JOURNAL OF ALGEBRA 13, 447–464 (1969)

Sets Recognized by n-Tape Automata

S. EILENBERG,* C. C. ELGOT,† AND J. C. SHEPHERDSON††

IBM Watson Research Center, Yorktown Heights, New York 10598

Communicated by Graham Higman

Received December 2, 1967

INTRODUCTION

The n-tape automata studied here, bear a very close resemblance to ordinary finite automata, since all n-tapes move simultaneously. This kind of tape action differs from that of the n-tape automata of [*4*], where tape motion is individual and is controlled by the state of the automaton.

The notion of "n-tape automaton" over an alphabet Σ gives rise to the notion of "n-recognizable" set of n-tuples of words in Σ. This latter notion coincides with what is called "FAD relation" in [*1*].

By means of a certain first-order interpreted theory, the notion that a set of n-tuples of words in Σ is "n-definable" is introduced. In contradistinction to the notion "n-recognizable," which is defined for fixed n, the notion "n-definable" must be defined simultaneously for all n. The main result asserts that in the case that Σ is finite and contains more than one letter, these two notions are extensionally equivalent.

1. n-TAPE AUTOMATA

We start with an informal description of n-tape automata. Let Σ be a set of elements (not necessarily finite) called an *alphabet*. As usual, we denote by Σ^* the free monoid (always with unit element) with base Σ and by Σ^{*n} the n-fold product $\Sigma^* \times \cdots \times \Sigma^*$. An element w of Σ^{*n} is then an n-tuple $w_1, ..., w_n$, where each w_i is a word in the alphabet Σ. Let S be a finite set (the elements of which will be called states). There is a distinguished *initial* state s_0 in S and a distinguished subset F of S of *final* states. An

* Columbia University and IBM Watson Research.

† IBM Watson Research.

†† University of Bristol, England.

481/13/4-1

element $w = (w_1, \ldots, w_n)$ acts on the set S in the following manner. Let $w = uw'$, where u_i is a single letter, if the length $lw_i > 0$, and $u_i = 1$, if $w_i = 1$. For any $s \in S$, su is then an element of S and sw is defined as $(su)\, w'$. This combined with the rule that $s1 = s$, where $1 = (1, \ldots, 1)$ is the unit element of Σ^{*n}, gives an inductive description of $sw \in \Sigma^{*n}$, for any $s \in S$ and $w \in \Sigma^{*n}$. The *behavior* $\mathscr{B}(\mathfrak{A})$ of an n-tape automaton is the set of all $w \in \Sigma^{*n}$ such that $s_0 w \in F$. A subset of Σ^{*n}, which is the behavior of some automaton, is called *n-recognizable.*

It should be noted that for $n = 1$, the automata described above are the ordinary finite automata, so that "1-recognizable" is "recognizable" in the ordinary sense. The extreme case $n = 0$ may also be included; Σ^{*n} in this case has only the unit element and the behavior of the automaton is the set consisting of the unit element if $s_0 \in F$ and is empty otherwise. Exactly the same phenomenon takes place in the other extreme case where Σ is empty and n is arbitrary.

A formal substitute for automata described above will be given in Section 4. The class of recognizable subsets of n-tape automata will be denoted by $\mathscr{R}_n(\Sigma)$. Note that $\mathscr{R}_1(\Sigma) = \mathscr{R}(\Sigma)$ is just the class of recognizable sets in the usual sense. Since the alphabet Σ is fixed throughout, we shall write $\mathscr{R}_n$ instead of $\mathscr{R}_n(\Sigma)$.

2. Definable Sets

We now describe a sequence $\mathscr{D} = \{\mathscr{D}_n \,;\, n = 0, 1, \ldots\}$, each $\mathscr{D}_n$ being a class of subsets of Σ^{*n}. The sequence $\mathscr{D}$ will be defined as the smallest one containing certain *basic sets* and closed with respect to certain operations. The basic sets are:

(2.1) $\Sigma^*\sigma = \{w \mid w \in \Sigma^*, \sigma \text{ is the terminal letter of } w\}$;

(2.2) $I = \{(w_1, w_2) \mid (w_1, w_2) \in \Sigma^{*2}, w_2 \leqslant w_1\}$,

where "$w_2 \leqslant w_1$" means w_2 is an initial segment of w_1;

(2.3) $E = \{(w_1, w_2) \mid (w_1, w_2) \in \Sigma^{*2}, lw_1 = lw_2\}$.

The operations are the following:

(2.4) *Binary intersection.* For every n, the intersection of any two sets in $\mathscr{D}_n$ is in $\mathscr{D}_n$.

(2.5) *Difference.* For any two sets C_1, C_2 in $\mathscr{D}_n$, the difference $C_1 \setminus C_2$ is in $\mathscr{D}_n$.

(2.6) *Permutation.* Given any permutation π of the set $\{1, 2, \ldots, n\}$ and given $w \in \Sigma^{*n}$, let $\pi w = (w_{\pi 1}, w_{\pi 2}, \ldots, w_{\pi n})$. Then for every C in $\mathscr{D}_n$, the set πC is in $\mathscr{D}_n$.

(2.7) *Projection.* Define $p : \Sigma^{*(n+1)} \to \Sigma^{*n}$ by setting $p(w_1, \ldots, w_{n+1}) = (w_1, \ldots, w_n)$. Then for every set C in $\mathscr{D}_{n+1}$, the set pC is in $\mathscr{D}_n$.

(2.8) *Cylindrification.* For every set C in $\mathscr{D}_n$, the set $p^{-1}C$ is in $\mathscr{D}_{n+1}$. Note that

$$p^{-1}C = \{w : w \in \Sigma^{*(n+1)}, (w_1, \ldots, w_n) \in C\}.$$

We observe that $pI = pE = \Sigma^* \in \mathscr{D}_1$. Hence, by repeated application of cylindrification, $\Sigma^{*n} \in \mathscr{D}_n$. Thus, by (2.5), $\mathscr{D}_n$ is closed with respect to

(2.9) *Complementation.* If $C \in \mathscr{D}_n$, the complement $\Sigma^{*n} \setminus C$ of C is in $\mathscr{D}_n$. In particular, for every n, $\phi \in \mathscr{D}_n$.

