REPRINTED from JOURNAL OF COMPUTER AND SYSTEM SCIENCES
All Rights Reserved by Academic Press, New York and London

Vol. 7, No. 2, April 1973
*Printed in Belgium*

# Group Theoretic Characterization of Linear Permutation Automata

J. HARTMANIS*

*Gesellschaft für Mathematik und Datenverarbeitung mbH Bonn*

*and*

*Department of Computer Science, Cornell University, Ithaca, N.Y.*

AND

H. WALTER

*Institut für Angewandte Mathematik, Universität des Saarlandes, 66 Saarbrücken*

Received February 14, 1972

In this paper we characterize all permutation automata which can be linearly realized over the field $GF(p)$ in terms of the group generated by the automaton. From this group theoretic characterization of linear permutation automata we derive, among other results, a complete characterization of all homomorphisms of a linear automaton which yield linearly realizable image automata as well as several results about the structure of linear automata.

## I. INTRODUCTION

The specific purpose of this paper is to give a group theoretic characterization of linearly realizable permutation automata and to derive several applications from this new characterization of linear automata.

The general purpose of this paper is to illustrate by these results how group theoretic methods can be used to obtain results about automata and not only about the groups of automata. This is achieved by explicitly characterizing how an automaton generates its group and by incorporating this characterization in the group theoretic arguments which then can yield specific results about the automaton.

We start our considerations with the known observation that all transitive representations of a group $G$ as a permutation group are characterized (up to isomorphism) by the subgroups of $G$ which contain no normal subgroups of $G$ besides $\{1\}$. For any such subgroup $H$ of $G$ the permutations induced by $G$ on the set of left cosets

* This research has been supported in part by National Science Foundation Grant GJ-155 and GJ-22171X.

of $H$ form a group isomorphic to $G$. Thus, if a connected finite automaton $M$ generates the group $G(M) = G$, then we can view the states of $M$ as the left cosets of some subgroup $H$ of $G$ which contains no normal subgroups of $G$ besides $\{1\}$. Therefore the state transitions of any permutation automaton $M$ are completely described (up to isomorphism) by a group $G$, a subgroup $H$ and a subset $I$ of $G$: the automaton $M$ generates the group $G$ as a permutation group on the left cosets of $H$ (induced by $G$) and $I$ is the set of the input permutations of $M$. In view of this, we shall write

$$M = M_{G,H,I}$$

and express many of our results in terms of $G$, $H$ and $I$.

We also observe that the homomorphisms of

$$M_{G,\{1\},I}$$

are uniquely characterized by the subgroups of $G$. The fact that these subgroups which define the homomorphisms of the automaton do not have to be normal subgroups of $G$, as in the case of group homomorphisms, will play a very important role in the characterization of those homomorphisms of a linear automaton which preserve linearity.

To obtain our desired characterization of linear permutation automata

$$M_{G,H,I}$$

in terms of $G$, $H$ and $I$, we make use of a recent result obtained by Ecker [6]. Ecker showed that if $M$ is a linear, nonsingular automaton over the field $GF(p)$ and $G$ is the group generated by $M$, $G(M) = G$, then

(a) $G$ contains a normal, abelian subgroup $N$ in which all elements, except 1, have order $p$,

(b) there exists an element $c$ in $G$ such that $N$ and $c$ generate $G$.

Furthermore, it was shown by Ecker that for every finite group $G$ which satisfies the above conditions there exists an automaton $M$ which generates $G$, $G = M(G)$, and which can be linearly realized over $GF(p)$. Thus the above conditions characterize the groups of linear automata.

Unfortunately, there are many automata which generate groups satisfying the two conditions but which cannot be linearly realized over $GF(p)$. Our results will show that there are two ways in which an automaton $M$ can fail to be linearly realizable even if $G(M)$ satisfies the necessary and sufficient properties to be a group of a linear automaton. We may have choosen the wrong set of inputs $I$ for $M$ or the group $H$ of $M_{G,H,I}$ is improperly chosen. The result states:

$M_{G,H,I}$ is linearly realizable over $GF(p)$ if and only if

(a) $G$ has a normal, abelian subgroup $N$ in which each element, except 1, has order $p$,

(b) there exists an element $c$ in $G$ such that $N$ and $c$ generate $G$,

(c) $N \cap H = \{1\}$,

(d) $I \subseteq Na$ for some $a$ in $G$.

Using this result we can easily characterize the linearity preserving homomorphisms of any linear automaton:

Let $M = M_{G,\{1\},I}$ be linearly realizable over $GF(p)$ using the normal subgroup $N$. Then the homomorphic image $M_{G,H,I}$ of $M$, defined by the subgroup $H$ of $G$, is linearly realizable if and only if $H \cap N$ is a normal subgroup of $G$.

It is interesting to note that it was shown before that linearly realizable automata may have homomorphic images which cannot be linearly realized [3]. On the other hand, the complete solution of this problem, as stated above, was achieved only by means of group theoretic arguments. It is also clear that the use of the group $H$ defining the homomorphism of $M = M_{G,\{1\},I}$ and the normal subgroup $N$ used in the linear realization $M$ gives a very natural formulation of this result.

In the last part of this paper we derive several structural results about linear automata and characterize those permutation automata which have input independent components.

## II. Preliminaries

In this section we give the necessary definitions and state some results from group theory which are used in this paper.

All through this paper we consider only finite, connected permutation automata. More precisely, a *finite automaton* $M$ is a quintuple

$$M = (S, I, 0, \delta, \lambda),$$

where $S$, $I$ and 0 are nonempty, finite sets of states, inputs and outputs, respectively, and $\delta$ and $\lambda$ are the next state and output functions:

$$\delta\colon S \times I \to S,$$

$$\lambda\colon S \times I \to 0.$$

In this paper we will not explicitly consider the output of $M$ and concern ourselves only with the state transitions of $M$.

