INFORMATION AND CONTROL 13, 75-84 (1968)

Computation over Galois Fields Using Shiftregisters

H. TANAKA, M. KASAHARA, Y. TEZUKA AND Y. KASAHARA

Faculty of Engineering, Osaka University, Osaka, Japan

This paper presents a technique for readily determining the shiftregister which multiplies by a given element of $GF(2^m)$, or which raises a given element of $GF(2^m)$ to a given power. A matrix (called a connection matrix) is derived from a primitive polynomial and is corresponded to a particular shiftregister. The nth power of the matrix corresponds to the shiftregister which multiplies by X^n. Examples are presented to illustrate the application of the technique.

THE LIST OF SYMBOLS

$GF(2)$	Galois Ground Field
$GF(2^m)$	Galois Extension Field of Degree m
α	A Root of Primitive Polynomial
F	Matrix Defined by any Primitive Polynomial
$\oplus$	modulus 2 Addition between Matrices
E	Unit Matrix

I. INTRODUCTION

This paper examines the problem of computation over the Galois extension field of degree m and characteristic 2, $GF(2^m)$. Given a primitive polynomial of degree m over $GF(2)$, a matrix F is defined which corresponds the polynomial with a shiftregister. Since the nth power of the matrix F corresponds to a shiftregister which multiplies its contents by X^n over $GF(2^m)$, the shiftregisters appropriate for multiplying and taking powers are readily determined. An example of an area in which the technique can be applied is the problem of solving simultaneous equations with several unknowns, and solving equations of higher degree with one unknown using shiftregisters.

II. THE GALOIS EXTENSION FIELD, $GF(2^m)$

The algebraic system under consideration in this paper is the extension field of degree m over the ground field of order 2. We denote the ele-

TABLE I

OPERATION ON $GF(2)$

Addition

+	0	1
0	0	1
1	1	0

Multiplication

•	0	1
0	0	0
1	0	1

TABLE II

ELEMENTS OF $GF(2^4)$ $(\alpha^4 + \alpha + 1 = 0)$

0	$= 0$	$(0\ 0\ 0\ 0)$	$GF(2)$ / $GF(2^4)$
α^0	$= 1$	$(1\ 0\ 0\ 0)$	$GF(2)$ / $GF(2^4)$
α^1	$= \alpha$	$(0\ 1\ 0\ 0)$	$GF(2^4)$
α^2	$= \alpha^2$	$(0\ 0\ 1\ 0)$	$GF(2^4)$
α^3	$= \alpha^3$	$(0\ 0\ 0\ 1)$	$GF(2^4)$
α^4	$= 1 + \alpha$	$(1\ 1\ 0\ 0)$	$GF(2^4)$
α^5	$= \alpha + \alpha^2$	$(0\ 1\ 1\ 0)$	$GF(2^4)$
α^6	$= \alpha^2 + \alpha^3$	$(0\ 0\ 1\ 1)$	$GF(2^4)$
α^7	$= 1 + \alpha + \alpha^3$	$(1\ 1\ 0\ 1)$	$GF(2^4)$
α^8	$= 1 + \alpha^2$	$(1\ 0\ 1\ 0)$	$GF(2^4)$
α^9	$= \alpha + \alpha^3$	$(0\ 1\ 0\ 1)$	$GF(2^4)$
α^{10}	$= 1 + \alpha + \alpha^2$	$(1\ 1\ 1\ 0)$	$GF(2^4)$
α^{11}	$= \alpha + \alpha^2 + \alpha^3$	$(0\ 1\ 1\ 1)$	$GF(2^4)$
α^{12}	$= 1 + \alpha + \alpha^2 + \alpha^3$	$(1\ 1\ 1\ 1)$	$GF(2^4)$
α^{13}	$= 1 + \alpha^2 + \alpha^3$	$(1\ 0\ 1\ 1)$	$GF(2^4)$
α^{14}	$= 1 + \alpha^3$	$(1\ 0\ 0\ 1)$	$GF(2^4)$
	....	....	
α^{15}	$= 1 = \alpha^0$		

ments of the ground field by 0 and 1, and define the operations of addition and multiplication as shown in Table I. The ground field is denoted by $GF(2)$. Let $f(X)$ be a primitive polynomial of degree m over $GF(2)$, and let α be a root of $f(X)$. The extension field is constructed by adding the element α to $GF(2)$. The order, or number of elements, of the extension field is 2^m, and we hence denote the field by $GF(2^m)$.

