CERTAIN ELEMENTARY FAMILIES OF AUTOMATA

M. P. Schutzenberger
Harvard Medical School, Harvard University

Reprinted from the
PROCEEDINGS OF THE SYMPOSIUM ON
MATHEMATICAL THEORY OF AUTOMATA

POLYTECHNIC INSTITUTE OF BROOKLYN
April 24, 25, 26, 1962

CERTAIN ELEMENTARY FAMILIES OF AUTOMATA

M. P. Schutzenberger*
Harvard Medical School, Harvard University

We attempt to relate the difficulty of the decision problem of certain algorithms (automata) with the underlying algebraic structure. In particular we discuss the connection between "push-down storage" and "extension of a free group by a finite monoid."

I. INTRODUCTION

This note is concerned with the definition of families of sets of words in a finite input alphabet X.

In contrast with the more usual approach, the motivation for this study is purely formal, the purpose being to obtain sets of words as near as possible to the family of the so-called "regular events" [25] by their definition and by their closure properties under the elementary set-theoretic operations.

As an illustration let us consider the case of X reduced to a single letter x. Then a set of words $F' = \{ x^{n_1}, x^{n_2}, \dots, x^{n_i}, \dots \}$ can be identified with the function from the natural numbers into $\{0, 1\}$ which, for each n, takes values 1 or 0 according to $x^n \in F'$ or not.

However, if one considers a process which *produces* the words of F' (as opposed to a process which *recognizes* or *accepts* them), more detailed information than " x^n is produced at least once" may be of some significance. Accordingly one may want to consider a numerical function (which we denote by (a, x^n)) expressing how many different ways (eventually zero) each word x^n is produced. A strictly equivalent procedure is to consider the *generating function*

$$a = \sum_{n \geq 0} (a, x^n) x^n$$

of the sequence (a, x^0), (a, x^1), $(a, x^2), \dots, (a, x^n), \dots$ With this notation, F' is the set of those x^n such that $(a, x^n) = 0$, that is, the *support* of the function a.

* Presently with the Faculte des Sciences, Poitiers, France.

Presented at the *Symposium on Mathematical Theory of Automata*, Polytechnic Institute of Brooklyn, April 24, 25, 26, 1962

In the present case, where $(a, x^n) \geq 0$ for all n, simple relations exist between the algebraic operations on generating functions and the elementary set-theoretic operations on their supports. In the more general case where (a, x^n) can be a negative integer, some analytic properties of the function a of x are reflected in the combinatorial nature of its support.

For instance, Skolem has proved[43] that if a is a rational function of x, it has an *ultimately periodic* support,[30] i. e., its support is a regular event. No corresponding result is known for a algebraic, but when the coefficient ring has non-zero characteristics, examples[27] show that the support is not necessarily a regular event. Moreover, the classical *gap theorems* [15] show that sets like $\{x^{n^2}: n > 0\}$ cannot be the support of an algebraic function over the field of complex numbers.

For the general case of X consisting of a finite number of variables, we need to define a non-commutative counterpart of the algebraic functions. This is done in Section II under certain restrictive hypotheses.

Then the algorithms by which the successive coefficients are computed can be reformulated in terms of automata, i. e., of representation of the free monoid F generated by X. As expected, these representations are among the most elementary from the point of view of the theory of monoids.

Indeed, the "algebraic" generating functions are associated with homomorphisms of F into a free group, i. e., with a special case of a so-called "push down storage." [37, 31]

In Section IV we list several problems concerning the supports which have been proved to be unsolvable.

Another presentation of this material but with a definitely different emphasis is given elsewhere by N. Chomsky and myself. [13] In fact, most of the remarks developed here (and especially the ones dealing with push down storage) are results of this collaboration over a period of many years.

II. FORMAL POWER SERIES

Let X be the finite input alphabet, F be the set of all words in the letters of X, and denote by (a, f) a mapping from F into the rational integers. To this mapping one associates the formal power series $a = \Sigma\{(a, f). f : f \in F\}$, which is an element of the completion of the free module generated by F. The set $R(X)$ of all such power series is a ring with addition $a + a' = \Sigma\{((a, f)(a', f)). f : f \in F\}$; non-commutative multiplication $aa' = \Sigma\{(a, f)(a', f'). f'' : f, f', f'' \in F; f'' = ff'\}$ (where ff' is the concatenation of f and f'); and multiplication by a scalar $n. a = \Sigma\{n(a, f). f : f \in F\}$. These are, of course, the usual operations when X consists of a single variable.

An element a of $R(X)$ is *quasi-regular* if the coefficient of the empty word in it is zero. Then a has a *quasi-inverse*

$$a^* = \sum_{n > 0} a^n$$

which satisfies $a^*a + a = a + aa^* = a^*$. R(X) also admits a *Hadamard product* (cf. reference 39) $a \circ a' = \Sigma \{ (a, f)(a', f). f : f \in F \}$. All these operations are continuous in the usual topology of R(X). The subset $R^{pos}(X)$ of the power series having non-negative coefficients is a *semi-ring* (i. e., it is closed under addition, multiplication and multiplication by a non-negative scalar) which contains the quasi-inverse of its quasi-regular elements.