A finite automaton $M$ is a *permutation automaton* if for all $x$ in $I$, $\delta$ is a permutation of $S$, i.e., for all $x$,

$$\{\delta(s, x) \mid s \in S\} = S.$$

An automaton $M$ is said to be *connected* if for every two states $s$ and $t$ in $S$ there exists an input sequence $w$, $w$ in $I^*$, such that

$$\delta(s, w) = t.$$

Here, without any danger of misinterpretation, the natural extension of the function $\delta$ to $S \times I^*$ is again denoted by $\delta$.

For any permutation automaton $M$ the set of inputs, viewed as permutations on $S$, generate a group (of permutations on $S$) which is denoted by $G(M)$ and we refered to it as the *group of* $M$.

It is important to realize that a group $G$ can be generated as a permutation group in many different ways and that, even under very general definitions of realization [4], two automata which generate the same group $G$ do not have to realize each other. Thus in general the automata which generate the same group are not related by isomorphisms or homomorphisms even if we permit a change of the input words.

In much of previous work with groups (or semigroups) of an automaton the group was treated as the most important aspect and the results were about the properties of the groups and not directly about the automata.

Our purpose in this paper is to use group theoretic concepts to obtain results about automata. To do that we need a standard result from group theory about the representation of groups as transitive permutation groups. For more details and proofs see Chapter 5 of [7].

We say that a group $P$ of permutations on a set $S$ is a *representation* of the group $G$ if there is a mapping of $G$ onto $P$, $g \mapsto \pi(g)$, $g$ in $G$ and $\pi(g)$ in $P$, such that

$$\pi(g_1)\,\pi(g_2) = \pi(g_1 g_2).$$

Clearly, $P$ is a homomorphic image of $G$. If $P$ is an isomorphic image of $G$, then the representation of $G$ by $P$ is a *faithful representation.*

If every element of $S$ can be mapped on to any other element by a permutation in $P$ then we refer to the group $P$ as a *transitive* permutation group and the representation of $G$ is then a *transitive representation.* Since we consider only connected permutation automata $M$ we see that we will be dealing only with transitive representations of the group $G = G(M)$ by the automaton $M$.

For any subgroup $H$ of a group $G$ the group $G$ induces a group of permutations on the set of left cosets of $H$: for each $g$ in $G$

$$\pi(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix}, \qquad x \in G.$$

The following result shows how all transitive representations of a group $G$ as a permutation group are characterized by subgroups of $G$.

THEOREM. *Let $H$ be a subgroup of $G$ and let $g \mapsto \pi(g)$ be the transitive representation of $G$ as a permutation group of left cosets of $H$. Then the elements of $G$ mapped onto the identity of the permutation group form the largest normal subgroup $N$ of $G$ contained in $H$, denoted by $N(H)$, and the permutation group is isomorphic to $G/N(H)$. Therefore, the representation is faithful if and only if $H$ contains no normal subgroups besides $\{1\}$. Furthermore, any faithful transitive representation of $G$ as a permutation group is given (up to an isomorphism) by such a subgroup $H$ without normal subgroups larger than the identity.*

For a proof of this result see [7].

We immediately observe that if $G$ is an abelian group then all faithful, transitive representations of $G$ as permutation groups are isomorphic since all subgroups are obviously normal in $G$. Thus if the order of the inputs does not change the state transitions of a permutation automaton $M$ then the states of $M$ can be interpreted as elements of $G = G(M)$, the inputs can also be identified with elements of a subset of $G$ and the transition function is then given by the group operations. If the group $G = M(G)$ is not abelian then we face a more complicated situation and have to make explicit use of the subgroup $H$ of the previous theorem. Since a permutation automaton $M$ is completely characterized (up to isomorphism) by $G = G(M)$, the subgroup $H$ and the subset $I$ of $G$ we will write $M = M_{G,H,I}$.

Our next result shows that for permutation automaton $M$ the subgroups of $G = G(M)$ completely characterize the homomorphisms of $M$.

THEOREM. *An equivalence relation $E$ on $S$ is a congruence relation (homomorphism) on $M_{G,\{1\},I}$ iff the equivalence classes of $E$ are the left cosets of a subgroup $H$ of $G$.*

*Proof.* See [4].

Thus all homomorphism of the automaton $M_{G,K,I}$ are given by the subgroups $H$ of $G$ which contain $K$. The corresponding homomorphic image

$$M' = M_{G',H',I'}$$

is characterized by $G' \simeq G/N(H)$ and the corresponding images $H'$ and $I'$ of $H$ and $I$, respectively.

Note that we always identify all inputs of $M$ which induce the same permutation on $S$.

The fact that the homomorphisms of a finite permutation automaton $M$ are defined by arbitrary subgroups of $G(M)$, clearly indicate that many important aspects of automata theory cannot be reflected in the group $G(M)$ and that we must consider how a homomorphism of $M = M_{G,H,I}$ changes $G$ as well as $H$.

## III. Linear Machines

In the following considerations we are interested only in the state behavior of an automaton and we consider only the linear realization of the state transition function. It should be pointed out that other authors have included the output function in the definition of linearity of an automaton. For comprehensive discussion of linear automata, see [1, 2].

