INFORMATION AND CONTROL 5, 91–107 (1962)

Finite Counting Automata

M. P. SCHÜTZENBERGER*

Harvard Medical School, Boston, Massachusetts

I. INTRODUCTION

The purpose of this note is to define a family $\mathfrak{R}_*$ of sets of words that is, in some sense, the simplest natural generalization of the family $\mathfrak{R}_0'$ of Kleene's (1956) regular events (cf, also, Bar-Hillel and Shamir (1960) and Shepherdson (1959) and below for an abstract definition). However, even if this point of view constitutes the main motivation and if it suggests the terminology, our treatment of the question will be entirely algebraic. In fact this paper can be considered as an attempt towards a classification of the (infinite) monoids of finite dimensional rational matrices which are the semidirect sum of finite monoids. A discussion of these points is to be found in Schützenberger (1962).

The set of F of the so-called *input words* (that is, the *free monoid* F generated by the finite set $X = \{x_i\}$) is assumed to be fixed. We recall that according to Bar-Hillel and Shamir (1960) a *regular event* F' is a subset F' of F such that $\varphi^{-1}\varphi F' = F'$ for some homomorphism φ of F into a finite monoid and our construction hinges upon the algorithm described in the following definition.

DEFINITION. A *finite counting automation* β of order q is the integral valued function of F that is given by:

(i) A finite set of $(q_j + 1)$-tuples $(\alpha_j) = (F'_{j,1}, F'_{j,2}, \cdots, F'_{j,q_j+1})$ of regular events $F'_{j,i}$ $(1 \leqq j \leqq M; q_1, q_2, \cdots, q_M \leqq q)$.

(ii) A polynomial $\bar{\beta}$ (with integral coefficients) in the variates $\alpha_1, \alpha_2, \cdots, \alpha_M$.

For each word f of F, $\beta f = \bar{\beta}(\alpha_1 f, \alpha_2 f, \cdots, \alpha_M f)$ where for each j, $\alpha_j f$ denotes the number of factorizations $f = f_1 f_2 \cdots f_{q_j+1}$ of f into $q_j + 1$ words such that $f_1 \in F'_{j,1}, f_2 \in F'_{j,2}, \cdots, f_{q_j+1} \in F'_{j,q_j+1}$.

(*) This work was done in part at the Department of Statistics of the University of North Carolina, under Contract AF 49 (638)-213 of the United States Air Force, and supported in part by a grant from the Commonwealth Fund.

The functions α_j themselves will be called *counters* and we shall say that β is a *linear finite counting automaton* if $\bar{\beta}$ reduces to a linear combination of the α_j's.

For instance, a counter α of order zero is defined by a single regular event F' and by the rule $\alpha f = 1$ if $f \in F'$, $\alpha f = 0$, otherwise. Hence, here α is, in fact, the *characteristic function* of F'.

Reciprocally, we define the *support* $F'(\beta)$ of the finite counting automaton β as the set of words $F'(\beta) = \{f \in F : \beta f \neq 0\}$.

It is easily verified that any finite counting automaton is equal to a linear one of sufficiently higher order and, denoting by $\mathfrak{R}_q$ the family of the supports of the linear finite counting automata of order q, we shall finally define $\mathfrak{R}_*$ as the union $\bigcup_{q \geqq 0} \mathfrak{R}_q$.

Clearly $\mathfrak{R}_0'$ (the family of regular events) is a subset of $\mathfrak{R}_*$ and it can be shown without difficulty that $\mathfrak{R}_0' = \mathfrak{R}_0$. In order to show that the finite counting automata allow operations exceeding the power of the conventional *one way one tape automata* of Rabin and Scott (1959) it suffices to consider the following example (cf. Elgot (1956)):

Let the regular event F_{x_i} be defined by the condition that the word f belongs to F_{x_i} if and only if its last letter is x_i. The counter of order one α_i, defined by the pair (F_{x_i}, F), enumerates the number of times x_i appears in the input word f. Taking, for instance, $\bar{\beta} = \alpha_1 - \alpha_2$, the corresponding linear counting automaton β is such that f belongs to $F'(\beta)$ if and only if it does not contain as many x_1's as x_2's. Obviously with the same type of counters, but with a polynomial $\bar{\beta}'$ of order three or more, the problem of deciding if $F'(\beta')$ is or is not equal to F (or if it is or is not the complement of a finite set of words) leads to the classical difficulties of diophantine analysis. Hence, there is some interest in obtaining an independent characterization of the parameter q. For this purpose let us say that $\overline{\deg}\ \beta = q'$ if q' is the least integer such that for all nonempty words f the absolute value of βf is bounded by a constant multiple of the q'th power $|f|^{q'}$ of the length $|f|$ of f. It is trivial that $\overline{\deg}\ \beta$ is finite for any finite counting automaton because for any $q'' > 0$ the total number of factorizations of a word f into $q'' + 1$ factors is itself bounded by a constant multiple of $|f|^{q''}$.

Our main result (to be proved in Section II) is that for *any* finite counting automaton β: (i) $\overline{\deg}\ \beta$ is equal to the greatest lower bound of the (not necessarily integral) numbers $r \geqq 0$ such that $\overline{\lim}_{|f| \to \infty} |f|^{-r} |\beta f| = 0$. (ii) There exists a *linear* finite counting automaton identically equal to β whose order is precisely $\overline{\deg}\ \beta$.

In fact each linear finite counting automaton β with $\overline{\deg}\,\beta = q > 0$ is closely associated with an extension by a finite monoid of a free nilpotent group of class at most q (of a free abelian group if $q = 1$). We intend to examine the special case of $\mathfrak{R}_1$ and $\mathfrak{R}_2$ in another paper.

In the last section of this paper we verify that $\mathfrak{R}_*$ is closed with respect to the operations of union, intersection, and set product and, by way of counterexamples, we show that nothing more of Kleene's (1956) theorem remains valid for $\mathfrak{R}_*$.

It may be mentioned that the family $\mathfrak{R}_*$ is a special case of the more general family of sets of words defined in Schützenberger (1961) and that it could be partially characterized by adding the following restriction to (a), (b), $\cdots$ (e) of Schützenberger (1961, p. 245).

(f). The ratio of the amount of information stored in the internal memory to the amount brought to the machine tends to zero with the length of the input word.

