JOURNAL OF COMPUTER AND SYSTEM SCIENCES 14, 150–155 (1977)

# A Semigroup Characterization of a Linearly Realizable Automaton over $GF(p)$

D. J. HARTFIEL AND C. J. MAXSON

*Department of Mathematics, Texas A & M University, College Station, Texas 77843*

Received February 10, 1976; revised May 28, 1976

This paper gives necessary and sufficient conditions on a semigroup to guarantee that if the semigroup is isomorphic to the semigroup of a finite automaton, then the finite automaton can be linearly realized over $GF(p)$, for some prime $p$.

## INTRODUCTION

In recent years, much research in the field of automata has been concerned with the problem of whether or not a finite automaton can be realized by a linear automaton over $GF(p)$. An algebraic approach to this problem is to determine necessary and sufficient conditions on the semigroup of the finite automaton which guarantee that the finite automaton can be realized by a linear automaton.

Using this algebraic approach, Ecker [1] studied the problem for those automata which were also permutation automata. In [1] he provided necessary and sufficient conditions for a group to be isomorphic to a group of *some* linear automaton over $GF(p)$. In [3], Hartmanis and Walter show that this does not resolve the problem for permutation automata by exhibiting a group which is isomorphic to the group of a linear automaton and which is also isomorphic to a group of a permutation automata that cannot be linearly realized over $GF(p)$. Hartmanis and Walter, then, by utilizing the work of Ecker, resolve the problem for finite automata which are also permutation automata.

Hartmanis and Walter remark in the conclusion of their paper [3], that "it would now be very interesting to see whether a similar characterization cannot be given in terms of the semigroup of all linearly realizable automaton over $GF(p)$." In this regard, Ecker in [2] provides necessary and sufficient conditions for a semigroup to be isomorphic to a semigroup of *some* linear automaton over $GF(p)$. However, by again using the example of Hartmanis and Walter in [3], this does not resolve the problem.

The purpose of this paper, then, is to provide necessary and sufficient conditions on a semigroup to guarantee that if the semigroup is a semigroup of a finite automaton, then the finite automaton can be linearly realized over $GF(p)$.





ISSN 0022-0000

## 1. Semigroups of Linear Automata

In this section we characterize those semigroups which can be shown to be isomorphic to a semigroup of *some* linear automaton. Ecker in [2] also provides such a set of conditions; however, we feel that since our conditions are more closely related to the generators of the semigroup of the automaton, our conditions provide greater insight into the problem. Further, we feel that our conditions are more compatable with the conditions given in [1, 3].

Our result requires the notation that if $S$ denotes a semigroup with $\phi_0, \phi_1, \ldots, \phi_r \in S$, then $\langle \phi_0, \phi_1, \ldots, \phi_r \rangle$ denotes the semigroup generated by $\phi_0, \phi_1, \ldots, \phi_r$. Using this notation we have the following.

THEOREM 1. *There is an isomorphism $\beta$ between a semigroup $S = \langle \phi_0, \phi_1, \ldots, \phi_r \rangle$ and a semigroup of a linear automaton with states in $V_n[GF(p)]$ where $(\beta\phi_i)(s) = As + Bx_i$ for $i = 1, 2, \ldots, r$ if and only if $S$ is a subsemigroup of a monoid $\mathscr{S} = \langle \phi_0, N \rangle$ where*

(a) *$N$ is an abelian group, containing the identity of $\mathscr{S}$, each element of which has order $p$.*

(b) $\phi_0 N = N\phi_0$,

(c) *if $\psi', \psi'' \in N$ with $\psi'\phi_0{}^k = \psi''\phi_0{}^k$ then $\psi' = \psi''$ and*

(d) $\{\phi_0, \phi_1, \ldots, \phi_r\} \subseteq N\phi_0$.

*Proof.* Suppose first, without loss of generality, that $S = \langle \phi_0, \phi_1, \ldots, \phi_r \rangle$ is a semigroup of a linear automaton where $\phi_i(s) = As + Bx_i$ for $i = 0, 1, \ldots, r$. Define $\psi_i(s) = s + Bx_i - Bx_0$. Then $\psi_i\phi_0(s) = \psi_i(As + Bx_0) = As + Bx_0 + Bx_i - Bx_0 = As + Bx_i = \phi_i(s)$. Hence, $\psi_i\phi_0 = \phi_i$ for $i = 1, 2, \ldots, r$. Set $N = \{\psi \mid \psi(s) = s + x$ for some $x \in V_n[GF(p)]\}$. It is easily seen that $N$ is an abelian group, each element of which has order $p$. Further, if $\psi \in N$, then $\phi_0\psi(s) = \phi_0(s + x) = As + Ax + Bx_0 = As + Bx_0 + Ax = \psi'[As + Bx_0] = \psi'\phi_0(s)$ where $\psi'(s) = s + Ax$. Thus, as $\psi' \in N$, $\phi_0 N = N\phi_0$.