The support, supp. a, of any $a \in R(X)$ is $\{ f \in F : (a, f) \neq 0 \}$. For any $a, a' \in R^{pos}(X)$:

$$\text{supp. } (a + a') = \text{supp. } a \cup \text{supp. } a';$$

$$\text{supp. } (a \circ a') = \text{supp. } a \cap \text{supp. } a';$$

$$\text{supp. } (a\, a') = (\text{supp. } a)\,(\text{supp. } a')$$

(= the "set product" of supp. a and supp. a').

If, further, a is quasi-regular,

$$\text{supp. } (a^*) = (\text{supp. } a)^* \left(= \cup \; \{ (\text{supp. } a)^n : n > 0 \}\right)$$

where in the right member (supp. a)* denotes Kleene's *star operation.*[25]

In fact these relations express the existence of a natural homomorphism (of semi-ring) sending $R^{pos}(X)$ onto the semi-ring B(X) of formal power series with boolean coefficients. For obvious reasons the direct study of $R^{pos}(X)$ is far more elementary than that of B(X).

DEFINITION 1: $R_{pol}(X)$ is the ring of the integral power series having a finite support. In other words, $R_{pol}(X)$ is the free (associative) algebra generated by X.

DEFINITION 2: $R^{pos}_{nil}(X)$ denotes the least semi-ring which contains every power series of the form $\Sigma \{ f : f \in F' \}$ where F' is an arbitrary regular event.

DEFINITION 3: $R^{pos}_{rat}(X)$ denotes the least semi-ring that contains X and the quasi-inverse of each of its quasi-regular elements.

Now let $Y = \{ y_j \}$ $(1 \leq j \leq N)$ be a set of $N < \infty$ new variables and consider an N-tuple $p = (p_j)$ of elements of $R_{pol}(X \cup Y)$. It is a *proper positive system* if it satisfies the conditions that for all $j, j' \leq N$:

1) $p_j \in R^{pos}(X \cup Y)$;

2) p_j is quasi regular;

3) $(p_j, y_{j'}) = 0$.

If, further, each $g \in$ supp. p_j has the form f or $fy_{j''}f'$ with f and f' belonging to the monoid generated by X, then p is a (two-sided) *linear system*. A linear system in which every f' is the empty word is a *right linear system*.

Let $u = (u_j)$ be an N-tuple of quasi-regular elements of $R(X)$ and define a homomorphism λ_u: $R(X \cup Y) \rightarrow R(X)$ by $\lambda_u y_j = u_j$, $\lambda_u x = x$ $(x \in X,\ y_j \in Y)$. It is trivial that any proper positive system p determines a *unique* quasi-regular N-tuple u such that for all $j \leq N$, $u_j = \lambda_u p_j$. Hence, u can be called "the solution" of p and we note that its coordinates belong to $R^{pos}(X)$.

DEFINITION 4: $R^{pos}_{alg}(X)$ is the least semi-ring that contains X and the coordinates of the solution of every proper positive system.

Clearly this definition is equivalent to the definition of the context free languages of Chomsky,[8, 9] and the coefficients in the solution precisely express the number of ways in which a word can be produced by the grammar corresponding to the system p.[18, 19]

It is trivial that $R^{pos}_{alg}(X)$ contains the quasi-inverses of its quasi-regular elements. Hence, $R^{pos}_{rat}(X)$ is a sub-semi-ring of $R^{pos}_{alg}(X)$. More accurately, an element of $R^{pos}_{alg}(X)$ belongs to $R^{pos}_{rat}(X)$ if and only if it is a coordinate of a proper positive linear right system. Thus, for any $a \in R^{pos}_{rat}(X)$, supp. a is a regular event.[8] Furthermore, $R^{pos}_{nil}(X)$ is a sub-semi-ring of $R^{pos}_{rat}(X)$ and $a \in R^{pos}_{rat}(X)$ belongs to $R^{pos}_{nil}(X)$ if and only if for all $\epsilon > 0$ and $f, f', f'' \in F$ one has $\lim\limits_{n \rightarrow \infty} (1+\epsilon)^{-n} (a, f'f^n f'') = 0$. The subset of $R^{pos}_{alg}(X)$, corresponding to the two-sided linear system, is not a semi-ring and $R^{pos}_{alg}(X)$ contains as a proper subset the least semi-ring which includes all these elements and the quasi-inverse of each of its quasi-regular members.

