JOURNAL OF COMPUTER AND SYSTEM SCIENCES 19, 18–26 (1979)

Automorphisms of Linear Automata

CARLTON J. MAXSON AND KIRBY C. SMITH

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

Received April 17, 1977; revised February 16, 1979

Relationships between the group, Aut(M), of automorphisms of a linear automaton M and the structure of M are determined. Linear automata in which Aut(M) is a group of translations are characterized in terms of the structure of the state space of M. Also, conditions are determined as to when Aut(M) contains only linear transformations.

I. INTRODUCTION

In this paper we continue our investigation of the relationships between the structural properties of linear automata and the morphism of these automata. In particular, we consider here relationships between the structure of the state space of a linear automaton, M, and the structure of the group of automorphisms of M. For references to previous investigations of morphisms of automata we refer the reader to the references in [6].

In this paper we deal exclusively with linear automata. To fix our notation, recall that an automaton $M \equiv \langle V, \Sigma, \delta \rangle$ with state set V, input set Σ and transition function δ: $V \times \Sigma \to V$ is linear if there is a finite field F such that $V = F^n$, $\Sigma = F^m$, and matrices A and B over F such that $\delta(v, \sigma) = Av + B\sigma$, $v \in V$, $\sigma \in \Sigma$. We denote a linear automaton M by the 5-tuple $M \equiv \langle V, \Sigma, A, B, F \rangle$ when we wish to call attention to the matrices A and B and the field F. For such a linear automaton M it is well-known that the subspace W_0 of V generated by $\{A^jB\sigma \mid \sigma \in \Sigma, j = 0, 1, 2, \ldots\}$ is the strongly connected component of the zero state ([2]).

An endomorphism of a linear automaton $M = \langle V, \Sigma, A, B, F \rangle$ is a function f: $V \to V$ such that $f(Av + B\sigma) = Af(v) + B\sigma$, $(v, \sigma) \in V \times \Sigma$. Under function composition the set End(M) of endomorphisms of M is a semigroup with identity I, where I: $V \to V$ is the identity map. As in [6] we have found it useful to consider the set $T_0 = \{f: V \to V \mid f(Av + B\sigma) = Af(v), (v, \sigma) \in V \times \Sigma\}$ in investigating End (M). The relationship between T_0 and End (M) is that $f \in T_0$ if and only if $I + f \in$ End (M). We note that any linear function commuting with A and having W_0 in its null space belongs to T_0.

The invertible elements of End(M) form a group, Aut(M), of automorphisms of M, and the set $T(M) = \{f: V \to V \mid f(v) = v + a$ where $Aa = a\}$ is a subgroup of Aut(M). We say that Aut(M) is *trivial* if Aut(M) = $T(M)$ and we call the elements in $T(M)$ *translations*. In [6] it was shown that End(M) = $T(M)$ if and only if $V = W_0$. Consequently if $V = W_0$, Aut(M) is trivial, but the converse is not true as will be shown in the sequel.

0022-0000/79/040018–09$02.00/0

II. Linear Automata with Trivial Automorphism Group

In this section we present a characterization of linear automata with trivialautomorphism group. Since $\mathrm{End}(M) = T(M)$ if M is strongly connected ([6]), we make the can following convention.

Convention. For the remainder of the paper, $V \neq W_0$.

As a first step toward our characterization we consider linear automata over fields with more than two elements. We first state a lemma whose proof is trivial.

Lemma 1. *Let M be a linear automaton and L a linear transformation in T_0. Then $I + L \in \mathrm{Aut}(M)$ if and only if -1 is not an eigenvalue of L.*

Theorem 1. *If M is a linear automaton over a field $F \neq Z_2$ and M is not strongly connected, then $\mathrm{Aut}(M)$ contains a non-identity linear transformation.*

Proof. Let S_0 be the set of linear transformations in T_0. Since $W_0 \neq V$, we know from [6] that $S_0 \neq \{0\}$. Under the operations of function addition and composition, S_0 forms a ring. If S_0 is a nilpotent ring then for each $L \in S_0$, $I + L$ is invertible. Hence $\mathrm{Aut}(M)$ contains a non-identity linear transformation. If S_0 is not nilpotent, then it contains an idempotent $E \neq 0$ [3, page 22]. Since $E^2 = E$, the only possible eigenvalues of E are 0 and 1. If $\mathrm{char}\, F \neq 2$ then by the lemma, $I + E \in \mathrm{Aut}(M)$. If $\mathrm{char}\, F = 2$, then since $F \neq Z_2$, there exists $\alpha \in F$, $\alpha \notin \{0, 1\}$. Then αE in T_0 has 0 and α as its only possible eigenvalues. Again by the lemma, $I + \alpha E \in \mathrm{Aut}(M)$.

