DECOMPOSITION THEOREMS FOR FINITE SEQUENTIAL MACHINES(1)*

BY
M. MAGIDOR

ABSTRACT

In this work we present a different proof of results by K.B. Krohn and J. L. Rhodes [1], and give a new result on the same lines. These authors proved that every function computed by a finite state machine can be constructed by "elementary operations" on a set of "prime functions." By extending the scope of elementary operations, we now show that all functions computed by finite machines are built from a single function.

0. **Introduction and summary of results.** We study the family of functions defined on the set of all tapes (over a finite alphabet) which are computed by finite machines.

We define three elementary operations on functions.

(i) *Taking divisors* — F divides G if $F = f \cdot G \cdot g$ where g is homomorphism (code) of the domain of F into the domain of G (both domains are free semigroups) and f is a function from the range of G into that of F.

(ii) *Direct product* — $F_1 \times F_2$ operates on the set of tapes over $\Sigma_1 \times \Sigma_2$ where Σ_i is the alphabet of F_i and

$$(F_1 \times F_2)((a_1,b_1),(a_2,b_2),\cdots,(a_n,b_n)) = (F_1(a_1,\cdots,a_n),\ F_2(b_1,\cdots,b_n)). \tag{0.1}$$

(iii) *Composition* — $F_1 \cdot h \cdot F_2^{\wedge}$ — where:

$$F_2^{\wedge}(a_1,\cdots,a_n) = F_2(a_1), F_2(a_1,a_2),\cdots,F_2(a_1,\cdots,a_n) \tag{0.2}$$

and h is a code from the range of $F_2^{\wedge}$ into the domain of F_1.

The main result of Krohn and Rhodes states that the set of functions computed by finite machines can be generated by elementary operations from the set:

$$\{F_G \mid G \text{ is a simple group}\} \cup \{F_U\} \tag{0.3}$$

Received March 18, 1968.

[1] This work is based on a M.Sc. Thesis prepared at the Hebrew University of Jerusalem under the supervision of Professor M. Rabin. The author is deeply indebted to Professor M. Rabin for his interest and help in this work, and to Professor E. Shamir for his help in preparing this work for publication.

* Partially supported by ONR Information Systems Branch Contract No. F 61052–67–0055.

where for a finite semigroup S we define F_S as a function over S-(as alphabet) by

$$(0.4)\qquad F_s(s_1,\cdots,s_n)=s_1\cdots s_n \qquad s_i\in S.$$

The semigroup U is $\{a,b,I\}$ where:

$$(0.5)\qquad x\cdot I=I\cdot x=x \qquad y\neq I\Rightarrow x\cdot y=y \qquad x,y\in U.$$

If we allow a fourth elementary operation, that of tape reversing:

$$(0.6)\qquad F^{+}(a_1,\cdots,a_n)=F(a_n,\cdots,a_1)$$

we can prove that every function of a finite machine can be obtained from one distinguished function B whose alphabet is $\{0,1\}$ and:

$$(0.7)\qquad B(x_1,\cdots,x_n)=1 \quad\Leftrightarrow\quad \text{there is } i\leqq n \text{ such that } x_i=1$$

$$B(x_1,\cdots,x_n)=0 \quad \text{otherwise.}$$

The proof given here for the first result differs from Krohn-Rhodes' in the extensive use we make of algebraic results by D. Rees [6] on the structure of semigroups.

Plan of the paper. §§ 1–2 contain basic definitions and results of Rabin-Scott, Myhill, Krohn-Rhodes and D. Rees. These are stated here for the sake of completeness. §3 contains our proof of the main results of Krohn and Rhodes. §4 gives two applications for the main theorem. §§5–7 contain proof of our result about constructibility with four elementary operations (including tape reversing).

1. Basic definitions and elementary results.

DEFINITION 1.1. Let Σ be a finite set. A *tape* over Σ is a finite sequence of elements (symbols) of Σ. Σ^* is the set of all tapes over Σ (not including the empty sequence ϕ). $a_1a_2\cdots a_n$ is the tape $a_1,a_2,\cdots,a_n$. If $x,y\in\Sigma^*$ xy—denotes the concatenation of x and y.

Σ^* is a semigroup under the operation of concatenation.

DEFINITION 1.2. A sequential machine is an ordered 6-tuple $\langle\Sigma,S,M,B,f,s_0\rangle$ where:

Σ is a finite set—the input alphabet of the machine.

S is a countable set — the states set of the machine.

f is a function $f\colon S\to B$ — the output function.

$s_0\in S$ — the initial state of the machine.

A sequential machine is finite if S and B are finite.

We shall extend M to function from $S \times \Sigma^*$ into S. M is already defined on $S \times \Sigma$ i.e. for tapes of length 1 in the second argument. It is extended by induction on the length of tapes in Σ^*:

$$(1.1) \qquad M(s,ax) = M(M(s,a),x) \qquad a \in \Sigma,\ x \in \Sigma^*.$$

DEFINITION 1.3. The function of the machine $\alpha = \langle \Sigma, S, M, B, f, s_0 \rangle$ is the function:

$$(1.2) \qquad F_\alpha : \Sigma^* \to B \qquad F_\alpha(x) = f(M(s_0, x)).$$

A function $F:\Sigma^* \to B$ is said to be computable by a finite machine if $F = F_\alpha$ for some finite machine α.