For example, consider the following polynomial of degree 4 over $GF(2)$

$$f(X) = 1 + X + X^4. \tag{1}$$

A primitive root, α, of $f(X) = 0$, satisfies the equation

$$1 + \alpha + \alpha^4 = 0. \tag{2}$$

All the elements of $GF(2^4)$ are listed in Table II. Any element whose power is larger than 3 is reduced to the polynomial of degree less than or equal to 3 by using the relation (2). This extension field will be used several times as an example in the following discussions.

III. THE SHIFTREGISTER CONNECTION MATRIX CORRESPONDING TO A PRIMITIVE POLYNOMIAL

III-1. Definition of the Connection Matrix

Consider a primitive polynomial of degree m over $GF(2)$,

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_{m-1}X^{m-1} + X^m. \tag{3}$$

The coefficients $a_i(0 \leqq i \leqq m - 1)$, being elements of $GF(2^m)$, are 0's or 1's. Given the coefficients a_i of $f(X)$, we define the matrix F as follows;

$$F = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 1 & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & & & & \cdot \\ \cdot & \cdot & \cdot & & & \cdot & & & \cdot \\ \cdot & \cdot & \cdot & & & & \cdot & & 0 \\ \cdot & \cdot & \cdot & & & & & \cdot & \\ 0 & 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 \\ a_0 & a_1 & & \cdot & \cdot & \cdot & \cdot & \cdot & a_{m-1} \end{bmatrix}. \tag{4}$$

Thus the matrix F is a matrix of rank m whose elements are zeros or ones. We shall now examine several properties of the matrix F. Let us denote the polynomial of the matrix F by $h(\lambda)$, i.e.,

$$h(\lambda) = | \lambda E - F | \tag{5}$$

where E denotes the unit (identity) matrix. We may now prove the following

Lemma 1.

$$f(\lambda) = h(\lambda). \tag{6}$$

Proof. We define a matrix as follows;

$$\Lambda = \begin{bmatrix} 1 & 0 & 0 & \cdot & \cdot & & \cdot & \cdot & 0 \\ \lambda & 1 & 0 & \cdot & \cdot & & \cdot & \cdot & 0 \\ \lambda^2 & \lambda & 1 & & & & & & \cdot \\ \lambda^3 & \lambda^2 & \lambda & 1 & & & & & \cdot \\ \cdot & \cdot & \cdot & & & \cdot & & & \cdot \\ \cdot & \cdot & \cdot & & & & & \cdot & 0 \\ \lambda^{m-1} & & \cdot & \cdot & \cdot & & \cdot & \cdot & 1 \end{bmatrix}. \tag{7}$$

Note that $|\Lambda| = 1$. We multiply $(\lambda E - F)$ by Λ, obtaining the following result.

$$\begin{bmatrix} \lambda & -1 & 0 & 0 & \cdot & \cdot & \cdot & & 0 \\ 0 & \lambda & -1 & 0 & \cdot & \cdot & \cdot & & 0 \\ 0 & 0 & \lambda & -1 & \cdot & \cdot & \cdot & & 0 \\ \cdot & \cdot & \cdot & & & & & & \cdot \\ \cdot & \cdot & & & & & & & \\ 0 & 0 & \cdot & \cdot & \cdot & 0 & \lambda & & -1 \\ -a_0 & -a_1 & & \cdot & \cdot & \cdot & \cdot & & (\lambda - a_{m-1}) \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ \lambda & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ \lambda^2 & \lambda & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \lambda^{m-1} & & \cdot & \cdot & \cdot & \cdot & \lambda & 1 \end{bmatrix} \tag{8}$$

$$= \begin{bmatrix} 0 & 1 & 0 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & & \cdot & \cdot & \cdot & & \vdots \\ \cdot & & \cdot & & \cdot & \cdot & \cdot & \\ \cdot & & & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & & 0 & 1 \\ f_1 & & f_2 & f_3 & \cdot & \cdot & \cdot & f_m \end{bmatrix}$$

where f_i, $i > 1$, denotes a polynomial in λ, and

$$f_1(\lambda) = -a_0 - a_1\lambda - \cdots - a^m{}_{-1}\lambda^{m-1} + \lambda^m$$
$$= f(\lambda)$$

over $GF(2)$. Using (8), we obtain

$$h(\lambda) = |\lambda E - F| = |\lambda E - F|\,|\Lambda| = |(\lambda E - F)\Lambda| = f_1(\lambda) = f(\lambda)$$

Q.E.D.

