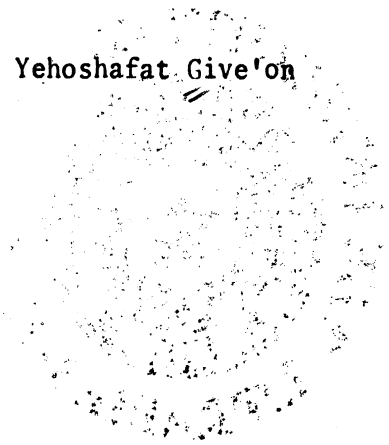
THE UNIVERSITY OF MICHIGAN

COLLEGE OF LITERATURE, SCIENCE, AND THE ARTS
Communication Sciences Program

Technical Report

THE APPLICATION OF ALGEBRAIC SYSTEMS TO FINITE AUTOMATA

Yehoshafat Give'on



ORA Project 04995

under contract with:

NATIONAL SCIENCE FOUNDATION
GRANT NO. 22258
WASHINGTON, D.C.

administered through:

OFFICE OF RESEARCH ADMINISTRATION ANN ARBOR

June 1963

§1 INTRODUCTION

In this paper we present a study of finite automata by means of the theory of finite monoids. In particular, we discuss constructions of direct products of finite automata. We do so in order to get Boolean combinations of finite automata and finite automata which define permutative events. In addition to these results, we reduce the basic decision procedures with regard to the behavior of finite automata to the study of the semi-ring extension of finite monoids.

Essentially, most of our results appear in various forms in the literature. However, by the application of the theory of finite monoids we get a uniform treatment of finite automata which yields more economical practical procedures.

§2 REGULAR ALGEBRAIC SYSTEMS

An algebraic structure of finite automata over the alphabet V can be described as a homomorphism of V*, the free monoid generated by V, in the following way.

Theorem 1 (Rabin-Scott): For any congruence relation ρ which is defined in V*, the set V^*/ρ of equivalence classes of ρ in V* forms a monoid (which is finite iff ρ is of a finite index) with respect to the operation defined in V^*/ρ by: $\rho(x)\cdot\rho(y) = \rho(xy)$.

Corollary 1.1: For any finite automaton $\mathcal{A}$, or any regular event $T(\mathcal{A})$, one can construct a system $\langle \rho, M_\rho, F \rangle$ where:

(i) M_ρ is a finite monoid,

(ii) ρ is a homomorphism of V* into M_ρ,

(iii) F is a subset of M_ρ;

such that

$$T(\mathcal{A}) = \rho^{-1}(F).$$

Thus, we can apply systems of the form defined in the corollary to Theorem 1, to describe finite automata and to generate regular events. We shall call such systems regular algebraic systems (or, in short, r.a. systems); $\langle \rho, M_\rho \rangle$ is said to be a structure of r.a. systems; and in particular, $\langle \rho, M_\rho \rangle$ is the structure of any r.a. system $\langle \rho, M_\rho, F \rangle$ for any $F \subseteq M_\rho$ (which will be called the designated set of $\langle \rho, M_\rho, F \rangle$).

The following theorem shows that regular algebraic systems form a special case of algebraic systems which generate regular events in the same way as r.a. systems do. The proof of Theorem 2 is straight forward and based on the application of right invariant relations to finite automata (Rabin-Scott, 1959).

Theorem 2: For any system of the form $\langle f, G, F \rangle$ where:

(i) G is a finite groupoid

(ii) f is a mapping of V^* into G which satisfies

$$f(xa) = f(x) \cdot f(a) \text{ for all } x \in V^* \text{ and } a \in V,$$

(iii) F is a subset of G;

the set $f^{-1}(F)$ is a regular event.

Remark: The condition stated in (ii) can be replaced by:

$f(ax) = f(a) \cdot f(x)$ for all $a \in V$ and $x \in V^*$; but now obviously, the equivalence relation induced by f is left invariant.

