Inverses of Linear Sequential Circuits

JAMES L. MASSEY, MEMBER, IEEE, AND MICHAEL K. SAIN, MEMBER, IEEE

Abstract—**This paper states the necessary and sufficient conditions for the existence of a feedforward inverse for a feedforward linear sequential circuit and gives an implicit procedure for constructing such inverses. It then goes on to give the necessary and sufficient conditions for the existence of general inverses with finite delay and gives procedures for constructing a class of such inverses. The discussion considers both the transfer function matrix description and the structural matrix description of the linear sequential circuit, together with the complementary nature of the results obtained from these two viewpoints. Finally, a large part of the work is motivated by results and techniques which have been applied in the study of continuous-time linear dynamical systems and thus serves to point out the advantages which may accrue through simultaneous study of both continuous-time systems and linear sequential circuits.**

Index Terms—**Convolution codes, feedforward sequential circuits, information lossless, inverses, linear sequential circuits.**

I. Introduction

THE STUDY of linear sequential circuits is well established as a "classical" subfield of automata theory by virtue of the depth and breadth of known results. This paper considers an aspect of the theory of linear sequential machines that seems to have received little attention, namely, the existence and construction of inverse circuits. Intuitively, a sequential circuit with N inputs and K outputs is an "inverse with delay L" for a linear sequential circuit with K inputs and N outputs if the former circuit, when cascaded with the latter, yields an overall sequential circuit which acts as a pure delay of L time units. An inverse with delay $L=0$ is called an "instantaneous" inverse.

In Section II, it is shown that a practical problem in error-correcting codes raises an interesting theoretical question concerning inverses, namely, when does a feedforward linear sequential circuit possess a feedforward inverse? A complete answer is provided in Sections III and IV, including an implicit construction technique when the inverse exists.

In Section V, the existence of inverses is treated in a more formal manner. A necessary and sufficient condition is given for the existence of an inverse with delay L in terms of the structural matrices which characterize the linear sequential circuit.

Finally, in Section VI, a construction procedure for inverses is formulated by analogy to techniques used in the study of linear dynamical systems. This construction technique proceeds from the structural matrices of the original linear sequential circuit to the structural matrices of the inverse.

Manuscript received August 28, 1967; revised January 4, 1968. This work was supported in part by National Science Foundation Grant GK 804. A preliminary version of these results was presented at the 8th Annual Symposium on Switching and Automata Theory, Austin, Tex., October 1967.

The authors are with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, Ind. 46556

II. Convolutional Codes and Feedforward Inverses

The class of error-correcting codes known as convolutional codes is becoming increasingly important in coding theory because of ease in implementation, suitability for sequential decoding, and certain inherent superiorities relative to block codes.[1] Convolutional codes may be conveniently described from a sequential circuit point of view,[2] and this description leads to an interesting problem concerning the existence of a special kind of inverse.

Let $i_j(0)$, $i_j(1)$, $i_j(2)$, $\cdots$, be a sequence of digits from a finite field $GF(q)$. The D transform of such a sequence will be denoted as

$$I_j(D) = i_j(0) + i_j(1)D + i_j(2)D^2 + \cdots.$$

Let $I_j(D)$, $j=1, 2, \cdots, K$ be considered as the transforms of K sequences of information digits to be encoded in a convolutional code of rate $R=K/N$. Such a code is defined by a set of polynomials, $G_{ij}(D)$, $i=1, 2, \cdots, N$, $j=1, 2, \cdots, K$, over $GF(q)$, called the "code-generating polynomials,"[3] such that the transforms of the N sequences of encoded digits $T_i(D)$, $i=1, 2, \cdots, N$ may be written as

$$T_i(D) = \sum_{j=1}^{K} G_{ij}(D)I_j(D). \tag{1}$$

Equation (1) may be written in matrix form as

$$\boldsymbol{T}(D) = \overline{\boldsymbol{G}}(D)\boldsymbol{I}(D) \tag{2}$$

where $\overline{\boldsymbol{G}}(D)$ is the $N\times K$ matrix whose ijth entry is $G_{ij}(D)$, and where $\boldsymbol{T}(D)$ and $\boldsymbol{I}(D)$ are vectors whose components are $T_j(D)$ and $I_j(D)$, respectively.

From a sequential circuit viewpoint, $\overline{\boldsymbol{G}}(D)$ can be interpreted as the transfer function matrix of a K-input N-output "linear sequential circuit" (LSC). The fact that these transfer functions are all polynomials specifies the LSC as having finite input-memory, that is, as having a "feedforward" (FF) realization in terms of delay units, $GF(q)$ adders, and $GF(q)$ scalors. From the coding standpoint, it is essential that this LSC should also possess an FF inverse, either instantaneous or with delay, so that decoding errors made on the corrupted encoded sequences received at the decoder do not interfere indefinitely with the recovery of the information sequences.

As an illustration of the necessity of this latter condition, consider the $K=1$, $N=2$ binary code with $G_{11}(D)=1+D$ and $G_{21}(D)=1+D^2$. The all-one information sequence with transform $I_1(D)=1/(1+D)$ then results in the encoded sequences having the transforms $T_1(D)=1$ and $T_2(D)=1+D$ which contain only three nonzero digits. If these digits are changed to zeros by the channel, the decoder will estimate $T_1(D)=T_2(D)=0$, and hence $I_1(D)=0$, since the actual received sequence is a valid encoded sequence. Thus, although only three errors have been made in decoding the received sequences, every information digit is decided incorrectly; that is, the decoding errors are never forgotten in passing from the encoded sequences to the information sequence. However, for the code $G_{11}(D)=1+D$ and $G_{21}(D)=1+D+D^2$, it is seen immediately that $DT_1(D)+T_2(D)=(D+D^2+1+D+D^2)I_1(D)=I_1(D)$, so that an FF inverse exists for the encoding LSC and decoding errors are forgotten after one time unit in recovering the information sequence from the encoded sequences.

The discussion above has singled out the following problem in automata theory as being of practical import in connection with convolutional coding: under what conditions does an FF LSC possess an FF inverse, either instantaneous or with delay? The solution to this problem is given in Sections III and IV.

In conclusion of Section II, it is convenient to prove a lemma which is useful in demonstrating when an FF inverse does not exist.

