THE FUNDAMENTAL LEMMA OF COMPLEXITY FOR ARBITRARY FINITE SEMIGROUPS[1]

BY JOHN RHODES[2]

Communicated by Saunders MacLane, June 26, 1968

1. Statement of the results and some corollaries. All semigroups considered are of finite order. In the recent paper [3] and in the recent book [2] the complexity of a semigroup was defined and definitive results were obtained for determining the complexity of a semigroup which was the union of groups. Herein we state generalizations, valid for arbitrary finite semigroups, of those previous results. All undefined notation is explained in [2].

We first recall the definition of complexity. See also [2] or [3]. One semigroup, S_1, is said to *divide* another semigroup, S_2, if and only if S_1 is a homomorphic image of a subsemigroup $S \leqq S_2$. If S is a semigroup, Endo(S) denotes the semigroup of endomorphisms of S under composition. If S_1 and S_2 are semigroups and Y is a homomorphism of S_1 into Endo(S_2), *the semidirect product of S_2 by S_1 with connecting homomorphism Y*, denoted by $S_2 \times_Y S_1$, is the semigroup with elements $S_2 \times S_1$ and product defined by $(s_2, s_1) \cdot (s_2', s_1') = (s_2 \cdot Y(s_1)(s_2'), s_1 \cdot s_1')$.

We can construct new semigroups from old ones by taking semidirect products and then divisors. $S_n \times_{Y_{n-1}} \cdots \times_{Y_2} S_2 \times_{Y_1} S_1$ denotes $(\cdots (S_n \times_{Y_{n-1}} S_{n-1}) \times_{Y_{n-2}} S_{n-2}) \cdots \times_{Y_1} S_1)$ where Y_{n-2} is a homomorphism of S_{n-2} into Endo$(S_n \times_{Y_{n-1}} S_{n-1})$, etc. We say S is a *combinatorial* semigroup if and only if the subsemigroups of S which are groups are singletons. The main theorem of [1] (see also [2, Chapter 5]) implies that for each semigroup S there exist semigroups $S_n, \cdots, S_1$ and connecting homomorphisms $Y_{n-1}, \cdots, Y_1$ so that

$$S \text{ divides } S_n \times_{Y_{n-1}} \cdots \times_{Y_1} S_1 \tag{1.1}$$

and S_k is either a simple nontrivial group dividing S or S_k is a combinatorial semigroup, for $k = 1, \cdots, n$.

$\#_G(S)$, the (group) complexity of S, is by definition the smallest nonnegative integer n such that

[1] This research was sponsored in part by the United States Air Force, Office of Scientific Research, Grant Number AF-AFOSR-68-1477.

[2] Alfred P. Sloan Research Fellow.

$$S \text{ divides } C_n \times_{Y_{n-1}} G_n \times_{Z_{n-1}} C_{n-1} \times_{Y_{n-2}} G_{n-1} \times_{Z_{n-2}} \cdots C_1 \times_{Y_0} G_1 \times_{Z_0} C_0 \tag{1.2}$$

with $C_n, \cdots, C_1, C_0$ combinatorial semigroups and $G_n, \cdots, G_1$ nontrivial groups. For extensive background see [2].

Let $\mathcal{S}_F$ denote the collection of all finite semigroups, $\mathcal{S}$ the collection of all finite semigroups which are union of groups and N the non-negative integers. Then $\#_G: S_F \to N$. In [3] and [2, Chapter 9], it was proved that $\#_G$ *restricted to* $\mathcal{S}$ satisfies the following axioms:

AXIOM I. $\#_G(S) = \max\{\#_G(S_i): i = i, \cdots, n\}$ if $S \leqq\leqq S_1 \times \cdots \times S_n$ where $\leqq\leqq$ denotes subdirect product. See [2].

AXIOM II. (FUNDAMENTAL LEMMA OF COMPLEXITY). Let I be a combinatorial ideal of S. Then

$$\#_G(S) = \#_G(S/I). \quad \text{Also} \quad \#_G(\{0\}) = 0. \tag{1.3}$$

AXIOM III. Let $S \neq \{0\}$ and let S be a group mapping (GM) semigroup with RLM the right letter mapping homomorphic image of S.[3] Then

$$\#_G(S) = \#_G(\mathrm{RLM}(S)) + 1. \tag{1.4}$$

We ask which Axioms remain valid for $\#_G: \mathcal{S}_F \to N$?