Let F be a function $F:\Sigma^* \to B$ (Σ is finite, B is countable). By, "the equivalence relation of F" we shall mean the relation on Σ^* defined by:

$$(1.3) \qquad x \overset{F}{\equiv} y \Leftrightarrow F(txs) = F(tys) \text{ for all } t,s \in \Sigma^* \cup \{\phi\}.$$

The relation $\overset{F}{\equiv}$ is clearly an equivalence and even a congruence relation over Σ^* (with respect to concatenation). Naturally the classess form a semigroup. This semigroup S_F is called the semigroup of F. Its elements are $[x]_F$. (The equivalence classes of the tapes mod F).

THEOREM 1.1. *F is computed by a finite machine iff S_F is a finite semigroup.*

The proof is almost a restatement of a theorem by Myhill (cf. Theorem 1 in Rabin-Scott [5]).

We thus associate with every finite machine, a finite semigroup S_{F_α} which we also denote by S_α. Conversely with each finite semigroup we associate a finite machine $\alpha_S = \langle |S|, |S| \cup \{I\}, M, |S|, f, I \rangle$ where $|S|$ is the set of elements of S. I is an element not in $|S|$, $M(I,s) = s$, $M(s,t) = s \cdot t$ (the dot stands for the multiplication of S). Finally $f(s) = s$, the identity function.

A simple computation will verify that $F_{\alpha_S}(s_1 \cdots s_n) = s_1 \cdot \cdots \cdot s_n$ and $S_{\alpha_S} = S$. We also use the notation F_S for F_{α_S} — the function of the semigroup S.

From now on unless otherwise stated "a function" means a function of a finite machine. If $F:\Sigma^* \to B$, then Σ is the input alphabet of F and B is its output set. Also a "semigroup" always means a finite one.

DEFINITION 1.4. The function G divides a function F (G/F) if there is homomorphism h of Σ^* (Σ is the alphabet of G) into Γ^* (Γ is the alphabet of F) and a function f from the output set of F into the output set of G such that $G = f \cdot F \cdot h$ ($\cdot$ stands for composition of functions.) The relation F/F_{S_F} obviously holds with $h(x) = [x]_F$.

DEFINITION 1.5. The direct product $F \times G$ of F and G is defined on $(\Sigma \times \Gamma)^*$—(Σ, Γ are the input alphabets of F and G respectively) into the direct product of their output sets by:

$$(1.4) \qquad (F \times G)(a_1, b_1), (a_2, b_2), \cdots, (a_n, b_n) = (F(a_1 \cdots a_n), G(a_1 \cdots a_n)).$$

Let F be a function $F : \Sigma^* \to B$. $F^\wedge$ will denote the function: $F^\wedge : \Sigma^* \to B^*$.

$$(1.5) \qquad F^\wedge(a_1 \cdots a_n) = F(a_1), F(a_1 a_2), \cdots F(a_1 \cdots a_n).$$

DEFINITION 1.6. A composition of F and G is a function of the form $F \cdot h \cdot G^\wedge$ where h is a code (homomorphism) of C^* into Σ^* (C the output set of G, Σ the alphabet of F).

DEFINITION 1.7. The operations of taking divisors, direct product, and composition of functions are *elementary operations.*

DEFINITION 1.8. The semigroup S divides G (S/G) if S is homomorphic image of a subsemigroup of G.

DEFINITION 1.9. Let S and G be semigroups. The wreath product of S and G is the semigroup GWS whose elements are the pairs (F, s) with F a function from S into G, and $s \in S$.

The multiplication is defined by:

$$(1.6) \qquad (F, s) \cdot (R, t) = (K, s \cdot t) \text{ where } K(x) = F(x) \cdot R(x \cdot s) \text{ for } x \in S.$$

The dots stand for multiplication in S, G or GWS according to case.

DEFINITION 1.10. The operations of taking divisors and wreath product of semigroups will be called *elementary operations on semigroups.*

The direct product of semigroups is contained as a subsemigroup in their wreath product as one easily verifies.

2. Correspondence of functions and semigroups.

DEFINITION 2.1. Let U be the semigroup $\{a, b, I\}$ with

$$(2.1) \qquad x \cdot I = x \quad x \cdot y = y \text{ for } y \neq I, \quad x, y \in U$$

In [1] Krohn and Rhodes proved that a function F is constructible by elementary operations from a set of functions $\mathscr{F}$ and F_U if and only if S_F is constructible by elementary operations from U and the set of semigroups corresponding to the members of $\mathscr{F}$.

Now we state some lemmas asserting that certain semigroups and functions can be constructed from other semigroups and functions.