An automaton $M = (S, I, \delta)$ is *linearly realizable* over the field $GF(p)$ iff there exists two injections $h_1$ and $h_2$ mapping $I$ and $S$ into the set of $k$- and $s$-tuples of elements of $GF(p)$, respectively; and two compatible matrices $A$ and $B$ with elements in $GF(p)$ such that

$$h_1[\delta(s, x)] = Ah_1(s) + Bh_2(x).$$

Thus $M$ is linearly realizable iff we have a one-to-one state and input encodings which yield a linear next-state function $\delta$ in the operations of $GF(p)$.

To see what properties the group $G = G(M)$ of a linear automaton $M$ must have we assume that the linear realization of $M$ over $GF(p)$ is given by

$$h_1[\delta(s, x)] = Ah_1(s) + Bh_2(x).$$

Consider now the nonempty set $N$ of permutations $\pi_i$ on the set of states $S$ of $M$ such that for some $w$ in $I^*$

$$h_1[\delta(s, w)] = h_1(s) + C(w),$$

for all $s$, and where $C(w)$ depends only on $w$. Clearly, $N$ is a commutative subgroup of $G(M)$ and every element of $N$, except 1, has order $p$. Let $y^{-1}$ denote the inverse of the permutation defined by the input $y$ in $I$. Then

$$h_1[\delta(s, y^{-1})] = A^{-1}h_1(s) - A^{-1}Bh_2(y)$$

and for any $w$ in $I^*$ which yields a permutation in $N$, we see that

$$h_1[\delta(s, ywy^{-1})] = h_1(s) + C(ywy^{-1}).$$

Thus for any $y$ in $I$ and $w$ in $N$, $ywy^{-1}$ is again in $N$ and therefore $N$ is a normal subgroup of $G(M)$. Furthermore, we see that the permutation induced by an input $y$ in $I$ and the permutations in $N$ generate the group $G(M)$.

These observations were first made by Ecker [6] who furthermore showed that if a finite group $G$ has the previously derived properties of $G(M)$, then there always exists a linearly realizable automaton $M'$ which generates $G$.

THEOREM E. *If a permutation automaton $M$ is linearly realizable over $GF(p)$ then $G = G(M)$ satisfies the following properties*:

(a) *$G$ has a normal, abelian subgroup $N$ in which every element, except* 1, *has order $p$,*

(b) *there exists an element $c$ in $G$ such that $N$ and $c$ generate $G$.*

*Furthermore, for any finite group $G$ which satisfies the two properties there exists a linearly realizable permutation automaton $M$ with group $G$.*

*Proof.* The proof of the first part of the theorem was outlined before the statement of this theorem. For the second part of the proof see [6].

Though the above result characterizes the groups of linear automata it turns out that it does not characterize linear automata. There exist automata which generate groups satisfying the two conditions of Theorem E but which cannot be linearly

| | A | B |
|---|---|---|
| 1 | a | b |
| a | c | e |
| b | f | 1 |
| c | d | g |
| d | 1 | f |
| e | b | a |
| f | g | d |
| g | e | c |

FIG. 1. Finite automaton $M$.

| | 1 | a | b | c | d | e | f | g |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | a | b | c | d | e | f | g |
| a | a | c | e | d | 1 | g | b | f |
| b | b | f | 1 | g | e | d | a | c |
| c | c | d | g | 1 | a | f | e | b |
| d | d | 1 | f | a | c | b | g | e |
| e | e | b | a | f | g | 1 | c | d |
| f | f | g | d | e | b | c | 1 | a |
| g | g | e | c | b | f | a | d | 1 |

FIG. 2. The group $G(M)$.

realized. To illustrate this situation and to motivate the following result we consider an example. The finite automaton $M$ whose transition function is given in Fig. 1, generates the group $G(M)$ which is given in Fig. 2. Note that $A = a$ and $B = b$. The lattice of subgroups of $G(M)$ is shown in Fig. 3, where the large circles denote the normal subgroups of $G(M)$. It is seen that the group $G(M)$ satisfies the two conditions of Theorem E for $GF(2)$. Just note that the elements 1, $c$, $e$, $f$ form a normal subgroup $N_1$ of $G$ which is commutative and for which $x$ in $N_1$ implies that $x^2 = 1$. Furthermore, $N_1$ and $g$ generate $G(M)$. It should be observed that the subgroup $N_2$ consisting of 1, $b$, $c$, $g$ with the element $f$ also satisfy the conditions of Theorem E.

The binary coding which yields the linear realization of $M$ over $GF(2)$ can be obtained by inspection or by known algorithms. For detailed discussion of tests for linear realizability, see [2].

Next we consider the three homomorphic images of $M$ shown in Fig. 4. The automaton $M_1$ is defined by the subgroup consisting of 1, $b$ of $G$ and the states of $M_1$ are the cosets

$$1 = \{1, b\}, \qquad 2 = \{c, g\}, \qquad 3 = \{d, e\}, \qquad 4 = \{a, f\}.$$

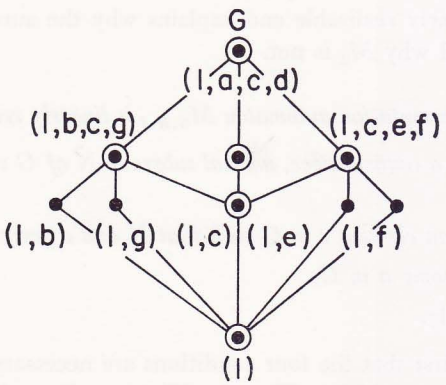


FIG. 3. Lattice of subgroups of $G(M)$.

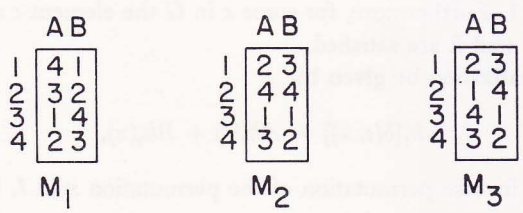


FIG. 4. Finite automata $M_1$, $M_2$, and $M_3$.