It is trivial to verify that Axiom I remains valid for $\mathcal{S}_F$. It is easy to see that Axiom III is false for $\mathcal{S}_F$, e.g. the symmetric inverse semigroup on n letters has complexity 1. See [7]. In fact, no function from $\mathcal{S}_F$ into N satisfies all three Axioms. In [2, Corollary 9.3.4], Axiom II is proved to be equivalent to Axiom II′.

AXIOM II′. Let the epimorphism $\theta: S \twoheadrightarrow T$ be one-to-one when restricted to each subgroup of S. Then $\#_G(S) = \#_G(T)$.

The epimorphisms of the hypothesis of Axiom II′ are called γ-epimorphisms in [2]. Our main result is the following theorem.

THEOREM. *Axiom* II, *or equivalently, Axiom* II′ *holds for all finite semigroups.*

It is well known (see [2, Proposition 8.2.17(b)]) that if S is a GM semigroup then either $\#_G(S)$ equals $\#_G(\mathrm{RLM}(S))+1$ or $\#_G(\mathrm{RLM}(S))$. We say S is a *pure group mapping* (PGM) semigroup if and only if S is a GM semigroup $\neq \{0\}$ and (1.4) holds for S.

---

[3] S is a GM semigroup iff S has a 0-minimal noncombinatorial ideal I so that S acts faithfully on I by right multiplication and also by left multiplication. RLM(S) is the action made faithful of S by right multiplication on the principal left ideals of I. See [2].

COROLLARY 1. *$\#_G(S)$ equals the largest nonnegative integer $n=\#_1(S)$ such that there exists a series*

$$(1.5)\qquad \begin{aligned} S \twoheadrightarrow \mathrm{PGM}_1 \twoheadrightarrow \mathrm{RLM}(\mathrm{PGM}_1) \twoheadrightarrow \cdots \\ \twoheadrightarrow \mathrm{PGM}_n \twoheadrightarrow \mathrm{RLM}(\mathrm{PGM}_n) \end{aligned}$$

where $\twoheadrightarrow$ denotes epimorphism, and PGM_k *denotes a* PGM *semigroup* $\neq \{0\}$ *for* $k=1, \cdots, n$.

PROOF. First $\#_1(S) \leqq \#_G(S)$ follows by the definition of PGM. The reverse inequality $\#_G(S) \leqq \#_1(S)$ follows from [2, Lemma 8.2.19(b)], Axiom II and the definition of PGM. See the proof of [2, Theorem 9.2.5].

COROLLARY 2.

$$S_{\mathcal{L}} \twoheadrightarrow T^4 \textit{ implies } \#G(T) \leqq \#G(S) \leqq \#G(T)+1.$$

PROOF. $S \twoheadrightarrow T_{\mathcal{L}^c}$ the minimal $\mathcal{L}'$ homomorphic image of S equals $S \twoheadrightarrow S^{\mathrm{RLM}}$ by [2, Fact 8.3.9(c)]. Now apply Corollary 1.

COROLLARY 3. (CONTINUITY OF COMPLEXITY WITH RESPECT TO HOMOMORPHISMS) *Let θ: $S \twoheadrightarrow T$ be an epimorphism, and let $\#_G(S)=n$ and $\#_G(T)=k$. Then there exists epimorphisms $S=S_n \twoheadrightarrow S_{n-1} \twoheadrightarrow \cdots \twoheadrightarrow S_k=T$, so that the composite epimorphism is θ, and $\#_G(S_j)=j$ for $j=k, \cdots, n$.*

PROOF. Apply [2, Theorem 8.1.14], the Theorem and Corollary 2.

COROLLARY 4. *$\#_G(S)$ equals the maximum of the $\#_G(S')$ where S' ranges over the $\phi(S)$ where ϕ is an irreducible representation of S into $n \times n$ complex matrices.*

PROOF. The direct sum of the ϕ's give a γ-epimorphism by [6].

2. **Indication of the proof.** Complete details will appear in [4]. Unfortunately they are long and messy. However, we will try to make the philosophy of the proof clear by the following discussion.

