DISCRETE MATHEMATICS 8 (1974) 345–349. © North-Holland Publishing Company

GENERALIZATION OF A THEOREM OF FLECK, HEDETNIEMI AND OEHMKE ON $\mathcal{S}^*$-SEMIGROUPS OF AUTOMATA

Dennis P. GELLER

School of Advanced Technology, Human Sciences and Technology,
State University of New York, Binghamton, N.Y. 13901, USA

Received 30 October 1973 *

Abstract. A solution to a conjecture of Fleck, Hedetniemi and Oehmke [4] on $\mathcal{S}^*$-semigroups of automata is presented. This also generalizes a result in [1].

A *finite automaton* or *machine* is a system (S, I, δ), where S and I are finite sets and $\delta : S \times I \to S$; here we will write $s\,i$ for $\delta(s, i)$. Elements of S are called *states*, and those of I are called *inputs*. A machine is *autonomous* if $|I| = 1$. Let I^* be the set of non-empty strings of symbols from I; we can extend δ to be a function $\delta : S \times I^* \to S$ by defining, for $i \in I$, $x \in I^*$, $s\,(i\,x) = (s\,i)\,x$. A machine is *strong* (strongly connected) if, given any $s, t \in S$, there is a string $w_{st} \in I^*$ such that $s\,w_{st} = t$.

In [1], Fleck, Hedetniemi and Oehmke define a semigroup structure on machines as follows.

If s; $t \in S$ and x is a string of symbols from I $(x \in I^*)$ such that $s\,x = t$, then we say that (s, x, t) is a *triple* of A; if $x = i \in I$, then $(s, x, s\,x)$ is an *elementary triple*. Let U and V be finite sets of triples of A; we define the product $U \circ V$ by

$$U \circ V = \{(s,x,t) \colon \exists\, (s,y,r) \in U,\ (r,z,t) \in V \text{ such that } x = y\,z\}\ .$$

Under the operation $\circ$ the finite sets of triples form a semigroup; we call this semigroup $\mathcal{S}^*(A)$. The empty set is a zero for $\mathcal{S}^*(A)$.

The following conjecture was made in [4]:

* Original version received 4 April 1973.

If A and A' are any two strong machines with the same number of states, then $\mathcal{S}^*(A)$ is isomorphically embedded in $\mathcal{S}^*(A')$, and vice-versa.

In this note we settle the conjecture completely: it is true if neither machine is autonomous, but if A is autonomous and A' is not, then, while $\mathcal{S}^*(A)$ is isomorphically embedded in $\mathcal{S}^*(A')$, the converse is not true. A special case of this result, for positive machines which are not autonomous, is presented (without proof) as Theorem 2 of [1].

Theorem 1. *Let $A = (S, I, \delta)$ be a strong machine with n states and at least two inputs, and let $A' = (S', I', \delta')$ be a strong automaton with $n' \leq n$ states. Then $\mathcal{S}^*(A')$ is isomorphic to a subsemigroup of $\mathcal{S}^*(A)$.*

Proof. We first note that since A is strong, for any states s and t, not necessarily distinct, there is a string w_{st} of length at least one such that $s\,w_{st} = t$.

Let ϕ be a one-to-one map from the states of A onto the states of A'; unless $|A| = |A'|$, the domain of ϕ will be a proper subset $\bar{S}$ of S. Let A' have input set $I' = \{i'_1, i'_2, ..., i'_a; a = |I'|\}$. We define a map $h : \bar{S} \times I' \to I^*$ in the following manner. First choose two distinct inputs η and $\bar{\eta}$ from I. Let $s \in \bar{S}$ and $i'_j \in I'$ be such that $(\phi(s), i'_j, t')$ is a triple of A'; choose $t \in \bar{S}$ such that $\phi(t) = t'$ and define

$$h(s, i'_j) = h_s(i'_j) = \eta^j \, \bar{\eta} \, w_{qt} \;,$$

where $q = s(\eta^j \bar{\eta})$. Clearly, h_s is 1–1 for each $s \in S$; also, for each $s \in S$ and $i'_j \in I'$, the relation $\phi(sh_s(i'_j)) = \phi(s)i'_j$ holds. (In fact, the pair (ϕ, h) defines a generalization of the classical automata-theoretic notion of realization; this is dealt with in detail in [2], see also [3].) We can also extend h to domain $\bar{S} \times (I')^*$ inductively by the usual device of setting $h_s(i'_j x') = h_s(i'_j)\, h_t(x')$, where $x' \in (I')^*$ and $t = sh_s(i'_j) \in \bar{S}$.

