INFORMATION AND CONTROL 4, 245-270 (1961)

On the Definition of a Family of Automata*

M. P. Schützenberger

Faculté des Sciences (Poitiers) and University of North Carolina, Chapel Hill, N.C.

I. INTRODUCTION

In this note we discuss the definition of a family α of automata derived from the family α_0 of the finite one-way one-tape automata (Rabin and Scott, 1959).

In loose terms, the automata from α are among the machines characterized by the following restrictions:

- (a) Their output consists in the acceptance (or rejection) of input words belonging to the set F of all words in the letters of a finite alphabet X.
- (b) The automaton operates sequentially on the sucessive letters of the input word without the possibility of coming back on the previously read letters and, thus, all the information to be used in the further computations has to be stored in the internal memory.
- (c) The unbounded part of the memory, V_N , is the finite dimensional vector space of the vectors with N integral coordinates; this part of the memory plays only a passive role and all the control of the automaton is performed by the finite part.
- (d) Only elementary arithmetic operations are used and the amount of computation allowed for each input letter is bounded in terms of the total number of additions and subtractions.
- (e) The rule by which it is decided to accept or reject a given input word is submitted to the same type of requirements and it involves only the storage of a finite amount of information.

Thus the family α is a very elementary modification of α_0 and it is not

^{*} This work has been done in part at the Department of Statistics of the University of North Carolina under contract number AF 49 (638)-213 of the United States Air Force.

claimed that it relates usefully to the Turing machines or to the algorithms used in actual computing practice. In a more formal manner we have

Definition 1. An automaton $\alpha \in \alpha$ is given by the following structures:

- (1) An automaton $\alpha_0 \in \mathfrak{A}_0$ (the *finite part of* α), that is, a finite set of states Σ , a mapping $(\Sigma, X) \to \Sigma$, an initial state $\sigma_1 \in \Sigma$, a distinguished subset of Σ' of Σ .
- (2) A finite integer N, an initial vector v_1 from V_N and for each state σ in Σ' a distinguished finite union $V_{\sigma'}$ of homogeneous linear subspaces of V_N .
- (3) For each pair (σ, x) in (Σ, X) a mapping $\eta: V_N \to V_N$ which is such that each of the coordinates v_j of $\eta(v, \sigma, x)$ can be computed by a finite computing program independent of the vector v and involving only the following operations: reduction of an integer modulo a positive integer at most equal to a finite bound $K_1(\sigma, x, j)$, multiplication of an integer by an integer of absolute value at most equal to a finite bound $K_2(\sigma, x, j)$, addition and subtraction of two integers.
- (4) For each input word $f=x_{i_1}\,x_{i_2}\,\cdots\,x_{i_n}$ the automaton computes recursively the sequence of states σ_{i_0} , σ_{i_1} , σ_{i_2} , \cdots , $\sigma_{i_n}=\sigma_1 f$ and the sequence of vectors v_{i_0} , v_{i_1} , v_{i_2} , \cdots , $v_{i_n}=v(f)$ by the rules

$$\sigma_{i_0} = \sigma_1 \quad ext{and} \quad \sigma_{i_m} = (\sigma_{i_{m-1}}, x_{i_m})$$
 $v_{i_0} = v_1 \quad ext{and} \quad v_{i_m} = \eta(v_{i_{m-1}}, \sigma_{i_{m-1}}, x_{i_m}).$

(5) The input word f belongs to the set F_{α} of the words accepted by α if and only if $\sigma_1 f \in \Sigma'$ and, then, if the vector $v(f) = v_{i_n}$ does not belong to $V'_{\sigma_1 f}$.

As expected, this definition can be considerably simplified and in Section I we verify that it is equivalent to the following one:

DEFINITION 1'. An automaton $\alpha \in \alpha$ is given by a (homomorphic) representation μ of the monoid F in the ring Z_N of the integral $N \times N$ matrices (N, finite) together with the rule

$$F\alpha = \{f \in F : \mu f_{1,N} \neq 0\}$$

where $\mu f_{1,N}$ denotes the (1, N) entry of the matrix μf .

It follows that the theory of Kleene (1956) can be applied and in Section III we verify that the family R of all the sets F_{α} with $\alpha \in \mathfrak{A}$ has the following property

If F' and F'' belong to R the same is true of their intersection, union, set product F'F'' (i.e., of the set of all words f = f'f'' with $f' \in F'$ and $f'' \in F''$), and formal inverse F'^0 (i.e., of the infinite union of all the set products F', F'F', F'F'F', \cdots , $F'F' \cdots F'$, \cdots).

However, because of the arbitrariness implied in the conditions (2) and (5) of Definition 1, it is not necessarily true that the complement F - F' of an F' from R also belongs to R. This, together with some miscellaneous remarks of a negative character, is verified in Section II by way of counterexamples.

Furthermore, I am unable to formulate for the family & the deep part of Kleene's theory, namely to characterize R starting from a reasonably simple subfamily of sets in terms of meaningful set theoretical operations.

In Section IV, the family $R_0 = \{F_\alpha : \alpha \in \alpha_0\}$ of the regular events is characterized in terms of our present notations and in the same section we apply some elementary remarks from the theory of sequential machines (Moore, 1956) or transducers (Huffman, 1959) in order to obtain a third definition of α .

I am most indebted to Professor D. Arden from M.I.T. for many discussions of the content matter of this paper which have greatly contributed to the development or to the clarification of several points.

A. Preliminary Reduction

We shall say that the automaton α from α is semi-reduced if there exists a collection of finite integral matrices $\mu(\sigma, x)$ which are such that the vector $\eta(v, \sigma, x)$ is simply the product $v\mu(\sigma, x)$.

I.A.1. To any $\alpha \in \mathfrak{A}$ there corresponds one equivalent semireduced $\alpha' \in \mathfrak{A}$ which is such that for every input word f the vector v(f) is a projection on a subspace of the vector v'(f) of the automaton α' .

Proof. Let us consider a fixed triple $(\sigma, \dot{x}, \dot{j})$ and write in explicit form the computing program giving the \dot{j} th coordinate of the vector $\eta(v, \sigma, x)$.

Since this program is assumed to be finite there exists a finite natural number $M[=M(\sigma,x,j)]$ and a set of M quadruples of integers $(i,i_1(i),i_2(i),o(i))$ satisfying the conditions: (a) $1 \le i \le M$; (b) for all values of $i,i_1(i)$ and $i_2(i)$ are nonegative numbers at most equal to N+i; (c) o(i)=1,2,3 or 4.

We now define a sequence of 1 + N + M numbers a(i, v) by the following conditions: (a) a(0, v) = 1; (b) a(i, v) is the *i*th coordinate

of v when $1 \leq i \leq N$; (c) a(N+M,v) is the jth coordinate of $\eta(v,\sigma,x)$ which we try to compute; (d) for each $i(1 \leq i \leq M)$, a(N+i,v) is the value of $a(i_1(i),v)$, reduced modulo $a(i_2(i),v)$, when o(i)=1 and, when o(i)=2, 3 or 4, it is respectively the value of the product, the sum, or the difference of $a(i_1(i),v)$ and $a(i_2(i),v)$. Here, as usual, by the value of a reduced modulo b we mean the smallest nonnegative integer which is congruent to a modulo b.

At the cost of some increase in the length of this program we can assume that only multiplications by bounded nonegative factors are used. Indeed, since by hypothesis $|a(i_2(i), v)| \leq K_2(\sigma, x, j)$ when o(i) = 2, we can always replace this line of the program by a subroutine which consists in a multiplication by the nonnegative number $K_2(\sigma, x, j) + a(i_2(i), v)$ followed by $K_2(i, x, j)$ subtractions of the multiplicand.

Also, since there exist only finitely many triples (σ, x, j) we can take a fixed finite constant K which is larger than 2 and larger than any of the numbers $2K_1(\sigma, x, j)$ and $2K_2(\sigma, x, j)$. We shall always denote by $\bar{a}(i, v)$ the value of a(i, v) reduced modulo K!.

Let W_{σ} be the set of the vectors v which can occur when the finite part of the automaton is in state σ , i.e., the set of all v which are such that v = v(f) for at least one input word f satisfying $\sigma_1 f = \sigma$. Let I' be the set of the addresses $i(0 \le i \le N + M)$ which are such that for every v in W_{σ} , the value of a(i, v) is nonnegative and at most equal to K.

Because of the hypothesis and of our convention that only multiplications by nonnegative factors are allowed we have:

```
If o(i) = 1, then i \in I'.
```

If o(i) = 1 or 2, then $i_2(i) \in I'$.

Let us denote by \bar{v} the vector whose coordinates are those of v reduced modulo K! and verify the following statement: If $v, v' \in W_{\sigma}$ and $\bar{v} = \bar{v}'$ then, for all $i, \bar{a}(i, v) = \bar{a}(i, v')$, and for all $i \in I'$, a(i, v) = a(i, v').

Indeed, because of our choice of K and I', a(i, v) is always equal to $\bar{a}(i, v)$ when $v \in W$ and $i \in I'$. Thus, since the statement is true by hypothesis when $i \leq N$, we can apply induction and it is an elementary consequence of the properties of the congruences that when $\bar{a}(i_1(i), v) = \bar{a}(i_1(i), v')$ and $\bar{a}(i_2(i), v) = \bar{a}(i_2(i), v')$ we also have $\bar{a}(i, v) = \bar{a}(i, v')$ for each of the four possible cases o(i) = 1, 2, 3, or 4.