We define the addition of two matrices, F_1 and F_2, in the usual sense, i.e., to mean addition modulus 2 between corresponding elements of F_1 and F_2.

LEMMA 2.

$$f(F) = 0. \tag{9}$$

Proof. Using Lemma 1,

$$f(F) = h(F) = | FE - F | = | F - F | = 0 \qquad \text{Q.E.D.}$$

Lemma 2 thus shows that the matrix F defined by $f(X)$ is a root of $f(X)$.

Let us now consider polynomials in F over $GF(2)$. Since $f(X)$ is primitive, and $f(\alpha) = 0$ and $f(F) = 0$, we have

LEMMA 3. *The algebra* $\Omega(F)$ *of residue classes of polynomials modulo* $\{f(F)\}$ *is isomorphic to* $GF(2^m)$.

Since every element of $GF(2^m)$ may be expressed as a linear combination of $\alpha^0, \alpha^1, \alpha^2, \cdots \alpha^{m-1}$, and since $\Omega(F)$ is isomorphic to $GF(2^m)$, we have the following lemma.

LEMMA 4. F^n *can be expressed as a combination of* $F^0 = E, F^1, F^2, F^3, \cdots, F^{m-1}$.

Suppose that F^n is expressed as

$$F^n = f_0E + f_1F + f_2F^2 + \cdots + f_{m-1}F^{m-1}, \tag{10}$$

where f_i $(0 \leqq i \leqq m - 1)$ are elements of $GF(2)$. Then f_i can be calculated as follows. Let us divide X^n by $f(X)$, designating the quotient by $Q(X)$ and the remainder by $R(X)$. By the Euclidean division algorithm, we may write

$$X^n = f(X)Q(X) + R(X) \tag{11}$$

where

$$R(X) = f_0 + f_1X + f_2X^2 + \cdots + f_{m-1}X^{m-1}. \tag{12}$$

Substituting F for X and the symbol $\oplus$ for $+$, we have

$$F^n = f(F)Q(F) \oplus R(F).$$

Since $f(F) = 0$ by Lemma 2,

$$F^n = R(F) = f_0E \oplus f_1F \oplus f_2F^2 \oplus \cdots \oplus f_{m-1}F^{\cdot-1}. \tag{13}$$

Hence, f_i $(0 \leqq i \leqq m - 1)$ are determined as the coefficients of $R(X)$.

III-2. CORRESPONDENCE OF THE MATRIX F TO A SHIFTREGISTER

Since the elements of the matrix F are zeros and ones, the matrix F is in one-to-one correspondence with a shiftregister. The element 1 in the ith row and jth column of the matrix F indicates that the output terminal of the ith flip-flop (storage device) and the input terminal number of the jth flip-flop are connected. The element 0 indicates non-connection.

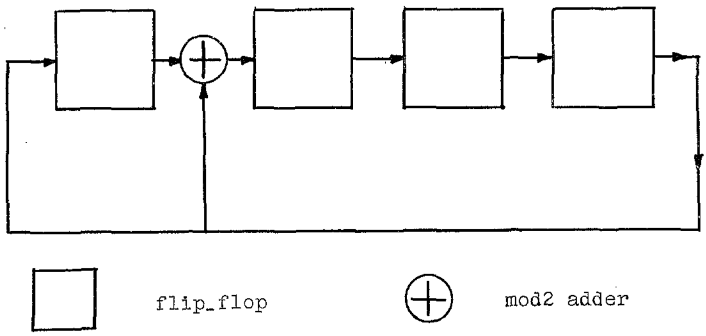

FIG. 1 Shiftregister corresponding to matrix F of (14)

For example, the element one is located in the first row and the second column of F, then the first flip-flop and the second are connected. The matrix F is called the connection matrix of its corresponding shiftregister. We illustrate the above with the following example. The matrix corresponding to the polynomial of (1) is

$$F = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}. \tag{14}$$

The shiftregister determined by this matrix is shown in Figure 1.

IV. RELATIONSHIP OF POWERS OF THE CONNECTION MATRIX TO MULTIPLICATION SHIFTREGISTERS

Multiplication circuits between elements in $GF(2^m)$ are of special interest from the viewpoint of coding theory. This section considers multiplication over $GF(2^m)$ using shiftregisters.

It is possible to easily determine multiplication circuits by performing computations with the matrix F and its powers.