Similarly, $M_2$ is defined by the subgroup $\{1, f\}$ and $M_3$ is defined by the subgroup $\{1, c\}$. Since, the subgroups consisting of 1, $b$ and 1, $f$ contain only the normal subgroup consisting of 1, we know that

$$G(M_1) = G(M_2) = G(M)$$

and that

$$M_1 = M_{G,\{1,b\},\{a,b\}} \qquad \text{and} \qquad M_2 = M_{G,\{1,f\},\{a,b\}}.$$

The automaton $M_3$ does not generate $G$ but generates only the group $G/\{1, c\}$ since the elements 1 and $c$ form a normal subgroup of $G$.

Furthermore, by inspection it can be seen that $M_1$ and $M_3$ are again linearly realizable. And on the other hand, $M_2$ is not linearly realizable since

$$\delta(1, A) \neq \delta(1, B) \qquad \text{and} \qquad \delta(2, A) = \delta(2, B),$$

which, one can easily see [2, 3] is not possible for a linearly realizable automaton. Thus in $M_2$ we have an example of a permutation automaton which generates a group satisfying the conditions of Theorem E but which is not linearly realizable.

Our next result gives necessary and sufficient conditions for a permutation automaton to be linearly realizable and explains why the automata $M_1$ and $M_3$ are linearly realizable and why $M_2$ is not.

THEOREM L. *A permutation automaton $M_{G,H,I}$ is linearly realizable over $GF(p)$ iff:*

(1) *There exists a commutative, normal subgroup $N$ of $G$ such that $n$ in $N$ implies that $n^p = 1$,*

(2) *there exists an element $c$ in $G$ such that $N$ and $c$ generate $G$,*

(3) *$I \subseteq Na$ for some $a$ in $G$,*

(4) *$H \cap N = \{1\}$.*

*Proof.* We show first that the four conditions are necessary. Assume that $M_{G,H,I}$ is linearly realizable over $GF(p)$. Then by Theorem E we know that there exists a normal, commutative subgroup $N$ which is used in this realization and that $n$ in $N$ implies that $n^p = 1$. Furthermore, for some $c$ in $G$ the element $c$ and $N$ generate $G$. Thus conditions 1 and 2 are satisfied.

Let the linear realization be given by

$$h_1[\delta(s, x)] = Ah_1(s) + Bh_2(x),$$

and let $x^{-1}$ be the inverse permutation of the permutation $x$ in $I$, that is,

$$h_1[\delta(s, x^{-1})] = A^{-1}h_1(s) - A^{-1}Bh_2(x).$$

Then for all $y$ in $I$

$$h_1[\delta(s, yx^{-1})] = A^{-1}[Ah_1(s) + Bh_2(y)] - A^{-1}Bh_2(x)$$
$$= h_1(s) + A^{-1}Bh_2(y) - A^{-1}Bh_2(x)$$

and therefore

$$yx^{-1} \in N \quad \text{and} \quad y \in Nx.$$

But then $I \subseteq Nx$ and we see that the third condition is satisfied for $x = a$. To derive the last condition let $r$ be in $N \cap H$ and let $w_r$ in $I^*$ be a word which induces the permutation $r$ on $S = \{H, Ha, ...\}$ of $M$. Since $r$ is in $H$, we know that

$$\delta(H, w_r) = Hr = H,$$

and since $r$ is $N$ we know that

$$h_1[\delta(H, w_r)] = h_1(H) + C(w_r).$$

But then

$$C(w_r) = 0$$

and we conclude that for all $s$, $\delta(s, w_r) = s$.

Since $M$ generates $G$ on the cosets of $H$ we conclude that $w_r$ is the identity permutation and thus $r = 1$. Therefore,

$$N \cap H = \{1\},$$

as was to be shown.

Next we show why any finite automaton $M_{G,H,I}$ satisfying the four conditions of the theorem is linearly realizable over $GF(p)$.

A close inspection of Ecker's proof [6] reveals that the proof holds for any faithful, transitive representation of $G$ as a permutation group on a set $S$, provided the orbits of the permutations in $N$, except 1, have length $p$. Once this condition is established the same construction can be carried out to obtain a linear realization of the automaton, provided $I \subseteq Na$. (Ecker's original construction was carried out for $M_{G,\{1\},Na}$.) To show that the orbits of the permutations in $N$ have length $p$, consider

$$n \text{ in } N, \quad n \neq 1 \quad \text{and} \quad a \text{ in } G.$$

We assert that the left cosets

$$Ha, Han, Han^2, ..., Han^{p-1}$$

are all different and thus the orbits have length $p$. Otherwise for some $k$, $1 \leqslant k \leqslant p - 1$,

$$Ha = Han^k,$$

which implies that

$$Ha = Hma,$$

for some $m$ in $N$, $m \neq 1$, since $N$ is a normal subgroup of $G$. But then

$$H = Hm$$

and we are forced to conclude that $m$ in $H \cap N$ and therefore $m = 1$ because $H \cap N = \{1\}$. Thus the $p$ cosets above are all distinct and we can carry out the original Ecker construction of the linear assignment for $M_{G,H,I}$. This completes the proof.