Consequently, any $\bar{a}(i, v)$, and in particular $\bar{a}(N + M, v)$, depends

only upon \bar{v} . But, the set \bar{V}_N of these reduced vectors contains only $(K!)^N$ distinct elements and for all practical purposes here it may be considered as an abstract finite set of states. Thus, we can replace α by an automaton α' for which the finite part α_0' has the union of \bar{V}_N and Σ as a set of states. Then, in α' , the computing program for any triple (σ', x, j) admits the following simplifications: o(i) is never 1; when o(i) = 2, the instruction consists in the multiplication of $a(i_1(i), v)$ by a factor which does not depend upon the vector v but only upon i, j, x and the state σ' in which is the finite part of α' .

By a simple induction, it follows that we can find integers $c_{j'}(\sigma, x, j)$ $(0 \le j' \le N)$ which are such that the jth coordinate of $\eta(v, \sigma, x)$ is the linear function

$$c_0(\sigma, x, j) + \sum_{1 \leq j' \leq N} v_{j'} c_{j'}(\sigma, x, j)$$

of the coordinates $v_{j'}$ of v; since, at the cost of increasing N by one unit we can always have a coordinate v_0 which is identically 1 for all f and, since, consequently we can make the above relations homogeneous the result is entirely proved.

Let us recall that a representation of the monoid F in the ring Z_N of the integral $N \times N$ matrices is a mapping $\mu: F \to Z_N$ which is such that $\mu f f' = \mu f \mu f'$ for all $f, f' \in F$. For any matrix m, $\operatorname{Tr}(m)$ denotes the sum of the elements lying in the main diagonal of m.

I.A.2. To any $\alpha \in \mathfrak{A}$ there corresponds one representation μ' in $Z_{N'}$ and a finite set P of matrices from the same ring that are such that

$$F_{\alpha} = \{ f \in F : \operatorname{Tr}(p\mu'f) \neq 0 \text{ for all } p \in P \}.$$

Proof. Let us assume that α is a semireduced automaton with M states in its finite part and, for each $x \in X$, let $\mu'x$ be the $(M \times N) \times (M \times N)$ matrix defined by

$$\mu' x_{ij,i'j'} = (\mu(\sigma,x))_{j,j'}$$
 if $\sigma_i x = \sigma_{i'}$; = 0, otherwise.

Assuming that σ_1 and v are respectively the initial state and the initial vector of α , we define the $M \times N$ vector v' by

$$v'_{ij} = v_j$$
 if $i = 1; = 0$ if $i \neq 1$.

It is easily verified that μ' is a representation of F in $Z_{N'}$ ($N' = M \times N$) and that for any input word f one has $(v'\mu'f)_{ij} = (v(f))_j$ if $\sigma_1 f = \sigma_i$; = 0, otherwise.

Let us now revert to the condition (5) of Definition 1 and observe that it implies that for each $\sigma \in \Sigma'$ a finite collection $W(\sigma)$ of N-vectors is given together with the rule that $f \in F_{\alpha}$ if and only if $\sigma_1 f \in \Sigma'$ and $v(f)w \neq 0$ for all w in $W(\sigma_1 f)$. For each state $\sigma_{i'} \in \Sigma'$ and, then, for each vector w in $W(\sigma_{i'})$ let w' be the $M \times N$ vector defined by $w'_{ij} = w_j$ if i = i'; = 0 otherwise.

Because of the relations established above we have $(v'\mu'f)w' = 0$ when $\sigma_1 f \neq \sigma_{i'}$. Thus if W' denotes the set of all the vectors such as w' we have $f \in F_\alpha$ if and only if not all the products $(v'\mu'f)w'$ $(w' \in W')$ are zero. This practically ends the proof because if p is the $M \times N$ matrix defined by

$$p_{ij,i'j'} = (w'_{ij}) \times (v'_{i'j'})$$

the relation $(v'\mu'f)w' \neq 0$ is equivalent to $\text{Tr}(p\mu'f) \neq 0$.

B. Equivalence of Definitions 1 and 1'

We recall that if $m \in Z_N$ and $m' \in Z_{N'}$, the kroneckerian product $m'' = m \otimes m'$ of m and m' is a matrix from $Z_{NN'}$ whose entries are defined by

$$m_{ii',jj'} = (m_{i,j}) \times (m'_{i',j'}).$$

Then, identically, for any $a, b \in Z_N$ and $a', b' \in Z_{N'}$ one has

$$(a \otimes a')(b \otimes b') = (ab) \otimes (a'b')$$

and

$$\operatorname{Tr}(a \otimes a') = \operatorname{Tr}(a) \operatorname{Tr}(a').$$

I.B.1. The Definitions 1 and 1' of the family α are equivalent.

Proof. On the one hand the statement is trivial because an automaton as defined by 1' is a special case of an automaton as defined by 1; indeed, given a representation μ of F, we take as initial vector v_1 the first row of μe . For any input word f the vector $v_1 \mu f$ is obtained by performing for each input letter a bounded number of additions and multiplications by bounded factors. Finally, f is accepted if and only if $v_1 \mu f$ does not belong to the linear subspace of the vectors whose last coordinate is zero.

On the other hand the statement is also trivial. Because of I.A.1 and I.A.2. we may assume that α is in reduced form, i.e., that α is given by a representation $\mu:F \to Z_N$ together with a finite subset P of Z_N . For

each $f \in F$, let $\mu'f = (\mu f) \otimes (\mu f)$ ($\in Z_{N^2}$) and let \bar{p} be the sum of the kroneckerian squares $p \otimes p$ over all $p \in P$. Because of the identities recalled above, μ' is a representation and for any $f \in F$, $\operatorname{Tr}(\bar{p}\mu'f)$ is the sum over all $p \in P$ of the square of $\operatorname{Tr}(p\mu f)$; thus, $\operatorname{Tr}(\bar{p}\mu'f) \neq 0$ if and only if $f \in F_{\alpha}$. It follows that without loss of generality we may reduce the verification of the statement to that of the following:

If μ is a representation of F in Z_N and p a matrix from the same ring there exists a representation μ' of F in Z_{N^2+2} which is such that for all f, $\operatorname{Tr}(p\mu f) = \mu' f_{1,N^2+2}$. Indeed, for each $f \in F$ let $\mu' f$ be the following $N' \times N'$ matrix $(N' = N^2 + 2)$:

- (i) $\mu' f_{N',j} = \mu' f_{j,1} = 0$ for all $1 \le j \le N'$; (i.e., the last row and the first column of every $\mu' f$ are identically zero).
- (ii) $\mu' f_{1,1+j+(k-1)N}$ for each pair (j, k) $(1 \leq j, k \leq N)$ is equal to the (j, k) entry of the matrix $p\mu f$; (i.e., for each k the subvector $\mu' f_{1,1+j+(k-1)N}$ (when $1 \leq j \leq N$) of the first row of $\mu' f$ is equal to the kth row vector of the matrix $p\mu f$).
- (ii') $\mu' f_{1+j+(k-1)N,N'}$ for each pair (j,k) $(1 \le j,k \le N)$ is equal to the (j,k) entry of μf .
 - (iii) $\mu' f_{1,N'}$ is equal to $Tr(p\mu f)$.
- (iv) The restriction of $\mu'f$ to the set of indices (i, j) strictly larger than 1 and strictly less than N' is the direct sum of N matrices identical to the matrix μf .

The verification that μ' is a representation is a straightforward computation and the result is proved because of the condition (iii).

As a simple consequence of these constructions we have:

I.B.2. The family R of all F_{α} ($\alpha \in \mathfrak{A}$) is closed under finite intersections and unions.

PROOF. Let F' and F'' be defined respectively by $\mu': F \to Z_{N'}$ and $\mu'': F \to Z_{N''}$. If for every f we define $\mu_i f$ as the kroneckerian product $(\mu'f) \otimes (\mu''f)$ we have $\mu_i f_{1,N'N''} \neq 0$ if and only if both $\mu'f_{1,N'}$ and $\mu''f_{1,N''}$ are different from zero; thus μ_i defines the intersection of F' and F''.

If for every f we define $\mu_u f$ as the direct sum of the kroneckerian squares of $\mu' f$ and $\mu'' f$, μ_u is still a representation and we can easily find a $(N'^2 + N''^2) \times (N'^2 + N''^2)$ matrix p which is such that for all f, $\text{Tr}(p\mu_u f)$ is the sum of the square of $\mu' f_{1,N'}$ and $\mu'' f_{1,N''}$; thus, by our last reduction μ_u can be used for defining the union of F' and F''. D. Arden has pointed out to me that by using the kroneckerian product of $\mu' f$ and $\mu'' f$ one can obtain more economically the same result.

II. COUNTER EXAMPLES

II.1. If X has a single letter, R reduces to R_0 (= the set of all regular events).

