strings to all natural numbers. Furthermore one can modify the proof of Theorem 4 to obtain; a relation $R(x_1,\ldots,x_n)$ is definable in [=, + , Pw_2] if and only if its adjoined $S(i_1,\ldots,i_n)$ under modified binary expansion is a regular relation on finite 2-strings.

Consequently the following two conditions on a relation $R(x_1,\ldots,x_n)$ on natural numbers are equivalent.

(1) The adjoined $S(i_1,\ldots,i_k)$ of $R(x_1,\ldots,x_k)$ under binary expansion is a regular relation on special predicates

(2) The adjoined $S_{sg}(i_1,\ldots,i_k)$ of $R(x_1,\ldots,x_k)$ under modified binary expansion is a regular relation on finite 2-strings

Let us call such a relation R a 2-regular relation on natural numbers so that,

Theorem 9. The relations definable in the first-order theory [=, + , Pw_2] are exactly the 2-regular relations on natural numbers.

For appropriate definition of k-regular relation (via adjoined under (modified) k-ary expansion) Theorem 9 holds if "2-regular" and "Pw_2" are replaced by "k-regular" and "Pw_k" ($Pw_k(x)$ means x is a power of k). It thus appears that the first-order theory [=, + , Pw_k] is suitable for a study of regularity on the alphabet $l_1,\ldots,l_k$ consisting of k letters. In this connection the following remarks are of interest.

1. Let N_k denote the set of all finite strings on the alphabet $l_1,\ldots,l_k$, and let the function $g_k: N_k \to N_1$ (N_1 = set of natural numbers) be defined by

$$g_k(o) = o$$

$$g_k(l_{\nu_o} l_{\nu_1} \cdots l_{\nu_h}) = \nu_o k^o + \nu_1 k^1 + \cdots + \nu_h k^h.$$

I.e., g_k is that one-to-one ennumeration of N_k in which every string of length h precedes every string of length $\ell > h$, while strings of equal length are enumerated in lexicographic order reading from right to left. The inverse g_k^{-1} yields the modified k-ary expansion of natural numbers. Let $+^k$ denote the adjoined to +, i.e.,

$$\underline{\underline{x}} +^k \underline{\underline{y}} = g_k^{-1}(g_k(\underline{\underline{x}}) + g_k(\underline{\underline{y}})), \text{ for } \underline{\underline{x}}, \underline{\underline{y}} \in N_k,$$

and let Pw^k denote the adjoined to Pw_k, i.e.,

$$Pw^k(\underline{\underline{x}}) \equiv Pw_k(g_k(\underline{\underline{x}})), \text{ for } \underline{\underline{x}} \in N_k.$$

We remark that it is easy to set up an algorithm for calculating $\underline{\underline{x}} +^k \underline{\underline{y}}$ (similar to the conventional algorithm for addition in ordinary expansion), and that

$Pw^k(\underline{\underline{x}})$ simply means that $\underline{\underline{x}}$ is 1_1 or $\underline{\underline{x}}$ is 1_k followed by zero or more occurrences of 1_{k-1}. Clearly $< N_1, +, Pw_k >$ is isomorphic to $< N_k, +^k, Pw^k >$, so that $[=, +, Pw_k]$ may be interpreted as first-order theory of either of these systems. Theorem 9 as well as the following remarks ought to be interpreted accordingly, and we will often speak of a relation when we actually mean it's adjoined under g.

2. Let $x <_k y$ and $x >_k y$ denote respectively the initial segment relation and terminal segment relation on N_k (or their adjoined). It is easy to construct a k;k|m-automaton with special output whose behavior is the relation $x <_k y$, so that by Theorem 9 (2 replaced by k), this relation is definable in $[=, +, Pw_k]$. Thus, by Theorem 4,

The first-order theory of $< N_k, <_k >$ is decidable.

In contrast we will show elsewhere that the first-order theory of $< N_k, <_k, >_k >$ is not decidable. Therefore, $x >_k y$ is not definable in $[=, +, Pw_k]$.