In the remainder of this section we reduce our original definition to a simpler form and we prove a few elementary results needed in Section II.

I.1. Every finite counting automaton is equal to a linear one.

PROOF. It is sufficient to prove that if α and α' are two counters, the function β defined by the identity $\beta f = \alpha f \alpha' f$ is equal to a linear finite automaton, and to use induction on the degree of the polynomial $\bar{\beta}$.

Let us recall first that to any finite family $\{F_j'\}$ of regular events F_j' there corresponds an homomorphism φ of the monoid F onto a finite quotient monoid $H = \varphi F$, and a collection $\{H_j'\}$ of subsets of H such that $f \in F_j'$ if and only if $\varphi f \in H_j'$ (Bar-Hillel and Shamir (1960)).

Hence to any counter α defined by a $(q+1)$-tuple $(F_1', F_2', \cdots, F_{q+1}')$ of regular events contained in the family $\{F_j\}$, we can associate the finite set of all the $(q+1)$-tuples $(\alpha_i) = (h_{i_1}, h_{i_2}, \cdots, h_{i_{q+1}})$ of elements of H which are such that

$$h_{i_1} \in H_1', h_{i_2} \in H_2', \cdots, h_{i_{q+1}} \in H_{i_{q+1}}'$$

Then α is equal to the linear finite counting automaton $\sum_i \alpha_i$, where for each i and input word f the counter α_i enumerates the number of distinct factorizations $f = f_1 f_2 \cdots f_{q+1}$ such that

$$\varphi f_1 = h_{i_1}, \varphi f_2 = h_{i_2}, \cdots, \varphi f_{q+1} = h_{i_{q+1}}'$$

Let us say that this factorization is *proper* if none of the words f_i is the empty word. For any $(q+1)$-tuple $(h_1, h_2, \cdots, h_{q+1})$ of elements of $H = F$, we say that the function $\bar{\alpha}$ of F is a φ-counter if it

enumerates the number of proper factorizations with

$$\varphi f_1 = h_1 , \varphi f_2 = h_2 , \cdots , \varphi f_{q+1} = h_{q+1}$$

or, as we shall say, if it enumerates the number of α-factorizations of the input word. It is clear that any of the counters α_i above is equal to the sum of the φ-counters defined by the same $(q + 1)$-tuple and of all the $(2^{q+1} - 2)$ φ-counters defined by the $(q' + 1)$-tuples $(q' < q)$ which result from the deletion of one or of several h_{i_j}'s in $(h_{i_1} , h_{i_2} , \cdots , h_{i_{q+1}})$.

Consequently, it suffices to prove the statement for the special case in which both α and $\bar{\alpha}$ are φ-counters. Then, in fact, the function β enumerates for each word f the number of pairs consisting of a α- and of a α'-factorization of f.

Let us consider an arbitrary monoid G, a $(q + 1)$-tuple $(d) = (g_1 , g_2 , \cdots , g_{q+1})$ and a $(q' + 1)$-tuple $(d') = (g_1' , g_2' , \cdots , g_{q'+1}')$ of elements of G.

We say that $(d'') = (g_1'', g_2'', \cdots , g_{q''+1}'')$ is a *refinement* of (d) and (d') if it has the following properties:

Every g_i of (d) is equal to a product $g_i = g_k''$ or $g_k'' g_{k+1}'' \cdots g_{k'}''$, of consecutive elements of (d''); the same is true for every g_i' of (d'); every $g_{i''}''$ of (d'') is the first factor of a product corresponding to an element of (d) or of (d').

Because of this last condition $q'' \leqq q + q'$ and, consequently, (d) and (d') have only finitely many distinct refinements when G is finite. The same is true when $G = F$, a free monoid, because, e.g., any relation of the form $f = f'f''$ uniquely determines f'' for given f, $f' \in F$.

For instance, if $(d) = (g_1 , g_2)$ and $(d') = (g_1', g_2')$, the set $\{(d'')\}$ of their refinements is empty unless $g_1 g_2 = g_1' g_2'$. If this condition is met, $\{(d'')\}$ consists of the triples (g_1 , g_2'', g_2') with $g_1 g_2'' = g_1'$, $g_2'' g_2' = g_2$ and of the triples (g_1', g_2'', g_2) with $g_1' g_2'' = g_1$, $g_2'' g_2 = g_2'$. If $g_1 = g_1'$ and $g_2 = g_2'$, the set $\{(d'')\}$ contains also the pair (g_1 , g_2).

This definition concludes the proof because β enumerates all the α''-factorizations of f where (α'') is a refinement of (α) and (α') and, consequently, $\beta = \sum \alpha''$ where the summation is over all the φ-counters corresponding to these refinements.

We shall have to consider now and in the following section matrix-valued functions of F. It will always be assumed that the matrices under consideration are finite dimensional matrices with rational entries. The matrix-valued function μ is a *representation* of F if the square matrices μf are such that $\mu f f' = \mu f \mu f'$ identically for all words f and f'; it is a

finite representation if the set $\{\mu f : f \in F\}$ is finite; it is a *representation with bounded denominator* if $p\mu f$ is an integral matrix for some integer p and all words f.

Any entry $\nu_{ii'}$ of a matrix-valued function determines a numerical function $\beta f = (\nu f)_{ii'}$ of F, and the quantity $\overline{\deg}\ \nu$ will be defined as the supremum of the same symbol over all functions determined by the entries of ν.

I.2. To every finite counting automaton β there corresponds at least one representation μ such that β is determined by one of its entries.

PROOF: According to I.1 it is sufficient to prove the statement for a linear finite automaton β of order q.

Let φ be a fixed homomorphism of F onto a finite monoid H, and consider the set α_j $(1 \leqq j \leqq N)$ of all the φ-counters of order at most q. Let the jth coordinate at the vector $v(f)$ be equal to $\alpha_j f$ for each j and $f \in F$. We verify that for each letter x of X there exists a $N \times N$ integral matrix μx such that $v(fx) = v(f)\mu x$ identically.

