INFORMATION AND CONTROL 27, 126–147 (1975)

Invertibility of Finite Group Homomorphic Sequential Systems

ALAN S. WILLSKY*

Electronic Systems Laboratory, Department of Electrical Engineering, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

A class of systems, introduced by Brockett and Willsky, that evolve homomorphically on finite groups is considered. A general result, extending the linear sequential circuit Hankel matrix result of Massey and Sain, is derived. Also, an analog of the Brockett–Mesarovic result is obtained when we restrict our attention to abelian group systems.

1. INTRODUCTION

The question of invertibility of a dynamical system—i.e., when does the output sequence (function) uniquely determine the input sequence (function)—has received a good deal of attention in the literature and has applications to problems in coding theory and functional controllability (the dual of invertibility). Massey and Sain (1968), Sain and Massey (1969), Brockett and Mesarovic (1965), and Forney (1970) have all dealt with invertibility conditions for linear systems. In this highly structured setting one can obtain quite detailed and explicit invertibility conditions. At the other structural extreme, Olson (1970) has obtained invertibility results for general finite state machines. Of course the results in this general setting are not nearly as detailed as the linear results.

Our work falls in between these structural extremes. Brockett and Willsky (1972, 1974) and Willsky (1973a) have introduced a class of finite state systems that evolve homomorphically on finite groups. As their results indicate, this class of systems, although much broader than the class of linear sequential

* This work was conducted in part while the author was a Fannie and John Hertz Foundation Fellow in the Dept. of Aeronautics and Astronautics at the Massachusetts Institute of Technology, and in part at the Decision and Control Sciences Group of the M.I.T. Electronic Systems Laboratory with partial support provided by AFOSR under Grant 72-2273.

circuits (which is included as a special subclass of the class of finite group systems) possess many of the properties of the more structured class of linear systems. In Section 2 we review some of the important results from Brockett and Willsky (1972) and Willsky (1973a) on controllability, observability, minimality, and realizability. Section 3 contains the analog of the Massey–Sain Hankel matrix result for linear sequential circuits. Our proof parallels that in Massey and Sain (1968), although we must work somewhat harder because of the more general (i.e., nonabelian) setting. In Section 4 we derive the analog of the Brockett–Mesarovic linear system result for the class of abelian group systems. Section 5 contains several examples and a brief discussion of the problem of constructing inverses for FGHSS's.

It should be noted that the basic ideas behind the proofs of the results in this paper closely follow the concepts developed for linear systems in Massey and Sain (1968) and Sain and Massey (1969). One of the major motivations behind the development of our results is a desire to gain insight as to which of the results in linear system theory can be generalized to systems endowed with "less" structure and which linear system results depend intrinsically upon the linear structure and at best have only restricted extensions to less structured classes of systems. It is hoped that this knowledge will aid in the development of a universal or categorical theory of dynamical systems.

Keeping these thoughts in mind, we urge the reader to compare our techniques with those developed by Massey and Sain to see how we are able to obtain analogs of many of the results in Massey and Sain (1968) and Sain and Massey (1969) solely with the aid of several of the most basic results in group theory. The brief discussion of inverse construction in Section 5 is an initial attempt to attack one system result for which only a restricted version of the corresponding linear result can be obtained in the group-homomorphic setting. It is our hope that a thorough investigation of the questions raised in Section 5 will lead to a deeper understanding of systems defined on various algebraic structures.

2. A Class of Finite Group Systems

In this section we review some of the basic definitions and results from Brockett and Willsky (1972) and Willsky (1973a). We first note that to be precise we should denote a group $\mathscr{G}$ by a pair $(G, *)$, where G is a set and $*$ is the group operation assigning to every pair $g_1, g_2 \in G$ the element $g_1 * g_2$. We will abuse this notation whenever there is no chance of ambiguity by identifying $\mathscr{G}$ with G and by denoting $g_1 * g_2$ by $g_1 g_2$.

Definition 1. Let X, U, and Y be finite state, input and output groups, respectively. The dynamical system

$$x(k+1) = b[u(k)]\, a[x(k)] \tag{1}$$

$$y(k) = c[x(k)], \tag{2}$$

where $a\colon X \to X$, $b\colon U \to X$, and $c\colon X \to Y$ are group homomorphisms, is called a *finite group homomorphic sequential system* (FGHSS).

The next few results, proven in Brockett and Willsky (1972) and Willsky (1973a), reflect the highly structured nature of the class of FGHSS's.

Theorem 1. *The input, state, and output of the FGHSS* (1), (2) *are related by*

$$x(k) = b[u(k-1)]\, ab[u(k-2)] \cdots a^{k-1}b[u(0)]\, a^k[x(0)] \tag{3}$$

$$y(k) = T_0[u(k-1)]\, T_1[u(k-2)] \cdots T_{k-1}[u(0)]\, ca^k[x(0)], \tag{4}$$

where $T_i : U \to Y$ is the homomorphism defined by

$$T_i = ca^ib.$$

Proof. See Brockett and Willsky (1972). ∎

The reader is referred to Brockett and Willsky (1972) for a result, much like the linear system result, on when a "weighting pattern" T_0, T_1, $T_2 \cdots$ can be realized as a FGHSS. The reader is also referred to the general definitions of controllability, distinguishability, and observability given in Brockett and Willsky (1972).

Theorem 2. *Consider the* FGHSS (1), (2) *with state group X. The system is controllable if and only if it is controllable from the identity state e. 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 $x_1x_2^{-1}$ is indistinguishable from e.*

Proof. See Brockett and Willsky (1972). ∎

We now note some of the complications and discrepancies with the results of linear theory caused by the present more general (non-abelian) setting (see Willsky (1973a) for details). The set R_k of states reachable from the identity e in k steps need not be a subgroup of X, although the set K_k of states indistinguishable from e over k steps is a *normal* subgroup. Here (Ra denotes range, ker denotes kernel)

$$\begin{aligned} R_k &= \mathrm{Ra}\{(u_0, \ldots, u_{k-1}) \mapsto b(u_{k-1})\, ab(u_{k-2}) \cdots a^{k-1}\, b(u_0)\} \\ K_k &= \ker\{x \mapsto (c(x), \ldots, ca^{k-1}(x))\}. \end{aligned}$$

Thus there need not be a controllable FGHSS realization of a FGHSS, although there always is an observable one. See Brockett and Willsky (1972) for the proof of the isomorphism of any two minimal (controllable, observable) FGHSS realizations of a given input–output map.

