JOURNAL OF COMPUTER AND SYSTEM SCIENCES: 1, 155-165 (1967)

Homomorphic Images of Linear Sequential Machines*

JURIS HARTMANIS

Department of Computer Science, Cornell University, Ithaca, New York

AND

WAYNE A. DAVIS

Electrical Engineering Department, University of Ottawa, and Defence Research Telecommunications Establishment, Ottawa, Ontario, Canada

ABSTRACT

In this paper we investigate homomorphisms on the state behavior of linear machines and characterize their homomorphic images. These results are then applied to characterize those nonlinear machines which can be realized by larger linear machines.

It has been shown [*1*] that, if a sequential machine is realizable by a linear machine, then a linear assignment can be obtained from the output of the machine; furthermore, by increasing the number of states we cannot make a nonlinear machine linear. However, if we are interested in the state behavior of machines, for which either the output is not given or is nonlinear, then the problem of finding linear realizations for the state behavior has been considered only for one-to-one state assignments [*2*]–[*4*].

In this paper we investigate homomorphisms of the state behavior of strongly connected linear machines in order to characterize those nonlinear machines whose state behavior can be realized by larger linear machines. Stated differently, we are investigating those nonlinear machines whose state behavior can be linearized by state splitting (that is, by enlarging the set of states).

The main result of this paper shows that if a linear machine M is mapped onto (reduced to) a nonlinear machine M' then either

(a) M and M' have nontrivial feedback-free parts

or

(b) M and M' have nontrivial autonomous clocks.

Thus any nonlinear machine which does not have a feedback-free part or an autonomous clock cannot be realized by a larger linear machine.

* This research was supported in part by National Science Foundation Grant No GP 6426.

This result has a simple interpretation in terms of machine decomposition. The only linear machines which can have nonlinear homomorphic images are machines which are series (or parallel) connections of two machines, one of which is either feedback-free or a clock. Furthermore, any nonlinear image machine is again a nontrivial series (or parallel) connection of two machines, one of which is a clock or is feedback-free.

1. Preliminaries

A *sequential machine* is a quintuplet

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

where S, I, O are, respectively, the nonvoid finite sets of states, inputs, and outputs;

$$\delta : S \times I \to S$$

is the next-state function, and

$$\lambda: S \times I \to O$$

is the output function.

Throughout this paper we assume for sake of brevity that $I = \{0, 1\}$ and since we are concerned only with the next-state behavior of machines we omit the output alphabet and function and write

$$M = (S, I, \delta).$$

We also extend the next-state function in the natural way by induction to input sequences x in I^* and to subsets of S (I^* is the set of all finite sequences over the alphabet I).

A machine is *strongly connected* if, and only if, for every s_1 and s_2 in S there exists an input sequence x in I^* that maps s_1 onto s_2,

$$\delta(s_1, x) = s_2.$$

We consider only strongly connected machines.

A machine is *uniformly connected* if and only if there exists a positive integer p such that, for every s_1 and s_2 in S, there exists an input sequence of length p that maps s_1 onto s_2.

It is easily shown that if M is strongly connected, but is not uniformly connected, then M can be realized as a serial connection of two smaller machines, one of which is an autonomous machine and we refer to it as a clock. Thus we will refer to non-uniformly connected machines as machines with clocks. For definitions see [5]; for related results see [6].

A machine M is a *permutation* machine if, and only if, every input permutes the set of states, that is, every next-state column contains all states of M:

$$\delta(S, x) = S \quad \text{for all} \quad x \text{ in } I.$$

A machine $M' = (S', I', \delta')$ is a *homomorphic image* of $M = (S, I, \delta)$ if and only if there exist two onto mappings

$$h_1 : S \to S',$$

$$h_2 : I \to I',$$

such that

$$h_1[\delta(s, x)] = \delta'[h_1(s), h_2(x)].$$

In this paper we assume that $I = I'$, and that h_2 is an identity map.