DEFINITION 2.2. $R_A : A^* \to A$, $L_A : A^* \to A$, $D_A : A^* \to A \cup \{I\}$ (for $I \notin A$) are the functions:

$$R_A(a_1, \cdots, a_n) = a_n$$

$$L_A(a_1, \cdots, a_n) = a_1 \tag{2.2}$$

$$D_A(a_1, \cdots, a_n) = a_{n-1},\ 1 < n \qquad D_A(a_1) = I.$$

For $A = \{a, b\}$ these functions will be denoted by R, L, D respectively.

A^R is the semigroup of R_A. (Its elements are the elements of A and $aa = ba = a$, $bb = ab = b$).

A^L is the semigroup of L_A.

LEMMA 2.1. *R_A, L_A, D_A are obtained from F_U by elementary operations.*

The construction of D_A uses a code which is not length preserving and this is the only place where we use such codes. We cannot avoid it completely because any function F obtained from F_U by elementary operations using length preserving code satisfies: $F(yxx) = F(yx)$ for each x, y in the alphabet of F whereas $D(yxx) = x \neq D(yx)$.

DEFINITION 2.3. $D_A^{(k)}$, the kth delay function on A, is the following function on A^*:

$$D_A^{(k)}\ (a_1 \cdots a_n) = a_{n-k} \quad \text{if } n > k \tag{2.3}$$

$$= n \qquad n \leqq k$$

LEMMA 2.3. *$D_A^{(k)}$ is obtained from D by elementary operations.*

Note that $D_A^{(0)} = R_A$, $D_A^{(1)} = D_A$. Again if $A = \{a, b\}$ we omit the subscript A.

DEFINITION 2.4. Let S be a semigroup. S^0 denote S with an external 0 adjoined and $\bar{S}$ denotes S with an external unit adjoined — (this unit is denoted by I_S).

LEMMA 2.3. *If S is obtained from a set of groups and U, then the same is true for $\bar{S}$ and S^0 using the same set of groups.*

DEFINITION 2.5. Let F: $\Sigma^* \to B$ then cF: $\{\Sigma \cup \{c\})^* \to B \cup \{c\}$ $(c \notin \Sigma)$ is the function:

$$cF(xcy) = F(y) \text{ for } y \in \Sigma^*, x \in (\Sigma \cup \{c\})^* \text{ and} \tag{2.4}$$

$$cF(xc) = c$$

(cF computes the value of F for the tail after the last occurrence of c).

LEMMA 2.4. *If F is obtained from $[\mathcal{F}_G \mid G \in \mathcal{G}\}$ where $\mathcal{G}$ is a set of groups and F_U, then the same is true for cF.*

Now we state some algebraic results used later:

THEOREM 2.5. ([6]): *In a finite semigroup the powers of each element contain idempotents.*

DEFINITION 2.6. An ideal $T \subset S$ is proper if $T \neq S$ and T contains more than one element.

DEFINITION 2.7. Let T be an ideal in S. $S - T$ will be the semigroup $(|S| - |T|) \cup \{0\}$ where the product $a \cdot b$ is changed to 0 if previously it was in T or if $a = 0$ or if $b = 0$.

DEFINITION 2.8. A semigroup is *simple* if it does not contain a proper ideal and it is not the semigroup $\{a, 0\}$ where $a \cdot 0 = 0 \cdot 0 = a \cdot a = 0 \cdot a = 0$. ($\{a, 0\}$ is called "the nilpotent semigroup.")

THEOREM 2.6. *Let S be finite. Then there exist a sequence of semigroups $S = S_0 \supset S_1 \cdots \supset S_n$ where S_{i+1} is an ideal of S_i while $S_i - S_{i+1}$ and S_n do not contain a proper ideal. (Such a sequence is called a composition series for S.)*

In fact one may further prove that the factors $S_{i+1} - S_i$ and S_n are unique in the sense that the same factors appear (possibly permutated) in any composition series (see [6]).

THEOREM 2.7. *S is simple iff $S = SxS$ for every $x \neq 0$, $x \in S$. (See [6]).*

COROLLARY 2.8. *Let S be finite and simple, then for every $x \in S$ there are idempotents l and f such that $lxf = x$.*

Proof. By Theorem 2.7 there are t and r in S such that $txr = x$ but then $t^p x r^p = x$ for any $p > 0$. The powers of each element contain idempotents (Theorem 4.1) and one can choose a common p such that t^p, r^p are idempotents.

THEOREM 2.9. *A finite simple semigroup with zero is of the form $L \times G^0 \times R - T$ where G is a group, and the product in $L \times G^0 \times R$ is defined by:*

$$(l, g, r)(t, h, s) = (l, gP_{r,t}h, s) \text{ where } P_{r,t} \in G^0. \tag{2.5}$$

Moreover for every $r \in R$ there is $l \in L$ such that $P_{r,l} \neq 0$ and for every $l \in L$ there is $r \in R$ such that $P_{r,l} \neq 0$. T is the ideal of all elements of the form $(l, 0, r)$.

For a proof see D. Rees [6] noting that by Corollary 2.8 every finite simple semigroup is completely simple in the sense of [6].