The sets $\mathscr{D}_n$ may be briefly described in the language of mathematical logic as the n-ary relations on Σ^* first-order definable from the binary relations I and E, and from the unary relations $\Sigma^*\sigma$, $\sigma \in \Sigma$. A set $C \in \Sigma^{*n}$ will be called *n-definable* iff $C \in \mathscr{D}_n$. Thus, C is n-definable iff there is a first-order formula $\mathscr{F}[w_1, \ldots, w_n]$ constructed from the atomic formulas

$$w \in \Sigma^*\sigma, \ (w, w') \in I, \ (w, w') \in E,$$

which defines C in the ordinary sense. Illustrations of the connection between formulas and the sets which they define, will be found in the proofs of Section 8. In particular, a sentence (formula without free variables) defines a subset of Σ^{*0} which, therefore, is either empty or is $\Sigma^{*0} = \{1\}$. In the latter case, the sentence is true.

3. Statement of Main Results

THEOREM 1. *For any alphabet Σ, every n-definable set is n-recognizable.*

THEOREM 2. *If Σ is a finite alphabet containing more than one letter, then every n-recognizable set is n-definable.*

In the excluded cases of Σ infinite or $\Sigma = \{\sigma\}$, Theorem 2 fails. The latter case is discussed fully in Section 9, where the definable sets for $\Sigma = \{\sigma\}$ are completely described by Theorem 9.1. In particular, $\mathscr{D}_1$ consists exactly of those sets which are finite or whose complements are finite. Thus, for example, the set $(\sigma\sigma)^*$ is in $\mathscr{R}_1$ but not in $\mathscr{D}_1$. The case of Σ infinite is treated in Section 10.

In the case that Σ is finite, the action of a finite automaton over Σ may be described by a finite table. It is a consequence of the fact that the proof of Theorem 1 is entirely effective, that the first-order theory based upon the relations $E, I, \Sigma^*\sigma$ is decidable. More explicitly, given finite automata

$\mathcal{A}_1$ and $\mathcal{A}_2$, there is a mechanical procedure for constructing an automaton $\mathcal{A}$ such that $\mathcal{B}\mathcal{A} = \mathcal{B}\mathcal{A}_1 \cap \mathcal{B}\mathcal{A}_2$ and a mechanical procedure for constructing $\mathcal{A}'$ so that $\mathcal{B}\mathcal{A}' = p\mathcal{B}\mathcal{A}_1$; similarly for (2.5), (2.6), and (2.8). The discussion of related decidability and undecidability results is, however, outside the scope of this paper.

Finally, Theorem 11.1 shows how sets in $\mathcal{R}_n$ may be decomposed into "homogeneous" sets.

4. Reduction to Ordinary Automata

Let Γ be a finite set with a binary relation $\gamma' \prec \gamma$. A word $w = \gamma_1\gamma_2 \cdots \gamma_r$, $\gamma_i \in \Gamma$, will be called *related* if $\gamma_r \prec \cdots \prec \gamma_2 \prec \gamma_1$. The set of all related words is denoted by G. We note that

$$G = \Gamma^* \setminus F,$$

where

$$F = \bigcup \Gamma^*\gamma_1\gamma_2\Gamma^*, \qquad \gamma_2 \text{ non} \prec \gamma_1 . \tag{4.1}$$

Proposition 4.1. *If Γ is finite, then G is a recognizable subset of Γ^*.*

Proof. Each of the summands in (4.1) is recognizable, e.g., by Kleene's theorem. Since Γ is finite, the union in (4.1) is finite so that F is recognizable and therefore also G.

The proposition fails if Γ is infinite. For example, let $\Gamma = \{\gamma_1, \gamma_2, \gamma_3, \ldots\}$ and define

$$\gamma \prec \gamma' \Leftrightarrow \gamma = \gamma_i \wedge \gamma' = \gamma_{i+1}, \qquad \text{for some } i.$$

Then G is not recognizable. Indeed, let $\mathcal{A}$ be an automaton recognizing G. Then, for every i, j, $i < j$, we have $\gamma_i \cdots \gamma_j \in G$, while

$$\gamma_1 \cdots \gamma_j\gamma_{i+1} \cdots \gamma_j \in \Gamma^* \setminus G.$$

Thus, the states $s_0\gamma_1\gamma_2 \cdots \gamma_i$ and $s_0\gamma_1\gamma_2 \cdots \gamma_j$ are distinct, where s_0 is the initial state of $\mathcal{A}$.

Returning to the alphabet Σ, consider $w = (w_1, \ldots, w_n) \in \Sigma^{*n}$, we define the length function $lw = \sup lw_i$ for $i = 1, \ldots, n$.

Let $\Gamma_n = \{w \mid w \in \Sigma^{*n}, lw = 1\}$. Thus, $w \in \Gamma_n$ provided both that $w_i \in \Sigma$ or $w_i = 1$ and that at least one w_i is an element of Σ. We define a relation $u \prec w$ on Γ_n by the condition

$$w_i = 1 \Rightarrow u_i = 1.$$

This gives us the subsets G_n and F_n of $\Gamma_n{}^*$ for each n.

Each $w \in \Sigma^{*n}$ admits a unique decomposition

$$w = \gamma_1 \cdots \gamma_k, \qquad \gamma_i \in \Gamma_n, \tag{4.2}$$

and

$$\gamma_k \prec \gamma_{k-1} \prec \cdots \prec \gamma_1 .$$

Further, in this decomposition $lw = k$.

This decomposition yields a mapping

$$\alpha : \Sigma^{*n} \to G_n ,$$

which is clearly a bijection. The inverse of this bijection is denoted by β. We are careful to avoid identification of Σ^{*n} with G_n because α is not multiplicative. We note, however, that β does preserve multiplication to the extent that multiplication is defined in G_n.