Lemma 1: If for a given LSC there exists an input sequence with infinitely many nonzero digits such that the corresponding output sequence has only finitely many nonzero digits, then the LSC has no FF inverse, with delay or without delay.

Proof: Note that the term sequence is used in the vector sense. It is assumed that no digits are stored in the encoder at the start of the information sequence. Accordingly, the all-zero information sequence yields the all-zero encoded sequence. Therefore, the all-zero encoded sequence must always be inverted as the all-zero information sequence. Hence if the inverse has input-memory M, then M time units after its last nonzero input it must commence to produce only zeros. Thus, the information sequence hypothesized in the lemma could not be recovered, and no finite-input-memory inverse can exist.

III. Single-Input LSCs and FF Inverses

Let $p_1(D)$, $p_2(D)$, $\cdots$, $p_n(D)$ be polynomials over some field. Their greatest common divisor, denoted

$$\text{GCD}\,[p_1(D), p_2(D), \cdots, p_n(D)],$$

is the monic (highest coefficient unity) polynomial of greatest degree which divides each polynomial. It is known[4] that there exist polynomials $a_1(D), a_2(D), \cdots, a_n(D)$ such that

$$a_1(D)p_1(D) + \cdots + a_n(D)p_n(D) = \text{GCD}\,[p_1(D), \cdots, p_n(D)]. \quad (3)$$

With this preliminary, the problem posed in the previous section is readily solved for the single-input ($K=1$) case.

Theorem 1: A single-input N-output FF LSC has an FF inverse, either with delay or without delay, if and only if

$$\text{GCD}\,[G_{11}(D), G_{21}(D), \cdots, G_{N1}(D)] = D^L \quad (4)$$

for some $L \geq 0$. Moreover, there exists an FF inverse with delay exactly L, and no inverse of any kind exists with smaller delay.

Proof: Suppose first that (4) is satisfied for some $L \geq 0$. Then by (3) there exist polynomials $Q_1(D)$, $Q_2(D)$, $\cdots$, $Q_N(D)$ such that

$$Q_1(D)G_{11}(D) + Q_2(D)G_{21}(D) + \cdots + Q_N(D)G_{N1}(D) = D^L. \quad (5)$$

When multiplied by $I_1(D)$, (5) becomes

$$Q_1(D)T_1(D) + Q_2(D)T_2(D) + \cdots + Q_N(D)T_N(D) = D^L I_1(D), \quad (6)$$

and hence the $Q_i(D)$ are the transfer functions of an N-input single-output FF LSC which recovers $I_1(D)$ with delay exactly L.

Conversely, suppose that (4) is violated, that is, there exists no non-negative integer L such that (4) is satisfied. Then there exists a polynomial $P(D)$ with $P(0)\neq 0$ and of degree at least one such that $P(D)$ divides $G_{j1}(D)$ for $j=1, 2, \cdots, N$. The input sequence whose transform is $I_1(D)=1/P(D)$ then contains infinitely many nonzero digits, but each output sequence $T_j(D)=G_{j1}(D)/P(D)$ is a polynomial and hence has only finitely many nonzero digits. From Lemma 1, it follows that no FF inverse exists.

Finally, if (4) is satisfied, each $G_{j1}(D)$ has D^L as a factor, and thus there is no nonzero response until L time units after an input is applied. Thus no inverse can have delay less than L.

The simplicity of the single-input case does not extend to the multiple-input situation which is treated in Section IV. It is important to remark, however, that the single-input problems are of greatest current interest in the theory of convolutional codes.

IV. Multiple-Input LSCs and FF Inverses

In the general case, $\overline{G}(D)$ is an $N\times K$ matrix having $\binom{N}{K}$ distinct $K\times K$ submatrices. Let $\Delta_i(D)$, $i=1, 2, \cdots, \binom{N}{K}$ denote the determinants of these submatrices. In terms of these quantities, the main result of this section can be stated as follows.

Theorem 2: A K-input N-output FF LSC has an FF inverse, either with delay or without delay, if and only if

$$\mathrm{GCD}\left[\Delta_i(D), i = 1, 2, \cdots, \binom{N}{K}\right] = D^L \qquad (7)$$

for some $L \geq 0$. Moreover, there exists an FF inverse with delay exactly L. (But, for $K>1$, there may exist FF inverses with delay less than L.)

Proof of Sufficiency of Condition (7): Let $\overline{G}(D)_n$ denote the nth $K \times K$ submatrix of $\overline{G}(D)$, and let $\overline{C}(D)_n$ be the matrix whose ijth element is the cofactor of the jith element of $\overline{G}(D)_n$. Note that the entries in $\overline{C}(D)_n$ are polynomials. Also, let $T(D)_n$ be the vector of K output transforms corresponding to the rows used to form $\overline{G}(D)_n$. Clearly,

$$\overline{C}(D)_n \overline{G}(D)_n = \Delta_n(D) \bar{I}_K, \qquad (8)$$

where $\bar{I}_K$ is the $K \times K$ identity matrix. Upon postmultiplying both sides of (8) by $I(D)$, it follows that

$$\overline{C}(D)_n T(D)_n = \Delta_n(D) I(D). \qquad (9)$$

From (9), it is seen that FF LSC's with transfer function matrices $\overline{C}(D)_n$ can be used to produce $\Delta_n(D) I_j(D)$, for each j and for $n = 1, 2, \cdots, \binom{N}{K}$. In addition, if condition (7) is satisfied, it is possible to find a further FF circuit to act on these $\binom{N}{K}$ outputs $\Delta_n(D) I_j(D)$, in accordance with Theorem 1, to produce the final output sequence $D^L I_j(D)$. The cascade of these FF LSCs is then an FF inverse with delay exactly L.

Before proceeding to the proof of necessity in Theorem 2, it is useful first to obtain certain ancillary results. Recall that a polynomial is called "irreducible" if it has degree at least one and cannot be expressed as the product of polynomials of a smaller degree. An irreducible factor $m(D)$ of a polynomial $P(D)$ has "multiplicity" e if $[m(D)]^e$ divides $P(D)$ but $[m(D)]^{e+1}$ does not.

Lemma 2: If $\Delta_n(D)$, the determinant of $\overline{G}(D)_n$, is nonzero and has an irreducible factor $m(D)$ of multiplicity e, then there is some element of $\overline{G}(D)_n$ whose cofactor is not divisible by $[m(D)]^e$.

