[13] J. LaSalle and S. Lefschetz, *Stability by Liapunov's Direct Method with Applications*. New York: Academic, 1961.
[14] T. K. C. Peng, "On guaranteed cost controller and its application to uncertain regulator systems," Ph.D. dissertation, submitted to State Univ. New York at Stony Brook, Stony Brook, Jan. 1971.
[15] A. E. Bryson, Jr., and Y. C. Ho, *Applied Optimal Control*. Waltham, Mass: Blaisdell, 1969.
[16] T. K. C. Peng, "Invariance and stability for bounded uncertain systems," *SIAM J. Contr.*, to be published Nov. 1972.
[17] W. M. Wonham, "On a matrix Riccati equation of stochastic control," *SIAM J. Contr.*, vol. 6, no. 4, 1968.
[18] J. J. Rissanen, "Performance deterioration of optimal systems," *IEEE Trans. Automat. Contr.*, vol. AC-11, pp. 530–532, July 1966.

**Sheldon S. L. Chang** (S'46–M'48–SM'53–F'62) was born in Peiping, China, on January 20, 1920. He received the B.S. and M.S. degrees from Tsinghua University, China, and the Ph.D. degree from Purdue University, Lafayette, Ind., in 1947.

After having worked in industry for several years, he joined the faculty of New York University, New York, in 1952. In 1963 he became Chairman of the Department of Electrical Sciences at the State University of New York, Stony Brook, where he is presently a Professor. He has served as a Consultant on automatic control, machine design, and electronics to many industrial firms. He is the author of *Synthesis of Optimum Control Systems* (McGraw-Hill, 1961) and *Energy Conversion* (Prentice-Hall, 1963).

Dr. Chang is a member of the American Mathematical Society and the Econometric Society.

**T. K. C. Peng** (S'69–M'70) was born in Hunan, China, on March 7, 1944. He received the B.S. degree in electrical engineering from Taiwan University, Taipei, Taiwan, China, in 1965, and the M.S. and Ph.D. degrees from the State University of New York, Stony Brook, in 1969 and 1971, respectively.

From September 1966 to January 1971 he held a University Fellowship and was a Research Assistant in the Department of Electrical Sciences at Stony Brook. Since February 1971 he has been a Post-Doctoral Fellow at the same school. His research interest in modern control theory and application includes optimal control, stability theory, feedback control of bounded uncertain systems, and macroeconomic modeling.

# Finite Group Homomorphic Sequential Systems

ROGER W. BROCKETT, MEMBER, IEEE, AND ALAN S. WILLSKY, STUDENT MEMBER, IEEE

*Abstract*—**Because many systems of practical interest fall outside the scope of linear theory, it is desirable to enlarge as much as possible the class of systems for which a complete structure theory is available. In this paper a class of finite-state sequential systems evolving in groups is considered. The concepts of controllability, observability, minimality, realizability, and the isomorphism of minimal realizations are developed.**

**Results that are analogous to, but differ in essential details from, those of linear system theory are derived. These results are potentially useful in such diverse areas as algorithmic design and algebraic decoding.**

## I. Introduction

THE PURPOSE of this paper is to discuss certain questions related to the modeling of the input–output behavior of dynamical systems. We work in the context of systems with finite input, output, and state sets that admit group operations. The motivation for this study comes from a desire to understand better the key results in linear system theory (linear sequential machines included), and, more importantly, it comes from a desire to embrace in an analogous theory a broader class of input–output models than has heretofore been possible. Our results are potentially useful in optimizing the basic recursions occurring in certain elementary numerical processes, the mechanization of algebraic decoding procedures, etc.

This paper might be regarded as a contribution to the investigation of system theory in the context of universal algebras. It does not include the vector space results as a special case, but it does shed new light on the previous proofs in that context, in that it makes clear which results depend only on the additive group structure inherent in a vector space. We have not worked for the weakest hypothesis for each individual theorem, but rather have sought to place all theorems in a common framework—one motivated by linear theory.

Thus, a number of the results and proofs have direct analogs in linear theory, and the proofs are presented to emphasize the universality of these arguments. That is,

Manuscript received July 15, 1971; revised March 7, 1972. Paper recommended by L. M. Silverman, Chairman of the IEEE S-CS Linear Systems Committee.

This work was supported in part by the U.S. Office of Naval Research under the Joint Services Electronics Program by Contract N00014-67-A-0298-0006 and by the National Aeronautics and Space Administration under Grant NGR 22-007-172, Harvard University, Cambridge, Mass.

R. W. Brockett is with the Division of Engineering and Applied Physics, Harvard University, Cambridge, Mass.

A. S. Willsky is with the Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, Mass.

one should read these results keeping the following in mind. In the theory of algebra, there are a few basic isomorphism theorems for groups, rings, vector spaces, etc., and one obtains the results in one setting from those in another simply by replacing the key words with their analogs, e.g., group for ring and normal subgroup for ideal. The results here indicate that the same type of universal structure and isomorphism results will hold in a system-theoretic framework.

One of the most difficult steps in constructing a realization of input–output maps is the state assignment problem. This step is crucial in the design of recursive algorithms, filters, etc. One of the essential features of our work is that we give a recipe for solving some problems of this type.

## II. Finite Group Homomorphic Sequential Systems

Of course, an empirical theory should avoid making assumptions that cannot be verified experimentally. However, it is nonetheless useful to be able to anticipate the consequences of various assumptions about the internal mechanism of a phenomenon under study, even if we are, in principle, incapable of verifying or denying the assumptions on the basis of experimentation. In this paper we want to investigate the properties of certain finite-state systems that evolve in state spaces that admit a group structure, and we verify in a constructive way the existence of this structure given the input–output data.

Specifically, we consider a class of dynamical models of the form

$$x(k+1) = b[u(k)] \circ a[x(k)]; \qquad y(k) = c[x(k)]$$

where the input, output, and state spaces are the finite groups $\mathfrak{U} = (U, \cdot)$, $\mathfrak{Y} = (Y, *)$, $\mathfrak{X} = (X, \circ)$, respectively. The maps $a: \mathfrak{X} \to \mathfrak{X}$, $b: \mathfrak{U} \to \mathfrak{X}$, and $c: \mathfrak{X} \to \mathfrak{Y}$ are assumed to be group homomorphisms. Invoking an analogy with linear sequential systems, which are a special case, we call this a *finite group homomorphic sequential system*. This class of systems has many things in common with discrete-time linear systems. The most obvious is the following result.