3. Let $x \frown^k y$ denote the operation of concatenation on N_k (or its adjoined on N). It is easy to see that

$$x \frown^k y = x + k^{lg_k(x)} \cdot y$$

whereby $lg_k(x)$ is the length of the string x, i.e.,

$$lg_k(x) = a \quad .\equiv. \quad k^a \leq x + 1 < k^{a+1}$$

However, there is no definition of $x \frown^k y$ in $[=, +, Pw_k]$, because this theory is decidable while it was shown by Quine [12] that $[=, \frown^k]$ is undecidable. It can be shown that $[=, \frown^k]$ and $[=, +, \cdot]$ are equivalent in the sense that the primitives of one of these theories are definable in the other.

4. We have shown (see also Rabin and Scott [13]) that the relations $x \sim y$ which are equiresponse relations modulo automata with one k-ary input are exactly those right-congruence relations of the operation $x^{\frown k}y$ which divide N_k into finitely many classes. This emphasizes the analogy (remark following Theorem 8') of these relations to ordinary congruence relations of $x + y \neq y^{\frown 1}y$. We remark that while $x^{\frown k}y$ is not definable in $[=, +, Pw_k]$, the equiresponse relations are definable.

5. The study of congruences is fundamental in elementary number theory. It would be of great importance for a better understanding of regularity (behavior of finite automata) to develop analogously a theory of those (right, left) congruence relations of $x^{\frown k}y$ whose partition is finite.

6. Every ultimately periodic set of natural numbers is definable in $[=, +]$. By Theorem 9 (extension to k) it follows,

> Every ultimately periodic (i.e., 1-regular) set of natural numbers is k-regular, for every k.

7. Let $A_{n,k}(x)$ stand for $lg_k(x) \equiv 0 \pmod{n}$. It then is easy to see that $A_{n,k}(x)$ is k-regular, and therefore definable in $[=, +, Pw_k]$. Because $Pw_{kn}(x) .\equiv. [Pw_k(x) \wedge A_{n,k}(x)] \vee [x = 1]$ it follows that Pw_{kn} is definable in $[=, +, Pw_k]$. Conversely, for $n \geq 2$, Pw_k is definable in $[=, +, Pw_{kn}]$, because $Pw_k(x) .\equiv. Pw_{kn}(x) \vee Pw_{kn}(kx) \vee \ldots \vee Pw_{kn}(k^{n-1}x)$. Thus, for any k and $n \neq 0$ the theories $[=, +, Pw_k]$ and $[=, +, Pw_{kn}]$ are equivalent with respect to definability. By theorem 9 (2 replaced by k) it follows,

For any k and $n \neq 0$, the k^n-regular relations on natural numbers are exactly the k-regular relations.

8. Suppose that $n \geq k$ and Pw_n is k-regular. Let A(x) stand for $(\exists t)[k^x \leq n^t + 1 < k^{x+1}]$. Then A is the set of lengths of elements of N_k which belong to the k-adjoined to Pw_n. Therefore, because Pw_n is k-regular it follows that A must be ultimately periodic. Let h = phase, p = period of A, and let q be the number of elements of A occurring in an interval (x, x+p-1), where $x > h$. Take $a > h$ such that A(a). Then also A(a+p), A(a+2p), ..., A(a+νp), ..., i.e., there are b, b_1, b_2, ... such that

$$(1)\qquad \begin{aligned} k^a &\leq n^b+1 < k^a+1 \\ k^{a+\nu p} &\leq n^b+1 < k^{a+\nu p+1} \qquad , \quad \nu = 1, 2, 3, \ldots \end{aligned}$$

