Mathematica Pannonica
4/1 (1993), 79 – 93

ENDOMORPHISMS OF GROUP AUTOMATA

S. C. Geller

Department of Mathematics, Texas A & M University, Collage Station, Texas 77843-3368

P. Natarajan

Department of Mathematics, Texas A & M University, Collage Station, Texas 77843-3368

K. C. Smith

Department of Mathematics, Texas A & M University, Collage Station, Texas 77843-3368

Received September 1991

AMS Subject Classification: 68 Q 68, 16 Y 30

Keywords: Automaton, endomorphism.

Abstract: Relationships between the structure of a group automaton M and its semigroup of endomorphisms $\mathrm{End}\,M$ are found. It is shown that $\mathrm{End}\,M$ is trivial precisely when M is strongly connected. Moreover if $\mathrm{End}\,M$ consists solely of linear maps then M has at most two components. Conditions are found as to when $\mathrm{End}\,M$ contains only linear maps.

1. Introduction

In [3] Maxson and Smith studied the endomorphism semigroup of a linear automaton. They showed that the endomorphisms of a linear automaton give information about the connectivity, or lack of connectivity, in the automaton. The methods used in [3] relied heavily

on the vector space structure of a linear automaton. It is the goal of this paper to obtain similar results for a group automaton. Since every linear automaton is a group automaton we will generalize the results in [3]. The arguments used are new, relying on the theory of finite groups. We will obtain connectivity results analogous to the linear case. It will soon be clear that our work essentially involves the study of certain maps on a finite group G which commute with a given endomorphism A of G.

The reader is referred to the references in [3] concerning the background of endomorphisms of automata as well as basic information on automata theory.

2. Preliminaries

Let $M \equiv \langle Q, \Sigma, F\rangle$ be a finite automaton with states Q, inputs Σ and transition function F: $Q \times \Sigma \to Q$. The automaton M is called a *group automaton* if Q and Σ are (finite) groups (written additively but not necessarily abelian) and F is a homomorphism from the group $Q \times \Sigma$ into Q. Throughout this paper $M = \langle Q, \Sigma, F\rangle$ will denote a group automaton with state group Q, input group Σ and state-transition homomorphism F.

The homomorphism F: $Q \times \Sigma \to Q$ gives rise to two other homomorphisms as follows. Define A: $Q \to Q$ by $Aq = F(q, 0)$ and B: $\Sigma \to Q$ by $B\sigma = F(0, \sigma)$. We have $F(q, \sigma) = F((q, 0) + (0, \sigma)) = F(q, 0) + F(0, \sigma) = Aq + B\sigma$. Moreover, since $(q, 0) + (0, \sigma) = (0, \sigma) + (q, 0)$ in $Q \times \Sigma$, we have $F(q, 0) + F(0, \sigma) = F(0, \sigma) + F(q, 0)$ in Q, or equivalently $Aq + B\sigma = B\sigma + Aq$. This proves the following lemma.

Lemma 1. *If $M = \langle Q, \Sigma, F\rangle$ is a group automaton with $F(q, \sigma) = Aq + B\sigma$ then every element in the range of A commutes with every element in the range of B. In particular if A is an automorphism of Q then W, the range of B, is a subgroup of the center of Q and therefore a normal subgroup of Q.*

In our investigation of the endomorphisms of the group automaton M we will make use of group theory results which we now review. Let G be a finite group and let A: $G \to G$ be an endomorphism of G. For each positive integer i, A^i is an endomorphism of G and we have a descending chain

$$G > A(G) > A^2(G) > \cdots > A^i(G) > \cdots$$

of subgroups of G. Since G is finite, there exists an integer $k > 0$ such that $A^k(G) = A^{k+1}(G) = \cdots$, which implies $\ker A^k = \ker A^{k+1} = \cdots$. Let $H = A^k(G)$ and $K = \ker A^k$. Then $H \cap K = \{0\}$, for if $x \in H \cap K$ then $A^k x = 0$, but A^k is one-to-one on H, so $x = 0$.

We show now that G is the sum of H and K. If $x \in G$ then there exists a $y \in H$ such that $A^k x = A^{2k} y$. We have $x = A^k y + (-A^k y + x)$ where $A^k y \in H$, and $-A^k y + x$ belongs to K since $A^k(-A^k y + x) = -A^{2k} y + A^k x = 0$. So $G = H + K$. Therefore G is a semidirect product of H and K since K is normal in G. This proves a version of Fitting's Lemma (see [2], page 84).

Lemma 2. *If G is a finite group and A: $G \to G$ is an endomorphism, then every $x \in G$ has the unique form $x = x_1 + x_0$ where, for some $k > 0$, $A^k x_1 = x_1$ and $A^k x_0 = 0$.*

Referring to Lemma 2, we will call an element $x_1 \in G$ such that $A^k x_1 = x_1$ for some $k > 0$ an *invertible element.* If $x_2 \in G$ such that $A^k x_2 = 0$ for some $k > 0$, then x_2 is a *nilpotent element.* From Lemma 2 every element in G is (uniquely) the sum of an invertible and a nilpotent element.

In $M = \langle Q, \Sigma, F \rangle$ we extend Σ to the free monoid Σ^* over Σ consisting of all finite sequences of elements of Σ (inputs), including the empty sequence $\emptyset$. If $w \in \Sigma^*$ then $w = \sigma_0 \sigma_1 \ldots \sigma_{n-1}$ where $\sigma_i \in \Sigma$ and one defines, for $q \in Q$,

$$\begin{aligned} F(q, w) &= F(q, \sigma_0 \sigma_1 \ldots \sigma_{n-1}) = F(F(q, \sigma_0), \sigma_1 \ldots \sigma_{n-1}) = \\ &= F(F(F(q, \sigma_0), \sigma_1), \sigma_2 \ldots \sigma_{n-1}) = \cdots \\ &= F(F(\ldots F(F(q, \sigma_0), \sigma_1), \sigma_2), \ldots, \sigma_{n-2}), \sigma_{n-1}). \end{aligned}$$

In terms of A, B we have

$$F(q, w) = A^n q + A^{n-1} B \sigma_0 + A^{n-2} B \sigma_1 + \cdots + AB\sigma_{n-2} + B\sigma_{n-1}.$$

If $w = \emptyset$, the empty sequence, then we define $F(q, \emptyset) = q$.