The relation between Rabin-Scott finite automata and regular algebraic systems is not one-one. An r.a. system $\langle \rho, M_\rho, F \rangle$ is said to generate the event $\rho^{-1}(F)$ and to simulate the Rabin-Scott finite automaton = $\langle M_\rho, M, e, F \rangle$ where M is the function from $M_\rho \times V$ to M_ρ defined by $M(m, a) = m \cdot \rho(a)$ and e is the identity element of M. Not every finite automaton can be simulated by an r.a. system (though it can be simulated by a system as described in Theorem 2); but as one can prove, if $\mathcal{A}$ is a minimal Rabin-Scott finite automaton, then the minimal r.a. system (with respect to the order of the monoid of the system) which generates $T(\mathcal{A})$ simulates $\mathcal{A}$. A compromise between the simulation of a given finite automaton and the generation of the event defined by the given finite automaton can be achieved by the following construction. Given the Rabin-Scott finite automaton $\mathcal{A} = \langle S, M, s_o, F \rangle$, the transition-monoid associated with $\mathcal{A}$ is the monoid of functions: $S \to S$ generated by

$\{f_a : a \in V\}$ where $f_a(s) =_{df} M(s, a)$. One can easily complete the transition monoid associated with $\mathcal{A}$ to be an r.a. system which generates $T(\mathcal{A})$ and represents $\mathcal{A}$ structurally (Buchi, 1960; Give'on, 1960). One can find a treatment of monoids associated with finite automata in this manner in (Myhill, 1960 & 1963).

§3 DIRECT PRODUCTS OF STRUCTURES OF R.A. SYSTEMS AND THEIR APPLICATIONS TO FINITE AUTOMATA

Our definition of direct products is a modification of the definition of direct product of finite automata (Rabin-Scott, 1959) in two aspects. We shall deal only with structures of finite automata via the structures of r.a. systems and leave the choice of the designated set free. This modification enables us to reduce various constructions of finite automata to the choice of a suitable designated set for a suitable direct product of structures. Furthermore, instead of using the direct product of the monoids under discussion, we take only a submonoid of it, which is in general a proper submonoid of the direct product. Thus, in general, we can save some unnecessary states.

Given two structures $\langle \rho, M_\rho \rangle$ and $\langle \sigma, M_\sigma \rangle$ we define

$$\langle \rho, M_\rho \rangle \times \langle \sigma, M_\sigma \rangle =_{df} \langle (\rho,\sigma), M_{(\rho,\sigma)} \rangle$$

where:

(i) $(\rho, \sigma): V^* \to M_\rho \otimes M_\sigma$ is defined by

$$(\rho, \sigma)(x) = (\rho(x), \sigma(x)) ,$$

(ii) $M_{(\rho, \sigma)}$ is the range of (ρ, σ), i.e., it is the submonoid of $M_\rho \otimes M_\sigma$, the direct product of M_ρ and M_σ, generated by

$$(\rho, \sigma)(V) = \{(\rho(a), \sigma(a)): \ a \in V \} .$$

For n structures $\langle \rho_i, M_{\rho_i} \rangle$ we define their direct product by induction:

$$\prod_{i=1}^{n} \langle \rho_i, M_{\rho_i} \rangle =_{df} \left(\prod_{i=1}^{n-1} \langle \rho_i, M_{\rho_i} \rangle \right) \times \langle \rho_n, M_{\rho_n} \rangle .$$

Clearly, any direct product grouping of n structures $\langle \rho_i, M_{\rho_i} \rangle$ is isomorphic to $\prod_{i=1}^{n} \langle \rho_i, M_{\rho_i} \rangle$ (the general associativity) and thus we can express it unambiguously by the form $\langle (\rho_1, \ldots, \rho_n) , M_{(\rho_1, \ldots, \rho_n)} \rangle$.