In Willsky (1973a) we investigated the use of additional assumptions to obtain more detailed results for FGHSS's. If one assumes that the various groups are abelian, a large number of the results of linear theory go through. A second less restrictive assumption is that $a : X \to X$ is a *normal endomorphism*—i.e., that

$$xa(y)\, x^{-1} = a(xyx^{-1}) \qquad \forall x, y \in X.$$

Note that this is always the case if X is abelian. In this case, as proven in Brockett and Willsky (1972), R_k is a subgroup of X for all k, and we have the following result (here card $\triangleq$ cardinality):

THEOREM 3. *Consider a* FGHSS *with* card $X = n$. *Let*

$$n = (p_1)^{k_1}(p_2)^{k_2} \cdots (p_s)^{k_s},$$

where the p_i are distinct primes and the k_i are positive integers. Define

$$k(n) \triangleq \sum_{i=1}^{s} k_s . \tag{5}$$

Then if R_k is a subgroup for all k (e.g., if a is normal or X is abelian), the set R of states reachable from e at some *time is given by*

$$R \triangleq \bigcup_{k \geqslant 0} R_k = R_{k(n)} .$$

Thus the system is controllable if and only if

$$R_{k(n)} = X.$$

Proof. See Willsky (1973a). ∎

The lack of controllability–observability duality for FGHSS's is illustrated by the fact that the observability analog of Theorem 3 is true for arbitrary FGHSS's.

THEOREM 4. *Consider a* FGHSS *with* card $X = n$. *Then for* $k \geqslant k(n)$

$$K_k = K_{k(n)} .$$

Thus the system is observable if and only if

$$K_{k(n)} = \{e\}.$$

Proof. See Willsky (1973a). ▌

We note that the basis of the proofs of Theorems 3 and 4 is Lagrange's Theorem (Rotman, 1965): if H is a subgroup of $G(H < G)$, card $H\backslash$card G [read: "card H *divides* card G" (evenly)]. We will use this in proving the main result of Section 4.

3. A General Invertibility Condition for FGHSS's

In this section we derive a characterization of invertibility for FGHSS's that is analogous to, and in fact generalizes, the linear system result derived in Massey and Sain (1968). We first define the concept of L-delay invertibility for a general discrete time system.

DEFINITION 2. Consider the general discrete time system

$$x(k + 1) = \lambda[x(k), u(k)], \tag{6}$$

$$y(k) = \delta[x(k)], \tag{7}$$

where $x \in X$, the state set, $u \in U$, the input set, and $y \in Y$, the output set. Define the input and output vectors

$$U_k = \begin{bmatrix} u(0) \\ \vdots \\ u(k) \end{bmatrix} \qquad Y_k = \begin{bmatrix} y(1) \\ \vdots \\ y(k) \end{bmatrix}.$$

Here $U_k \in U^{k+1}$ (the $(k + 1)$-fold Cartesian product of U with itself) and $Y_k \in Y^k$. We say that the system (6), (7) is *invertible with delay L* or has an *inverse of delay L* if (given $x(0)$) U_k can be recovered from Y_{k+L+1} $\forall k \geqslant 0$—i.e., if Y_{k+L+1} uniquely specifies U_k.

To provide some perspective for our results, we include the Massey–Sain result. Let X, U, and Y be vector spaces and $A\colon X \to X$, $B\colon U \to X$, $C\colon X \to Y$ be linear maps. Consider the linear system

$$x(k+1) = Ax(k) + Bu(k) \tag{8}$$

$$y(k) = Cx(k). \tag{9}$$

If $x(0) = 0$, we have

$$Y_k = M_k U_{k-1},$$

$$M_k = \begin{bmatrix} T_0 & 0 & 0 & \cdots & 0 \\ T_1 & T_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ T_{k-1} & T_{k-2} & T_{k-3} & \cdots & T_0 \end{bmatrix}$$

$$T_i = CA^iB.$$

For linear systems, since we can "subtract out" the effect of $x(0)$ on Y_k (because of superposition), we need only consider L-invertibility with $x(0) = 0$, which we now tacitly assume is the case.

THEOREM 5. *Given the linear system* (8), (9) *with* dim $U = s$. *Then there exists an L-delay inverse if and only if*

$$\operatorname{rank} M_{L+1} = \operatorname{rank} M_L + s. \tag{10}$$

Proof. See Massey and Sain (1968). ▮

Now suppose that the base field F for the linear system has $q < \infty$ elements. In this case we call (8), (9) a *linear sequential circuit* (LSC) and (8), (9) define define a FGHSS. Also, if V is a finite dimensional vector space over F, card $V = q^{\dim V}$. Thus (10) is equivalent to

$$\text{card Ra } M_{L+1} = m \text{ card Ra } M_L,$$

where card $U = m$. It is this result that we shall generalize, and the reader is referred to the parallel LSC arguments in Massey and Sain (1968).

Recalling the general invertibility definition, our problem here is the following: consider a FGHSS (1), (2) with $x(0) = e$ (as with LSC's, we can "divide out" the effect of a nonidentity initial condition—see (3), (4)), card $X = n$, card $U = m <$ card $Y = p$ (we need this to have any chance of inverting the system); we wish to find conditions on the system such that an L-delay inverse exists, (as we will discuss, the inverse system need not be a FGHSS, although there always is a LSC inverse of a LSC). Defining the input–output homomorphisms $T_i = ca^i b$, we see that we have the relation

$$Y_k = M_k U_{k-1},$$

where $M_k : U^k \to Y^k$ is defined by

$$\begin{aligned} y(1) &= T_0[u(0)] \\ y(2) &= T_0[u(1)]\, T_1[u(0)] \\ &\vdots \\ y(k) &= T_0[u(k-1)]\, T_1[u(k-2)] \cdots T_{k-1}[u(0)]. \end{aligned}$$

Note that unlike M_k in the LSC case and much like the input-state map for FGHSS's, for a FGHSS M_k need *not* be a homomorphism [for any direct or semidirect product structure on the U^k; see Brockett and Willsky (1972)]. However, it is always a homomorphism if Y is abelian (we can then put the direct product structure on U^k and Y^k).