COROLLARY 2.10. *In a finite simple semigroup if $x_1 \cdots x_n = 0$ then there is $1 \leqq i \leqq n$ such that $x_i \cdot x_{i+1} = 0$.*

The assertion follows from Theorem 2.9. Indeed $x_1 \cdots x_n$ is zero if one of the x_i is zero or there are x_i and x_{i+1} of the form (m, g, n), (k, h, t) such that $P_{n,k} = 0$.

COROLLARY 2.11. *If* $x \cdot l = x$ *and* $x \cdot y = 0$ *(in a simple semigroup), then* $x \neq 0$ *implies* $l \cdot y = 0$ because if $x = (m, g, n)$ $y = (t, h, n)$ and $x \cdot y = 0$ then $P_{n,t} = 0$. Now $x \cdot l = x$ implies $l = (k, f, n)$ and then $l \cdot y = 0$.

DEFINITION 2.9. A finite semigroup is solvable if each of the factors $S_i - S_{i+1}$, S_n in its composition series which is not nilpotent semigroup is of the form $L \times G^0 \times R - T$ where G is a solvable group.

3. The main construction theorem.

In this section we find a minimal basis for the class of all functions computed by finite machines. Equivalently (by theorems of §2) we may consider semigroups instead of functions and define a basis for the finite semigroups. The corresponding functions will serve as functions basis.

DEFINITION 3.1. A prime semigroup is a finite simple group or U. A function is prime if it is of the form F_S where S is prime.

We can use the theorems of §2 freely because our basis contains F_U. If D was also included we could confine ourselves to the more restricted kind of elementary operations defined by length preserving codes.

THEOREM 3.1. *A semigroup without proper ideals is constructible from U and the prime groups dividing S.*

Proof. (a) The nilpotent semigroup is constructible because its function is obtained from R and D by first coding $h(x) = (x, x)$ $x \in \{0, a\}$, then operating with $R_{\{0,a\}} \times D_{\{0,a\}}$ and finally decoding by $f((x, y)) = 0$ $y \neq I$, $f((x, I)) = x$. The result is always zero unless the tape has length 1, in which case the tape is reproduced.

(b) Let S be a simple semigroup. We can assume that S contains a zero element, otherwise we deal with S^0 which is also simple and get S as a subsemigroup of S^0. The semigroup S is of the form $L \times G^0 \times R - T$ (cf. Theorem 2.9). It suffices to construct $S' = L \times G^0 \times R$ because S is a homomorphic image of it. Now:

$$S' \subseteq L \times (G^0 W \bar{R}) \tag{3.1}$$

L, R are semigroups of the form A^L, A^R respectively.

To prove this formula we define a homomorphism f of S' into $L \times (G^0 W \bar{R})$

$$\begin{aligned} f((l, g, r)) &= (l, F_{g,l}, r) \text{ where } F_{g,l}(I_R) = g \\ F_{g,l}(x) &= P_{x,l} \cdot g \end{aligned} \tag{3.2}$$

f is clearly one-to-one. Now:

$$f((l', y', r')) \cdot f((l, y, r)) \tag{3.3}$$
$$= (l', F_{g',l'}, r') \cdot (l, F_{g,l}, r) = (l', F, r)$$

where:

$$F(x) = F_{g'l'}(x) \cdot F_{g,l}(x \cdot r') \tag{3.4}$$

and since $x \cdot r' = r'$

$$F(x) = P_{xl'}g'P_{r'l}g = F_{g'P_{r'l}g}(x) \tag{3.5}$$

which proves that f is a homomorphism.

Since L and R are constructible from U we have only to show that every group is constructible from its normal divisors. For this it suffices to show that $G \subseteq NW(G/N)$. For the proof of this fact see [1].

THEOREM 3.2. *If S is a finite semigroup then F_S is obtained from the prime functions dividing it and F_U.*

Proof. By induction on the number of elements in S. If S is simple we use Theorem 3.1. Otherwise let J be a maximal proper ideal in S. Then $S - J$ contains no proper ideals. We distinguish two cases:

(1) $S - J$ is the nilpotent semigroup. This means that S is of the form $S = \{a\} \cup J$ with $a^2 \in J$ and $Ja \cup aJ \subseteq J$.

We code a given tape by $h(x) = (x, c)$ for $x \in J$ and $h(a) = (c, a)$. Then we operate with $(cR_{|J|} \times cD^{(k)})^{\wedge}$ where k is the least number such that there is an $n > k$ satisfying $a^n = a^k$ (see Theorem 2.5).

There results a tape in which the symbol (x, c) occurs if the original symbol was $x \in J$; (c, i) or (c, a) occurs if the original symbol was the ith 'a' in a run of 'a's ((c, i) if $1 \leqq i \leqq k$ and (c, a) if $i > k$.)

If we now have a tape $t_0 t_1 \cdots t_k$ we transform it into

$$(t_0, I)(t_1, t_0) \cdots (t_k, t_{k-1}) \cdots \tag{3.6}$$

by using a code $t \rightarrow (t, t)$ and a function $(R \times D)^{\wedge}$. Now we use the code:

(3.7) $((c, 1), I) \rightarrow (I_J, 1)$

$((c, i), (c, j) \rightarrow (I_J, i)$

$((x, c), (c, i)) \rightarrow (a^i \cdot x, c)$ $1 \leqq i < k$ $x \in J$ (note $a^i x \in J$).