We now assume $F = Z_2$ for the remainder of this section.

Let C be a nonzero element in S_0 and let $m_C(x)$ denote the minimal polynomial for C, that is,

$$m_C(x) = x^{n_1}(x + 1)^{n_2} p_3(x)^{n_3} \cdots p_k(x)^{n_k},$$

a product of irreducibles. From the primary decomposition theorem [4, page 180]

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$$

where $V_1 = \mathrm{Ker}\, C^{n_1}$, $V_2 = \mathrm{Ker}(C + I)^{n_3}$,..., $V_k = \mathrm{Ker}\, p_k(C)^{n_k}$.

Suppose $m_C(x)$ has an irreducible factor $p_3(x) \neq x$, $x + 1$. Then define $\tilde{C}$: $V \to V$ as follows:

$$\tilde{C}(v_3) = C(v_3),\ v_3 \in V_3,$$

$$\tilde{C}(v_i) = 0,\ v_i \in V_i,\ i \neq 3,$$

and extend $\tilde{C}$ linearly to all of V. Since each V_i is an A-invariant subspace, $\tilde{C} \in S_0$. But $m_{\tilde{C}}(x) = x p_3(x)^{n_3}$, so $\tilde{C}$ does not have $-1 = 1$ as an eigenvalue, which means $I + \tilde{C}$ is a non-identity linear transformation in $\mathrm{Aut}(M)$.

Using a similar argument we may now assume that every C in S_0 has a minimal polynomial of the form $m_C(x) = x^{n_1}(x + 1)^{n_2}$, $n_1, n_2 \in \{0, 1\}$. Hence S_0 is a ring consisting

entirely of idempotents, i.e., S_0 is a Boolean ring. It is well known that every finite Boolean ring has an identity element, so let $E \neq 0$ be the identity for S_0. We have

$$V = V_1 \oplus V_2$$

where $E(V_1) = \{0\}$, $E(v_2) = v_2$ for each $v_2 \in V_2$, and V_1, V_2 are A-invariant subspaces with $W_0 \subseteq V_1$.

Let $A_2 : V_2 \to V_2$ be A restricted to V_2. From the above we must have $m_{A_2}(x) = x(x+1)$ or x or $x+1$.

Every element of S_0 annihilates V_1. This implies that $W_0 = V_1$, for otherwise there exists, as in [6], a linear transformation $\tilde{C}: V_1 \to V_1$ such that $\tilde{C}$ commutes with $A_1 = A \mid V_1$ and $\tilde{C}(W_0) = \{0\}$. Extending $\tilde{C}$ to V by $\tilde{C}(v_2) = v_2$, $v_2 \in V_2$, gives an element in S_0 for which $\tilde{C}(V_1) \neq \{0\}$. This is a contradiction.

We thus have the following three situations:

$$\text{(i)} \quad V = W_0 \oplus V_2, \qquad m_{A_2}(x) = x(x+1);$$

$$\text{(ii)} \quad V = W_0 \oplus V_2, \qquad m_{A_2}(x) = x;$$

$$\text{(iii)} \quad V = W_0 \oplus V_2, \qquad m_{A_2}(x) = x+1.$$

Consider the first situation, $V = W_0 \oplus V_3 \oplus V_4$ where $Av_3 = 0$, $v_3 \in V_3$, $Av_4 = v_4$, $v_4 \in V_4$.

