ALGEBRAIC THEORY OF MACHINES. I. PRIME DECOMPOSITION THEOREM FOR FINITE SEMIGROUPS AND MACHINES

BY

KENNETH KROHN([1]) AND JOHN RHODES

Introduction. In the following all semigroups are of finite order. One semigroup S_1 is said to divide another semigroup S_2, written $S_1|S_2$, if S_1 is a homomorphic image of a subsemigroup of S_2. The semidirect product of S_2 by S_1, with connecting homomorphism Y, is written $S_2 \times_Y S_1$. See Definition 1.6. A semigroup S is called irreducible if for all finite semigroups S_2 and S_1 and all connecting homomorphisms Y, $S|(S_2 \times_Y S_1)$ implies $S|S_2$ or $S|S_1$. It is shown that S is irreducible if and only if either:

(i) S is a nontrivial simple group, in which case S is called a prime; or

(ii) S is one of the four divisors of a certain three element semigroup U_3 (see Definition 2.1) in which case S is called a unit.

We remark that an anti-isomorphism of a unit need not be a unit. Thus the theory is not symmetric. The explanation is that semidirect product can be written from the left or from the right.

Let $\mathcal{S}$ be a collection of finite semigroups. We define $K(\mathcal{S})$ as the closure of $\mathcal{S}$ under the operations of division and semidirect product. See Definition 3.2. Then it is proved that $S \in K(\mathcal{S} \cup \{U_3\})$ if and only if $\text{PRIMES}(S) \subseteq \text{PRIMES}(\mathcal{S})$. Here $\text{PRIMES}(S) = \{P|\ P$ is a nontrivial simple group and P divides $S\}$ and $\text{PRIMES}(\mathcal{S}) = \bigcup \{\text{PRIMES}(S) | S \in \mathcal{S}\}$. In particular, $S \in K(\text{PRIMES}(S) \cup \{U_3\})$. A counterexample to the conjecture that $S \in K(\text{IRR}(S))$ justifies the distinction between primes and units as well as the inclusion of U_3 in the above formulas.

A novel feature of this paper is the use of functions on free semigroups, i.e. machines, to prove facts about finite semigroups.

These above results are obtained as an immediate corollary of a more general theorem (proved here) which finds application as the basis for a prime decomposition theorem for finite state sequential machines. Further, by applying this theorem together with the powerful solvability criteria of Feit and Thompson and of Burnside, we find that Corollary 4.1 answers in important cases the question "What machines can be constructed by series-parallel from counters, delays and units?" See §4. A heuristic discussion of this paper occurs in [6].

Received by the editors July 16, 1963.

([1]) This research was sponsored in part by the Office of Naval Research, Information Systems Branch, Contract Number: Nonr-4138(00).

Both authors want to thank Professor Warren Ambrose for his important encouragement in the early days of this work.

1. Elementary properties of machines.

NOTATION 1.1. In this paper $A, B, C, \cdots$ will denote nonempty sets. $\sum A$ denotes the free noncommutative semigroup without identity on the generators A. A machine will be any mapping $f: \sum A \to B$([2]). The natural "extension" $\bar{f}: \sum A \to \sum B$ is defined by $\bar{f}(a_1, \cdots, a_n) = (f(a_1), \cdots, f(a_1, \cdots, a_n))$. We also write $\bar{f}$ as $(f)^e$.

Let $h: A \to B$. Then $\hat{h}$ is the unique extension of h to a homomorphism of $\sum A$ into $\sum B$. Thus $\hat{h}(a_1, \cdots, a_n) = (h(a_1), \cdots, h(a_n))$.

DEFINITION 1.1. Let $f: \sum A \to B$ and $g: \sum C \to D$. Then $f|g$, read f divides g, if and only if there exists a homomorphism $H: \sum A \to \sum C$ and a function $h: D \to B$ so that $f = hgH$.

DEFINITION 1.2. Let $f: \sum A \to B$. Then S_f is the semigroup given by the congruence $\equiv_f$ on $\sum A$. Here $t \equiv_f r$ if and only if $f(\alpha t \beta) = f(\alpha r \beta)$ for all α, β in $\sum A$ or α, β empty. The equivalence class containing t will be denoted by $[t]_f$. The mapping $j_f: S_f \to B$ sending $[t]_f$ to $f(t)$ induces the partition P_f on S_f and (S_f, P_f) is termed the normal form of f. $\mathrm{NF}(f) = (S_f, P_f)$.

DEFINITION 1.3. Let (S_1, P_1) and (S_2, P_2) be two semigroups with partitions. Then $(S_1, P_1)|(S_2, P_2)$, read (S_1, P_1) divides (S_2, P_2), if and only if there exists a subsemigroup $S \subseteq S_2$ and a homomorphism ϕ of S onto S_1 so that $s \equiv s' \pmod{P_2}$ implies $\phi(s) \equiv \phi(s') \pmod{P_1}$. $S_1|S_2$ if and only if S_1 is a homomorphic image of a subsemigroup $S \subseteq S_2$.

DEFINITION 1.4. Let S be a semigroup. Then $f_S: \sum(S) \to S$, read the machine of S, is defined by $f_S(s_1, \cdots, s_n) = \prod_{i=1}^{n} s_i$. Let $\mathscr{S}$ be a collection of semigroups. Then $f_{\mathscr{S}} = \{f_S | S \in \mathscr{S}\}$.

PROPOSITION 1.1. *Let $f: \sum A \to B$ and $g: \sum C \to D$. Then*

(a) *$f | j_f f_{S_f}$ and $j_f f_{S_f} | f$, and*

(b) *$f|g$ if and only if $\mathrm{NF}(f)|\mathrm{NF}(g)$.*

Proof. To prove (a) we define $h_f: A \to S_f$ by $h_f(a) = [a]_f$. Then

$$f = j_f f_{S_f} \hat{h}_f \tag{1.1}$$

showing f divides $j_f f_{S_f}$. Further, we define the homomorphism $H_f: \sum S_f \to \sum A$ by $H_f(s) = (a_1, \cdots, a_n)$. Here $(a_1, \cdots, a_n)$ is any fixed sequence of $\sum A$ such that $[(a_1, \cdots, a_n)]_f = s$. Then $j_f f_{S_f} = f H_f$ showing $j_f f_{S_f}$ divides f and proving (a).

We next show that $f|g$ implies $\mathrm{NF}(f)|\mathrm{NF}(g)$. Suppose $hgH = f$ and consider $S'_g = \{[H(t)]_g \in S_g | t \in \sum A\}$. S'_g is a subsemigroup of S_g since H is a homomorphism. Then $[H(t)]_g \to [t]_f$ is a well-defined homomorphism of S'_g

([2]) See references [3], [4], [6], and [7], and §4 of this paper for a discussion of machines and automata. See reference [5] for group theory and references [1] and [8] for semigroup theory.

onto S_f satisfying the conditions of Definition 1.3. This last assertion is proved by direct verification.

We now show that $\mathrm{NF}(f)\,|\,\mathrm{NF}(g)$ implies $f|g$. Let S_g' be a subsemigroup of S_g and ϕ a homomorphism of S_g' onto S_f satisfying the conditions of Definition 1.3. Now by (a) it is sufficient to show that $j_f f_{S_f} | j_g f_{S_g}$.

Let j_g' be j_g restricted to S_g'. And let $H\colon \sum S_f \to \sum S_g'$ be a homomophism such that for each $s \in S_f$, $H(s) = \bar{s}$ with $\phi(\bar{s}) = s$. Also there exists a function h so that $j_f \phi = h j_g'$ since ϕ carries the partitions as is required in Definition 1.3. Then $j_f f_{S_f} = j_f(\phi f_{S_g'} H) = h j_g' f_{S_g'} H$. So $j_f f_{S_f} | j_{g'} f_{S_{g'}} | j_g f_{S_g}$. This proves (b) and Proposition 1.1.