The above result asserts that as long as $H$, the subgroup of $G$ whose left cosets are the states of $M$, does not overlap $N$, the normal abelian subgroup used for coding the states of $M$, then $M$ can be linearly realized. Our results in the next section will show that as long as $H \cap N$ is a normal subgroup of $G$ we get again a linearly realizable machine which is a homomorphic image of $M_{G,\{1\},I}$. Thus the only way to destroy linearity of a linearly realizable $M_{G,\{1\},I}$ is by choosing an $H$ which intersects $N$ in a subgroup which is not normal in $G$.

COROLLARY L. *A permutation automaton $M_{G,H,I}$ is linearly realizable over $GF(p)$ iff:*

(1) *There exists a commutative, normal subgroup $N$ of $G$ such that $n$ in $N$ implies that $n^p = 1$,*

(2) *$I \subseteq Na$ for some $a$ in $G$,*

(3) *$H \cap N = \{1\}$.*

*Proof.* Note that in Theorem L conditions (1) and (3) imply condition (2).

The finite automata of Fig. 4 illustrate the above result. We know that $M_1 = M_{G,H_1,I}$ with $H_1 = \{1, b\}$ and $I = \{a, b\}$. Since we can choose $N = \{1, c, e, f\}$ we see that $I \subseteq Nb$ and that

$$H_1 \cap N = \{1\}.$$

Since $G$ satisfies the first two conditions of our theorem for $GF(2)$ we see that $M_1$ is linearly realizable over $GF(2)$. On the other hand, $M_2 = M_{G,H_2,I}$, with $H_2 = \{1, f\}$, and since $I \subseteq Na$ but $N \cap H_2 = H_2 \neq \{1\}$, we see why $M_2$ is not linearly realizable over $GF(2)$.

It is interesting to note that if we are allowed to replace the inputs of $M_2$ by other input words which generate the same permutations on the set of states of $M_2$, then we can select these input words so that $M_2$ is linearly realizable. To achieve this note that the permutations $a$, $e$ of $G$ generate $G$; furthermore, considered as permutations,

$$A = a, \qquad AB = e, \qquad \text{and} \qquad B = ea.$$

If we now consider

$$M_4 = M_{G,H_2,\{a,e\}},$$

then we see that

$$N_2 = \{1, b, c, g\}$$

is a normal subgroup of $G$ satisfying the first two conditions of Theorem L for $GF(2)$, and

$$I \subseteq N_2 e \qquad \text{and} \qquad N_2 \cap H_2 = \{1\}.$$

Thus we know that $M_4$ is linearly realizable over $GF(2)$. Clearly this was only possible because we had two different normal subgroups $N_1$ and $N_2$ in $G(M)$ which could be utilized for a linear realization. Nevertheless, the above theorem shows how inputs of an automaton $M$ can be recoded into input words to achieve linear realizability if the conditions 1, 2 and 4 of Theorem L are satisfied for $M$.

The next example shows that even for a fixed set of inputs of an automaton $M$ the normal subgroup $N$ used in a linear realization of $M$ does not have to be unique. Consider the abelian group $G$ of order 12 which is obtained by taking a direct product of two cyclic groups of order two and one cyclic group of order three. We represent $G$ as the additive group over the set of elements

$$\{(x, y, z) \mid x, y \in \{0, 1\}, z \in \{0, 1, 2\}\}.$$

Let

$$M = M_{G,H,I}$$

with $H = \{(0, 0, 0)\}$ and $I = \{(0, 1, 1), (1, 1, 1)\}$. Then we see that the (normal) subgroups

$$N_1 = \{(0, 0, 0), (1, 0, 0)\}$$

and

$$N_2 = \{(0, 0, 0), (1, 0, 0), (0, 1, 0), (1, 1, 0)\}$$

of $G$ satisfy the first two conditions of Theorem L. Since

$$H \cap N_1 = H \cap N_2 = \{(0, 0, 0)\}$$

and

$$I \subseteq N_1 + (0, 1, 1) \qquad \text{and} \qquad I \subseteq N_2 + (0, 1, 1),$$

we see that $M_{G,H,I}$ satisfies the last two conditions with $N_1$ and $N_2$. Thus we see that $M_{G,H,I}$ is linearly realizable by means of two different normal subgroups $N_1$ and $N_2$ of $G$.

Observe that if an automaton $M_{G,H,I}$ is linearly realizable over $GF(p)$, using the normal subgroup $N$, then the input set $I$ can have atmost $|N|$ elements. Thus the size of $N$ determines the maximal number of inputs which can be linearly realized

using $N$. For any given automaton $M_{G,H,I}$ which can be linearly realized over $GF(p)$ we will refer to the maximal number of inputs (containing the set $I$) which can be simultaneously linearly realized over $GF(p)$ as the *width of the linear realization of* $M_{G,H,I}$ *over* $GF(p)$.

Our next result shows that any automaton with linear width of 2 over $GF(p)$ must be a commutative automaton (i.e., $G(M)$ is abelian group). We note that if the linear width is 2 then the realization must be over $GF(2)$.

COROLLARY. *If $M$ is linearly realizable over $GF(2)$ with linear width 2, then $M$ is a commutative automaton and $G(M)$ is isomorphic to the direct product of two cyclic groups.*

*Proof.* Since the linear width of $M_{G,H,I}$ is 2 we know that the linear realization of $M_{G,H,I}$ uses a normal subgroup $N$ consisting of two elements, $|N| = 2$. But then by Theorem E or L there exists a cyclic subgroup $\langle c \rangle$ generated by $c$ in $G$, such that $N$ and $\langle c \rangle$ generate $G$. Therefore $\langle c \rangle$ can have atmost two distinct left cosets in $G$ and we conclude that $\langle c \rangle$ is a normal subgroup of $G$. Thus either

$$N \subseteq \langle c \rangle \quad \text{or} \quad N \cap \langle c \rangle = \{1\}.$$

In the first case, $G = M(G) = \langle c \rangle$ which is clearly a commutative group; in the second case, since $N$ and $\langle c \rangle$ are normal subgroups of $G$ and $N$ and $\langle c \rangle$ generate $G$ we know that

$$G \cong G/N \times G/\langle c \rangle.$$

Thus $G$ is a commutative group, as was to be shown.