We say that a machine M *realizes* another machine M' if and only if M' is a homomorphic image (of a submachine) of M.

Every homomorphism of M onto M' induces a congruence relation or S.P. partition π on the set of states of M, if we define

$$s \equiv t(\pi) \text{ if and only if } h_1(s) = h_1(t).$$

Conversely, every S.P. partition defines a homomorphism of M onto M' with

$$S' = \{B_i \mid B_i \text{ in } \pi\},$$

$$\delta'(B_i, x) = B_j \text{ for } B_j \text{ such that } \delta(B_i, x) \subseteq B_j,$$

and

$$h_1(s) = \{t \mid t \equiv s(\pi)\}.$$

A sequential machine M is said to be *linear* (over the field of two elements) if and only if there exists a one-to-one state assignment

$$S \to \{(y_1, y_2, \ldots, y_\alpha)\},\ 2^{\alpha-1} < |S| \leqslant 2^\alpha,$$

for which the next-state variables are linear functions of the input and present-state variables

$$y_i' = b_i + a_i x + \sum_{1 \leqslant j \leqslant \alpha} a_{ij} y_j \quad \text{for } 1 \leqslant i \leqslant \alpha,$$

which we abbreviate to

$$\bar{y}' = \bar{b} + \bar{a}\, x + A\, \bar{y}.$$

2. Homomorphisms of Linear Machines

We now investigate the homomorphisms of linear machines.

Lemma 1. *If M is a linear machine and, for some a in I, $\delta(s_1, a) = \delta(s_2, a)$, then $\delta(s_1, x) = \delta(s_2, x)$ for all x in I.*

Furthermore, if, for some s_1 in S, $\delta(s_1, 0) = \delta(s_1, 1)$, then $\delta(s, 0) = \delta(s, 1)$ for all s in S.

Proof. The proof follows directly from the definition of a linear machine.

Thus a linear machine is either a permutation machine or it has at least two identical next-state rows in its flow table. Since for a permutation machine the parts that are not strongly connected are disjoint, our consideration of only strongly connected machines is not very restrictive.

We proceed to show that uniformly connected linear permutation machines can only have linear image machines.

Theorem 1. *If M is a uniformly connected linear permutation machine, then all its homomorphic images M_π are linear.*

Proof. Consider a linear assignment for M which contains $(0, 0,..., 0) = \bar{0}$, and let the matrix period for this realization be k. Since M is uniformly connected, every state can be reached from every other state in km steps. Thus if $\bar{y}$ is mapped onto $\bar{y}'$ by an input string x of length km, denoted by $l(x) = km$, we have

$$\bar{y}' = A^{km}\bar{y} + K_x,$$

where K_x is a constant determined by x. Since

$$A^{km} = I,$$

we have

$$\bar{y}' = \bar{y} + K_x.$$

Consider the block B of π which contains $\bar{0}$ and let

$$C = \{K_x \mid \delta(B, x) = B \text{ and } l(x) = km,\ m = 1, 2,...\}.$$

Then

$$B + C = B,$$

and since all the states in B can be reached from $\bar{0}$ in km steps, we conclude that

$$B = C.$$

Furthermore if K_x and K_y are in C and $\bar{y}$ in B then

$$\bar{y}' = \bar{y} + K_x + K_y \text{ is in } B,$$

and therefore there is a K_z in C such that

$$K_x + K_y = K_z .$$

This implies that C is a linear subspace.

Consider any other block B_1 of π. This block can be reached from B in km steps and therefore there exists a K_x such that

$$B_1 = B + K_x .$$

But then

$$B_1 + C = B + K_x + C = B + K_x = B_1$$

and we conclude that C is the set of vectors which leaves the blocks of π invariant.