It is clear that if λ is the endomorphism of $R(X)$ induced by a mapping $\lambda x_i = a_i$ with $a_i \in R^{pos}_{rat}(X)$, the restriction of λ to $R^{pos}_{alg}(X)$ $\left[\text{resp. to } R^{pos}_{rat}(X)\right]$ is an endomorphism. Hence, as a variant of Jungen's theorem,[13] one verifies that $R^{pos}_{nil}(X)$ and $R^{pos}_{rat}(X)$

are closed for the Hadamard product and that $a \in R^{pos}_{rat}(X)$, $a' \in R^{pos}_{alg}(X)$ implies $a \circ a' \in R^{pos}_{alg}(X)$. It is well known[23] that $R^{pos}_{alg}(X)$ is not closed for the Hadamard product (even with X reduced to a single letter or with a more classical definition of the Hadamard product.[21, 4, 7]) In fact one has even the stronger result that for some pairs $a, a' \in R^{pos}_{alg}(X)$ the intersection of the supports of a and a' cannot be the support of a power series of the form $a'' - a'''$ where $a'', a''' \in R^{pos}_{alg}(X)$. $\left(\text{Take for instance } a = \Sigma\{x_1^n x_2^n x_3^{n'} : n, n' > 0\}\right.$ $\left. a' = \Sigma\{x_1^n x_2^{n'} x_3^{n'} : n, n' > 0\}\right)$. However, as in the commutative case, if p is an N-tuple of elements of $R^{pos}_{alg}(X \cup Y)$ satisfying conditions (1), (2) and (3) above, the system $\{y_j = p_j\}$ has a unique quasi-regular "solution" whose coordinates still belong to $R^{pos}_{alg}(X)$.

DEFINITION 5: $R_{nil}(X)$ (resp. $R_{rat}(X)$, $R_{alg}(X)$) is the least ring containing $R^{pos}_{nil}(X)$ (resp. $R^{pos}_{rat}(X)$, $R^{pos}_{alg}(X)$).

It follows from the definition of the semi-rings considered that each element of these rings can be expressed (in infinitely many ways) as the difference of *two* elements of the corresponding semi-rings. Hence, one could obtain directly $R_{nil}(X)$, $R_{rat}(X)$ or $R_{alg}(X)$ by replacing in definitions 2 and 3 the word *semi-ring* by the word *ring* or by omitting condition (1) in the definition of a proper system.

I stress once more that the only motivation I can offer for introducing the rings $R_{nil}(X)$, $R_{rat}(X)$, and $R_{alg}(X)$ is the strictly personal opinion that their definition is, in a sense, as simple as possible and, accordingly, that some reasonable families of sets of words are likely to include (or be included in) the corresponding families of supports.

Let α be the canonical homomorphism sending $R_{pol}(X)$ onto the ring of the ordinary (i. e., commutative) polynomials with integer coefficients. Clearly, one can extend α to epimorphisms of $R_{rat}(X)$ and $R_{alg}(X)$ onto the ring of the Taylor series expansions (with integer coefficients) of the ordinary rational and algebraic functions because,[3] for any $a \in R^{pos}_{alg}(X)$, there exists a finite constant $K > 0$ such that the quantity $(a, f)K^{-|f|}$ (where $|f|$ denotes the length of f) remains bounded over all $f \in F$.

If X consists of a single letter, $R_{nil}(X) = \alpha R_{nil}(X)$ is a rather classical object of study. I have no direct characterization of $\alpha\, R_{nil}(X)$ in the general case.

More specifically, let $\bar{a}$ be an ordinary rational function of the (commuting) variables $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_M$ $(1 < M < \infty)$ and assume that the coefficients of its Taylor series expansion $\bar{a} = \Sigma\, \bar{a}_{n_1, n_2, \ldots, n_M} \times \bar{x}_1^{n_1} \bar{x}_2^{n_2} \ldots \bar{x}_M^{n_M}$ are integers satisfying identically $|\bar{a}_{n_1, n_2, \ldots, n_M}| \leq (k + n_1 + n_2 + \ldots + n_M)!\, (n_1!)^{-1} (n_2!)^{-1} \ldots (n_M!)^{-1}$ for some fixed finite k. What supplementary conditions are needed to insure that $\bar{a} = \alpha\, a$ for at least one $a \in R_{nil}(X)$?

III. THE QUOTIENT MONOID OF AN AUTOMATON

Now we describe algorithms by which the coefficients in these formal power series can be computed.

For this purpose F (the set of all input words) is considered as the free monoid generated by the input alphabet X (with the concatenation as product). Then if an automaton $\bar{\sigma}$ is given by a set of states S and the so-called "next state" function[17] $(S, X) \to S$, one may identify $\bar{\sigma}$ with the representation of F by mappings $S \to S$ that extends $(S, X) \to S$ in a natural fashion. Thus $\bar{\sigma}$ determines a homomorphism σ of F onto a quotient monoid σF (the "quotient monoid of the automaton") by:

> for all $f, f' \in F$, $\sigma f = \sigma f'$ if and only if for all $s \in S$, $s.f = s.f'$ (i.e., if for any choice of an initial state $s \in S$, the states $s.f$ and $s.f'$ reached after reading f or f' are the same).

In other words, if $\sigma f = \sigma f'$ the automaton $\bar{\sigma}$ offers no possibility of distinguishing between them. Hence, the set F_σ of the words accepted by $\bar{\sigma}$ has the closure property $F_\sigma = \sigma^{-1} \sigma F_\sigma$.[2, 42]

For instance, Bar Hillel and Shamir have pointed out that the regular events are characterized by this closure property with respect to the homomorphisms σ of F into a *finite* monoid. This allows one to translate into algebraic language certain of the operations performed on the sets of words. Thus, trivially, if $F_1 = \sigma_1^{-1} \sigma_1 F_1$ and $F_2 = \sigma_2^{-1} \sigma_2 F_2$ are two subsets of F having the closure property with respect to the homomorphisms σ_1 and σ_2, their union and intersection are closed with respect to the homomorphism σ_3: $F \to \sigma_1 F \times \sigma_2 F$.

