Equivalence of Nonlinear Shift-Registers

J. L. MASSEY, MEMBER, IEEE AND R. W. LIU, MEMBER, IEEE

Summary—Two forms of nonlinear-feedback shift-registers are considered. In the Type-I register, the feedback output is added to the shift-register contents at an arbitrary number of stages. In the type-II register, the feedback is input to the first stage only. It is shown that for every Type-I register there is an equivalent Type-II register in the sense that the autonomous state diagrams differ only by a labelling of the states. Moreover, the mapping between equivalent states can always be chosen to be a linear transformation. This theorem is a well-known result in the theory of linear-feedback shift-registers and is thus seen to apply unchanged to the nonlinear case.

IN THIS PAPER, we will show that an equivalence relation known to hold for linear-feedback shift-registers is also valid for nonlinear-feedback shift-registers. This fact materially simplifies the analysis of a class of nonlinear-feedback shift-registers encountered in the study of convolutional codes.

It was shown recently by the authors[1] that the error-propagation effect in binary convolutional codes is closely related to the autonomous behavior of the binary nonlinear-feedback shift-register (NFSR) shown in Fig. 1. In this figure, the feedback function is an arbitrary Boolean function of the shift-register contents s_0, s_1, $\cdots$ s_{m-1}. The column vector $\mathbf{s} = (s_0, s_1, \cdots s_{m-1})$ will be called the *state* of the NFSR. Each g_i in Fig. 1 is equal to one or zero, accordingly, as the feedback output is or is not an input to the corresponding modulo-two adder. The NFSR of Fig. 1 will be called a *type-I NFSR* for ease of reference.

The NFSR of Fig. 2 is an important, special case of that found in Fig. 1; namely the case where the feedback output is an input only to the first stage of the shift-register. The NFSR of Fig. 2 will be referred to as a *type-II NFSR*.

Let θ be the "next-state operator", *i.e.*, $\theta\mathbf{s}$ is the next state of an NFSR with current state $\mathbf{s}$. The autonomous behavior of type-I and type-II NFSR's can then be described, respectively, by

$$\theta\mathbf{s} = A\mathbf{s} \oplus f(\mathbf{s})\mathbf{g} \tag{1}$$

and

$$\theta\mathbf{s}' = A\mathbf{s}' \oplus f'(\mathbf{s}')\mathbf{u} \tag{2}$$

where $\mathbf{s}$ and $\mathbf{s}'$ are the states of type-I and type-II NFSR's, respectively. f' is the feedback function of the type-II NFSR; $\oplus$ indicates summation modulo-two.

Manuscript received March 25, 1964. This work was supported by the National Science Foundation under Grant No. GP-2547.

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

[1] J. L. Massey and R. Liu, "Application of Lyapunov's direct method to the error-propagation effect in convolutional codes," IEEE TRANS. ON INFORMATION THEORY (Correspondence), vol. IT-10, pp. 248–250; July, 1964.

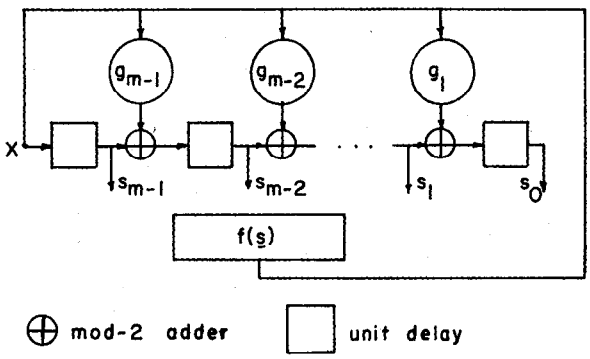

Fig. 1—Type-I nonlinear-feedback shift-register.

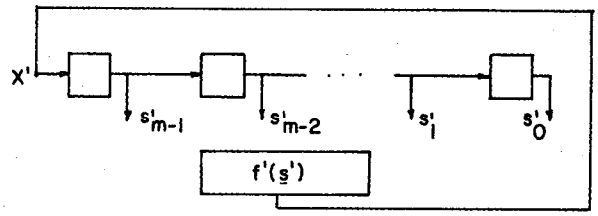

Fig. 2—Type-II nonlinear-feedback shift-register.

A is the $m \times m$ shifting matrix

$$A = \begin{bmatrix} 0 & 1 & & \cdots & 0 \\ & 0 & 1 & & \\ & & \ddots & & \\ & & & \ddots & \\ 0 & & \cdots & 0 & 1 \\ 0 & & \cdots & & 0 \end{bmatrix}$$

and $\mathbf{g}$ and $\mathbf{u}$ are the column vectors

$$\mathbf{g} = (g_1, g_2, \cdots g_{m-1}, 1)$$

$$\mathbf{u} = (0, 0, \cdots 0, 1).$$

In the linear case, *i.e.*, when $f(\mathbf{s}) = \sum_{i=0}^{m-1} c_i s_i$, it is well-known that for any type-I shift-register there is an equivalent type-II linear-feedback shift-register in the sense that the autonomous state diagrams of the two machines differ only by a labelling of the states.[2] In other words, there exists in this case a one-one transformation, $T(\mathbf{s}) = \mathbf{s}'$, such that $T(\theta\mathbf{s}) = \theta(T(\mathbf{s}))$ for all $\mathbf{s}$. Thus, if $\mathbf{s}$ and $\mathbf{s}'$ are equivalent states, then so are $\theta\mathbf{s}$ and $\theta\mathbf{s}'$. We show here the somewhat surprising fact that the same result is true for the nonlinear case; thus the autonomous behavior of any type-I NFSR can be de-

[2] W. W. Peterson, "Error-Correcting Codes," M. I. T. Press, Cambridge, Mass., and John Wiley and Sons, Inc., New York, N. Y., ch. 7; 1961.

termined by the study of the equivalent type-II NFSR. This is a result of practical importance since a considerable body of theory about the autonomous behavior of type-II NFSR's already exists.[3,4,5]

Theorem: For every type-I NFSR there is a type-II NFSR with the same autonomous behavior, *i.e.*, there exists a one-one transformation, $T(\mathbf{s}) = \mathbf{s}'$ such that $T(\theta\mathbf{s}) = \theta(T(\mathbf{s}))$ for all $\mathbf{s}$. In particular, T can always be chosen as a linear transformation, and the restriction $f(\mathbf{s}) = f'(T(\mathbf{s}))$ can always be imposed, (*i.e.*, both registers have the same feedback output for equivalent states).