DEFINITION 1.5. Let $f\colon \sum A \to B$ and $g\colon \sum C \to D$. Then $f \times g\colon \sum (A \times C) \to B \times D$, called the direct sum of f and g, is defined by $f \times g((a_1, c_1), \cdots, (a_n, c_n)) = (f(a_1, \cdots, a_n), g(c_1, \cdots, c_n))$. The direct sum of any finite number of machines is defined in a similar fashion. We introduce the notation $(f_1 \times \cdots \times f_n)^{\sigma}$ for $\bar{F}$ where the f_i for $i = 1, \cdots, n$ are machines and $F = f_1 \times \cdots \times f_n$.

Let H be a homomorphism of $\sum B$ into $\sum C$. Then $gH\bar{f}$ is termed the composition of $\bar{f}$ followed by g with connecting homomorphism H. We now wish to compute $\mathrm{NF}(gH\bar{f})$ in terms of S_g and S_f, forgetting H so far as is possible. Towards this end we require the following definitions.

DEFINITION 1.6. Let S_1 and S_2 be semigroups and let Y be a homomorphism of S_1 into endomorphisms of S_2. Then the semigroup $S_2 \times_Y S_1$ is the semidirect product of S_1 by S_2 with connecting homomorphism Y. $S_2 \times_Y S_1$ has elements $S_2 \times S_1$ and multiplication given by

$$(s_2, s_1) \cdot (s_2', s_1') = (s_2(Y(s_1)(s_2')), s_1 s_1').$$

DEFINITION 1.7. The wreath product of S_1 by S_2, written $S_2 \mathrm{w} S_1$, is $F((S_1)^1, S_2) \times_Y S_1$. Here $(S_1)^1$, as throughout this paper, is S_1 with a two-sided identity added if S_1 has none and otherwise S_1. $F((S_1)^1, S_2)$ is the semigroup of all functions l of $(S_1)^1$ into S_2 under pointwise multiplication. Also $Y(s_1)(l)(s_1') = l(s_1' s_1)$. Thus in $S_2 \mathrm{w} S_1$, $(l_1, s_1) \cdot (l_1', s_1') = (l, s_1 s_1')$ with $l(x) = l_1(x) l_1'(x s_1)$.

By convention $S_1 \mathrm{w} \cdots \mathrm{w} S_n = R_n$ is defined inductively by $R_1 = S_1$ and $R_n = R_{n-1} \mathrm{w} S_n$. Notice the reversal of indices.

PROPOSITION 1.2. *There exists a partition P so that* $\mathrm{NF}(gH\bar{f}) \,|\, (S_g \mathrm{w} S_f, P)$. *In particular* $S_{gH\bar{f}} | S_g \mathrm{w} S_f$.

Proof. By equation (1.1) we have $gH\bar{f} = j_g f_{S_g}(\hat{h}_g H \hat{j}_f) \bar{f}_{S_f} \hat{h}_f = j_g f_{S_g} \hat{i} \bar{f}_{S_f} \hat{h}_f$ where $i\colon S_f \to S_g$ and $i(s) = f_{S_g} h_g H j_f(s)$.

Now let $t = (t_1, \cdots, t_n) \in \sum A$ and let $h_f(t_k) = s_k \in S_f$ for $k = 1, \cdots, n$. Then define $({}^2(t), {}^1(t)) \in S_g \mathrm{w} S_f$ by ${}^1(t) = \prod_{k=1}^{n} s_k$ and ${}^2(t)\colon (S_f)^1 \to S_g$ with ${}^2(t)(s) = i(s s_1) i(s s_1 s_2) \cdots i(s s_1 \cdots s_n)$. Then $t \to ({}^2(t), {}^1(t))$ is a homomorphism of $\sum A$ onto the subsemigroup I_f of $S_g \mathrm{w} S_f$. Further $gH\bar{f}(t) = j_g({}^2(t)(1))$.

Now let P be the partition induced on $S_g \mathrm{w} S_f$ by the mapping $(l, s) \to j_g(l(1))$ and let $F = gHf$. Then it follows that $({}^2(t), {}^1(t)) \to [t]_F$ is a well-defined homomorphism of (I_f, P) onto $\mathrm{NF}(gH\bar{f})$ which preserves the partitions in the sense that $({}^2(t), {}^1(t)) \equiv ({}^2(t'), {}^1(t')) \pmod{P}$ if and only if $[t]_F \equiv [t']_F \pmod{P_F}$. This proves Proposition 1.2.

2. Statement of the theorem.

NOTATION 2.1. In the remainder of this paper $A, B, \cdots$ will be *finite* nonempty sets. $S, T, U, V, \cdots$ with various superscripts and subscripts will denote *finite* semigroups. G, H and P will denote *finite* groups. $\mathscr{S}$ will denote a collection of *finite* semigroups and $\mathscr{F}$ will denote a collection of machines.

The following semigroups and machines will play a special and important role.

DEFINITION 2.1. PRIMES will denote the collection of all nontrivial finite simple groups. $\mathrm{PRIMES}(S) = \{P \in \mathrm{PRIMES} \mid P \text{ divides } S\}$. $\mathrm{PRIMES}(\mathscr{S}) = \bigcup \{\mathrm{PRIMES}(S) \mid S \in \mathscr{S}\}$.

$R_A(L_A)$ denotes the semigroup with elements A and multiplication $a \cdot a' = a'(a \cdot a' = a)$. $U_3 = (R_{\{r_0, r_1\}})^1$.

$\mathrm{UNITS} = \{S \mid S \text{ divides } U_3\}$. The UNITS are $U_0 = \{1\}$, $U_1 = R_{\{r_0, r_1\}}$, $U_2 = \{r_0\}^1$ and U_3.

The delay machine D_A: $\sum A \to (A \cup \{*\})$ is defined by $D_A(a_1, \cdots, a_n) = a_{n-1}$ for $n \geqq 2$ and $D_A(a_1) = *$. D_1 denotes D_A with $A = \{r_0, r_1\}$ and $* = 1$.

We now wish to combine machines by composition and direct sums.

DEFINITION 2.2. $\mathrm{SP}(\mathscr{F})$, read series-parallel closure of $\mathscr{F}$, is defined inductively as follows: $\mathrm{SP}_1(\mathscr{F}) = \mathscr{F}$ and $\mathrm{SP}_{i+1}(\mathscr{F}) = \{f_2 \times f_1, f_2 \hat{m} \bar{f}_1, j f_1 \hat{n} \mid f_1$ and f_2 lie in $\mathrm{SP}_i(\mathscr{F})$ and m, n and j are functions so $\hat{m}$ and $\hat{n}$ are length preserving homomorphisms$\}$. $\mathrm{SP}(\mathscr{F}) = \bigcup \{\mathrm{SP}_i(\mathscr{F}),\ i = 1, 2, \cdots\}$.

REMARK 2.1. (a) Let $f_{U_1} \in \mathscr{F}$. Then since $\bar{f}_{U_1}$ is the identity map on $\sum \{r_0, r_1\}$ it follows that for each finite set A there exists an $f \in \mathrm{SP}(\mathscr{F})$ so that $\bar{f}$ is the identity map on $\sum A$. From this the reader may easily verify that $f_{U_1} \in \mathscr{F}$ implies that $\mathrm{SP}(\mathscr{F})$ equals the set of all machines g: $\sum C \to D$ such that

$$g = h_{n+1} g_n \hat{h}_n \bar{g}_{n-1} \cdots \hat{h}_2 \bar{g}_1 \hat{h}_1 \tag{2.1}$$

where each g_i is a finite direct sum of members of $\mathscr{F}$ and each h_i for $i = 1, \cdots, n+1$ is a function. Here g_i: $\sum A_{i1} \to A_{i2}$ for $i = 1, \cdots, n$ and h_1: $C \to A_{11}$, h_2: $A_{12} \to A_{21}, \cdots, h_n$: $A_{n-12} \to A_{n1}$ and h_{n+1}: $A_{n2} \to D$. Each $\hat{h}_i$ for $i = 1, \cdots, n$ is a length preserving homomorphism.