THEOREM 1. *The connection matrix of the shiftregister that automatically multiplies by α^n is the matrix F^n. Hence if α^i and α^j are any elements of $GF(2^m)$, then multiplying α^i by α^j, for example,*

$$\alpha^i \cdot \alpha^j = \alpha^{i+j}$$

is carried out by shifting once the shiftregister which has initial state (contents) α^i and connection matrix F^j, where

$$F^j = f_0 \oplus f_1F \oplus f_2F^2 \oplus \cdots \oplus f_{m-1}F^{m-1}. \tag{15}$$

This multiplication circuit is shown in Figure 3.

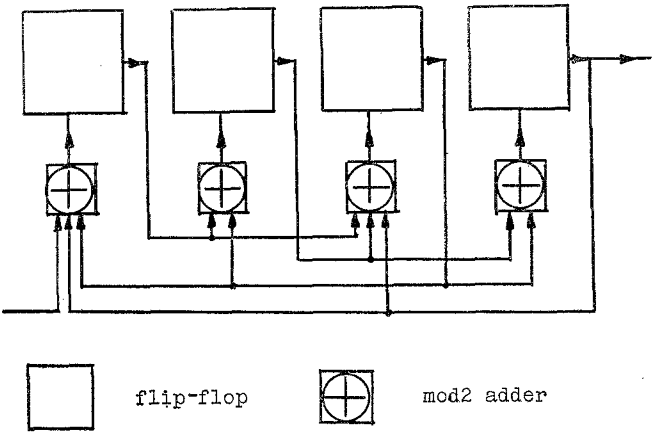

FIG. 2 Shiftregister corresponding to F^5

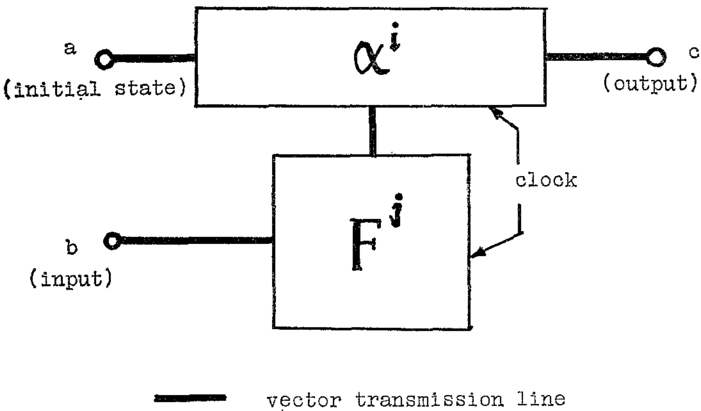

FIG. 3 Multiplication circuit

As an example, we consider the matrix F of (14) and show how to multiply α^3 by α^5. From (13) and Table II,

$$F^5 = F \cdot F^4 = F(E \oplus F) = F \oplus F^2.$$

Since

$$F = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad F^2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix},$$

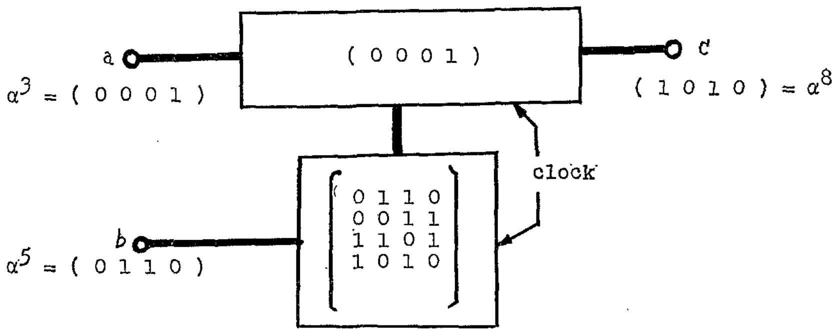

FIG. 4 Computation of $\alpha^3 \times \alpha^5$

we have

$$F^5 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

This is the connection matrix corresponding to α^5. The shiftregister having this connection matrix is shown in Figure 2. The initial state of the shiftregister is $\alpha^3 = (0001)$. The result $\alpha^3 . \alpha^5$ is computed by shifting this shiftregister once. After one bit time, the state becomes

$$\alpha^3 . \alpha^5 = (1010) = \alpha^8.$$

For simplicity the shiftregister corresponding to F^n will be pictured as in Figure 3. Figure 4 then corresponds to the preceding example.

V. POWER COMPUTATION

Shiftregisters for computing powers of elements can be determined by applying the following theorem.