Since C is a linear subspace we map by a nonsingular linear transformation C onto the last β variables. In this new linear assignment for M the first $\alpha - \beta$ variables are constant in each block of π and different for different blocks of π. Thus the first $\alpha - \beta$ variables yield a one-to-one state assignment for M_π. Furthermore, this is a linear assignment for M_π, since π has the substitution property and therefore the input and the first $\alpha - \beta$ variables uniquely determine the first $\alpha - \beta$ variables for the next state of M_π. Thus by just removing the last β variables from the linear realization of M we get a linear realization of M_π.

COROLLARY. *A uniformly connected, linear permutation machine has* 2^n *states.*

Proof. If we let π of the previous theorem be the trivial one-block partition

$$\pi = \{S\},$$

then the proof of Theorem 1 shows that the set of codes of this machine form a linear subspace and therefore the machine has 2^n states.

The previous theorem can be sharpened and we show next that, even if a linear permutation machine is not uniformly connected, its uniformly connected image machines are linear.

THEOREM 2. *If M is a linear permutation machine and its homomorphic image M_π is uniformly connected then M_π is linear.*

Proof. If M does not contain a clock then by Theorem 1 the image machine M_π is linear.

If M is not uniformly connected then there exists an r such that the sets of states which can be reached from s in $r + 1, r + 2, \ldots, r + p$ steps

$$S_{r+1}, S_{r+2}, \ldots, S_{r+p},$$

are the blocks of an S.P. partition π_c. Furthermore, the image machine

$$M_{\pi_c}$$

is the largest autonomous image of M.

Consider now a linear assignment for M which contains the code $\bar{0}$ and let $\bar{0}$ be contained in B of π_c.

Let the matrix period be k and let

$$C = \{K_x \mid \delta(B, x) = B \text{ and } l(x) = km, m = 1, 2,...\}.$$

Since every state of B can be reached from $\bar{0}$ in km steps we conclude that

$$C = B$$

and that B is a linear subspace which leaves the blocks of π_c invariant,

$$B_i + B = B_i .$$

(Actually for $\bar{y} \in B_i$ we have $\bar{y} + B = B_i$.)

We will now show that if M_π is a uniformly connected image machine of M then M_π is linear.

Let D be the block of π which contains $\bar{0}$ and let

$$C' = \{K_x \mid \delta(\bar{0}, x) \in D \text{ and } l(x) = km, m = 1, 2,...\}$$

Then C' is a linear subspace, for every D_i of π

$$D_i + C' = D_i ,$$

and

$$C' \subseteq D \text{ and } C' \subseteq B \text{ (of } \pi_c).$$

By a nonsingular linear transformation we now obtain a new linear assignment in which $C = B$ is mapped onto the first β variables and C' is mapped onto the last γ variables of these first β variables. We will show that the first $\beta - \gamma$ variables of this new assignment form a linear assignment for M_π. To do this we have to show that the first $\beta - \gamma$ variables are constant in the blocks of π and have different values for different blocks of π. By construction C' is the largest subspace of B which leaves the blocks of π invariant. Therefore the first $\beta - \gamma$ variables (are not affected by C' and) stay constant in the blocks of π. To see that the first $\beta - \gamma$ variables are different in different blocks we recall that M_π is uniformly connected and therefore every block of π can be reached from s in r, $r + 1$,... steps. This implies that if $\bar{y}$ is in D of π, then D contains all the states of M whose codes differ from $\bar{y}$ only in the clock variables. The same is true for the last γ variables of the first β variables. Thus the states in different blocks of π must differ in the first $\beta - \gamma$ variables, and we have a one-to-one

assignment. Since π has S.P. and since first $\beta - \gamma$ variables come from a linear assignment we conclude that M_π is a linear machine.