$((x, c)), (c, a)) \rightarrow (x, c)$

$((c, a), t) \rightarrow (a^{r+1}, c)$ t any symbol and r is a number such that for every $n \geqq k$ $a^n \cdot a^r = a^n$.

(Such a number exists by Theorem 2.5 and [6].
a^r is the unit of the cyclic group.)

$((c,k),t) \to (a^k,t)$ t any symbol.

The idea here is to count length of 'a' runs. If it is less than k we multiply the element (of J) following the run by the power of 'a'. If the run is longer than k we replace the ith a ($i < k$) by (I_S, i) and the kth 'a' by (a^k, c). For 'a's beyond the 'k'th the product will not change if we replace 'a' by a^{r+1} since $a^{n+r} = a^n$ for $n \geqq k$. The second coordinate takes care of the case when the original tape concludes with an 'a' run.

Now we use $F_{\bar{J}} \times R_{[c,1,2,\dots,k-1]}$ and get (x,c) if the value of F_S on the original tape is x or (x,i) if that value is $x \cdot a^i$.

(2) $S - J$ is a simple semigroup. S consists of elements of J and of $|S| - |J|$. First we shall get rid of the case where a run of elements of $|S| - |J|$ in the tape multiplies to an element of J.

By Corollary 2.10 we can get an element of J only by multiplying two neighboring elements of $|S| - |J|$. By using the same kind of code and function as in the proof of the first case we pass from the tape $x_1 \dots x_n$ to (x_0, I), $(x_1 x_0) \dots (x_s, x_{s-1})$ (cf. Formula 3.6). Whenever we get a pair (x,y) where $x,y \in |S| - |J|$ and $y \cdot x \in J$ (that is $y \cdot x = 0$ in $S-J$), we know by Corollary 2.8 that there is an l, element in $|S| - |J|$ such that $y \cdot l = y$, hence by Corollary 2.11 $l \cdot x = 0$ (the product is in $S-J$). Hence $l \cdot x \in J$. Thus we replace those pairs by $(l \cdot x, c)$ and other pairs (x,y) by (x,c) if $x \in J$ or by (c,x) if $x \in S - J$.

Having done this, a run of elements of $S - J$ does not drop down to J. We compute the product by $(cR_J \times cF_{S-J})^{\wedge}$. We again use an appropriate coding and function to couple each element with its predecessor (or I) and code $((x,c)), (c,y)) \to (y \cdot x, c)$ (if $x \in J$ then $y \cdot x \in J$) $((c,y),t) \to (I_J, y)$ t any symbol $((x,c), (y,c)) \to (x,c)$, $((x,c),I) \to (x,c)$. This has the effect of adjoining the product of elements of $S - J$ to the succeeding element of J. We operate with $F_{\bar{J}} \times cR_{S-J}$ and get either (x,c) if the value of F_S on the original tape is x and (x,y) if the value of F_S on the original tape is $x \cdot y$. (We set $I_J \cdot y = y$ when $y \in S - J$.) The y appears whenever a certain tail of the original tape consists of elements of $S - J$. So finally we proved that we get F_S from F_{S-J}, F_J and U, which by the induction hypothesis proves the theorem. Q.E.D.

4. **Remarks and applications of the main theorem.** One also has a kind of uniqueness for the construction which follows from:

THEOREM 4.1. *Let G be a prime semigroup. If G/SWT then G/S or G/T.*

This Theorem is proved by Krohn-Rhodes ([1]).

Remark. Krohn and Rhodes in [2] introduced the notion of "complexity" of the semigroup S, $\#(S)$, defined as the minimal numbers of "blocks" of groups appearing in any construction of S from prime semigroups by elementary operations.

In [3] they proved a result about "continuity" of $\#(S) - \#(I) \leqq \#(S) \leqq \#(I) + 1$ where I is a maximal proper ideal in S. This result follows immediately from our way of proving the main theorem.

The simplest kind of a finite machine is a *counter*. A counter is a machine with alphabet $\{1\}$ and output $\{0, \cdots, k-1\}$ for some $k > 0$. The machine computes the length of the tape msololo k. In [1] it is actually proved that:

Theorem 4.2. *A function F is constructible by elementary operations from counters and F_U iff S_f is a solvable semigroup.*

Definition 4.1. A function is k definite if it depends only on the last k symbols of the tape. ($F(xy) = F(y)$ whenever the length of y is greater than k). A function is definite if it is k definite for some $k > 0$.

Theorem 4.3. *F is definite iff it is obtained by elementary operations from R and D.*

5. **The operation of tape reversing.** We add to our elementary operations on functions a new operation — tape reversing.

(5.1) $$F^{+}(a_1 \cdots a_n) = F(a_n \cdots a_1) \quad F^{+} \text{ is the reverse of } F.$$

The corresponding operation on semigroups, the reversing of a semigroup is the anti-isomorphic image of the semigroup. We denote the reverse of S by S^{+}. It will be convenient to use, instead of wreath product, another algebraic operation.