Proof: From (8), it is seen that

$$[\Delta_n(D)] \times \det [\overline{C}(D)_n] = [\Delta_n(D)]^K, \qquad (10)$$

or equivalently

$$\det [\overline{C}(D)_n] = [\Delta_n(D)]^{K-1}.$$

But if every cofactor has $[m(D)]^e$ as a factor, then the left-hand side of (10) has $m(D)$ as an irreducible factor of multiplicity at least Ke. The right member of (10), however, has $m(D)$ as an irreducible factor of multiplicity only $(K-1)e$. The lemma follows, therefore, by contradiction.

Lemma 3: Under the hypothesis of Lemma 2, there exists a vector of polynomials $P(D) = (P_1(D), \cdots, P_K(D))$ such that for at least one index r, $[m(D)]^e$ does not divide $P_r(D)$, and such that

$$\overline{G}(D)_n P(D) = \Delta_n(D) Q(D), \qquad (11)$$

where $Q(D) = (Q_1(D), \cdots, Q_K(D))$ is also a vector of polynomials.

Proof: By Lemma 2, there is some row of $\overline{C}(D)_n$, say the rth, whose greatest common divisor $P_r(D)$ is not divisible by $[m(D)]^e$. Further, there exist polynomials $Q_1(D), \cdots, Q_K(D)$ such that

$$P_r(D) = Q_1(D) C_{r1}(D)_n + \cdots + Q_K(D) C_{rK}(D)_n,$$

where $C_{ij}(D)_n$ denotes the ijth element of $\overline{C}(D)_n$. Define $P_i(D)$, $i \neq r$, from the relation

$$P(D) = \overline{C}(D)_n Q(D). \qquad (12)$$

Multiplying both sides in (12) by $\overline{G}(D)_n$, (11) follows, and the lemma is proved.

Lemma 4: For any polynomial vector $P(D)$ satisfying (11), and for any index j, $1 \leq j \leq N$, the jth row of $\overline{G}(D)$ satisfies

$$\sum_{i=1}^{K} G_{ji}(D) P_i(D) = \Delta(D) A_j(D), \qquad (13)$$

where $\Delta(D) = \mathrm{GCD}\ [\Delta_i(D),\ i = 1,\ 2, \cdots, \binom{N}{K}]$ and $A_j(D)$ is some polynomial.

Proof: If j corresponds to one of the rows of $\overline{G}(D)_n$, then (13) follows directly from (11). For other j, define the polynomials $B_1(D), \cdots, B_K(D)$ as the solutions of

$$[B_1(D), \cdots, B_K(D)] \overline{G}(D)_n = \Delta_n(D) [G_{j1}(D), \cdots, G_{jk}(D)]. \qquad (14)$$

Postmultiplying by $\overline{C}(D)_n$ in (14), it follows that

$$[B_1(D), \cdots, B_K(D)] = [G_{j1}(D), \cdots, G_{jK}(D)] \overline{C}(D)_n \qquad (15)$$

from which it is seen that each $B_i(D)$ is the determinant of some $K \times K$ submatrix of $\overline{G}(D)$ and hence is divisible by $\Delta(D)$, the greatest common divisor of these determinants. Moreover, upon postmultiplying by $P(D)$ in (14), (11) implies

$$[B_1(D), \cdots, B_K(D)] Q(D) = \sum_{i=1}^{K} G_{ji}(D) P_i(D). \qquad (16)$$

Defining the left member of (16) as $A_j(D)\ \Delta(D)$ gives (13).

With the completion of these preliminaries, it is possible to return to the question of necessity in Theorem 2.

Proof of the Necessity of Condition (7): Suppose that the greatest common divisor $\Delta(D)$ of the $\Delta_i(D)$ is not D^j for some j and further suppose that $\Delta(D) \neq 0$. Then let $m(D) \neq D$ be an irreducible factor of $\Delta(D)$ of multiplicity e. There is then some index, say n, such that

$\Delta_n(D)$ has $m(D)$ as an irreducible factor of multiplicity exactly e. For this n, define $\boldsymbol{P}(D)$ as the polynomial vector given in Lemma 3 and define the input sequences by the transforms

$$I_i(D) = P_i(D)/[m(D)]^e, \quad i = 1, 2, \cdots, K. \quad (17)$$

From Lemma 3, it follows that at least one of these input sequences has infinitely many nonzero digits. The corresponding output sequences have transforms given by

$$T_j(D) = \sum_{i=1}^{K} G_{ji}(D)I_i(D) = [\Delta(D)A_j(D)]/[m(D)]^e,$$
$$j = 1, 2, \cdots, N, \quad (18)$$

where (13) from Lemma 4 has been employed. But the right member of (18) is a polynomial since $[m(D)]^e$ divides $\Delta(D)$, so that there are only finitely many nonzero digits in each output sequence. By Lemma 1, no FF inverse exists. Hence, the necessity of condition (7) is established.

In coding theory, attention is often restricted to "systematic" codes in which $\overline{G}(D)_1 = \overline{I}_K$, so that condition (7) is automatically satisfied with $L=0$. However, nonsystematic codes are of special importance in connection with sequential decoding, so that condition (7) is one that should always be considered when choosing a nonsystematic convolutional code. It is interesting to note that if the $G_{ji}(D)$ are selected randomly, as is often considered in coding theory, then there is a significant probability that condition (7) will not be satisfied. For instance, with $K=1$ and $N=2$, the probability is 1/2 in the binary case that $G_{j1}(D), j=1, 2$ will have an even number of terms and hence be divisible by $(1+D)$. Thus, the probability is 1/4 that $\Delta(D)$ will have $(1+D)$ as a factor.

Theorems 1 and 2 are not restricted to systems defined over finite fields, but apply just as well to sampled-data circuits in which the field in question is that of the real numbers.

As an example of a case in which L in (7) is not the least delay for an FF inverse system, consider the K-input K-output LSC with $\overline{G}(D) = D\overline{I}_K$, where $\overline{I}_K$ is the $K \times K$ identity matrix. Clearly, there is an FF inverse with delay unity, but $\Delta(D) = D^K$ so that $L > 1$ if $K > 1$.