PROPOSITION 4.2. *G_n is a recognizable subset of $\Gamma_n{}^*$.*

Proof. Since the relation $\prec$ is a preorder, we obtain an equivalence relation in Γ_n by defining

$$\gamma_1 \equiv \gamma_2 \Leftrightarrow \gamma_1 \prec \gamma_2 \wedge \gamma_2 \prec \gamma_1 .$$

Let $\hat{\Gamma}_n = \Gamma_n/\equiv$. First note that $\hat{\Gamma}_n$ is finite. Secondly, the preorder in Γ_n becomes an order in $\hat{\Gamma}_n$. By Proposition 4.1, $\hat{G}_n$ is a recognizable subset of $\hat{\Gamma}_n{}^*$. If $\eta : \Gamma_n{}^* \to \hat{\Gamma}_n{}^*$ is the natural morphism, then $G_n = \eta^{-1}\hat{G}_n$. Consequently, G_n is recognizable.

Let $\mathcal{A}$ be an automaton in the usual sense on the alphabet Γ_n. Then its behavior $\mathcal{B}(\mathcal{A})$ is a subset of $\Gamma_n{}^*$. This automaton may also be viewed as an n-tape automaton in the sense of Section 1, since each $w \in \Sigma^{*n}$ acts on the states by virtue of formula (4.2).

The behavior $\mathcal{B}_n(\mathcal{A})$ of the n-tape automaton is then a subset of Σ^{*n}. The two behaviors are related by the formula

$$\mathcal{B}_n(\mathcal{A}) = \beta(G_n \cap \mathcal{B}(\mathcal{A})).$$

This leads to the following

PROPOSITION 4.3. *A subset X of Σ^{*n} is n-recognizable iff αX is a recognizable subset of $\Gamma_n{}^*$.*

Proof. If $X = \mathcal{B}_n(\mathcal{A})$, then $\alpha X = G_n \cap \mathcal{B}(\mathcal{A})$. This set is recognizable since G_n is recognizable. Conversely, if αX is recognizable, then there exists an automaton $\mathcal{A}$ such that $\mathcal{B}(\mathcal{A}) = \alpha X$, then

$$\mathcal{B}_n(\mathcal{A}) = \beta(G_n \cap \mathcal{B}(\mathcal{A})) = \beta(G_n \cap \alpha X) = \beta\alpha X = X.$$

For future use, we introduce the projection morphism

$$q : \Gamma_{n+1}^{*} \to \Gamma_n ,$$

by defining for $\gamma = (w_1, \ldots, w_{n+1}) \in \Gamma_{n+1}$ (so that $w_i \in \Sigma$ or $w_i = 1$),

$$q\gamma = 1 \qquad \text{if} \quad w_1 = \cdots = w_n = 1$$

$$q\gamma = (w_1, \ldots, w_n) \qquad \text{otherwise.}$$

Observe that $qG_{n+1} = G_n$. The projection q is related to the projection $p : \Sigma^{*(n+1)} \to \Sigma^{*n}$ by the formal rules:

$$\alpha pX = q\alpha X \qquad \text{for} \quad X \subset \Sigma^{*(n+1)} \tag{4.3}$$

$$\alpha p^{-1}X = G_{n+1} \cap q^{-1}\alpha X \qquad \text{for} \quad X \subset \Sigma^{*n}. \tag{4.4}$$

PROPOSITION 4.4. *If X is a recognizable subset of Γ_{n+1}^{*}, then qX is a recognizable subset of $\Gamma_n{}^{*}$.*

Proof. This follows from the following slightly more general fact: If Ω and Θ are arbitrary alphabets and $f : \Omega^* \to \Theta^*$ is a morphism such that $f\omega \in \Theta$, or $f\omega = 1$, for all $\omega \in \Omega$, then f transforms recognizable sets into recognizable sets. Indeed, let X be a recognizable subset of Ω^*, and let $Y = fX$. There is then a finite monoid A and a morphism $g : \Omega^* \to A$, such that $X = g^{-1}C$ for some $C \subset A$. The morphism g determines a morphism $G : P(\Omega^*) \to P(A)$, where $P(\Omega^*)$ and $P(A)$ are the monoids of all subsets of Ω^* and A respectively. Consider the mapping $f^{-1} : \Theta^* \to P(\Omega^*)$. The condition imposed on f implies that $f^{-1}(xy) = (f^{-1}x)(f^{-1}y)$ for $x, y \in \Theta^*$. Then $Gf^{-1} : \Theta^* \to P(A)$ is a multiplicative mapping. Let B be the image of Gf^{-1}. Then B is a finite monoid and $h = Gf^{-1} : \Theta^* \to B$ is a morphism of monoids. Now verify that

$$h^{-1}(D \cap B) = Y,$$

where

$$D = \{U \mid U \in P(A),\ U \cap C \neq \varnothing\}.$$

5. PROOF OF THEOREM 1

First we show that the basic sets (2.1), (2.2), and (2.3) are 1-recognizable respectively 2-recognizable.

Ad(2.1) The following automaton recognizes $\Sigma^*\sigma$:

$$S = \{s_0, s_1\}, \qquad F = \{s_1\},$$

$$s_i\sigma = s_1, \qquad s_i\sigma' = s_0 \qquad \text{for} \quad \sigma' \neq \sigma.$$

Ad(2.2) The following automaton recognizes I:

$$\begin{aligned} S &= \{s_0, s_1, s_2\}, \qquad F = \{s_0, s_1\}, \\ s_0(\sigma, \sigma) &= s_0 \\ s_i(\sigma, 1) &= s_1 \qquad \text{for} \quad i = 0, 1 \\ s\gamma &= s_2 \qquad \text{in all other cases.} \end{aligned}$$

Ad(2.3) The following automaton recognizes E:

$$\begin{aligned} S &= \{s_0, s_1\}, \qquad F = \{s_0\}, \\ s_0\gamma &= s_0, \qquad \text{for} \quad \gamma \in \Sigma^2 \\ s\gamma &= s_1, \qquad \text{in all other cases.} \end{aligned}$$

The next step is to verify that rules (2.4)–(2.8) hold with $\mathscr{R}_n$ replacing $\mathscr{D}_n$. This is clear for rules (2.4)–(2.6).