As another example, $\bar{\sigma}$ being a given automaton, let $\{F_i' : 1 \leq i \leq N'\}$ and $\{F_i'' : 1 \leq i \leq N''\}$ be two partitions of F into a finite number of regular events and let τ be an arbitrary mapping into F of the set of all triples (i', x, i'') $(1 \leq i' \leq N', x \in X, 1 \leq i'' \leq N'')$. Consider now a device $\bar{\tau}$ (see reference 22) which associates with each input word $f = x_1 x_2 \ldots x_m$ the word

$\tau f = \tau(i'_1, x_1, i''_1)\, \tau(i'_2, x_2, i''_2) \; . \; . \; . \; \tau(i'_m, x_m, i''_m)$ where, for each j, i'_j and i''_j are determined by $x_1 x_2 \, . \, . \, . \, x_{j-1} \in F'_{i'_j}$ and $x_{j+1} \ldots x_{m-1} x_m \in F''_{i''_j}$. Finally, we cascade $\bar{t}$ and $\bar{\sigma}$ in the sense that we take τf instead of f as the input of $\bar{\sigma}$. Denoting this composite automaton by $\bar{\sigma}'$, it is easily verified that the corresponding homomorphism σ' is a homomorphism into the *extension of* σF *by a finite monoid* in the sense of Redei.[36] (Let A and B be two monoids and denote by b^a ($a \in A$, $b \in B$) a representation of A by endomorphisms of B. If the mapping β: $(A, A) \rightarrow B$ is such that the product $(a, b)\,(a', b') = (aa', b^{a'}, \beta(a, a')b'^{\,a})$ on (A, B) is associative, the corresponding monoid is called an extension of B by A).

Let us now consider the simplest type of infinite monoid, i. e., the infinite cyclic group. An automaton $\bar{\sigma}$ such that σF is a submonoid of this group consists of a single "counter." It is described by associating with each $x \in X$ a positive or negative integer σx so that for each $f = x_1 x_2 \ldots x_m$, the counter records the total $\sigma x + \sigma x_2 + \ldots + \sigma x_m$. We say that an input word f is *accepted* if and only if σf does not belong to some specified *finite* subset of integers. Then, trivially, the set F_σ of the words accepted by $\bar{\sigma}$ is the support of a formal power series $a \in R_{nil}(X)$. It is easily shown that conversely:

If $a \in R_{rat}(X)$ is such that $|(a, f)| \; | \; 1 + |f| \; | \;^{-1}$ is bounded over all $f \in F$, then supp. a is the set of the words accepted by a finite automaton $\bar{\sigma}$ such that

1) σF is a submonoid of the extension of an infinite cyclic group by a finite monoid.

2) f is accepted only if it does not belong to a certain prescribed finite collection of cosets (i. e., if $s_o f \notin S'$ where the initial state $s_o \in S$ and the final *finite* subset S' of S are given).

With the same type of quotient monoid σF but with an opposite definition of the rule for accepting words (that is, f being accepted if and only if $s_o f$ does belong to some prescribed *finite* collection of integers), one easily shows that $\Sigma\{f : f \in F_\sigma\}$ belongs to $R^{pos}_{alg}(X)$. A well-known example of a set of this type is the set of all well-formed formula in parenthesis free notation. Several theorems on a similar but more general problem have been proved by Raney.[35]

I mention that this last example can be converted into a classical probabilistic problem, viz., finding the probability generating function corresponding to the usual random walk problem for an arbitrary (finite state) Markov process.

Following the customary hierarchy which ranks nilpotent groups next above abelian groups in order of simplicity, we have:

A necessary and sufficient condition that $F_\sigma \in \{\text{supp. } a: a \in R_{nil}(X)\}$ is that

1) σF be a submonoid of the extension by a finite monoid of a free nilpotent group;

2) f is accepted if and only if σf does not belong to some prescribed finite subset of σF.

As mentioned above this is a weak form of a well-known result in the theory of rational functions. A similar property holds for $\{\text{supp. } a: a \in R_{rat}(X)\}$ with (2) as before and (1) replaced by

1') σF is a submonoid of the ring Z_N of the NxN-integral matrices $(N < \infty)$.

In this more general case, the automaton $\bar{\sigma}$ consists of a finite part $\bar{\sigma}_0$ and of a "memory" in which an N-dimensional integral vector v can be stored. When reading the input word

$$f = x_{i_1} x_{i_2} \dots x_{i_j} \dots x_{i_n},$$

each successive letter x_{i_j} determines a bounded sequence of computation amounting to the multiplication of v by a certain NxN integral matrix μx_{i_j}. Thus, at the end of f, the memory contains the vector $v(f) = v_0 \, \mu x_{i_1} \mu x_{i_2} \dots \mu x_{i_n}$, and f is accepted if and only if v(f) does not satisfy a finite number of linear equations. These are the automata of the family A.