V. The Existence of Inverses with Delay L

In the preceding sections, LSCs have been characterized by their transfer function matrices. The alternative formulation in terms of the structural matrices $\overline{A}$, $\overline{B}$, $\overline{C}$, and $\overline{E}$ will be exploited in the sequel.

Let $i(k)$ denote the K vector whose components are the input digits at time unit k, $i_j(k)$, $j=1, 2, \cdots, K$. Similarly let $t(k)$ denote the N vector of output digits at time unit k. Then a "state vector" $x(k)$ having S components, and matrices $\overline{A}$, $\overline{B}$, $\overline{C}$, and $\overline{E}$ can be de-

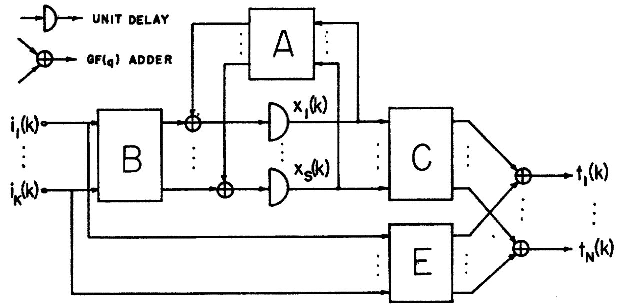

Fig. 1. Canonical realization of an LSC in terms of its structural matrices.

fined so that operation of the LSC may be expressed as[5]

$$x(k+1) = \overline{A}x(k) + \overline{B}i(k) \quad (19a)$$

$$t(k) = \overline{C}x(k) + \overline{E}i(k) \quad (19b)$$

for $k=0, 1, 2, \cdots$. It is assumed throughout the remainder of the paper that $x(0) = \mathbf{0}$, where $\mathbf{0}$ denotes the all-zero vector; that is, it is assumed that the LSC is initially at rest.

A canonical realization of the LSC in terms of its structural matrices is shown in Fig. 1. The state vector is taken as the outputs of a set of S unit delay stages. The blocks in the figure which are labelled with the structural matrices denote the necessary scalors (constant multipliers) and $GF(q)$ adders so that the vector output of the block is the associated matrix applied to the vector of inputs. Conversely, any LSC constructed from unit delays, scalors, and adders may be considered as in the canonical realization of Fig. 1, and its structural matrices may be readily determined. When desired, the transfer function matrix can always be found from the relation

$$\overline{G}(D) = \overline{C}[D^{-1}\overline{I}_S - \overline{A}]^{-1}\overline{B} + \overline{E}, \quad (20)$$

where the entries in (20) are, in general, rational functions in D rather than simply polynomials as was the case for the FF LSCs considered in Sections II through IV.

Under the assumption that $x(0) = \mathbf{0}$, (19) can be solved to obtain

$$t(0) = \overline{E}i(0) \quad (21a)$$

$$t(k) = \sum_{j=1}^{k} \overline{C}\overline{A}^{j-1}\overline{B}i(k-j) + \overline{E}i(k) \quad (21b)$$

for $k=1, 2, \cdots$. For convenience, introduce the notation

$$\overline{J}_0 = \overline{E}$$
$$\overline{J}_j = \overline{C}\overline{A}^{j-1}\overline{B}, \quad j = 1, 2, \cdots,$$

so that (21) can be rewritten as

$$t(k) = \sum_{j=0}^{k} \overline{J}_j i(k-j). \quad (22)$$

From (22), it follows that the response over the first $L+1$ time units is given by the matrix equation

$$\begin{bmatrix} t(0) \\ t(1) \\ \cdot \\ \cdot \\ t(L) \end{bmatrix} = \begin{bmatrix} \bar{J}_0 & \bar{0} & \cdots & \bar{0} \\ \bar{J}_1 & \bar{J}_0 & \cdots & \bar{0} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \bar{J}_L & \bar{J}_{L-1} & \cdots & \bar{J}_0 \end{bmatrix} \begin{bmatrix} i(0) \\ i(1) \\ \cdot \\ \cdot \\ i(L) \end{bmatrix} \tag{23}$$

which will be abbreviated to

$$T_L = \overline{M}_L I_L. \tag{24}$$

T_L, the left member of (23), is the "response segment" over time units 0 through L. Similarly, I_L is the "input segment" over the same period. $\overline{M}_L$ is the matrix which via (23) connects the output and input segments.

The following formal definition may now be stated.

Definition 1: An LSC "has an inverse with delay L" if for every non-negative integer k, the input segment I_k is uniquely determined by the response segment T_{k+L}.

From the linearity of an LSC, Theorem 3 readily follows.

Theorem 3: An LSC has an inverse with delay L if and only if I_0 is uniquely determined by T_L, that is, if and only if (24) may be uniquely solved for $i(0)$.

Proof: Necessity follows directly from Definition 1. Sufficiency may be shown as follows. Suppose $i(0)$ can be found from T_L. Then the effect of $i(0)$ on the entire output sequence can be subtracted out. The remaining modified output sequence, omitting the time-unit-0 portion, is the same as if $i(1)$ were the first input to the LSC. Hence $i(1)$ can also be found from its first $L+1$-time-unit portion. Thus I_1 can be found from T_{L+1}. By a similar argument I_k can be found from T_{L+k} for every k.

Now the rank of the matrix $\overline{M}_L$, denoted rank $(\overline{M}_L)$, is the maximum number of linearly independent columns (or rows) that can be found in $\overline{M}_L$. Alternatively, rank $(\overline{M}_L)$ is the dimension of the column space (or row space) of $\overline{M}_L$, that is, the dimension of the vector space consisting of all distinct linear combinations of columns (or rows) of $\overline{M}_L$.

It is now possible to state the main result of this section. By way of convention, rank $(\overline{M}_{-1})$ is taken to be 0.

Theorem 4: An LSC has an inverse with delay L if and only if

$$\text{rank}\,(\overline{M}_L) = \text{rank}\,(\overline{M}_{L-1}) + K, \tag{25}$$

where K is the number of inputs for the LSC.