Definition 7.1. Let S and T be semigroups, X—an antihomomorphism of S into the endomorphisms semigroup of T, Y — a homomorphism of S into the endomorphisms semigroup of T and assume that every endomorphism Y_s permutes with every endomorphism X_{t},. Then the semidirect product of $\# S$ and $\# T$ directed by X and Y is $|T| \times |S|$ with multiplication:

(5.2) $$(\mu, s)(v, t) = (X_t(\mu) \cdot Y_s(v), s \cdot t).$$

We use the notation $\langle S, Y, T, X \rangle$ for this product. The conditions imposed on X and Y ensure that the multiplication is associative. We shall show that taking the wreath product instead of the semi-direct product as an elementary operation does not change the closure of a set of semigroups with respect to the enlarged set of elementary operations. I.e. the class of constructible semigroups is the same in both cases.

THEOREM 5.1. *$\langle S, Y, T, X\rangle$ is obtained by elementary operations from $\bar{S}$ and T.*

Proof. We extend X and Y to $\bar{S}$ by $X_{I_S}(\mu) = \mu$ and $Y_{I_S}(\mu) = \mu$ for all $\mu \in T$. To show $\langle S, Y, T, X\rangle \subseteq ((S_2 W\bar{S}_1)^+ W(\overline{S_1}{}^+)^+$ we define an isomorphism f from left to the right by

$$(5.3) \qquad f((\mu, s)) = (F_{\mu,s}, s) \text{ where } F_{\mu,s}(x) = (G_{\mu,x}, s) \text{ where}$$
$$G_{\mu,x}(z) = X_x Y_z(\mu) \qquad x, z \in \bar{S}$$

f is one-to-one because $F_{\mu,s}(I) = (G_{\mu,x}, s)$ and $G_{\mu,I_S}(I_S) = X_I(Y_I(\mu)) = \mu$ so $f((\mu \cdot s)) = f((\eta, t))$ implies $(\mu, s) = (\eta, t)$. That f is a homomorphism can be verified by direct computation using the permutability of X and Y.

The direct product is a particular case of semidirect product by choosing $X_s(\mu) = Y_s(\mu) = \mu$ for all $s \in S$, $\mu \in T$.

THEOREM 5.2. *The wreath product is obtained from S and T by semidirect products.*

Proof. We present TWS as a semidirect product of S and T^n (n is the number of elements in S). We take $X_s(F) = F$, $Y_s(F)(t) = F(t \cdot s)$ for all $s \in S$, $t \in T$.

Using the method of proof of our Lemma 2.3 in [1] we can prove (where "elementary operations" are in the new sense):

THEOREM 5.3. *If S is constructible by elementary operations from a set of semigroups with unit then S is constructible from the same set and U. (Actually we use only $\{a, I\} \subseteq U$).*

6. Finite automata.

DEFINITION 6.1. A finite automaton is a finite machine whose output alphabet is $\{0, 1\}$.

Let α be a finite automaton. The set of tapes generated by α is the set $K_\alpha = \{x \mid x \in \Sigma^*,\ F_\alpha(x) = 1\}$.

THEOREM 6.1. (*Kleene Representation Theorem*): *The class of sets of tapes over Σ^* generated by finite automata coincides with the closure of the class of finite sets of tapes under the operations:*

(a) *Union of two sets.*

(b) *Product of sets, given by $X \cdot Y = \{x \cdot y \mid x \in X, y \in Y\}$.*

(c) *The star operation X^* given by $\bigcup_{n=1}^{\infty} X^n$ where $X^1 = X$, $X^n = X^{n-1} \cdot X$.*

For proof see S. C. Kleene [4].

There are finite semigroups which are not semigroups of finite automaton, for instance A^R whenever A contains more than two elements, however every finite semigroup divides a direct product of semigroups of finite automata. This follows from:

THEOREM 6.2. *Let F be a function of a finite machine. There are finite automata $\alpha_1,\cdots,\alpha_n$ such that $F/F_{\alpha_1} \times \cdots \times F_{\alpha_n}$.*

7. **Construction with tape reversing.** In this section we prove that when the elementary operations include tape reversing then all functions are constructible from a single function B: $\{0,1\}^* \to \{0,1\}$ given by:

$$B(x_1,\cdots,x_n) = 1 \text{ if some } x_i = 1;\ B(0,\cdots,0) = 0 \tag{7.1}$$

The associated semigroup is also denoted by B. $B = \{a,I\} \subseteq U$.

By Theorems 5.1 and 5.2 in §5, we can use the semidirect product instead of wreath product as elementary operation on semigroups. Thus our elementary operations on semigroups are: Taking divisors, semidirect product, and anti-isomorphism. In order to use the results of §2 we must prove:

THEOREM 7.1. *F_U is constructible from B by elementary operations on functions.*

Proof. F_U is the reverse of $L:\{a,b,I\} \to \{a,b,I\}$ where

$$L(x_1\cdots x_m) = \text{The first } x_i \text{ different from } I \tag{7.2}$$

$$\text{if there is such } x_i \text{ and } I \text{ otherwise.}$$

To construct L we code the input tape $t_1\cdots t_n$ by $a \to \begin{pmatrix}1\\1\end{pmatrix}$ $b \to \begin{pmatrix}1\\0\end{pmatrix} I \to \begin{pmatrix}0\\0\end{pmatrix}$ and use $(BxB)^\wedge$.