THEOREM 6. *A* FGHSS *has an inverse with delay L if and only if* U_0 *can be determined from* Y_{L+1}.

Proof. We need only show sufficiency, since it is necessary by definition. Thus suppose $u(0) = U_0$ can be determined from Y_{L+1}. We can then "divide out" the effects of $u(0)$ on Y_k. If we omit $z(1)$ $(=e)$, the modified outputs $z(k)$, given by

$$z(k) = y(k)[T_{k-1}[u(0)]]^{-1}$$

are the same as they would be if $u(1)$ were the first input to the system (stationarity is important here). Thus $u(1)$ can be determined from Y_{L+2}. Continuing this procedure, we see that U_k can be recovered from Y_{k+L+1}. ∎

Define the maps $A_k : U \to Y^k$, $D_k : U^{k-1} \to Y^k$

$$A_k(u) = (T_0(u), T_1(u),..., T_{k-1}(u)) \tag{11}$$

$$D_k(u_1,..., u_{k-1}) = (e, M_{k-1}(u_1,..., u_{k-1})) \tag{12}$$

and endow Y^k with the direct product group structure. Note that A_k is a homomorphism, D_k need not be, and

$$M_k[u(0),..., u(k-1)] = D_k[u(1),..., u(k-1)]\, A_k[u(0)]. \tag{13}$$

LEMMA 1. *A* FGHSS *has an inverse with delay L if and only if*

(i) A_{L+1} *is one-to-one*;

(ii) *if* $x \in \operatorname{Ra} A_{L+1}$, $y \in \operatorname{Ra} D_{L+1}$, *then*

$$yx \in \operatorname{Ra} A_{L+1} \Rightarrow y = (e,..., e)$$
$$yx \in \operatorname{Ra} D_{L+1} \Rightarrow x = (e,..., e).$$

Proof (*Necessity*). Suppose the FGHSS has an L-delay inverse. Clearly A_{L+1} must be one-to-one, or else there exists an input $u(0) \neq e$ such that $A_{L+1}(u(0)) = (e,..., e)$. Then, from (13)

$$M_{L+1}(u(0), e,..., e) = (e,..., e) = Y_{L+1} = M_{L+1}(e,..., e)$$

so $u(0)$ cannot be recovered from Y_{L+1}. Now suppose we have $x \in \operatorname{Ra} A_{L+1}$, $y \in \operatorname{Ra} D_{L+1}$ such that $yx \in \operatorname{Ra} A_{L+1}$. This implies that there exists an input sequence $u(0),..., u(L)$ and another input $u'(0)$, such that

$$\begin{aligned} yx &= D_{L+1}(u(1),..., u(L))\, A_{L+1}(u(0)) \\ &= M_{L+1}(u(0), u(1),..., u(L)) = M_{L+1}(u'(0), 0,..., 0) \\ &= A_{L+1}(u'(0)). \end{aligned}$$

Since we are assuming L-delay invertibility, we must have $u(0) = u'(0)$, but then we must have $y = (e,..., e)$. Now assume $x \in \operatorname{Ra} A_{L+1}$, $y \in \operatorname{Ra} D_{L+1}$ such that $yx \in \operatorname{Ra} D_{L+1}$. Then there is an input sequence $u(0),..., u(L)$ such that the response to this is the same as the response to e, $u'(1),..., u'(L)$. Thus, by L-invertibility, $u(0) = e$, and $x = A_{L+1}(u(0)) = (e,..., e)$.

Proof (*Sufficiency*). We now assume conditions (i) and (ii) of the lemma statement hold. Suppose we have two different input sequences $u(0),..., u(L)$ and $u'(0),..., u'(L)$ such that

$$\begin{aligned} Y_{L+1} &= M_{L+1}(u(0),..., u(L)) \\ &= M_{L+1}(u'(0),..., u'(L)) = Y'_{L+1}. \end{aligned} \tag{14}$$

Referring to the definition of M_k in (13), we see that (14) is equivalent to

$$D_{L+1}[u(1),..., u(L)]\, A_{L+1}[u(0)\, u'(0)^{-1}] = D_{L+1}[u'(1),..., u'(L)].$$

By condition (ii), we must have $A_{L+1}[u(0)\, u'(0)^{-1}] = (e,..., e)$, and by (i), $u(0)\, u'(0)^{-1} = e$—i.e., $u(0) = u'(0)$. Thus we recover $u(0)$ *uniquely* from Y_{L+1} and our system is L-delay invertible. ▌

We refer the reader to the proof of Theorem 4 in Massey and Sain (1968). Lemma 1 is the analog of the part of that proof concerning the linear independence of certain columns of the matrix M_L in the LSC case. We can now prove the analog of Theorem 5.

THEOREM 7. *A* FGHSS *has an inverse with delay L if and only if*

$$\text{card Ra } M_{L+1} = m \text{ card Ra } M_L, \tag{15}$$

where card $U = m$.

Proof. Note that

$$\text{card Ra } D_{L+1} = \text{card Ra } M_L. \tag{16}$$

We also see that condition (i) of Lemma 1 is equivalent to card Ra $A_{L+1} = m$, and we claim that (ii) is equivalent to the following: if $x_1, x_2 \in \text{Ra } A_{L+1}$, $y_1, y_2 \in \text{Ra } D_{L+1}$, then

$$y_1x_1 = y_2x_2 \Rightarrow y_1 = y_2, \qquad x_1 = x_2. \tag{17}$$

Suppose (ii) holds. Then if $y_1x_1 = y_2x_2$,

$$y_1x_1x_2^{-1} = y_2,$$

but Ra A_{L+1} is a group, so $x_1x_2^{-1} \in \text{Ra } A_{L+1}$. Then by (ii), $x_1x_2^{-1} = e$, which implies $x_1 = x_2$, $y_1 = y_2$. Now suppose (17) holds. Then, if $y_1x_1 = x_2 \in \text{Ra } A_{L+1}$, $y_1x_1 = ex_2 (e \in \text{Ra } D_{L+1})$, which implies $y_1 = e$ by (17). Similarly, $y_1x_1 = y_2 \in \text{Ra } D_{L+1}$ and $e \in \text{Ra } A_{L+1}$ imply $x_1 = e$ by (17).