As a simple example of this result, consider the binary LSC with $K=2$, $N=2$, and $S=1$, defined by

$$\bar{A} = [0], \quad \bar{B} = [0 \quad 1], \quad \bar{C} = [0 \quad 1]', \quad \bar{E} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},$$

where the superscript (′) denotes transposition. A simple calculation yields

$$\overline{M}_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \text{rank}\,(\overline{M}_0) = 1,$$

$$\overline{M}_1 = \left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{array}\right], \quad \text{rank}\,(\overline{M}_1) = 3,$$

so that an inverse with delay $L=1$ does exist but there is no inverse with delay $L=0$.

Before proving Theorem 4, it is convenient first to establish the following.

Lemma 5: An LSC has an inverse with delay L if and only if $T_L = \mathbf{0}$ implies that $i(0) = \mathbf{0}$.

Proof: From Theorem 3, it follows that an inverse with delay L exists if and only if the same T_L cannot result from two input segments I_L with differing values of $i(0)$. This latter condition, by linearity, is equivalent to the condition that the difference of these two input segments, which is an I_L with $i(0) \neq \mathbf{0}$, must not result in the response segment $T_L = \mathbf{0}$. But this is the condition in Lemma 5, which is thereby established.

Proof of Theorem 4: From (24) and Lemma 5, it follows that an inverse with delay L exists if and only if both of the following conditions are satisfied.

1) The first K columns of $\overline{M}_L$ are linearly independent, for otherwise and only then will there be an $i(0) \neq \mathbf{0}$, with $i(1) = i(2) = \cdots = i(L) = \mathbf{0}$, which results in $T_L = \mathbf{0}$.

2) The column space of the first K columns of $\overline{M}_L$ and the column space of the remaining KL columns of $\overline{M}_L$ have only $\mathbf{0}$ in common, for otherwise and only then will there be an $i(0) \neq \mathbf{0}$, together with values of $i(1)$, $i(2), \cdots, i(L)$ not all zero, such that $T_L = \mathbf{0}$.

Next note directly from (24) that the column space of the last KL columns of $\overline{M}_L$ has dimension just rank $(\overline{M}_{L-1})$. Moreover, conditions 1) and 2) above will both be satisfied if and only if adding the first K columns increases the dimension of the column space by K. Hence the theorem follows.

Similar arguments can be used to show that rank $(\overline{M}_L) -$ rank $(\overline{M}_{L-1})$ is a monotonically nondecreasing function of L. Since this difference is at most K, it follows that the following limit always exists

$$\lim_{L\to\infty} \frac{1}{K} [\text{rank}\,(\overline{M}_L) - \text{rank}\,(\overline{M}_{L-1})]$$

and equals unity when and only when there is some finite L such that an inverse with delay L exists.

In the proof of Theorem 4, condition 1), namely that the first K columns of $\overline{M}_L$ are linearly independent, has an interesting interpretation. These K columns are partitioned by rows into the blocks $\bar{J}_0, \bar{J}_1, \cdots, \bar{J}_L$, which is evident in (23). Condition 1) can then be restated as a corollary.

Corollary 1: An LSC has an inverse with delay L only if

$$\operatorname{rank}(\bar{J}_0' \bar{J}_1' \cdots \bar{J}_L') = K. \tag{26}$$

By the Cayley–Hamilton result and Corollary 1 the necessary condition (26) can be strengthened to the following corollary.

Corollary 2: If condition (26) is not satisfied for $L=S$, then it is never satisfied, and no inverse with finite delay exists.

Consider now the input sequence $\boldsymbol{i}(0), \mathbf{0}, \mathbf{0}, \mathbf{0}, \cdots$. For this situation, (24) becomes

$$\boldsymbol{T}_L = [\bar{J}_0' \bar{J}_1' \bar{J}_2' \cdots \bar{J}_L']' \boldsymbol{i}(0), \tag{27}$$

which by the linearity of the LSC is the relationship governing the determination of the input at a single nonzero point in time from the observed outputs. This suggests the following definition.

Definition 2: An LSC is "pointwise input observable" if every $\boldsymbol{i}(0)$ in the input sequence $\boldsymbol{i}(0), \mathbf{0}, \mathbf{0}, \mathbf{0}, \cdots$, is uniquely determined from the output sequence $\boldsymbol{t}(0), \boldsymbol{t}(1), \boldsymbol{t}(2), \cdots$.

From (27) and Corollary 2, it is clear that an LSC is pointwise input observable if and only if

$$\operatorname{rank}(\bar{J}_0' \bar{J}_1' \bar{J}_2' \cdots \bar{J}_S') = K. \tag{28}$$

Moreover, pointwise input observability is then a necessary condition for an LSC to have an inverse with finite delay L.

VI. The Construction of Inverses with Finite Delay

The present section continues the assumptions of Section V, namely, that the LSC is described in the manner of (19) by a four-tuple of matrices $(\bar{\boldsymbol{A}}, \bar{\boldsymbol{B}}, \bar{\boldsymbol{C}}, \bar{\boldsymbol{E}})$ and that it is initially at rest. The results are motivated by the work of Youla and Dorato[6] on continuous-time, linear dynamical systems for the case $N=K$, and extensions are made herein for the case $N>K$. The development serves as an explicit example of the applicability of certain algebraic approaches in both LSCs and continuous-time dynamical systems.

Denote the first nonzero matrix in the sequence $\bar{J}_0, \bar{J}_1, \bar{J}_2, \cdots$, as $\bar{J}_I$. The discussion divides naturally into two parts, according to whether the rank $(\bar{J}_I)$ is equal to K or is not equal to K.

Theorem 5: Let rank $(\bar{J}_I)=K$. Then the LSC has an inverse with delay I which can be realized in the form

$$\begin{aligned} \boldsymbol{i}(k) &= -(\bar{F}\bar{J}_I)^{-1}\bar{F}\bar{C}\bar{A}^I \boldsymbol{x}(k) \\ &\quad + (\bar{F}\bar{J}_I)^{-1}\bar{F}\boldsymbol{t}(k+I) \end{aligned} \tag{29a}$$

$$\begin{aligned} \boldsymbol{x}(k+1) &= [\bar{A} - \bar{B}(\bar{F}\bar{J}_I)^{-1}\bar{F}\bar{C}\bar{A}^I]\boldsymbol{x}(k) \\ &\quad + \bar{B}(\bar{F}\bar{J}_I)^{-1}\bar{F}\boldsymbol{t}(k+I), \end{aligned} \tag{29b}$$

where (29) is initiated with $\boldsymbol{x}(0)=\mathbf{0}$ just I time units after (19) is initiated and where $\bar{F}$ is any $K \times N$ matrix such that $\bar{F}\bar{J}^I$ has an inverse. Moreover, there is no inverse with less delay.