In a group automaton $M = \langle Q, \Sigma, F \rangle$ we define, for $q \in Q$, the *reach* of q to be $\operatorname{reach}(q) = \{q' \in Q \mid F(q, w) = q' \text{ for some } w \in \Sigma^*\}$. So $\operatorname{reach}(q) = \{A^n q + A^{n-1} B \sigma_0 + \cdots + AB\sigma_{n-2} + B\sigma_{n-1} \mid n \text{ is a nonnegative integer and each } \sigma_i \in \Sigma\}$. Finally the component of q in Q is defined to be $\operatorname{comp}(q) = \{q' \in \operatorname{reach}(q) \mid \text{there exists a } w' \in \Sigma^* \text{ with } F(q', w') = q\}$.

Lemma 3. *In a group automaton,* $\operatorname{comp}(0) = \operatorname{reach}(0)$

Proof. Clearly $\mathrm{comp}(0) \subseteq \mathrm{reach}(0)$. Let $x \in \mathrm{reach}(0)$. Then there exists a positive integer k and elements $\sigma_0, \sigma_1, \ldots, \sigma_k$ in Σ such that $x = A^k B\sigma_0 + \cdots + AB\sigma_{k-1} + B\sigma_k$.

Suppose x is invertible. Then there exists a positive integer s such that $x = A^s x = A^{2s} x = \cdots$; so we may assume $s > k$. Let $w = 0 \ldots 0(-\sigma_0)(-\sigma_1)\ldots(-\sigma_k)$ ($s-k-1$ zeros). Then (using Lemma 1 repeatedly)

$$\begin{aligned} F(x,w) &= F(A^{s-k-1}x, (-\sigma_0)(-\sigma_1)\ldots(-\sigma_k)) = \\ &= A^s x - A^k B\sigma_0 - \cdots - AB\sigma_{k-1} - B\sigma_k = \\ &= A^s x - (B\sigma_k + AB\sigma_{k-1} + \cdots + A^k B\sigma_0) = \\ &= A^s x - (A^k B\sigma_0 + \cdots + AB\sigma_{k-1} + B\sigma_k) = x - x = 0. \end{aligned}$$

So $x \in \mathrm{comp}(0)$.

Suppose x is nilpotent with $A^s x = 0$. Then let $w = 0 \ldots 0$ (s zeros) and we have $F(x,w) = A^s x = 0$. So $x \in \mathrm{comp}(0)$.

For x arbitrary we have $x = x_1 + x_0$ where x_1 is invertible and x_0 is nilpotent. So if $A^t x_0 = 0$ and $A^s x_1 = x_1$, then $A^s A^t x = A^t x$. Let $w = 0 \ldots 0$ ($s-k-1$ zeros) and $\widetilde{w} = 0 \ldots 0$ (t zeros). Then $F(x, w(-\sigma_0)\ldots(-\sigma_k)\widetilde{w}) = A^{s+t}x - A^t x = 0$ as above. Thus x belongs to $\mathrm{comp}(0)$. ◊

Lemma 4. *In a group automaton $M = \langle Q, \Sigma, F\rangle$, $\mathrm{comp}(0)$ is a subgroup of Q. If A is invertible then $\mathrm{comp}(0)$ is a normal subgroup of Q contained in the center of Q.*

Proof. From Lemma 3 $\mathrm{comp}(0) = \{A^n B\sigma_0 + \cdots + AB\sigma_{n-1} + B\sigma_n \mid n$ is a nonnegative integer and $\sigma_i \in \Sigma\}$. Repeated use of Lemma 1 shows $\mathrm{comp}(0)$ is closed under addition. The normality of $\mathrm{comp}(0)$ when A is invertible follows from Lemma 1 and the fact that every element in Q has the form Ax, so each $A^i B\sigma_{n-i}$ belongs to the center of Q. ◊

3. Endomorphisms of group automata

An *endomorphism* of a group automaton $M = \langle Q, \Sigma, F\rangle$ is a function $g\colon Q \to Q$ such that $g(F(q,\sigma)) = F(g(q),\sigma)$ for all $q \in Q, \sigma \in \Sigma$. In terms of the linear maps $A\colon Q \to Q$ and $B\colon \Sigma \to Q$ for M we have that g is an endomorphism of M if $g(Aq + B\sigma) = Ag(q) + B\sigma$ for all $q \in Q, \sigma \in \Sigma$. We let $\mathrm{End}\, M$ denote the set of endomorphisms of M.

For $g \in \mathrm{End}\, M$ we can write $g = 1 + (-1 + g)$ where $1\colon Q \to Q$ is the identity map. The function $-1 + g$ has the property that

$$(-1+g)(Aq+B\sigma) = -(Aq+B\sigma) + g(Aq+B\sigma) =$$
$$= -B\sigma - Aq + Ag(q) + B\sigma = -Aq + Ag(q) =$$
$$= A(-1+g)(q).$$

So if $g \in \operatorname{End} M$ then the function $-1+g$ belongs to the set

$$T \equiv \{f: Q \to Q \mid f(Aq+B\sigma) = Af(q), q \in Q, \sigma \in \Sigma\}.$$

Conversely it is easy to verify that if $f \in T$ then $1+f$ is in $\operatorname{End} M$.

Lemma 5. $\operatorname{End} M = 1+T$.

In creating endomorphisms of a group automaton M we will find it convenient to create elements of T and then use Lemma 5. The properties of functions in T are listed in the following result.