Proof. Let α be defined by the representation $\mu: F \to Z_N$ and consider the following integral power series in the variate t:

$$a(t) = a_0 + \sum_{n>0} t^n (\mu x^n)_{1,N}.$$

By definition, F_{α} is the set of those words x^n which are such that $(\mu x^n)_{1,N} \neq 0$; however, as a function of t, a(t) is the Taylor series of a rational function whose denominator is a factor of $\det(1-t\mu x)$. Thus according to the theorem of Skolem (1934), there exists a finite set of finite integers m, p, d_1 , d_2 , \cdots , d_k which have the property that for any n larger than m, the coefficient of t^n in a(t) (i.e., $(\mu x^n)_{1,N}$) is zero if and only if n is congruent modulo p to one of the d_j 's. Consequently F_{α} reduces to a regular event when X has a single letter and there exist quite simple sets (as, e.g., the set of the words x^{n^2} where n runs over all integers) which do not belong to R. It can be observed that Skolem's theorem shows that for any $F_{\alpha} \in R$ and $f \in F$, the intersection of F_{α} with the infinite set f, f^2 , f^3 , \cdots , f^n , \cdots also reduces to a regular event.

II.2. When X has two letters or more there exists at least one $F_{\alpha} \in \mathsf{R}$ which has the following properties: F_{α} does not belong to R_0 ; the complement $F - F_{\alpha}$ of F_{α} does not belong to R .

PROOF. Let $X = \{x, y\}$; $\Sigma = \{\sigma_i\}$, i = 1, 2, 3, 4, 5, and $(\Sigma, X) \to \Sigma$ defined by

$$\sigma_1 x = \sigma_2 x = \sigma_2$$
; $\sigma_3 x = \sigma_4 x = \sigma_4$; $\sigma_5 x = \sigma_5$
 $\sigma_1 y = \sigma_3 y = \sigma_4 y = \sigma_5 y = \sigma_5$; $\sigma_2 y = \sigma_3$.

Let $\mu(\sigma_i, x)$ be the following matrices

$$\mu(\sigma_1, x) = \mu(\sigma_2, x) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix};$$

$$\mu(\sigma_3, x) = \mu(\sigma_4, x) = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix};$$

 $\mu(\sigma_2, y)$ = the identity matrix; $\mu(\sigma, x)$ = the zero matrix in all other cases.

The initial state is σ_1 and the initial vector v=(1,0). Σ' is Σ itself and f is accepted in all cases except if $\sigma_1 f=\sigma_4$ and then if the second coordinate of v(f) is zero.

By looking at the diagram (Fig. 1) one easily sees that $\sigma_1 f = \sigma_4$ if and only if $f = x^{1+n}yx^{1+n'}$ and that, then, v(f) = (1, n - n').

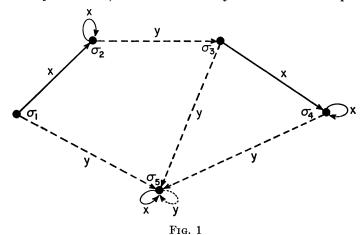
Thus F_{α} consists of all words except those which have the form $x^{1+n}yx^{1+n}$; and, according to a metamathematical proof of Calvin Elgot (1960), F_{α} is not a regular event.

Let us verify that $F'=F-F\alpha$ does not belong to R; indeed, let us assume that there exists a representation $\mu':F\to Z_N$ which has the property that $\mu'f_{1,N}\neq 0$ if and only if f does not belong to F_α .

Since $\mu'x$ is a $N \times N$ matrix it satisfies an equation of degree at most N and for every pair (i, j) and matrix m from Z_N there exists a linear relationship between the (i, j) entries of the N+1 matrices m, $m\mu x$, $m\mu x^2$, \cdots , $m\mu x^N$. Since, by hypothesis, for every finite n the (1, N) entry of the matrix $\mu' x^{1+n} y x^{n'}$ ($= \mu' x^{1+n} y \mu' x^{n'}$) is zero for $0 \le n' \le n$ and different from zero for n' = n + 1, we have shown that N' must be at least equal to every finite integer n. Consequently, the representation μ' is an infinite representation, i.e., $F - F_{\alpha}$ does not belong to R. Some elementary properties of this type of sets have been described in Schützenberger (1959).

II.3. The family $\bar{R} = \{F - F_{\alpha} : \alpha \in \alpha\}$ is closed under (finite) union and intersection but not under set multiplication.

Proof. By definition, $\bar{F}_{\alpha} \in \bar{R}$ if and only if there exists a representa-



tion $\mu: F \to Z_N$ (with N finite), that is, such that $\bar{F}_{\alpha} = \{ f \in F : \mu f_{1,N} = 0 \}$. Thus the closure properties of \bar{R} for the union and the intersection are a simple consequence of I.3.2.

Let $X = \{x, y\};$

$$\mu x = \mu' x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}; \qquad \mu y = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}; \qquad \mu' y = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}.$$

The sets

$$\bar{F}_{\alpha} = \{ f \in F : \mu f_{1,2} = 0 \} = \{ f \in F : |f|_x = |f|_y \}$$

and

$$\bar{F}_{\alpha'} = \{ f \in F : \mu' f_{1,2} = 0 \} = \{ f \in F : |f|_x = 2 |f|_y \}$$

(where $|f|_z$ denotes the number of times the letter z appears in f) both belong to \overline{R} and we shall verify that $F'' = \overline{F}_{\alpha}\overline{F}_{\alpha'}$ does not belong to \overline{R} .

Let us define W(f) as the set of the words f' which are such that $ff' \in F''$. We have (i) For all $f \in F$ and $f'' \in \bar{F}_{\alpha}$, W(f) is contained in W(f''f). Indeed, $ff' \in F''$ means that $ff' = f_1f_2$ where $f_1 \in \bar{F}_{\alpha}$ and $f_2 \in \bar{F}_{\alpha'}$. Thus $f''ff' = f''f_1f_2$ belongs to F'' since by hypothesis $f''f_1 \in \bar{F}_{\alpha}$. (ii) If both f and f'' belong to \bar{F}_{α} , W(f''f) = W(f) implies that f'' = e (the empty word of F). Indeed, let $f''f \in \bar{F}_{\alpha}$, that is $|f''f|_x = |f''f|_y = k$, say. The product $f''fx^k$ satisfies the relations $|f''fx^k|_x = 2k$ and $|f''fx^k|_y = k$ and, consequently, it belongs to $\bar{F}_{\alpha'}$; thus, since $\bar{F}_{\alpha'}$ is a subset of F'' (because $e \in \bar{F}_{\alpha}$) the word x^k belongs to W(f''f) and we shall show that it does not belong to W(f).

Assume for the sake of contradiction that $fx^k = f_1f_2$ with $f_1 \in \bar{F}_{\alpha}$ and $f_2 \in \bar{F}_{\alpha'}$; this implies that $f = f_1f_3$ with $f_3 \in \bar{F}_{\alpha}$ and, consequently, $|f_3x^k|_x = |f_3|_x + k = 2|f_3|_y$; $|f_3|_x = |f_3|_y$. It follows that $|f_3|_x = k$ and finally that $|f''f_3|_x = |f''f_1f_3|_x = k$, i.e., |f''| = e.

Thus, using (i) and (ii), we can find at least one strictly increasing infinite sequence of sets W, viz., W(f), W(f''f), $W(f''^2f)$, \cdots , $W(f'''^nf)$, \cdots .

Let us assume now that $F'' = \{f \in F : \mu'' f_{1,N''} = 0\}$; we observe that for given f the set $\bar{W}(f)$ of the vectors consisting of the N''th row of the matrices $\mu''f'$ where $f' \in W(f)$ form a linear space whose dimension is at most N''. Since we can build an infinite strictly increasing sequence $\bar{W}(f''''f)$ of such spaces it follows that N'' is infinite, i.e., that $\bar{F}_{\alpha}\bar{F}_{\alpha'} = F''$ does not belong to \bar{R} .

II.4. If X contains two letters or more, there corresponds to any subset F' of F one automaton satisfying the conditions (1), (3), and (4) of Definition 1 and having F' as its set of accepted words.

Proof. This is a trivial consequence of the existence of isomorphic, integral, finite dimensional representations of the monoid F.

Let first $X = \{x, y\}$;

$$\mu x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}; \qquad \mu y = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix};$$

and take v=(1,1) as initial vector. According to a theorem of Harrington (1951), the relation $v\mu f=v\mu f'$ implies f=f'; thus for any subset F' of F if the subset V' of V_2 is defined by $V'=\{v'=v\mu f: f\in F'\}$, we have reciprocally $F'=\{f\in F: v\mu f\in V'\}$. Clearly, this algorithm satisfies the conditions (1), (3), and (4) but not necessarily (2) and (5).

When X contains $n \ge 3$ letters z_i , the same result subsists because we can associate to each z_i the matrix μf_i where $f_1 = x$, $f_n = y^{n-1}$ and $f_i = y^{i-1}x$ when $2 \le i \le n-1$.

III. KLEENE'S THEOREM

Although this part could be written without explicitly using the notion of the ring \bar{A} of the formal integral power series in the noncommutative variates $x \in X$, it seems more natural to do so and we recall here, without proofs, a few definitions and results on \bar{A} . These are very special and shallow cases of theorems used by many authors in the study of other problems. An especially valuable reference is Lazard (1955).

Definition 2. \bar{A} is the ring of all formal infinite sums

$$a = \sum_{f \in F} f(a, f)$$

with integral coefficients (a, f).