Note that there are exactly $q \leq p$ members a, a_2, ..., a_q of A occurring in the interval (a, a+p-1), and that, because $n \geq k$, no $n^{t_1} \neq n^{t_2}$ can have the same length x ($n^{t_1} + 1$ and $n^{t_2} + 1$ cannot belong to the same interval (k^x, $k^{x+1}-1$)). It follows that a, a_2, ..., a_q, a+p are in order the lengths of n^b, n^{b+1}, ..., n^{b+q-1}, $n^{b+q} = n^{b_1}$. Therefore $b_1 = b+q$, and similarly one shows $b_\nu = b+\nu q$, $\nu = 1, 2, 3, \ldots$. It follows by (1) that

$$(k^{a+\nu p}-1) \mid k^{a+1} \quad < \quad n^{\nu q} \quad < \quad k^{a+\nu p+1} \mid (k^a-1) \qquad , \quad \nu = 1, 2, 3, \ldots$$

Therefore,

$$\sqrt[\nu]{(k^{\nu p}-k^{-a})} \cdot \sqrt[\nu]{k^{-1}} < n^q < \sqrt[\nu]{k^{a+1} \mid (k^a-1)} \cdot k^p \qquad , \nu = 1, 2, 3, \ldots$$

Letting ν approach infinity this clearly yields $n^q = k^p$.

Thus we have shown that for $n \leq k$, if Pw_n is k-regular then $n^q = k^p$ for some $p \neq 0$ and $q \neq 0$. This assertion extends to all $n \geq 2$; because if $n \geq 2$ there is an a such that $n^a \geq k$, and by 7 if Pw_n is k-regular then also $Pw_n a$ is k-

regular, so that there are $p \neq 0$ and $q \neq 0$ such that $n^{aq} = k^p$. Consequently, if one defines

(a) $x \approx y$: $(\exists uv)[u \neq 0 \wedge v \neq 0 \wedge x^u = y^v]$ one obtains by 7,

(b) If $n \geq 2$ then Pw_n is k-regular (definable in $[=, +, Pw_k]$) if and only if $n \approx k$.

(c) The k-regular relations are exactly the n-regular relations if and only if $n \approx k$.

(d) If $n \geq 2$ and Pw_n is k-regular (definable in $[=, +, Pw_k]$) then also Pw_k is n-regular (definable in $[=, +, Pw_n]$), and k-regularity and n-regularity have the same meaning.

These facts can, of course, be stated in terms of sequences. For example, the one-to-one mapping $g_n^{-1} g_k$ of N_k takes regular relations on N_k onto regular relations on N_n just in case $n \approx k$.

To better understand the equivalence relation $\approx$, let us say that a number x is <u>simple</u> if $[x = 0 \vee x = 1 \vee \sim (\exists uv)(v \neq 1 \wedge x = u^v)]$, and let spl(y) stand for that simple number x of which y is a power. Then by elementary number theoretic considerations (prime-decomposition) one shows,

(e) $x \approx u \ .\equiv. \ spl(x) = spl(y)$

Furthermore, the simple numbers constitute a system of representatives for $\approx$, and the equivalence class of a simple number x is $\{x^n | n \neq 0\}$.

Because of (b), (c), (d) it follows that it is sufficient to deal with k-regularity for simple k. The theory $[=, +, Pw_n]$ is equivalent to $[=, +, Pw_k]$, for $k = spl(n)$. (Note that a number k is simple just in case g.c.d.$(a_1, \ldots, a_n) = 1$ if $k = p_1^{a_1} \ldots p_n^{a_n}$ is the prime-decomposition of k.)

By (b) it follows that Pw_2 is not 3-regular. This seems to mean that there is no finite automation with binary input and ternary output which translates binary expansions of numbers into the corresponding ternary expansions.

8. REMARKS ON FEEDBACK

The essentially new element added to pure switching circuits to obtain sequential circuits is feedback. The presence of feedback in our finite automata is reflected in the recursiveness of the definition of the input to transit operation $\underline{r} = \psi(\underline{i})$ of a finite automaton. In contrast, for a pure switching circuit this operation is introduced by explicit definition. The relationship of feedback to recursions was first clearly realized by Burks and Wright [2] and Kleene [6], and is emphasized by Church's contribution to automata theory [3].