Proof: Under the assumptions of the theorem, namely, $\bar{J}_0=\bar{J}_1= \cdots =\bar{J}_{I-1}=\bar{0}$, it is always possible to write

$$\boldsymbol{t}(j) = \mathbf{0}, \quad j = 0, 1, 2, \cdots, I-1, \tag{30a}$$

$$\boldsymbol{t}(k+I) = \bar{C}\bar{A}^I \boldsymbol{x}(k) + \bar{J}_I \boldsymbol{i}(k), \quad k = 0, 1, 2, \cdots. \tag{30b}$$

That there is no inverse with delay less than I follows immediately from (30a). Moreover, (30b) can be viewed as N equations in K unknowns (which are the K components of $\boldsymbol{i}(k)$). That these equations have a solution follows from construction; that the solution is unique follows from the fact that rank $(\bar{J}_I)=K$. Premultiplication of both members of (30b) by a matrix $\bar{F}$ which selects a set of K linearly independent equations from the N equations, which are given, yields

$$\bar{F}\boldsymbol{t}(k+I) = \bar{F}\bar{C}\bar{A}^I \boldsymbol{x}(k) + \bar{F}\bar{J}_I \boldsymbol{i}(k),$$

where $\bar{F}\bar{J}_I$ has an inverse. Inversion gives (29a) and substitution of (29a) into (19a) gives (29b), and thus the theorem is established. Although in Theorem 5 the existence of the inverse with delay I was established by construction, it should be observed that Theorem 4 predicts the existence of such a construction, since

$$\operatorname{rank}(\bar{J}_I) = \operatorname{rank}(\bar{J}_{I-1}) + K = 0 + K = K.$$

As an example illustrating the difference between the inverses of Theorems 1 and 5, consider the $K=1$, $N=2$ binary LSC with $G_{11}(D)=D$ and $G_{21}(D)=1+D+D^2$. By Theorem 1 this FF LSC must have an instantaneous FF inverse. This is indeed the case, for $(1+D)G_{11}(D) + G_{21}(D)=1$. The realization (19) can be given in the form

$$\bar{A} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \qquad \bar{B} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\bar{C} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \qquad \bar{E} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Since $\bar{J}_0=\bar{E}$ has rank one, Theorem 4 shows the existence of the instantaneous inverse, and Theorem 5 (with $\bar{F}=[0\ \ 1]$) constructs such an inverse having the transfer functions $H_{11}(D)=0$ and $H_{12}(D)=1/(1+D+D^2)$ which is clearly not FF.

More generally, the transfer function matrix $\bar{H}(D)$ associated with (29) by means of (20) is given by

$$\begin{aligned} \bar{H}(D) &= [-(\bar{F}\bar{J}_I)^{-1}\bar{F}\bar{C}\bar{A}^I[D^{-1}\bar{I}_S - \bar{A} \\ &\quad + \bar{B}(\bar{F}\bar{J}_I)^{-1}\bar{F}\bar{C}\bar{A}^I]^{-1}\bar{B}(\bar{F}\bar{J}_I)^{-1}\bar{F} + (\bar{F}\bar{J}_I)^{-1}\bar{F}]D^{-I} \\ &= [D^{-I}(\bar{F}\bar{J}_I)^{-1}\bar{F}][\bar{I}_N - \bar{C}\bar{A}^I(D^{-1}\bar{I}_S - \bar{A})^{-1} \\ &\quad \cdot [\bar{I}_S + \bar{B}(\bar{F}\bar{J}_I)^{-1}\bar{F}\bar{C}\bar{A}^I(D^{-1}\bar{I}_S - \bar{A})^{-1}]^{-1} \\ &\quad \cdot \bar{B}(\bar{F}\bar{J}_I)^{-1}\bar{F}] \\ &= D^{-I}(\bar{F}\bar{J}_I)^{-1}\bar{F}[\bar{I}_N \\ &\quad + \bar{C}\bar{A}^I(D^{-1}\bar{I}_S - \bar{A})^{-1}\bar{B}(\bar{F}\bar{J}_I)^{-1}\bar{F}]^{-1}, \end{aligned} \tag{31}$$

where the last step follows from a well-known matrix inverse identity.[7] In order to make (31) causal, and to conform with Theorem 5 in initiating (29) with an I-time-unit lag, the inverse transfer function matrix will be written $D^I\overline{H}(D)$. The original LSC transfer function matrix $\overline{G}(D)$ obtained from (19) and (30b) is

$$\begin{aligned}\bar{G}(D) &= D^I[\bar{J}_I + \bar{C}\bar{A}^I(D^{-1}\bar{I}_S - \bar{A})^{-1}\bar{B}] \\ &= D^I[\bar{I}_N + \bar{C}\bar{A}^I(D^{-1}\bar{I}_S - \bar{A})^{-1}\bar{B}(\bar{F}\bar{J}_I)^{-1}\bar{F}]\bar{J}_I. \quad (32)\end{aligned}$$

From (31) and (32) it is seen that $D^I\overline{H}(D)\overline{G}(D) = D^I\overline{I}_K$ as desired. Moreover, it is also apparent that if $\overline{G}(D)$ is a matrix of polynomials corresponding to an FF LSC, then $D^I\overline{H}(D)$ will, in general, have elements which are rational functions of D as a result of the inversion in (31). As an example of this assertion, it is instructive to consider the case $K=1$.