The addition and multiplication in \bar{A} are defined respectively by:

$$a + a' = \sum_{f \in F} f((a, f) + (a'f)); \qquad aa' = \sum_{f \in F} f(\sum_{f'f''=f} (a, f')(a', f''))$$

where, as always in this section, $\sum_{f'f''=f}$ means a summation over all factorizations f = f'f'' of f.

It may be easier to visualize any element of \bar{A} as a generating function in which every word f has a (positive or negative) integral coefficient

(a, f). Thus, in particular, to each subset F' of F there corresponds the formal sum (its *characteristic function*)

$$\sum_{f \in F} f = \sum_{f \in F} f \chi_{F'}(f)$$

with $\chi_{F'}(f) = 1$ or 0 according to $f \in F'$ or not.

The multiplication is simply the ordinary multiplication of series using infinite distributivity, that is aa' can also be formally expressed as

$$\sum_{f \in F} f(a, f) a' = \sum_{f \in F} a f(a', f) = \sum_{f, f' \in F} f f'(a, f) (a', f').$$

It may not be unnecessary to stress that this product is *not* the Hadamard product $\Sigma f(a, f)(a', f)$ to which we were led by the construction of the kroneckerian product of matrices in Section I.

We shall always denote the empty word by e and by \bar{A}^* the subset of all $a \in \bar{A}$ in which (a, e), the coefficient of e, is zero. The elements of \bar{A}^* are usually called quasi regular and we denote by a^* the mapping $\bar{A} \to \bar{A}^*$ defined by a - (a, e)e. If and only if a is quasi regular (i.e., $a = a^*$), it has a quasi inverse $a^0 = \sum_{n \geq 1} a^n$ which satisfies $aa^0 + a = a^0a + a = a^0$. In a perfectly equivalent manner an element $a \in \bar{A}$ has an inverse $a^{-1}(a^{-1}a = a^{-1}a = e)$ if and only if it belongs to the group $G \subset \bar{A}$ of the elements a' which are the sum of e and of the quasi regular element a'^* ; then $a'^{-1} = e + (-a'^*)^0$ because

$$a'a'^{-1} = (e + a'^*)(e + (-a'^*)^0)$$

$$= e + a'^* + (-a'^*)^0 + a'^*(-a'^*)^0$$

$$= e + a'^* - a'^* = e.$$

We shall find it more convenient to deal with the *quasi* notions because if a has nonnegative coefficients the same is true of $(a^*)^0$ but not necessarily of $(e + a^*)^{-1}$.

All the above operations are legitimate because \bar{A}^* is a continuous topological algebra with continuous inverse when the distance between a and $a'(a \neq a')$ is defined as the supremum of the inverse of the length of those f for which $(a, f) \neq (a', f)$.

A. The Subring $ar{R}$ of the Rational Elements

DEFINITION 3. The subset \bar{R} of \bar{A} is the subset of the formal power series r which have the form $r = \sum_{f \in F} f \mu f_{1,N}$ for some representation μ of F in Z_N (N finite) which is said to produce r.

We shall verify that \bar{R} is in fact the smallest subring of \bar{A} that contains all the generators $x \in X$ of \bar{A} and is such that its intersection with G is a subgroup; this last restriction is not trivial because, for an arbitrary subring \bar{A}' of \bar{A} it may well happen that some a belongs to the intersection of G and \bar{A}' but that a^{-1} does not belong to \bar{A}' . If the variates x were commutative, \bar{R}' would be the ring of the ordinary rational functions with integral coefficients and it seems natural to extend this terminology to the noncommutative case. A slightly different definition of \bar{R} is given below.

III.A.1. \bar{R} is a submodule of \bar{A} .

Proof. If

$$a = \sum_{f \in F} f(\mu f)_{1,N}, \qquad a' = \sum_{f \in F} f(\mu' f)_{1,N'}$$

we take the direct sum $\mu'': F \to Z_{N+N'}$ of μ and μ' and we apply the remarks of I.3.1. for reducing to the desired form.

III.A.2. \bar{R} is a subring.

PROOF. We have to prove that if a is produced by μ and a' by μ' we can construct some μ'' which produces aa'. It will be simpler to prove the result under the additional assumption that a, $a' \in \bar{A}^*$ and to observe that the general case follows from III.A.1 because $aa' = a^*a'^* + (a,e)a'^* + a^*(a',e) + (a,e)(a',e)e$. We can also assume that μe and $\mu' e$ are the identity matrices of Z_N and Z_N' respectively. After these preliminaries we proceed to the actual construction.

For each $x \in X$ we define $\mu''x \in Z_{N+N'}$ as the matrix

$$\begin{pmatrix} \mu x & (\mu x)u \\ 0 & \mu' x \end{pmatrix}$$

where by $(\mu x)u$ we mean the $N \times N'$ matrix in which all columns are zero except for the first one which is equal to the Nth one of μx . Then, after taking $\mu''e$ as the identity matrix of $Z_{N+N'}$, we extend μ'' to a representation $\mu'': F \to Z_{N+N'}$ in the usual manner.

Because of our assumptions the following relations are surely true if f = e or x:

$$\mu'' f_{1,i} = \mu f_{1,i} \text{ when } 1 \le i \le N;$$

$$\mu'' f_{1,N+i} = \sum_{f'f''=f} \mu f'_{1,N} \mu' f''_{1,i} \text{ when } 1 \le i \le N'$$

Let us verify now that if they hold for f they also hold for fx. Indeed we

have for $1 \leq i \leq N$:

$$\mu'' f x_{1,i} = \sum_{1 \le j \le N+N'} \mu'' f_{1,j} \mu'' x_{j,i} = \sum_{1 \le j \le N} \mu f_{1,j} \mu x_{j,i} = \mu f x_{1,i}$$

and for $1 \leq i' \leq N'$:

$$\mu'' f x_{1,N+i'} = \sum_{1 \le j \le N} \mu f_{1,j}((\mu x) u)_{j,i'} + \sum_{1 \le j \le N'} \mu'' f_{1,N+j} \mu' x_{j,i'}.$$

The first sum is just $\mu f x_{1,N}$ when i=1 and zero otherwise. By the induction hypothesis the second sum is

$$\sum_{f'f''=f} \sum_{1 \leq j \leq N} \mu f'_{1,N} \mu' f''_{1,j} \mu' x_{j,i'} = \sum_{f'f''=f} \mu f'_{1,N} \mu' f'' x_{1,i'}.$$

When $i' \neq 1$ this can also be written as

$$\sum_{g'g''=fx} \mu g'_{1,N} \mu' g''_{1,i'}$$

since $\mu'e_{1,i'} = 0$. On the contrary when i' = 1 we have

$$\mu''fx_{1,N+1} = \mu fx_{1,N} + \sum_{\substack{g'g''=fx\\g''\neq e}} \mu g'_{1,N}\mu'g''_{1,1} = \sum_{\substack{g'g''=fx}} \mu g'_{1,N}\mu'g''_{1,1}$$

and the above relations are true for all cases. Since they imply that

$$\sum_{f \in F} f(\mu'' f)_{1,N+N'} = \sum_{f \in F} f(\sum_{f'f''=f} (\mu f')_{1,N} (\mu' f'')_{1,N'}) = aa'$$

the result is proved.

III.A.3. \bar{R} contains the quasi inverse of each of its quasi-regular elements. Proof. As above we assume that μe is the identity matrix and we define $\bar{\mu}e$ as μe . For each $x \in X$, we take $\bar{\mu}x$ equal to the sum of μx and of a matrix $(\mu x)u \in Z_N$ which has all columns zero except for the first one which is equal to the Nth column of μx . For f = e or x we have

$$\bar{\mu}f_{1,i} = \mu f_{1,i} + \sum_{f'f''=f} \bar{\mu}f'_{1,N}\mu f''_{1,i}$$
.

As in the last proof above:

$$\mu f x_{1,i} = \sum_{1 \leq i' \leq N} \bar{\mu} f x_{1,i'} \bar{\mu} x_{i',i} + \sum_{f'f''=f} \sum_{1 \leq i' \leq N} \bar{\mu} f'_{1,N} \mu f''_{1,i'} \bar{\mu} x_{i',i}.$$

Thus: if i = 1.

$$\bar{\mu}fx_{1,1} = \mu fx_{1,1} + \mu fx_{1,N} + \sum_{f'f''=f} \bar{\mu}f'_{1,N}\mu f''x_{1,1} + \sum_{f'f''=f} \bar{\mu}f'_{1,N}\mu f''x_{1,N}$$

If $i \neq 1$,

$$\mu f x_{1,i} = \mu f x_{1,i} + \sum_{g'g''=g} \bar{\mu} g'_{1,N} \mu g''_{1,i}$$
.

Consequently, the initial relation is valid in all cases. Let us now compute \bar{a}_i . We have

$$\bar{a}_i = \sum_{f \in F} f_{\bar{\mu}} f_{1,i} = \sum_{f \in F} f_{\mu} f_{1,i} + \sum_{f',f'' \in F} (f'_{\bar{\mu}} f'_{1,N}) (f''_{\mu} f''_{1,i}).$$

In particular, for i = N, we have $\bar{a}_N = a + \bar{a}_N a$, that is, $e = (e + \bar{a}_N)$ (e - a) and, since a is assumed to be quasi regular, $a_N = (e - a)^{-1} - e = a^0$.