The next example shows that a linear permutation machine that is not uniformly connected can have nonlinear image machines. Machine A, given below

	0	1
0	4	6
1	6	4
2	5	7
3	7	5
4	2	0
5	0	2
6	3	1
7	1	3

is easily shown to be a linear machine. On the other hand, the S.P. partition

$$\pi = \{\overline{0, 1}; \overline{2, 3}; \overline{4, 5}; \overline{6, 7}\}$$
$$= \{\bar{A}; \bar{B}; \bar{C}; \bar{D}\}$$

defines the image machine A_π shown below.

	0	1
A	C	D
B	D	C
C	A	A
D	B	B

Since

$$\delta(C, 0) = \delta(C, 1) \text{ and } \delta(B, 0) \neq \delta(B, 1),$$

machine A_π is not linear because of Lemma 1.

The next example shows that a linear machine which is not a permutation machine can have nonlinear image machines. Machine B,

	0	1
0	0	2
1	0	2
2	1	3
3	1	3

is a two-stage binary shift register and thus a linear machine. On the other hand, the S.P. partition

$$\pi = \{\overline{0, 1}; \bar{2}; \bar{3}\} = \{\bar{A}; \bar{B}; \bar{C}\},$$

defines the image machine B_π:

	0	1
A	A	B
B	A	C
C	A	C

Since

$$\delta(A, 0) = \delta(B, 0) \text{ and } \delta(A, 1) \neq \delta(B, 1),$$

machine B is not linear by Lemma 1.

Our next result shows that such machines will always have nonlinear image machines. We first show that any machine, like B_π, which has n states and n-1 different next-state rows is not linear.

LEMMA 2. *An n-state machine, for $n \geqslant 3$, with exactly n-1 distinct next-state rows is not linear.*

Proof. Since two distinct states of M are mapped onto the same state, the matrix for the linear assignment must be singular. Therefore, we can transform this assignment by a nonsingular linear transformation onto another assignment in which the last variable y_α does not depend on the previous state. But then all the states in

$$\delta(S, 0)$$

have the same last variable, say $y_\alpha = 0$. Since M is strongly connected and one state is missing from $\delta(S, 0)$ this state must appear in $\delta(S, 1)$ and furthermore it must have

$$y_\alpha = 1.$$

But then all states in $\delta(S, 1)$ must have $y_\alpha = 1$, which leads to a contradiction, since only one state can have $y_\alpha = 1$. Thus M is not linear.

THEOREM 3. *Let M be a strongly connected machine with more than two states and at least two identical next-state rows* (i.e., *M is not a permutation machine*). *Then M has a nonlinear homomorphic image machine.*

Proof. Our proof shows that any machine satisfying the hypothesis of the theorem

can be mapped homomorphically onto a machine with more than two states and with exactly two identical next-state rows, which by the proceeding lemma is nonlinear.

If M has exactly two identical next-state rows (and more than two states), then it is not linear. If M has more than two identical next-state rows, then let π be a partition which identifies all but two of the identical next-state rows. The partition π defines a homomorphism of M onto M_π. Clearly M_π must have at least three states and if it has exactly two identical next-state rows, then it is not linear. If it has exactly three states, then it has exactly two identical next-state rows (otherwise it is not strongly connected and therefore M is not strongly connected) and is not linear. If M_π has more than two identical next-state rows, then it has more than three states and we repeat the process of taking its homomorphic images as above, and by induction in a finite number of steps, we obtain a nonlinear image machine.

In the proceeding proof we obtained the nonlinear image machine by partially collapsing the feedback-free part. If the homomorphism identifies all the states with identical next-state rows of a linear machine, then the image is again linear. To make this precise we introduce some notation.

Let $M(0) = \tau_1$ be the partition on S of M which is obtained by identifying all states with identical next-state rows; that is,

$$s \equiv t(\tau_1) \text{ if and only if, for all } x \text{ in } I,\ \delta(s, x) = \delta(t, x).$$

This partition has the substitution property and defines an image machine M_{τ_1}. If M_{τ_1} has identical next-state rows, we can repeat this process and arrive, in a finite number of steps, at the largest homomorphic image machine M_τ, which has no identical next-state rows. The S.P. partition τ in the notation of [5] or [7] is given by

$$\tau = M^k(0) \quad \text{for } k \text{ such that } M^k(0) = M^{k+1}(0).$$

Note that any machine M can be realized by a serial connection of M_τ to a feedback-free tail machine [5].