We next show that the extended maps h_s are also one-to-one. Let $j_1 \ldots j_m$ and $k_1 \ldots k_{m'}$ be two non-empty strings over I' and let $h_s(j_1 \ldots j_m) = h_s(k_1 \ldots k_{m'}) = w$. Then, by definition, there are states r, $t \in \bar{S}$ such that $w = h_s(j_1)\, h_r(j_2 \ldots j_m) = h_s(k_1)\, h_t(k_2 \ldots k_{m'})$. But there is a unique positive integer b such that the prefix of w having length $b + 1$ is the string $\eta^b \, \bar{\eta}$. This uniquely determines $j_1 = k_1 = i'_b$, so that

$r = t = sh_s(i'_b)$. Then $h_r(j_2 \ldots j_m) = h_r(k_2 \ldots k_{m'})$, and we can repeat the above process until we arrive at $m = m'$ and $j_p = k_p$, $p = 1, 2, \ldots, m$.

Note that for the extended maps to be one-to-one it is not sufficient to simply have h_s be one-to-one on symbols for each $s \in \overline{S}$. For, using the above notation, suppose $h_s(j_1) = c$, $h_s(k_1) = c\,d$, $h_r(j_2) = d\,e$, $h_t(k_2) = e$. Then $h_s(j_1\,j_2) = h_s(k_1\,k_2) = c\,d\,e$, but $j_1\,j_2 \neq k_1\,k_2$.

We now have the machinery necessary to prove the theorem.

Let $b' = \{(s', x', t')\}$ be a singleton in $\mathcal{S}^*(A')$ and set $g(b') = \{(s, h_s(x'), t) \colon \phi(s) = s'\}$; since ϕ is one-to-one and onto, $g(b')$ is a singleton. Note that we must have $\phi(t) = t'$. Also, since h_s is one-to-one for each $s \in \overline{S}$, $g(b'_1) = g(b'_2)$ if and only if $b'_1 = b'_2$; i.e., g is one-to-one. Let $b'_1 = \{(s'_1, x'_1, r')\}$ and $b'_2 = \{(r', x'_2, t'_2)\}$. Let $b_1 = \{(s_1, x_1, r)\} = g(b'_1)$ and $b_2 = \{(r, x_2, t_2)\} = g(b'_2)$. Then $b_1 \circ b_2 = \{(s_1, h_{s_1}(x'_1 x'_2), t_2)\}$ is a singleton of $\mathcal{S}^*(M)$ and, as $\phi(t_2) = t'_2$, $b_1 \circ b_2 = g(b'_1 \circ b'_2)$. Thus $g(b'_1) \circ g(b'_2) = g(b'_1 \circ b'_2)$. On the other hand, if $b'_1 = \{(s'_1, x'_1, t'_1)\}$, $b'_2 = \{(s'_2, x'_2, t'_2)\}$, $g(b'_1) = \{(s_1, x_1, t_1)\}$, $g(b'_2) = \{(s_2, x_2, t_2)\}$ and $t'_1 \neq s'_2$, then $t_1 \neq s_2$, so that $b'_1 \circ b'_2 = 0$ and $g(b'_1) \circ g(b'_2) = 0$.

Now let V' be any element of $\mathcal{S}^*(A')$; V' is a finite set of triples of M'. Extend g to g^* by $g^*(V') = \{g(b') \colon b \in V'\}$. Let $\mathcal{S}^*_{A'}(A)$ be $\{g^*(V') \colon V' \in \mathcal{S}^*(A')\}$.