Ad(2.7) If $X \in \mathscr{R}_{n+1}$, then αX is a recognizable subset of G_{n+1}. Thus, by Proposition 4.4, $q\alpha X$ is a recognizable subset of G_n. By (4.3), $q\alpha X = \alpha p X$ and, therefore, $pX \in \mathscr{R}_n$.

Ad(2.8) If $X \in \mathscr{R}_n$, then αX is a recognizable subset of G_n. Then $G_{n+1} \cap q^{-1}\alpha X$ is a recognizable subset of G_{n+1}. By (4.4), $\alpha p^{-1} X$ is a recognizable subset of G_{n+1} and, therefore, $p^{-1}X \in \mathscr{R}_{n+1}$.

This concludes the proof of Theorem 1.

6. Local Sets

Let Ω be a finite alphabet. The subsets of Ω^* of the form

$$\{1\}, \omega\Omega^*, \Omega^*\omega, \Omega^*\omega, \omega'\Omega^*, \tag{6.1}$$

with $\omega, \omega' \in \Omega$, will be called *basic local* sets. The union of any set of basic *local* sets will be called a local set.

Proposition 6.1. *If Ω is a subset of a finite set Θ, then for every local subset L of Ω^*, there exists a local subset K of Θ^* such that*

$$\Omega^* \setminus L = \Theta^* \setminus K.$$

Proof. We must have

$$K = (\Theta^* \setminus \Omega^*) \cup L;$$

so we only need to prove that this set is local in Θ^*. First we enlarge L to a set L' obtained by replacing each summand of L in (6.1) by the corresponding set

$$\{1\}, \omega\Theta^*, \Theta^*\omega, \Theta^*\omega\omega'\Theta^*.$$

There results a set L' local in Θ^* such that $L' \cap \Omega^* = L$. Consequently,

$$K = (\Theta^* \setminus \Omega^*) \cup L'.$$

The set $\Theta^* \setminus \Omega^*$ is the union of the sets

$$\theta\Theta^*, \Theta^*\theta, \Theta^*\theta\theta'\Theta^*, \Theta^*\theta'\theta\Theta^*,$$

for all $\theta \in \Theta \setminus \Omega$ and all $\theta' \in \Theta$. Thus, $\Theta^* \setminus \Omega^*$ is local. Consequently, K is local.

PROPOSITION 6.2. *If Θ is a finite alphabet and X is a recognizable subset of Θ^*, then there exists a finite alphabet Ω, a function $f : \Omega \to \Theta$, and a local subset L of Ω^* such that*

$$X = f^*(\Omega^* \setminus L).$$

Here f^* denotes the morphism $\Omega^* \to \Theta^*$ determined by f.

Proof. This proposition should be regarded as well known. For the sake of completeness we include a proof.

Let $\mathfrak{A}$ be a finite Θ-automaton which recognizes the set X. Let S be the set of states, $s_0 \in S$ the initial state and $F \subset S$ the set of final states. Let $\Omega = S \times \Theta$, $f(s, \theta) = \theta$. Let L be the union of the following basic local sets in Ω^*

$$\begin{aligned} (s, \theta)\, \Omega^* \quad & \text{for} \quad s \neq s_0 \\ \Omega^*(s, \theta)(s', \theta')\, \Omega^* \quad & \text{for} \quad s' \neq s\theta \\ \Omega^*(s, \theta) \quad & \text{for} \quad s\theta \notin F. \end{aligned}$$

If $w \in \Omega^* \setminus L$, then $s_0 f^*w \in F$ and, therefore, $f^*w \in X$. Conversely, let $v = \theta_1 \cdots \theta_n \in X$. Consider

$$w = (s_0, \theta_1)(s_1, \theta_2) \cdots (s_{n-1}, \theta_n),$$

where $s_i = s_{i-1}\theta_i$ for $i = 1,..., n-1$. Then $s_{n-1}\theta_n = s_0 v \in F$. Thus, $w \in \Omega^* \setminus L$ and $f^*w = v$ as required.

7. REDUCTION OF THEOREM 2

PROPOSITION 7.1. *Assume that the alphabet Σ is finite and has at least two letters. If a subset X of G_n is recognizable, then there exists an integer $r \geqslant 0$ and a local subset K of Γ_{n+r}^* such that*

$$X = q^r(G_{n+r} \setminus K), \tag{7.1}$$

where q^r is the iterated projection

$$\Gamma_{n+r}^* \xrightarrow{q} \Gamma_{n+r-1}^* \xrightarrow{q} \cdots \xrightarrow{q} \Gamma_n^*.$$

Proof. By Proposition 6.2 there exists an alphabet Ω, a mapping $f : \Omega \to \Gamma_n$, and a local subset L of Ω^* such that

$$f^*(\Omega^* \setminus L) = X. \tag{7.2}$$

Since Σ has at least two letters, there exists an integer $r \geqslant 0$, for which Σ^r will have more elements than Ω. Let $j : \Omega \to \Sigma^r$ be an injective mapping.

We turn our attention to Γ_{n+r}^*. Each $\gamma \in \Gamma_{n+r}$ may be written in one of the forms

$$(\gamma_1, \gamma_2), (\gamma_1, 1), (1, \gamma_2),$$

with $\gamma_1 \in \Gamma_n$, $\gamma_2 \in \Gamma_r$. Further, $q^r\gamma = \gamma_1$ in the first two cases while $q^r\gamma = 1$ in the third case.