A formalism, sufficiently rich to provide notations for all behaviors of finite automata, must contain an operator corresponding to feedback. In Kleene's [6] formalism of regular expressions, this operation is $*$. Copi, Elgot, and Wright [4] and Myhill [8], in their modified version of Kleene's theory use a related monadic operator *. In W.2.A. = [o, ', $\exists_o i$] it is the finite-set-quantifier $\exists_o i$ which corresponds to feedback. This is best shown by indicating how the primitive operators $\cup$, $\cdot$, and * on regular sets can be obtained in W.2.A.

For this purpose to every Sg_n-formula $\underline{\underline{C}}(\underline{i})$ of W.2.A we define the formulas $\underline{\underline{C}}^{y}_{x}(\underline{i})$ and $\underline{\underline{C}}^{\omega}_{x}(\underline{i})$ as follows. First obtain a normal form of $\underline{\underline{C}}(\underline{i})$, say

$$\underline{\underline{C}}(\underline{i}) : (\exists \underline{j}).K[\underline{j}(o)] \wedge (\forall t)\, B[\underline{i}(t), \underline{j}(t), \underline{j}(t')]$$

Then define

$$\underline{\underline{C}}^{y}_{x}(\underline{i}) : (\exists j) \cdot K[\underline{j}(x)] \wedge (\forall t)^{y}_{x} B(t) \wedge B[\underline{\vee}, \underline{j}(y), \underline{j}(y')] \wedge (\forall t)^{\omega}_{y}, B[\underline{\wedge}, \underline{j}(t), \underline{j}(t')]$$

$$\underline{\underline{C}}^{\omega}_{x}(\underline{i}) : (\exists \underline{j}) \cdot K[\underline{j}(x)] \wedge (\forall t)^{\omega}_{x} B[\underline{i}(t), \underline{j}(t), \underline{j}(t')]$$

Next for any Sg_n-formulas $\underline{\underline{C}}(\underline{i})$, $\underline{\underline{D}}(\underline{i})$ of W.2.A. we define $\underline{\underline{C}} \cup \underline{\underline{D}}$, $\underline{\underline{C}} \cdot \underline{\underline{D}}$, $\underline{\underline{C}}^{*}$ by

$$[\underline{\underline{C}} \cup \underline{\underline{D}}](\underline{i}) : \underline{\underline{C}}(\underline{i}) \vee \underline{\underline{D}}(\underline{i})$$

$$[\underline{\underline{C}} \cdot \underline{\underline{D}}](\underline{i}) : (\exists y) \cdot \underline{\underline{C}}^{y}_{o}(\underline{i}) \wedge \underline{\underline{D}}^{\omega}_{y}(\underline{i})$$

$$[\underline{\underline{C}}^{*}](\underline{i}) : (\exists s) \cdot (\forall xy)[s(x)\ s(y)\ (\forall t)^{y}_{x}, \tilde{s}(t) \supset \underline{\underline{C}}^{y}_{x}(\underline{i})] \wedge (\forall x)[s(x)(\forall t)^{\omega}_{x}, \tilde{s}(t) \supset \underline{\underline{C}}^{\omega}_{x}(\underline{i})]$$

It is easy to see that these operators on Sg_n-formulas of W.2.A. define the operations $\cup$, $\cdot$, * on sets of finite n-strings. Note that $\cdot$ corresponds to individual quantification, while the feedback-operation * is reflected as a finite-set quantification.

9. AN UNSOLVED PROBLEM

In essence our main result says that in [o, ', $\exists_o$i] one can define only very simple recursive operators u = $\psi(\underline{i})$, namely, input to output operators of finite automata. In contrast [o, ', 2x, $\exists_o$i] contains definitions for all recursive operators u = $\psi(\underline{i})$ (see Robinson [14]).