(b) We cannot infer $f_1 \in \mathrm{SP}(\mathscr{F})$ from $f_1 | f_2$ and $f_2 \in \mathrm{SP}(\mathscr{F})$. For example, it can be shown that D_1 divides a member of $\mathrm{SP}(\{f_{U_3}\})$ (see equations (3.1)) but does not lie in $\mathrm{SP}(\{f_{U_3}\})$. However, the theorem of this paper implies that $\mathrm{SP}(f_{\mathscr{S}} \cup \{f_{U_3}, D_1\})$ is closed under division.

DEFINITION 2.3. Let S have the property that for all S_1, S_2 and Y, $S|S_2 \times_Y S_1$ implies $S|S_2$ or $S|S_1$. Then S is said to be irreducible. IRR denotes the set of all irreducible semigroups.

THEOREM. (i) *Let* $f: \sum A \to B$ *be a machine with* S_f *of finite order. Then* $f \in \mathrm{SP}(f_{\mathcal{S}} \cup \{D_1, f_{U_3}\})$ *if and only if* PRIMES $(S_f) \subseteq$ PRIMES $(\mathcal{S})$. *In particular*

$$f \in \mathrm{SP}(f_{\mathrm{PRIMES}(S_f)} \cup \{D_1, f_{U_3}\}). \tag{2.2}$$

(ii) PRIMES $\cup$ UNITS = IRR.

3. **Proof of the theorem.** In this section we write $F(A, B)$ for the set of all mappings of A into B.

The proof proceeds via several lemmas. First we give a converse to Proposition 1.2.

LEMMA 3.1. *Let* S_1 *and* S_2 *be semigroups. Then* $f_{S_2 \mathrm{w} S_1} \in \mathrm{SP}(\{f_{S_1}, f_{S_2}, D_1, f_{U_1}\})$.

Proof. One shows by direct computation that $f_{S_2 \mathrm{w} S_1}$ equals

$$h_4((b)_1 \times \cdots \times (b)_n \times d) h_3(g \times D_{S_1} \times d)^{\sigma} h_2(g \times f_{S_1})^{\sigma} h_1.$$

Here $S_1 = \{s_1, \cdots, s_n\}$ and $g = f_R \times \cdots \times f_R$ (taken n times) and $R = R_{F(S_1, S_2)}$. $R \times \cdots \times R$ (taken n times) is R^n. Further, $b = f_{S_2}$ and $(b)_i = b$. Also $d = f_{R_1}$ with $R_1 = R_{S_1}$. Here h_1: $S_2 \mathrm{w} S_1 \to R^n \times S_1$ and $h_1(l, s) = (l, \cdots, l, s)$. Further $h_2: R^n \times S_1 \to R^n \times S_1 \times S_1$ and $h_2(l_1, \cdots, l_n, s) = (l_1, \cdots, l_n, s, s)$. Further $h_3: R^n \times (S_1 \cup \{*\}) \times S_1 \to (S_2)^n \times S_1$ with

$$h_3(l_1, \cdots, l_n, s, s') = (l_1(s_1 s), \cdots, l_n(s_n s), s')$$

and $* = 1$. Finally h_4: $S_2^n \times S_1 \to S_2 \mathrm{w} S_1$ and $h_4(k_1, \cdots, k_n, s) = (l, s)$ with $l(s_i) = k_i$.

Now for any finite set A, R_A is a subsemigroup of a suitably large finite direct sum of U_1 with itself. Further a restriction of a suitably large finite direct sum of D_1 with itself yields D_A. Thus the above expression lies in $\mathrm{SP}(\{f_{S_1}, f_{S_2}, D_1, f_{U_1}\})$ and Lemma 3.1 is proved.

LEMMA 3.2. PRIMES $\cup$ UNITS $\subseteq$ IRR.

Proof. We first show that PRIMES $\subseteq$ IRR. Let $G' \in$ PRIMES and $G'|S_2 \times_Y S_1$. Thus there exists a subsemigroup $S \subseteq S_2 \times_Y S_1$ and a homomorphism ϕ of S onto G'. Let G be a subsemigroup of S of smallest order so that $\phi(G) = G'$. Then $\phi(g \cdot G) = \phi(g) \cdot G' = G'$ and similarly $\phi(G \cdot g) = G'$ for all $g \in G$. Thus $g \cdot G = G \cdot g = G$ for all $g \in G$ and so G is a subgroup of $S_2 \times_Y S_1$. Let $p_1(s_2, s_1) = s_1$ and set $p_1(G) = G_1$. Then p_1 is a homomorphism and thus G_1 is a subgroup of S_1. Let $l = (l_2, l_1)$ be the identity of G. Set $G_2' = \{(s_2, l_1) \in G\}$. Then $\psi(s_2, l_1) = Y(l_1)(s_2)$ is a homomorphism of G_2' into

S_2 and is 1:1 since $\psi(s_2, l_1) = \psi(s_2', l_1)$ implies

$$(s_2, l_1) = (l_2, l_1)(s_2, l_1) = (l_2(Y(l_1)(s_2)), l_1) = (l_2(Y(l_1)(s_2')), l_1) = (l_2, l_1)(s_2', l_1)$$
$$= (s_2', l_1).$$

Setting $G_2 = \psi(G_2')$ we have that G is an extension of the subgroup G_2 of S_2 by the subgroup G_1 of S_1. Since G' is a homomorphic image of G under ϕ and G' is simple, $\neq \{1\}$, it follows that K the kernel of ϕ is a maximal normal subgroup of G and that $G'|G_1 \subseteq S_1$ or $G'|G_2 \subseteq S_2$ depending on whether $K \cdot G_2'$ equals K or G. This proves PRIMES $\subseteq$ IRR.

We now prove UNITS $\subseteq$ IRR. We shall prove irreducibility for U_3. The proofs for the remaining units are analogous and easier. We first show $U_3|S$ implies $U_3 \subseteq S$. Let $S' \subseteq S$ and let ϕ be a homomorphism of S' onto U_3. Let $x' \in S'$ and $\phi(x') = 1$. Then some power e of x' is an idempotent and $\phi(e) = 1$. Then $\phi(eS'e) = U_3$ and e is an identity for $eS'e$. Let S_1 be a subsemigroup of $eS'e$ of smallest order so that $\phi(S_1) = U_1$. Then for each $s_1 \in S_1$ we have $\phi(s_1 \cdot S_1) = \phi(s_1) \cdot \phi(S_1) = \phi(s_1) \cdot U_1 = U_1$ since U_1 is right simple. Thus $s_1 \cdot S_1 = S_1$ for all $s_1 \in S_1$ and so S_1 is right simple. Then by a well-known theorem (see [1]) S_1 is isomorphic to $G \times R_B$. B must contain at least two distinct members b_1 and b_2 since U_1 is not a group. Then