*Theorem 1:* The input, initial state, and output of a finite group homomorphic sequential system

$$x(k+1) = b[u(k)] \circ a[x(k)]; \qquad y(k) = c[x(k)]$$

are related by

$$\begin{aligned} x(k) &= b[u(k-1)] \circ a[b[u(k-2)]] \circ \cdots \circ \\ &\qquad a^{k-1}[b[u(0)]] \circ a^k[x(0)] \\ &\triangleq \left\{ \prod_{i=0}^{k-1} a^{k-i-1}[b[u(i)]] \right\} \circ a^k[x(0)] \\ y(k) &= c[b[u(k-1)]] * c[a[b[u(k-2)]]] * \cdots * \\ &\qquad c[a^{k-1}[b[u(0)]]] * c[a^k[x(0)]] \\ &\triangleq \left\{ \prod_{i=0}^{k-1} c[a^{k-i-1}[b[u(i)]]] \right\} * c[a^k[x(0)]] \end{aligned}$$

where $a^k$ denotes $k$ compositions of $a$ with itself.

*Proof:* This result follows directly from the system equations and the fact that $a$ and $c$ are homomorphisms. Q.E.D.

## III. Realizability Criteria

In this section we give necessary and sufficient conditions for an input–output map to have a sequential realization of the type under consideration here. Recall that a sequence of linear maps of $E^m$ into $E^q$ is realizable as the weighting patterns of a finite-dimensional discrete-time linear system if and only if the sequence satisfies a linear recursion. What we find here is that a sequence of homomorphisms of $\mathfrak{U}$ into $\mathfrak{Y}$ is realizable as the "weighting pattern" of a finite group homomorphic sequential system if and only if the sequence satisfies a homomorphic recursion.

Let $\mathfrak{U} = (U, \cdot)$ and $\mathfrak{Y} = (Y, *)$ be finite groups. We then define $F(\mathfrak{U},\mathfrak{Y})$ to be the finite set of maps of $\mathfrak{U}$ into $\mathfrak{Y}$. $F(\mathfrak{U},\mathfrak{Y})$ is a semigroup under the operation

$$(fg)(u) \triangleq f(u) * g(u) \qquad f,g \in F(\mathfrak{U},\mathfrak{Y}).$$

Suppose $\pi$ is a homomorphism of $\mathfrak{Y} \times \cdots \times \mathfrak{Y}$ ($r$ factors) $\triangleq \mathfrak{Y}^r$ into $\mathfrak{Y}$. Then $\pi$ naturally induces a homomorphism $\hat{\pi}$ of $F(\mathfrak{U},\mathfrak{Y})^r$ into $F(\mathfrak{U},\mathfrak{Y})$:

$$\hat{\pi}(A_1,\cdots,A_r)(u) \triangleq \pi(A_1(u),\cdots,A_r(u)), \qquad \forall u \in \mathfrak{U},$$
$$A_1,\cdots,A_r \in F(\mathfrak{U},\mathfrak{Y}).$$

*Theorem 2:*[1] Let $\mathfrak{U}$ and $\mathfrak{Y}$ be finite groups. Given a sequence of group homomorphisms $T_i: \mathfrak{U} \to \mathfrak{Y}$, $i = 0,1,2, \cdots$, there exists a finite group $\mathfrak{X}$ and group homomorphisms $a: \mathfrak{X} \to \mathfrak{X}$, $b: \mathfrak{U} \to \mathfrak{X}$, and $c: \mathfrak{X} \to \mathfrak{Y}$ such that

$$T_i(\cdot) = c[a^i[b(\cdot)]]$$

if and only if there is an integer $r > 0$ and a homomorphism

$$p: \mathfrak{Y}^r \to \mathfrak{Y}$$

such that for $i = 0,1,2,\cdots$

$$\hat{p}(T_i,\cdots,T_{i+r-1}) = T_{i+r}.$$

*Proof (Sufficiency):* Suppose such a homomorphism exists. We construct the analog of what has, in the context of linear system theory, been called the standard observable realization [1]. Consider the map of $\mathfrak{Y}^r$ into itself defined by

$$a: (x_1,x_2,\cdots,x_{r-1},x_r) \to (x_2,x_3,\cdots,x_r,p(x_1,x_2,\cdots,x_r)).$$

This is clearly a homomorphism if $p$ is. Now define $b$, taking $\mathfrak{U}$ into $\mathfrak{Y}^r$ by

$$b: u \to (T_0(u),T_1(u),\cdots,T_{r-1}(u)).$$

Again, this is a homomorphism if each of the $T$'s is. Define $c$ taking $\mathfrak{Y}^r$ into $\mathfrak{Y}$ according to

$$c: (y_1,y_2,\cdots,y_r) \to y_1.$$

This too is a homomorphism. We claim that $c[a^i[b(\cdot)]] =$

[1] It has recently been pointed out to us that, for the special case of Abelian groups, a realizability result is given in [6].

$T_i(\cdot)$. This is true because of the recursion given by $\hat{p}$:

$$\begin{aligned} c[b(\cdot)] &= c(T_0(\cdot),T_1(\cdot),\cdots,T_{r-1}(\cdot)) = T_0(\cdot) \\ c[a[b(\cdot)]] &= c(T_1(\cdot),T_2(\cdot),\cdots,\hat{p}(T_0,T_1,\cdots,T_{r-1})(\cdot)) \\ &= c(T_1(\cdot),T_2(\cdot),\cdots,T_r(\cdot)) = T_1(\cdot) \\ &\vdots \\ c[a^{r-1}[b(\cdot)]] &= c(T_{r-1}(\cdot),T_r(\cdot),\cdots,T_{2r-2}(\cdot)) = T_{r-1}(\cdot). \end{aligned}$$

The rest of the relations follow in a similar manner by applying the recursion. Thus we may take $x = y^r$.