III.A.4. Reciprocally, any element $a = \sum_{f \in F} f(\mu f)_{1,N}$, of \bar{R} , can be obtained from the generators $x \in X$ by a finite number of ring operations and formation of the quasi inverse (of quasi-regular elements).

PROOF. It is convenient to verify first the following statement: If s is a $N \times N$ matrix whose entries s_{ij} are N^2 distinct noncommutative variates, any entry of the quasi inverse u of s is a rational element with integral coefficients in the ring of the formal power series in the variates s_{ij} .

When N=1, the statement is trivial because, then, u reduces to u_{11} which is equal to the quasi inverse of s_{11} ; when $N \ge 2$ we shall use induction and base the verification upon the popular fact that any entry u_{ij} can be interpreted as the sum of all paths from i to j on the complete graph with vertices $1, 2, \dots, N$. Since any such path can be decomposed in a unique manner described below with respect to the return of the vertex 1, the verification is a straightforward clerical operation.

Let us assume that the result is already proved for N-1 and consider the $(N-1) \times (N-1)$ matrix t obtained from s by replacing by zero all the entries s_{1j} and $s_{j1} (1 \le j \le N)$ of s; by the induction hypothesis the quasi inverse v of t does exist and its entries $v_{ij} (2 \le i, j \le N)$ have the desired properties. We define a $N \times N$ matrix u by the following relations below and we shall verify later that it is the quasi inverse of s by showing that us = u - s.

$$u_{11} = \left(s_{i1} + \sum_{2 \le i \le N} s_{1i} s_{is} + \sum_{2 \le i, j \le N} s_{1i} v_{ij} s_{j1}\right)^{0}$$

If $i \neq 1$,

$$u_{1i} = \bar{u}_{1i} + u_{11}\bar{u}_{1i}$$
; $u_{i1} = \bar{u}_{i1} + \bar{u}_{i1} + u_{i1}u_{11}$

where, as an abbreviation,

By the induction hypothesis, all the u_{ij} 's can be obtained from generators by the specified operations and we verify that us = u - s. We have to examine four cases:

Case 1.

$$(us)_{11} = u_{11}s_{11} + \sum_{2 \le j \le N} u_{1j}s_{j1} = u_{11}s_{11} + \sum_{2 \le j \le N} \bar{u}_{1j}s_{j1} + u_{11} \sum_{2 \le j \le N} \bar{u}_{1j}s_{j1}$$

$$= u_{11}s_{11} + (e + u_{11})(\sum_{2 \le j \le N} s_{1j}s_{j1} + \sum_{2 \le j,j \le N} s_{1j}v_{j'j}s_{j'1})$$

$$= u_{11}s_{11} + (e + u_{11})(e - s_{11} - (e + u_{11})^{-1}) = u_{11} - s_{11}.$$

$$Case \ 2. \ If \ 2 \le i \le N$$

$$(us)_{1i} = u_{11}s_{1i} + (e + u_{11}) \sum_{2 \le j \le N} \bar{u}_{1j}s_{ji}$$

$$= u_{11}s_{1i} + (e + u_{11})(\sum_{2 \le j \le N} s_{1j}s_{ji} + \sum_{2 \le j,j' \le N} s_{1j'}v_{j'j}s_{ji})$$

$$= u_{11}s_{1i} + (e + u_{11})(\sum_{2 \le j \le N} s_{ij}s_{ji} + \sum_{2 \le j' \le N} s_{1j'}(v_{j'i} - s_{j'i}))$$

$$= u_{11}s_{1i} + (e + u_{11})(\sum_{2 \le j \le N} s_{ij}s_{ji} + \sum_{2 \le j' \le N} s_{1j'}(v_{j'i} - s_{j'i}))$$

$$= u_{11}s_{1i} + (e + u_{11})(\bar{u}_{1i} - s_{1i})$$

$$= u_{11}s_{1i} + \sum_{2 \le j \le N} u_{ij}s_{ji}$$

$$= \bar{u}_{11}s_{11} + \sum_{2 \le j \le N} u_{ij}s_{ji}$$

$$= \bar{u}_{i1}s_{11} + \bar{u}_{i1}u_{11}s_{11} + \sum_{2 \le j \le N} v_{ij}s_{ji} + \sum_{2 \le j \le N} \bar{u}_{i1}(e + u_{11})\bar{u}_{1j}s_{ji}$$

$$= \bar{u}_{i1}[s_{11} + u_{11}s_{11} + e + \sum_{2 \le j \le N} s_{1j}s_{ji} + \sum_{2 \le j \le N} \bar{u}_{i1}(e + u_{11})\bar{u}_{1j}s_{ji}] - s_{i1}$$

$$= \bar{u}_{i1}[e + (e + u_{11})(s_{11} + \sum_{2 \le j \le N} s_{1j}s_{ji} + \sum_{2 \le j,j \le N} s_{1j'}v_{j'j}s_{ji})] - s_{i1}$$

$$= \bar{u}_{i1}(e + u_{i1}) - s_{i1} = u_{i1} - s_{i1} .$$

$$Case \ 4. \ \text{Finally, if } i, j \ne 1$$

$$(us)_{ij} = u_{is}s_{ij} + \sum_{2 \le j' \le N} u_{ij'}s_{j'j}$$

$$= \bar{u}_{i1}s_{1j} + \bar{u}_{i1}u_{11}s_{ij} + v_{ij} - s_{ij} + \sum_{2 \le j' \le N} \bar{u}_{i1}(e + u_{i1})u_{1j'}s_{j'j}$$

$$= \bar{u}_{i1}s_{1j} + \bar{u}_{i1}u_{11}s_{ij} + v_{ij} - s_{ij} + \sum_{2 \le j' \le N} \bar{u}_{i1}(e + u_{i1})u_{1j'}s_{j'j}] = u_{ij} - s_{ij} + \bar{u}_{ij} - s_{ij}$$

and the statement is verified.

We now revert to the proof of III.A.4 and we consider an element $r \in \bar{R}$ produced by the representation $\mu \colon F \to Z_N$. Without loss of generality we may assume that r is quasi regular and we consider the formal sum $s = \sum_{x \in X} x \mu x$, that is a $N \times N$ matrix whose entries s_{ij} are the elements $\sum_{x \in X} x \mu x_{ij}$ from \bar{R} . The sum s can be interpreted as a quasiregular element of the ring of the power series in the variates $x \in X$ with coefficients in Z_N . Let us observe that for any two elements of this ring having the form $f \mu f$ and $f' \mu f'$ the product $(f \mu f)(f' \mu f')$ is equal to $f f' \mu f f'$. Consequently, the quasi inverse u of s is equal to the sum of $f \mu f$ extended of all the elements of F except e and the entry u_{ij} is the sum of $f \mu f_{ij}$ extended to the same set. Since we have seen previously that u_{ij} is a rational element in the entries of s, the same is true in particular of $u_{1N} = a$ and the result is verified.

As a point of marginal interest in the applications of probabilities to regular events, we consider the homomorphism (of ring) λ which sends every $r \in \bar{R}$ with finitely many nonzero coefficients onto the corresponding ordinary polynomial in the commutative variates $\bar{x} = \lambda x$; λ extends in a natural fashion to \bar{R} and we have

III.A.5. For each $r \in \bar{R}$, λr is a power series, converging in some open domain around zero and representing there an ordinary rational function in the commutative variates $\bar{x} = \lambda x$.

PROOF. Let $r = \sum_{f \in F} f \mu f_{1,N}$. We consider the matrix $\sum_{x \in X} \bar{x} \mu x = s$ and the ordinary polynomial equal to $\det(I - s)$ in the commutative variates $\bar{x} = \lambda x$. For small enough ϵ , $\det(I - \lambda s)$ has its value arbitrarily close to 1 when all the \bar{x} are less than ϵ . Under this condition the matrix $I + \sum_{n \geq 1} s^n = (I - s)^{-1} = [\det(I - s)]^{-1} \operatorname{Adj}(I - s)$ exists and its (1, N) entry, that is, λr , is a rational function of the ordinary variates \bar{x} .

B. REDUCTION TO STANDARD FORM

In this section, we apply classical algebraic techniques to obtain a minimal representation producing a given element r of \bar{R} ; at variance with the other parts of this paper we deal here with arbitrary (not necessarily integral) numbers.

III.B.1. To any element $r \in \bar{R}$, there corresponds a unique integer \bar{N} and a representation $\bar{\mu}$ of F by $\bar{N} \times \bar{N}$ rational matrices that has the following properties:

(i) There exists two sets T and S of \bar{N} words each, a finite integer K and \bar{N}^2 matrices $\pi(t,s)$ from Z_N which are such that for all $f \in F$ the matrix $\bar{\mu}f$

is identically equal to the sum $\Sigma K^{-1}(r, tfs)\pi(t, s)$ extended to all the pairs $(t, s) \in T \times S$.