Suppose $\dim V_3 > 1$. Let C be a linear transformation on V_3 such that 1 is not an eigenvalue of C. Extend C to V by $C(\alpha w + \beta v_3 + \gamma v_4) = C(\beta v_3)$, $w \in W_0$, $v_3 \in V_3$, $v_4 \in V_4$. Since $CA = AC$ and $C(W_0) = \{0\}$, then $C \in S_0$. Moreover 1 is not an eigenvalue of C. Hence $I + C \in \mathrm{Aut}(M)$.

In a similar manner if $\dim V_4 > 1$, $\mathrm{Aut}(M)$ contains a nontrivial linear transformation.

Assume then that $\dim V_3 = 1$, $\dim V_4 = 1$, say $V_3 = \{0, v_3\}$ and $V_4 = \{0, v_4\}$. Suppose $\mathrm{Ker}\, A \cap W_0 \neq \{0\}$, say $k \in \mathrm{Ker}\, A - \{0, v_3\}$. Define $C: V \to V$ by $C(v_3) = k$, $C(w) = 0$, $w \in W_0$, $C(v_4) = 0$ and extend linearly to V. Then $C \in S_0$ and $I + C$ is in $\mathrm{Aut}(M)$. Further if $\underline{X} \cap W_0 \neq \{0\}$, where $\underline{X}$ is the eigenspace of 1 for A, then let $0 \neq w_0 \in \underline{X} \cap W_0$ and define $C: V \to V$ by $C(v_4) = w_0$, $C(w) = 0$, $w \in W_0$, $C(v_3) = 0$ and extend linearly to V. Again $C \in S_0$ and $I + C \in \mathrm{Aut}(M)$.

Summarizing the above, we find that in the first situation if $\mathrm{Aut}(M)$ contains no nontrivial linear transformations then $\dim V_3 = 1$, $\dim V_4 = 1$, $\mathrm{Ker}\, A \cap W_0 = \{0\}$ and $\underline{X} \cap W_0 = \{0\}$.

The second and third situations are similar. For (ii), if $\mathrm{Aut}(M)$ contains no nontrivial linear transformations then $V = W_0 \oplus V_2$, $V_2 = \{0, v_2\}$, $Av_2 = \{0\}$ and $\mathrm{Ker}\, A = V_2$. For (iii), if $\mathrm{Aut}(M)$ contains no nontrivial linear transformations then $V = W_0 \oplus V_2$, $V_2 = \{0, v_2\}$, $Av_2 = v_2$, $\underline{X} = V_2$.

This establishes the necessity of the conditions in the following theorem.

THEOREM 2. *Let $M = \langle V, \Sigma, A, B, Z_2 \rangle$ be a linear automaton with $W_0 \neq V$. Then* $\mathrm{Aut}(M)$ *consists entirely of translations if and only if one of the following occurs*:

(i) $V = W_0 \oplus V_3 \oplus V_4$, $V_3 = \{0, v_3\}$, $V_4 = \{0, v_4\}$ Ker $A = V_3$, $\underline{X} = V_4$

(ii) $V = W_0 \oplus V_2$, $V_2 = \{0, v_2\}$, Ker $A = V_2$

(iii) $V = W_0 \oplus V_2$, $V_2 = \{0, v_2\}$, $\underline{X} = V_2$,

where $\underline{X}$ *is the eigenspace of* 1 *for* A.

Proof. It remains to show that in the situations described the only automorphisms are translations. This is computational and omitted.

In the second case of the above theorem we note that $\mathrm{Aut}(M) = \{I\}$ if 1 is not an eigenvalue of A. Combining this with a remark in [6] we obtain the following characterization of linear automata in which the identity is the only automorphism.

COROLLARY 1. *Let* $M = \langle V, \Sigma, A, B, F\rangle$ *be a linear automaton,* 1 *not an eigenvalue of* A. *Then* $\mathrm{Aut}(M) = \{I\}$ *if and only if* M *is strongly connected or* $F = Z_2$, $V = W_0 \oplus \mathrm{Ker}\ A$, $\mathrm{Ker}\ A = \{0, v_1\}$.

Also from the above discussion we have the following.