This is trivial if $q = 0$ and we consider a fixed counter α of order $q > 0$ with $(\alpha) = (h_1, h_2, \cdots, h_{q+1})$. We denote by α' the φ-counter $(h_1, h_2, \cdots, h_q)$ of order $q - 1$ and by α_k'' $(1 \leqq k \leqq K)$ the set of all the φ-counters α_k'' of order q with $(\alpha_k'') = (h_1, h_2, \cdots, h_q, h'')$ where h'' satisfies the condition $h''\varphi x = h_{q+1}$. Since $\alpha fx = \alpha' f + \sum_k \alpha_k'' f$ or $\alpha fx = \sum_k \alpha_k'' f$ according to $\varphi x = h_{q+1}$ or $\varphi x \neq h_{q+1}$, our preliminary result is proved.

Since β is a linear combination of the α_j's, this shows that, in fact, β is determined by an automaton of the family $\mathfrak{A}$ described in the definition 1 of Schützenberger (1961) and the complete result follows from an elementary construction explained in detail in the same paper.

Let μ be a given representation of F. A representation $\bar{\mu}$ of the same dimension will be called a *finite part of order q* of μ if it is a finite representation and if for any $(2q - 1)$-tuple of words $(f_1, f_2, \cdots, f_{2q-1})$ the product

$$\bar{\mu}f_1\mu f_2\bar{\mu}f_3 \cdots \bar{\mu}f_{2i-1}\mu f_{2i}\bar{\mu}f_{2i+1} \cdots \mu f_{2q}\bar{\mu}f_{2q-1}$$

where $\bar{\mu}f_i = \mu f_i - \bar{\mu}f_i$, is identically zero. Thus the hypothesis that $\bar{\mu}$ is a finite part of μ implies that every matrix $\bar{\mu}$ belongs to the radical of the algebra generated by the matrices μx $(x \in X)$. We define Ord μ as the lowest possible order of a finite part of μ with the convention that Ord μ is infinite if μ has no finite part of finite order.

I.3. If Ord μ is finite, every function of F determined by an entry of μ

is equal up to a constant factor to a linear finite counting automaton whose order is at most Ord μ.

PROOF: If Ord $\mu = 0$, the statement is trivial because the hypothesis amounts to the assumption that μ itself is finite and we can assume now that $0 < q = \text{Ord } \mu$.

We consider an homomorphism φ of F onto the quotient monoid H that is defined by the following conditions:

(i) $\varphi f \neq \varphi e$ if f is not the empty word e.

(ii) For all $f, f' \in F$ and $x, x' \in X$, $\varphi fx = \varphi f'x' = h$, say if and only if $\bar{\mu}f\mu x = \bar{\mu}f'\mu x'$ and $\bar{\mu}fx = \bar{\mu}f'x'$.

By hypothesis H is a finite monoid. We define a representation μ (with finite part $\bar{\mu}$) of $H = \{h\}$ by setting $\mu h = \bar{\mu}f\mu x$ and $\bar{\mu}h = \bar{\mu}fx$. To every $(q+1)$-tuple $(\alpha) = (h_1, h_2, \cdots, h_{q'+1})$ of elements of H we associate the matrix

$$\mu\alpha = \bar{\mu}h_1\bar{\mu}h_2 \cdots \bar{\mu}h_i \cdots \bar{\mu}h_{q'}\bar{\mu}h_{q'+1}$$

where, of course, $\bar{\mu} = 0$ and $\bar{\mu}e =$ the unit matrix. Let now $f = x_1x_2 \cdots x_n$ be an arbitrary word expressed as a product of the generators. Since $\mu = \bar{\mu} + \bar{\mu}$ we have

$$\mu f = (\bar{\mu}x_1 + \bar{\mu}x_1)(\bar{\mu}x_2 + \bar{\mu}x_2) \cdots (\bar{\mu}x_n + \bar{\mu}x_n).$$

Developing this expression and observing that on the one hand $\bar{\mu}$ is a representation and on the other hand any product containing $q+1$ matrices $\bar{\mu}$ is zero, we obtain μf as a sum of terms of the form

$$\bar{\mu}f_1\bar{\mu}x_1\bar{\mu}f_2\bar{\mu}x_2 \cdots \bar{\mu}f_{q'}\bar{\mu}x_{q'}\bar{\mu}f_{q'+1}$$

with $q' \leqq q$. Clearly each of these terms is equal to some matrix $\mu\alpha$ as defined above and, more accurately, we have the identity $\mu f = \sum \alpha f \mu\alpha$ where the summation is over all the counters α of order at most q defined above.

Since the set of all these matrices $\mu\alpha$ is finite, it is trivial that $K\mu f$ is an integral matrix for all f of F and some fixed integer K and the result is proved.

If φ is any homomorphism of F onto a finite monoid we say that the $(2p+1)$-tuple $(s) = (f_1, f_2, \cdots, f_{2p+1})$ of elements of F is *φ-special* if for each $i = 1, 2, \cdots, p$

$$\varphi f_{2i-1}f_{2i} = \varphi f_{2i-1}, \varphi f_{2i}^2 = \varphi f_{2i}, \varphi f_{2i}f_{2i+1} = f_{2i+1}.$$

Since φf is finite, there corresponds to any $(s') = (f_1', f_2', \cdots, f_{2p+1}')$

a finite positive inter a such that

$$(s) = (f_1 f_2'^b, f_2'^a, f_2'^b f_3' f_4^b, f_4'^a, \cdots, f_{2p}'^a, f_{2p}'^b f_{2p+1}')$$

is φ-special for all large enough b.

Also we shall use the abbreviation $s^{(k)}$ for denoting the word $f_1 f_2^k f_3 f_4^k \cdots f_{2p}^k f_{2p+1}$.

I.4. If Ord $\mu = q$ is finite and if (s) is φ-special, there exists $q+1$ matrices ${}_0\underline{\mu}s, {}_1\underline{\mu}s, \cdots, {}_q\underline{\mu}s$ such that for all k

$$\mu s^{(k)} = \sum_{0 \leqq j \leqq q} k^j {}_j\underline{\mu}s$$

PROOF. By straightforward computation using the development of $\mu s^{(k)}$ as a product of matrices $\bar{\mu}$ and $\bar{\bar{\mu}}$.

I.5. If $0 < Ord\ \mu < \infty$, μ is equivalent to a representation of the form $\begin{pmatrix} \mu' & \nu \\ 0 & \mu'' \end{pmatrix}$ where μ' is a finite representation and μ'' a representation with $Ord\ \mu'' = Ord\ \mu - 1$.