Since $f\omega \in \Gamma_n$ and $jw \in \Sigma^r \subset \Gamma_r$, we may embed Ω into Γ_{n+r} by identifying each $\omega \in \Omega$ with $(f\omega, j\omega) \in \Gamma_{n+r}$. Then formula (7.2) becomes

$$q^r(\Omega^* \setminus L) = X. \tag{7.3}$$

Next we show that

$$\Omega^* \setminus L \subset G_{n+r}.$$

Indeed, let

$$w = \omega_1 \cdots \omega_k \in \Omega^* \setminus L.$$

Then, $f^*w \in X \subset G_n$, so that $f\omega_k \prec f\omega_{k-1} \prec \cdots \prec f\omega_1$. Since

$$j\omega_k \prec j\omega_{k-1} \prec \cdots \prec j\omega_1$$

holds automatically because $j\omega_i \in \Sigma^*$, it follows that $\omega_k \prec \omega_{k-1} \prec \cdots \prec \omega_1$; i.e., $w \in G_{n+r}$. Hence, $\Omega^* \setminus L \subset G_{n+r}$.

By Proposition 6.1, there exists a local subset K of Γ_{n+r}^* such that $\Omega^* \setminus L = \Gamma_{n+r}^* \setminus K$. Since $\Gamma_{n+r}^* \setminus K \subset G_{n+r}$, we have $\Gamma_{n+r}^* \setminus K = G_{n+r} \setminus K$. This implies (7.1) as required.

The proposition just proved will now be used to reduce the problem of proving the inclusion $\mathscr{R}_n \subset \mathscr{D}_n$ to a lemma concerning basic local sets in Γ_n^*. This lemma will be established in Section 8.

Let $X \in \mathscr{R}_n$. Then αX is a recognizable subset of G_n, and by the proposition we have

$$\alpha X = q^r(G_{n+r} \setminus K),$$

for a local set K in Γ_{n+r}^*. Therefore,

$$X = \beta q^r(G_{n+r} \setminus K) = p^r\beta(G_{n+r} \setminus K).$$

To show that $X \in \mathscr{D}_n$, it suffices to show that $\beta(G_{n+r} \setminus K) \in \mathscr{D}_{n+r}$. Let $K = \bigcup_i K_i$ be the finite union of basic local sets and let $m = n + r$. Then

$$G_m \setminus K = \bigcap_i (G_m \setminus K_i),$$

so that

$$\beta(G_m \setminus K) = \bigcap_i \beta(G_m \setminus K_i).$$

Since $\beta(G_m \setminus K_i) = \Sigma^{*m} \setminus \beta(G_m \cap K_i)$, and since $\mathscr{D}_m$ is closed under boolean operations, it suffices to prove

LEMMA 7.2. *For any alphabet Σ and for any basic local subset K of $\Gamma_n{}^*$, the set $\beta(G_n \cap K)$ is n-definable. This will be proved in the next section.*

8. PROOF OF LEMMA 7.2

There will be a string of preliminary lemmas. Throughout, the letters w, w_1, w_i, etc., will designate elements of Σ^*; thus, (w_1, w_2) will automatically be an element of Σ^{*2}, etc., where Σ is an arbitrary alphabet.

LEMMA 8.1. *For $k = 0, 1, \ldots$, the sets*

$$L_k = \{(w_1, w_2) \mid k + lw_2 \leqslant lw_1\}$$
$$L_k' = \{(w_1, w_2) \mid k + lw_2 = lw_1\}$$
$$L_k'' = \{(w_1, w_2) \mid k + lw_2 \geqslant lw_1\},$$

are 2-definable, and the sets

$$M_k = \{w \mid k \leqslant lw\}$$
$$M_k' = \{w \mid k = lw\}$$
$$M_k'' = \{w \mid k \geqslant lw\},$$

are 1-definable.

Proof. Consider the following two equivalences:

$$lw_2 \leqslant lw_1 \Leftrightarrow \exists w_3(lw_2 = lw_3 \wedge w_3 \leqslant w_1)$$
$$k + 1 + lw_2 \leqslant lw_1 \Leftrightarrow \exists w_3(k + lw_3 \leqslant lw_1 \wedge lw_3 \leqslant lw_2 \wedge lw_3 \neq lw_2)$$

The first formula implies that

$$L_0 = p(Q_1 \cap Q_2)$$
$$Q_1 = \{w_1, w_2, w_3 \mid lw_2 = lw_3\}$$
$$Q_2 = \{w_1, w_2, w_3 \mid w_3 \leqslant w_1\}.$$

The latter sets are obtainable from the sets E and I by permutation and cylindrification. Thus, $Q_1, Q_2 \in \mathscr{D}_3$ and, therefore, $L_0 \in \mathscr{D}_2$.

The second formula shows that

$$L_{k+1} = p(R_1 \cap R_2 \setminus R_3),$$

R_1, R_2, R_3 obtainable from L_k, L_0, and E by permutation and cylindrification. Thus, if $L_k \in \mathscr{D}_2$, then $R_1, R_2, R_3 \in \mathscr{D}_3$ and $L_{k+1} \in \mathscr{D}_2$. Hence, by induction on k, $L_k \in \mathscr{D}_2$ for all k.

$$L_k'' = \Sigma^{*2} \setminus L_{k+1}, \qquad L_k' = L_k \cap L_k''.$$

Next,

$$k \leqslant lw_1 \Leftrightarrow \exists_{w_2} (k + lw_2 \leqslant lw_1).$$

Thus, $M_k = pL_k \in \mathscr{D}_1$. Further,

$$M_k'' = \Sigma^* \setminus M_{k+1}, \qquad M_k' = M_k \cap M_k''$$

so that $M_k, M_k'' \in \mathscr{D}_1$.

LEMMA 8.2. *For any $\sigma, \sigma' \in \Sigma$ the sets*

$$V_\sigma = \{(w_1, w_2) \mid w_1 = w_2\sigma\}$$
$$V_{\sigma\sigma'} = \{(w_1, w_2) \mid w_1 = w_2\sigma\sigma'\}$$
$$U_{\sigma\sigma'} = \{(w_1, w_2) \mid w_2\sigma\sigma' \leqslant w_1\},$$

are 2-definable.