- (ii) The representation $\bar{\mu}$ produces r in that sense that $\bar{\mu}f_{1N}=(r,f)$ if r is quasi regular and that $\bar{\mu}f_{11}=(r,f)(r,e)^{-1}$ if $(r,e)\neq 0$ (that is, $\pi(e,e)$ has a single nonzero entry).
- (iii) If μ is any representation of F by $N \times N$ matrices that produces r, then $N \geq \bar{N}$ and there exists a pair of matrices (\bar{u}, \bar{u}') which is such that $(\bar{u}\mu f\bar{u}')_{ij} = \bar{\mu}f_{ij}$, if $i \leq i, j, \leq N$ and i = 0, otherwise (i.e. $\bar{\mu}$ is a projection of μ).

PROOF. In the first steps of the proof we start from a given N-dimensional representation μ of F that produces r and we construct by iteration of the procedure described in 1 below the \bar{N} -dimensional representation $\bar{\mu}$ which has the properties (i), (ii), and (iii) with respect to μ ; in the last step we verify that this representation does not depend upon μ but only upon r.

1. Let I be a fixed one to one mapping of F onto the natural numbers that satisfies the inequality $If \leq Iff'$, for all words f and f', and let v be the vector equal to the first row of μe . We construct a set of words T' by the two following rules: (a) $I^{-1}1$ (that is, e) belongs to T'; (b) inductively, $I^{-1}j = f$ belongs to T' if and only if f = f'x where $f' \in T'$ and $x \in X$ and if $v\mu f$ is (linearly) independent of the vectors $v\mu f''$ where $f'' \in T'$ and If'' < If.

By construction, T' contains $N' \leq N$ elements and, without loss of generality, it may be assumed that $T' = \{f: If \leq N'\}$ since $ff' \in T'$ implies $f \in T'$.

Let χf be the $N' \times N$ matrix whose jth row is the vector $v \mu f' f$ where If' = j; by construction $\chi f = \chi e \mu f$ identically.

Observe that for any $t \in T'$ and $x \in X$ either $tx \in T'$ or, else, the vector $v\mu tx$ is a linear combination of the vectors $v\mu t'$ ($t' \in T'$), that is, of the rows of χe ; in other words, the matrix χx is equal to the product $\mu' x \chi e$ where $\mu' x$ is a certain $N' \times N'$ matrix. For any word $f = x_{i_1} x_{i_2} \cdots x_{i_n}$ we define $\mu' f$ as $\mu' x_{i_1} \mu' x_{i_2} \cdots \mu' x_{i_n}$ and we verify by induction that the representation μ , the associated representation μ' , and the interwinning matrix χe are linked by the identity

$$\chi f = \chi e \mu f = \mu' f \chi e$$
.

In fact, since the rank of χe is by construction equal to the number N' of its rows, there exists a pair (a, b) of nonsingular matrices which is such that $(a\chi e \ b)_{ij} = 1$ if $1 \le i = j \le N'$; = 0, otherwise.

The identity $(a\chi e b)(b^{-1}\mu f b) = (a\mu'fa^{-1})(a\chi e b)$ shows that

$$(b^{-1} \mu f b)_{ij} = (a\mu' f a^{-1})ij \text{ if } 1 \leq i, j \leq N'$$

= 0 if $1 \leq i \leq N' \text{ and } N' < j \leq N.$

Thus, there exists a pair (u, u') of matrices which are such that the restriction of $u\mu fu'$ to the indices less than N' is equal to $\mu'f$ and that any other entry of $u\mu fu'$ is zero, that is, μ' is a projection of μ .

Finally, we point out that the construction of μ' implies that any vector $v\mu f(f \in F)$ is a linear combination of the N' independent vectors $v\mu t(t \in T')$ and that consequently N' can be defined, without reference to I, as the rank of the vector space spanned by the vectors $v\mu f(f \in F)$.

2. Let \tilde{I} be a one to one mapping of F onto the natural numbers that satisfies $\tilde{I}f \leq \tilde{I}f'f$ for all words f and f', and let v' be the (column) vector equal to the Nth column of χe . It is clear that by replacing I by \tilde{I} and by exchanging everywhere left and right multiplications we obtain a set S analogous to T' and that we can associate to the representation μ' a third representation $\tilde{\mu}$ of dimension $\tilde{N} \leq N'$ and an interwinning matrix $\tilde{\chi}e$ that satisfies the identity:

$$\tilde{\chi}f = \mu'f\tilde{\chi}e = \tilde{\chi}e\tilde{\mu}f.$$

Again, reverting to I and taking a basic vector \tilde{v} equal to the first row of $\tilde{\chi}e$, we can apply the same construction once more and obtain a set T, a representation $\bar{\mu}$ of dimension $\bar{N} \leq \tilde{N}$ associated to $\bar{\mu}$, and an intertwinning matrix $\bar{\chi}e$.

However, by definition, $(\tilde{\chi}f)_{ij} = (r, tfs)$ where It = i and $\tilde{I}s = j$. Consequently T is a subset of T' and $\tilde{\chi}f$ is obtained from $\tilde{\chi}f$ by deleting a certain subset of $N' - \tilde{N}$ rows. Let us observe that the rank of $\tilde{\chi}e$ is equal to \tilde{N} , its number of columns and that, by construction, T is a set of words corresponding to a maximal set of independent rows of $\tilde{\chi}e$. Thus, $\tilde{N} = \tilde{N}$ and we conclude that $\tilde{\chi}e$ is a nonsingular matrix.

3. Let us consider the intertwinning identity

$$\bar{\chi}f = \bar{\chi}e\bar{\mu}f = \bar{\mu}f\bar{\chi}e.$$

Since $\bar{\chi}e$ is nonsingular, we have identically $\tilde{\mu}f = (\bar{\chi}e)^{-1}\bar{\chi}f$ and $\tilde{\mu}$ has the property i of the statement.

Since the (1,1) entry of $\bar{\chi}f$ is exactly (r,f) we have $\text{Tr}(q\bar{\mu}f)=(r,f)$ where q is obtained from $\bar{\chi}e$ by replacing by zero every row except the first one; thus, depending upon (r,e)=0 or not we can find a nonsingular matrix m which is such that mqm^{-1} is a matrix in which all the entries

are zero except for the (1,1) entry or for the (N,1) entry, and the representation $\bar{\mu}f = m\tilde{\mu}fm^{-1}$ has the properties (i) and (ii).

We have already seen that μ' is a projection of μ and, by the same argument, it is easily verified that $\bar{\mu}$ is a projection of μ' , that is, finally, of μ .

4. Let us say that the set of words F' is (right) independent if the only linear relation

$$\sum_{f' \in F'} c_{f'}(r, ff') = 0$$

which is valid for all $f \in F$ is the trivial one in which all the coefficients $c_{f'}$ are zero.

It results instantly from the construction of $\tilde{\mu}$ and $\bar{\mu}$ that for given $r \in \bar{R}$ and \tilde{I} , the set S can be defined intrinsically as the maximal (right) independent set which is such that $f \in S$ implies that the set union of f and of the words $s \in S$ with $\tilde{I}s < \tilde{I}f$ is not (right) independent. In similar manner T can be defined intrinsically in terms of r and I only.

Consequently, if ν is any N''-dimensional representation of F, that is, such that $(r, f) = \nu f_{1N''}$ identically, we can apply to ν the construction described in 1 and 2 for μ and, although the first set T'' may be different from T', we are sure to obtain at the second and third steps the same sets S and T. Thus, $\tilde{\mu}$ is also a projection of ν and, consequently, $N'' \geq \bar{N}$; in particular, if $N'' = \bar{N}$, this implies that $a\nu fa^{-1} = \bar{\mu}f$ identically for some nonsingular matrix a and this concludes the proof.

This, of course, does not preclude the possibility that $(r, f) = \text{Tr}(p\nu'f)$ for some representation ν' of dimension less than \bar{N} and matrix p or sufficient rank.

However, the complete discussion of this case, i.e., of the algebra associated to r would take us too far away from the strictly linear techniques used in this note and it will be given elsewhere.

Since we have not proved that the matrices $\bar{\mu}x(x \in X)$ are integral matrices, it may be worthwhile verifying that the following definition of \bar{R} is equivalent to our previous one (cf. Fatou, 1904).

DEFINITION 3'. An element $a \in \bar{A}$ (i.e., a formal sum with integral coefficients) belongs to \bar{R} if and only if there exists a representation ν of F by arbitrary finite dimensional matrices which is such that $(a, f) = Tr(p\nu f)$ for some fixed matrix p.

Proof. By using the construction given in I.B.1. and then the construction of III.B.1, we may assume without loss of generality that, in fact, (a, f) is equal to the (1, N) entry of the matrix $\bar{\mu}f$ divided by a constant factor. Consequently, because of the intertwining identity $\bar{\chi}f$

 $\bar{\chi}em^{-1}\bar{\mu}fm$, i.e., $\bar{\mu}f = m(\bar{\chi}e)^{-1}\bar{\chi}fm^{-1}$, each entry of μf is a rational fraction in which the denominator K is an integer independent of f.

Thus, if v(f) is the vector equal to the first row of $\overline{\mu}f$, we can write $v(f) = v'(f) + K^{-1}v''(f)$ where v'(f) has integral coordinates and where the bounded vector v''(f) is equal to Kv(f) reduced modulo K. It follows that for any $x \in X$ the 2N-dimensional vector (v'(fx),v''(fx)) is entirely determined by x and the 2N-dimensional vector (v'(f),v''(f)) in the sense of Definition 1 and this concludes the proof via the reduction procedure of Section I.