Next we code

$$\begin{pmatrix}0\\0\end{pmatrix} \to \begin{pmatrix}0\\0\end{pmatrix} \quad \begin{pmatrix}1\\0\end{pmatrix} \to \begin{pmatrix}1\\0\end{pmatrix} \quad \begin{pmatrix}1\\1\end{pmatrix} \to \begin{pmatrix}0\\0\end{pmatrix} \tag{7.3}$$

and operate with $B \times B$. By calculation it is verified that the result is L, by approprite decoding.

Now to prove that every finite semigroup is obtained from B by elementary operations, it suffices by Theorem 6.2 to consider the semigroups of finite automata.

DEFINITION 7.1. Let F be a function. $F:\Sigma^* \to C$ then $\operatorname{Div} F:\Sigma^* \to \{0,1\}^{(c\times c)}$ is defined by: $\operatorname{Div} F(x_1\cdots x_n) = G$ where $G(a,b) = 1$ if the tape $x_1\cdots x_n$ is divisible into two tapes such that $F(x_1\cdots x_i) = a$, $F(x_{i+1}\cdots x_n) = b$.

THEOREM 7.2. *If F is obtained from B by elementary operations then the same is true for* $\operatorname{div} F$.

Proof. If F is obtained from B then S_F is constructible from B. We prove that:

(7.4) $$S_{div\,F}/\langle S_F, Y, B^{|S_F|^2}, X\rangle \text{ for suitable } X \text{ and } Y.$$

Indeed let $t \in |S_F|^2$ and $G: |S_F|^2 \to B$. We define X and Y by:

(7.5) $$X_s(G)(t) = 1 \Leftrightarrow \text{there is a } z = (x,y) \in |S_F|^2 \text{ such that } F(z) = 1 \quad \text{and} \quad t = (x, y \cdot s).$$

(7.6) $$Y_s(F)(t) = 1 \Leftrightarrow \text{ there is } z = (x,y) \in |S_F|^2 \text{ such that } F(z) = 1 \quad \text{and} \quad t = (s \cdot x, y).$$

It is verified directly that X and Y fulfil all conditions of semidirect products. We prove (7.4) by defining a homomorphism $\mathscr{F}$ of Σ^* into $\langle S_F, Y, B^{|S_F|^2}, X\rangle$ and showing that:

(7.7) $$\mathscr{F}(t) = \mathscr{F}(s) \text{ implies } t \overset{\operatorname{div} F}{\equiv} s.$$

$$\mathscr{F}(x_1 \cdots x_n) = (G, [x_1 \cdots x_n]_F) \text{ where}$$

(7.8) $$G((s,t)) = 1 \Leftrightarrow s = [x_1 \cdots x_n]_F \text{ and } t = I_{S_F} \text{ or } s = I_{S_F} \text{ and } t = [x_1 \cdots x_n]_F \text{ or there is } 1 \leqq i < n \text{ such that } s = [x_1 \cdots x_i]_F \text{ and } t = [x_{i+1} \cdots x_n]_F.$$

It is easily verified that $\mathscr{F}$ is homomorphism where in concatenation of two tapes X_s takes care of any division that cuts through the first tape and Y_s takes care of any division that cuts through the second tape. The implication (7.7) is a direct consequence of the definition of $\mathscr{F}$.

We denote $\langle S, Y, B^{|S|^2}, X\rangle$, X and Y as before by $\operatorname{Div} S$.

THEOREM 7.3. *Every semigroup of a finite automaton α is constructible from B by elementary operations.*

Proof. We use Kleene representation theorem (Theorem 6.1) to prove the theorem by induction on the sequence of Kleene's operations which constructs K_α from a class of finite sets of tapes. We can even start with finite automaton β that generates just one tape of length one.

The semigroup of such automata is easily seen to be the nilpotent semigroup and by Theorem 3.1 can be constructed from U which in turn, by Theorem 7.1, can be obtained from B. Next we examine the three inductive steps:

(a) $K = K_1 \cup K_2$ when K, K_i are generated by finite automata when the corresponding semigroups are S, S_i respectively. Then $S/S_1 \times S_2$ because the familiar construction of the finite automaton that generates $K_1 \cup K_2$ is the direct product of the finite automata that generate K_1 and K_2 (cf. Rabin-Scott [5], Theorem 6).

(b) $K = K_1 \cdot K_2$ with S, S_i as before, then $S/\mathrm{Div}(S_1 \times S_2)$ because a tape belongs to $K_1 \cdot K_2$ if it can be divided into two tapes which are of equivalence classes (x, y), (s, t) with respect to $F_{S_1 \times S_2}$ and x is an equivalence class of tapes belonging to K_1 and s is an equivalence class of tapes that belong to K_2. Therefore all the division possibilities of a tape with respect to $F_{S_1 \times S_2}$ determine its behaviour with respect to F_S and so also with respect to $K_1 \cdot K_2$.