$$U_3 \cong \{e, (1, b_1), (1, b_2)\} \subseteq S_1 \subseteq S.$$

Suppose now that $U_3|S_2 \times_Y S_1$. By the above $U_3 = \{(b_I, a_I), (b_0, a_0), (b_1, a_1)\} \subseteq S_2 \times_Y S_1$. As before, let p_1 be the homomorphism $p_1(b, a) = a$. $p_1(U_3) = \{a_I, a_0, a_1\} = S_1$. If $a_0 \neq a_1$, then $p_1(U_3) \subseteq S_1$ is isomorphic to U_3 and $U_3|S_1$. This is so because for $i = 0$ or $i = 1$, $a_I = a_i$ implies $za_I = za_i$ which implies $z = a_i$ for all $z \in \{a_I, a_0, a_1\}$. Therefore we may assume that $a_0 = a_1$. Necessarily $b_0 \neq b_1$. Let p_2: $U_3 \to S_2$ with $p_2(b, a) = Y(a_0)(b)$. By examining the nine possibilities and noting that $Y(a_I) \cdot Y(a_0) = Y(a_0) \cdot Y(a_I) = Y(a_0)$ one easily sees that p_2 is a homomorphism. Further, p_2 is 1:1 since assuming otherwise leads to $b_0 = b_1$. This follows since $Y(a_0)(b_0) = Y(a_0)(b_1)$ implies $(b_1, a_0) = (b_0, a_0)(b_1, a_0) = (b_0 \cdot (Y(a_0)(b_1)), a_0) = (b_0 \cdot (Y(a_0)(b_0)), a_0) = (b_0, a_0)(b_0, a_0) = (b_0, a_0)$ so $b_0 = b_1$. Also $Y(a_0)(b_0) = Y(a_0)(b_I)$ implies $(b_0, a_0) = (b_1, a_0)(b_0, a_0) = (b_1(Y(a_0)(b_0)), a_0) = (b_1(Y(a_0)(b_I)), a_0)$ so $b_0 = b_1 \cdot (Y(a_0)(b_I))$. But $(b_1, a_0)(b_I, a_I) = (b_1 \cdot (Y(a_0)(b_I)), a_0) = (b_1, a_0)$. Thus also $b_1 = b_1(Y(a_0)(b_I))$ which when compared with the above gives $b_0 = b_1$.

Similarly we find $Y(a_0)(b_1) \neq Y(a_0)(b_I)$. Therefore, in this case, $p_2(U_3)$ is isomorphic to U_3 and $p_2(U_3) \subseteq S_2$ and so $U_3|S_2$. This completes the proof of lemma 3.2.

We next prove equation (2.2) via Lemmas 3.3—3.8. From equation (2.2) and Lemma 3.2, the entire theorem follows relatively easily.

We prove equation (2.2) by induction on the order of S_f. The critical induction step separates into three cases.

LEMMA 3.3. *Let S be a finite semigroup. Then either:*

(i) *S is a cyclic semigroup,*

(ii) *S is left simple so $S = G \times L_A$, or*

(iii) *There exists a proper left ideal $T \subset S$, $T \neq S$, and a proper subsemigroup $V \subset S$, $V \neq S$, so that $S = T \cup V$.*

Proof. Let $S = \{0\}$. Then (i) holds, so we may assume $S \neq \{0\}$. Let N be a maximal proper two-sided ideal of S and if S has none let N be empty. Let $F = S/N$ ([3]). As is well known, either F is the two point zero semigroup or F is simple or F is 0-simple.

Assume the first case arises so F is the two point zero semigroup. Then N is not empty. Let V equal the cyclic semigroup generated by q where $S - N = \{x \in S | x \notin N\} = \{q\}$ and $T = N$. If $V = S$, then (i) holds. If $V \subset S$, $V \neq S$, then (iii) holds.

Now assume F is either simple or 0-simple. Then either: (1) F has no proper left ideals except possibly zero, or (2) F has a proper left ideal H different from zero.

Let case (1) hold. Then N being empty implies F is left simple which implies by the well known result that (ii) holds. See [1].

If N is not empty and (1) holds, then the theorem of Rees applied to F (see [1] or [8]) implies $S - N$ is a proper subsemigroup of F and hence $S - N$ is a proper subsemigroup of S. In this case (iii) holds with $T = N$ and $V = S - N$.

Now assume case (2) holds so F has a proper left ideal H different from zero. Let $V = (F - H) \cup N$ and $T = (H - \{0\}) \cup N$. Then the theorem of Rees applies to F implies V is a proper left ideal of S and T is a proper left ideal of S. Now $V \cup T = S$, so (iii) holds in this case.

This completes the proof of Lemma 3.3.

LEMMA 3.4. *Let $f: \sum A \to B$ and let S_f be left simple. Then equation* (2.2) *holds for f.*

Proof. As is well known, $S_f = G \times L_A$, see [1]. From equation (1.1) it is sufficient to show equation (2.2) holds for f_{S_f}.

Let G have a normal subgroup G_2 and factor group G_1 and let $\{\bar{g}_1 | g_1 \in G_1\}$ be a set of representatives of the cosets of G_2 in G. Assume $\bar{1} = 1$ and let N be the natural homomorphism of G onto G_1 with kernel G_2. Then, as is well known, $\psi(g) = (f_g, N(g)) \in G_2 \mathrm{w}\, G_1$ with $f_g(g_1) = \bar{g}_1 \cdot g \cdot (\bar{r})^{-1}$ where $r = g_1 \cdot N(g)$ is a 1:1 homomorphism of G into $G_2 \mathrm{w}\, G_1$.

By induction we can obtain the following. Let $G = G_0 \supset G_1 \supset G_2 \cdots \supset G_n = \{1\}$ be a composition series of G with simple factors $H_i = G_{i-1}/G_i$ for

([3]) $S/\phi = S$. If N is not empty let $S/N = (S - N) \cup \{0\} = \{s \in S | s \notin N\} \cup \{0\}$. Here 0 is a zero of S/N and for $s_1, s_2 \in S - N$, $s_1 \cdot s_2$ in S/N is $s_1 s_2$ when this lies in $S - N$ and otherwise 0. In this proof we follow exactly the notation of [1].

$i = 1, \cdots, n$. Then there exists a 1:1 homomorphism ψ of G into $H_n \mathrm{w} \cdots \mathrm{w} H_1$.

However, PRIMES (G) = PRIMES $(\{H_n, \cdots, H_1\})$. Thus utilizing Lemma 3.1 and an obvious induction argument, we see that equation (2.2) holds for f_G.

Now let $L = L_{\{0,1\}}$. Then f_L equals $m_3 f_{U_3} \hat{m}_2 (D_1 \times f_{U_1})^r \hat{m}_1$. Here m_1: $\{0,1\} \to U_1 \times U_1$ with $m_1(x) = (r_x, r_x)$; m_2: $U_3 \times U_1 \to U_3$ with $m_2(1,x) = x$ and $m_2(r_i, x) = 1$; finally m_3: $U_3 \to \{0,1\}$ with $m_3(r_i) = i$ for $i =$ 0 or 1 and $m_3(1) = 1$. Thus $f_L \in \mathrm{SP}(\{D_1, f_{U_3}\})$. Now a restriction of a sufficiently large finite direct sum of f_L with itself yields f_{L_A}. Thus equation (2.2) holds for f_{L_A}. This completes the proof of Lemma 3.4.

In considering case (iii) of Lemma 3.3 we require the following definitions.

DEFINITION 3.1. Let f: $\sum A \to B$ and let $c \notin A \cup B$. If $t \in \sum (A \cup \{c\})$ let t_c be that member of $(\sum A)^1$ given by striking out all members of t occurring before the last c and this last c itself. Then PPf: $\sum (A \cup \{c\}) \to (B \cup \{c\})$, read partial-product f, is defined by PP$f(t) = f(t_c)$ with the convention that $f(1)$ equals c.

Let f: $\sum A \to B$ and let $e \notin A \cup B$. If $t \in \sum (A \cup \{e\})$ let t_e be that member of $(\sum A)^1$ given by striking out all occurences of e in t. Then

$$ef\colon \sum (A \cup \{e\}) \to B \cup \{e\}$$

is defined by $ef(t) = f(t_e)$ with the convention that $f(1)$ equals e.

Both PPf and ef are extensions of f.