*Proof (Necessity):* Suppose that $T_i(\cdot) = c[a^i[b(\cdot)]]$ for some set of homomorphisms $a$, $b$, and $c$ with $a:\mathfrak{X} \to \mathfrak{X}$ being defined on a finite group. Since the set of all maps of $\mathfrak{X}$ into itself is a finite set, we see that $a^r = a^k$ for some $r > k \geq 0$. Then $a^{r+m} = a^{k+m}$ for all $m \geq 0$. Then defining $p$ as the projection onto the $(k+1)$th component of an $r$-tuple

$$p(y_0,\cdots,y_{r-1}) = y_k$$

we see that

$$\begin{aligned} \hat{p}(T_i,T_{i+1},\cdots,T_{i+r-1})(\cdot) &= T_{i+k}(\cdot) = c[a^{i+k}[b(\cdot)]] \\ &= c[a^{i+r}[b(\cdot)]] = T_{i+r}(\cdot). \quad \text{Q.E.D.} \end{aligned}$$

We remark that the proof shows that the only sequences of homomorphisms $\{T_i\}$ that can be realized by a finite-group system are those that are periodic after a finite number of terms (see Fig. 1). The next result shows that $a$ is an automorphism if and only if there is no "tail."

*Corollary:* Under the hypotheses of Theorem 2, there exists a realization with $a$ an automorphism if and only if $T_{k+l} = T_k$ for some $l$ and all $k = 0,1,2,\cdots$.

*Proof:* This follows from the fact that $a$ is an automorphism of a finite group if and only if $a^k$ is the identity automorphism for some $k > 0$. Q.E.D.

In automata theory, one usually considers systems described by maps of the form $f:U^* \to Y$ where $U^*$ is the set of all finite strings of elements in $U$ and $f(u_0,\cdots,u_{n-1})$ is the output of the system at time $n$ following the application of the input string $u_0,\cdots,u_{n-1}$ (in this order). One can then ask which $f$'s come from finite group homomorphic sequential systems.

*Theorem 3:* Given finite groups $\mathfrak{U} = (U, \cdot)$ and $\mathfrak{Y} = (Y, *)$, and an input–output map $f:U^* \to Y$, this can be realized as a finite group homomorphic sequential system if and only if $T_i:\mathfrak{U} \to \mathfrak{Y}$, defined by

$$T_i(u) = f(\underbrace{u,e,\cdots,e}_{i \text{ identity inputs}})$$

are homomorphisms satisfying the conditions of Theorem 2, and

$$f(u_0,\cdots,u_n) = T_0(u_n)*T_1(u_{n-1})*\cdots*T_n(u_0).$$

*Proof:* The proof is a straightforward calculation. Q.E.D.

Note that the second condition in Theorem 3 is equivalent to the following: if $\omega_1, \omega_2 \in U^*$ and the length of $\omega_2$ is $k$, then

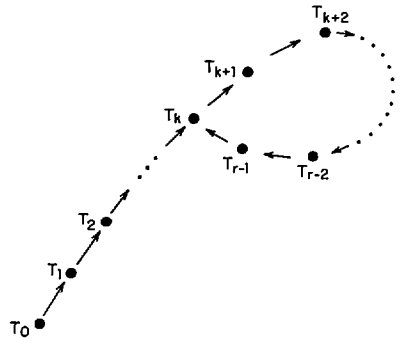



Fig. 1. Realizability condition.

$$f(\omega_1,\omega_2) = f(\omega_2)*f(\omega_1,e^k)$$

where $e^k \in U^*$ is the string of $k$ identity inputs.

For an input–output map $f$ corresponding to a finite group homomorphic sequential system, one should think of the map from $U^r$ into $Y^r$ given by

$$\begin{aligned} y_r &= f(u_0,\cdots,u_{r-1}) = T_0(u_{r-1})*T_1(u_{r-2})*\cdots*T_{r-1}(u_0) \\ y_{r+1} &= f(u_0,\cdots,u_{r-1},e) = T_1(u_{r-1})*T_2(u_{r-2})*\cdots*T_r(u_0) \\ &\vdots \\ y_{2r-1} &= f(u_0,\cdots,u_{r-1},e^{r-1}) = T_{r-1}(u_{r-1})* \\ &\qquad T_r(u_{r-2})*\cdots*T_{2r-2}(u_0) \end{aligned}$$

as being the analog of the map corresponding to the Hankel matrix. As will be shown, the number of elements in the image space of this map equals the number of states in the "minimal realization," just as the rank of the Hankel matrix determines the dimension of the state space of a minimal linear realization.

## IV. Controllability, Observability, and Minimal Systems

One of the crucial results in linear system theory is that a system is minimal if and only if it is controllable and observable, and any two controllable and observable realizations of the same input–output map differ at most by a choice of basis for the state space. This result has a natural analog here, but the analog of a related result, namely, the fact that any input–output map that has a linear realization has a controllable and observable linear realization, fails. This means we must characterize all those systems that have controllable and observable realizations and this is done in Theorem 8 below. We note that finite dimensional vector spaces over the same field are isomorphic if and only if they are of the same dimension, whereas finite groups can have the same number of elements and not be isomorphic. Thus the state space isomorphism theorems are decidedly more interesting here.

We say that the homomorphic sequential system

$$x(k+1) = b[u(k)] \circ a[x(k)]; \qquad y(k) = c[x(k)]$$

which evolves in the group $\mathfrak{X} = (X, \circ)$ is *controllable from* $x_1 \in X$ if for any $x_2 \in X$ there exists a sequence of controls in the input group such that the state is driven

from $x_1$ to $x_2$ by this sequence. The system is said to be *controllable* if it is controllable from all $x \in X$. Two states $x_1, x_2 \in X$ are said to be *indistinguishable* if, given any input sequence, the corresponding output sequences from the initial states $x_1$ and $x_2$ are identical. Otherwise, $x_1$ and $x_2$ are said to be *distinguishable*, and an input sequence that yields different output sequences from $x_1$ and $x_2$ is said to *distinguish between* $x_1$ *and* $x_2$. We call the system *observable* if any distinct pair of states is distinguishable.