Now note that (17) holds if and only if

$$\text{card}[(\text{Ra } D_{L+1})(\text{Ra } A_{L+1})] = [\text{card Ra } D_{L+1}][\text{card Ra } A_{L+1}]. \tag{18}$$

Then, referring to (13), (16), and (18), we see that (15) holds. ▌

We now define the concept of pointwise observability as in Massey and Sain (1968).

DEFINITION 3. A FGHSS is *pointwise input observable* if any $u(0) \in U$ in the input sequence $u(0), e, e, \ldots,$ is uniquely determined from the output sequence $y(1), y(2), \ldots$.

THEOREM 8. *A* FGHSS *with* card $X = n$ *is pointwise input observable if and only if* $A_{k(n)}$ *is one-to-one.*

Proof. It is easy to see that the system is pointwise input observable if and only if

$$\ker cb \cap \ker cab \cap \cdots \cap \ker ca^r b = \{e\} \tag{19}$$

for some r. Now if b is not one-to-one, we cannot satisfy (19). Thus assume b is one-to-one (and card $U > 1$ or everything is trivial), and, since

$$b[\ker cb \cap \cdots \cap \ker ca^r b] = \ker c \cap \cdots \cap \ker ca^r \cap b(U)$$

we have that (19) holds if and only if

$$\ker c \cap \cdots \cap \ker ca^r \cap b(U) = \{e\}. \tag{20}$$

By Theorem 4, if (20) holds, it holds for $r = k(n) - 1$, and, referring to (11), we see that we have A_k is one-to-one for some k (i.e., the system is pointwise input observable) if and only if $A_{k(n)}$ is. ∎

THEOREM 9. *Consider a* FGHSS *with* card $U = m$, card $Y = r$. *Then* A_k *cannot be one-to-one for*

$$k < k_0 = \min(\ell \mid m \backslash r^\ell)$$

and thus $(k_0 - 1)$ is a lower bound on the delay in any inverse of the system.

Proof. Consider $A_k : U \rightarrow Y^k$. Then by the First Isomorphism Theorem for groups (Rotman, 1965):

$$U/\ker A_k \simeq A_k(U) < Y^k$$

so

$$m \backslash r^k \text{ card } \ker A_k$$

and $\ker A_k = \{e\} \Leftrightarrow m \backslash r^k$. ∎

Note that this result has no analog for LSC's—i.e., there is no lower bound on the delay of an inverse for a LSC. The reason is that in the LSC case $m = q^{s_1}$ and $r = q^{s_2}$, where q is the cardinality of the underlying field and the s_i are the dimensions of the input and output space. Since we must have $m \leqslant r$, we have $m \backslash r$, so $k_0 = 1$.

We now wish to consider analogs of other LSC results. However, we run into the same type of problem that confronted us in considering the question of controllability. We first wish to consider an alternative characterization of invertibility analogous to Lemma 5 of Massey and Sain (1968). The idea for LSC's is the following: Since the M_k are linear maps, a system is L-invertible if and only if it is "kernel-free"—i.e., if and only if $Y_{L+1} = 0$ implies $u(0) = 0$. In the FGHSS case, the M_k are not homomorphisms (it appears that they need not be homomorphisms even if a is a normal endomorphism), and thus in general one does not have the guarantee that $Y_{L+1} = e \Rightarrow u(0) = e$ is the same as L-invertibility. However, we do have the following:

THEOREM 10. *Consider a* FGHSS (1), (2) *with a a normal endomorphism. Then the system is L-invertible if and only if $Y_{L+1} = e$ implies $u(0) = e$.*

Proof. The proof of this result is relatively lengthy, and we do not include it here. Instead, the reader is referred to Willsky (1973a). ▮

Although the assumption that a is a normal endomorphism allows us to prove the preceding result, we cannot derive analogs of the invertibility conditions in Sain and Massey (1964), Brockett and Mesarovic (1965), and Willsky (1974) without even stronger assumptions. In the next section we will derive a result of the desired form for the case of abelian group systems.

4. AN INVERTIBILITY CONDITION FOR ABELIAN FGHSS'S

As we did in the previous section, we now state the LSC result for which we will derive a FGHSS analog. The LSC result is a strengthened version, proved in Willsky (1974), of the result derived in Sain and Massey (1969).

THEOREM 11. *Consider the linear system* (8), (9) *with* $\dim U = m$, $\dim X = n$. *The system is invertible if and only if it is invertible with delay $L \leqslant n - m$—i.e., if and only if*

$$\operatorname{rank} M_{n-m+1} = \operatorname{rank} M_{n-m} + m,$$

which is true if and only if we have the following condition: given $u(0),\ldots, u(n - m + 1)$, such that the output of the system (started at $x(0) = 0$) in response to this string followed by all 0's is identically 0, then $u(0) = \cdots = u(n - m + 1) = 0$.

Proof. See Willsky (1974). ▮

We remark that if one considers an output equation with direct feedthrough—i.e., $y(k) = Cx(k) + Du(k)$—and if we let $q =$ dimension of the nullspace of D, we can show that the system must have an inverse with delay $\leqslant n - q$. Theorem 11 is a special case of this result.