Proof. The set V_σ is defined by the formula

$$w_2 \leqslant w_1 \wedge (w_1, w_2) \in L_1' \wedge w_1 \in \Sigma^*\sigma.$$

Thus, $V_\sigma \in \mathscr{D}_2$. Now $V_{\sigma\sigma'}$ is defined by

$$\exists w_3(w_3 = w_2\sigma \wedge w_1 = w_3\sigma').$$

Therefore, $V_{\sigma\sigma'} \in \mathscr{D}_2$. Finally, $U_{\sigma\sigma'}$ is given by

$$\exists w_3(w_3 = w_2\sigma\sigma' \wedge w_3 \leqslant w_1).$$

Thus, $U_{\sigma\sigma'} \in \mathscr{D}_2$.

LEMMA 8.3. *The sets $\sigma\Sigma^*$ are 1-definable for all $\sigma \in \Sigma$.*

Proof. Note that $\sigma\Sigma^*$ is defined by the formula

$$\exists w_2(w_2 \in M_1' \wedge w_2 \in \Sigma^*\sigma \wedge w_2 \leqslant w_1).$$

LEMMA 8.4. *$\beta(G_n \cap \gamma\Gamma_n^*)$ is n-definable.*

Proof. Applying an appropriate permutation, we may assume that

$$\gamma = (\sigma_1, \ldots, \sigma_r, 1, \ldots, 1) \qquad \text{with} \quad 1 \leqslant r \leqslant n.$$

Then $\beta(G_n \cap \gamma\Gamma_n^*)$ is the intersection of the subsets of Σ^{*n} defined by the following conditions:

$$w_i \in \sigma_i \Sigma^* \qquad \text{for} \quad 1 \leqslant i \leqslant r$$

$$w_i = 1 \qquad \text{for} \quad r < i \leqslant n.$$

This proves the lemma.

If in the above argument we set $r = 0$, we obtain

LEMMA 8.4′. *$\beta(G_n \cap \{1\})$ is n-definable.*

LEMMA 8.5. *$\beta(G_n \cap \Gamma_n^*\gamma\gamma'\Gamma_n^*)$ is n-definable.*

Proof. Using an appropriate permutation, we may assume that

$$\gamma = (\sigma_1, \ldots, \sigma_r, 1, \ldots, 1)$$

$$\gamma' = (\sigma_1', \ldots, \sigma_s', 1, \ldots, 1),$$

with $0 < s \leqslant r \leqslant n$. We then see that

$$\beta(G_n \cap \Gamma_n^*\gamma\gamma'\Gamma_n^*) = p^r M,$$

where M is the subset of $\Sigma^{*(n+r)}$ defined by the following conditions:

$$\begin{aligned} w_{n+i}\sigma\sigma' &\leqslant w_i && \text{for} \quad i = 1, \ldots, s \\ w_{n+i}\sigma &= w_i && \text{for} \quad i = s+1, \ldots, r \\ lw_i &\leqslant lw_{n+r} && \text{for} \quad i = r+1, \ldots, n \\ lw_i &= lw_{n+r} && \text{for} \quad i = n+1, \ldots, n+r-1. \end{aligned}$$

This proves the lemma. Setting $s = 0$ in the above argument, we obtain

LEMMA 8.5′. *$\beta(G_n \cap \Gamma_n^*\gamma)$ is n-definable.*

The last four lemmas constitute a proof of Lemma 7.2.

9. THE CASE OF A SINGLE-LETTER ALPHABET

If Σ is a single letter, then Σ^* may be identified with the monoid N of nonnegative integers.

The basic definable sets then are

$$1 + N = \{x \mid 0 < x\}, \qquad I = \{x_1, x_2 \mid x_1 \leqslant x_2\}.$$

Since $E = \{x_1, x_2 \mid x_1 = x_2\}$ is obtainable from I, it has been suppressed.

Call a subset X of N^n *primitive* if it is the solution of a single inequality of the type

$$x_i \leqslant x_j + a \qquad \text{or} \qquad x_i \leqslant a \qquad \text{or} \qquad a \leqslant x_i ,$$

for some $i, j = 1, \ldots, n$ and some $a \geqslant 0$. The intersection of a finite number of primitive sets will be called *elementary*.

Let $\mathscr{E}_n$ denote the class of finite unions of elementary subsets of N^n.

THEOREM 9.1. $\mathscr{E}_n = \mathscr{D}_n$.

Proof. The fact that each primitive subset of N^n is in $\mathscr{D}_n$ follows from Lemma 8.1. Therefore, $\mathscr{E}_n \subset \mathscr{D}_n$, for all $n = 1, \ldots$.

To prove the opposite inclusion $\mathscr{D}_n \subset \mathscr{E}_n$, we first note that the basic definable sets are primitive. Further, the class of primitive sets is closed with respect to complementation and cylindrification. Therefore, the sequence $\{\mathscr{E}_n\}$ satisfies rules (2.4), (2.5), (2.6), and (2.8). To verify rule (2.7), it suffices to show that if $X \subset N^{n+1}$ is elementary, then so is the projection $pX \subset N^n$.

For any $x \in N^{n+1}$ it will be convenient to denote the last coordinate by y, while retaining the notation $x_1, \ldots, x_n$ for the first n coordinates. The inequalities defining the set X may now be recorded as follows:

(9.1) inequalities involving only $x_1, \ldots, x_n$

(9.2) $\qquad x_i + a_i \leqslant y \qquad -\infty < a_i < \infty$

(9.3) $\qquad y \leqslant x_j + b_j \qquad -\infty < b_j < \infty$

(9.4) $\qquad c \leqslant y \leqslant d \qquad 0 \leqslant c \leqslant d \leqslant \infty,$

with the indices i, j ranging over subsets I, J of $\{1, \ldots, n\}$.