*Theorem 4:* Consider the finite group homomorphic sequential system

$$x(k+1) = b[u(k)] \circ a[x(k)]; \qquad y(k) = c[x(k)]$$

with state group $\mathfrak{X} = (X, \circ)$. Let $e_x \in X$ be the identity in $\mathfrak{X}$. Then the system is controllable if and only if it is controllable from $e_x$. The states $x_1$ and $x_2$ are distinguishable if and only if the identity control sequence distinguishes between them. Also, $x_1$ is indistinguishable from $x_2$ if and only if $x_1 x_2^{-1}$ is indistinguishable from $e_x$.

*Proof:* These results are obtained by straightforward calculations. Q.E.D.

Thus, as in the case of linear systems, the test for controllability reduces to a test for controllability from the identity, and the test for observability reduces to a test for indistinguishability from the identity.

The next theorem gives a formula for the set reachable from the identity and the set indistinguishable from the identity.

*Theorem 5:* If the finite group homomorphic sequential system

$$x(k+1) = b[u(k)] \circ a[x(k)]; \qquad y(k) = c[x(k)]$$

evolves in a group $\mathfrak{X} = (X, \circ)$ with $n$ elements then the set of states reachable from the identity is

$$\mathfrak{R} = \{b(u_1) \circ a[b(u_2)] \circ \cdots \circ a^{n-1}[b(u_n)] \mid u_1, \cdots, u_n \in U\}$$
$$\triangleq b(U) \circ ab(U) \circ \cdots \circ a^{n-1} b(U).$$

The set of states indistinguishable from the identity is

$$\mathfrak{K} = \ker c(\cdot) \cap \ker c[a(\cdot)] \cap \cdots \cap \ker c[a^{n-1}(\cdot)].$$

The set $\mathfrak{R}$ is not necessarily a group, but $\mathfrak{K}$ is a normal subgroup of $\mathfrak{X}$.

*Proof:* With respect to the reachable set, this result is immediate from the formula

$$x(k+1) = b(u(k)) \circ a[b(u(k-1))] \circ \cdots \circ a^{k-1}[b(u(1))] \circ a^k[x(1)]$$

and the observation that, because of the stationarity of the system, any state reachable from the identity is reachable along a trajectory that contains no state more than once and thus is of length less than or equal to $n$.

If the input sequence is a string of identity elements, then the output sequence from the identity state is simply a string of identity elements in $\mathfrak{Y}$. If the output from the state $x$ is to be indistinguishable from this string, then it must happen that

$$c(x) = c[a(x)] = \cdots = c[a^{n-1}(x)] = \text{identity}.$$

Can it happen that this set of equalities holds but $c[a^p(x)] \neq$ identity for some $p \geq n$? Clearly not, because for any $x$, $a^i(x) = a^j(x)$ for some $n \geq i > j \geq 0$ because there are only $n$ elements in $X$. This means that for any $x$ and any positive integer $p$ we have $a^p(x) = a^k(x)$ with $0 \leq k \leq n-1$, where $k$, of course, depends on $x$ and $p$. (Actually for $n \geq 2$, we can replace $n-1$ by $n-2$ in the expressions for $\mathfrak{R}$ and $\mathfrak{K}$, but while this is easy to prove for $\mathfrak{R}$, the result for $\mathfrak{K}$ is more cumbersome and we have thus omitted it.)

To see that $\mathfrak{K}$ is a normal subgroup, we need only observe that the map of $\mathfrak{X}$ into $\mathfrak{Y}^n$ defined by

$$x \to (c(x), c[a(x)], \cdots, c[a^{n-1}(x)])$$

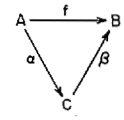
is a homomorphism and $\mathfrak{K}$ is its kernel. That $\mathfrak{R}$ need not be a subgroup of $\mathfrak{X}$ will be shown by example later.

Q.E.D.

*Corollary:* Under the hypotheses of Theorem 5, the set $\mathfrak{R}$ is a subgroup if $\mathfrak{X}$ is an Abelian group.

*Proof:* We need only note that for all $m \geq 0$, $a^m b(U)$ is a subgroup, and that the product of two subgroups of an Abelian group is itself a subgroup. Q.E.D.

We now recall some of the concepts of abstract realization theory ([2], ch. 10). If $A$ and $B$ are sets and we have an input–output map $f: A \to B$, a *factorization* of $f$ through a state set $C$ is a pair of maps $\alpha: A \to C$ and $\beta: C \to B$ such that $f = \beta \circ \alpha$, i.e., the following diagram commutes.



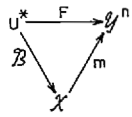

This factorization is *canonical* if $\alpha$ is onto and $\beta$ is one-to-one.

In this case, the "size" of $C$ is minimal in some sense. For instance, if $A$, $B$, and $C$ are vector spaces and $f$, $\alpha$, and $\beta$ are linear maps, and if $\hat{C}$, $\hat{\alpha}$, $\hat{\beta}$ is any other, not necessarily canonical, factorization, then $\dim C \leq \dim \hat{C}$. Also, if $A$, $B$, $C$, and $\hat{C}$ are finite sets, with $C$ corresponding to a canonical and $\hat{C}$ to any other factorization, then $\text{card}\,(C) \leq \text{card}\,(\hat{C})$.

Suppose we have an input group $\mathfrak{U} = (U, \cdot)$, an output group $\mathfrak{Y} = (Y, *)$, and an input–output map $f: U^* \to Y$ that has at least one realization as a finite group homomorphic sequential system:

$$x(k+1) = b[u(k)] \circ a[x(k)], \qquad y(k) = c[x(k)]$$

with finite state group $\mathfrak{X} = (X, \circ)$. Suppose $\mathfrak{X}$ has $n$ elements, and define $F: U^* \to Y^n$ by $f(u_0, \cdots, u_k) = (f(u_0, \cdots, u_k), f(u_0, \cdots, u_k, e), \cdots, F(u_0, \cdots, u_k, e^{n-1}))$. We then have a factorization of $F$:



where

$$\mathcal{B}(u_0,\cdots,u_k) = b(u_k)\circ ab(u_{k-1})\circ\cdots\circ a^k b(u_0)$$
$$m(x) = (c(x),ca(x),\cdots,ca^{n-1}(x)).$$

We immediately see that the above factorization is minimal if and only if the system is controllable and observable. In this case, we say that the triple of homomorphisms $(a,b,c)$ defines a *minimal realization.*

Another result of abstract realization theory is the following: given $f:A \to B$ and two canonical factorizations —that is, two sets $C$ and $\hat{C}$ and corresponding maps $\alpha:A \to C$, $\hat{\alpha}:A \to \hat{C}$, both onto, and $\beta:C \to B$, $\hat{\beta}:\hat{C} \to B$, both one-to-one, such that $f = \beta\circ\alpha = \hat{\beta}\circ\hat{\alpha}$—then the two are *equivalent,* in that there exists a unique one-to-one and onto map $\gamma:C \to \hat{C}$, such that $\hat{\alpha} = \gamma\circ\alpha$ and $\beta = \hat{\beta}\circ\gamma$.

