THE AUTOMATA THEORY OF SEMIGROUP EMBEDDINGS

MICHAEL ARBIB

(Received 5 September 1967)

1. Abstract

The theorem of Trevor Evans [1] that every countable semigroup can be embedded in a two-generator semigroup becomes obvious in automata theory as the statement that every countable automaton can be embedded in one with binary inputs. Standard techniques of automata theory [1], [3] yield a proof of the Evans Theorem using wreath products, as in Neumann [4].

2.

An automaton M (without output) is a triple (Q, X, δ) where Q is the set of states, X is the input set, and $\delta : Q \times X \to Q$. The semigroup $S(M)$ is the subsemigroup of Q^Q generated by the maps $\delta(\cdot, x) : Q \to Q$. M is called countable [finite] if Q is countable [finite].

Given a countable semigroup S with generators $G(S)$, we may represent it as the semigroup of the machine $M_S = (S^1, G(S), \delta_S)$ where δ_S is multiplication in the semigroup S, and S^1 is S with a unit adjoined only if S is not a monoid.

We then replace M_S by a machine which has input set $\{0, 1\}$ and which reads in strings until a code (i.e., a monomorphism of $\mathscr{F}_{G(S)}$, the free semigroup generated by $G(S)$, into $\mathscr{F}_{\{0,1\}}$) for an element of $G(S)$ has been read, and then acts accordingly.

We now give two examples of codes and the corresponding constructions.

One which works whether or not $G(S) = \{s_1, s_2, \cdots\}$ is finite is to code s_j as $1^j 0$, i.e. a string of j ones followed by a zero. Then

$$M_1 = (N \times S^1, \{0, 1\}, \delta_2) \qquad (\text{taking } N = \{1, 2, 3, \cdots\})$$

with

$$\delta_1((n, s), 0) = (0, s \cdot s_n)$$
$$\delta_1((n, s), 1) = (n+1, s)$$

and the map $s_j \to 1^j 0$ yields an embedding of S in the two-generator semigroup $S(M_1)$. If $G(S) = \{s_1, \cdots, s_d\}$ is finite, we can replace N by $\{1, \cdots, d\}$, addition then being modulo d to handle sequences not coding words of S, so that $S(M_1)$ *is finite if* S *is finite.*

If $G(S) = \{s_1, \cdots, s_d\}$ is finite and $2^{m-1} < d \leqq 2^m$ we may give a 'faster' construction, encoding each s_j as a distinct string t_j of m 0's and 1's. Then if A is the set of strings of at most $m-1$ 0's and 1's (including the empty string Λ) we may set

$$M_2 = (A \times S^1, \{0, 1\}, \delta_2)$$

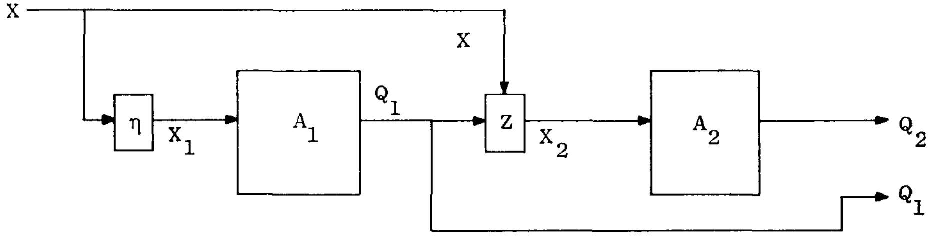
with

$$\delta_2([u_1 \cdots u_k, s], u) = \begin{cases} [u_1 \cdots u_k u, s] & \text{if } \ 0 \leqq k < n-1 \\ [\Lambda, s \cdot s_j] & \text{if } \ k = n-1 \text{ and } t_j = u_1 \cdots u_k u \\ [\Lambda, s] & \text{else} \end{cases}$$

and the map $s_j \to t_j$ yields an embedding of S in the two-generator semigroup $S(M_2)$.

It should be clear how this construction can be extended to arbitrary codes.

We now show how our result yields Neumann's wreath-product approach. The cascade $A_2 \times_Z^\eta A_1$ of any two automata $A_j = (Q_j, X_j, \lambda_j)$ with connecting map $Z : Q_1 \times X \to X_2$ and encoder $\eta : X \to X_1$ is the automaton with $\lambda_Z^\eta([q_2, q_1], x) = [\lambda_2(q_2, Z(q_1, x)), \lambda_1(q_1, \eta(x))]$ and (as was first pointed out by Krohn and Rhodes [3], see also [1]) the semigroup of $A_2 \times_Z^\eta A_1$ can be embedded in the wreath product of $S(A_2)$ and $S(A_1)$.



$(Q_2 \times Q_1, X, \lambda_Z)$

Now it is clear from the definitions of δ_1 and δ_2 that both M_1 and M_2 are cascades of some machine A_1 with M_{S^1}. In the case of the first construction, the semigroup T_0 of A_1 is $N^0[\{1, \cdots, d\}^0$ if $G(S)$ is finite] — that is, the integers under addition [modulo d] with a *multiplicative* zero adjoined. In either case, we see that S can be embedded in a two-generator semigroup which can in turn be embedded in the wreath product of $S(A_1)$ and S^1. The first construction yields what is essentially Neumann's proof. However, where Neumann [4] took the order m of his cyclic group T to be at least $3d$

in the finite case, we only need take $m = d$, though we must adjoin our 0 to T whereas he adjoins his zero to S. It then becomes a simple exercise to obtain the results of Neumann's Section 5 with improved bounds. We hope this note will encourage further applications of automata theory to the algebraic theory of semigroups.

This research was supported in part by the U. S. Air Force Office of Scientific Research (Information Sciences Directorate) under Contract No. AF-AFOSR-1198-67.

My thanks to Shafee Give'on for a helpful reading of the manuscript.

References

[1] M. A. Arbib, 'Automaton Decompositions and Semigroup Extensions', in: *The Algebraic Theory of Machines, Languages and Semigroups*, M. A. Arbib (Editor), Academic Press, (1968), 37—54.

[2] T. Evans, 'Embedding Theorems for Multiplicative Systems and Projective Geometries', *Proc. Amer. Math. Soc.* 3 (1952), 614—620.

[3] K. Krohn and J. L. Rhodes, 'Algebraic Theory of Machines, I: The Decomposition Results', *Trans. Amer. Math. Soc.* 116 (1965), 450—464.

[4] B. H. Neumann, 'Embedding Theorems for Semigroups', *J. London Math. Soc.* 35 (1960), 184—192.

Electrical Engineering Department
Stanford University
Stanford, California 94305 U.S.A.