Lemma 6. *If $f: Q \to Q$ belongs to T then*

(i) $fA = Af$;
(ii) $f(0)$ *is a fixed point of* A, *that is* $Af(0) = f(0)$;
(iii) $f(x) = f(0)$ *for all* x *in* $\operatorname{comp}(0)$;
(iv) *If* A *is invertible then* f *is constant on each left coset of* $\operatorname{comp}(0)$ *in* Q.

Proof. Parts (i) – (iii) are easily proved. For (iv) we note that Q finite and A an automorphism mean $A^k = 1$, the identity map, for some positive integer k. If $x, y \in Q$ such that $-x+y \in \operatorname{comp}(0)$, then there exist elements $\sigma_0, \sigma_1, \ldots, \sigma_t \in \Sigma$ such that

$$y = x + A^t B\sigma_0 + \cdots + AB\sigma_{t-1} + B\sigma_t.$$

There exists an $s > t$ such that $x = A^s x$ so

$$y = A^s x + A^t B\sigma_0 + \cdots + AB\sigma_{t-1} + B\sigma_t$$

and repeated use of the fact that $f \in T$ gives $f(y) = A^s f(x) = f(A^s x) = f(x)$. ◊

An automaton $M = \langle Q, \Sigma, F\rangle$ is called *strongly connected* if $\operatorname{comp}(0) = Q$. Our next result says that if M is strongly connected then its endomorphisms are, in a sense, trivial, i.e. translation maps using fixed points of A.

Theorem 1. *If* $M = \langle Q, \Sigma, F\rangle$ *is strongly connected then* $\operatorname{End} M = \{g: Q \to Q \mid g(x) = x + a$ *where* $a \in Q$ *such that* $Aa = a\}$.

This follows directly from Lemmas 5 and 6 (iii). ◊

We now begin to show that the converse of Th. 1 is also true, that is, if $M = \langle Q, \Sigma, F\rangle$ is not strongly connected then $\operatorname{End} M$ contains functions which are not translation maps. We split our investigation up into two cases: A invertible and A not invertible. In the invertible case we will need a group theory result, found in [1], page 334. Recall

that an automorphism A of a group G is fixed point free if $Ax = x$ only when $x = 0$.

Lemma 7. *Let G be a finite group and let $A: G \to G$ be a fixed point free automorphism of G. Then every element in G can be uniquely expressed in the form $-x + Ax$ for a suitable x in G.*

Proof. Suppose $x, y \in G$ with $-x + Ax = -y + Ay$. Then $y - x = A(y - x)$. Since A is fixed point free then $y - x = 0$ or $y = x$. This shows that the map $h: G \to G$ defined by $h(x) = -x + Ax$ is one-to-one. Since G is finite, h is onto. $\Diamond$

Corollary 1. *Let G be a finite group and let $A: G \to G$ be a fixed point free automorphism. If W is an A-invariant subgroup of G, then $-x + Ax$ belongs to W if and only if x belongs to W.*

Proof. Since W is A-invariant, $x \in W$ implies $-x + Ax \in W$. Suppose now that x belongs to G with $-x + Ax$ in W. Since W is A-invariant, A is fixed point free on W, and so by Lemma 7 there is a $w \in W$ such that $-x + Ax = -w + Aw$. But A is fixed point free on G, so $w = x$ and $x \in W$.

Corollary 2. *Let $A: G \to G$ be an automorphism of G and let W be an A-invariant subgroup of G. If x belongs to G such that x does not belong to W and if $-x + A^k x$ belongs to W for some positive integer k, then A^k is not fixed point free on G.*

We are assuming that A is invertible and $M = \langle Q, \Sigma, F \rangle$ is not strongly connected. If $H = \text{comp}(0)$, then $H \neq Q$. Select $x \in Q \backslash H$ (so $x \in Q$ but $x \notin H$). We show now that the relation "$y \in \text{reach}(x)$" is symmetric and transitive if A is invertible.

Suppose $y \in \text{reach}(x)$. Then y has the form $y = A^r x + A^{r-1} B\sigma_0 + \cdots + AB\sigma_{r-2} + B\sigma_{r-1}$ where each $\sigma_j \in \Sigma$. Solving for $A^r x$ gives $A^r x = y + A^{r-1} B(-\sigma_0) + \cdots + AB(-\sigma_{r-2}) + B(-\sigma_{r-1})$, using Lemma 1. Since A is invertible there exists a positive integer $t \geq r$ such that $A^{t-r} = 1$, so $x = A^{t-r} A^r x = A^{t-r} y + A^{t-1} B(-\sigma_0) + \cdots + AB(-\sigma_{r-2}) + B(-\sigma_{r-1})$ and $x \in \text{reach}(y)$.

If $y \in \text{reach}(x)$ and $z \in \text{reach}(y)$ then $y = A^r x + A^{r-1} B\sigma_0 + \cdots + AB\sigma_{r-2} + B\sigma_{r-1}$ and $z = A^s y + A^{s-1} B\tau_0 + \cdots + AB\tau_{s-2} + B\tau_{s-1}$ where each $\sigma_i \in \Sigma$ and each $\tau_j \in \Sigma$. This means $A^s y = A^{s+r} x + A^{s+r-1} B\sigma_0 + \cdots + A^{s+1} B\sigma_{r-2} + A^s B\sigma_{r-1}$ and so

$$z = A^{s+r} x + A^{s+r-1} B\sigma_0 + \cdots + A^{s+1} B\sigma_{r-2} + A^s B\sigma_{r-1} + A^{s-1} B\tau_0 + \cdots + AB\tau_{s-2} + B\tau_{s-1}$$

and $z \in \text{reach}(x)$.

The following lemma describes $\operatorname{comp}(x)$.

Lemma 8. *Let A be invertible and $M = \langle Q, \Sigma, F\rangle$ be not strongly connected. If $x \in Q\backslash \operatorname{comp}(0)$ then* $\operatorname{comp}(x) = \operatorname{reach}(x) = \bigcup_{i=0}^{k-1} A^i x +$ $+\operatorname{comp}(0)$ *where k is minimal such that $-x+A^k x$ belongs to* $\operatorname{comp}(0)$.