When we apply this result to the problem of finite group homomorphic sequential systems, we obtain stronger results, as in linear theory, because of the structure of the systems.

*Theorem 6:* Suppose $\mathfrak{U} = (U, \cdot)$ and $\mathfrak{Y} = (Y, *)$ are finite groups, and $f:U^* \to Y$ is an input–output map that has two controllable and observable finite group homomorphic sequential realizations

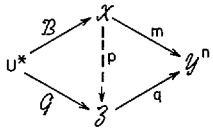
$$x(k+1) = b[u(k)]\circ a[x(k)]; \qquad y(k) = c[x(k)] \quad (1)$$
$$z(k+1) = g[u(k)]\circ f[z(k)]; \qquad y(k) = h[z(k)] \quad (2)$$

where the system (1) evolves in a finite state group $\mathfrak{X} = (X, \circ)$ and system (2) evolves in a finite state group $\mathfrak{Z} = (Z, \circ)$. Then there exists a group isomorphism $p:\mathfrak{X} \to \mathfrak{Z}$ such that $f = pap^{-1}$, $g = pb$, and $h = cp^{-1}$. The two realizations are said to be *conjugate.*

*Proof:* Suppose the cardinality of $\mathfrak{X}$ is $n$. Then the same is true of $\mathfrak{Z}$ by the comments preceding the theorem. Let $F:U^* \to \mathfrak{Y}^n$, $\mathcal{B}:U^* \to \mathfrak{X}$, and $m:\mathfrak{X} \to \mathfrak{Y}^n$ be as before, and define $\mathcal{G}:U^* \to \mathfrak{Z}$ and $q:\mathfrak{Z} \to \mathfrak{Y}^n$ by

$$\mathcal{G}(u_0,\cdots,u_k) = g(u_k)\circ fg(u_{k-1})\circ\cdots\circ f^k g(u_0)$$
$$q(z) = (h(z),hf(z),\cdots,hf^{n-1}(z)).$$

Then, by controllability and observability, we have two canonical factorizations of $F$ and the commutative diagram




where $p$ is the unique one-to-one and onto map such that the diagram remains commutative.

Let $x_1,x_2 \in X$. Then we have

$$q[p(x_1\circ x_2)] = m(x_1\circ x_2) = m(x_1)*m(x_2)$$
$$= q[p(x_1)]*q[p(x_2)] = q[p(x_1)\circ p(x_2)].$$

Since $q$ is one-to-one $p(x_1\circ x_2) = p(x_1)\circ p(x_2)$. Thus $p$ is an isomorphism. It is then a simple computation to arrive at the relation betwen $(a,b,c)$ and $(f,g,h)$. Q.E.D.

Note that in the theorem, the group structure of $\mathfrak{U}$ is never used, however the group structure of $\mathfrak{Y}$ and the fact that $m$ and $q$ are both one-to-one homomorphisms are used to show that $p$ is an isomorphism. This lack of symmetry in the arguments is discussed in the next section.

As was mentioned in Theorem 5, $\mathcal{R}$—the set of states reachable from the identity—need not be a subgroup. Thus, given a finite group homomorphic sequential system, there need *not* exist a controllable system of this type with the same input–output description. In fact, one might expect that a homomorphic sequential system has a minimal realization as a homomorphic sequential system if and only if the set $\mathcal{R}$ of states reachable from $e_x$ is, in any particular realization, a subgroup. The example below shows that this need not be the case. If $\mathcal{R}$ *is* a subgroup, we can restrict our homomorphisms to $\mathcal{R}$, modulo the kernel of $(c,ca,\cdots,ca^{n-1}):\mathfrak{X} \to \mathfrak{Y}^n$, and thus construct a controllable and observable homomorphic realization (a simple check shows that one can redefine the homomorphisms in a well-defined manner after extracting the kernel—therefore, there always exists an *observable* homomorphic realization). Thus, for example, if there exists a homomorphic realization with an Abelian state group, there exists a controllable and observable homomorphic realization.

An example will illustrate these ideas. The dihedral group $D_n$ is a group of order $2n$ generated by two elements $x$ and $y$ that satisfy the relations

$$x^n = e, \qquad y^2 = e; \qquad xyx = y$$

where $e$ is the group identity. The cyclic group of order $n$ will be denoted as $Z_n$, and its elements are $\{0,1,\cdots, n-1\}$. Consider the finite group homomorphic sequential system

$$x(k+1) = b[u(k)]\circ a[x(k)]; \qquad y(k) = c[x(k)]$$

where $\mathfrak{U} = \mathfrak{Y} = Z_2$, $\mathfrak{X} = D_4$, and $a$, $b$, and $c$ are homomorphisms uniquely determined by

$$b(1) = y$$
$$a(x) = e, \qquad a(y) = xy$$
$$c(x) = 0, \qquad c(y) = 1.$$

The set of states reachable from $e$ may be shown to be

$$\mathcal{R} = \{e,y,xy,x^3\}$$

which is *not* a subgroup.