LEMMA 3.5. *Let S, T and V be as in* (iii) *of Lemma* 3.3. *Then*

$$f_S \in \mathrm{SP}(\{ef_T, \mathrm{PP}f_V, D_1, f_{U_1}\}).$$

Proof. By direct computation we verify that $f_S = m_3(ef_T \times f_{R_X}) \hat{m}_2 (\overline{2}_A)$ $(f_{R_Y} \times \mathrm{PP}f_V)^r \hat{m}_1$. Here $2_A = (D_A \times f_{R_A})m$ where $\hat{m}$. $A \to A \times A$ with $m(a) = (a,a)$. Also $Y = R_1 = T \cup \{e\}$, $R_2 = X = V \cup \{c\}$ and $A = R_1 \times R_2$. Further m_1: $S \to R_1 \times R_2$ with $m_1(s) = (s,c)$ if $s \in T$ and $m_1(s) = (e,s)$ if $s \in S - T = \{x \in S | x \notin T\}$. Also m_2: $(A \cup \{*\}) \times A \to A$ with $m_2((x_1,y_1),(x_2,y_2)) = (y_1 x_2, y_2)$ if $y_1 \neq c$ and $y_2 = c$ and $m_2((x_1,y_1))(x_2,y_2)) = (x_2,y_2)$ otherwise. Finally m_3: $R_1 \times R_2 \to S$ is defined by $m_3(x_1,y_1) = x_1 y_1$ where e and c are ignored (left out). Notice (e,c) will not occur.

LEMMA 3.6. *Let equation* (2.2) *hold for f. Then* PPf *and* $ef \in \mathrm{SP}(f_{\mathrm{PRIMES}(S_f)} \cup \{D_1, f_{U_3}\})$.

Proof. The proof is given via the following string of statements (a)-(g).

(a) D_1 *and* f_{U_1} *in* SP$(\mathscr{F})$ *implies* PP$D_1 \in \mathrm{SP}(\mathscr{F})$.

Proof of (a). PPD_1 equals $p(D_1 \times D_1 \times f_{U_1})\hat{m}$ where m: $(U_1 \cup \{c\}) \to U_1 \times U_1 \times U_1$ with $m(c) = (r_0, r_1, r_1)$ and $m(r_i) = (r_i, r_0, r_0)$ for i equaling 0 or 1. Also p: $U_3 \times U_3 \times U_1 \to U_3 \cup \{c\}$ with $p(x,y,r_1) = c$ for all $x, y \in U_3$. Further, $p(r_0, r_1, r_0) = 1$, $p(r_0, r_0, r_0) = r_0$ and $p(r_1, r_0, r_0) = r_1$. Finally $p(1,1,r_0) = 1$ and $p(1,1,r_1) = c$. Notice (r_1, r_1, r_0) will never occur.

(b) *f_G and f_{U_3} in* $\mathrm{SP}(\mathscr{F})$ *implies* $\mathrm{PP}f_G \in \mathrm{SP}(\mathscr{F})$

Proof of (b). $\mathrm{PP}f_G$ equals $m_3(f_{R_G} \times f_S \times f_{R_{\{c,*\}}})\hat{m}_2(f_G \times f_{R_{(G\cup\{c\})}})^e\hat{m}_1$ with $S = (R_G)^1$. Here m_1: $G \cup \{c\} \to G \times (G \cup \{c\})$ with $m_1(c) = (1_G, c)$ and $m_1(x) = (x, x)$ for $x \neq c$. Here 1_G is the identity of G. Further m_2: $G \times (G \cup \{c\}) \to G \times (G \cup \{1\}) \times \{c, *\}$ with 1 the identity of S and $m_2(g, c) = (g, g, c)$ while $m_2(g, g') = (g, 1, *)$. Further, m_3: $G \times (G \cup \{1\}) \times \{c, *\} \to G \cup \{c\}$ where $m_3(a, b, c) = c$ for all a and b and $m_3(a, b, *) = b^{-1}a$ for $b \neq 1$ and $m_3(a, b, *) = a$ when $b = 1$.

Now since a restriction of a suitably large finite direct sum of $f_{U_3}(f_{U_1})$ with itself yields $f_S(f_{R_A})$ the proof of (b) is complete.

(c) *Let U be a unit. Then f_U and f_{U_1} in* $\mathrm{SP}(\mathscr{F})$ *implies* $\mathrm{PP}f_U \in \mathrm{SP}(\mathscr{F})$.

Proof of (c). We give the proof only for $U = U_3$. The other cases are easier. $\mathrm{PP}f_{U_3}$ equals $m_2(f_S \times f_{U_1} \times f_{U_1})\hat{m}_1$ with $S = (R_A)^1$ and $A = \{r_0, r_1, r_2\}$. Here m_1: $U_3 \cup \{c\} \to S \times U_1 \times U_1$ with $m_1(c) = (r_2, r_1, r_1)$ and $m_1(r_i) \to (r_i, r_0, r_0)$ for $i = 0$ and 1 and $m^1(1) = (1, r_1, r_0)$. Also m_2: $S \times U_1 \times U_1 \to U_3 \cup \{c\}$ with m_2 being m_1 inverse on the image of m_1 and $m_2(r_i, r_1, r_0) = r_i$ for $i = 0$ and 1 and $m_2(r_2, r_1, r_0) = 1$. Otherwise m_2 is arbitrary. This proves (c).

(d) *Let* $\{\mathrm{PP}f | f \in \mathscr{F}\} \subseteq \mathrm{SP}(\mathscr{F})$. *Then* $f \in \mathrm{SP}(\mathscr{F})$ *implies* $\mathrm{PP}f \in \mathrm{SP}(\mathscr{F})$.

Proof of (d). By hypothesis $\{\mathrm{PP}f | f \in \mathrm{SP}_1(\mathscr{F})\} \subseteq \mathrm{SP}(\mathscr{F})$. Assuming that $\{\mathrm{PP}f | f \in \mathrm{SP}_n(\mathscr{F})\} \subseteq \mathrm{SP}(\mathscr{F})$ we will show that $\{\mathrm{PP}f | f \in \mathrm{SP}_{n+1}(\mathscr{F})\} \subseteq \mathrm{SP}(\mathscr{F})$ which by induction will complete the proof of (d).

Let $f \in \mathrm{SP}_{n+1}(\mathscr{F})$. Then by Definition 2.2 either: (i) $f = f_2\hat{m}\bar{f}_1$, (ii) $f = f_1 \times f_2$, or (iii) $f = jf_1\hat{n}$ with $f_1, f_2 \in \mathrm{SP}_n(\mathscr{F})$. By assumption, $\mathrm{PP}f_1$ and $\mathrm{PP}f_2$ lie in $\mathrm{SP}(\mathscr{F})$. Thus in case (i) we find $\mathrm{PP}f$ equal to $\mathrm{PP}f_2\hat{m}_c(\mathrm{PP}f_1)^e$ where m_c is m extended to c by $m_c(c) = c$. Cases (ii) and (iii) are also handled in the obvious manner and (d) is proved.

(e) *Let S equal $(S_{D_1})^1$. Then* $f_S \in \mathrm{SP}(\{D_1, f_{U_3}\})$.

Proof of (e). We first see that

$$D_1 = f_{U_3}\hat{m}(f_{U_3} \times f_{U_1})^e H. \tag{3.1}$$

Here H: $\sum U_1 \to \sum(U_3 \times U_1)$ and H is a homomorphism with $H(x) = ((1, r_0), (x, r_1))$. Further m: $U_3 \times U_1 \to U_3$ with $m(y, r_0) = y$ and $m(y, r_1) = 1$ for all $y \in U_3$.

Now by applying Propositions 1.1 and 1.2 to equation (3.1) we find

$$S_{D_1} | U_3 \mathrm{w} (U_3 \times U_1) | U_3 \mathrm{w} (U_3 \times U_3) = T. \tag{3.2}$$

Further since T is a monoid $(S_{D_1})^1 = S | T$. Now applying Lemma 3.1 to f_T we complete the proof of (e).

(f) *Let f: $\sum A \to B$ and g: $\sum C \to D$. Then*

(i) *$g = jfh$ implies $eg = j_e efh_e$ for suitable functions j_e and h_e.*

(ii) *Let S be a monoid and let f_{U_2} and $f_S \in \mathrm{SP}(\mathscr{F})$. Then $ef_S \in \mathrm{SP}(\mathscr{F})$.*

(iii) *Let U be any unit and G any group. Then eD_1, ef_U and ef_G all lie in* $\mathrm{SP}(\{D_1, f_G, f_{U_3}\})$.