It can be shown that there exist automata which are linearly realizable over $GF(3)$ with linear width 3 but which are not abelian.

## IV. Homomorphisms of Linearly Realizable Automata

The previous theorem can be used to characterize all homomorphisms of a linear automata which yield linearly realizable image automata.

THEOREM M. *Let $M_{G,\{1\},Na}$ be linearly realizable over $GF(p)$ using the normal subgroup $N$. Then every homomorphic image of $M_{G,\{1\},Na}$ is determined by a subgroup $H$ of $G$ and the image automaton*

$$M_{G,H,Na}$$

*is linearly realizable over $GF(p)$ if and only if*

$$N \cap H$$

*is a normal subgroup of $G$.*

*(Note that the subgroup $H$ may contain nontrivial normal subgroups of $G$ and therefore the homomorphic image of $M_{G,\{1\},Na}$ defined by $H$ may not generate the group $G$ but a homomorphic image of $G$. To avoid unnecessary complications in notation we will occasionally write*

$$M_{G,H,Na}$$

*with the understanding that $G(M_{G,H,Na})$ is the group induced by $G$ on the left cosets of $H$. If we denote the largest normal subgroup of $G$ in $H$ by $N(H)$, then clearly $G(M_{G,H,Na}) \cong G/N(H)$.)*

*Proof.* First we show that the condition is sufficient.

Let $H$ define the homomorphism of $M_{G,\{1\},Na}$ and let $N \cap H = N_1$, where $N_1$ is a normal subgroup of $G$. Then the image automaton is given by

$$M' = M_{G',H',N'a'},$$

where

$$G' \cong G/N(H),$$

and $H'$ and $N'a'$ are the corresponding images of $H$ and $Na$, respectively. Since $N_1 \subseteq N(H)$, we have that

$$N' \cap H' = \{1\},$$

and therefore, we can easily see, that the four conditions of Theorem L hold for $M'$. Thus $M'$ is again linearly realizable over $GF(p)$.

Next we show that the condition is necessary. We will show that if $L = N \cap H$ is not a normal subgroup of $G$, then $M_{G,H,Na}$ is not linearly realizable. If $L$ is not a normal subgroup of $G$ then

$$N \cap N(H) \subset L,$$

and therefore there exist two elements $r$ and $t$ in $L$ which induce different permutations on the left cosets of $H$. Let $w_r$ and $w_t$ in $I^* = (Na)^*$ induce the permutations $r$ and $t$, respectively. Then for $M_{G,H,Na}$

$$\delta(H', w_r') = H'r' = H' = H't' = \delta(H', w_t'),$$

since $r$ and $t$ are in $H$. But then we know that $M_{G,H,Na}$ is not linearly realizable, since, in a linear realization,

$$\delta(H', w_r') = \delta(H', w_t')$$

implies that

$$\delta(H'x', w_r') = \delta(H'x', w_t')$$

for all $x'$ in $G'$; a contradiction. Thus, $H \cap N$ must be a normal subgroup of $G$, as was to be shown.

From the above result we see that the only way a homomorphism defined by $H$ can destroy the linear realizability of the automaton $M_{G,\{1\},Na}$, is if $H$ overlaps $N$ in a subgroup which as not normal in $G$. Since this cannot happen in an abelian group we get our next result.

COROLLARY. *If $M = M_{G,\{1\},I}$ is linearly realizable over $GF(p)$ and if the inputs of $M$ commute, then any homomorphic image of $M$ is again linearly realizable over $GF(p)$.*

*Proof.* Obvious consequence of Theorem M or L.

From the above theorem we can also derive some previously known results about homomorphism of linear machines which were obtained by different methods [3].

We say that an automaton $M$ is *uniformly connected* iff from every state $s$ of $S$ we can reach any pair of states, $p$, $q$ in $S$, with the same number of inputs.

The next result shows that for linearly realizable automata uniform connectedness is equivalent to the existance of an input which maps some state on to itself.

LEMMA. *Let $M = M_{G,H,Na}$, where $N$ is a normal subgroup of $G$. Then $M$ is uniformly connected iff there exists an input $x$ in $Na$ and an $s$ in $S$ such that $\delta(s, x) = s$.*

*Proof.* Since $M$ is strongly connected the existance of an $x$ and $s$ such that $\delta(s, x) = s$ implies that $M$ is uniformly connected.

On the other hand, if $M$ is uniformly connected, then for some integer $k$ and $m_1$ and $m_2$ in $N$

$$\delta(Ha, m_1a^k) = \delta(H, m_2a^k)$$

or

$$Ham_1a^k = Hm_2a^k$$

or

$$Hna = H, \qquad \text{for some } n \text{ in } N.$$

But then $na$ is in $H$ and we see that

$$\delta(H, na) = H$$

with $x = na$ in $I = Na$. This completes the proof.

From this lemma we see that in the following results the condition of uniform connectedness can be replaced by the existance of an input $x$ in $Na$ which maps some state onto itself.