However if we compute the input–output homomorphisms $T_i = ca^ib:Z_2 \to Z_2$, we find that

$$T_k = \text{identity for all } k \geqslant 0.$$

Although the above nonminimal realization has an identity-reachable set that is not a group, there still exists a minimal homomorphic sequential system. In fact, such a realization is found by taking $\mathfrak{U} = \mathfrak{X} = \mathfrak{Y} = Z_2$ and $a = b = c =$ identity. The reason we can find

such a realization is that our original system is not observable. It is easy to see that there exists a controllable and observable homomorphic sequential realization of a given input–output map if and only if the identity-reachable set in any particular *observable* realization is a group. An example of an observable system for which $\mathcal{R}$ is not a group is found by modifying the previous example. Let $\mathcal{U}$, $\mathcal{X}$, $a$, and $b$ be as above, but let $\mathcal{Y} = \mathcal{X} = D_4$ and $c$ = identity (i.e., state output). This is observable, and $\mathcal{R}$ is the same as before.

There are conditions under which $\mathcal{R}$ is a subgroup, in which case we do have a controllable and observable homomorphic realization. The following theorem indicates one such condition.

*Theorem 7:* Under the hypotheses of Theorem 5, the set $\mathcal{R}$ of states reachable from the identity is a subgroup of $\mathcal{X}$ if $a$ is an automorphism.

*Proof:* The group of automorphisms of a finite group is itself a finite group with function composition as the group operation. Thus there exists a $k > 0$ such that

$$a^k = \text{identity automorphism.}$$

From Theorem 1 we see that the set $\mathcal{R}$ of states reachable from the identity can be written in the form

$$\mathcal{R} = \bigcup_{m \geq 0} \prod_{i=0}^{m} a^{m-i}b(U) = \bigcup_{m \geq 1} [b(U) \circ ab(U) \circ \cdots \circ a^{k-1}b(U)]^m$$

where $U$ is the input group and for $H \subset X$

$$H^m \triangleq \{h_1 \circ h_2 \circ \cdots \circ h_m | h_i \in H\}.$$

Thus if $x, y \in \mathcal{R}$, we have that $x \in [b(U) \circ ab(U) \circ \cdots \circ a^{k-1}b(U)]^{m_1}$ and $y \in [b(U) \circ ab(U) \circ \cdots \circ a^{k-1}b(U)]^{m_2}$ for some $m_1$ and $m_2$. Then $x \circ y \in [b(U) \circ ab(U) \circ \cdots \circ a^{k-1}b(U)]^{m_1+m_2}$. We see that for all $n > 0$, $x^n \in \mathcal{R}$ if $x \in \mathcal{R}$. Since $\mathcal{X}$ is a finite group, there exists on $N > 0$ such that $x^{-1} = x^N$. Therefore $\mathcal{R}$ is a subgroup. Q.E.D.

The next theorem completely characterizes those sequences of input–output homomorphisms that have controllable and observable finite group homomorphic sequential realizations. To do this, we must define what we mean by a free response of a system. If a system is given in recursive form (as our first equation), a free response is the identity input response of the system from some initial state. If the system is given in input–output form, it is the response to an input sequence, which consists of the identity only, from some point onward, and where the response is observed from the point in time where the nonidentity inputs stop. Thus we apply a (possibly) nonidentity input up to time $k$ and record the output from time $k + 1$ on. Note that the set of free responses of an input–output map corresponds to the set of free responses of a homomorphic realization of that map started in a state reachable from the identity state. In what follows, free responses refer to the input–output system description. Note that we can consider the set of free responses as a subset of the infinite direct product group $\mathcal{Y} \times \mathcal{Y} \times \cdots \times \mathcal{Y} \times \cdots$.

*Theorem 8:* Let the sequence of homomorphisms $T_i$: $\mathcal{U} \to \mathcal{Y}$, $i = 0,1,2, \cdots$, with $\mathcal{U}$ and $\mathcal{Y}$ finite groups, satisfy the hypotheses of Theorem 2. Then there exists a controllable and observable finite group homomorphic sequential realization if and only if the set of free responses form a subgroup of the infinite direct product group.

*Proof (Sufficiency):* Let $\mathcal{F}$ be the group of all free responses. Let $\mathcal{F}_n$ be defined as follows.

$$\mathcal{F}_n = \left\{ (y_0,y_1,\cdots,y_{n-1}) \in \mathcal{Y}^n \;\middle|\; \begin{array}{l} y_0,y_1,\cdots,y_{n-1} \text{ are the} \\ \text{first } n \text{ elements of a} \\ \text{free response} \in \mathcal{F} \end{array} \right\}.$$

Obviously $\mathcal{F}_n$ is a subgroup of $\mathcal{Y}^n$ if $\mathcal{F}$ is a subgroup of the infinite direct product.

Consider the standard observable realization given in the proof of Theorem 2. In that realization, the state space is $\mathcal{Y}^r$, and it is easy to see that the set $\mathcal{R}$ of states reachable from the identity is just $\mathcal{F}_r$. Then, restricting our homomorphisms to $\mathcal{F}_r$, we have a minimal homomorphic realization.

*Proof (Necessity):* Suppose we have a minimal homomorphic realization of the $T_i$:

$$x(k+1) = b[u(k)] \circ a[x(k)]; \qquad y(k) = c[x(k)].$$

Since every state is reachable from the identity, the set of free responses in the input–output sense is identical to the set of free responses in the state space sense. Consider the map from $\mathcal{X}$ into the infinite direct product group $\mathcal{Y} \times \mathcal{Y} \times \cdots \times \mathcal{Y} \times \cdots$ given by

$$x \to (c(x),ca(x),\cdots,ca^k(x),\cdots).$$

This is obviously a homomorphism, and its image is $\mathcal{F}$, which therefore must be a group. Q.E.D.

*Corollary:* Under the hypothesis of Theorem 8, if $\mathcal{F}$ is a group, $\mathcal{F}$ is isomorphic to $\mathcal{F}_n$ for some $n$.

*Proof:* Suppose $a$ is the state transition homomorphism for a minimal realization. Then there exist $k > p \geq 0$ such that $a^k = a^p$, and then

$$(c(x),ca(x),\cdots,ca^n(x),\cdots) = (c(x),ca(x),\cdots,ca^{k-1}(x), ca^p(x),\cdots,ca^{k-1}(x),\cdots)$$

and the isomorphism is obvious. Note that even if $\mathcal{F}$ is not a group, there exists an $n$ such that the elements of $\mathcal{F}$ and $\mathcal{F}_n$ are in one-to-one correspondence. Q.E.D.