It is clear that the direct product of structures of r.a. systems is a structure of r.a. systems. Moreover, going back to Rabin-Scott's construction (Theorem 1), one can find that the congruence relation induced by the

homomorphism $(\rho_1,\ldots,\rho_n)$ is the intersection of the congruence relations induced by $\rho_1,\ldots,\rho_n$. This observation leads us to the first example of the application of direct products to finite automata; namely, to the construction of Boolean combinations of r.a. systems by means of direct products of structures of r.a. systems.

For any Boolean set function $\beta_S(X_1,\ldots,X_n)$, we denote by $\beta_P(X_1,\ldots,X_n)$ the corresponding Boolean propositional function which is isomorphic to $\beta_S(X_1,\ldots,X_n)$. (For example, if $\beta_S(X_1, X_2, X_3) = (X_1 \cap X_2) \cup (\overline{X}_1 \cap X_3)$, then $\beta_P(X_1, X_2, X_3) = (X_1 \,\&\, X_2) \vee (\sim X_1 \,\&\, X_3)$.)

Given n regular algebraic systems $\mathfrak{A}_i = \langle \rho_i, M\rho_i, F_i \rangle$ and a Boolean set function $\beta_S(X_1,\ldots,X_n)$ of n variables, we define:

$$\beta(\mathfrak{A}_1,\ldots,\mathfrak{A}_n) =_{df} \langle (\rho_1,\ldots,\rho_n),\ M_{(\rho_1,\ldots,\rho_n)},\ \beta^*(F_1,\ldots,F_n)\rangle$$

where:

(i) $\langle (\rho_1,\ldots,\rho_n),\ M_{(\rho_1,\ldots,\rho_n)}\rangle$ is the direct product of $\langle \rho_i, M\rho_i \rangle$,

(ii) $\beta^*(F_1,\ldots,F_n) =_{df} \{(m_1,\ldots,m_n) \in M_{(\rho_1,\ldots,\rho_n)}:\ \beta_P(m_1 \in F_1,\ldots,m_n \in F_n)\}$.

Theorem 3: For any Boolean set function $\beta_S(X_1,\ldots,X_n)$ of n variables and any n regular algebraic systems $\mathcal{A}_i = \langle \rho_i, M_{\rho i}, F_i \rangle$ we have

$$T(\beta(\mathcal{A}_1,\ldots,\mathcal{A}_n)) = \beta_S(T(\mathcal{A}_1),\ldots,T(\mathcal{A}_n))$$

(where $T(\mathcal{A})$ is the event generated by $\mathcal{A}$).

Proof: $x \in T(\beta(\mathcal{A}_1,\ldots,\mathcal{A}_n))$ iff $(\rho_1,\ldots,\rho_n)(x) \in \beta^*(F_1,\ldots,F_n)$; i.e., iff $\beta p(\rho_1(x) \in F_1,\ldots,\rho_n(x) \in F_n)$. Hence $x \in T(\beta(\mathcal{A}_1,\ldots,\mathcal{A}_n))$ iff $x \in \beta_S(T(\mathcal{A}_1),\ldots,T(\mathcal{A}_n))$.

Corollary 3.1: Given n k_i-state finite automata, any Boolean combination of the events defined by them is defined by a finite automaton with no more than $\prod_{i=1}^{n} k_i$ states.

Our next application of the direct product of structures of r.a. systems yields a characterization of the regular permutative events. An event $E \subseteq V^*$ is said to be permutative (or commutative in the terminology of Laing & Wright, 1962) iff for all $x \in E$ if y is a permutation of x then $y \in E$.

Let $V = \{a_1,\ldots,a_n\}$; we shall denote by $V^{(*)}$ the regular event

$a_1^* \cdot a_2^* \cdot \ldots \cdot a_n^*$.

Theorem 4: Let $E \subseteq V^*$ be a permutative event. E is regular iff $E \cap V^{(*)}$ is regular.

Corollary 4.1: $E \subseteq V^*$ is a regular permutative event iff it is the permutation-closure of a regular sub-event of $V^{(*)}$.

Proof: If E is regular then clearly $E \in V^{(*)}$, being an intersection of two regular events, is a regular event.