Incidentally, it shows that if all the coefficients (r, f) of some $r \in \overline{R}$ are divisible by K, the element $K^{-1}r$ also belongs to \overline{R} .

C. Applications to the Theory of Kleene

III.C.1. If
$$F_{\alpha}$$
, $F_{\alpha'} \in \mathbb{R}$, then $F_{\alpha}F_{\alpha'} \in \mathbb{R}$.

PROOF. Let $F_{\alpha} = \{f: \mu f_{1N} \neq 0\}$; $F_{\alpha'} = \{f: \mu' f_{1,N'} \neq 0\}$. We can assume that for all $f, \mu f_{1,N}$ and $\mu' f_{1N'}$ are both nonnegative (cf. Section I.B). Then, if

$$r = \sum_{f \in F} f(\mu f)_{1N}$$
 and $r' = \sum_{f \in F} f \mu' f_{1N'}$,

we have

$$(rr',f) = \sum_{f'f'' \in F} (\mu f')_{1,N} (\mu' f'')_{1,N'}$$

that is, $(rr', f) \neq 0$ if and only if there exists at least one factorization f = f'f'' for which $\mu f'_{1,N} \neq 0$ and $\mu' f''_{1,N'} \neq 0$. Thus $F_{\alpha}F_{\alpha'} = \{f: (rr', f) \neq 0\}$. Since we know by III.A.2 how to construct $\mu'': F \to Z_{N+N'}$ such that $(rr', f) = \mu'' f_{1,N+N'}$ the result is proved.

III.C.2. If
$$F_{\alpha} \in \mathbb{R}$$
 then $F_{\alpha}^{0} \in \mathbb{R}$.

PROOF. Let $F_{\alpha} = f:(z,f) = \mu f_{1,N} \neq 0$ with $(z,f) \geq 0$ for all f, as above. We can write $F_{\alpha}^{\ 0} = \{e\} \cup (F_{\alpha} - \{e\})^{0}$ and, consequently, we can assume that F_{α} does not contain e. Then, as in III.B.3, it is easily checked that $F_{\alpha}^{\ 0} = \{f:(r^{0},f) \neq 0\}$ and the result follows from III.A.3.

There exists another type of invariance of the family of regular events which carries over to the family R; in order to describe it we still need the following definition.

Definition 4. A restricted right transducer η is given by the following structure:

- (1) A finite automaton with a (finite) input alphabet Y, a (finite) set of states Σ and a mapping $(\Sigma, Y) \to \Sigma$.
 - (2) A mapping $\eta:(\Sigma, Y) \to F$ where F is the monoid generated by

the (finite) alphabet X; η is extended in a natural fashion to a mapping $(\Sigma, F_Y) \to F$ (where F_Y is the monoid generated by Y) by the following rules:

For any state $\sigma_j \in \Sigma$, $\eta_j e = e$ (e: the empty word). For any state $\sigma_j \in \Sigma$ and input word $g = y_{i_1} y_{i_2} \cdots y_{i_n}$,

$$\eta_{j}g = \eta(\sigma_{i_{0}}, y_{i_{1}}) \eta(\sigma_{i_{1}}, y_{i_{2}}) \cdots \eta(\sigma_{i_{n-1}}, y_{i_{n}})$$

where $\sigma_{i_0} = \sigma_j$ and, inductively, $\sigma_{i_m} = (\sigma_{i_{m-1}}, y_{i_m})$.

(3) The two mappings $(\Sigma, Y) \to \Sigma$ and η satisfy the condition that if the state σ_j is such that $\sigma_j g = \sigma_j$ and $\eta_j g = e$ for some $g \neq e$, then $\eta_j g' = e$ for all input words $g' \in F_Y$ (we say then that σ_j is a sink).

Given a restricted right transducer η and an initial state σ_1 , we shall define an element $a \in \bar{A}$ (the sum *produced* by η) according to the following rule: For each $f \in F$, (a, f) is equal to the number of distinct words $g \in F_r$ which are such that $\sigma_1 g$ is not a sink and that $\eta_1 g = f$.

III.C.3. If the subset F' of F_Y belongs to R_Y (defined for Y as R was defined for X) then, for any state σ_i of Σ , the set $F_\alpha = \eta_i F' = \{\eta_i g \colon g \in F'; \sigma_j g \text{ is not a sink}\}$ belongs to R .

PROOF. The result is true if every state of Σ is a sink; let Σ' be the set of the states of Σ which are not a sink and assume that Σ' contains $M \ge 1$ elements.

For each finite N we shall consider the ring \bar{B}_N of the $N \times N$ matrices whose entries belong to the ring \bar{A} of the formal power series in the letters from X. To any $y \in Y$ we associate the matrix νy from \bar{B}_M with entries

$$\nu y_{jj'} = \eta(\sigma_j, y)$$
 if $\sigma_j y = \sigma_{j'}$; = 0, otherwise.

The matrices νg form a representation of F_Y in \bar{B}_N and for any $g \in F_Y$ and σ_j , $\sigma_{j'} \in \Sigma'$ we have

$$\nu g_{jj'} = \eta_j g$$
 if $\sigma_j g = \sigma_{j'}$; = 0, otherwise.

Let us now assume that $F' = \{g \in F_Y : \mu g_{1N} \neq 0\}$ where μ is a representation of F_Y in Z_N ; for the sake of simplicity we assume that $r = \sum_{g \in F_Y} g \mu g_{1N}$ is quasi regular. By applying the construction described in I.B.2. we can also assume that $\mu g_{1N} \geq 0$ for all $g \in F_Y$. Finally, for any $g \in Y$, let $\bar{\mu} y$ denote the matrix from $\bar{B}_{N \times M}$ obtained by replacing in μy each entry $\mu y_{ii'}$ by a submatrix identical to $(\mu y_{ii'}) \nu y$. Again this gives us a representation of F_Y which has the property that for any $g \in F_Y$ and σ_j , $\sigma_{j'} \in \Sigma$ the (1j,Nj') entry of $\bar{\mu} g$ is equal to (μg_{1N}) $\eta_j g$ if $\sigma_j g = \sigma_{j'}$ and to 0 otherwise.

Because of the condition (3) and of the hypothesis that r is quasi regular, the matrix $s = \sum_{u \in Y} \bar{\mu} y$ is also quasi regular and the (1j,Nj') entry of the quasi inverse u of s is equal to the sum $b_{jj'}$ of (μg_{1N}) $\eta_j g$ extended to all the words g from F_Y which send σ_j onto $\sigma_{j'}$. According to the remark III.A.4 and to the fact that every entry of s belongs to \bar{R} , this sum is also an element of \bar{R} . Consequently the sum b_j of all $b_{jj'}$ (where $\sigma_{j'} \in \Sigma'$) also belongs to \bar{R} and this proves the statement since $F_{\alpha} = \{f \in F: (b_j, f) \neq 0\}$ because of our hypothesis that $\mu g_{1,N}$ is always nonnegative.

IV. AN ELEMENTARY CHARACTERIZATION OF REGULAR EVENTS

We begin by verifying two remarks that are needed later.

Definition 5. Let \bar{R}^{pos} be the smallest subset (in fact, the smallest semiring) of \bar{A} which satisfies the following conditions:

- (i) $x \in \bar{R}^{pos}$ for any $x \in X$ and $e \in \bar{R}^{pos}$.
- (ii) If $a, a' \in \bar{R}^{pos}$ then a + a' and aa' also belong to \bar{R}^{pos} .
- (iii) If $a \in \bar{R}^{\text{pos}}$, then $a^{*0} \in \bar{R}^{\text{pos}}$.

IV.1. A necessary and sufficient condition that $a \in \bar{R}^{pos}$ is that $a = \sum_{f \in F} f \mu f_{1,N}$ where $\mu: F \to Z_N^{pos}$ and where Z_N^{pos} denotes the subset (in fact, the semiring) of the integral $N \times N$ matrices with nonnegative entries.

PROOF. It is sufficient to revert to I.B, III.A.2, and III.A.3 and to observe that if a, a' are produced by representations into Z_N^{pos} the same is true of a+a', aa' and a^0 ; also, trivially, μe and all the matrices μx belong to Z_N^{pos} . The construction performed in III.A.4. does not use subtraction either, and consequently $\sum f \mu f_{1,N} \in \bar{R}^{\text{pos}}$.

IV.2. \bar{R} is the smallest submodule of \bar{A} that contains \bar{R}^{pos} and any $r \in \Re$ can be written under the form r = r' - r'' with r', $r'' \in \bar{R}^{\text{pos}}$.

PROOF. Since every $r \in \bar{R}$ can be obtained from the generators x by a finite number of additions, subtractions, multiplications, and formation of inverses it is sufficient to prove that if the result is true for r_1 , $r_2 \in \bar{R}$ it is still true for $r_3 = r_1 + r_2$; $r_4 = r_1 - r_2$; $r_5 = r_1 r_2$ and $r_6 = (e - r_1^*)^{-1}$. Let us assume that $r_1 = r_1' - r_1''$; $r_2 = r_2' - r_2''$ where r_1' , $r_2'r_1''$ and r_2'' belongs to \bar{R}^{reg} . We have:

$$r_3 = (r_1' + r_2') - (r_1'' + r_2'');$$
 $r_4 = (r_1' + r_2'') - (r_1'' + r_2');$ $r_5 = (r_1'r_2' + r_1''r_2'') - (r_1'r_2'' + r_1''r_2')$

where again all the elements between brackets belong to \bar{R}^{pos} since this set is a semiring.