## V. Some Comments on State Space Reduction

A number of questions were raised in the preceding sections. We have derived the standard observable realization; what about a "standard controllable realization" in the sense of [1]? The set of states indistinguishable from the identity is a (normal) subgroup; why is not the set of states reachable from the identity necessarily a subgroup? In Theorem 6 we used the fact that $m$ and $q$ are homomorphisms; what about $\mathcal{B}$ and $\mathcal{G}$? We have seen that $\mathcal{R}$ need

not be a group, and for similar reasons $\mathcal{B}$ and $\mathcal{G}$ are not homomorphisms and there is no standard controllable realization.

Note that these difficulties arise from the following consideration. Suppose we have a set of homomorphisms $c_i$, $i = 1,2,\cdots,m$, mapping a finite group $\mathfrak{X}$ into a finite group $\mathfrak{Y}$. Then the "fan-out" map taking $\mathfrak{X}$ into $\mathfrak{Y}^n$

$$x \to (c_1(x),\cdots,c_n(x))$$

is always a homomorphism, but the "fan-in" map taking $\mathfrak{X}^n$ into $\mathfrak{Y}$

$$(x_1,\cdots,x_n) \to c_1(x_1)\cdot c_2(x_2)\cdot \cdots \cdot c_n(x_n)$$

need *not* be a homomorphism. (For example, the map of $\mathfrak{X} \times \mathfrak{X}$ into $\mathfrak{X}$ defined by group multiplication is typically not a homomorphism.)

In the rest of this section, we will discuss these problems in some depth. We will also present some additional conditions which enable us to circumvent some of the difficulties.

Even if $\mathcal{R}$ is a group, we cannot be sure that the map $\mathcal{B}$ is a homomorphism. If $\mathfrak{X}$ has $n$ elements, then the map $\mathcal{B}$ defined by

$$\mathcal{B}:\mathfrak{U} \times \cdots \times \mathfrak{U} \ (n \text{ times}) \to \mathcal{R}$$

$$\mathcal{B}(u_0,\cdots,u_{n-1}) \triangleq b(u_{n-1})\circ ab(u_{n-2})\circ\cdots\circ a^{n-1}b(u_0)$$

is onto. We would like to investigate putting a semidirect product structure on $\mathfrak{U} \times \cdots \times \mathfrak{U}$ in order to make $\mathcal{B}$ a homomorphism. We have the following necessary condition.

*Theorem 9:* Consider a finite group homomorphic sequential system. If there exists a semidirect product structure on $\mathfrak{U} \times \cdots \times \mathfrak{U}$ ($n$ times) such that $\mathcal{B}:\mathfrak{U} \times \cdots \times \mathfrak{U} \to \mathfrak{X}$ is a homomorphism, then the set of states reachable from the identity in $k$ steps is a group for all $k > 0$.

*Proof:* Choose $k \in \{1,\cdots,n\}$. Consider the set of input strings

$$\mathcal{W}_k = \{(e_u{}^{n-k},u_0,\cdots,u_{k-1}) | u_0,\cdots,u_{k-1} \in U\}.$$

For any semidirect product structure on $\mathfrak{U} \times \cdots \times \mathfrak{U}$, this is a subgroup. Thus $\mathcal{B}(\mathcal{W}_k)$ is a subgroup if $\mathcal{B}$ is a homomorphism and $\mathcal{B}(W_k)$ is just the set of elements reachable from the identity in $k$ steps. For $k > n$ use Theorem 5. Q.E.D.

We now modify the earlier example. We concern ourselves with the input-state side of the system only. Again let $\mathfrak{U} = Z_2$, $\mathfrak{X} = D_4$, and let $b$ be as before, but redefine $a$ by

$$a(y) = xy \qquad a(xy) = y.$$

It is easy to check that $a$ is an automorphism of $D_4$, and thus by Theorem 7 $\mathcal{R}$ is a subgroup. However,

$$\mathcal{B}(\mathcal{W}_2) = \{e,y,xy,x^3\},$$

which is not a group, and thus $\mathcal{B}$ is not a homomorphism for any semidirect product structure on $\mathfrak{U} \times \cdots \times \mathfrak{U}$.

These examples illustrate an asymmetry in the theory. Unlike linear system theory—or even the Abelian group case here, where it is clear that none of these difficulties appear—we do not have a naïve duality theory without additional assumptions.

An assumption that avoids some of these difficulties is that of requiring $a$ to be a normal endomorphism. A homomorphism $f$ of a group $\mathcal{G}$ into itself is called a normal endomorphism if for all $x, y \in \mathcal{G}$

$$xf(y)x^{-1} = f(xyx^{-1}).$$

*Theorem 10:* Consider the finite group homomorphic sequential system

$$x(k+1) = b[u(k)]\circ a[x(k)]; \qquad y(k) = c[x(k)]$$

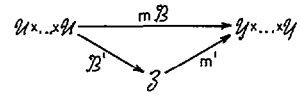
evolving in a finite group $\mathfrak{X}$ of order $n$. Suppose $a$ is a normal endomorphism. Then there exists a semidirect product structure on $\mathfrak{U} \times \cdots \times \mathfrak{U}$ ($n$ times) such that the input-state map $\mathcal{B}$ is a homomorphism, and thus the identity-reachable set $\mathcal{R}$ is a subgroup.

*Proof:* Define the binary operation on $\mathfrak{U} \times \cdots \times \mathfrak{U}$ ($n$ times)

$$\begin{aligned}(u_0,u_1,\cdots,u_{n-1})&(v_0,v_1,\cdots,v_{n-1})\\ &\triangleq (v_1{}^{-1}\cdot v_2{}^{-1}\cdot \cdots \cdot v_{n-1}{}^{-1}u_0v_{n-1}\cdot \cdots\\ &\quad \cdot v_2v_1v_0,v_2{}^{-1}v_3{}^{-1}\cdot \cdots \cdot v_{n-1}{}^{-1}u_1v_{n-1}\cdot \cdots\\ &\quad \cdot v_3v_2v_1,\cdots,v_{n-1}{}^{-1}u_{n-2}v_{n-1}v_{n-2},u_{n-1}v_{n-1}).\end{aligned}$$

Direct computation verifies that this does define a semidirect product structure on $\mathfrak{U} \times \cdots \times \mathfrak{U}$ ($n$ times), and another computation, using the fact that $a$ is a normal endomorphism verifies that $\mathcal{B}$ is a homomorphism. Q.E.D.