Let $|v(F)|$ denote the length of the vector v(f). By construction, $|v(f)|$ does not grow faster than an exponential function of the length, $|f|$, of the word f, but it may grow exactly at this rate. Hence, since the number of distinct words of length k or less is an exponential function of k, the memory V may be so well employed that $v(f) \neq v(f')$ for any two distinct words f and f', that is σ may be an isomorphism. In other words, the mapping f → v(f) may involve no compression of the data. Hence, it may be interesting to define a subfamily by requirements implying $\sigma F \neq F$.

The simplest condition is that $|v(f)|$ does not grow as fast as an exponential function of $|f|$, that is:

(*) For any $\epsilon > 0$ there exists a finite K such that $|v(f)| < (1+\epsilon)^{|f|}$ for all $f \in F$ of length $> K$.

Of course, this condition is equivalent to the one defining $R_{nil}(X)$ and it can be verified that for each $a \in R_{nil}(X)$ there exists a natural number d, the "degree" of a, having the following properties:

1) $(a, f)|f|^{-d}$ is bounded over all $f \in F$;

2) There are infinitely many words f such that $|(a, f)| |f|^{-d} \geq 1$.

Thus, the smaller the "degree" of a, the "smaller" is the homomorphic image σF. In particular, $d = 0$ characterizes the (infinite) regular events and the finite automata; $d = 1$ characterizes the example described at the beginning of this section.

An unsolved problem is to replace the rather obvious condition (*) by one involving only the rate of growth of the number of distinct vectors v(f) with the length of f.

Pushdown Storage

I am unable to construct a family of automata which would serve for $R_{alg}(X)$ in exactly the same fashion as the family A does for $R_{rat}(X)$. However, under a certain relaxation of the conditions, such a family has been devised by N. Chomsky[10] for $R^{pos}_{alg}(X)$. Related results have been obtained independently by R. G. Evey. The nearest approximation to the desired results involves the following definition.

DEFINITION: A subset F' or F is a D-event if and only if it is the intersection of a regular event with the kernel of a homomorphism of F into a free group. Then:

A necessary and sufficient condition that $a \in R_{alg}(X)$ is that $a = \Sigma \{\theta f\colon f \in F'\}$ for some homomorphism $\theta : F \rightarrow R_{pol}(X)$ and D-event F'.

(This, of course, provided that the infinite sum exists.)

The corresponding statement with $R_{rat}(X)$ instead of $R_{alg}(X)$ and F' a regular (instead of D-) event is trival. In both statements the regular event F" used can belong to the special subfamily of the sets F" defined by two subsets V' and V" of (X, X) and the condition:

$$f = x_{i_1} x_{i_2} \ldots x_{i_m} \in F'' \text{ if and only if } (x_{i_1}, x_{i_m}) \in V'$$

$$\text{and, for all } j, \ (x_{i_j}, x_{i_{j+1}}) \in V''.$$

In other words F" is the intersection of the complement of a *two-sided ideal* with a *quasi-ideal*. It is to be noted that the results are valid for any *unital* coefficient ring R (commutative or not) and that $\theta : F \rightarrow R_{pol}(X)$ can be restricted by the condition $\theta x = r.f$ with $r \in R$, $f \in F$ for all $x \in X$. Also the condition "F' is a D-event" can be replaced by "F' is the inverse image of a finite set for some homomorphism of F into the extension of a free group by a finite monoid."

In a still more restricted manner the D-event F' can be given the form $F' = F'' \cap F'''$ with F" as above and F''' defined in the following fashion:

Let $X = \left\{x_i\right\}$, $(i = \pm 1, \pm 2, \ldots, \pm N)$ where $N \geq 2$. Clearly, there exists a unique epimorphism γ of F(X) onto the free group G generated by all x_i's with $i > 0$ that identically satisfies $\gamma x_i \, \gamma x_{-i} = 1$. Then F''' is precisely the kernel of γ.

The fact that $\Sigma \left\{f\colon f \in F'\right\}$ belongs to $R^{\text{pol}}_{\text{alg}}(X)$ for any D-event F' follows from the construction which we now describe.

Let $\bar{\sigma}$ be an automaton consisting of a finite set of states S and of a tape (the "memory" of $\bar{\sigma}$) on which both writing and erasing are possible. Let Z be the alphabet used on this tape ánd G be the free monoid generated by Z. The automaton $\bar{\sigma}$ is given by:

1) A homomorphism ψ of G onto a finite monoid K;

2) A mapping $\sigma'\colon (S, K, X) \to S$;

3) A mapping χ of (S, K, X) into the set of all subsets of K,

4) A mapping $\alpha'\colon (S, K, X) \to G$.

Thus, the state of $\bar{\sigma}$ is a pair $(s, g) \in (S, G)$, and if the incoming input letter is x, the following operations are performed:

i) The finite part goes to $s' = \sigma'(s, \psi g, x)$;

ii) The word g is factored into a product $g' g''$ where g is the right factor of minimal degree such that $\psi g'' \in \chi(s, \psi g, x)$. (g" is the empty word if no such factor exists);

iii) g" is erased and replaced by the word $\alpha'(s, \psi g, x) (= g''')$.