Reciprocally, if the representation μ is in the semireduced form

$$\mu = \begin{pmatrix} \mu' & \nu \\ 0 & \mu'' \end{pmatrix}$$

then $Ord\ \mu \leqq Ord\ \mu' + Ord\ \mu'' + 1$.

PROOF: Let V denote the set of all the vectors v such that for all words f', $f''\bar{\mu}f'\mu f''v = 0$.

Because of the hypothesis that μ admits a finite part $\bar{\mu}$ of order $q = \text{Ord}\ \mu < \infty$, V is not empty and, after performing a suitable linear transformation, we can assume that V consists of all the vectors having their M last coordinates zero. Then, since for all f', $f'' \in F$ and $v \in V$ one has $\mu f''v \in V$ and $\bar{\mu}f'v = 0$, μ and $\bar{\bar{\mu}}$ have, respectively, the forms

$$\mu = \begin{pmatrix} \mu' & \nu \\ 0 & \mu'' \end{pmatrix} \quad \text{and} \quad \mu = \begin{pmatrix} 0 & \nu' \\ 0 & \bar{\mu}'' \end{pmatrix}$$

where μ' and μ'' are representations and where $\dim \mu'' = M$.

It follows that $\bar{\mu} = \mu - \bar{\mu}$ has the form

$$\begin{pmatrix} \mu' & \nu - \nu' \\ 0 & \mu'' - \bar{\mu}'' \end{pmatrix}$$

and, since it is a finite representation, the same is true of μ'.

Observe now that the module V^* spanned by all the row vectors of

all the matrices $\bar{\mu}f'\mu f''(f', f'' \in F)$ consists of the vectors having their first $N-M$ coordinates zero where $N = \dim \mu$ is strictly larger than M because of the hypothesis that $0 < \operatorname{Ord} \mu$.

Direct computation shows that any product $\bar{\mu}f_1\mu f_2\bar{\mu}f_3 \cdots \mu f_{2q-2}\bar{\mu}f_{2q-1}$ has the form $\begin{pmatrix} 0 & \mathbf{n} \\ 0 & \mathbf{m} \end{pmatrix}$ where $\mathbf{n} = \nu' f_1\mu'' f_2\,\mathbf{m}'$, $\mathbf{m} = \bar{\mu}'' f_1\mu' f_2\mathbf{m}'$ and $\mathbf{m}' = \bar{\mu}'' f_3\mu''\bar{\mu}f_4'' f_5 \cdots \mu'' f_{2q-2}''\bar{\mu}f_{2q-1}$. Because of our remark above on V^*, the condition that $\mathbf{n} = \mathbf{m} = 0$ identically, which is implied by $\operatorname{Ord} \mu = q$, implies itself that $\mathbf{m}' = 0$ identically, that is, finally, that $\operatorname{Ord} \mu'' = q - 1$ and the direct part of the statement if proved.

With respect to the second part of the statement, it suffices to prove it for $\operatorname{Ord} \mu' = 0$ and to apply induction on $\operatorname{Ord} \mu$. However, if $\operatorname{Ord} \mu' = 0$ we can use the notations introduced above and the hypothesis that $\operatorname{Ord} \mu'' = q - 1$ implies that the matrix $\mathbf{m}'$ is identically zero. Hence, the matrices $\mathbf{m}$ and $\mathbf{n}$ are also identically zero and consequently $\operatorname{Ord} \mu \leqq q$. This concludes the proof of I.5.

II. VERIFICATION OF THE MAIN PROPERTY

Let ν be any matrix valued function of F. If

$$\overline{\lim}_{k\to\infty} |s^{(k)}|^{-1} \mid \nu s^{(k)} \mid = 0$$

for any $(2p + 1)$-tuple (s) (and $s^{(k)}$ defined as in I.4), we write $\underline{\deg}\ \nu = 0$. If it is not so, there exists a largest integer q (possibly $q = \infty$) such that there exists an integer p and a $(2p + 1)$-tuple (s) for which $\overline{\lim}_{k\to\infty} \mid s^{(k)} \mid^{-q} \mid \nu s^{(k)} \mid \neq 0$. Then we write $\underline{\deg}\ \nu = q$ and we say that (s) is *effective* for ν. Necessarily $\underline{\deg}\ \nu \leqq \overline{\deg}\ \nu$ and, if these two parameters are equal, their common values is the greatest lower bound of the numbers $r \geqq 0$ such that $\overline{\lim}_{|f|\to\infty} |f|^{-r} \mid \nu f \mid = 0$.

As for the symbols $\overline{\deg}$ and Ord, it is trivial that $\underline{\deg}\ \mu = \underline{\deg}\ \mu'$ for any representation μ' equivalent to μ.

Finally, let it be observed that (with the notations of I.4) $\underline{\deg}\ \mu$ can be defined as the largest q' such that ${}_{q'}\underline{\mu s} \neq 0$ for some $\bar{\mu}$-special $(2p + 1)$-tuple (s). Indeed, under these last conditions $\overline{\lim}_{k\to\infty} \mid s^{(k)} \mid^{-q'} \mid \mu s^{(k)} \mid$ is proportional to ${}_{q'}\underline{\mu s}$. Reciprocally, given any effective $(2p + 1)$-tuple (s') we can choose the integers a and b in such a way that $(s) = (f', f_2'^b, f_2'^a, \cdots f_{2p}'^a, f_{2p}'^a f_{2p+1}')$ is both effective and φ-special for any fixed φ and in particular for $\varphi = \bar{\mu}$.

In order to simplify the proof of the main property II.4, we verify it separately in the special case of $\overline{\deg}\ \mu = 0, 1$. Our first and fundamental preliminary result is a modified version of a classical theorem of Burnside (1911, note j).

II.1. The three following conditions on a rationally irreducible representation μ with bounded denominator are equivalent:

(i) *Ord* $\mu = 0$.

(ii) *For all* $f, f', f'' \in F$ *and,* $\epsilon > 0$, $\overline{\lim}_{k\to\infty}(1 - \epsilon)^k \mid \mu f' f^k f'' \mid = 0$.

(iii) *The set* $\{\mathrm{Tr}\ \mu f : f \in F\}$ *is finite.*

PROOF: (i)⇒(ii). The condition (i) is equivalent to the condition that μ is a finite representation. Hence, it implies that $\underline{\deg}\ \mu = \overline{\deg}\ \mu = 0$. Since, trivially, $\underline{\deg}\ \mu = 0$ implies (ii) the result is proved.