Proof. Since Q is finite and A is an automorphism of Q there exists a positive integer s such that $A^s = 1$, the identity map on Q. Let $H = \operatorname{comp}(0)$, a normal subgroup of Q by Lemma 4. For $x \in Q\backslash H$ we have $\operatorname{comp}(x) \subseteq \operatorname{reach}(x) = \{A^r x + A^{r-1}B\sigma_0 + \cdots + AB\sigma_{r-2} + +B\sigma_{r-1} \mid r$ is a positive integer and each $\sigma_i \in \Sigma\} = \bigcup_{i=0}^{s-1} A^i x + H = \bigcup_{i=0}^{k-1} A^i x + H$, where k is minimal such that $-x+A^k x \in H$. Conversely if $y \in \bigcup_{i=0}^{k-1} A^i x + H$ then

$$y = A^t x + A^j B\sigma_0 + \cdots + AB\sigma_{j-1} + B\sigma_j$$

where each $\sigma_i \in \Sigma$. Since $A^s = 1$, we can change t if necessary so that $t > j$. We now have $y = A^t x + \sum_{i=0}^{t-1} A^i B\sigma_{t-1-i}$ where some of the σ_i's may be 0. Hence $y = F(x, w)$ where $w = \sigma_0\sigma_1 \ldots \sigma_{t-1}$ and $y \in \operatorname{comp}(x)$. $\Diamond$

Proposition 1. *If A is invertible then the group automaton $M = \langle Q, \Sigma, F\rangle$ is strongly connected iff* $\operatorname{End} M$ *is trivial.*

Proof. It suffices to show that, if M is not strongly connected, then $\operatorname{End} M$ is not trivial. Select $x \in Q\backslash H$ where $H = \operatorname{comp}(0)$ and let $k > 0$ be minimal such that $-x + A^k x \in H$. Since H is A-invariant, by Cor. 2 A^k is not fixed point free on Q. So there exists a $y \neq 0$ in Q such that $A^k y = y$. Define $f: Q \to Q$ as follows:

(i) if $z \in \operatorname{comp}(x)$, whence $z = A^i x + h$ where $h \in H$, let $f(z) = f(A^i x + h) = A^i y$,

(ii) if $z \notin \operatorname{comp}(x)$, let $f(z) = 0$.

We need to show f is well-defined. Assume $z = A^i x + h = A^j x + h'$ where $h' \in H$ and $j \geq i$. Then $-A^i x + A^j x = h - h' = A^i(-x + A^{j-i}x)$ belongs to H. Since H is A-invariant, $-x + A^{j-i}x$ belongs to H, so k divides $j - i$ due to the minimality of k. This implies that $f(z) = A^j y = A^i y$ since $A^k y = y$. So f is well-defined.

We now show that f belongs to T. If $z \notin \operatorname{comp}(x)$ then $Az + B\sigma \notin \notin \operatorname{comp}(x)$ for any $\sigma \in \Sigma$ and conversely since A is invertible. We have

$f(Az + B\sigma) = 0 = Af(z)$. If $z \in \operatorname{comp}(x)$ then $z = A^i x + h$ where $0 \leq i < k$ and $h \in H$. For $\sigma \in \Sigma$ we have $Ah + B\sigma \in H$ and

$$\begin{aligned} f(Az + B\sigma) &= f(A^{i+1}x + Ah + B\sigma) \\ &= \begin{cases} A^{i+1}y & \text{if} \quad 0 \leq i+1 < k \\ y & \text{if} \quad i+1 = k \end{cases} \\ &= Af(z). \end{aligned}$$

So f belongs to T and f is not constant. Hence $\operatorname{End} M = 1 + T$ is not trivial.

We now can describe all the functions in T and hence all the endomorphisms of M. Since Q is finite we have elements $x_1, \ldots, x_t \in Q \backslash H$ with

$$Q = \operatorname{comp}(x_0) \cup \operatorname{comp}(x_1) \cup \ldots \cup \operatorname{comp}(x_t)$$

where $\operatorname{comp}(x_0) = \operatorname{comp}(0) = H$ and $\operatorname{comp}(x_i) \cap \operatorname{comp}(x_j) = \emptyset$ if $i \neq j$. By Lemma 8, $\operatorname{comp}(x_j) = \bigcup_{i=0}^{k_j - 1} A^i x_j + H$ where $k_j > 0$ is minimal such that $-x_j + A^{k_j} x_j \in H$. (Each component of Q is a union of cosets of H in Q.) By Lemma 6 part (iv) each $f \in T$ is constant on any coset of H in Q. So to define a function f in T it is enough to define f on $x_0, x_1, \ldots, x_t$. Moreover we must have $f(x_j) = y_j$ where $A^{k_j} y_j = y_j$. It is now easy to check that $f: Q \to Q$ defined by $f(A^i x_j + h) = A^i y_j$ is a function belonging to T. $\Diamond$

If A is not invertible we have the same result but by a different route.

Proposition 2. *If A is not invertible then the group automaton $M = \langle Q, \Sigma, F \rangle$ is strongly connected iff $\operatorname{End} M$ is trivial.*

Proof. Again it is enough to show that, if M is strongly connected, then $\operatorname{End} M$ is not trivial. We split the argument up into two cases.