Thus, the "next state function" is $(s, g)\cdot x = (s', g' g''')$. No essential gain in generality would accrue if the factorization $g = g'g''$ was determined by *two* finite state automata (with set of states S' and S") and a condition of the form:

g' and g" are such that

1) $s'_0 \cdot g' \in \bar{S}'$, $s''_0 \cdot g'' \in \bar{S}''$ where $\bar{S}' \subset S'$ and $\bar{S}'' \subset S''$ are functions of $s \in S$, ψg, and x;

2) g" has maximal or minimal length depending upon the triple $(s \in S, \psi g \in K, x \in X)$.

In some sense, $\bar{\sigma}$ can be considered as a very special case of a "pushdown storage." [31, 37] Here the essential restrictions are:

1) The memory consists of a single tape;

2) Any feedback from the memory to the finite part is via the

image of g by a fixed homomorphism into a *finite* monoid;

3) For each input letter only a ***bounded number*** of erasing and writing operations are permitted.

Now let $(s_o \in S,\ g_o \in G)$ be an initial state and $\overline{S}_1 = \{(s_{1,i}, g_{1,i})\}$ and $\overline{S}_2 = \{(s_{2,i}, g_{2,i})\}$ be two finite sets of states. We define

$$F_\sigma = \{ f \in F : (s_o, g_o) \cdot f \in \overline{S}_1,\ (s_o, g_o) \cdot f' \notin \overline{S}_2$$

for all left factor f' of $f\}$. Direct computation shows that

$$\Sigma \{ f : f \in F_\sigma \} \in R^{pos}_{alg}(X) .$$

Clearly the D-events (or the inverse image of a finite set for a homomorphism of F into the extension of a free group by a finite monoid) are special cases of such sets F_σ. This provides an independent verification of certain results of Kesten[24] concerning random walks over free groups.

It is conjectured that, conversely, if the inverse image F' of a finite set for some homomorphism ϕ of F into a group is such that $\Sigma\{ f : f \in F' \} \in R_{alg}(X)$, then ϕF is a submonoid of the extension by a *finite* group of a *free* group.

IV. SOME PROBLEMS CONCERNING THE SUPPORTS

We have defined six families of sets $\mathfrak{R}^i_j = \{ \text{supp. } a \in : a \in R^i_j(X)\}$ (i = nothing or pos, j = rat, nil, or alg), and we know that $\mathfrak{R}^{pos}_{nil} = \mathfrak{R}^{pos}_{rat}$ = the family $\mathfrak{R}_o$ of regular events. It can easily be proved that $\mathfrak{R}_{nil, d} = \{ \text{supp. } a : a \in R_{nil}(X),\ \text{Deg } a \leq d \}$ is a strictly increasing function of d and that $\mathfrak{R}_{nil, 2}$ contains sets which do not belong to $\mathfrak{R}^{pos}_{alg}$ (e. g., $\{ x^n y^m z^p : n^2 \neq mp\}$). Conversely, $\{ x^n y^n : n > 0 \} \in R^{pos}_{alg}$ but it does not belong to $\mathfrak{R}_{rat}$ (cf. reference 16).

Simple examples show that none of these families (except $\mathfrak{R}^{pos}_{rat}(X)$, of course) is closed under complementation.[38]

The first question is to determine whether or not $F' = F$ for a given set F' described as a member of one of these families; or, in other words, whether or not the corresponding automaton accepts all the possible input words.

It is trivial that to any diophantine equation E of degree d there corresponds at least one element $a \in R_{nil}(X)$ of the same "degree" such that E has a solution if and only if $0 = (a, f)$ for at least one $f \in F$, that is, if and only if supp. a F.

Conversely, for $d = 0, 1$ the problem of determining if supp. $a = F$ admits elementary solutions. The same problem for $d = 2$ (corresponding to the quadratic case for diophantine equations) relates to a question on (infinite) nilpotent monoids of class 1. For $d \geq 3$ the problem is at least as unsolvable as the ordinary diophantine problem.

For $a \in R_{rat}(X)$, a theorem of Markov shows that the same problem is unsolvable.[28] A fortiori, a similar negative result holds for $R_{alg}(X)$ and even for $R^{pos}_{alg}(X)$. However, in this case many more undecidability properties can be established because of the following construction due to Bar Hillel, Perles and Shamir.[1]

For each $f = x_{i_1} x_{i_2} \ldots x_{i_m} \in F$ we denote by $\widetilde{F}$ the word $x_{i_m} \ldots x_{i_2} x_{i_1}$ and, given a homomorphism $\alpha: F \to F$ we consider the two-sided linear equation $y = x_o + \Sigma\{ xy\, \alpha x: x \in X \}$ where x_o is a new letter not contained in X.

Its solution is the power series $a \in R^{pos}_{alg}(X \cup \{x_o\})$:

$$a = \Sigma\{\widetilde{f}\, x_o\, \alpha f: f \in F.$$

Repeating the same construction with a second homomorphism $\alpha' : F \longrightarrow F$, we obtain the power series $a' = \Sigma\{ f\, x_o\, \alpha' f: f \in F\}$.