(ii)⇒(iii). For any $f \in F$ and k, $\mathrm{Tr}\ \mu f^k$ is the sum of the kth powers of the characteristic roots ρ_j of μf. Hence, (ii) implies that for all $\epsilon > 0$, $\overline{\lim}_{k\to\infty} \sum_j \rho_j{}^k (1 - \epsilon)^k = 0$ and, consequently, that $\mid \rho_j \mid \leqq 1$ for every root ρ_j. It follows that $\mid \mathrm{Tr}\ \mu f \mid \leqq \sum_j \mid \rho_j \mid \leqq \dim \mu$, a bounded quantity. Since by hypothesis $\mathrm{Tr}\ \mu f$ is a rational number with bounded denominator, the implication (ii)⇒(iii) is proved.

(iii)⇒(i). Let $\{f_j\}\ (1 \leqq j \leqq N' \leqq N^2)$ be a basis of the module $\mathfrak{M}$ over the rationals spanned by all the matrices $\mu f (f \in F)$ and write $f' \equiv f''$ if and only if for all $j = 1, 2, \cdots, N'$ one has $\mathrm{Tr}\ \mu f' f_j = \mathrm{Tr}\ \mu f'' f_j$. The condition (iii) implies that the equivalence $\equiv$ has only finitely many classes and it suffices to verify that in fact $f' \equiv f''$ only if $\mu f' - \mu f'' = 0$.

Indeed, let $\mathfrak{M}'$ be the module of all matrices m' of $\mathfrak{M}$, such that for all $m \in \mathfrak{M}$, $\mathrm{Tr}\ m'm = 0$. By definition, for any $m' \in \mathfrak{M}'$, $m \in \mathfrak{M}$ and k, $\mathrm{Tr}\ m'^k m = 0$ and, consequently, all the characteristic roots of $m'm$ are zero. Hence, for given $m' \in \mathfrak{M}'$, there exists no $m \in \mathfrak{M}$ such that the first row of $m'm$ is the vector $(1, 0, 0, \cdots, 0)$. Since the representation μ is assumed to be irreducible, this shows that the first row of m' is the zero vector. The same remark applies to any row of any matrix of $\mathfrak{M}'$ and it shows that this set reduces to the zero matrix. By definition, $f' \equiv f''$ only if $\mu f' - \mu f'' \in \mathfrak{M}'$ and the proof of (iii)⇒(i) (and, consequently, of I.1) is completed.

Let us consider a representation $\mu = \begin{pmatrix} \mu' & \nu \\ 0 & \mu'' \end{pmatrix}$ such that $\bar{\mu} = \begin{pmatrix} \mu' & 0 \\ 0 & \mu'' \end{pmatrix}$ is a finite representation. If v is any vector, it follows from I.5 that the vector valued function μv (defined as $\mu f v$ for each f of F) satisfies the

inequality $\underline{\deg}\ \mu v \leqq \overline{\deg}\ \mu v \leqq \operatorname{Ord} \mu = 0$ or $= 1$. There is no loss in generality in assuming that after a suitable linear transformation $V = \{v : \underline{\deg}\ \mu v = 0\}$ consists of the vectors having their last M coordinates zero where, possibly, $M = 0$. We say then that μ is in *standard form.*

II.2. Under the hypothesis stated

$$\mu'' = \begin{pmatrix} \mu_0'' & \nu_0'' \\ 0 & \mu_1 \end{pmatrix} \quad \text{and} \quad \mu = \begin{pmatrix} \mu' & \nu_0' & \nu_1' \\ 0 & \mu_0'' & \nu_0'' \\ 0 & 0 & \mu_1 \end{pmatrix}$$

where both $\mu_0 = \begin{pmatrix} \mu' & \nu_0' \\ 0 & \mu_0'' \end{pmatrix}$ *and* μ_1 *are finite representations with dim* $\mu_1 = M$.

PROOF. By hypothesis the monoid $\bar{\mu}F = \{\bar{\mu}f : f \in F\}$ has a finite number H of elements. If the triple of words $(t) = (f', f, f'')$ is such that $\bar{\mu}f'f = \bar{\mu}f'$, $\bar{\mu}ff'' = \bar{\mu}f''$, $|f| > 0$ we write $(t) \in T$ (or $\in T_{\bar{\mu}}$).

Trivially, any word g of F of length $|g| > H^2$ admits at least one factorization $g = g_1g_2g_3$ with $(g_1, g_2, g_3) \in T$. Direct computation shows that if $(t) = (f', f, f'') \in T$, the matrix $\mu t^{(k)} = \mu f'f^k f''$ is equal to $\mu t^{(0)} = \mu f'f''$ plus k times the matrix $\begin{pmatrix} 0 & \nu t \\ 0 & 0 \end{pmatrix}$ where, by definition, $\nu t = \mu' f' \nu f \mu'' f''$.

It follows that either $\nu t' = 0$ for all (t') of T and, then, the monoid μF contains at most H^2 distinct elements or, otherwise, $\nu t' \neq 0$ for at least one $(t') \in T$ (which is an *effective* triple) and $\underline{\deg}\ \mu = \overline{\deg}\ \mu = \operatorname{Ord} \mu = 1$. More generally, for any fixed vector w, either $\begin{pmatrix} 0 & \nu t \\ 0 & 0 \end{pmatrix} w = 0$ for all (t) of T and then the set $\{\mu f w : f \in F\}$ contains at most H^2 distinct vectors, or, otherwise, $\underline{\deg}\ \mu w = 1$.

Thus, we can assume now that $M > 0$ and, trivially, $M \leqq \dim \mu''$ since μ' is a finite representation. According to the definition of V, it follows that μ has the form

$$\begin{pmatrix} \mu' & \nu_0' & \nu_1' \\ 0 & \mu_0'' & \nu_0'' \\ 0 & \mu'' & \mu_1 \end{pmatrix}$$

where the following conditions are satisfied:

(i) $\dim \mu_1 = M$;

(ii) The module spanned by all the row vectors of all the matrices

$\nu_1' t$ ($(t) \in T$) has rank equal to its dimension M;

(iii) $\nu_0' t = 0$ for all (t) of T.