COROLLARY 1. *The linear system* (8), (9) *is invertible if and only if*

$$\operatorname{rank} P = (n - m + 2)m,$$

where

$$P = \begin{bmatrix} CB & 0 & \cdots & 0 \\ CAB & CB & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ CA^{n-m+1}B & CA^{n-m}B & \cdots & CB \\ CA^{n-m+2}B & CA^{n-m+1}B & \cdots & CAB \\ \vdots & \vdots & \vdots & \vdots \\ CA^{2n-m}B & CA^{2n-m-1}B & \cdots & CA^{n-1}B \end{bmatrix}.$$

Proof. The proof is a direct analog of the proof of Theorem 3 in Sain and Massey (1969). ▮

COROLLARY 2. *The linear system is invertible if and only if*

$$\operatorname{rank} M_{n-m+1} \geqslant (n - m + 1)(m - 1) + 1.$$

Proof. This is an immediate consequence of Theorem 11. ▮

Returning to the FGHSS case, we assume that Y is an abelian group. Let U_c be the *commutator subgroup of* U

$$U_c = \text{subgroup generated by } \{aba^{-1}b^{-1} \mid a, b \in U\}.$$

Note that U is abelian if and only if $U_c = \{e\}$, and for any homomorphism $\gamma\colon U \to Y$

$$\gamma(U_c) = \{e\}.$$

Thus for our system to have any chance of being invertible, we must also assume that U is abelian. In this case, $M_k : U^k$ (direct product) $\to Y^k$ (direct product) *is* a homomorphism $\forall k$ (the sum of homomorphisms on abelian groups is itself a homomorphism), as is $D_k : U^{k-1} \to Y^k$, defined by (12).

THEOREM 12. *Consider a* FGHSS *with U and Y abelian, and consider $A_k : U \to Y^k$ and $D_k : U^{k-1} \to Y^k$ defined by* (11) *and* (12), *respectively. Then*

$$\frac{\text{Ra}\, M_{L+1}}{\text{Ra}\, D_{L+1}} \approx \frac{\text{Ra}\, A_{L+1}}{\text{Ra}\, A_{L+1} \cap \text{Ra}\, D_{L+1}} \tag{21}$$

and

$$\frac{\text{card Ra}\, M_{L+1}}{\text{card Ra}\, M_L} = \frac{\text{card Ra}\, A_{L+1}}{\text{card}[\text{Ra}\, A_{L+1} \cap \text{Ra}\, D_{L+1}]}\,. \tag{22}$$

Proof. We first note that Ra A_{L+1} and Ra D_{L+1} are groups and from (13)

$$\text{Ra}\, M_{L+1} = \text{Ra}\, A_{L+1} + \text{Ra}\, D_{L+1}\,. \tag{23}$$

We also recall the Second Isomorphism Theorem for groups (Rotman, 1965): let G be a group, S a subgroup, and T a normal subgroup; then $S \cap T$ is a normal subgroup of S, and

$$ST/T \approx S/S \cap T. \tag{24}$$

Letting $G = Y^{L+1}$, $S = \text{Ra}\, A_{L+1}$, $T = \text{Ra}\, D_{L+1}$ and using the fact that all subgroups of abelian groups are normal, we see that (23) and (24) imply (21). We then obtain (22) by noting that if H is normal in G

$$\text{card}\left(\frac{G}{H}\right) = \frac{\text{card}\, G}{\text{card}\, H}$$

and that

$$\text{card Ra}\, D_{L+1} = \text{card Ra}\, M_L\,. \quad \blacksquare$$

Note that Theorem 12 also proves that the quantity in (22) is an integer. We now prove that the ratio (22) is a nondecreasing function of L. This is a key part of the proof of the main result of this section.

LEMMA 2. *Consider a* FGHSS *under the same hypotheses as in Theorem* 12. *Then the ratio* (22) *is a nondecreasing function of L.*

Proof. We will show that

$$\frac{\text{card Ra}\, M_{L+1}}{\text{card Ra}\, M_L} \geqslant \frac{\text{card Ra}\, M_L}{\text{card Ra}\, M_{L-1}}\,.$$

For any $\alpha \in \operatorname{Ra} A_{L+1} \cap \operatorname{Ra} D_{L+1}$ there exist $u_0, u_1, \ldots, u_L$ such that

$$\alpha = \begin{bmatrix} T_0(u_0) \\ T_1(u_0) \\ \vdots \\ T_L(u_0) \end{bmatrix} = \begin{bmatrix} e \\ T_0(u_1) \\ \vdots \\ T_0(u_L) + \cdots + T_{L-1}(u_1) \end{bmatrix}.$$

We define $\alpha^c \in \operatorname{Ra} A_L \cap \operatorname{Ra} D_L$ as the first L "components" of α

$$\alpha^c = \begin{bmatrix} T_0(u_0) \\ \vdots \\ T_{L-1}(u_0) \end{bmatrix} = \begin{bmatrix} e \\ \vdots \\ T_0(u_{L-1}) + \cdots + T_{L-2}(u_1) \end{bmatrix}.$$

We wish to find an upper bound on the number of $\alpha \in \operatorname{Ra} A_{L+1} \cap \operatorname{Ra} D_{L+1}$ that yield the same $\alpha^c \in \operatorname{Ra} A_L \cap \operatorname{Ra} D_L$. Thus suppose $\alpha \neq \beta$, but $\alpha^c = \beta^c$. This is the same as saying there exist u and v such that

$$\alpha = A_{L+1}(u) \neq A_{L+1}(v) = \beta$$

but

$$\alpha^c = A_L(u) = A_L(v) = \beta^c.$$

That is

$$u - v \in \ker A_L \qquad u - v \notin \ker A_{L+1}. \tag{25}$$

It is clear that $\ker A_{L+1} < \ker A_L$, and in fact is a normal subgroup because U is abelian. Thus $\ker A_L / \ker A_{L+1}$ is a group with cardinality

$$\operatorname{card} \frac{\ker A_L}{\ker A_{L+1}} = \frac{\operatorname{card} \ker A_L}{\operatorname{card} \ker A_{L+1}} \triangleq q_L. \tag{26}$$

Then, given u and v satisfying (25), we see that they must be elements of *distinct cosets* in $\ker A_L / \ker A_{L+1}$, and therefore for any $\gamma \in \operatorname{Ra} A_L \cap \operatorname{Ra} D_L$ there are *at most* q_L $\alpha \in \operatorname{Ra} A_{L+1} \cap \operatorname{Ra} D_{L+1}$ such that $\gamma = \alpha^c$. Thus

$$\operatorname{card}[\operatorname{Ra} A_{L+1} \cap \operatorname{Ra} D_{L+1}] \leqslant q_L \operatorname{card}[\operatorname{Ra} A_L \cap \operatorname{Ra} D_L]. \tag{27}$$