Finally if $\psi', \psi'' \in N$ and $\psi'\phi_0{}^k = \psi''\phi_0{}^k$ then as $\psi'\phi_0{}^k(s) = \phi_0{}^k(s) + x'$ and $\psi''\phi_0{}^k(s) = \phi_0{}^k(s) + x''$ it follows that $x' = x''$ and $\psi' = \psi''$.

Thus, $S$ is a subsemigroup of the monoid $\mathscr{S} = \langle \phi_0, N \rangle$ which satisfies properties (a) through (d).

Conversely, suppose $S$ is a subsemigroup of a semigroup $\mathscr{S} = \langle \phi_0, N \rangle$ which satisfies properties (a) through (d). Define a relation on $\mathscr{S}$ as follows. Set $\sigma\mu\gamma$ in $\mathscr{S}$ if and only if there is a $\psi \in N$ so that $\sigma = \psi\gamma$. Since $N$ is a group, this relation is an equivalence relation. Thus, this equivalence relation partitions $\mathscr{S}$ into disjoint equivalence classes. We show these classes to be $N, N\phi_0, \ldots, N\phi_0{}^t$ for some $t$.

For this, note that it is clear that each $N\phi_0{}^i$ is a subset of some equivalence class. Thus suppose $N\phi_0{}^i$ and $N\phi_0{}^j$ are subsets of the same equivalence class. Then, $\phi_0{}^i\mu\phi_0{}^j$ so that $N\phi_0{}^i = N\phi_0{}^j$. Hence, the equivalence classes of $\mathscr{S}$ are $N, N\phi_0, \ldots, N\phi_0{}^t$, for some $t$.

By (c), each element $\phi \in N\phi_0{}^k$ has a unique representation $\phi = \psi\phi_0{}^k$ for some $\psi \in N$. Since $N$ is a finite elementary abelian $p$-group, $N$ is trivially isomorphic to $V_s[GF(p)]$,

hence $n$ has a basis say $\psi_1, \psi_2, \ldots, \psi_s$. Set $n = s + t$. Define a mapping $\mathscr{E}$ of $n$ into $V_n[GF(p)]$ by setting

$$\mathscr{E}(\psi_i) = e^i \qquad \text{for} \quad i = 1, 2, \ldots, s$$

and

$$\mathscr{E}(\psi_1^{l_1} \cdots \psi_s^{l_s}) = l_1 e^1 + \cdots + l_s e^s.$$

Extending $\mathscr{E}$ to the remaining equivalence classes of $S$, define

$$\mathscr{E}(\psi\phi_0^{\,k}) = \mathscr{E}(\psi) + e^{s+k} \qquad \text{for} \quad \psi \in N \qquad \text{and} \qquad 1 \leqslant k \leqslant t.$$

Define

$$A = (\mathscr{E}(\phi_0\psi_1) - \mathscr{E}(\phi_0), \ldots, \mathscr{E}(\phi_0\psi_s) - \mathscr{E}(\phi_0), \mathscr{E}(\phi_0^{\,2}) - \mathscr{E}(\phi_0), \ldots, \mathscr{E}(\phi_0^{\,t+1}) - \mathscr{E}(\phi_0)).$$

Using property (d), write $\phi_i = \phi_0\hat{\psi}_i$ for $i = 1, 2, \ldots, r$.

Define

$$B = (A[\mathscr{E}(\hat{\psi}_1)] + \mathscr{E}(\phi_0), \ldots, A[\mathscr{E}(\hat{\psi}_r)] + \mathscr{E}(\phi_0), \mathscr{E}(\phi_0), 0, \ldots, 0).$$