LEMMA 3. *If M is a linear machine then M_τ is also linear.*

Proof. If M has identical next-state rows then the matrix is singular and by a linear transformation we can obtain a new linear assignment in which the variables of the new state do not depend on the last β, $\beta \geq 1$, variables of the old state. Thus we can remove the β variables and obtain a linear image machine. By repeating this process a finite number of times we arrive at the linear image machine M_τ.

Combining the results with Theorem 2 we obtain the next theorem.

THEOREM 4. *If M is a linear machine and its image M_τ is uniformly connected and has no identical next-state rows then M_π is linear.*

3. Realization by Linear Machines

We now apply the results of the previous section to show that a large class of nonlinear machines cannot be linearized no matter how much their sets of states are enlarged. We also characterize these machines that can be realized by larger linear machines.

THEOREM 5. *If M is not a permutation machine and has no identical next-state rows, then M is not a homomorphic image of a linear machine.*

Proof. The machine M cannot be a homomorphic image of a permutation machine, since permutation machines are always mapped onto permutation machines.

From Lemmas 1 and 3 we conclude that if M' is a linear machine, then its largest homomorphic image M'_τ, which has no identical next-state rows, is a linear permutation machine. To see that M cannot be the image of M', assume that, for some S.P. partition π,

$$M'_\pi \cong M.$$

Since M has no identical next-state rows,

$$\pi \geqslant \tau.$$

This implies that M is a homomorphic image of the permutation machine M'_τ, which is impossible. Thus M is not an image of a linear machine.

This result permits us to construct large classes of machines which are not homomorphic images of linear machines. For example, any machine that has no identical next-state rows, but which has some input that maps two states onto identical next states, is not an image of a linear machine.

Finally, combining the previous results and observing that any feedback-free machine is realized by a linear machine, we can derive our last results.

COROLLARY. *A nonlinear machine M is a homomorphic image of a linear machine if and only if the largest homomorphic image of M, which has no identical next state rows, is a permutation machine that is a homomorphic image of a linear machine.*

COROLLARY. *A uniformly connected nonlinear machine is a homomorphic image of a linear machine if and only if the largest homomorphic image of M, which has no identical next state rows, is a linear machine.*

These results show that the nonlinear machines that can be realized by larger linear machines are exactly those machines that are obtained by a serial connection of a linearly realizable permutation machine to a feedback-free machine. If all the non-

linearity of the machine is not in its feedback-free tail part, then M_τ must contain a nontrivial clock or else no linear machine can be used to realize it.

Finally, these results easily yield our last observation.

COROLLARY. *If a nonlinear machine M has only trivial congruence relations, then it cannot be realized by a larger linear machine.*

REFERENCES

1. M. COHN AND S. EVEN. *IEEE Trans. Electronic Computers*, **14**, 367-376 (1965).
2. C. V. SRINIVASSAN. *J. Franklin Institute* **273**, 383-418, (1962).
3. W. A. DAVIS AND J. A. BRZOZOWSKI. *IEEE Trans. Electronic Computers* **15**, 21-29 (1966).
4. J. HARTMANIS. *IEEE Trans. Electronic Computers* **14**, 781-786 (1965).
5. J. HARTMANIS AND R. E. STEARNS. "Algebraic Structure Theory of Sequential Machines." Prentice Hall, Englewood Cliffs, New Jersey, 1966.
6. M. COHN. *IRE. Trans. Circuit Theory* **9**, 74-78 (1962).
7. J. HARTMANIS AND R. E. STEARNS. *IEEE Trans. Electronic Computers* **12**, 223-232 (1963).