Also, by the First Isomorphism Theorem

$$\operatorname{Ra} A_k \approx U / \ker A_k \tag{28}$$

and (26) implies card Ra $A_k \backslash$card Ra A_j if $k > j$, so

$$\frac{\operatorname{card} \operatorname{Ra} A_{L+1}}{\operatorname{card} \operatorname{Ra} A_L} = \frac{\operatorname{card} \ker A_L}{\operatorname{card} \ker A_{L+1}} = q_L \tag{29}$$

(i.e., the cardinality of the range increases at the same rate as the cardinality of the kernel decreases—this is the analog of the linear algebra result dim Range + dim Nullspace = dim Domain). Combining (22), (27), and (29), we have

$$\frac{\text{card Ra}\, M_{L+1}}{\text{card Ra}\, M_L} = \frac{\text{card Ra}\, A_{L+1}}{\text{card}[\text{Ra}\, A_{L+1} \cap \text{Ra}\, D_{L+1}]}$$

$$\geqslant \frac{q_L\, \text{card Ra}\, A_L}{q_L\, \text{card}[\text{Ra}\, A_L \cap \text{Ra}\, D_L]} = \frac{\text{card Ra}\, M_L}{\text{card Ra}\, M_{L-1}},$$

We now wish to bound the maximum possible value for the minimum delay in any inverse of an abelian FGHSS. We put the direct product structure on U^k and Y^k. Using (28), (22), and the fact that $\text{Ra}\, A_k \cap \text{Ra}\, D_k < \text{Ra}\, A_k$, we can show that

$$\frac{\text{card Ra}\, M_{k+1}}{\text{card Ra}\, M_k} \Big\backslash m = \text{card}\, U. \tag{30}$$

Suppose no inverse with delay L exists. Then no inverse with delay less than L exists, and therefore

$$\frac{\text{card Ra}\, M_{k+1}}{\text{card Ra}\, M_k} < m \qquad k = 0,\ldots, L, \tag{31}$$

where

$$\text{card Ra}\, M_0 \triangleq 1. \tag{32}$$

Define

$$s_m = \text{the smallest integer greater than 1 that divides } m \tag{33}$$

$$r_m = \text{the largest integer less than } m \text{ that divides } m (= m/s_m). \tag{34}$$

Combining (30)–(34), we have

$$\text{card Ra}\, M_{L+1} \leqslant r_m\, \text{card Ra}\, M_L \leqslant r_m{}^2\, \text{card Ra}\, M_{L-1} \leqslant \cdots \leqslant r_m^{L+1} \tag{35}$$

(we note that one can show that (35) holds if and only if the system is not L-invertible). Since $M_{L+1} : U^{L+1} \to Y^{L+1}$ and card $U^{L+1} = m^{L+1}$, we have

$$\text{card ker}\, M_{L+1} \geqslant s_m^{L+1}. \tag{36}$$

We now restrict our attention to ker $M_{L+1} \triangleq \mathcal{N}_{L+1}$. We now assume that $u(0),\ldots, u(L) \in \mathcal{N}_{L+1}$ have been applied, and we apply another input

$u(L+1) \in U$. The set $\mathscr{N}_{L+1} \times U$ of such input strings is a subgroup of U^{L+2} and, referring to (36)

$$\mathrm{card}(\mathscr{N}_{L+1} \times U) \geqslant m s_m^{L+1}. \tag{37}$$

Consider the input-state map $E_{L+1} : \mathscr{N}_{L+1} \times U \to X$

$$E_{L+1}(u(0),..., u(L+1)) = b[u(L+1)] + ab[u(L)] + \cdots + a^{L+1}b[u(0)].$$

This is a homomorphism, and, if $\mathrm{card}(\mathscr{N}_{L+1} \times U) > n = \mathrm{card}\, X$, E_{L+1} has a nontrivial kernel—i.e., there exists a string $u(0),..., u(L+1)$ not identically zero such that $y(1) = y(2) = \cdots = y(L+1) = e$ $((u(0),..., u(L)) \in \mathscr{N}_{L+1})$ and $x(L+2) = e$. Thus the output response to the string $u(0),..., u(L+1)$, e, e,..., is the same as that to the all identity sequence. Thus the system is not invertible. Referring to (37), we see that the hypothesis $\mathrm{card}(\mathscr{N}_{L+1} \times U) > n$ holds if

$$m s_m^{L+1} \geqslant n + 1.$$

Thus, the smallest L such that this holds is

$$L_0 = \left\lceil \log_{s_m} \left(\frac{n+1}{m}\right) \right\rceil - 1 \triangleq q\left(m, \frac{n+1}{m}\right) - 1, \tag{38}$$

where $\lceil x \rceil$ = smallest integer $\geqslant x$. We have proven the following:

THEOREM 13. *Consider an abelian* FGHSS *with* card $U = m$, card $X = n$. *Then if the system does not have an inverse with delay* L_0, *where* L_0 *is given by* (38), *it is not invertible. Also the system is* L_0 *invertible if and only if we have the following condition*: *given* $u(0),..., u(L_0 + 1)$, *such that the output of the system* (*started at* $x(0) = e$) *in response to this string followed by all e's is identically e, then* $u(0) = \cdots = u(L_0 + 1) = e$. ▌

This result is the analog of Theorem 11. We also have the following results which are the analogs of the corollaries to Theorem 11.