Then by direct calculation,

$$\begin{aligned}
A[\mathscr{E}(\psi_1^{l_1} \cdots \psi_s^{l_s}\phi_0^{\,k})] &= A[\mathscr{E}(\psi_1^{l_1} \cdots \psi_s^{l_s}) + \mathscr{E}(\phi_0^{\,k})] \\
&= l_1(\mathscr{E}(\phi_0\psi_1) - \mathscr{E}(\phi_0)) + \cdots + l_s(\mathscr{E}(\phi_0\psi_s) - \mathscr{E}(\phi_0)) + \mathscr{E}(\phi_0^{\,k+1}) - \mathscr{E}(\phi_0) \\
&= l_1(\mathscr{E}(\bar{\psi}_1\phi_0) - \mathscr{E}(\phi_0)) + \cdots + l_s(\mathscr{E}(\bar{\psi}_s\phi_0) - \mathscr{E}(\phi_0)) + \mathscr{E}(\psi_0^{k+1}) - \mathscr{E}(\phi_0) \\
&= l_1\mathscr{E}(\bar{\psi}_1) + \cdots + l_s\mathscr{E}(\bar{\psi}_s) + \mathscr{E}(\phi_0^{k+1}) - \mathscr{E}(\phi_0) \\
&= \mathscr{E}(\bar{\psi}_1^{l_1} \cdots \bar{\psi}_s^{l_s}\phi_0^{k+1}) - \mathscr{E}(\phi_0) \\
&= \mathscr{E}(\phi_0\psi_1^{l_1} \cdots \psi_s^{l_s}\phi_0^{\,k}) - \mathscr{E}(\phi_0).
\end{aligned}$$

Thus

$$\begin{aligned}
\mathscr{E}[\phi_0(\psi_1^{l_1} \cdots \psi_s^{l_s}\phi_0^{\,k})] &= A[\mathscr{E}(\psi_1^{l_1} \cdots \psi_s^{l_s}\phi_0^{\,k})] + \mathscr{E}(\phi_0) \\
&= A[\mathscr{E}(\psi_1^{l_1} \cdots \psi_s^{l_s}\phi_0^{\,k})] + B(e^{r+1}).
\end{aligned}$$

Now, since $\phi_i = \phi_0\hat{\psi}_i$ for $i = 1, 2, \ldots, r$, by direct calculation,

$$\begin{aligned}
\mathscr{E}[\phi_i(\psi_1^{l_1} \cdots \psi_s^{l_s}\phi_0^{\,k})] &= \mathscr{E}[\phi_0(\hat{\psi}_1\psi_1^{l_1} \cdots \psi_s^{l_s}\phi_0^{\,k})] \\
&= A[\mathscr{E}(\hat{\psi}_i\psi_1^{l_1} \cdots \psi_s^{l_s}\phi_0^{\,k})] + \mathscr{E}(\phi_0) \\
&= A[\mathscr{E}(\hat{\psi}_i\psi_1^{l_1} \cdots \psi_s^{l_s}) + \mathscr{E}(\psi_0^{\,k})] + \mathscr{E}(\phi_0) \\
&= A[\mathscr{E}(\hat{\psi}_i) + \mathscr{E}(\psi_1^{l_1} \cdots \psi_s^{l_s}) + \mathscr{E}(\psi_0^{\,k})] + \mathscr{E}(\phi_0) \\
&= A[\mathscr{E}(\psi_1^{l_1} \cdots \psi_s^{l_s}\phi_0^{\,k})] + A[\mathscr{E}(\hat{\psi}_i)] + \mathscr{E}(\phi_0) \\
&= A[\mathscr{E}(\psi_1^{l_1} \cdots \psi_s^{l_s}\phi_0^{\,k})] + B(e^i).
\end{aligned}$$

Define mappings on $V_n[GF(p)]$ as follows.

$$\pi_0(s) = As + B(e^{r+1})$$

and

$$\pi_i(s) = As + B(e^i) \qquad \text{for} \quad i = 1, 2,..., r.$$

Then $\langle \pi_0 , \pi_1 ,..., \pi_r \rangle$ is a monoid of a linear automaton. Thus, as $S = \langle \phi_0 , \phi_1 ,..., \phi_r \rangle$, the matching $\beta(\phi_i) = \pi_i$ for $i = 0, 1,..., r$ shows that $S$ is isomorphic to a semigroup of a linear automaton.

As explained in the Introduction, this theorem does not provide necessary and sufficient conditions for a semigroup to be a semigroup of a finite automaton which can be linearly realized over $GF(p)$. For this result, we include the next section.

## 2. A Semigroup Characterization of Linear Automa

In this section we use the construction given in Theorem 1 to answer the question posed by Hartmanis and Walter in [3]. That is, we obtain a semigroup characterization of those automata which can be linearly realized over the field $GF(p)$.