Assume that $E \cap V^{(*)}$ is regular and generated by the r.a. system $\mathcal{A} = \langle \rho, M_\rho, F \rangle$.

For each $1 \leq i \leq n$ we define the structure $\langle \rho_i, M_{\rho i} \rangle$ where:

(i) $M_{\rho i}$ is the submonoid of M_ρ generated by $\rho(a_i)$,

hence, $M_{\rho_i} =_{df} \{\rho(y): y \in a_i^*\}$;

(ii) ρ_i: $V^* \to M_{\rho i}$ is defined recursively by

1. $\rho_i(\lambda) = e$ (λ is the empty word over V and e is the identity element of M_ρ),

2. $\rho_i(a_i) = \rho(a_i)$, $\rho_i(a_j) = e$ for $i \neq j$,

3. $\rho_i(xy) = \rho_i(x)\rho_i(y)$.

Now let $\mathcal{A}^\pi =_{df} \langle(\rho_1,\ldots,\rho_n), M_{(\rho_1,\ldots,\rho_n)}, F^{(*)}\rangle$ where $\langle(\rho_1,\ldots,\rho_n), M_{(\rho_1,\ldots,\rho_n)}\rangle$ is the direct product of $\langle\rho_i, M_{\rho_i}\rangle$ and

$$F^{(*)} =_{df} \{(m_1,\ldots,m_n) \in M_{(\rho_1,\ldots,\rho_n)} : m_1 \cdot m_2 \cdot \ldots \cdot m_n \in F\}.$$

Clearly, if $x \in V^*$ and y is a permutation of x then $(\rho_1,\ldots,\rho_n)(x) = (\rho_1,\ldots,\rho_n)(y)$. Let $x \in V^{(*)}$, say $x = a_1^{k_1}a_2^{k_2}\ldots a_n^{k_n}$, then $\rho(x) = \rho_1(a_1^{k_1})\cdot\rho_2(a_2^{k_2})\cdot\ldots\cdot\rho_n(a_n^{k_n})$; hence if y is a permutation of $x \in E \cap V^{(*)}$ then $(\rho_1,\ldots,\rho_n)(y) \in F^{(*)}$. On the other hand, if $y \in V^*$ such that $(\rho_1,\ldots,\rho_n)(y) \in F^{(*)}$ then y is a permutation of $x \in E \cap V^{(*)}$. Hence, since E is permutative, $\mathcal{A}^\pi$ generates E and therefore E is regular.

§4 THE SEMI-RING EXTENSION OF MONOIDS AND ITS APPLICATIONS TO REGULAR ALGEBRAIC SYSTEMS

A system $\langle R, \circ, + \rangle$ is said to be a <u>semi-ring</u> iff:

(i) $\langle R, \circ \rangle$ is a monoid,

(ii) $\langle R, + \rangle$ is a commutative monoid,

(iii) $\circ$ is distributive over $+$ from both sides.

A semi-ring $\langle R, \circ, + \rangle$ is said to be <u>partially-ordered</u> iff R is partially ordered by the relation $\leqslant$ which is defined in R by $A \leqslant B$ iff_{df} $A + B = B$.

Obviously, a semi-ring $\langle R, \circ, + \rangle$ is partially-ordered iff $\langle R, + \rangle$ is an idempotent monoid.

For any given monoid M, let M^R be the monoid of the right translations of M which is isomorphic to M (under the correspondence $x \to f^R_x$ where f^R_x: $M \to M$ is defined by $yf^R_x =_{df} yx$; this is the monoid-theoretic generalization of Cayley's Theorem). Let R_M be the subalgebra of the binary relations in M with regard to complex-products and disjunctions which is generated by

M^R and contains 0 (the empty binary relation in M).

Clearly, the set of relations of R_M is the minimal set of binary relations in M which is closed under disjunction and includes M^R and contains 0. It is achieved by taking all the finite disjunctions of the relations in M^R including the empty disjunction which yields 0. Furthermore, R_M is a partially-ordered semi-ring which is finite iff M is finite.