COROLLARY 2. *Let* $M = \langle V, \Sigma, A, B, F\rangle$ *be a linear automaton. Then* $\mathrm{Aut}(M)$ *contains a non-identity linear transformation if and only if* $\mathrm{Aut}(M)$ *does not consist of translations.*

III. Linear Transformations in Aut(M)

In this section we determine conditions under which $\mathrm{Aut}(M)$ contains only linear transformations. Throughout we assume $W_0 \neq V$ for the linear automaton $M = \langle V, \Sigma, A, B, F\rangle$. If 1 is an eigenvalue of A then $\mathrm{Aut}(M)$ contains nonidentity translations, so we may also assume that 1 is not an eigenvalue of A.

Recall from [6] that a vector $v \in V$ is said to have W_0-order n if n is the least nonnegative integer such that $A^n v \in W_0$. If no such integer exists, v has W_0-order ∞. Thus if $v \in W_0$, v has W_0-order 0. From this we have

$$V = W_0 \cup S \cup I,$$

a disjoint union where $S = \{v \mid v \text{ has finite nonzero } W_0\text{-order}\}$ and $I = \{v \mid v \text{ has infinite } W_0\text{-order}\}$. Further, $W_0 \cup S$ is an A-invariant subspace of V which we denote by W_1.

For $v \in I$, consider $v, Av, A^2v, \ldots, A^jv, \ldots$. Let $l > 0$ be minimal such that $A^l v = A^k v + w$ for some k, $0 \leqslant k < l$, and some $w \in W_1 = W_0 \cup S$. We claim $k = 0$. For we have $A^k(A^{l-k} - I)v \in W_1$ and this implies $(A^{l-k} - I)v \in W_1$, contradicting the minimality of l unless $k = 0$.

For $v \in I$ we define the *block* of I determined by v to be the set $\mathscr{C} = \bigcup_{i=0}^{l-1} (A^i v + W_1)$ where l is minimal such that $(A^l - I)v \in W_1$. We note that $I = \mathscr{C}_1 \cup \mathscr{C}_2 \cup \cdots \cup \mathscr{C}_m$, a disjoint union of blocks. Moreover, any element of $\mathscr{C}_i$ generates $\mathscr{C}_i$, that is, if $v_i \in \mathscr{C}_i$ then $\mathscr{C}_i = \bigcup_{j=0}^{l_i-1} (A^j v_i + W_1)$. Of course if $S = \varnothing$, then each block is a connected component of M.

As a first step in our characterization of those linear automata having only linear automorphisms we show that if in the decomposition $V = W_1 \cup I$, I has more than one block then Aut(M) contains nonlinear functions. In this step there are several instances in which functions must be verified to be automorphisms. Since these functions arise in a similar manner, we present their definition in the following rather technical lemma, whose proof is omitted.

LEMMA 2. *Let $V = W_1 \cup \mathscr{C}_1 \cup \cdots \cup \mathscr{C}_m$, where $\mathscr{C}_i$ is a block, $m \geqslant 1$, and v_i is a generator of $\mathscr{C}_i$, $i = 1, 2,..., m$. Let j be arbitrary but fixed, $1 \leqslant j \leqslant m$, and define a function f: $V \to V$ as follows:*

$$f(v) = v, \qquad v \notin \mathscr{C}_j ;$$

$$f(v_j) = \tilde{v}_j \qquad \text{where} \quad \tilde{v}_j \in \mathscr{C}_j \qquad \text{with} \quad (A^{l_j} - I)\,\tilde{v}_j = (A^{l_j} - I)\,v_j ;$$

and

$$f(A^k v_j + w) = A^k \tilde{v}_j + w,\ w \in W_1,\ k = 0, 1,..., (l_j - 1).$$

Then

$$f \in \text{Aut}(M).$$

We call an automorphism of the above type *normal*. We note that such an automorphism is completely determined as soon as the value $\tilde{v}_j = f(v_j)$ is known. Thus, in order to define nonidentity normal automorphisms we need to find for some $\mathscr{C}_j$, elements $v_j \neq \tilde{v}_j$ in $\mathscr{C}_j$ such that $(A^{l_j} - I)\tilde{v}_j = (A^{l_j} - I)v_j$. We now show this is true for every block $\mathscr{C}_i$ in the decomposition of I.