We now record some consequences of these inequalities:

(9.5) $\qquad x_i + a_i \leqslant x_j + b_j \qquad i \in I, j \in J$

(9.6) $\qquad x_i + a_i \leqslant d \qquad i \in I$

(9.7) $\qquad c \leqslant x_j + b_j \qquad j \in J$

Let Y denote the elementary subset of N^n defined by the inequalities (9.1), (9.5)–(9.7). We assert that $pX = Y$. Since (9.5)–(9.7) are consequences of

(9.2)–(9.4), we certainly have $pX \subset Y$. To prove the converse, let $x = (x_1, ..., x_n) \in Y$. Define $x' = (x_1, ..., x_n, y)$ with

$$y = \mathrm{Inf}(d, x_j + b_j), \qquad j \in J.$$

Then $x' \in X$ and $px' = x$. Thus, $pX = Y$.

The following is immediate.

COROLLARY 9.2. *$\mathscr{D}_1$ consists of those subsets of N which are either finite or have finite complement.*

This result appears in the literature [*3*], cf. p. 354 and [*2*]. The proof of Theorem 9.1 is essentially the argument used in [*2*] to obtain the corollary.

10. THE CASE OF AN INFINITE ALPHABET

Let Σ be an infinite alphabet. Any permutation π of Σ induces an isomorphism $\pi^{*n} : \Sigma^{*n} \to \Sigma^{*n}$. A subset X of Σ^{*n} will be called *finitary* if there exists a finite subset F (called a *carrier* for X), such that for any permutation π of Σ leaving F pointwise-fixed, we have $\pi^{*n}X = X$.

PROPOSITION 10.1. *Every n-definable set is finitary.*

Proof. The basic sets $\Sigma^*\sigma$ are finitary with carriers $\{\sigma\}$. The basic sets I and E are finitary with carrier ϕ. Next consider the rules (2.4)–(2.8). If X_1 and X_2 are finitary with carriers F_1 and F_2, then $X_1 \cap X_2$ resp. $X_1 \setminus X_2$ is finitary with carrier $F_1 \cup F_2$. Thus, rules (2.4) and (2.5) hold. The rules (2.6)–(2.8) hold without change of carrier. This yields the conclusion.

EXAMPLE 1. Let Ξ be a subset of Σ which is infinite and such that $\Sigma \setminus \Xi$ also is infinite. Then Ξ is not finitary and, therefore, is not 1-definable. However, Ξ is recognized by the automaton

$$S = \{s_0, s_1, s_2\}, \qquad F = \{s_1\}$$
$$s_0\chi = s_1 \qquad \text{if } \chi \in \Xi$$
$$s\sigma = s_2 \qquad \text{in all other cases.}$$

EXAMPLE 2. The set

$$\{(\sigma w_1, \sigma w_2) \mid \sigma \in \Sigma\}$$

is definable.

Indeed, the set is defined by the formula

$$\exists w_3[lw_3 = 1 \wedge w_3 \leqslant w_1 \wedge w_3 \leqslant w_2].$$

EXAMPLE 3. The sets

$$\{(w_1\sigma, w_2\sigma) \mid \sigma \in \Sigma\},$$
$$\{(\sigma, \sigma'\sigma) \mid \sigma', \sigma \in \Sigma\},$$

are not 2-recognizable and hence also not 2-definable.

Indeed, let C be one of the two sets. Then, for $\sigma' \neq \sigma''$,

$$(\sigma', \sigma)(1, \sigma') \in C, \qquad (\sigma'', \sigma)(1, \sigma') \notin C.$$

Then for any automaton $\mathfrak{A}$ recognizing C, we must have $s_0(\sigma', \sigma) \neq s_0(\sigma'', \sigma)$, for $\sigma' \neq \sigma''$. Therefore, $\mathfrak{A}$ is not finite.

EXAMPLE 4. The sets

$$\{(w_1\sigma, w_2\sigma) \mid lw_1 = lw_2 , \sigma \in \Sigma\},$$
$$\{(\sigma_1\sigma, \sigma_2\sigma) \mid \sigma_1 , \sigma_2 , \sigma \in \Sigma\},$$

are 2-recognizable.

Indeed the automata recognizing these sets are

$$S = \{s_0 , s_1 , s_2\} \qquad F = \{s_1\}$$
$$\begin{aligned} s_0(\sigma_1 , \sigma_2) &= s_0 && \text{if} \quad \sigma_1 \neq \sigma_2 \\ s_0(\sigma, \sigma) &= s_1 \\ s_1(\sigma_1 , \sigma_2) &= s_0 && \text{if} \quad \sigma_1 \neq \sigma_2 \\ s_1(\sigma, \sigma) &= s_1 \\ s\gamma &= s_2 && \text{in all other cases.} \end{aligned}$$

$$S = \{s_0 , s_1 , s_2 , s_3\} \qquad F = \{s_2\}$$
$$\begin{aligned} s_0(\sigma_1 , \sigma_2) &= s_1 \\ s_1(\sigma, \sigma) &= s_2 \\ s\gamma &= s_3 && \text{in all other cases.} \end{aligned}$$

PROBLEM 1. Are the sets in Example 4 2-definable?

PROBLEM 2. If a subset of Σ^{*n} is both finitary and n-recognizable, is it n-definable?

PROBLEM 3. If a definable set is invariant under all permutations of the alphabet, is it then first order definable from E and I *only* (without use of $\Sigma^*\sigma$)?

11. Decomposition into Homogeneous Sets

Let A be a non-empty subset of $\{1,..., n\}$. An element $w = (w_1, ..., w_n)$ of Σ^{*n} is called *homogeneous of Type A* provided

$$w_i = 1 \qquad \text{for} \quad i \notin A \tag{11.1}$$

$$lw_i = lw_j \qquad \text{for} \quad i, j \in A. \tag{11.2}$$

In particular, the unit element of Σ^{*n} is homogeneous of any type. The set of all homogeneous elements of Type A form a submonoid of Σ^{*n}. This submonoid may be identified with the monoid Σ^{A*}, where Σ^A is the set of all functions $A \to \Sigma$.