The power series $a + a'$ also belongs to $R^{pos}_{alg}(X \cup \{ x_o\})$. Clearly, $a + a'$ has at least one coefficient ≥ 2 if and only if the supports of a and a' have a non-empty intersection; this last question is equivalent to Post's correspondence problem.[33]

Hence, trivially, the problem of determining whether an arbitary $b \in R^{pos}_{alg}(X)$ is or is not the generating function of its support (i. e., if an arbitrary context free grammar is or is not ambiguous[32]) is unsolvable.

In fact, Post's problem can be translated in many ways into the terminology used in this paper. For example, to any (one-way) two tapes finite automaton, one can associate a linear system whose solution is $\Sigma\{\widetilde{f}\, x_o\, f'\}$ where the summation is over all accepted pairs (f, f') of words. An especially simple case is the following.

Let us consider the equation

$$y = x_o + \Sigma\{\widetilde{\alpha' x}\, y\, \alpha x: x \in X\}$$

(with α, α' as above) whose solution is

$$a'' = x_o + \Sigma\{\alpha' \; \widetilde{f}\, x_o\, \alpha f: \; f \in F(X)\}$$

Let a''_o be the special case corresponding to $\alpha = \alpha' =$ the identity mapping. The support of a''_0 is the so-called ***mirror-image language*** of Chomsky.[8] Again $a'' + a''_0$ has at least one coefficient larger than one if and only if the Post's problem for α and α' has a solution

Assume now that α and α' are homomorphisms into the submonoid F' of F generated by $X' \subset X$ and that

1) All the words αx have the same fixed degree d.

2) For all $x, x' \in X$ if αx and $\alpha x'$ belong to the same proper left ideal of F then $\alpha' x = \alpha' x'$.

With this hypothesis, for any fixed word $\bar{f}' \in F'$, the problem of determining if the supports of a'' and $a''_0\bar{f}$ have a non-empty intersection is precisely the so-called "Tag problem."[29]

Many other unsolvability properties have been established by Bar Hillel, Perles and Shamir[1] using these constructions, and the remark that when α (or α') is a monomorphism of $F(X)$ into $F(X')$ (that is, when, e. g., the set $\{\alpha' x : x \in X\}$ is a set of ***code words*** having the ***unique decipherability*** property), then the generating function of the complement of supp. a'' in $F(X')$ is also the solution of a linear system.

REFERENCES

1. Y. Bar-Hillel, M. Perles, and E. Shamir, "On Formal Properties of Simple Phrase Structure Grammars," Tech. Report 4, Applied Logic Branch, Hebrew University of Jerusalem (July 1960).

2. Y. Bar-Hillel and E. Shamir, "Finite-State Languages," *Bull. Res. Council Israel,* Vol. 8F, pp. 155-166 (1960).

3. R. Birkeland, "Sur la Convergence des Devellopements qui Expriment des Racines de l' Equation Algebrique Generale...," *C.R. Acad. Sciences,* Vol. 171, pp. 1370-1372 (1920); Vol. 172, pp. 309-311 (1921).

4. S. Bochner and W.T. Martin, "Singularities of Composite Functions in Several Variables," *Ann. Math.,* Vol. 38, pp. 293-302 (1938).

5. A.W. Burks and H. Wang, "The Logic of Automata," *J. Assoc. Comp. Mach.,* Vol. 4, pp. 193-218, 279-297 (1957).

6. A.W. Burks, D.W. Warren, and J.B. Wright, "An Analysis of a Logical Machine Using Parenthesis-Free Notation," *Math. Tables and Other Aids to Computation,* Vol. 8, pp. 53-57 (1954).

7. R.H. Cameron and W.T. Martin, "Analytic Continuation of Diagonals," *Trans. Am. Math. Soc.,* Vol. 44, pp. 1-7 (1938).

8. N. Chomsky, "On Certain Formal Properties of Grammar," *Information and Control,* Vol. 2, pp. 137-167 (1959).

9. N. Chomsky, "A Note on Phrase Structure Grammars, *Information and Control,* Vol. 2, pp. 393-395 (1959).

10. N. Chomsky, "Context Free Languages and Push-Down Storage," Quart. Prog. Rep. No. 65, Research Laboratory of Electronics, M.I.T. (1962).

11. N. Chomsky and G.A. Miller, "Finite State Languages," *Information and Control*, Vol. 1, pp. 91-112 (1958).

12. N. Chomsky and G.A. Miller, "Mathematical Models of Language," in Luce, Bush and Galanter (Eds.) *Handbook of Mathematical Psychology*

13. N. Chomsky and M.P. Schutzenberger, "The Algebraic Theory of Context-Free Languages," in *Computer Programming and Formal Systems*, P. Braffort and D. Hirschberg, Eds. ["Studies in Logic Series"] (Amsterdam: North Holland Pub. Co.).

14. C.C. Elgot, "Decision Problems of Finite Automata Design and Related Arithmetics," *Trans. Am. Math. Soc.*, Vol. 48, pp. 21-51 (1961).

15. E. Fabry, "Sur les Points Singuliers d'une Fonction Donnee par Son Developpement de Taylor," Ann. Ecole Normale Sup. Paris (3), Vol. 13, pp. 367-399 (1896).