LEMMA 3. *If $I = \mathscr{C}_1 \cup \cdots \cup \mathscr{C}_m$, $m \geqslant 1$ then for each $v \in \mathscr{C}_i$, $i = 1, 2,..., m$ there exists $\tilde{v} \in \mathscr{C}_i$, $\tilde{v} \neq v$, such that $(A^{l_i} - I)\tilde{v} = (A^{l_i} - I)v$.*

Proof. We first observe that $|\mathscr{C}_i| > |W_1|$ for each i. Otherwise, if $|\mathscr{C}_i| = |W_1|$ then $l_i = 1$ which in turn implies that $(x - 1)$ divides the minimal polynomial of A contradicting the fact that 1 is not an eigenvalue of A.

Now, since $(A^{l_i} - I)v_i \in W_1$, $(A^{l_i} - I)\mathscr{C}_i \subseteq W_1$. Hence, reselecting v_i if necessary we find $\tilde{v}_i \in \mathscr{C}_i$ such that $(A^{l_i} - I)\tilde{v}_i = (A^{l_i} - I)v_i$. Since $\mathscr{C}_i = \bigcup_{j=0}^{l_i - 1} (A^j v_i + W_1)$ it is easily seen that *for every* $v \in \mathscr{C}_i$ there is a $\tilde{v} \neq v$ in $\mathscr{C}_i$ such that $(A^{l_i} - I)\tilde{v} = (A^{l_i} - I)v$. Since this is true for each i, the lemma follows.

THEOREM 3. *Let $M = \langle V, \Sigma, A, B, F\rangle$ be a linear automaton such that $V = W_1 \cup \mathscr{C}_1 \cup \cdots \mathscr{C}_m$. If $m > 1$,* Aut(M) *contains a nonlinear map.*

Proof. The result is established by constructing nonlinear normal automorphisms.

Suppose, for some i, we have v_i, $v_i' \in \mathscr{C}_i$ with $v_i + v_i' = v_j$ where $v_j \in \mathscr{C}_j$, $j \neq i$. We define f: $V \to V$ as follows: $f(v) = v$, if $v \notin \mathscr{C}_j$; and for $v_j = v_i + v_i' \in \mathscr{C}_j$, $f(v_j) = \tilde{v}_j$ where $\tilde{v}_j$ is as given in Lemma3. Thus we obtain a normal automorphism f. But, f is not linear since $f(v_i + v_i') \neq f(v_i) + f(v_i')$.

The alternative to the above is that $W_1 \cup \mathscr{C}_i$ is a subgroup of $(V, +)$ for every i. Consider $V_1 = W_1 \cup \mathscr{C}_1 \cup \mathscr{C}_2$. But then V_1 cannot be a group since otherwise

$$V_1 = (W_1 \cup \mathscr{C}_1) \cup (W_1 \cup \mathscr{C}_2),$$

a union of two proper subgroups, which is impossible. Thus there exist vectors $v_1 \in \mathscr{C}_1$, $v_2 \in \mathscr{C}_2$ such that $v_1 + v_2 \in \mathscr{C}_j$, $j \notin \{1, 2\}$. Define the normal automorphism f as follows:

$$f(x) = x \text{ if } x \neq \mathscr{C}_j$$

$$f(v_j) = \tilde{v}_j \text{ where } v_j = v_1 + v_2 .$$

Then f is not linear since $f(v_1 + v_2) \neq f(v_1) + f(v_2)$.

We turn now to the situation in which there is at most one block in I. Of course if $S = \varnothing$ there must be such a block since $V \neq W_0$. Our next step is to investigate this case.

THEOREM 4. *Let $M = \langle V, \Sigma, A, B, F\rangle$ be a linear automaton such that $V = W_0 \cup \mathscr{C}_1$. Then* Aut($M$) *contains a nonlinear automorphism if and only if* End(M) *contains a nonlinear endomorphism.*

Proof. Suppose every automorphism is linear. Then as in [6], a generator v_1 can be chosen for $\mathscr{C}_1$ with the property that $A^m v_1 = v_1$ for some integer $m > 1$. Moreover since v_1 has this invertibility property, for any f in End(M), $f(A^s v_1 + w) = A^s f(v_1) + w$, $w \in W_0$.