For cases such as this one, in which $K \leq N$, it is usually more convenient to invert a $K \times K$ matrix rather than an $N \times N$ matrix. Therefore, rewrite (31) in the manner

$$\begin{aligned}D^I\bar{H}(D) &= (\bar{F}\bar{J}_I)^{-1}\bar{F}[\bar{I}_N - \bar{C}\bar{A}^I(D^{-1}\bar{I}_S - \bar{A})^{-1}\bar{B}[\bar{I}_K \\ &\quad + (\bar{F}\bar{J}_I)^{-1}\bar{F}\bar{C}\bar{A}^I(D^{-1}\bar{I}_S - \bar{A})^{-1}\bar{B}]^{-1}(\bar{F}\bar{J}_I)^{-1}\bar{F}]. \quad (33)\end{aligned}$$

Equation (33) has a special advantage over (31) in this instance, when $K=1$, for then (33) simplifies to

$$D^I\bar{H}(D) = \bar{F}/[(\bar{F}\bar{J}_I) + \bar{F}\bar{C}\bar{A}^I(D^{-1}\bar{I}_S - \bar{A})^{-1}\bar{B}]. \quad (34)$$

But the denominator of (34) is simply related to $\overline{G}(D)$ by (32), so that

$$\bar{H}(D) = \bar{F}/\bar{F}\bar{G}(D), \quad (35)$$

from which it is clear that $\overline{H}(D)$ has elements which are reciprocals of polynomials when $\overline{G}(D)$ has elements which are polynomials.

The remaining development of this section is concerned with displaying an inverse construction procedure for the case in which rank $(\overline{J}_I) \neq K$. It is assumed that the LSC has an inverse, that is, the set of determinants $\Delta_i(D)$, $i=1, 2, \cdots, \binom{N}{K}$, are not all identically zero. Consider now the matrix $D^{-I}\overline{G}(D)$, denoted $\overline{G}^1(D)$, and note that $\overline{J}_I = \overline{G}^1(0)$. Let the $\binom{N}{K}$ distinct determinants which can be formed from $K \times K$ minors of $\overline{G}^1(D)$ be denoted $\Delta_i^1(D)$, $i=1, 2, \cdots, \binom{N}{K}$. By assumption, they are not all identically zero. Since rank $(\overline{J}_I) \neq K$, then there exists a positive integer m such that

$$\text{GCF}\left[\Delta_i^1(D),\ i = 1, 2, \cdots, \binom{N}{K}\right] = D^m R_1(D),^1 \quad (36)$$

where $R_1(D)$ is a rational function satisfying $R_1(0) \neq 0$. Let $\Delta_n^1(D)$ be any of the $\binom{N}{K}$ determinants satisfying $\Delta_n^1(D) = D^m R(D)$ where $R(0) \neq 0$, and let $\overline{G}^1(D)_n$ be the submatrix of $\overline{G}^1(D)$ with the corresponding K rows.

[1] The greatest common factor (GCF) of the rational functions $P_i(D)/Q_i(D)$, $i=1, 2, \cdots, n$, where GCD $[P_i(D), Q_i(D)]=1$, is here defined as GCD $[P_i(D), \cdots, P_n(D)]$/GCD $[Q_i(D), \cdots, Q_n(D)]$.

Then there exists a nonsingular $K \times K$ matrix $\overline{W}^1(D)$, such that $D\overline{W}^1(D)$ is a matrix of polynomials in D, and such that

$$\text{GCF}\left[\Delta_i^2(D),\ i=1, 2, \cdots, \binom{N}{K}\right] = D^{m-1}R_2(\text{D}), \quad (37)$$

where $R_2(0) \neq 0$ and the $\Delta_i^2(D)$ are the determinants formed from $K \times K$ minors of

$$\bar{G}^2(D) = \bar{G}^1(D)\overline{W}^1(D). \quad (38)$$

Moreover, $\overline{G}^2(D)$ has a structural realization in the form $(\overline{A},\ \overline{B}\overline{W}_2^1 + \overline{A}\overline{B}\overline{W}_1^1,\ \overline{C}\overline{A}^I,\ \overline{J}_I\overline{W}_2^1 + \overline{C}\overline{A}^I\overline{B}\overline{W}_1^1)$, where $\overline{W}_2^1$ contains the elements of $\overline{W}^1(D)$ which are independent of D and $\overline{W}_1^1 = D(\overline{W}^1(D) - \overline{W}_2^1)$.

In order to verify the assertions above, note that there exists at least one K vector $\boldsymbol{a}^1 \neq \boldsymbol{0}$ such that $\overline{J}_I\boldsymbol{a}^1 = \boldsymbol{0}$. Since $\boldsymbol{a}^1 \neq \boldsymbol{0}$, it has at least one nonzero component, say the jth component a_{1j}. Define $\overline{W}^1(D)$ to be the matrix with jth column $\boldsymbol{a}^1 D^{-1}$ and all other columns equal to those of the identity matrix $\overline{I}_K$. Observe that the determinant of $\overline{W}^1(D) = D^{-1}a_{1j}$. Equation (37) is then established by noting that the determinant of $\overline{G}^2(D)_i$ is just the product of the determinants of $\overline{G}^1(D)_i$ and $\overline{W}^1(D)$. In order to examine the question of a structural realization for $\overline{G}^2(D)$, consider the formal series expansion

$$\begin{aligned}\bar{G}^1(D) &= \bar{J}_I + (\bar{C}\bar{A}^I)\bar{B}D + (\bar{C}\bar{A}^I)\bar{A}\bar{B}D^2 \\ &\quad + (\bar{C}\bar{A}^I)\bar{A}^2\bar{B}D^3 + \cdots. \quad (39)\end{aligned}$$

By virtue of the fact that $\overline{W}_1^1$ has zeros everywhere, except in the jth column, where it has $\boldsymbol{a}^1$, and since $\overline{W}_2^1$ is independent of D, it is possible to write

$$\begin{aligned}\bar{G}^2(D) &= \bar{G}^1(D)[\bar{W}_1^1 D^{-1} + \bar{W}_2^1] \\ &= [\bar{J}_I\bar{W}_2^1 + (\bar{C}\bar{A}^I)\bar{B}\bar{W}_1^1] \\ &\quad + [(\bar{C}\bar{A}^I)\bar{B}\bar{W}_2^1 + (\bar{C}\bar{A}^I)\bar{A}\bar{B}\bar{W}_1^1]D + \cdots \quad (40)\end{aligned}$$

which can be identified with the structural matrices asserted above.

The discussion above can be generalized and stated as a lemma.