16. P. Fatou, "Sur les Series Entieres a Coefficients Entiers," *C.R. Acad. Sciences*, Vol. 138, pp. 342-344 (1904).

17. S. Ginsburg, "Some Remarks on Abstract Machines," *Trans. Am. Math. Soc.*, Vol. 96, pp. 400-444 (1960).

18. S. Ginsburg and H.G. Rice, "Two Families of Languages Related to Algol," Technical Memo., System Development Corporation, Santa Monica, Calif. (1961).

19. S. Ginsburg and G.F. Rose, "Operations which Preserve Definability in Languages, Technical Memo., System Development Corporation, Santa Monica, Calif. (1961).

20. J. Giveon, "Boolean Matrices and Their Application to Finite Automata," Technical Report No. 5, Applied Logic Branch, The Hebrew University of Jerusalem (September 1960).

21. U.S. Haslam-Jones, "An Extension of Hadamard Multiplication Theorem," *Proc. London Math Soc.*, Vol. II, Ser. 27, pp. 223-232 (1928).

22. D.A. Huffman, "Information Lossless Finite State Automata," *Nuevo Cimento Supp.*, Vol. 13, pp. 397-405 (1959).

23. R. Jungen, "Sur les Series de Taylor n'Ayant que des Singularites Algebrico-Logarithmiques sur Leur Cercle de Convergence," *Comm. Math. Helvetici*, Vol. 3, pp. 236-306 (1931).

24. M. Kesten, "Symmetric Random Walks on Groups," *Trans Am. Math. Soc.*, Vol. 92, pp. 336-354 (1954).

25. S.C. Kleene, "Representation of Events in Nerve Nets and Finite Automata," in *Automata Studies* (Princeton, N.J.: Princeton Univ. Press, 1956), pp. 3-41.

26. C.Y. Lee, "Automata and Finite Automata," *Bell Syst Tech J*, Vol. 39, pp. 1267-1296 (1960).

27. K. Mahler, "On a Theorem of Liouville in Fields of Positive Characteristic," *Canadian J Math*, Vol. 1, pp. 397-400 (1949).

28. M.A. Markov, "Ob odnoi nervazresimoi probleme," *Doklady Akad. Nauk: n s.*, Vol. 78, pp. 1089-1092 (1951).

29. M.L. Minsky, "Recursive Unsolvability of Post.s Problem of Tag," *Ann. Math.*, Vol. 74, pp. 437-455 (1961).

30. A. Nerode, "Linear Automaton Transformation," *Proc. Am. Math Soc.*, Vol. 9, pp. 541-544 (1958).

31. A.G. Oettinger, "Automatic Syntactic Analysis and the Pushdown Store," in *Proc. Symposia in Applied Math*, Vol. 12: *Structure of Language and Its Mathematical Aspects* (Am. Math. Soc., 1961), pp. 104-124.

32. R.J. Parikh, "Language Generating Devices," Quart. Prog. Report No. 60., Research Laboratory of Electronics, M.I.T., pp. 199-212 (January 1961).

33. E. Post, "A Variant of a Recursively Unsolvable Problem," *Bull Am Math Soc* , Vol. 52, pp. 264-268 (1946).

34. M.O. Rabin and D. Scott, "Finite Automata and Their Decision Problems," *I.B.M. J Res.*, Vol. 3, pp. 115-125 (1959).

35. G.N. Raney, "Functional Composition Patterns and Power-Series Reversion," *Trans Am Math Soc* , Vol. 94, pp. 441-451 (1960).

36. L. Redei, "Die Verallgemeinerung der Schreierschen Erweiterungs Theorie," *Act. Sci Math , Szeyed,* Vol. 14, pp. 252-273 (1952).

37. K. Samelson and F.L. Bauer, "Sequential Formula Translation," *Comm Assoc Comp Mach* Vol. 3, pp. 76-83 (1960).

38. S. Scheinberg, "Note on the Boolean Properties of Context Free Languages," *Information and Control,* Vol. 31, pp. 372-375 (1960).

39. S. Schottlander, "Der Hadamardsche Multiplicationsatz und weitere Kompositionsatze der Functionentheorie," *Math. Nachr.*, Vol. 11, pp. 239-294 (1954).

40. M.P. Schutzenberger, "Some Remarks on Chomsky's Context Free Languages," Quart. Prog. Report No. 63, Research Laboratory of Electronics, M.I.T. (October 1961).

41. M.P. Schutzenberger, "On Context-Free Languages and Push-Down Automata," to appear in *Information and Control,* 1963.

42. J.C. Shepherdson, "The Reduction ot Two-Way Automata to One-Way Automata," *IBM J.*, Vol. 3, pp. 198-299 (1959).

43. T. Skolem, *Comptes Rendus* (8-eme Congres des Math. Scandinaves, Stockholm, 1934), pp. 163-170.

44. G. Szego, "Uber Potenzreihen mit Endli ch Vielen Verschiedenen Koeffigenten," *Sitzber Preuss Akad. Wiss., Math Phys Kl.,* pp. 88-91 (1922).