If for $f \in \text{End}(M)$, $f(v_1) \in \mathscr{C}_1$, say $f(v_1) = A^i v_1 + w_1$, then f is onto. For $f(w) = w$, $w \in W_0$ and if $A^s v_1 + \bar{w} \in \mathscr{C}_1$ then

$$f(A^{s-i} v_1 + \bar{w} - A^{s-i} w_1) = A^{s-i} f(v_1) + \bar{w} - A^{s-i} w_1 = A^s v_1 + \bar{w}.$$

Hence $f \in \text{Aut}(M)$ and consequently f is linear. (Note that if, in the above, $s < i$ then $A^s v_i + \bar{w} = A^{s+km} v_1 + \bar{w}$ for all integers k, $k \geqslant 0$. Hence we may assume $s > i$.)

It remains to consider those $f \in \text{End}(M)$ with $f(v_1) = w_1 \in W_0$. If $g \in \text{End}(M)$ is linear then $g + f - I = (g - I + f - I) + I \in \text{End}(M)$ and $(g + f - I)v_1 = g(v_1) + f(v_1) - v_1 = g(v_1) + w_1 - v_1$. If $g(v_1) \neq v_1 + w$ for some $w \in W_0$ then $(g + f - I)v_1 \in \mathscr{C}_1$ which means $g + f - I$ is an automorphism and therefore linear. Hence f is linear.

So we may assume every automorphism of M has the property $f(v_1) = v_1 + w$ for some $w \in W_0$.

Let $p(x) \in F[x]$ be minimal such that $p(A)v_1 \in W_0$. We have from [6],

$$f \in \text{End}(M) \text{ if and only if } (A^{l_1} - I) f(v_1) = (A^{l_1} - I)v_1$$

and

$$f \text{ is linear if and only if } p(A) f(v_1) = p(A)v_1 .$$

Since every $f \in \mathrm{End}(M)$ with the property that $f(v_1) = v_1 + w$ is an automorphism and hence linear, then

$$(A^{l_1} - I) f(v_1) = (A^{l_1} - I)v_1$$
$$(A^{l_1} - I)(v_1 + w) = (A^{l_1} - I)v_1$$
$$(A^{l_1} - I)w = 0$$

and

$$p(A) f(v_1) = p(A)v_1$$
$$p(A)w = 0.$$

The above steps are reversible so

$$(A^{l_1} - I)w = 0 \text{ if and only if } p(A)w = 0.$$

Hence in W_0 we have $\mathrm{Ker}(A^{l_1} - I) = \mathrm{Ker}\, p(A)$. Now assume $f \in \mathrm{End}(M)$ is not an automorphism. Then $f(v_1) \in W_0$. This means

$$(A^{l_1} - I) f(v_1) = (A^{l_1} - I)v_1 = \hat{w} \in W_0 .$$

Hence the number of $f \in \mathrm{End}(M)$ which are not automorphisms equals the number of w's in W_0 which are solutions to

$$(A^{l_1} - I)w = \hat{w}.$$

This number is precisely equal to $|\, \mathrm{Ker}(A^{l_1} - I) \cap W_0 \,|$. Likewise the number of $f \in \mathrm{End}(M)$ which are linear but not automorphism equals the number of w's in W_0 which are solutions to

$$p(A)w = p(A)v_1 \in W_0 .$$

This number is $|\, \mathrm{Ker}\, p(A) \cap W_0 \,|$. Since $|\, \mathrm{Ker}\, p(A) \cap W_0 \,| = |\, \mathrm{Ker}(A^{l_1} - I) \cap W_0 \,|$, every nonautomorphism of $\mathrm{End}(M)$ is linear.

Since the reverse implication is obvious the proof is complete.