COROLLARY 1. *An abelian* FGHSS *is invertible if and only if*

$$\ker P = \{e\},$$

where P: $U^{L_0+1} \to Y^{L_0+k(n)+1}$ is defined by

$$P[u(0),\dots, u(L_0+1)] = \begin{bmatrix} cb[u(0)] \\ cab[u(0)] + cb[u(1)] \\ \vdots \\ ca^{L_0+1}b[u(0)] + ca^{L_0}b[u(1)] + \cdots + cb[u(L_0+1)] \\ ca^{L_0+2}b[u(0)] + \cdots + cab[u(L_0+1)] \\ \vdots \\ ca^{L_0+k(n)}b[u(0)] + \cdots + ca^{k(n)-1}b[u(L_0+1)] \end{bmatrix} \tag{39}$$

and $k(n)$ is given by (5). *That is, the system is invertible if and only if*

$$\text{card Ra } P = mq(m, (n+1)/m).$$

Proof. By Theorem 13, our system is invertible if and only if the response to $u(0),\dots, u(L_0+1), e, e,\dots$ is not all e's if any of the $u(i) \neq e$. The map P gives the first $L_0 + k(n) + 1$ outputs in response to this sequence. Let

$$x = a^{L_0+1}b[u(0)] + a^{L_0}b[u(1)] + \cdots + b[u(L_0+1)].$$

Then the last $k(n)$ outputs in (39) are $c(x)$, $ca(x),\dots, ca^{k(n)-1}(x)$. If these are all equal to e, then, by Theorem 4, $ca^k(x) = e\ \forall k \geqslant 0$. Thus, we need only check the kernel of P to see if the system is invertible. ▮

Corollary 2. *An abelian* FGHSS *is invertible if and only if*

$$\text{card Ra } M_{L_0+1} \geqslant r_m^{L_0+1} + 1.$$

Proof. This follows from (35). ▮

We note that one can make comments relating these results to the LSC results much like those comments made in Willsky (1973a), and we refer the reader to those remarks.

5. Several Examples and the Construction of Inverses

We first present three examples illustrating several points concerning invertible FGHSS's. The first example shows that the bound in Theorem 13 can be realized.

Example 1. Let $U = Y = Z_2$, $X = Z_2{}^r$ with $r \geqslant 2$ and define a: $X \to X$, b: $U \to X$, c: $X \to Y$ as follows:

$$\begin{aligned} a(x_1, \dots, x_r) &= (0, x_1, \dots, x_{r-1}), \\ b(x) &= (x, 0, \dots, 0), \\ c(x_1, \dots, x_r) &= x_r . \end{aligned}$$

Then

$$\begin{aligned} cb = cab = \cdots &= ca^{r-2} = 0, \\ ca^{r-1}b &= \text{identity}. \end{aligned}$$

Thus the system is $(r - 1)$-invertible but not k-invertible for $k < (r - 1)$, and

$$L_0 = q(2, 2^{r-1} + \tfrac{1}{2}) - 1 = r - 1.$$

Example 2. We next consider an abelian FGHSS that is not a LSC. Let $U = Z_3 \times Z_2$, $X = Z_6 \times Z_6$, $Y = Z_6$ and define the homomorphisms a: $X \to X$, b: $U \to X$, c: $X \to Y$ by

$$\begin{aligned} a(x, y) &= (x + y, x), \\ b(1, 1) &= (2, 3), \\ c(x, y) &= x. \end{aligned}$$

We can check that this system is controllable and observable. Also, consider the definitions of A_k and D_k in (11) and (12). We compute

$$\begin{aligned} \operatorname{Ra} A_1 &= \{0, 2, 4\} < Y, \\ \operatorname{Ra} A_2 &= \{(0, 0), (2, 2), (4, 4), (0, 3), (2, 5), (4, 1)\} < Y^2, \\ \operatorname{Ra} D_1 &= \{0\}, \\ \operatorname{Ra} D_2 &= \{(0, 0), (0, 2), (0, 4)\}. \end{aligned}$$

Then using (22)

$$\frac{\text{card Ra } M_1}{\text{card Ra } M_0} = \frac{\text{card Ra } A_1}{\text{card}[\text{Ra } A_1 \cap \text{Ra } D_1]} = 3$$

$$\frac{\text{card Ra } M_2}{\text{card Ra } M_1} = 6 = \text{card } U,$$

so no inverse of delay zero exists, but an inverse of delay one does.

EXAMPLE 3. Finally, we give a nonabelian example. We define the *quaternion group* Q as the group of order 8 having two generators p and t satisfying the relations

$$p^4 = e \qquad t^2 = p^2 \qquad pt = tp^3.$$

This group is isomorphic to the group of 2 × 2 complex matrices (under matrix multiplication) generated by

$$P = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \qquad T = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

The quaternion group is also isomorphic to the set $\{\pm 1, \pm i, \pm j, \pm k\}$ under the operation

$$i^2 = j^2 = k^2 = -1 \qquad ij = -ji = k \qquad jk = -kj = i \qquad ki = -ik = j.$$

One should note that Q is a *hamiltonian group* (Rotman, 1965)—i.e., all its subgroup are normal. Thus, since the product of normal subgroups is a subgroup, the reachable set for any FGHSS with Q or any other hamiltonian group as the state group is a group.

Consider the following FGHSS: $U = Z_4$, $X = Q \times Q$, $Y = Q$, and define $b\colon U \to X$, $c\colon X \to Y$, and $a\colon X \to X$ to be the homomorphisms uniquely defined by

$$\begin{aligned} b(1) &= (e, p), \\ c(q_1, q_2) &= q_1 \quad \forall q_1, q_2 \in Q, \\ a(q_1, q_2) &= (f(q_2), q_1) \quad \forall q_1, q_2 \in Q, \end{aligned}$$

where $f\colon Q \to Q$ is the homomorphism uniquely defined by

$$f(p) = p^3t \qquad f(t) = t.$$

One can check that this system is controllable and observable. Also

$$\begin{aligned} \operatorname{Ra} A_1 &= \{e\} < Y, \\ \operatorname{Ra} A_2 &= \{(e, e), (e, p^3t), (e, p^2), (e, pt)\} < Y, \\ \operatorname{Ra} D_2 &= \{(e, e)\} < Y, \end{aligned}$$

so from (13)

$$\begin{aligned} \operatorname{card} \operatorname{Ra} M_1 &= 1, \\ \operatorname{card} \operatorname{Ra} M_2 &= 4 = \operatorname{card} U. \end{aligned}$$

Thus no zero delay inverse exists but a one-delay inverse does.