Proof: Let T be a one-one transformation between a state $\mathbf{s}$ of the type-I NFSR and a state $\mathbf{s}'$ of a type-II NFSR. Then by applying the transformation to (1), we obtain

$$T(\theta\mathbf{s}) = T(A\mathbf{s} \oplus f(\mathbf{s})\mathbf{g}).$$

If we now require that T be a linear transformation, then T must be a nonsingular $m \times m$ matrix, and the preceding equation becomes

$$T(\theta\mathbf{s}) = TA\mathbf{s} \oplus f(\mathbf{s})T\mathbf{g}. \tag{3}$$

Similarly, since $\mathbf{s}' = T\mathbf{s}$, (2) becomes

$$\theta(T\mathbf{s}) = AT\mathbf{s} \oplus f'(T\mathbf{s})\mathbf{u}. \tag{4}$$

We now impose the further restriction that $f(\mathbf{s}) = f'(T\mathbf{s})$. It is then evident from (3) and (4) that the equivalence condition $T(\theta\mathbf{s}) = \theta(T\mathbf{s})$ for all $\mathbf{s}$ will be met if we have both

$$TA = AT \tag{5}$$

and

$$T\mathbf{g} = \mathbf{u}. \tag{6}$$

Thus, the proof will be complete if we can find a nonsingular matrix T that satisfies (5) and (6).

Let T be represented as the matrix

$$T = \begin{bmatrix} t_{1,1} & t_{1,2} & \cdots & t_{1,m} \\ \vdots & & & \\ t_{m,1} & t_{m,2} & \cdots & t_{m,m} \end{bmatrix}.$$

Then, from the structure of the matrix A, we see that

$$TA = \begin{bmatrix} 0 & t_{1,1} & t_{1,2} & \cdots & t_{1,m-1} \\ \vdots & & & & \\ 0 & t_{m,1} & t_{m,2} & \cdots & t_{m,m-1} \end{bmatrix}$$

and

$$AT = \begin{bmatrix} t_{2,1} & t_{2,2} & \cdots & t_{2,m} \\ \vdots & & & \\ t_{m,1} & t_{m,2} & \cdots & t_{m,m} \\ 0 & 0 & \cdots & 0 \end{bmatrix}.$$

In words, postmultiplication by A shifts the first $m - 1$ columns of T one position to the right and inserts a new first column of zeroes, while premultiplication by A shifts the last $m - 1$ rows of T one position upward and inserts a new last row of zeroes. Thus (5) will be satisfied if and only if T is a triangular matrix with the structure

$$T = \begin{bmatrix} t_1 & t_2 & t_3 & \cdots & t_m \\ 0 & t_1 & t_2 & \cdots & t_{m-1} \\ & & \ddots & \ddots & \\ 0 & 0 & 0 & \cdots & t_1 \end{bmatrix} \tag{7}$$

where $t_1, t_2, \cdots t_m$ are arbitrary binary numbers.

Assuming that T has the form given in (7), we find

$$T\mathbf{g} = (t_1g_1 \oplus t_2g_2 \oplus \cdots t_m,\ t_1g_2 \oplus t_2g_3 \oplus \cdots t_{m-1},\ \cdots,\ t_1),$$

and thus (6) will be satisfied if and only if

$$\begin{aligned} t_1 &= 1 \\ t_1g_{m-1} \oplus t_2 &= 0 \\ &\vdots \\ t_1g_2 \oplus t_2g_3 \oplus \cdots \oplus t_{m-1} &= 0 \\ t_1g_1 \oplus t_2g_2 \oplus \cdots \oplus t_m &= 0. \end{aligned} \tag{8}$$

The first equation in set (8) guarantees that T is nonsingular. It is readily seen that the remaining equations are satisfiable by a unique choice of $t_2, t_3, \cdots t_m$. This completes the proof of the theorem.

Some further remarks are in order. First, the theorem is easily generalized to the case where the components of $\mathbf{s}$ are elements in any finite field. Second, the theorem may be generalized to include inputs (*i.e.*, nonautonomous behavior) to the shift registers. However, an input at point X alone for the type-I NFSR in Fig. 1 will in general correspond to an input at more points than X' alone for the equivalent type-II NFSR of Fig. 2. Thus, the equivalence is not so useful as in the autonomous case.

[3] S. W. Golomb and L. R. Welch, "Non-Linear Shift Register Sequences," California Inst. of Tech., Pasadena, JPL Memo. 20–149; October, 1957.

[4] S. W. Golomb, *et al.*, "Cycles from Non-linear Shift-Registers," California Inst. of Tech., Pasadena, JPL Progress Rept. 20-389; August, 1959.

[5] K. B. Magleby, "The Synthesis of Nonlinear Feedback Shift Registers," Stanford Electron. Labs., Stanford, Calif., Tech. Rept. No. 6207-1; October, 1963.