Suppose now $S \neq \varnothing$. By an exhaustion of cases, it can be shown that if $\mathrm{Aut}(M)$ consists solely of linear transformations then either

(*) $|\, V \,| \leqslant 4$ and V is exemplified by one of the following situations

(i) $V = Z_2 \times Z_2$, $\quad \Sigma = Z_2$, $\quad A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\quad B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\quad F = Z_2$;

(ii) $V = Z_2 \times Z_2$, $\quad \Sigma = Z_2$, $\quad A = (0)$, $\quad B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\quad F = Z_2$;

(iii) $V = Z_2 \times Z_2$, $\Sigma = Z_2$, $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $B = (0)$, $F = Z_2$;

(iv) $V = Z_2 \times Z_2$, $\Sigma = Z_2$, $A = (0)$, $B = (0)$, $F = Z_2$;

(v) $V = Z_3$, $\Sigma = Z_3$, $A = (0)$, $B = (0)$, $F = Z_3$;

(vi) $V = Z_2$, $\Sigma = Z_2$, $A = (0)$, $B = (0)$, $F = Z_2$;

or

(**) $V = W_0 \cup (k + W_0) \cup \mathscr{C}_1$, Ker $A = \{0, k\}$.

For the first case, it is straightforward to verify that the automorphisms of the linear automata described in (i)–(vi) are linear.

For the second case we first note that for every automorphism f of M we must have $f(w_1) = w_1$ for all $w_1 \in W_1$. In fact, we know $f(w_0) = w_0$, $w_0 \in W_0$. Now $A(f(k + \bar{w})) = f(A\bar{w}) = A\bar{w}$ which in turn implies that $f(k + \bar{w}) - \bar{w} \in \text{Ker } A$. But since $f \in \text{Aut}(M)$, $f(k + \bar{w}) \neq f(\bar{w})$. Thus $f(k + \bar{w}) = \bar{w} + k$ for each $\bar{w} \in W_0$. But this shows that $f(w_1) = w_1$ for each $w_1 \in W_1$. Hence an automorphism f is completely determined by its action on a single element, say v_1, of $\mathscr{C}_1$. We know $f(v_1) \in \mathscr{C}_1$ and $(A^{l_1} - I)f(v_1) = (A^{l_1} - I)v_1$. Further, f is linear if and only if $p(A)f(v_1) = p(A)v_1$ where $p(x)$ is minimal such that $p(A)v_1 \in W_1$. If

$$K_1 = \{y \in \mathscr{C}_1 \mid (A^{l_1} - I)y = (A^{l_1} - I)v_1\}$$

and

$$K_2 = \{y \in \mathscr{C}_1 \mid p(A)y = p(A)v_1\}$$

then every automorphism of M is linear if and only if $K_1 = K_2$.

THEOREM 5. *Let $M = \langle V, \Sigma, A, B, F \rangle$ be a linear automaton such that 1 is not an eigenvalue of A. Let $V = W_0 \cup S \cup I$ where $S \neq \varnothing$.*

(*) *If $V \neq W_0 \cup (k + W_0) \cup \mathscr{C}_1$, Ker $A = \{0, k\}$ then* Aut(M) *consists solely of linear transformations if and only if M is one of the automata described in* (i)–(vi).

(**) *If $V = W_0 \cup (k + W_0) \cup \mathscr{C}_1$, Ker $A = \{0, k\}$, then* Aut(M) *consists solely of linear transformations if and only if $K_1 = K_2$, where K_1 and K_2 are as above.*

This concludes our study of linear automata M such that Aut(M) contains only linear transformations. We found in Theorem 3 that if V has two or more blocks then Aut(M) contains nonlinear functions. If V has exactly one block and no elements of finite nonzero order then Theorem 4 says Aut(M) contains only linear transformations if and only if the same is true for End(M). Finally in Theorem 5 the remaining situation in which Aut(M) contains only linear transformations is classified.

REFERENCES

1. G. FEICHTINGER, Some results on the relation between automata and their automorphism groups, *Computing* 1 (1966), 327–340.
2. M. HARRISON, "Lectures on Linear Sequential Machines," Academic Press, New York, 1969.
3. I. HERSTEIN, "Noncommutative Rings," Carus Monograph No. 15, Math. Assoc. Amer., Washington, D. C., 1968.
4. K. HOFFMAN AND R. KUNZE, "Linear Algebra," Prentice–Hall, Englewood Cliffs, N. J., 1961.
5. N. JACOBSON, "Lectures in Abstract Algebra," Vol. II, Van Nostrand, New York, 1953.
6. C. MAXSON AND K. SMITH, Endomorphisms of linear automata, *J. Comput. System Sci.* **17** (1978), 98–107.