Problem 1: Is the weak second-order theory [o, 2x+1, 2x+2, $\exists_o$i] decidable? Which are the recursive operators definable in this theory?

These questions are of interest for automata theory, because via the enumeration of finite strings on two letters 1_1, 1_2 (see Section 7,1). The theory $[o, 2x+1, 2x+2, \exists_o i]$ is equal to the theory $[o, 1_1\widehat{\ }x, 1_2\widehat{\ }x, \exists_o i]$ on the set N_2 of finite strings. Let $\exists_{oo} i$ denote quantification over all finite subsets of N_k which in addition are chains with respect to the terminal segment relation on N_k. Then by a straightforward extension of the methods used in this paper one obtains:

Theorem 10: The "very weak" second-order theory $[o, 1_1\widehat{\ }x, \ldots, 1_k\widehat{\ }x, \exists_{oo} i]$ is decidable. All regular sets, and only regular sets, on the alphabet 1_1, $\ldots$, 1_k can be defined by formulas $\underline{\underline{C}}(x)$ of this theory.

BIBLIOGRAPHY

1. Behmann, Heinrich, "Beiträge zur Algebra der Logik, insbesondere zum Entscheidungsproblem," Mathematische Annalen, Vol. 86, pp. 163-229 (1922).

2. Burks, A. W., and Wright, J. B., "Theory of Logical Nets," Proc. IRE, 41, 1357-1365 (1953).

3. Church, Alonzo, "Application of Recursive Arithmetic to the Problem of Circuit Synthesis," Proceedings of the Cornell Logic Conference, Cornell University, 1957. Also see "Application of Recursive Arithmetic in the Theory of Computing and Automata," notes for a summer course, The University of Michigan, 1959.

4. Copi, I. M., Elgot, C.C., and Wright, J. B., "Realization of Events by Logical Nets," Journal of the Association for Computing Machinery, 5, pp. 181-196 (1958).

5. Gödel, Kurt, "On undecidable propositions of formal mathematical systems," Notes by S. C. Kleene and Barkley Rosser on lectures at the Institute for Advanced Study, 1934. Mimeographed, Princeton, N. J., 30 pp.

6. Kleene, S. C., "Representation of Events in Nerve Nets and Finite Automata," Automata Studies, Princeton University Press, 1956, pp. 3-41.

7. Medvedev, I. T., "On a Class of Events Representable in a Finite Automaton," MIT Lincoln Laboratory Group Report, 34-73, translated from the Russian by J. Schorr-Kon, June 30, 1958.

8. Myhill, John, "Finite Automata and Representation of Events," WADC Report TR 57-624, Fundamental Concepts in the Theory of Systems, October, 1957, pp. 112-137.

9. Moore, E. F., "Gedanken-Experiments on Sequential Machines," Automata Studies, Princeton, 1956, pp. 129-153.

10. Presberger, M., Über die Vollstandigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt." Comptes-rendus du I Congres des Mathematiciens des Pays Slavs, Warsaw, 1930, pp. 92-101, 395.

11. Putnam, H., "Decidability and Essential Undecidability," Journal of Symbolic Logic, Vol. 22 (1957) pp. 39-54.

12. Quine, W. V., Mathematical Logic. Harvard Univ. Press, Cambridge, 1947.

13. Rabin, M., and Scott, D., "Finite Automata and Their Decision Problems," IBM Journal, April, 1959, pp. 114-125.

14. Robinson, R. M., "Restricted Set-Theoretical Definitions in Arithmetic," Proc. American Mathematical Society, Vol. 9, (1958), pp. 238-242.

15. Skolem, Thoralf, "Untersuchungen über die Axiome des Klassenkalkuls und über Produktations- und Summationsprobleme, welche gewisse Klassen von Aussagen betreffen," Skrifter utgit av Videnskapsselskapet i Kristiania, I. Matematisk-naturvidenskabelig klasse 1919, No. 3, 37 pp.