Case 1: Assume $\operatorname{reach}(x) \cap H = \emptyset$ for every $x \in Q \backslash H$ where $H = \operatorname{comp}(0)$. From Lemma 2 we have $Q = G_1 + G_0$, a semidirect sum of subgroups G_1, G_0 where G_1 contains the A-invertible elements and G_0 consists of the A-nilpotent elements of Q. Our assumption in Case 1 implies $H \supseteq G_0$. Since $H \supseteq G_0$ and since every element in G_1 belongs to the range of A, Lemma 1 implies that H is a normal subgroup of Q. If $x \in Q \backslash H$ then $x = x_1 + x_0$ where x_1 is invertible and x_0 is nilpotent. Since $\operatorname{reach}(x) \cap H = \emptyset, x_1 \neq 0$. As in the proof of Lemma 8 we have $\operatorname{reach}(x) = \operatorname{reach}(x_1) = \operatorname{comp}(x_1)$. Also $\operatorname{comp}(x_1) = \bigcup_{j=0}^{k-1} A^j x_1 + H$

where $k > 0$ is minimal such that $-x_1 + A^k x_1$ belongs to H. Since G_1 is a group and since A restricted to G_1 is an automorphism of G_1, Cor. 2 implies that A^k is not fixed point free on G_1. So there exists a $y \in G_1$ such that $y \neq 0$ and $A^k y = y$. Define $f: Q \to Q$ as follows:

(i) if $z \in \text{reach}(x) = \text{reach}(x_1) = \text{comp}(x_1)$ with $z = A^i x_1 + h$, then $f(z) = f(A^i x_1 + h) = A^i y$;

(ii) if $z \notin \text{reach}(x)$ then $f(z) = 0$.

As in the proof of Th. 2, f is well defined, it belongs to T and is not constant. So $\text{End}\, M = 1 + T$ is not trivial.

Case 2: Assume that A is not invertible and that there exists an $x \in Q \backslash H$ such that $\text{reach}(x) \cap H \neq \emptyset$. For $y \in Q$ let y have *H-order* $n > 0$ if $A^n y \in H$ but $A^{n-1} y \notin H$. If $A^n y \notin H$ for all n then y has *H-order* ∞. If $y \in H$ then y has *H-order 0*. Our assumption in Case 2 means that there exist elements in Q of finite H-order greater than 0.

Let $x \in Q \backslash H$ have finite H-order $n > 0$. So $A^n x \in H$. From Lemma 2, $x = x_1 + x_0$, where x_1 is invertible and x_0 is nilpotent. Since $A^n x = A^n x_1 + A^n x_0$ belongs to H and since x_1 is invertible, we must have $x_1 \in H$. This means x_0 has H-order n.

For $x_0 \in Q$ such that $x_0 \neq 0$ is nilpotent let $n > 0$ be such that $A^n x_0 = 0$ but $A^{n-1} x_0 \neq 0$. Call n the *nilpotent order* of x_0. Among all the nilpotent elements in Q select z_0 to have maximal nilpotent order, say $k > 0$. From the above observation, if $x \in Q$ has finite H-order t then $t \leq k$.

Define $f: Q \to Q$ as follows:

(i) $f(y) = 0$ if y has H-order 0 or ∞;

(ii) $f(y) = A^{k-i} z_0$ if y has H-order $i > 0$.

We show now that f belongs to T. If $Ay + B\sigma$ has H-order $i > 0$ then y has H order $i + 1$ and

$$f(Ay + B\sigma) = A^{k-i} z_0 = A A^{k-(i+1)} z_0 = A f(y).$$

If $Ay + B\sigma$ has H-order 0 then y has H-order 0 or 1, so

$$f(Ay + B\sigma) = 0 = A f(y).$$

If $Ay + B\sigma$ has H-order ∞ then so does y and conversely. Thus $f(Ay + B\sigma) = 0 = A f(y)$. This shows $f \in T$. Since $k > 1$ then f is not the zero function, and T does not consist of constant maps, i.e. $\text{End}\, M$ is not trivial. $\Diamond$

Propositions 1 and 2 establish the following theorem.

Theorem 2. *A group automaton $M = \langle Q, \Sigma, F \rangle$ is strongly connected iff* $\text{End}\, M$ *is trivial, i.e.* $\text{End}\, M = \{g: Q \to Q \mid g(x) = x + a \text{ with } Aa = a\}$.

4. Linear endomorphisms

If $M = \langle Q, \Sigma, F\rangle$ is a group automaton, is it possible that $\operatorname{End} M$ consists only of linear maps? If M is strongly connected then Th. 1 implies $\operatorname{End} M$ is linear iff the only fixed point of A is 0, in which case $\operatorname{End} M = \{1\}$. If M is not strongly connected it can happen that $\operatorname{End} M$ is linear.

We investigate the linearity of $\operatorname{End} M$ only when A is invertible. Then Q is partitioned into disjoint components $Q = \operatorname{comp}(x_0) \cup \cup \operatorname{comp}(x_1) \cup \ldots \cup \operatorname{comp}(x_n)$ where $\operatorname{comp}(x_0) = \operatorname{comp}(0) = H$, and $\operatorname{comp}(x_i) = \bigcup_{j=0}^{k_i-1} A^j x_i + H$ where $k_i > 0$ is minimal such that $-x_i + A^{k_i} x_i \in H$.

Proposition 3. *Suppose $M = \langle Q, \Sigma, F\rangle$ and A is invertible. Let Q be the union of at least three disjoint components. Then $\operatorname{End} M$ contains nonlinear maps.*

Proof. We have $Q = \operatorname{comp}(0) \cup \operatorname{comp}(x_1) \cup \operatorname{comp}(x_2) \cup \ldots \cup \operatorname{comp}(x_n)$, a disjoint union as above. Define $f: Q \to Q$ as follows: let $f(z) = 0$ if $z \notin \operatorname{comp}(x_1)$ and $f(x_1) = y$ where $y \neq 0$ is such that $A^{k_1} y = y$. Then f belongs to T and $g = 1 + f$ belongs to $\operatorname{End} M$ by Lemma 5. Suppose $x_1 + x_2 \notin \operatorname{comp}(x_1)$, then $g(x_1 + x_2) = x_1 + x_2 \neq x_1 + y + x_2 = g(x_1) + g(x_2)$ and g is not linear. So in order for g to be linear we must have $x_1 + x_2 \in \operatorname{comp}(x_1)$. But then define $f': Q \to Q$ by $f'(z) = 0$ if $z \notin \operatorname{comp}(x_2)$ and $f'(x_2) = y'$ where $A^{k_2} y' = y'$ with $y' \neq 0$. Then $g' = 1 + f'$ belongs to $\operatorname{End} M$ and g' is not linear because $x_1 + x_2 \in \in \operatorname{comp}(x_1)$ means $g'(x_1 + x_2) = x_1 + x_2 \neq x_1 + x_2 + y = g'(x_1) + g'(x_2)$.