Observe now that for any $f''' \in F$ and $(t) = (f', f, f'') \in T$ the triple $(f') = (f', f, f''f''')$ also belongs to T. Consequently, since $\nu_0' t' = \nu_1' t \mu''' f''' = 0$ by (iii), it follows from (ii) that μ''' is identically zero. Since we have seen that $\{\nu_0' f : f \in F\}$ is a finite set, the proof of II.2 is completed.

II.3. Let the representation

$$\mu = \begin{pmatrix} \mu_0 & \nu_1 & \nu_3 \\ 0 & \mu_1 & \nu_2 \\ 0 & 0 & \mu_2 \end{pmatrix}$$

be in the standard form of II.2 with:

$$\mu_0 \to \begin{pmatrix} \mu' & \nu_0' \\ 0 & \mu_0'' \end{pmatrix}, \quad \nu_1 \to \begin{pmatrix} \nu_1' \\ \nu_0'' \end{pmatrix}, \quad \mu_1 \to \mu_1$$

and satisfy the conditions:

$$\underline{\deg} \begin{pmatrix} \mu_0 & \nu_1 \\ 0 & \mu_1 \end{pmatrix} = \operatorname{Ord} \begin{pmatrix} \mu_0 & \nu_1 \\ 0 & \mu_1 \end{pmatrix} = 1; \quad \underline{\deg}\, \mu_2 < \underline{\deg} \begin{pmatrix} \mu_1 & \nu_2 \\ 0 & \mu_3 \end{pmatrix} (= q < \infty).$$

Then $\underline{\deg}\, \mu \geqq q + 1$.

PROOF: According to the remarks made at the beginning of this section, (ii) implies that $\begin{pmatrix} \mu_1 & \nu_2 \\ 0 & \mu_3 \end{pmatrix}$ admits at least one effective $(2p + 1)$-tuple $(s) = (f_1, f_2, \cdots, f_{2p+1})$ which is $\bar{\mu}$-special. Thus, $\underline{\deg}\, \mu \geqq q + 1$ unless ${}_j\mu s = 0$ for all $j \geqq 0$ as we shall assume now. Then, by hypothesis,

$${}_q\mu s = \begin{pmatrix} 0 & \mathbf{n}_1' & \mathbf{n}_3' \\ 0 & 0 & \mathbf{n}_2' \\ 0 & 0 & 0 \end{pmatrix}$$

with $n_2' \neq 0$.

Because of the hypothesis that $\begin{pmatrix} \mu_0 & \nu_1 \\ 0 & \mu_1 \end{pmatrix}$ is in standard form, there exists at least one triple $(t') = (g_1, g_2', g_3)$ satisfying the conditions of II.2 which is such that $\nu t' \mathbf{n}_2 \neq 0$. By taking c large enough we can deduce from (t') a triple $(t) = (g_1, g_2 = g_2'^c, g_3)$ which is $\bar{\mu}$-special

and for which we have

$$_1\underline{\mu t} = \begin{pmatrix} 0 & \mathbf{n}_1 & \mathbf{n}_3 \\ 0 & 0 & \mathbf{n}_2 \\ 0 & 0 & \mathbf{m}_1 \end{pmatrix}$$

with $\mathbf{n}_1\mathbf{n}_2 = c\nu_1' t\mathbf{n}_2 \neq 0$.

We claim that by a suitable choice of $a, b > 0$ the $(2p + 3)$-tuple $(u) = (g_1, g_2^a, g_3 f_1, f_2^b, f_3, \cdots, f_{2i}^b, \cdots, f_{2p+1})$ which is $\bar{\mu}$-special by construction, satisfies the inequality ${}_{q+1}\underline{\mu} u \neq 0$ from which the result instantly follows.

Indeed, we have $\mu u^{(k)} = \sum_{0 \leqq j''} k^{j''} (\sum_{j+j'=j''} a^j b^{j'} {}_j\underline{\mu t}_{j'} \underline{\mu} s)$ and, because of the linear independence of the monomials $a^j b^{j'}$, it suffices to show that ${}_j\underline{\mu t}_{j'} \underline{\mu} s \neq 0$ for at least one pair (j, j') such that $q + 1 = j + j'$. Since for $j = 1$ and $j' = q$ we have

$$_1\underline{\mu t}_q \underline{\mu} s = \begin{pmatrix} 0 & 0 & \mathbf{n}_1\mathbf{n}_2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \neq 0,$$

the statement II.3 is proved.

II.4. If μ is a representation with bounded denominator, then $\underline{\deg}\ \mu = \overline{\deg}\ \mu = \mathrm{Ord}\ \mu$. Furthermore, if $q = \mathrm{Ord}\ \mu$ is finite, μ has an effective $(2q + 1)$-tuple which is $\bar{\mu}$-special for some finite part $\bar{\mu}$ of order q of μ.

PROOF: Since $\underline{\deg} \leqq \overline{\deg} \leqq \mathrm{Ord}$, trivially, we have only to prove that $\underline{\deg} \geqq \overline{\deg}$ and $\overline{\deg} \geqq \mathrm{Ord}$. The proof is by induction on $\dim \mu$, the initial case being trivial.

If μ is irreducible, the result has already been proved in II.1 since this remark shows that $\underline{\deg}\ \mu = \overline{\deg}\ \mu = \mathrm{Ord}\ \mu = 0$ or $=$ infinity. In the latter case, the condition (ii) of II.1 shows that there exists an effective triple.

Consequently, we can assume now that $\mu = \begin{pmatrix} \mu_0 & \nu_0 \\ 0 & \mu_1 \end{pmatrix}$ with $\dim \mu_0 > 0$ where μ_0 is irreducible and where (by I.5 and the induction hypothesis) $\underline{\deg}\ \mu_1 = \overline{\deg}\ \mu_1 = \mathrm{Ord}\ \mu_1 = \overline{\deg}\ \mu$ or $= \overline{\deg}\ \mu - 1$. Again the result is trivial unless $q = \deg \mu$ is finite as we shall always assume it now.

If μ_1 is a finite representation (in particular if it is irreducible), the result is already proved by II.2 which shows that $\underline{\deg}\ \mu = \overline{\deg}\ \mu = \mathrm{Ord}\ \mu = 1$ or $= 0$ according as there exists or not an effective triple.

Consequently, we can assume that Ord $\mu_1 = q_1 > 0$ and, by I.5, that

$$\mu_1 = \begin{pmatrix} \mu_{10} & \nu_{11} \\ 0 & \mu_{11} \end{pmatrix}$$

where Ord $\mu_{10} = 0$ and Ord $\mu_{11} = q_1 - 1$.