We begin by recalling some definitions from semigroup theory. A set $X$ is an $S$-set for the monoid $S$ if there is an action $S \times X \to X$ denoted by $(s, x) \to sx$ such that $(st)x = s(tx)$ and $1x = x$ where 1 is the identity in $S$. If $X_1$ and $X_2$ are $S$-sets, a mapping $f: X_1 \to X_2$ is an $S$-homomorphism if $f(sx) = sf(x)$, $s \in S$, $x \in X$. Continuing, we recall that an equivalence relation $\rho$ on $S$ is a left congruence on $S$ if whenever $a\rho b$ then $ca\rho cb$ for each $c$ in $S$. Thus, if $\rho$ is a left congruence, $S/\rho$ is an $S$-set.

Let $M$ be an automaton with states $Q$, inputs $I$ and, without loss of generality, starting state $s_0$. Let $S$ denote the monoid of functions generated by $M$. The following result, a matter of folklore, shows that $M$ is completely determined (up to an isomorphism) by the semigroup $S$, the inputs $I$ and a left congruence $\rho$ on $S$.

Lemma. *Let $M$ be an automaton with states $Q$, inputs $I$, and starting state $s_0$. Then there exists a left congruence $\rho$ on $S$ such that $S/\rho$ is a cyclic $S$-set and $Q$ is $S$-isomorphic $S/\rho$. Conversely, if $S$ is a semigroup with generators $I$ and left congruence $\rho$ such that $S/\rho$ is cyclic with generator $x_0$ then there is an automaton with starting state $x_0$, inputs $I$, and states $S/\rho$.*

In view of the above lemma we shall denote the automaton $M$ by $M(S, I, \rho)$ and express our characterization of automata which are linearly realizable in terms of $S$, $I$, and $\rho$.

Before stating our characterization we need one further remark. Recall that in the construction, given in the proof of Theorem 1, of a linear automaton from the semigroup $S$, an equivalence relation $\mu$ was defined on $\mathscr{S}$ by $s\mu t$ if $s = \psi t$ for $\psi$ in $N$. Using properties

of $\mathscr{S}$, we note that $\mu$ is a left congruence on $\mathscr{S}$. In fact for $r \in \mathscr{S}$, we note that $r = \chi\phi_0^k$, $\chi \in N$. Thus if $s = \psi t$, then

$$rs = r\psi t = \chi\phi_0^k\psi t = \chi\bar{\psi}\phi_0^k t = \bar{\psi}\chi\phi_0^k t = \bar{\psi}rt.$$

Hence $\mu$ is a left congruence. We now give our semigroup characterization of linear automata.

THEOREM 2. *Let $M = M(S, I, \rho)$ be an automaton with $I = \{\phi_0, \phi_1, ..., \phi_r\}$. Then $M$ is linearly realizable over the field $GF(p)$ if and only if $S$ is a subsemigroup of a monoid $\mathscr{S} = \langle \phi_0, N \rangle$ where*

(a) *$N$ is an elementary abelian $p$-group containing the identity of $\mathscr{S}$,*

(b) *$N\phi_0 = \phi_0 N$,*

(c) *if $\psi', \psi'' \in N$ with $\psi'\phi_0^k = \psi''\phi_0^k$, then $\psi' = \psi''$,*

(d) *$\{\phi_0, \phi_1, ..., \phi_r\} \subseteq N\phi_0$, and*

(e) *$\rho$ can be extended to a left congruence $\bar{\rho}$ on $\mathscr{S}$ such that $\bar{\rho} \cap \mu = \mathrm{id}$.*

*Proof.* Suppose $M(S, I, \rho)$ is linearly realizable over $GF(p)$. The existence of the semigroup $\mathscr{S}$ with the desired properties follows from Theorem 1. Thus we must show that $\rho$ extends to a left congruence $\bar{\rho}$ on $\mathscr{S}$ having trivial intersection with the left congruence $\mu$. For this, let $s, t \in \mathscr{S}$, $s = \chi_1\phi_0^j$ and $t = \chi_2\phi_0^k$. Define $\bar{\rho}$ on $\mathscr{S}$ by $s\bar{\rho}t$ if $\chi_1 = \chi_2$ and $\phi_0^j\rho\phi_0^k$. Clearly $\bar{\rho}$ is an equivalence relation on $\mathscr{S}$. Let $r \in \mathscr{S}$, $r = \chi_3\phi_0^l$. Then $rs = \chi_3\phi_0^l\chi_1\phi_0^j = \chi_3\bar{\chi}_1\phi_0^{l+j}$ while $rt = \chi_3\bar{\chi}_2\phi_0^{l+k}$. Thus if $s\bar{\rho}t$ then $\chi_1 = \chi_2$ and $\phi_0^{l+j}\rho\phi_0^{l+k}$ since $\rho$ is a left congruence on $S$. Hence $\bar{\rho}$ is a left congruence on $\mathscr{S}$. Suppose $(s, t) \in \bar{\rho} \cap \mu$. Then $s\mu t$ implies $s = \psi t$ for some $\psi \in N$ and thus by our coding, $\mathscr{E}(s) = \mathscr{E}(t) + \mathscr{E}(\psi)$. On the other hand, $s\bar{\rho}t$ implies $\mathscr{E}(s) = \mathscr{E}(t)$. Therefore $\mathscr{E}(\psi) = 0$. Thus $\psi$ is the identity in $N$ and hence $s = t$ as desired.