Suppose for each semigroup S we can construct another semigroup $\alpha(S)$ such that

$$(2.1)\qquad \alpha(S) \twoheadrightarrow S$$

and if I is a combinatorial ideal of S then

---

[4] θ:$S \twoheadrightarrow T$ is an $\mathcal{L}$ (resp. $\mathcal{L}'$) epimorphism iff $s_1, s_2 \in S$ (and s_1, s_2 regular elements) and $\theta_1(s_1)=\theta_1(s_2)$ implies $S^1s_1=S^1s_2$. See [2].

$$\text{(2.2)}\qquad \begin{aligned}&\alpha(S) \text{ divides } C \mathrm{~w~} \alpha[(S/I)] \text{ or at least}\\ &C(\alpha(S)) \leqq (\mathbf{C}, 1) \oplus C(\alpha(S/I)).\end{aligned}$$ [5]

Then clearly to prove the Theorem it suffices to prove

$$(*)\qquad C(\alpha(S)) \leqq (\mathbf{C}, 1) \oplus C(S)$$

or equivalently by (2.1)

$$(*)\qquad C(\alpha(S)) \approx C(S)$$

where $C(S) \approx C(T)$ iff $C(S) \leqq (\mathbf{C}, 1) \oplus C(T)$ and $C(T) \leqq (\mathbf{C}, 1) \oplus C(S)$.

EXAMPLES OF α. Before continuing we list some good examples of α. With reference to [2, §5.4], we suppose that for each S we choose a system of subsemigroups $S_n, \cdots, S_1$ and we let $\alpha(S)$ be the subsemigroup of

$$(S_n^I, (S_n^I)^\sim) \mathrm{~w~} \cdots \mathrm{~w~} (S_1^I, (S_1^I)^\sim)$$

generated by $\{\hat{s}: s \in S\}$ defined in the proof of Lemma 5.4.4 of [2]. Clearly (2.1) holds.

(2.3) If S is a union of groups and the system is chosen to be the $\mathcal{J}$-classes of S as in Remark 5.4.14 of [2], then $\alpha(S)$ satisfies (2.2), as can be verified. See [3] or Chapter 9 of [2].

(2.4) If I is a combinatorial ideal of S, then the system $S_n, \cdots, S_1$ can be chosen so that either $S_i \cap I = \varnothing$ or S_i is combinatorial and contains I. In this case (2.2) can be verified. See [4] for complete details.

Yet another way to construct α's is the following.

(2.5) Consider the right regular representation (S^I, S) and apply the method of Zeiger (see [9] and Chapter 4 of [2]). Let $\alpha(S)$ be the subsemigroup of the wreath product of permutation-reset mapping semigroups so obtained which maps homomorphically onto S. Thus (2.1) holds and (2.2) can be verified. See [4] for complete details.

Now we give a method by which (*) can be proved. We first note that if S is a union of groups and α is given by (2.3), then (*) can be verified by brute force using the machine method of [1]. For the details see [3] or Chapter 9 of [2]. The general case seems difficult by direct methods and we proceed indirectly as follows.

[5] $S_2 \mathrm{~w~} S_1$ denotes the wreath product of the right regular representation of S_1 by S_2, i.e., $S_2 \mathrm{~w~} S_1 = (S_2^I, S_2) \wr (S_1^I, S_1)$. Let $n = \#(S)$ be as defined just before (2.10). Then by definition $C(S) = (\mathbf{C}, n)$, resp. $(\mathbf{G}, n)$, resp. $(\mathbf{C} \vee \mathbf{G}, n)$ if S satisfies (2.10) (b) and not (2.10) (a), resp. S satisfies (2.10) (a) and not (2.10(b), resp. S satisfies both (2.10)(a) and (b). By definition, $(\mathbf{C}, 1) \oplus (\mathbf{C}, n) = (\mathbf{C}, 1) \oplus (\mathbf{C} \vee \mathbf{G}, n) = (\mathbf{C}, 1) \oplus (\mathbf{G}, n-1) = (\mathbf{C}, n)$. Finally, by definition $(\alpha, v) \leqq (\beta, j)$ iff $v \leqq j$, or $v = j$ and $\alpha = \beta$, or $v = j$ and $\alpha = \mathbf{C} \vee \mathbf{G}$. See [2].

Suppose one can show

(2.6), (2.6)′ (ENLARGING LEMMA). *If* $C(S) \approx C(T)$ *and* S *divides* T (*resp.* $T \twoheadrightarrow S$) *and* (*) *holds for* T, *then* (*) *holds for* S.

(2.7) Let $\theta: S \twoheadleftarrow\!\!\twoheadrightarrow T$ be a $\gamma(\mathcal{H})$-epimorphism.[6] Then $\alpha(S)$ divides $C \text{ w } \alpha(T)$ with C combinatorial or at least

$$C(\alpha(S)) \leqq (\mathbf{C}, 1) \oplus C(\alpha(T)).$$

(2.8), (2.8)′ Suppose $\theta: S \twoheadrightarrow T$ and θ is an $\mathcal{L}$ (resp. $\mathcal{L}'$) epimorphism. Then $\alpha(S)$ divides $C_1 \text{ w } G \text{ w } C_2 \text{ w } \alpha(T)$ or at least $C(\alpha(S)) \leqq (\mathbf{C}, 3) \oplus C(\alpha(T))$.