A different method of embedding M in a partially-ordered semi-ring which is isomorphic to R_M is as follows.

Let $\langle P_f M, \circ, + \rangle$ be the algebra defined by:

(i) $P_f M$ is the set of all finite subsets of M,

(ii) $\circ$ is the operation of complex-product of subsets,

i.e., $A \circ B = \{ab: \ a \in A \ \& \ b \in B\}$,

(iii) + is the operation of set-union,

i.e., $A+B = A \cup B$.

Theorem 5: For any monoid M, $\langle P_f M, \circ, + \rangle$ is isomorphic to R_M under the correspondence f^R defined by $f^R(A) =_{df} \bigvee\{f^R_a: a \in A\}$.

Proof: Since any relation in R_M is a finite disjunction of the relations in M^R we get that f^R is a mapping of $P_f M$ onto R_M.

It is immediate that:

$$f^R(A+B) = f^R(A) \vee f^R(B) ,$$

and

$$f^R(A \circ B) = f^R(A) \cdot f^R(B) ,$$

hence f^R is a homomorphism of $\langle P_f M, \circ, + \rangle$ onto R_M.

Now, let A be any finite subset of M then $(e,a) \in f^R(A)$ iff $a \in A$, therefore $A = \{a: (e, a) \in f^R(A)\}$. Hence, if $f^R(A) = f^R(B)$ we get $\{a: (e, a) \in f^R(A)\} = \{b: (e, b) \in f^R(B)\}$ and therefore A = B.

Going back to finite monoids we have that R_M is isomorphic to the algebra of the subsets of M with regard to complex-products and unions of sets. Hence, we are allowed to use the simple notation of the algebra of the subsets of M in referring to R_M also. The proof of the following theorem

can be derived from the properties of n×n binary relations (as a special case of n×n lattice matrices, Give'on, 1963) or can be constructed independently.

Theorem 6: Let M be a finite monoid of order n. For any $A \varepsilon R_M$ we define $A^* =_{df} (I+A)^{n-1}$ where I = {e}; and get:

(i) for all $k \geq 0$: $A^k \leq A^*$ and thus $A^* = \bigvee_{k=o}^{\infty} A^k$;

(ii) for all $k \geq 0$: $A^k \cdot (A^n \cdot A^*) = A^n \cdot A^*$.

The importance of R_M to the study of finite automata, and in particular the importance of Theorem 6, is derived from the introduction of the analogue of the transition matrix associated with a finite automaton (Give'on, 1960) which was suggested first by Burks & Wang (as the characteristic matrix in Burks & Wang, 1957).

We associate with a given structure $\langle \rho, M_\rho \rangle$, of regular algebraic systems over the alphabet V, the element T_ρ of R_{M_ρ} which is defined by

$$T_\rho =_{df} \rho(V) = \{\rho(a): \ a \varepsilon V\} .$$

Clearly, $$T^k = \{\rho(x): \ x \varepsilon V^k\} = \rho(V^k)$$

and $T_\rho^* = \{\rho(x): \ x \in V^*\} = \rho(V^*)$.

Thus, Theorem 6 implies directly:

Corollary 6.1 Let $\mathcal{A} = \langle \rho, M_\rho, F \rangle$ be a regular algebraic system over the alphabet V, where M_ρ is a finite monoid of order n.

Then: (i) $\mathcal{A}$ generates a word of length k iff $T_\rho^k \cap F \neq \emptyset$

(ii) $\mathcal{A}$ generates a non-empty event iff $T_\rho^* \cap F \neq \emptyset$

(iii) $\mathcal{A}$ generates an infinite event iff $(T_\rho^n \circ T_\rho^*) \cap F \neq \emptyset$.