The remaining case is the one in which Q has two components, $Q = \operatorname{comp}(0) \cup \operatorname{comp}(x)$. We have $H = \operatorname{comp}(0)$ is a subgroup of the center of Q and $\operatorname{comp}(x) = \bigcup_{i=0}^{k-1} A^i x + H$ where $k > 0$ is minimal such that $-x + A^k x \in H$.

Lemma 9. *Let Q and H be as above. Then $Q/H \cong Z_p \oplus \cdots \oplus Z_p$ for some prime p.*

Proof. $Q/H = \{A^i x + H \mid i = 0, 1, \ldots, k-1\} \cup \{0 + H\}$ since $\operatorname{comp}(x) = \bigcup_{i=0}^{k-1} A^i x + H$. The automorphism A of Q induces an automorphism $\widetilde{A}$ on Q/H defined by $\widetilde{A}(y + H) = Ay + H$. The cyclic group $\langle \widetilde{A} \rangle$ acts transitively on the nonzero elements of Q/H, from which

it follows that Q/H is a p-group of exponent p. Since p-groups have nontrivial centers and since the center of a group is invariant under automorphisms, the center of Q/H is all of Q/H, i.e. Q/H is abelian, whence $Q/H \cong Z_p \oplus \cdots \oplus Z_p$. $\Diamond$

Lemma 10. *Let $M = \langle Q, \Sigma, F\rangle$ with A invertible and $Q = \operatorname{comp}(0) \cup \cup \operatorname{comp}(x)$. Let g be an endomorphism of M with $g = 1 + f$ where $f \in T$. Then g is linear if and only if*

$$f(A^i x + A^j x) = -A^j x + f(A^i x) + A^j x + f(A^j x)$$

for all i, j.

Proof. Let $H = \operatorname{comp}(0)$. Since H is a subgroup of the center of Q, $A^i x + h = h + A^i x$ for all i and all $h \in H$. If g is linear then for all i, j and all $h_i, h_j \in H$, we have

$$(1) \qquad g(A^i x + h_i + A^j x + h_j) = g(A^i x + h_i) + g(A^j x + h_j).$$

Let $A^i x + h_i + A^j x + h_j = A^t x + h_t$. Then since $g = 1 + f$ we have from (1)

$$A^i x + h_i + A^j x + h_j + f(A^t x) = A^i x + h_i + f(A^i x) + A^j x + h_j + f(A^j x)$$

or

$$A^j x + f(A^t x) = f(A^i x) + A^j x + f(A^j x)$$

or

$$f(A^i x + A^j x) = -A^j x + f(A^i x) + A^j x + f(A^j x).$$

The above steps are reversible. $\Diamond$

Corollary 3. *Let $g \in \operatorname{End}(M)$ with $g = 1 + f$ where $f \in T$. Let $Q = \operatorname{comp}(0) \cup \operatorname{comp}(x)$. Then*

(i) *if $f(x) \in \operatorname{comp}(0)$ then g is linear if and only if f is linear;*

(ii) *if Q is abelian then g is linear if and only if f is linear.*

Lemmas 9 and 10 raise the following question: if $\operatorname{End} M$ is linear must T also be linear? If Q is abelian the answer is yes. If $\operatorname{comp}(x) = \bigcup_{i=0}^{k-1} A^i x + H$ and A^k is fixed point free on $\operatorname{comp}(x)$ the answer is yes, for if $f \in T$ then f is completely determined by the value $f(x) = y$ and y must have the property that $A^k y = y$. This means $y \in H = \operatorname{comp}(0)$ and f is linear by Lemma 10 (because y is central).

The question now reduces to the following situation: $Q = \operatorname{comp}(0) \cup \operatorname{comp}(x)$, $\operatorname{comp}(x) = \bigcup_{i=0}^{k-1} A^i x + H$ and there exists a $y \in \operatorname{comp}(x)$ such that $A^k y = y$. Without loss of generality we may

assume $y = x$, i.e. $A^k x = x$. We now define $f: Q \to Q$ by $f(h) = 0$ if $h \in H = \operatorname{comp}(0)$ and $f(A^i x + h) = A^i x$. Since $A^k x = x$, we have that f belongs to T and $g = 1 + f$ belongs to $\operatorname{End} M$. If g is linear then by Lemma 10

$$f(A^i x + A^j x) = -A^j x + A^i x + A^j x + A^j x \tag{2}$$

for all i, j. If $A^i x + A^j x = A^t x + h$ then (2) says that

$$A^t x = -A^j x + A^i x + A^j x + A^j x\,. \tag{3}$$

We now define a new binary operation $*$ on the set Q in terms of the old binary operation $+$ as follows: if $y, z \in Q$ then $y * z = -z + y + z + z$. Since Q/H is abelian and since H is a subgroup of the center of Q then every commutator of Q belongs to the center of Q. Because of the above properties of $(Q, +)$, we have that $(Q, *)$ is a group. (To verify associativity, let a, b, c be in Q. Using multiplicative notation and the fact that $c^{-1}b^{-1}cb$ is central gives

$$\begin{aligned} a * (b * c) &= a * (c^{-1}bcc) = c^{-1}c^{-1}b^{-1}cac^{-1}bccc^{-1}bcc \\ &= c^{-1}(c^{-1}b^{-1}cb)b^{-1}ac^{-1}bcbcc = c^{-1}b^{-1}ac^{-1}bc(c^{-1}b^{-1}cb)bcc \\ &= c^{-1}b^{-1}abbcc = (a * b) * c\,.) \end{aligned}$$

We note that if y or z belongs to the center of $(Q, +)$ then $y * z = y + z$. Since "$*$" is defined in terms of "$+$", the automorphism A on $(Q, +)$ is also an automorphism on $(Q, *)$. Also $(Q, *) = \operatorname{comp}(0) \cup \cup \operatorname{comp}(x)$ where $H = \operatorname{comp}(0)$ is a subgroup of the center of $(Q, *)$, and A acts transitively on $(Q/H, *)$. Moreover by Lemma 9, $Q/H \cong \cong Z_p \oplus \cdots \oplus Z_p$. We have $\operatorname{comp}(x) = \bigcup_{i=0}^{k-1} A^i x + H$ where $A^k x = x, k$ minimal.