Theorem 11.1. *Let Σ be a finite alphabet. A subset X of Σ^{*n} is n-recognizable if and only if X is the finite union of sets which are products.*

$$X_1 \cdots X_k \qquad k = 1, 2, ..., \tag{11.3}$$

where

$$X_i \text{ is a recognizable subset of } \Sigma^{A_i *}. \tag{11.4}$$

$$A_1 \supset \cdots \supset A_k. \tag{11.5}$$

For the proof we first develop analogous notions in the monoid Γ_n^* associated with the alphabet Σ. Let $\gamma \in \Gamma_n$. Then

$$\gamma = (w_1, ..., w_n), \qquad w_i \in \Sigma^*, \qquad \sup_i lw_i = 1.$$

Let

$$|\gamma| = \{i \mid w_i \in \Sigma\}.$$

Then

$$\phi \neq |\gamma| \subset \{1, ..., n\}.$$

For any non-empty subset A of $\{1,..., n\}$, set

$$\Gamma_A = \{\gamma \mid \gamma \in \Gamma_n, |\gamma| = A\}.$$

Theorem 11.2. *Let Σ be any alphabet. A subset Y of G_n is rational (i.e., regular in the sense of Kleene), if and only if, Y is the finite union of sets which are products*

$$Y_1 \cdots Y_k \qquad k = 1, 2, ..., \tag{11.3'}$$

where

$$Y_i \text{ is a rational subset of } \Gamma_{A_i}^* \tag{11.4'}$$

$$A_1 \supset \cdots \supset A_k. \tag{11.5'}$$

We first show how the second theorem implies the first. Indeed, if Σ is finite, then so is Γ_n. Thus, in Theorem 11.2, "rational" may be replaced by "recognizable." Further, the bijection $\alpha : \Sigma^{*n} \to G_n$ maps the submonoids Σ^{A*} of Σ^{*n} isomorphically onto the submonoid, $\Gamma_A{}^*$ of Γ_n. Further, α maps every set (11.3), satisfying (11.4) and (11.5), onto a set (11.3′) satisfying (11.4′) and (11.5′). The mapping $\beta : G_n \to \Sigma^{*n}$ does the opposite.

To prove Theorem 11.2, denote by $\mathscr{E}_1$ the class of all subsets of $\Gamma_n{}^*$ which are finite unions of sets (11.3′) satisfying (11.4′) and (11.5′). Denote by $\mathscr{E}_2$ the class of all subsets Y of $\Gamma_n{}^*$ for which $Y \setminus G_n \neq \phi$. Then set $\mathscr{E} = \mathscr{E}_1 \cup \mathscr{E}_2$.

First note that $\{w\} \in \mathscr{E}$ for every $w \in \Gamma_n{}^*$. Indeed, if $w \notin G_n$, then $\{w\} \in \mathscr{E}_2$. If $w \in G_n$, then

$$w = \gamma_1 \cdots \gamma_k , \qquad | \gamma_1 | \supset \cdots \supset | \gamma_n |.$$

Thus, $\{w\}$ has the form (11.3′) with (11.4′) and (11.5′) satisfied. Hence, $\{w\} \in \mathscr{E}_1$.

Next observe that $\mathscr{E}$ is closed with respect to finite unions. To prove that $\mathscr{E}$ is closed with respect to products, consider

$$\underset{\sim}{Q} = YZ, \qquad Y, Z \in \mathscr{E}.$$

If $Q \setminus G_n \neq \phi$ then $Q \in \mathscr{E}_2 \subset \mathscr{E}$. Thus, we may assume that $Q \subset G_n$. This implies $Y \subset G_n$, $Z \subset G_n$ or, equivalently, $Y, Z \in \mathscr{E}_1$. By distributivity, it suffices to consider

$$Y = Y_1 \cdots Y_k , \qquad Y_i \subset \Gamma^*_{A_i}, \qquad A_1 \supset \cdots \supset A_k , \qquad Y_i \neq \{1\}$$

$$Z = Z_1 \cdots Z_l , \qquad Z_j \subset \Gamma^*_{B_j}, \qquad B_1 \supset \cdots \supset B_l , \qquad Z_i \neq \{1\}.$$

Let $y \in Y_k$, $z \in Z_1$, $y \neq 1 \neq z$. Since $YZ \subset G_n$, we have $yz \in G_n$, which implies $A_k \supset B_1$. Thus, $YZ = Y_1 \cdots Y_k Z_1 \cdots Z_l$ has the required form, and hence $\underset{\sim}{Q} \in \mathscr{E}_1$.

Finally, let $T \in \mathscr{E}$ and consider T^*. If $T \in \mathscr{E}_2$, then $T \setminus G_n \neq \varnothing$. Therefore, $T^* \setminus G_n \neq \varnothing$ and $T^* \in \mathscr{E}_2$. Thus we may assume

$$T \in \mathscr{E}_1, \qquad T^* \subset G_n.$$

Let Y and Z be any two (not necessarily distinct) summands of T satisfying (11.4′) and (11.5′). Then $YZ \subset T^* \subset G_n$ and, therefore, by the argument above, $A_k \supset B_1$. Similarly, since $ZY \subset T^* \subset G_n$, we have $B_l \supset A_1$. Consequently, $A_1 = \cdots = A_k = B_1 = \cdots = B_l$. Therefore, T is a rational subset of $\Gamma_A{}^*$ for some A. Hence $T^* \in \mathscr{E}_1$.

Since the class $\mathscr{E}$ is closed under the Kleene operations, and contains the individual elements of $\Gamma_n{}^*$, it follows that it contains all the rational subsets of $\Gamma_n{}^*$. Hence, every rational subset of G_n is in $\mathscr{E}_1$ as required.

References

1. ELGOT, C. C. AND MEZEI, J. E. On relations defined by generalized finite automata. *IBM J. Res. Develop.* **9** (1965).
2. ELGOT, C. C. AND WRIGHT, J. B. Quantifier elimination in a problem of logical design. *Mich. Math. J.* **6** (1959).
3. HILBERT AND BERNAYS. "Grundlagen der Mathematik." Vol. 1, (cf. p. 354). Springer, Berlin, 1934.
4. RABIN, M. O. AND SCOTT, D. Finite automata and their problems. *IBM J. Res. Develop.* **3** (1959).