We now briefly consider the construction of inverses for FGHSS's. We will explicitly consider the analog of Theorem 5 in Massey and Sain (1968). Suppose $T_0, \ldots, T_{i-1}$ are the trivial homomorphism (map everything onto e), and T_i is one-to-one. We then have

$$\begin{aligned} y(1) &= y(2) = \cdots = y(i) = e, \\ y(k+i+1) &= T_i[u(k)]\, ca^{i+1}[x(k)]. \end{aligned} \tag{40}$$

We now must make an assumption that is not necessary for LSC's but is for FGHSS's (even in general for abelian FGHSS's). We assume that there is a normal subgroup N of Y and a homomorphism θ: $T_i(U) \to \mathrm{Aut}(N)$ (the group of automorphisms of N) such that

$$Y \simeq N x_\theta T_i(U). \tag{41}$$

The First Isomorphism Theorem tells us that $U \simeq T_i(U)$, and (41) implies that there exists a homomorphism M: $Y \to U$ such that $M \circ T_i \in \mathrm{Aut}(U)$. Then from (40)

$$\begin{aligned} u_k &= (M \circ T_i)^{-1}\, [M[y(k+i+1)]\, Mca^{i+1}[x(k)^{-1}]], \\ x_{k+1} &= \{b(M \circ T_i)^{-1}\, M[y(k+i+1)]\}\{b(M \circ T_i)^{-1}\, Mca^{i+1}[x(k)^{-1}]\}\, a(x_k). \end{aligned}$$

These equations define an inverse of our FGHSS, but it may not be homomorphic. Indeed, although it is homomorphic if the system is abelian, it is *not* homomorphic in any other case because the map

$$x \mapsto x^{-1}$$

is not a homomorphism (it is an anti-homomorphism—i.e.,

$$f(xy) = f(y) f(x)).$$

Example 4. We present two examples that show that (41) need not hold—i.e., we will choose U, Y and f: $U \to Y$ a homomorphism with $\ker f = \{e\}$ such that there exists *no* homomorphism g: $Y \to U$ such that $g \circ f \in \mathrm{Aut}(U)$. Let $U = Z_4$, $Y = \{e, x, x^2, x^3, y, xy, x^2y, x^3y \mid x^4 = y^2 = e;\ xyx = y\}$, and

$$f(n) = x^n \qquad n = 0, 1, 2, 3.$$

The reader can check that there is no g in this case. A second example indicates that we still have problems even in the abelian case. Let $U = Z_2$, $Y = Z_4$ and

$$f(0) = 0 \qquad f(1) = 2.$$

The reader can check that again there is no g.

We refer the reader to Rotman (1965) to see that there exists a homomorphism M: $Y \to U$ such that $M \circ T_i \in \mathrm{Aut}(U)$ if and only if (41) holds.

6. Conclusions

In this paper we have studied the invertibility properties of a class of systems evolving homomorphically on finite groups. Although this setting is much more general than that for the class of linear sequential circuits, we have been able to derive results that are strikingly similar to those for LSC's. We have obtained the analog of one characterization (Massey and Sain, 1968) of LSC invertibility for the full class of FGHSS's, and, after restricting our attention to abelian systems, we have derived the analog of another LSC result (Sain and Massey, 1969; Brockett and Mesarovic, 1965; Willsky, 1974).

Several problems associated with the lack of a vector space setting for FGHSS's have been encountered, and it is precisely these difficulties that make our results all the more interesting. That is, our work indicates that many of the results for linear systems do not require all of the structure provided by the vector space setting, while other results—such as the construction of inverse systems—do not extend quite as readily to more general settings. It is hoped that our results will aid in the development of a universal theory of dynamical systems by placing into proper perspective many of the concepts first developed in the linear system setting.

Finally, we have presented several examples of invertible FGHSS's. The theory of finite groups is so rich that it is strongly felt that the class of invertible FGHSS's is quite large. Noting that the class of convolutional encoders (Forney, 1970) is a relatively small subclass of the class of FGHSS's, it is hoped that our results will lead to the development of new types of sequential coding systems.

Received: October 15, 1973; revised: July 17, 1974

References

BROCKETT, R. W. AND MESAROVIC, M. D. (1965), The reproduciblity of multivariable systems, *J. Math. Anal. Appl.* **11**, 548–563.

BROCKETT, R. W. AND WILLSKY, A. S. (1972), Finite group homomorphic sequential systems, *IEEE Trans. Automatic Control* **AC-17**, 483–490.

BROCKETT, R. W. AND WILLSKY, A. S. (1974), Some structural properties of automata defined on groups, *in* "Proceedings of the First International Symposium on Category Theory Applied to Computation and Control" (E. G. Manes, Ed.), Dept. of Mathematics and Dept. of Computer and Information Science, Univ. of Massachusetts at Amherst.

FORNEY, G. D., JR. (1970), Convolutional codes I: Algebraic structure, *IEEE Trans. Inform. Theory* **IT-16**, 720–738.

MASSEY, J. L. AND SAIN, M. K. (1968), Inverses of linear sequential cricuits, *IEEE Trans. Computers* **C-17**, 330–337.

OLSON, R. R. (1970), On the invertibility of finite state machines, Dept. of Elec. Eng., Univ. of Notre Dame, Tech. Rept. EE-703.

SAIN, M. K. AND MASSEY, J. L. (1969), Invertibility of linear time-invariant dynamical systems, *IEEE Trans. Automatic Control* **AC-14**, 141–149.

ROTMAN, J. (1965), "The Theory of Groups: An Introduction," Allyn and Bacon, Boston.

WILLSKY, A. S. (1973a), "Dynamical Systems Defined on Groups: Structural Properties and Estimation," Ph.D. Thesis, Department of Aeronautics and Astronautics, M.I.T.

WILLSKY, A. S. (1973b), "Invertibility Conditions for a Class of Finite State Systems Evolving on Groups," Proceedings of the Eleventh Allerton Conference, Univ. of Illinois.

WILLSKY, A. S. (1974), On the invertibility of linear systems, *IEEE Trans. Automatic Control* **AC-19**, 272–274.