COROLLARY. *If $M = M_{G,\{1\},Na}$ is a linearly realizable automaton over $GF(p)$, then any uniformly connected homomorphic image $M'$ of $M$ is again linearly realizable over $GF(p)$.*

*Proof.* Without loss of generality we can assume that the homomorphic image $M'$ of $M$ is given by

$$M_{G,K,Na},$$

where $K$ is a subgroup of $G$ such that $N(K) = \{1\}$. Otherwise we can first take the homomorphism of $M$ defined by the normal subgroup $N(K)$ of $G$ and obtain $M''$, which by Theorem M is linearly realizable, and on which the homomorphism yielding $M'$ has the desired property, namely,

$$N(K/N(K)) = \{1\}.$$

We will show that the condition that $M' = M_{H,K,Na}$ is uniformly connected implies that

$$N \cap K = L$$

is a normal subgroup of $G$ and therefore $L = \{1\}$. But then by Theorem M we know that

$$M' = M_{G,K,Na}$$

is linearly realizable over $GF(p)$.

Recall that $M'$ is uniformly connected and that we can view the left cosets of $K$ as states of $M'$. Therefore, for some $s$ there exist $w_1$ and $w_2$ in $I^s = (Na)^s$ such that

$$\delta(K, w_1) = K \quad \text{and} \quad \delta(Ka, w_2) = K.$$

But then

$$Kw_1 = Kaw_2,$$

and we conclude that for some $n_1$ and $n_2$ in $N$

$$Ka^s n_1 = Ka^{s+1} n_2 .$$

Thus for some $n_3$ in $N$,

$$Kn_3 = Ka$$

and therefore

$$a = kn$$

for some $k$ in $K$ and $n$ in $N$. Thus any element $t$ of $G$ can be written for some integer $s$ as

$$t = k^s m, \qquad m \in N.$$

Since

$$L = N \cap K,$$

we have

$$kL = Lk,$$

and therefore

$$tL = k^s mL = k^s Lm = Lk^s m = Lt,$$

which shows that $L$ is a normal subgroup of $G$. Thus by assumption $L = \{1\}$ and therefore by Theorem M we know that $M'$ is linearly realizable over $GF(p)$, as was to be shown.

The previous proof showed that if $M_{G,H,Na}$, where $N$ is a normal subgroup of $G$, is uniformly connected, then $G \cap H$ is a normal subgroup of $G$. This observation yields a new proof of a known result [3].

COROLLARY. *The homomorphic images of a uniformly connected, linearly realizable automaton over $GF(p)$ are again linearly realizable over $GF(p)$.*

*Proof.* If $M_{G,H,Na}$ is linearly realizable and uniformly connected then, because of the previous observation, any homomorphism must be defined by a subgroup $K$, $H \subseteq K$, such that $N \cap K$ is a normal subgroup of $G$. But by Theorem M such homomorphism define linearly realizable machines.

From these results we can also easily read off the following known result [3].

COROLLARY. *Any uniformly connected automaton which can be linearly realized over $GF(p)$ has $p^s$ states for some integer $s$.*

## V. Structure of Linear Permutation Automata

In this section we derive from our previous results several theorems about the structure of linear automata. Since input-free parts (or clocks) of automata play an important role in these results, we derive first an auxiliary result about clocks in automata.

An automaton $M_1 = (S_1, I_1, \delta_1)$ is *input-free* iff $|I_1| = 1$.

An automaton $M = (S, I, \delta)$ has a *nontrivial* clock iff either $|I| = 1$ or $M$ is isomorphic to a subautomaton of a serial connection of an input-free automaton $M_1$ to an automaton $M_2$, each of which has fewer states than $M$, that is,

$$|S_1| < |S| \quad \text{and} \quad |S_2| < |S|.$$

When we consider permutation automata, then, in the above definition, we only have to require that $M$ is isomorphic to the serial connection of $M_1$ and $M_2$.

For a detailed discussion of clocks in automata, see [4].

Lemma. *Let $M = M_{G,\{1\},I}$ and let $M_{G,K,I}$ be input-free. Then $I \subseteq Ka$ for some $a$ in $G$ and $K$ is a normal subgroup of $G$.*

*Proof.* Assume that $M_{G,K,I}$ is input-free. Then for all $a$ and $a_i$ in $I$ we must have that

$$Ka = Ka_i,$$

but then for some $k_i$ in $K$

$$a = k_i a_i$$

and we see that $I \subseteq Ka$.

To show that $K$ is a normal subgroup of $G$, it suffices to show that for any $k$ in $K$ there exists a $k'$ in $K$ such that

$$k'a = ak,$$

since then for all $g$ in $G$ it follows that

$$gK = Kg,$$

because $I \subseteq Ka$ generates $G$. Let $k$ be in $K$ and let $w = k$ for $w$ in $I^*$. Then

$$Kwa = Kaw,$$

since $M_{G,K,I}$ is input-free and $wa$, $aw$ are both in $I^s$ for some $s$. But then, for some $k_2$ in $K$,

$$k_2wa = aw,$$

which implies that, for some $k'$ in $K$,

$$k'a = ak.$$

Thus $K$ is a normal subgroup of $G$, as was to be shown.

THEOREM. *The automaton $M = M_{G,\{1\},I}$, with $|I| > 1$, has a nontrivial clock iff $G = G(M)$ has a nontrivial normal subgroup $K$ such that $I \subseteq Ka$ for some $a$ in $G$.*

*Proof.* If there exists a nontrivial, normal subgroup $K$ of $G$ such that $I \subseteq Ka$, then we know that $K$ defines an input-free homomorphic image $M' = M_{G',\{1'\},\{a'\}}$ of $M$, where $G' \cong G/K$ and $a'$ is the image of $a$. But then it follows from the general decomposition theory of automata [4] that $M$ is isomorphic to the serial connection of $M_1 = M'$ and $M_2$, with $|S_1|, |S_2| < |S|$. Since $M_1$ is input-free we have the desired decomposition. Conversely, if $M = M_{G,\{1\},I}$ has a nontrivial clock then it can be decomposed into input-free automaton $M_1$ connected to $M_2$. By the general decomposition theory of automata this implies that $M_1$ is a homomorphic image of $M$. Since all homomorphic images of $M$ are defined by subgroups of $G$ we know that there exists a subgroup $K$ of $G$ such that $M_{G,K,I}$ is input-free. But then we know from the preceding lemma that $I \subseteq Ka$ and that $K$ is a normal subgroup of $G$. This completes the proof.