Then, μ has the form

$$\begin{pmatrix} \mu_0 & \nu_{00} & \nu_{01} \\ 0 & \mu_{10} & \nu_{11} \\ 0 & 0 & \mu_{11} \end{pmatrix}$$

and, by applying II.2, we can bring $\begin{pmatrix} \mu_0 & \nu_{00} \\ 0 & \mu_{10} \end{pmatrix}$ into standard form. Thus, finally, μ has the form

$$\mu = \begin{pmatrix} \mu_0 & \nu_{000} & \nu_{001} & \nu_{011} \\ 0 & \mu_{100} & \nu_{100} & \nu_{110} \\ 0 & 0 & \mu_{101} & \nu_{111} \\ 0 & 0 & 0 & \mu_{11} \end{pmatrix} = \begin{pmatrix} \mu_0' & \nu_0' \\ 0 & \mu_1' \end{pmatrix}$$

where dim $\mu_{101} = 0$ if and only if $\underline{\deg} \begin{pmatrix} \mu_0 & \nu_{00} \\ 0 & \mu_{10} \end{pmatrix}$ is 0. In any case, we have $\mu_0' = \begin{pmatrix} \mu_0 & \nu_{000} \\ 0 & \mu_{100} \end{pmatrix}$ = a finite representation, $\mu_1' = \begin{pmatrix} \mu_{101} & \nu_{111} \\ 0 & \mu_{100} \end{pmatrix}$ = a representation with Ord $\mu_1' = q_1$ or $q_1 - 1$.

Let us distinguish the two possibilities:

(i) μ_1' admits a finite part $\bar{\mu}_1'$ of order $q_1 - 1$. Then $\begin{pmatrix} \bar{\mu}_0' & 0 \\ 0 & \bar{\mu}_1' \end{pmatrix}$ is a finite part of order q_1 of μ. Since Ord $\mu \geqq \overline{\deg}\ \mu = q$, this shows that $q_1 = q$. Hence, trivially, Ord $\mu = \overline{\deg}\ \mu$ and by the induction hypothesis $\underline{\deg}\ \mu_1 = q$ with an effective $(2q + 1)$-tuple of the required type. Since $\underline{\deg}\ \mu$ is at most equal to q and at least equal to $\underline{\deg}\ \mu_1$, the double equality is proved.

(ii) Ord $\mu_1' = q_1$. Since Ord $\mu_{11} = q_1 - 1$, by construction, we have surely dim $\mu_{101} \neq 0$ and we can apply II.3 with the correspondence $\mu_0' \to \mu_0$, $\mu_{101} \to \mu_2$ and $\mu_{11} \to \mu_3$. This shows that $\underline{\deg}\ \mu \geqq q_1 + 1$ and consequently, $q_1 = q - 1$. It follows that $\underline{\deg}\ \mu = \overline{\deg}\ \mu = q$ with the required type of effective $(2q + 1)$-tuple. Furthermore, μ_1 admits a finite part $\bar{\mu}_1$ of order $q - 1$ and, consequently, $\begin{pmatrix} \mu_0 & 0 \\ 0 & \bar{\mu}_1 \end{pmatrix}$ is a finite part

of μ of order at most q. This proves the double equality in the second case and it concludes the proof of the main property.

III. TWO COUNTEREXAMPLES

It has been seen in I.1 that any finite counting automaton is equal to a linear one of sufficiently higher order. Our first counter example is intended to show that, of course, the converse proposition is not true.

III.1. There exists at least one linear counting automaton of order two such that its support cannot be the support of any finite counting automaton of order one.

PROOF: Let the regular events Fx_i and x_iF be defined by the condition that f belongs to Fx_i (respectively to x_iF) if and only if its last letter (respectively its first letter) is x_i. Assume for simplicity that $X = \{y, z\}$ and define $\beta = \alpha - \alpha'$ where $(\alpha) = (Fy, F, zF)$ and $(\alpha') = (Fz, F, yF)$. Direct computation shows that if $f_i = y^iz$, $f_j = y^jz$, $i \neq j$ there exists for every $p > 0$ at least one word f' and integer k such that $\beta f_i f_i^{kp} f_j^{kp} f_i f' = 0$ and $\beta f_i f_j^{kp} f_i^{kp} f_j f' \neq 0$.

Let now β' be a finite counting automaton of order one defined by a polynomial function of the linear finite counting automata $\beta_i (i = 1, 2, \cdots, M)$ of order one. Using the notations of II.2, we assume that each β_i is determined by an entry of a representation μ_i admitting a finite part $\bar{\mu}_i$ of order one. Hence, there exists an homomorphism φ such that $\varphi f = \varphi f'$ if and only if $\bar{\mu}_i f = \bar{\mu}_i f'$ for $i = 1, 2, \cdots, M$ and φF is a finite monoid.

Trivially, if $\varphi f = \varphi f'$, there exists a finite p such that for each i, $\mu_i f^p$ is idempotent and direct computation shows that $\mu_i f f^{kp} f' f^{kp} f' = \mu_i f f'^{kp} f^{kp} f'$, hence $\beta f f^{kp} f'^{kp} f' = \beta f f'^{kp} f^{kp} f'$, for every k.

However, the words f_i considered above constitute an infinite family of words which, pairwise, do not satisfy this relation whence the conclusion follows instantly.

We now prove the closure properties of $\mathfrak{R}_*$.

III.2. The family of the supports of the finite counting automata of order at most q is closed under intersection and union.

PROOF: Let β and β' be two finite counting automata of order at most q. According to the very definition of this algorithm, the function β'' and β''' of F defined respectively by the identities $\beta'' f = \beta f \beta' f$ and $\beta''' f = (\beta f)^2 + (\beta' f)^2$ are also finite counting automata of order at

most q and we have

$$F'(\beta'') = \{f \in F : \beta f \beta' f \neq 0\} = F'(\beta) \cap F'(\beta')$$

$$F'(\beta''') = \{f \in F : (\beta f)^2 + (\beta' f)^2 \neq 0\} = F'(\beta) \cup F'(\beta'').$$

III.3. The family $\mathfrak{R}_*$ is closed under set product.