Now, if $V'_1, V'_2 \in \mathcal{S}^*(A')$,

$$\begin{aligned} g^*(V'_1) \circ g^*(V'_2) &= [\bigcup \{g(b'_i) \colon b'_i \in V'_1\}] \circ [\bigcup \{g(d'_j) \colon d'_j \in V'_2\}] \\ &= \bigcup_{i,j} \{g(b'_i) \circ g(d'_j) \colon b'_i \in V'_1, d'_j \in V'_2\} \\ &= \bigcup_{i,j} \{g(b'_i \circ d'_j) \colon b'_i \in V'_1, d'_j \in V'_2\} \\ &= \bigcup \{g(f'_k) \colon f'_k \in V'_1 \circ V'_2\} = g^*(V'_1 \circ V'_2)\,. \end{aligned}$$

Thus $\mathcal{S}^*_{A'}(A)$ is a subsemigroup of $\mathcal{S}^*(A)$, and g^* is a homomorphism. We wish to show that g^* is one-to-one. Suppose $g^*(V'_1) = g^*(V'_2)$. Choose a triple $b'_1 \in V'_1$, and let $\{b\} = g(\{b'_1\})$. Then there is a triple $b'_2 \in V'_2$ such that $\{b\} = g(\{b'_2\})$. If $b = (s, w, t)$, $b'_1 = (\phi(s), x'_1, \phi(t))$ and $b'_2 = (\phi(s), x'_2, \phi(t))$, where $w = h_s(x'_1) = h_s(x'_2)$. Then, since h_s is one-to-one, $x'_1 = x'_2$, so $b'_1 = b'_2$ and $V'_1 \subseteq V'_2$. The symmetric argument gives $V'_1 = V'_2$ so that g^* is $1-1$, and hence g^* is an isomorphism between $\mathcal{S}^*(A')$ and $\mathcal{S}^*_{A'}(A)$.

Corollary 2. *Let A and A' be strong machines, with $|S| = |S'|$. Then, unless A is autonomous but A' is not, $\mathcal{S}^*(A')$ is isomorphic to a subsemigroup of $\mathcal{S}^*(A)$.*

Proof. If M is not autonomous, then $\mathcal{S}^*(A') \cong \mathcal{S}^*_{A'}(A)$, by the theorem. On the other hand, if both machines are autonomous, then they are isomorphic, so the result follows trivially.

We now proceed to consider the remaining case of the conjecture. For $n \geq 2$, let R_n be the *complete reset machine* (Q_n, X_n, δ_n), where $Q_n = \{q_1, ..., q_n\}$, $X_n = \{x_1, ..., x_n\}$ and for any j, $q_j x_i = q_i$. Also, let C_n be the unique strong autonomous machine $(K_n, \{1\}, \delta'_n)$, where $K_n = \{k_1, k_2, ..., k_n\}$ and $k_i 1 = k_{i+1}$; $1 \leq i < n$ and $k_n 1 = k_1$.

Theorem 3. *The semigroup $\mathcal{S}^*(R_n)$ cannot be isomorphically embedded in $\mathcal{S}^*(C_n)$.*

Proof. Let $\phi : \mathcal{S}^*(R_n) \to \mathcal{T}^* \subseteq \mathcal{S}^*(C_n)$ be an isomorphism. In any semigroup $\mathcal{S}$ with zero, for each $s \in \mathcal{S}$, define $s^{\perp} = \{t: st \neq 0\}$ and $s^{\top} = \{t: ts \neq 0\}$. Since ϕ is an isomorphism, it follows that for each $s \in \mathcal{S}^*(R_n)$, $\phi(s^{\perp}) = \phi(s)^{\perp}$ and $\phi(s^{\top}) = \phi(s)^{\top}$. (Further results on these annihilation operations appear in [5].)

For any triple $b = (r, x, t)$, define $i(b) = r$ and $f(b) = t$; for a set S of triples $i(S) = \{i(b): b \in S\}$ and $f(S) = \{f(b): b \in S\}$. Clearly, for any semigroup element s, $s^{\perp} = \{u: f(s) \cap i(u) \neq \emptyset\}$ and $s^{\top} = \{u: f(u) \cap i(s) \neq \emptyset\}$.