By equation (3) we see that $K = \{A^i x \mid i = 0, 1, \ldots, k-1\} \cup \{0\}$ is a group under $*$. This means that $(Q, *)$ is a direct sum of H and K and so $(Q, *)$ is abelian.

We now need some group theory results. For these we switch to the multiplicative notation in our finite group Q. As above we define a new group $(Q, *)$ using $a * b = b^{-1}abb$ where $a, b \in Q$.

Lemma 11. *Let G be a group such that $(G, *)$ forms an abelian group then $(ab)^3 = a^3b^3$ for all $a, b \in G$, or equivalently $(ab)^2 = b^2a^2$ for all $a, b \in G$.*

Proof. In $(G, *), a * b = b * a$ for all a, b implies $b^{-1}abb = a^{-1}baa$ for all a, b in G. Rearranging factors gives $b^{-1}ab^{-1}a = aab^{-1}b^{-1}$,

or $ab^{-1}ab^{-1}ab^{-1} = aaab^{-1}b^{-1}b^{-1}$, or $(ab^{-1})^3 = a^3(b^{-1})^3$ for all a, b in G. $\Diamond$

Lemma 12. *Let G be a group such that $(G,*)$ is abelian and such that G', the commutator subgroup of G, is a subgroup of $Z(G)$, the center of G. Then a^3 belongs to $Z(G)$ for every $a \in G$.*

Proof. By Lemma 11 we have $(ab)^3 = a^3b^3$ for every $a, b \in G$. Since G' is a subgroup of $Z(G)$, $aba^{-1}b^{-1} = c$ is a central element. We have $ab = cba$ and $b^2a^2 = (ab)^2 = abab = c^2baba = c^3b^2a^2$, so $c^3 = 1$. Also $(ab)^3 = ababab = c^3bababa = c^6bbbaaa = b^3a^3$ since $c^3 = 1$. We now have

$$b^3a^3 = (ab)^3 = (ab)^2ab = b^2a^2ab = b^2a^3b$$

which implies $ba^3 = a^3b$, so a^3 is central in G. $\Diamond$

Lemma 13. *Suppose $Q = \operatorname{comp}(0) \cup \operatorname{comp}(x)$ where $\operatorname{comp}(x) = \bigcup_{i=0}^{k-1} A^ix+H, H = \operatorname{comp}(0)$ and k is minimal such that $-x+A^kx \in H$. If s is a positive integer such that s divides k and $s \neq k$ and if A^s has a fixed point $y \neq 0$ in Q, then $\operatorname{End} M$ contains nonlinear maps.*

Proof. We have $A^sy = y$ with $y \neq 0$ $s < k$ and s divides k. We show now that y must belong to H. If $y \notin H$ then $y = A^ix + h$ where $0 \leq i < k-1$ and $h \in H$. We have $0 = (1-A^s)y = (1-A^s)(A^ix+h) = = A^i(1-A^s)x+(1-A^s)h$. This implies $A^i(1-A^s)x$ belongs to H and thus $(1-A^s)x = x - A^sx$ belongs to H. But this is not possible since $s < k$. So y belongs to H.

Define $f: Q \to Q$ by $f(A^ix+h) = A^iy$ and $f(h) = 0$ for all $h \in H$. Since s divides k then f belongs to T. Since $s < k$ then $-x + A^sx \notin H$ and so $f(-x + A^s) \neq 0$. If f were linear then $f(-x + A^sx) = f(-x) + +f(A^sx) = -f(x) + A^sf(x) = -y + A^sy = 0$. So f is not linear. The endomorphism $g = 1 + f$ is not linear since f is not linear and $f(x) = y$ is in $H = \operatorname{comp}(0)$ (Cor. 3). $\Diamond$

Lemma 14. ([1], page 336) *If A is a fixed point free automorphism of order 2 in a finite group G, then G is abelian.*

Proof. By Lemma 7 every element in G has the form $-x + Ax$, and so $A(-x + Ax) = -Ax + A^2x = -Ax + x = -(-x + Ax)$. This means $Ay = -y$ for all y in G. So $-x - y = A(y + x) = Ay + Ax = -y - x$ and G is abelian. $\Diamond$

We return to our group of states $(Q,+)$ where $Q = \operatorname{comp}(0) \cup \cup \operatorname{comp}(x)$, $\operatorname{End} M$ linear and $A^kx = x$. Then $(Q,*)$ is abelian and Lemma 11 and 12 apply to Q. In particular we have $3y$ belongs to the

center of Q for every $y \in Q$. Using Lemma 9 we now have $Q/H \cong$ $\cong Z_3 \oplus \cdots \oplus Z_3$, i.e. Q/H is a 3-group.

Theorem 3. *If $M = \langle Q, \Sigma, F\rangle$ is a group automaton such that $Q =$ $= \operatorname{comp}(0) \cup \operatorname{comp}(x)$, then $\operatorname{End} M$ is linear iff T is linear.*

Proof. We have seen that we may assume $A^k x = x$ and Q/H is an elementary abelian 3-group. Since A acts transitively on Q/H and since k is minimal such that $A^k x = x, k = |Q/H| - 1 = 3^t - 1$ for some integer $t > 0$. In particular k is even, so let $r = k/2$. If A^r has any nonzero fixed points in Q then $\operatorname{End} M$ and T contain nonlinear maps by Lemma 13. So A^r must be fixed point free on Q. Also $(A^r)^2 = A^{2r} = A^k$.