PROOF: Observe that if $(\alpha') = (F_1', F_2', \cdots, F_{q'}')$ and $(\alpha'') = (F_1'', F_2'', \cdots, F_{q''}'')$ define the two counters α' and α'', the $(q' + q'')$-tuple (α''') of regular events $(\alpha''') = (F_1', F_2', \cdots, F_{q'}', F_1'', F_2'', \cdots, F_{q''}'')$ defines a counter α''' which satisfies the convolution identity $\alpha''' f = \sum \{\alpha' f' \alpha'' f'' : f' f'' = f\}$.

Since the convolution product is distributive over the addition, we can associate to any pair of finite counting automata β' and β'' a third finite counting automaton β''' such that $\beta''' f = \sum \{(\beta' f')^2 (\beta'' f'')^2 : f' f'' = f\}$, identically, and the result is proved since, by construction, $F'(\beta''') = F'(\beta') F'(\beta''')$.

It has been shown elsewhere (Schützenberger (1961, counterexamples II.2 and II.3)) that the family of the sets of the form

$$\bar{F}(\beta) = F - F'(\beta) = \{f \in F : \beta f = 0\}$$

is distinct from $\mathfrak{R}_*$ and that it is *not* closed under the formation of set products.

III.4. For each $q > 0$, $\mathfrak{R}_{q-1} \neq \mathfrak{R}_q$ and, consequently, $\mathfrak{R}_*$ is not closed under Kleene's star operation $*$.

PROOF: Let again $X = \{y, z\}$ and define the following regular events:

$$Y^* = \{y, y^2, \cdots, y^n, \cdots\}, \qquad Z^* = \{z, z^2, \cdots, z^n, \cdots\}$$

$$G_q = (Y^* Z^*)^q \text{ (with } G_0 = \{e\}).$$

Hence, $f \in G_q$ if and only if $f = y^{k_1} z^{k_1'} \cdots y^{k} p z^{k_p'} \cdots y^{k_q} z^{k_q'} = g^{(K)}$, say, where all the coordinates $k_1, k_1', \cdots, k_q, k_q'$ of the vector K are positive integers.

If (α_p) denotes the pair $(G_p(Y^* \cup \{e\}), G_{q-p})$ of regular events, it is clear that the corresponding counter α_p of order one is such that $\alpha_p f = k_p$ if $p \in G_q$, $\alpha_p f = 0$, otherwise. A similar construction holds for k_p' and it follows that the following function β_q is a linear finite counting automata of order q:

$$\beta_q f = 0 \text{ if } f \text{ is not in } G_q;$$

$$\beta_q f = (k_1 - k_1')(k_2 - k_2') \cdots (k_q - k_q') \quad \text{if} \quad f = g^{(K)}.$$

Hence, f belongs to $F'(\beta_q)$ in all cases except if $f \in G_q$ and if $k_p = k_p'$ for some pair of coordinates of K. We show that $F'(\beta)$ does not belong to $\mathfrak{R}_{q-1}$.

Indeed, by II.4 any linear finite counting automaton β' of order q' is determined by some entry of a matrix representation μ of F admitting a finite part $\bar{\mu}$ of order q'.

For suitable integers a and b the $(4q + 1)$-tuple $(s) = (y^b, y^a, y^b z^b, z^a, z^b y^b, \cdots, y^b z^b, z^a, z^b)$ is $\bar{\mu}$-special and for any vector $\bar{K}$ the word $s^{(\bar{K})} = y^{2b+a\bar{k}_1} z^{2b+a\bar{k}_1'} \cdots y^{2b+a\bar{k}_q} z^{2b+a\bar{k}_q'}$ is equal to $g^{(K)}$ where $K = 2bU + a\bar{K}$ with $U = (1, 1, \cdots 1)$.

Consequently, according to I.3, $\beta' s^{(K)}$ is a polynomial, say $b'(\bar{K})$, of degree at most Ord β' in the coordinate of $\bar{K}$. Now, if $F(\beta') = F(\beta_q)$ they have the same intersection with the set $\{s^{(\bar{K})}\}$ and, consequently, $b'(\bar{K})$ must be zero whenever $k_i = k_i'$ for some $i \leqq q$. Hence $b'(\bar{K})$ has degree at least q since it admits the product $(\bar{k}_1 - \bar{k}_1')(\bar{k}_2 - \bar{k}_2') \cdots (\bar{k}_q - \bar{k}_q')$ as a factor.

This concludes the proof that if $F(\beta') = F(\beta_q)$ then $F(\beta')$ is not contained in $\mathfrak{R}_{q-1}$.

We have seen that $G_1 = Y^* Z^*$ belongs to $\mathfrak{R}_1$ and by definition $G_1^* = \cup\{G_q : q > 0\}$.

By the same argument as above it follows that $F(\beta')$ cannot be equal to G_1^* if β' has a finite order since this would imply that $\bar{b}'(\bar{K})$ has infinite degree. Thus, $\mathfrak{R}_*$ is not closed under Kleene's star operation.

Of course for any set F' of $\mathfrak{R}_*$ it is possible to construct a *finite* dimensional integral representation μ of F such that a word f belongs to F'^* if and only if some fixed entry of μf is not zero [cf. Schützenberger (1961), p. 258 and 265]. Thus, as a byproduct, we have obtained the result that $\mathfrak{R}_*$ is a proper subfamily of the family of the sets words accepted by the automata of $\mathfrak{A}$.

RECEIVED January 23, 1962

REFERENCES

BAR-HILLEL, Y., AND SHAMIR, E. (1960). *Bull. Research Council Israel* **8F**, 155.

BURNSIDE, W. (1911). "Theory of Groups of Finite Order," 2nd ed. Cambridge Univ. Press.

ELGOT, C. C. (1960). *Trans. Am. Math. Soc.* **9?**, 61.

KLEENE, S. C. (1956). *In* "Automata Studies." Princeton Univ. Press, Princeton, New Jersey.

RABIN, M., AND SCOTT, D. (1959). *I.B.M. J. Research* **3**, 114.

SCHÜTZENBERGER, M. P. (1961). *Information and Control* **4**, 245.

SCHÜTZENBERGER, M. P. (1962). Certain elementary families of automata. *Proc. Polytech. Inst. Brooklyn. Symposium on Math. Theory of Automata.*

SHEPHERDSON, J. C. (1959). *I.B.M. J. Research* **3**, 198.