With respect to r_6 we observe first that $r_1^* = r_1'^* - r_1''^*$ and that $r \in \bar{R}^{\text{pos}}$ implies $(e - r^*)^{-1} - e = s \in \bar{R}^{\text{pos}}$ and, then, $r^* \in \bar{R}^{\text{pos}}$ since $r^* = (e - s)^{-1} - e$.

Now, for any $a, b \in \bar{R}$ with $a = a^*, b = b^*$ we have

$$e - a + b = (e - a)(e + (e - a)^{-1}b)$$

$$= (e - a)(e + (e - a)^{-1}b)(e - (e - a)^{-1}b)$$

$$(e - (e - a)^{-1}b)^{-1}$$

$$= (e - a)(e - ((e - a)^{-1}b)^{2})(e - (e - a)^{-1}b)^{-1}.$$

From this we get the identity

$$(e - a + b)^{-1} = (e - (e - a)^{-1}b)$$

$$(e - (e - a)^{-1}b(e - a)^{-1}b)^{-1}(e - a)^{-1}$$

$$= [(e - (e - a)^{-1}b(e - a)^{-1}b)^{-1}(e - a)^{-1}]$$

$$- [(e - a)^{-1}b(e - (e - a)^{-1}b(e - a)^{-1}b)^{-1}(e - a)^{-1}].$$

Thus, taking, $a = r_1'^*$ and $b = r_1''^*$, we can display $(e - r_1'^* + r_1''^*)^{-1}$ as the difference of two elements from \bar{R}^{pos} and the result is proved.

IV.3. A necessary and sufficient condition that $F_{\alpha} \in \mathsf{R}_0$ is that there exists some $r \in \bar{R}^{\mathsf{pos}}$ which is such that

$$F_{\alpha} = \{ f \in F : (r, f) \neq 0 \}.$$

Proof. The condition is necessary because, if $\alpha \in \mathfrak{C}_0$ is defined by a set Σ of N states, a mapping $(\Sigma, X) \to \Sigma$, an initial state σ_1 , a distinguished subset Σ' of Σ we can associate to every f the $N \times N$ matrix $\mu f_{ii'} = 1$ if $\sigma_i f = \sigma_{i'}$; = 0, otherwise, which gives a representation of F in $\mathbb{Z}_N^{\text{pos}}$. Trivially, if p is defined by $p_{ii'} = 1$ if i' = 1 and $\sigma_i \in \Sigma'$; = 0, otherwise, we have $\text{Tr}(p\mu f) = 1$ or 0 according to $f \in F_\alpha$ or not.

Thus, using the construction described in I.B.1 we can find a representation μ' of F in $Z_{N'}^{pos}$ which is such that the sum

$$r = \sum_{f \in F} f \mu' f_{1N'} = \sum_{f \in F} f \operatorname{Tr}(p \mu f)$$

has the desired properties.

 $m \in Z_N^{pos}$ as the matrix whose entries are $\beta(m_{ij}) \in 0,1$. Trivially, for any $m,m' \in Z_N^{pos}$ we have $\beta mm' = \beta m\beta m'$ and βZ_N^{pos} has at most $2^{N^2} < \infty$ distinct elements. Thus, the set βmf : $f \in F$ is a finite monoid M and $F_{\alpha} = \{f: \mu f_N \neq 0\} = \{f: \beta \mu f_{1,N} \neq 0\}$ is the inverse image by the homomorphism $\beta \mu : F \to M$ of a subset of M. In other words, F_{α} satisfies the condition that $F_{\alpha} = \beta^{-1}\beta F_{\alpha}$ where β is a homomorphism of the free monoid F into a finite monoid and, according to the theorem 6 of Bar-Hillel and Shamir, this is a necessary and sufficient condition that F_{α} belongs to R_0 .

IV.4. A necessary and sufficient condition that $F_{\alpha} \in \mathsf{R}_0$ is that there exists an element $r \in \bar{R}$ which is such that $\mid (r,f) \mid$ is bounded for all $f \in F$ and that $F_{\alpha} = \{ f \in F : (r, f) \neq 0 \}.$

Proof. The construction indicated in the proof of IV.3 shows that the condition is necessary. In order to prove that it is sufficient, it is enough to take any prime number p at least equal to twice the upper bound of | (r, f) | and to observe that the homomorphism γ which sends every integer upon its residue modulo p extends naturally to an homomorphism of Z_N onto the finite algebra of the $N \times N$ matrices over the Galois field of characteristic p; thus $F_{\alpha} = \{ f \in F : \mu f_{1N} \neq 0 \} = \{ f \in F : \gamma \mu f_{1N} \neq 0 \}$ and our remark is again a simple consequence of the theorem of Bar-Hillel and Shamir.

A. AN INTUITIVE DESCRIPTION OF @

IV.A.1. A necessary and sufficient condition that the element a from \bar{A} belongs to \bar{R}^{pos} is that it be produced by a restricted right transducer.

Proof. It is trivial that 0, e and each letter x from X can be produced by a (restricted, right) transducer; let us assume that the elements r and r' of \bar{R}^{pos} are produced by the transducers (η, Y, Σ) and (η', Y', Σ') respectively where, without loss of generality, we may assume that the two input alphabets Y and Y' and the two sets of states Σ and Σ' are disjoint. We consider new transducers η'' whose input alphabet Y'' is the union of Y and Y' and whose set of states Σ'' is the union of Σ , Σ' , a new initial state σ_1'' and a new sink σ_0'' ; for any such η'' we shall have the following rules:

- (i) $\sigma_1''y'' = \sigma_1 y$ and $\eta''(\sigma_1'', y'') = \eta(\sigma_1, y)$ if $y'' = y \in Y$; $\sigma_1''y'' = \eta(\sigma_1, y)$
- (i) of g and $\eta''(\sigma_1'', y'') = \eta'(\sigma_1', y')$ if $y'' = y' \in Y'$. (ii) $\sigma''y'' = \sigma y$ and $\eta''(\sigma'', y'') = \eta(\sigma, y)$ if $\sigma'' = \sigma \in \Sigma$ and $y'' = y \in Y'$ and, similarly, $\sigma''y'' = \sigma'y'$ and $\eta''(\sigma'', y'') = \eta'(\sigma'y')$ if $\sigma'' = \sigma' \in \Sigma'$ and if $y'' = y' \in Y'$.

- 1. Let now η_a'' be defined by the supplementary rule
- (iii) $\sigma''y'' = \sigma_0''$ when $\sigma'' = \sigma' \in \Sigma'$ and $y'' = y \in Y$ when $\sigma'' = \sigma \in \Sigma$ and $y'' = y' \in Y'$.

By construction η_a'' produces the sum r + r'.

- 2. Let η_m'' be defined by the rule (iii) when $\sigma'' = \sigma' \in \Sigma'$ and $y'' = y \in Y$ and the rule
- (iv) $\sigma''y'' = \sigma_1'y'$ and $\eta''(\sigma'', y'') = \eta'(\sigma_1', y')$ when $\sigma'' = \sigma \in \Sigma$ and $y'' = y' \in Y'$.

By construction, η_m'' produces rr'.

3. Let us assume that r is quasi regular and take for (η', Y', Σ') a copy of (η, Y, Σ) ; if η_{g}'' is defined by (iv) and the rule (iv') obtained by exchanging in (iv) the alphabets Y and Y' and the sets Σ and Σ' we obtain a transducer which produces the quasi inverse of r. According to Definition 5 this proves the necessity of the condition IV.A.1; that this condition is sufficient is a simple consequence of the construction indicated in the verification of III.B.3.

Since it has been remarked in IV.2 that any element of \bar{R} can be expressed as the difference of two elements of \bar{R}^{pos} we have at the same time verified that the definition 1 of α is equivalent with the following:

DEFINITION 1". An automaton α of α consists of a pair of restricted right transducers together with the rule that a word $f \in F$ is accepted if and only if $(r, f) \neq (r', f)$ where r and r' are the formal sums produced by the two transducers.

RECEIVED: April 3, 1961 REVISED: June 7, 1961

References

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

ELGOT, C. C. (1960). Trans. Am. Math. Soc. 98, 21.

FATOU, P. (1904). Compt. Rend. Acad. Sci. Paris 138, 342.

HARRINGTON, W. J. (1951). Am. Math. Monthly 58, 114.

HUFFMAN, D. (1954). Proc. Symp. Inf. Networks, p. 291. Polytechnic. Inst., Brooklyn, New York.

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

LAZARD, M. (1955). Ann. Sci. Ecole Normale Sup. (3) 72, 299.

MOORE, E. F. (1956). In "Automata Studies." Princeton Univ. Press, Princeton, New Jersey.

RABIN, M. AND SCOTT, D. (1958). I.B.M. Res. J. 3, 115.

Schützenberger, M. P. (1959). Seminaire Dubreil-Pisot, 1959-1960, Inst. H. Poincaré', Paris.

SKOLEM, T. (1934). Compt. Rend. 8 ème Congres Math. Scandinaves, Stockholm, p. 163.