Proof of (f). We see that (i) is trivial by taking j_e to be the extension of j to e given by $j_e(e) = e$ and h_e to be the extension of h to e given by $h_e(e) = e$.

To prove (ii) we have that ef_S equals $p(f_S \times f_{U_2})\hat{m}$ where m: $S \cup \{e\} \to S \times U_2$ with $m(e) = (1,1)$ and $m(s) = (s, r_0)$. Further, p: $S \times U_2 \to S \cup \{e\}$ with $p(x,1) = e$ and $p(x, r_0) = x$.

We now prove (iii). The assertions for ef_G and ef_{U_3} follow from (ii). The assertion for ef_U follows from (i) and the assertion for ef_{U_3}.

Let S equal $(S_{D_1})^1$. Then, that ef_S lies in $\mathrm{SP}(\{D_1, f_{U_3}\})$ follows from (e) and (ii) of (f) above. Now the assertion for eD_1 follows from equation (1.1) and (i) of (f) above.

This proves (f).

(g) *Let $\{ef \mid f \in \mathscr{F}\} \subseteq \mathrm{SP}(\mathscr{F})$. Then $f \in \mathrm{SP}(\mathscr{F})$ implies $ef \in \mathrm{SP}(\mathscr{F})$.*

Proof of (g). We proceed as in the proof of (d). In case (i) we have $ef = e(f_2 \hat{m} \bar{f}_1) = ef_2 \hat{m}_2 (ef_1 \times f_{R_R})^e \hat{m}_1$ with f_i: $\sum A_i \to B_i$ for $i = 1$ and 2 and $R = A_1 \cup \{e\}$. Here m_1: $(A_1 \cup \{e\}) \to (A_1 \cup \{e\}) \times (A_1 \cup \{e\})$ with $m_1(x) = (x, x)$. Also m_2: $(B_1 \cup \{e\}) \times (A_1 \cup \{e\}) \to (A_2 \cup \{e\})$ with $m_2(x, y) = e$ when $y = e$ and $m_2(x, y) = m(x)$ if $y \neq e$. Case (iii) is given by (i) of (f). Case (ii) is handled in the obvious fashion and (g) is proved.

Now (a)-(d) implies the first assertion of Lemma 3.6 and (e)-(g) imply the second assertion. This proves Lemma 3.6.

LEMMA 3.7. *Let S be a cyclic semigroup. Then equation* (2.2) *holds for f_S.*

Proof. Let $T_n = U_2 \mathrm{w} \cdots \mathrm{w}\, U_2$ with n factors. Then T_n contains as a subsemigroup a cyclic semigroup $C_{(n,1)}$ with index n and period 1. $C_{(n,1)} = \{q_n = q_n^1, q_n^2, \cdots, q_n^n\}$ where $q_n^i \neq q_n^j$ for $1 \leqq i \neq j \leqq n$ and $q_n^{n+1} = q_n^n$. This is established by induction on n. $C_{(1,1)} = \{0\} \subset U_2$. Now suppose $C_{(n-1,1)} \subset T_{n-1}$. Let $q_n = (l, 0) \in T_{n-1} \mathrm{w}\, U_2 = T_n$. Here l: $U_2 \to T_{n-1}$ with $l(r_0) = q_{n-1} \in T_{n-1}$ and $l(1) = 1$. Then $q_n^K = (l,0)^K = (l_K, 0)$ where l_K: $U_2 \to T_{n-1}$ with $l_K(r_0) = q_{n-1}^K$ and $l_K(1) = q_{n-1}^{K-1}$. Thus q_n generates $C_{(n,1)} \subset T_n$.

Let Z_m be the additive integers mod m. Then $C_{(n,m)} | Z_m \times C_{(n,1)}$. Now by Lemma 3.4 equation (2.2) holds for f_{Z_m}. Further, by Lemma 3.1 it follows that equation (2.2) holds for f_{T_n} with PRIMES (T_n) empty and thus for f_C with $C = C_{(n,1)}$. Thus equation (2.2) is valid for $C_{(n,m)}$ since PRIMES $(C_{(n,m)})$ = PRIMES (Z_m). This proves Lemma 3.7.

LEMMA 3.8. *Equation* (2.2) *is valid.*

Proof. By equation (1.1) $f = j_f f_{S_f} h_f$. Thus it is sufficient to prove equation (2.2) for f_S where S is a finite semigroup.

We proceed by induction on the order of S. The case $|S| = 1$ is trivial. Now assume equation (2.2) holds for all $f_{S'}$ with $|S'| \leqq n$. Let $|S| = n + 1$ and apply Lemma 3.3 to S. In case (i), Lemma 3.7 applies and we are done.

In case (ii), Lemma 3.4 applies and we are done. In case (iii), Lemma 3.5 and Lemma 3.6 apply and we are done. This proves Lemma 3.8.

To complete the proof of the theorem we require the following definition.

DEFINITION 3.2. $K(\mathcal{S})$, read the semidirect and divisor closure of $\mathcal{S}$, is defined inductively as follows: $K_1(\mathcal{S}) = \mathcal{S}$ and $K_{i+1}(\mathcal{S}) = \{S' | S' \text{ divides } S \text{ for some } S \in K_i(\mathcal{S})\} \cup \{S_2 \times_Y S_1 | S_2 \text{ and } S_1 \text{ belong to } K_i(\mathcal{S})\}$. See Definition 1.6. $K(\mathcal{S}) = \bigcup \{K_i(\mathcal{S}) | i = 1, 2, \cdots\}$.

LEMMA 3.9. (a) *Let* $S \in \text{IRR}$ *and* $S \in K(\mathcal{S})$. *Then* $S | S'$ *for some* $S' \in \mathcal{S}$.
(b) $\{S_f | f \in \text{SP}(\mathcal{F})\} \subseteq K(\{S_f | f \in \mathcal{F}\})$.

Proof. The proof of (a) follows by an obvious induction on i of K_i and the definition of irreducible as given in Definition 2.3.

The proof of (b) follows by obvious induction on i of SP_i as the proof of Lemma 3.6(d). In case (i) we use Proposition 1.2. We remark that $F((S_1)^1, S_2)$ is isomorphic with the direct sum of S_2 taken $|(S_1)^1|$ times. For (ii) we remark that $S_{f \times g} | S_f \times S_g$. In the case (iii) we use Proposition 1.1. This proves Lemma 3.9.

Proof of the theorem. We first prove part (i) of the theorem. Lemma 3.8 proves equation (2.2). Thus

$$\text{PRIMES}(S_f) \subseteq \text{PRIMES}(\mathcal{S}) \text{ implies } f \in \text{SP}(f_{\mathcal{S}} \cup \{D_1, f_{U_3}\}).$$

Now assume $f \in \text{SP}(f_{\mathcal{S}} \cup \{D_1, f_{U_3}\})$. Then by Lemma 3.9(b)

$$S_f \in K(\mathcal{S} \cup \{U_3, S_{D_1}\}) \subseteq K(\mathcal{S} \cup \{U_3\})$$

with the last inclusion following from equation (3.2). Thus $P \in \text{PRIMES}(S_f)$ lies in $K(\mathcal{S} \cup \{U_3\})$ and thus by Lemmas 3.2 and 3.9(a) P divides S for some $S \in \mathcal{S}$ or P divides U_3. P divides U_3 is impossible so P divides S. Thus $\text{PRIMES}(S_f) \subseteq \text{PRIMES}(\mathcal{S})$. Thus proves part (i) of the theorem.

$$\text{PRIMES} \cup \text{UNITS} \subseteq \text{IRR}$$

is proved by Lemma 3.2. To prove the opposite inclusion let $S \in \text{IRR}$. Then by equation (2.2) for f_S and (b) and (a) of Lemma 3.9 either S divides $P \in \text{PRIMES}(S)$, S divides U_3, or S divides S_{D_1}. In the first case $S \in \text{PRIMES}$ or $S = \{1\}$ in which case S is a unit and in the second case $S \in \text{UNITS}$. Since by equation (3.2) $S_{D_1} \in K(\{U_3\})$, we find in the third case that $S \in K(\{U_3\})$. Thus by Lemma 3.9(a) S divides U_3 and $S \in \text{UNITS}$. This proves the theorem.