Let Q_x be the subgroup of Q generated by $\{x, Ax, A^2x, \ldots, A^{k-1}x\}$. Then Q_x is A-invariant and $A^k = 1$ on Q_x since $A^k x = x$. On Q_x, A^r is fixed point free and has order 2. By Lemma 14 Q_x is abelian, and this implies Q is abelian. The result follows from Cor. 3. $\Diamond$

Theorem 4. *Let $M = \langle Q, \Sigma, F\rangle$ be a group automaton with A invertible.*

(i) *If M is strongly connected then $\operatorname{End} M$ is linear iff the only fixed point of A is 0;*

(ii) *If M has at least three components then $\operatorname{End} M$ is not linear;*

(iii) *Suppose M has two components, $Q = \operatorname{comp}(0) \cup \operatorname{comp}(x)$. Let $k > 0$ be minimal such that $-x + A^k x$ belongs to $H = \operatorname{comp}(0)$. Then $\operatorname{End} M$ is linear if and only if whenever $y \neq 0$ in Q is such that $A^k y = y$ then $\{A^i y \mid i = 0, \ldots, k-1\} \cup \{0\}$ is an elementary abelian p-group isomorphic to Q/H via $A^i y \to A^i x + H$.*

Proof. It suffices to prove part (iii). By Th. 3 $\operatorname{End} M$ is linear iff T is linear, so we may replace $\operatorname{End} M$ by T. If $f \in T$ is linear with $f(x) = y$ then f induces an isomorphism of the elementary abelian p-group Q/H onto $\{A^i y \mid i = 0, \ldots, k-1\} \cup \{0\}$ given by $A^i x + H \to A^i y$. Moreover if $y \neq 0 \in Q$ is such that $A^k y = y$ then there exists an $f \in T$ with $f(x) = y$. Also k is minimal such that $A^k y = y$ otherwise f is not linear (Lemma 13).

Conversely select $y \neq 0$ in Q such that $A^k y = y$. Then $\{A^i y \mid i = 0, \ldots, k-1\} \cup \{0\}$ is a group isomorphic to Q/H via $\phi: A^i y \to A^i x + H$. This implies $A^j y \neq y$ for $1 \leq j < k$. Define $f \in T$ by $f(x) = y$. If $A^i x + h_i, A^j x + h_j \in Q$ with $h_i, h_j \in H$ and $(A^i x + h_i) + (A^j x + h_j) = A^t x + h_t, h_t \in H$, then

$$f(A^ix + h_i + A^jx + h_j) = f(A^tx + h_t) = A^ty = \phi^{-1}(A^tx + H) =$$
$$= \phi^{-1}(A^ix + H) + \phi^{-1}(A^jx + H) =$$
$$= A^iy + A^jy = f(A^ix + h_i) + f(A^jx + h_j),$$

and f is linear. But every f in T arises in this way, so T is linear. $\Diamond$

We end with an **example** of a group automaton M with two components such that $\operatorname{End} M$ is linear. Let $K = GF(p^n)$, the finite field with p^n elements where p is prime. The multiplicative group K^* of nonzero elements of K is cyclic ([2], page 279); so let α be a generator of K^*. Let $M = \langle Q, \Sigma, F\rangle = \langle K^2, K, F\rangle$ where $F\colon K^2 \times K \to K^2$ is defined by $F(q,\sigma) = F((\beta_1,\beta_2),\gamma) = \binom{\alpha 1}{0\alpha}\binom{\beta_1}{\beta_2} + \binom{\gamma}{0}$. We have $H = \operatorname{comp}(0,0) = \{(\beta,0) \mid \beta \in K\}$ and $Q\backslash H = \operatorname{comp}(x) = \bigcup_{i=0}^{k-1} A^ix + H$ where $x = (0,1), A = \binom{\alpha 1}{0\alpha}$ and $k = p^n - 1$. Since $A^k = \begin{pmatrix} 1 & k\alpha^{k-1} \\ 0 & 1 \end{pmatrix}$, $A^kz \neq z$ for all $z \in \operatorname{comp}(x)$. If $f \in T$ then $f(x) = y$ where $A^ky = y$, which means $y \in H$. Thus $f(x) = (\gamma, 0)$ for some $\gamma \in K$. Since α generates K^*, A^i is fixed point free on Q for all i, $1 \leq i \leq k-1$.

We show now that $T = \left\{ \begin{pmatrix} 0 & \gamma \\ 0 & 0 \end{pmatrix} \middle| \gamma \in K \right\}$. For all $i \geq 0$ we have $A^if(x) = A^i\binom{\gamma}{0} = \binom{\alpha^i\gamma}{0}$ and $A^if(x) = f\left(A^i\binom{0}{1}\right) = f\binom{i\alpha^{i-1}}{\alpha^i}$. This shows $f\binom{i\alpha^{i-1}}{\alpha^i} = \binom{\alpha^i\gamma}{0}$. For any $\beta \in K$ we have $f\binom{\beta}{\alpha^i} = f\left(\binom{i\alpha^{i-1}}{\alpha^i} + \right.$ $\left. + \binom{\beta - i\alpha^{i-1}}{0}\right) = f\left(A^i\binom{0}{1} + \binom{\beta - i\alpha^{i-1}}{0}\right) = A^if(x) = A^i\binom{\gamma}{0} = \binom{\gamma\alpha^i}{0}$. Since f annihilates $H = \{(\beta,0) \mid \beta \in K\}$ then $f = \begin{pmatrix} 0 & \gamma \\ 0 & 0 \end{pmatrix}$.

This show T consists of linear maps. By Cor. 3, $\operatorname{End} M$ is also linear.

References

[1] GORENSTEIN, D.: Finite Groups (2^{nd}) edition, Chelsea, New York, 1980.

[2] HUNGERFORD, T. W.: Algebra, Springer-Verlag, 1974.

[3] MAXSON, C. and SMITH, K.: Endomorphism of Linear Automata, *J. of Computer and System Sciences* **17** (1978), 98–107.