Lemma 6: Suppose that rank $(\overline{J}_I) \neq K$. Let m be the positive integer defined in (36). Then there exists a sequence of LSCs $\overline{G}^i(D)$, $i=1, 2, \cdots, m+1$, such that rank $(\overline{G}^{m+1}(0)) = K$. Moreover, the $\overline{G}^i(D)$ can be defined recursively in the manner

$$\begin{aligned}\bar{G}^{i+1}(D) &= \bar{G}^i(D)\bar{W}^i(D), \\ &\qquad i = 1, 2, \cdots, m,\ \bar{G}^1(D) = D^{-I}\bar{G}(D), \quad (41)\end{aligned}$$

where each $\overline{G}^i(D)$ has the structural realization $\overline{J}_I{}^i + \overline{C}\overline{A}^I(D^{-1}\overline{I}_S - \overline{A})^{-1}\overline{B}^i$ and where $\overline{W}^i(D)$ is a $K \times K$ matrix which is equal to $\overline{I}_K$ in all columns except one, say the jth, in which it has a K vector $\boldsymbol{a}^i$ (satisfying $\overline{J}_I{}^i\boldsymbol{a}^i = \boldsymbol{0}$, $\boldsymbol{a}_{ij} \neq 0$) multiplied by D^{-1}. Finally, the structural matrices $\bar{J}_I{}^i$ and $\bar{B}^i$ are defined by the recursions $\bar{J}_I{}^{i+1} = \bar{J}_I{}^i \bar{W}_2{}^i + \bar{C}\bar{A}^I \bar{B}^i \bar{W}_1{}^i$ and $\bar{B}^{i+1} = \bar{B}^i \bar{W}_2{}^i + \bar{A}\bar{B}^i \bar{W}_1{}^i$, under the initial conditions $\bar{J}_I{}^1 = \bar{J}_I$ and $\bar{B}^1 = \bar{B}$, for $i = 1, 2, \cdots, m$. The nonzero elements of $\bar{W}_2{}^i$ are those of $\bar{W}^i(D)$ which do not depend on D, and $\bar{W}_1{}^i = D(\bar{W}^i(D) - \bar{W}_2{}^i.)$

Proof: The proof of Lemma 6 follows by induction on the case $i=1$ discussed in preceding paragraphs. It is important to point out, nonetheless, that the existence of $\boldsymbol{a}^i$, $i = 1, 2, \cdots, m$, is assured by (36) and the construction (41) which together imply that rank $(\bar{J}_I{}^i) \neq K$, $i = 1, 2, \cdots, m$.

Lemma 6 is indicative of a series of nonsingular transformations $\bar{W}^i(D)$, $i = 1, 2, \cdots, m$, by means of which the transfer function matrix $\bar{G}^1(D)$, to which Theorem 5 does not apply, is converted to a transfer function matrix $\bar{G}^{m+1}(D)$, to which Theorem 5 does apply. By means of the relations (41) and the definition of $\bar{G}(D)$, it follows that

$$\begin{aligned} \bar{G}(D) &= D^I \bar{G}^{m+1}(D)[\bar{W}^m(D)]^{-1}[\bar{W}^{m-1}(D)]^{-1} \cdots \\ &\quad \cdot [\bar{W}^1(D)]^{-1} \\ &= [D^I \bar{G}^{m+1}(D)][D\bar{W}^m(D)]^{-1} \cdots [D\bar{W}^1(D)]^{-1} D^m, \end{aligned} \tag{42}$$

which permits the statement of the main result of the section.

Theorem 6: Under the hypotheses of Lemma 6, the LSC has an inverse which can be constructed as the cascade of the inverse of $D^I \bar{G}^{m+1}(D)$, according to Theorem 5, with the unit-delay LSCs $D\bar{W}^m(D)$, $D\bar{W}^{m-1}(D), \cdots, D\bar{W}^1(D)$. The inverse has finite delay $L = I + m$.

Proof: Theorem 6 follows directly from (42) and Lemma 6.

VII. Conclusions

The question of the existence of and realizations for inverse linear sequential circuits is of considerable interest in the theory of information processing. For example, certain desirable properties of convolutional error-correcting code schemes suggest the study of feedforward inverses for feedforward linear sequential circuits.

This paper establishes the necessary and sufficient conditions for a feedforward linear sequential circuit to have a feedforward inverse and gives an implicit procedure for its construction. The concept of an inverse with finite delay is defined, and necessary and sufficient conditions are given for the existence of such an inverse. Finally, construction techniques for inverses with finite delay are given in recursive form by analogy with known results in continuous-time linear dynamical systems.

The first part of the paper approaches the linear sequential circuit from the viewpoint of its transfer function matrix, whereas the second part describes the circuit in terms of state variables and structural matrices. The results are complementary in nature and serve to emphasize the need of further investigations to interrelate methods associated with the two descriptions. Further incentive for such studies is derived from the fact that the second part of the paper is motivated largely by studies in continuous-time systems.

Finally, we remark that our Definition 1 for the existence of an inverse with delay L for an LSC is equivalent for LSCs to Huffman's[8] general concept of "information lossless of finite order L" for a sequential circuit.

Acknowledgment

Prof. Sain wishes to acknowledge beneficial conversations with Prof. R. J. Leake and Prof. C. R. Souza at the University of Notre Dame. He is also indebted to Prof. W. R. Perkins of the University of Illinois for calling the results of Youla and Dorato to his attention.

References

[1] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE Trans. Information Theory*, vol. IT-13, pp. 260–269, April 1967.

[2] J. L. Massey and M. K. Sain, "Codes, automata, and continuous systems: explicit interconnections," *IEEE Trans. Automatic Control*, vol. AC-12, pp. 645–650, December 1967.

[3] J. L. Massey, *Threshold Decoding*. Cambridge, Mass.: M.I.T. Press, 1963.

[4] G. Birkhoff and S. Maclane, *A Survey of Modern Algebra*, 3rd ed. New York: Macmillan, 1965, p. 71.

[5] A. Gill, *Linear Sequential Circuits*. New York: McGraw-Hill, 1966, pp. 21–26.

[6] D. C. Youla and P. Dorato, "On the inverse of linear dynamical systems," Polytechnic Institute of Brooklyn, N. Y., Electrophysics Memorandum PIBMRI-1319-66, March 1966.

[7] M. K. Sain, "On 'A useful matrix inversion formula and its applications,' " *Proc. IEEE* (*Letters*), vol. 55, p. 1753, October 1967.

[8] D. A. Huffman, "Canonical forms for information-lossless finite-state logical machines," *IRE Trans. Circuit Theory*, vol. CT-6, pp. 41–59, March 1959.