From these results and the characterization of linear automata we obtain a structural result.

THEOREM. *Let $M = M_{G,\{1\},Na}$ be linearly realizable over $GF(p)$. Then $M$ is isomorphic to the serial connection of an $|G/N|$-state input-free automaton $M_1$ to an $|N|$-state automaton $M_2$. Furthermore,*

$$G(M_1) \cong G/N,$$

*and $M_2$ can be so chosen that*

$$G(M_2) \cong N.$$

*Proof.* This result follows from the preceding results and the general decomposition theory of finite automata; see [4]. Clearly, the last automaton $M_2$ can be further decomposed into a parallel connection of automata whose groups are the cyclic group of order $p$.

THEOREM. *Let* $M = M_{G,\{1\},Na}$ *be linearly realizable over* $GF(p)$. *Then* $M$ *is isomorphic to the serial connection of an* $|\, G/N \,|$*-state input-free automaton* $M_1$ *and an* $|\, N \,|$*-state uniformly connected automaton* $M_2$. *If* $p^2$ *does not divide the order of the element* $a$ (*i.e.*, $p^2 \nmid |\langle a \rangle|$) *then* $M$ *is isomorphic to a parallel connection of* $M_1$ *and* $M_2$.

*Proof.* The first part of the theorem follows from the general decomposition theory of finite automata.

If $p$ does not divide the order of the element $a$ then

$$N \cap \langle a \rangle = \{1\},$$

since the cyclic group $\langle a \rangle$ must intersect $N$ in a cyclic group whose order is not $p$. But then, since $N$ and $\langle a \rangle$ generate $G$, $N$ and $\langle a \rangle$, define two homomorphisms on $M$ which yield a parallel decomposition of $M$ into the component machines

$$M_1 = M_{G/N,\{1\},a'}$$

and

$$M_2 = M_{G,\langle a \rangle,I}.$$

A similar proof shows that if $p^2$ does not divide $|\langle a \rangle|$ then we can pick a subgroup $\langle b \rangle$ of $\langle a \rangle$, whose order is not divisible by $p$ and such that $N$ and $b$ generate $G$, and repeat the argument for $\langle b \rangle$. This completes the proof.

It should be noted that in the last result the homomorphism defined by the subgroup $\langle a \rangle$, which may not be a normal subgroup of $G$, can yield an image automaton which again generates the group $G$. Nevertheless, this is a decomposition of $M$ into smaller component machines and a separation of the input independent part of $M$ from the uniformly connected part.

It should also be noted that, even if

$$N \cap \langle a \rangle = \{1\}$$

and we know that $M$ can be decomposed in the serial connection of $M_1$ to $M_2$ with

$$G(M_1) \cong G/N \qquad \text{and} \qquad G(M_2) \cong N,$$

then, in the parallel connection guaranteed by the last theorem, $M_2$ cannot necessarily be chosen such that

$$G(M_2) \cong N.$$

If this were possible then $M$ would necessarily be a commutative automaton which does not always have to be the case.

## VI. Conclusion

In this paper we utilized Ecker's results to give a complete characterization of all permutation automata which can be linearly realized over $GF(p)$ in terms of the group generated by the automaton. We showed how these results can be used to characterize all linearity preserving homomorphisms of linear permutation automata and read off from these results several older results about homomorphisms of linear automata. We are convinced that these methods have further applications in the study of linear automata as well as for other types of automata.

It would now be very interesting to see whether a similar characterization cannot be given in terms of the semigroup of an automaton of *all* linearly realizable automata over $GF(p)$. This appears to be a very difficult problem but its solution is very likely to give deeper insights into automata theory.

The above results can be extended to linear realizations over finite rings using the methods of [5].

## Acknowledgment

The first author woult like to express his gratitude to Dr. B. Reusch for his help and to acknowledge his influence in the writing of this paper. Thanks are also due to the Gesellschaft für Mathematik und Datenverarbeitung for its support and for providing a stimulating research environment in which this work cold be done.

## References

1. A. Gill, "Linear Sequential Circuits," McGraw–Hill, New York, 1966.
2. B. Reusch, "Lineare Automaten," BI Hochschulskripten 708, Bibliographisches Institut, Mannheim, 1969.
3. J. Hartmanis and W. A. Davis, Homomorphic images of linear sequential machines, *J. Comp. System Sci.* 1 (1967), 155–165.
4. J. Hartmanis and R. E. Stearns, "Algebraic Structure Theory of Sequential Machines," Prentice–Hall, Englewood Cliffs, NJ, 1966.
5. H. K.-G. Walter, "Synchronous Simulations of Sequential Machines," Bericht des Mathematischen Instituts und des Instituts für Angewandte Mathematik, Universität des Saarlandes, A 71/09, Saarbrücken, Dezember 1971.
6. K. H. Ecker, On the semigroup of a linear nonsingular automaton, *Math. Systems Theory,* to appear.
7. M. Hall, "The Theory of Groups," Macimillan, New York, 1959.

Printed by the St Catherine Press Ltd., Tempelhof 37, Bruges, Belgium.