Thus, in this case, we can reduce our system to a minimal homomorphic realization by first restricting the homomorphisms to $\mathcal{R}$ and then taking $\mathcal{R}$ modulo the kernel of $m$, the state-output map (see Theorem 6). We then have the following canonical factorization of the input–output map $m\mathcal{B}$




where $\mathcal{Z}$ is the reduced state group, and $\mathcal{B}'$ and $m'$ are the reduced input-state and state-output homomorphisms, with $\mathcal{B}'$ onto and $m'$ one-to-one.

Another question arises in the case where $\mathcal{R}$ is not a group. When this happens, we have $x_1,x_2 \in \mathcal{R}$ such that $x_1\circ x_2 \notin \mathcal{R}$. Thus this particular group multiplication never occurs in the operation of the system and is irrelevant information. One can then ask whether or not we can redefine these irrelevant multiplications in such a manner as to make $\mathcal{R}$ a group, while at the same time requiring that $a$, $b$, and $c$ remain homomorphisms when restricted to $\mathcal{R}$. The example given previously shows that, at least in some cases, this can be done. Again let $\mathfrak{U} = \mathfrak{Y} = Z_2$, $\mathfrak{X} = D_4$ with $a$, $b$, $c$ defined by $b(1) = y$;

$a(x) = e, a(y) = xy; c(x) = 0, c(y) = 1$. We saw that

$$\mathfrak{R} = \{e,y,xy,x^3\}.$$

The superfluous multiplications are $(xy)\circ y$, $(xy)\circ x^3$, $x^3\circ y$, and $x^3\circ x^3$. If we define these as follows:

$$(xy)\circ y \triangleq x^3 \qquad x^3\circ y \triangleq xy$$

$$(xy)\circ x^3 \triangleq y \qquad x^3\circ x^3 \triangleq e$$

then $\mathfrak{R}$ is the Klein-4 group, and it is easy to check that $a$, $b$, and $c$ are still homomorphisms. In fact, since the Klein-4 group is Abelian, $a$ is a normal endomorphism, and we can reduce our system as described above.

## VI. Conclusion

In this paper we have considered a broader class of input–output relations than those found in linear system theory and have derived results analogous to some of the more crucial properties of linear systems. In particular, we have considered dynamical systems of the form

$$x(k+1) = b[u(k)]\circ a[x(k)]; \qquad y(k) = c[x(k)]$$

where the input, state, and output spaces are finite groups, and $a$, $b$, and $c$ are homomorphisms. The concepts of controllability, observability, and minimality are developed, and conditions for the realization of an input–output map by such a system are given. As in the linear case, the equivalence of any two minimal homomorphic realizations is established.

In addition, several problems, all directly or indirectly related to duality, arise in considering this broader class of systems. These are discussed, and it is shown that an additional assumption removes these problems.

The analogy with linear theory has by no means been completely exploited. Concepts such as transform theory have not been considered at all. Also, extensions of some of these results to infinite group problems can be made, possibly making contact with the study of dynamical systems on topological groups [7].

## Acknowledgment

The author wishes to thank Prof. M. Arbib, of the University of Massachusetts, and Prof. R. Book, of Harvard, for helpful comments on an earlier draft.

## References

[1] R. W. Brockett, *Finite Dimensional Linear Systems.* New York: Wiley, 1970.
[2] R. E. Kalman, P. Falb, and M. Arbib, *Topics in Mathematical System Theory.* New York: McGraw-Hill, 1969.
[3] J. J. Rotman, *The Theory of Groups: An Introduction.* Boston: Allyn and Bacon, 1965.
[4] P. Zeiger, "Ho's algorithm, commutative diagrams, and the uniqueness of minimal linear systems," *Inform. Contr.*, vol. 11, pp. 71–79, 1967.
[5] A. Gill, *Linear Sequential Circuits; Analysis, Synthesis, and Applications.* New York: McGraw-Hill, 1967.
[6] M. A. Arbib, "Decomposition theory for automata and biological systems," IEEE Control Systems Society, Catalog 71C61-CSS, A. S. Morse, Ed., 1971.
[7] R. W. Brockett, "System theory on group manifolds and coset spaces," *SIAM J. Contr.*, vol. 10, May 1972.

**Roger W. Brockett** (S'62–M'63) received the Ph.D. degree from Case Western Reserve University, Cleveland, Ohio.

From 1963 to 1969 he taught courses in system theory in the Department of Electrical Engineering, Massachusetts Institute of Technology, Cambridge. He is presently Gordon McKay Professor of Applied Mathematics in the Division of Engineering and Applied Physics, Harvard University, Cambridge, Mass. At Harvard he participates in the Interdisciplinary Decision and Control Program through teaching and research. He is a consultant to various industrial and research organizations, including the M.I.T. Lincoln Laboratory. He is coeditor (with H. H. Rosenbrock) of the series *Studies in Dynamical Systems* (Thomas Nelson and Sons Ltd.) and author of the book *Finite Dimensional Linear Systems* (Wiley). In 1968 he was a recipient of the American Automatic Control Council's Donald P. Eckman Award, and in 1969 he received a U.K. Science Research Council Senior Post-Doctoral Fellowship for study at Warwick University.

**Alan S. Willsky** (S'70) was born in Newark, N.J., on March 16, 1948. He received the S.B. degree in aeronautics and astronautics from the Massachusetts Institute of Technology, Cambridge, in 1969.

Since 1969 he has held a fellowship awarded from the Fannie and John Hertz Foundation, while working toward the Ph.D. degree in the Department of Aeronautics and Astronautics at M.I.T. His present interest is in the development of techniques for the synthesis of dynamical systems for estimation, control, and computation.

Mr. Willsky is a member of Tau Beta Pi and Sigma Gamma Tau.