Let the set of elementary triples of $\mathcal{S}^*(R_n)$ be $B = \{b_{ij} = (q_i, x_j, q_j)\}$. For each i, j and k, $b_{ij}^{\top} = b_{ik}^{\top}$ and $b_{ji}^{\perp} = b_{ki}^{\perp}$. Note that if $i \neq j$, there is no elementary triple b such that both $b_{ki}b$ and $b_{kj}b$ are non-zero. Suppose that for two triples b_{rp} and b_{rq}, $p \neq q$, there is an element $e \in f(\phi(b_{rp})) \cap f(\phi(b_{rq}))$. Then e cannot be an element of $i(\phi(b))$ for any $b \in B$, as otherwise both $\phi(b_{rp})\,\phi(b) \neq 0$ and $\phi(b_{rq})\,\phi(b) \neq 0$, and hence both $b_{rp}b$ and $b_{rq}b$, would be non-zero. However, for each elementary triple b_{rp}, $\phi(b_{rp})^{\perp} \neq \emptyset$. Thus each set $f(\phi(b_{ri}))$, $i = 1, ..., n$, must contain some element from K_n which is not contained in any of the others. This is only possible if each set $f(\phi(b_{ri}))$ is a singleton. As this analysis holds for each r, it follows that there is a mapping $\eta : Q_n \xrightarrow{1-1} K_n$ such that $f(\phi(b_{ij})) = \eta(q_j)$. Similarly, there must be a mapping $\mu : Q_n \xrightarrow{1-1} K_n$ such that

$i(\phi(b_{ij})) = \mu(q_i)$; however, since $b_{ij}\, b_{jk} \neq 0$, it must be the case that for each j, $\mu(q_j) = \eta(q_j)$.

Thus, for each elementary triple b_{ij}, $\phi(b_{ij})$ is a set of triples $\{(\eta(q_i), 1^{n_{ijk}}, \eta(q_j)) \colon n_{ijk} > 0,\ 1 \leq k \leq N_{ij}\}$. Consider $\alpha_1 = b_{12}\, b_{22}\, b_{21}\, b_{12}$ and $\alpha_2 = b_{12}\, b_{21}\, b_{12}\, b_{22}$. Clearly, $i(\alpha_1) = i(\alpha_2) = \eta(q_1)$ and $f(\alpha_1) = f(\alpha_2) = \eta(q_2)$. If $(\eta(q_1), 1^n, \eta(q_2)) \in \phi(\alpha_1)$, then n can be written as follows: $n = n_{12k_1} + n_{22k_2} + n_{21k_3} + n_{12k_4}$. But, of course, $n = n_{12k_1} + n_{21k_3} + n_{12k_4} + n_{22k_2}$, so that $(\eta(q_1), 1^n, \eta(q_2)) \in \phi(\alpha_2)$. Conversely, $\phi(\alpha_2) \subset \phi(\alpha_1)$, so that $\phi(\alpha_1) = \phi(\alpha_2)$ even though $\alpha_1 \neq \alpha_2$; hence ϕ is not an isomorphism.

Corollary 4. *If A is a strong machine with n states and at least 2 inputs, then $\mathcal{S}^*(A)$ cannot be isomorphically embedded in $\mathcal{S}^*(C_n)$.*

Proof. This follows immediately since, by the previous result, $\mathcal{S}^*(R_n)$ can be isomorphically embedded in $\mathcal{S}^*(A)$.

References

[1] A.C. Fleck, S.T. Hedetniemi and R.H. Oehmke, $\mathcal{S}$-semigroups of automata, J. Assoc. Comput. Mach. 19 (1972) 3–10.

[2] D.P. Geller, Realization with feedback encoding, Doctoral Thesis, Department of Computer and Communication Sciences, Univ. of Michigan, Ann Arbor, Mich., 1972.

[3] D.P. Geller, Realization with feedback encoding I. Analogues for the classical theory, SIAM J. Comput., to appear.

[4] S.T. Hedetniemi and A.C. Fleck, $\mathcal{S}$-semigroups of automata, Technical Report 6, THEMIS Project, Univ. of Iowa (1970).

[5] R.H. Oehmke, On $\mathcal{S}$*-semigroups of automata, Technical Report 8, THEMIS Projec' Univ. of Iowa (1969).