Conversely, suppose $\rho$ extends to $\bar{\rho}$ on $\mathscr{S}$ with $\bar{\rho} \cap \mu = \mathrm{id}$. Let $\bar{a}$ be any $\bar{\rho}$-class. If for $\psi \in N$, $\bar{a}, \bar{\psi}a, ..., \overline{\psi^{p-1}}a$ are all distinct then as in Theorem 1 a linear realization of $M(S, I, \rho)$ can be obtained. Suppose to the contrary that $\overline{\psi^j a} = \overline{\psi^k a}$, $j \neq k$. Without loss of generality, suppose $j > k$. Then $\psi^j a \bar{\rho} \psi^k a$ and since $\psi^j a = \psi^{j-k}\psi^k a$ we have $\psi^j a \mu \psi^k a$. Thus $\psi^j a = \psi^k a$. But then using the cancellation property we find that $j = k$, a contradiction. Therefore the $\bar{\rho}$-classes $\bar{a}, \overline{\psi a}, ..., \overline{\psi^{p-1}}a$ are distinct.

Since $\bar{\rho} \cap \mu = \mathrm{id}$, each element of $N$ is in a different $\bar{\rho}$-class. Thus the classes determined by $N$ are coded as in Theorem 1. If $\bar{s}$ is a class not yet coded, code $\bar{s}$ by $e^{r+1}$. Hence the classes $\overline{\psi s}$ are coded where $\psi$ ranges over $N$. Continuing in this manner we obtain a coding for $\mathscr{S}/\bar{\rho}$ and as in Theorem 1 we obtain a linear automaton. Since $\bar{\rho}$ extends $\rho$, the restriction to $S/\rho$ gives a linear realization of the automaton $M(S, I, \rho)$. This completes the proof of the theorem.

As an aid to the understanding of both Theorem 1 and Theorem 2, we give the following example.

EXAMPLE. Consider the semigroup $\mathscr{S}$ given by the following table.

| | $\psi_0$ | $\psi_1$ | $\phi_0$ | $\phi_1$ |
|---|---|---|---|---|
| $\psi_0$ | $\psi_0$ | $\psi_1$ | $\phi_0$ | $\phi_1$ |
| $\psi_1$ | $\psi_1$ | $\psi_0$ | $\phi_1$ | $\phi_0$ |
| $\phi_0$ | $\phi_0$ | $\phi_1$ | $\phi_0$ | $\phi_1$ |
| $\phi_1$ | $\phi_1$ | $\phi_1$ | $\phi_1$ | $\phi_0$ . |

It is clear that $\mathscr{S}$ and $S = \langle \phi_0 , \phi_1 \rangle$ with $I = \{\phi_0 , \phi_1\}$ and $N = \{\psi_0 , \psi_1\}$ satisfy the four properties of Theorem 1. Further, the classes for the equivalence $\mu$ are $N = \{\psi_0 , \psi_1\}$ and $N\phi_0 = \{\phi_0 , \phi_1\}$.

If $M = M(S, I, \mathrm{id})$ where id is the identity congruence on $S$, then, by extending id to the identity congruence on $\mathscr{S}$ we find that $M(S, I, \mathrm{id})$ is linearly realizable over $GF(2)$.

On the other hand, if $M = M(S, I, \rho)$ where $\rho$ is the universal congruence on $S$, then by extending $\rho$ to the congruence $\mu$ on $\mathscr{S}$ we see that $M(S, I, \rho)$ is not linearly realizable over $GF(2)$.

## References

1. K. H. Ecker, On the semigroup of a linear nonsingular automaton, *Math. Systems Theory* **6** (1973), 353–358.
2. K. H. Ecker, "Algebraische eigenschaften linearer automaten," Gesellschaft für Mathematik und Datenverarbeitung, Bonn, Nr. 87, 1974.
3. J. Hartmanis and H. Walter, Group theoretic characterization of linear permutation automata, *J. Comput. System Sci.* **7** (1973), 168–188.

*Printed in Belgium*