COROLLARY 3.1. (a) $S \in K(\mathcal{S} \cup \{U_3\})$ *if and only if* $\text{PRIMES}(S) \subseteq \text{PRIMES}(\mathcal{S})$,
(b) $S \in K(\text{PRIMES}(S) \cup \{U_3\})$.

Proof. Let $S(\mathcal{S}) = \{S_f | f \in \text{SP}(f_{\mathcal{S}} \cup \{D_1, f_{U_3}\})\}$. Now the theorem implies that $T \in S(\mathcal{S})$ if $\text{PRIMES}(T) \subseteq \text{PRIMES}(\mathcal{S})$. Thus to prove

the corollary it is sufficient to show $K(\mathcal{S} \cup \{U_3\}) = S(\mathcal{S})$.

That $S(\mathcal{S}) \subseteq K(\mathcal{S} \cup \{U_3\})$ follows from Lemma 3.9(b) and equation (3.2). On the other hand $T \in K(\mathcal{S} \cup \{U_3\})$ implies, by the irreducibility of the PRIMES and Lemma 3.9(a), that PRIMES $(T) \subseteq$ PRIMES $(\mathcal{S})$. Thus $T \in S(\mathcal{S})$ and the corollary is proved.

REMARK 3.1. $S \in K(\mathcal{S})$ iff IRR $(S) \subseteq$ IRR $(\mathcal{S})$ is seen to be *false* by taking $S = L_{\{0,1\}}$.

REMARK 3.2 (a) Let $W(\mathcal{S})$ be the closure of $\mathcal{S}$ under division and wreath product. Then the statement and the proof of Corollary 3.1 holds if K is replaced throughout by W.

(b) Let $E(\mathcal{S})$ be the closure of $\mathcal{S}$ under division and Schreier extensions adapted to monoids. Thus S_1 and $S_2 \in E(\mathcal{S})$ implies all Schreier extensions of S_1^1 by S_2^1 lie in $E(\mathcal{S})$. Then, again, the statement and the proof of Corollary 3.1 hold if K is replaced throughout by E. This is so since any extension of S_1^1 by S_2^1 is a subsemigroup of $S_2^1 \mathrm{w} S_1^1$([4]) and conversely $S_2^1 \mathrm{w} S_1^1$ is a Schreier extension of a finite direct sum of S_2^1 by S_1^1.

Thus each $P \in$ PRIMES is irreducible with respect to E.

COROLLARY 3.2. (a) $S \mid S_1 \mathrm{w} S_2 \mathrm{w} \cdots \mathrm{w} S_q \mathrm{w} \cdots \mathrm{w} S_n$ *for some sequence* $S_1, \cdots, S_n$ *where* $S_q \in$ PRIMES $(S) \cup$ UNITS,

(b) $S \mid T$ *for some monoid* T *which is constructed by successive Schreier extensions adapted to monoids with factors* $S_1, \cdots, S_n$. *Here each* S_i *may be taken to be* U_3 *or a Jordan-Hölder factor of maximal subgroup of* S.

Proof. Statement (a) follows from Remark 3.2 (a) since one may verify that W(PRIMES $(S) \cup \{U_3\}$) consists of all divisors of $S_1 \mathrm{w} \cdots \mathrm{w} S_n$ where $S_i \in$ PRIMES $(S) \cup$ UNITS.

To prove (b) we first remark that PRIMES $(S) =$ PRIMES $(\{P \mid P$ is a Jordan-Hölder factor of a maximal subgroup of $S\})$. This follows from elementary group theory. Also $T_i \mid S_i$ for $i = 1, \cdots, n$ implies $T_1 \mathrm{w} \cdots \mathrm{w} T_n \mid S_1 \mathrm{w} \cdots \mathrm{w} S_n$. Thus (b) follows from (a).

4. **Application to sequential machines.** We first give a quick review of some well-known elementary results on sequential machines. See [3], [4], [6], and [7]. $M = (A, B, Q, \lambda, \delta)$, with A, B and Q finite nonempty sets, λ: $Q \times A \to Q$ and δ: $Q \times A \to B$, is called a finite state sequential machine. Q is the set of states.

For each $q \in Q$, M_q: $\sum A \to B$ is defined inductively by $M_q(a) = \delta(q, a)$ and $M_q(a_1, \cdots, a_n) = M_{\lambda(q,a_1)}(a_2, \cdots, a_n)$ for $n \geqq 2$. M is said to be reduced if $q \to M_q$ is 1: 1.

Let f: $\sum A \to B$ and define $M(f) = (A, B, \{fL_t \mid t \in (\sum A)^1\}, \lambda, \delta)$. Here L is the left regular representation so L_t: $\sum A \to \sum A$ with $L_t(r) = t \cdot r$. Further, $\lambda(fL_t, a) = fL_t L_a = fL_{t \cdot a}$ and $\delta(fL_t, a) = fL_t(a)$. Then $M(f)_{fL_t} = fL_t$ and,

([4])The proof is similar to the group extension case as is given in the proof of Lemma 3.4.

up to isomorphism, $M(f)$ is the unique smallest reduced machine realizing f as some M_q.

Let $M = (A, B, Q, \lambda, \delta)$ be a machine. For each $t \in \sum A$ define $\hat{\lambda}(t)\colon Q \to Q$ inductively as follows: $(\hat{\lambda}(a_1))(q) = \lambda(q, a_1)$ for $a_1 \in A$, and $(\hat{\lambda}(a_1, \cdots, a_n))(q) = \hat{\lambda}(a_n)[\hat{\lambda}(a_1, \cdots, a_{n-1})(q)]$ for $n \geqq 2$.

Let $F_C(Q, Q)$ be a semigroup under the composition $(f \circ g)(q) = g(f(q))$. Then $t \to \hat{\lambda}(t)$ is a homomorphism of $\sum A$ into $F_C(Q, Q)$. Let $Q_q = \{q' \in Q | \hat{\lambda}(t)(q) = q' \text{ or } q' = q\}$. Let $\psi(t) = \hat{\lambda}(t)$ restricted to Q_q. Then ψ is a homomorphism of $\sum A$ into $F_C(Q_q, Q_q)$. We set $\psi(\sum A)$ equal to S_q.

Now let $M_q = f$ and assume M is reduced. Then it is easy to verify that the left regular representation of S_f is isomorphic with S_q. In particular the maximal subgroups of S_f and S_q are isomorphic so

$$\text{PRIMES}(S_f) = \text{PRIMES}(S_q).$$

Let $t \in \sum A$. We say $q_1, \cdots, q_n, q_{n+1} = q_1$ is a t-loop of length $n \geqq 1$ of M iff $q_i \in Q$ for $i = 1, \cdots, n$ and $q_i \neq q_j$ for $1 \leqq i \neq j \leqq n$, and $\hat{\lambda}(t)(q_i) = q_{i+1}$ for $i = 1, \cdots, n$.

DEFINITION 4.1. Prime loop $(M) = \{p | p$ is a prime integer and there exists a $t \in \sum A$ so that M has a t-loop of length $p\}$.

$M \in \text{SP}(\mathscr{F})$ if and only if $M_q \in \text{SP}(\mathscr{F})$ for all q.

Z_p denotes the integers under addition mod p.

COROLLARY 4.1 (CONSTRUCTABILITY FROM COUNTERS). *Let M be a reduced finite state sequential machine. Then*

I. $M \in \text{SP}(\{f_{U_3}, D_1\})$ *if and only if prime loop* (M) *is empty.*

II. $M \in \text{SP}(\{f_{U_3}, D_1, f_{Z_p}\})$ *for p one fixed prime if and only if prime loop* $(M) \subseteq \{p\}$.