In fact, by introducing T_ρ, we associate with $\mathcal{A} = \langle \rho, M_\rho, F \rangle$, which is an r.a. system over V, another r.a. system $|\mathcal{A}| = \langle \tau, t_\rho^*, t_\rho^* \cap F \rangle$ over a single-letter alphabet {t}, where:

(i) t_ρ^* is the submonoid of R_M generated by T_ρ ,

(ii) τ is the homomorphism of $\{t\}^*$, the free monoid generated by t, onto t_ρ^* induced by $\tau(t) = T_\rho$.

The relation between $|\mathcal{A}|$ and $\mathcal{A}$ is given in statement (i) of Corollary 6.1, i.e.: $|\mathcal{A}|$ generates a word of length k iff $\mathcal{A}$ generates a

word of length k.

As an immediate result of this construction, we get the following well known property of regular events:

Corollary 6.2: Let E be any regular event and let $|E|$ be the set of non-negative integers defined by:

$k \varepsilon |E|$ iff$_{df}$ E contains a word of length k.

Then $|E| = S_1 \cup S_2$ where:

(i) S_1 is a finite set,

(ii) S_2 is a finite union of ultimately periodic sets with the same period.

Clearly, Corollary 6.1 provides us with effective procedures for the following basic decision problems concerning finite automata:

To decide whether a given regular algebraic system (or a given finite automaton) -

(i) generates a word of a given length;

(ii) generates a non-empty event;

(iii) generates an infinite event.

These three decision procedures are almost independent of the number of letters in V (only the construction of T_ρ is dependent on it). By the association of $|\mathcal{A}|$ they are, in fact, reduced to Rabin-Scott's procedures as applied to a single letter automaton.

The fact that $|\mathcal{A}|$ represents (in the manner discussed at the end of §2,) an n-state non-deterministic automaton, which is in general equivalent to a 2^n-state deterministic automaton; or the fact that there is no guarantee that t^*_ρ is of order n do not invalidate Corollary 6.1 as it stands.

Moreover, if we replace in Theorem 6 and in Corollary 6.1 the expression "M_ρ is a finite monoid of order n" by "M_ρ is isomorphic to a monoid of n×n binary relations" (or even "of n×n lattice matrices", Give'on 1963) then both Theorem 6 and Corollary 6.1 are applicable even to n-state non-deterministic automata since these automata are representable by r.a. systems with monoids of n×n binary relations.

We can shorten the computations involved in the decision procedures implied by Corollary 6.1 . Observe that for any $A \varepsilon R_M$, where M is of order n (or where M is isomorphic to a monoid of n×n binary relations) we have:

$$A^* = A([\lg_2(n)]+1) \ ;$$

where A(k) is defined recursively by:

$$A(1) = I+A, \ A(k+1) = (A(k))^2 \ .$$

Note also that in the case where M is isomorphic to a monoid of n×n binary relations (or of n×n lattice matrices) R_M can be taken as the minimal sub-semi-ring of n×n binary relations (lattice matrices) which includes M, which is a homomorphic image of the original R_M.

BIBLIOGRAPHY

[1] J. R. Buchi, "Mathematical Theory of Automata: Notes for a seminar," given by J. B. Wright and J. R. Buchi, Fall 1960, The University of Michigan

[2] A. W. Burks & H. Wang, "The Logic of Automata," J. ACM, Vol. 4, No. 2-3, April-July 1957.

[3] Y. Give'on , "Boolean Matrices and Their Application to Finite Automata," Technical Report No. 5 , Applied Logic Branch, The Hebrew University of Jerusalem, September 1960.

[4] - - - - - , "Lattice Matrices,"

[5] R. Laing & J. B. Wright , "Commutative Machines," Technical Note, The University of Michigan (ORA), December 1962.

[6] J. Myhill , "Transformation Groups Associated with Finite Automata," Programming Concepts, Automata and Adaptive Systems, College of Engineering, The University of Michigan, 1960 Summer Session.

[7] - - - - - , "Finite Automata, Semigroups and Simmulation," Automata Theory, College of Engineering, The University of Michigan, 1963 Summer Session.