(c) S is the semigroup of K^*, G is that of K then $S/\langle \mathrm{Div}\, G, Y, B^{|\bar{G}|^3}, X \rangle$ for suitable X and Y. X and Y are defined by:

(7.9) $X_g(F)(\mu) = 1 \Leftrightarrow \mu = (x, y, z) \quad g = (M, \sigma) \quad M: |\bar{G}|^2 \to B$
and there is z_1 such that $z = z_1 \cdot \sigma$ and $F((x, y_1, z_1)) = 1$
or there is $(t, z) \in |\bar{G}|^2$ and $(x, y_1, z_1) \in |G|^3$ such that
$y = y_1 \cdot z_1 \cdot t$, $z_1 \cdot t$ is an equivalence class of tapes
in K, $M((t, z)) = 1$ and $F(x, y_1, z_1) = 1$.

(7.10) $Y_g(F)(\mu) = 1 \Leftrightarrow \mu = (x, y, z) \quad g = (M, \sigma) \quad M: |G|^2 \to B$
and there is x_1 such that $x = \sigma \cdot x_1$ and $F(x_1, y_1, z) = 1$
or there is $(x, t) \in |\bar{G}|^2$ and $(x_1, y_1, z) \in |G|^3$ such that
$y = t \cdot x \cdot y$ and $t \cdot x_1$ is an equivalence class of tapes in K,
$M(x, t) = 1$ and $F(x, y_1, z) = 1$.

A tedious computation, however without any essential difficulty, proves that X and Y fulfil all conditions for semidirect products. We define a homomorphism $\mathscr{F}$ of Σ^* into $\langle \mathrm{Div}\, G, Y, B^{|\bar{G}|^3}, X \rangle$ such that two tapes that are mapped to the same element are equivalent with respect to K^*.

(7.11) $\mathscr{F}(t) = (F, [t]_{\mathrm{Div}\, F_G})$ where $F(x, y, z) = 1 \Leftrightarrow$ there is a division of the tape t into three tapes of the classes x, y, z with respect to K and the middle tape belongs to K^* or it is the empty tape. (We allow the case that one or two of the tapes occurring in the division of t are empty, in that case the corresponding coordinate in (x, y, z) is I_G.)

$\mathscr{F}$ is verified to be a homomorphism of Σ^*. Moreover, the value of $\mathscr{F}(t)$ determines the behaviour of t with respect to K^* so we get the result. Q.E.D.

Now we prove that B is really elementary because:

THEOREM 7.3. *If $B/\langle S, Y, T, X \rangle$ then either B/S or B/T.*

Proof. Suppose $B/\langle S, Y, T, X \rangle$ then $B = f(H)$, f homomorphism $H \subseteq \langle S, Y, T, X \rangle$ and H is minimal. Let I be an idempotent such that $f(I) = 0$.

(The set of elements of H such that $f(x)=0$ is a subsemigroup of H.) $f(lHl)=f(l)\cdot f(H)\cdot f(l)=0\cdot B\cdot 0=B$ therefore by minimality of H $l\cdot H\cdot l=H$ and l is a unit element of H. Let a be an idempotent such that $f(a)=1$ then $\{a,l\}$ is isomorphic to B.

Let $l=(I_1,I_2)$ $a=(a_1,a_2)$. Clearly $I_2\cdot a_2=a_2\cdot I_2=a_2\cdot a_2=a_2$ and $I_2\cdot I_2=I_2$.

If $a_2\neq I_2$ then $\{a_2,I_2\}$ is isomorphic to B and $B\subseteq S$. If $a_2=I_2$ we get $l'=Y_{I_2}(X_{I_2}(I_1))$ and $a'=Y_{I_2}(X_{I_2}(a_1))$. Using the fact that $\{l,a\}$ is isomorphic to B we can show $a'\neq l'$ and $\{a',l'\}$ is isomorphic to B and so $B\subseteq T$. Q.E.D.

References

1. K. B. Krohn and J. L. Rhodes: *Algebraic theory of machines. Prime decomposition theorem for semigroups and machines*, Trans. Amer. Math. Soc., **116** (1965), 450–464.

2. K. B. Krohn and J. L. Rhodes: *Complexity of finite semigroups and finite state machines*, to appear in Proc. of the Conference on Algebraic Theory of Machines, Languages and Semigroups.

3. K. B. Krohn, R. Mateosian and J. L. Rhodes: *Ideals in finite semigroup and finite state machines*, Mathematical System Theory **1** (1967), 59–66.

4. S. C. Kleene. *Representation of events in nerve nets*, Automata Studies, Princeton (1956), 3–41.

5. M. O. Rabin and D. Scott: *Finite automata and their decision problems*, IBM Journal of Research and Development, **3** (April 1959), 114–122.

6. D. Rees: *On semigroups*, Proc. of the Cambridge Phil. Soc., (1940), 387–400.

The Hebrew University of Jerusalem