III. (*Burnside*) $M \in \text{SP}(\{f_{U_3}, D_1, f_{Z_p}, f_{Z_q}\})$ *for p and q two fixed primes if and only if prime loop* $(M) \subseteq \{p, q\}$.

IV. (*Feit, Thompson*) $M \in \text{SP}(\{f_{U_3}, D_1\} \cup \{f_{Z_p} | p \in \pi\})$ *where π is a set of odd primes if and only if prime loop* $(M) \subseteq \pi$.

Proof. By utilizing the well-known fact that a prime p divides the order of G if and only if G has an element of order p and canonical facts concerning mapping representations of Z_p, see [5], we find that prime loop (M) is exactly that set of primes which divide the order of some (maximal) subgroup of S_{M_q} for some $q \in Q$.

Now equation (2.2) implies $f \in \text{SP}(\{f_{U_3}, D_1\} \cup \{f_{Z_p} | p \in \pi\})$ for a set of primes π if and only if the (maximal) subgroups of S_f are *solvable* and the prime divisors of their orders are among the primes π. This is so since by elementary group theory the (maximal) subgroups of S are solvable iff PRIMES $(S) = \{Z_p | p$ divides the order of a (maximal) subgroup of S and p is prime$\}$.

Now I immediately follows. II follows from the well-known theorem that p-groups are solvable. See [5].

III follows from Burnside's theorem of the solvability of groups of order $p^\alpha q^\beta$. See [5].

Feit and Thompson in [2] have proved solvability of groups of odd order, proving IV and Corollary 4.1.

DEFINITION 4.2. Let $\mathscr{F}_k$ be the collection of all f: $\sum A \to B$ so that $f = M_q$ for some finite state sequential machine M with k or less states. We remark that $f \in \mathscr{F}_k$ for some k if and only if S_f is finite.

Let f: $\sum A \to B$ with S_f of finite order. Then size (f) is the smallest integer k so that $f \in \mathrm{SP}(\mathscr{F}_k)$.

COROLLARY 4.2. *Let* g: $\sum C \to D$ *with* S_g *of finite order and* size $(g) \geqq 2$. *Then* size (g) *is the maximum of* $\{\text{size } (f_P) \mid P \in \text{PRIMES } (S_g)\}$ *and* 2.

Proof. Clearly size (f_{U_2}) and size (f_{U_1}) are both 2. Further it can be shown that size $(f_{U_3}) = 2$ and $D_1 \in \mathrm{SP}(\{f_{U_3}, f_{Z_2}\})$. Thus size $(D_1) =$ size $(f_U) = 2$ for all units $U \neq \{1\}$.

Let s_g equal the maximum of $\{\text{size } (f_P) \mid P \in \text{PRIMES } (S_g)\}$ and 2. Then the above plus equation (2.2) implies size $(g) \leqq s_g$.

By assumption, size $(g) \geqq 2$ and trivially $s_g \geqq 2$. Thus if $s_g = 2$ we have $s_g =$ size (g). Suppose $s_g > 2$. Then PRIMES (S_g) is nonempty. So let $P \in$ PRIMES (S_g). We will show if g has any decomposition as in (2.1) with $g_i = f_{i1} \times \cdots \times f_{in_i}$ then some f_{ij} is such that the number of states of $M(f_{ij}) \geqq$ size (f_P).

Let $\mathscr{S} = \{S_{f_{ij}} | f_{ij}$ occurs as a summand in g_i for $i = 1, \cdots, n\}$. Then $P \in K(\mathscr{S})$ since equation (1.1) applied to each f_{ij} yields $g \in \mathrm{SP}(f_{\mathscr{S}})$ and thus Lemma 3.9 (b) applies. Thus by Lemma 3.9 (a) and the irreducibility of P we have $P | S_{f_{ij}}$ for some f_{ij}.

Let m be the number of states of $M(f_{ij})$. We will show size $(f_P) \leqq m$. From the proof of Lemma 3.2 there exists a subgroup G of $S_{f_{ij}}$ so that P is a homomorphic image of G. The left regular representation of $S_{f_{ij}}$, and hence G, is faithfully represented by mappings on m letters. Thus G is faithfully represented by permutations on $m^{(1)} \leqq m$ letters by restricting the representation to those $m^{(1)}$ letters fixed by the identity of G. Now write G as a subdirect product of its transitive components. See [5]. Now P, being irreducible, must divide one of the components and thus P divides a group G_i which has a faithful transitive permutation representation on $m^{(2)} \leqq m^{(1)} \leqq m$ letters. Now choose G_i' to be a subgroup of G_i which has P as a homomorphic image. Then G_i' has a faithful permutation representation on $m^{(2)}$ letters which is not necessarily transitive. By continuing the above process we finally obtain a group $G^{(1)}$ which has a faithful transitive permutation representation on

$m^{(3)} \leqq m$ letters and P is a homomorphic image of $G^{(1)}$. Now from the elementary theory of such representations, see [5], we find that P itself has a faithful transitive representation on $m^{(4)}$ letters with $m^{(4)}$ dividing $m^{(3)}$ and thus $m^{(4)} \leqq m$. The corollary now follows from the following lemma.

LEMMA 4.1. *Let G be a simple group and let $f: \sum A \to B$ with $S = G$. Then* size (f) = size $(f_G) = n$. *Further, n equals the smallest number of letters on which G has a faithful transitive permutation representation.*

Proof. Let ϕ be a faithful transitive permutation representation of G on the smallest number of letters L. Consider the machine $M = (G, L, L, \phi, \phi)$. Let $\tilde{f} = M_e$ for some $e \in L$. Then $\tilde{f} = jf_G$ and $S_f = G$ and thus size (f) equals the minimum of $\{\text{size } (f') \mid S_{f'} = G\}$, which is the order of L.

Now, by equation (1.1) it is sufficient to prove size $(\tilde{f})$ = size (f_G). Let $\text{NF}(\tilde{f}) = (G, \tilde{P})$. Then $xg_1y \equiv xg_2y \pmod{\tilde{P}}$ for all x and y in G implies $g_1 = g_2$. Now for each $(g_1, g_2) \in G \times G$ let $f_{(g_1,g_2)} = j(f_G L_{g_1})\hat{h}_{g_2}$. Here h_{g_2}: $G \to G$ with $h_{g_2}(g) = g_2 g g_2^{-1}$ and L_{g_1}: $\sum G \to \sum G$ with $L_{g_1}(g_1', \cdots, g_n') = (g_1, g_1', \cdots, g_n')$. Let f' be the direct sum of $f_{(g_1,g_2)}$ for all $(g_1, g_2) \in G \times G$. Then by the property of the NF given above there must exist a function j' so that $j'f' = f_G$. This proves size (f_G) = size $(\tilde{f}) = |L| = n$ proving the lemma and hence the corollary.

BIBLIOGRAPHY

1. A. H. Clifford and G. R. Preston, *The algebraic theory of semigroups*, Vol. 1, Math. Surveys No. 7, Amer. Math. Soc., Providence, R. I., 1962.

2. Walter Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13**(1963), no. 3, 775-1029.

3. S. Ginsburg, *An introduction to mathematical machine theory*, Addison-Wesley, Reading, Mass., 1962.

4. V. M. Glushkov, *The abstract theory of automata*, Uspehi Mat. Nauk **16**(1961), no. 5(101), 3-62. (Russian)

5. M. Hall, Jr., *The theory of groups*, Macmillan, New York, 1959.

6. K. Krohn and J. Rhodes, *Algebraic theory of machines*, Proc. Symposium on Automata Theory, pp. 341-384, Polytechnic Institute of Brooklyn, 1962.

7. M. O. Rabin and D. Scott, *Finite automata and their decision problems*, IBM Res. J. **3**(1959).

8. D. Rees, *On semigroups*, Proc. Cambridge Philos. Soc. **36**(1940), 387-400.

PARIS, FRANCE,
UNIVERSITY OF CALIFORNIA,
BERKELEY, CALIFORNIA