Then

LEMMA (2.9). (2.1), (2.6)–(2.8) *or* (2.1), (2.6)′, (2.7) *and* (2.8)′ *imply* (*).

PROOF. Suppose (2.9) is false and let S be a counter-example whose complexity number (defined next) $\#(S) = n$ is as small as possible. By the definition of complexity number $\#(S)$ either

(2.10)(a) $\quad S$ divides $G_n \text{ w } C_{n-1} \text{ w } G_{n-2} \text{ w } C_{n-2} \text{ w } \cdots = W$

or

(2.10)(b) $\quad S$ divides $C_n \text{ w } G_{n-1} \text{ w } C_{n-2} \text{ w } G_{n-2} \text{ w } \cdots = W$

where G_j's are groups and the C_u's are combinatorial monoids and for no smaller n is (2.10) (a) or (b) true. But $C(S) \approx C(W)$ so (2.6) implies (*) is false for W. But in Case (2.10) (b)

(2.11)(b) $$W \underset{\gamma(\mathcal{H})}{\twoheadrightarrow} W_{-1} = p_{-1}(W)$$

where p_{-1} is the projection onto the first $n-1$ coordinates. In case (2.10) (a)

(2.11)(a) $$W \underset{\mathcal{L}}{\twoheadrightarrow} W_{-1} = p_{-1}(W)$$

and in either case $\#(W_{-1}) = \#(W) - 1 = \#(S) - 1$. Thus by induction (*) holds for W_{-1} and we have

(2.12)(a) $$C(W_{-1}) = (\mathbf{C}, n-1)$$

(2.12)(b) $$C(W_{-1}) = (\mathbf{G}, n-1)$$

respectively. But then (2.11), (2.12) and (2.7) and (2.8) implies (*) holds for W, a contradiction. The other case with (2.6)′, etc. proceeds similarly. This proves (2.9).

[6] θ restricted to each $\mathcal{H}$-class of S is one-to-one.

SKETCH OF THE PROOF OF THE THEOREM. Using α of (2.4) *which we denote by* α^* we verify (2.1) and (2.2) and further show that

$$\alpha^*(S) \xrightarrow[\gamma(\mathcal{H})]{} S.$$

We do *not* verify (2.6)–(2.8) directly for α^* of (2.4).

Then using α of (2.5) *which we denote by* Z, we verify (2.1) but *not* (2.2) for Z because I can contain large nonregular $\mathcal{H}$-classes of S. However, we can verify (2.6), (2.7) and (2.8) for Z by using the classification of maximal proper epimorphisms proved in [5]. Then Lemma (2.9) implies (*) for $Z(S)$. Then (*) for Z and (2.7) implies

$$C(S) \approx C(T) \quad \text{if} \quad S \xrightarrow[\gamma(\mathcal{H})]{} T.$$

But from the first paragraph

$$\alpha^*(S) \xrightarrow[\gamma(\mathcal{H})]{} S$$

so (*) holds for α^*, so (2.1), (2.2) and (*) holds for α^* and the Theorem follows.

For further results on complexity see [7].

REFERENCES

1. Kenneth Krohn and John Rhodes, *Algebraic theory of machines*. I. *Prime decomposition theorem for finite semigroups and machines*, Trans. Amer. Math. Soc. **116** (1965), 450–464.

2. Kenneth Krohn, John Rhodes and Bret Tilson, "Lectures on the algebraic theory of finite semigroups and finite state machines," Chapters 1, 5–9 (Chapter 6 with M. A. Arbib, in *Algebraic theory of machines, languages, and semigroups*, edited by M. A. Arbib, Academic Press, New York, 1968.

3. Kenneth Krohn and John Rhodes, *Complexity of finite semigroups*, Ann. of Math. **88** (1968), 128–160.

4. John Rhodes, *A proof of the fundamental lemma of complexity for arbitrary finite semigroups*, to be submitted to Math. Systems Theory.

5. ———, *A homomorphism theorem for finite semigroups*, J. Math Systems Theory **1** (1967), 289–304.

6. ———, *Complexity and characters of finite semigroups*. J. Combinatorial Theory (to appear).

7. John Rhodes and Bret Tilson, *Lower bounds for complexity of finite semigroups*, submitted to Math. Systems Theory.

8. H. P. Zeiger, *Cascade synthesis of finite-state machines*, Information and Control **10** (1967), 419–433, plus erratum.

UNIVERSITY OF CALIFORNIA, BERKELEY