THEOREM 2. *To raise any element, α^i of $GF(2^m)$ to the power n, shift once the shiftregister whose state corresponds to the element α^i, and whose connection matrix is given by*

$$(F^{n-1})^i = f_0 E \oplus f_1 F^{n-1} \oplus \cdots \oplus f_{m-1}(F^{n-1})^{m-1}, \qquad (16)$$

where the f_i $(0 \leqq i \leqq m-1)$ are the coefficients of the element α^i in $GF(2^m)$ expressed by a polynomial.

Proof. Set $n = i$ and substitute F^{n-1} for F in Theorem 1. The result of this computation is

$$\alpha^i(\alpha^{n-1})^i = \alpha^{ni} = (\alpha^i)^n. \qquad \text{Q.E.D.}$$

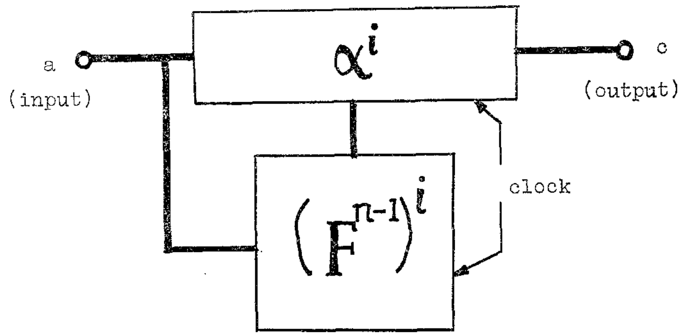

FIG. 5 Power computation circuit

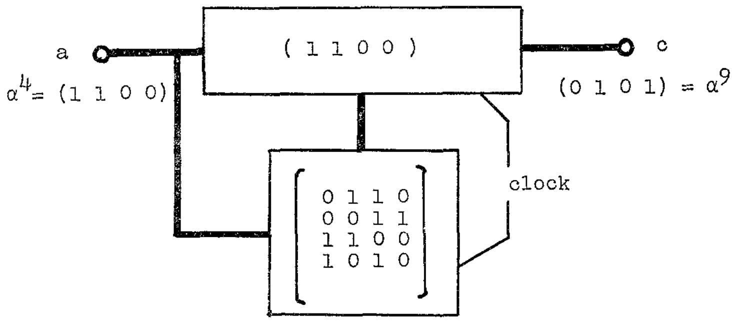

FIG. 6 Computation of α^4 to power 6

This circuit is shown in Figure 5. Hence any element in $GF(2^m)$ may be raised to the power n in one bit time, using above computational method. Note, however, that the configuration of the shiftregister depends both on the element and on the power.

For example, the procedure of computation of α^4 to power 6 proceeds as follows. We have

$$\alpha^4 = 1 + \alpha = (1100).$$

From Theorem 2, the connection matrix is

$$(F^{6-1})^4 = (F^5)^4 = F^{20} = F^5,$$

and the state is $\alpha^4 = (1100)$. Shifting once, we obtain

$$(\alpha^4)^6 = \alpha^{24} = \alpha^9 = \alpha + \alpha^3 = (0101).$$

Thus $(1100)^6 = (0101)$, as may be verified from Table II. The circuit is illustrated in Figure 6.

VI. CONCLUSION

We have developed a procedure for easily determining shiftregisters capable of performing multiplication or taking powers over $GF(2^m)$. The shiftregisters are especially useful for performing computations involved in solving either simultaneous linear equations such as Newton's identities, which arise in decoding Bose-Chaudhuri-Hocquenghem codes, or equations of higher degree in a single unknown.

ACKNOWLEDGEMENT

The authors wish to acknowledge the stimulating discussions on the subject of this paper with Dr. T. Hasegawa, who is the associate professor of Kyoto University, and the members of Kasahara Research Laboratory. The authors also would like to express deep appreciation to the referees for their kind revision.

RECEIVED: April 5, 1967, REVISED: June 20, 1968

REFERENCES

PETERSON, W. W. (1961) "Error Correcting Codes." The M.I.T. Press, Cambridge, Massachusetts.

GOLOMB, S. W. (1964) "Digital Communications." Prentice Hall, Englewood Cliffs, New Jersey.

ELSPAS, B. (1965) The theory of autonomous linear sequential networks. *I.R.E. Trans. Comm. Theory* **6**, 45–60.

TOYAMA, H. (1965) "Matrix Theory." Kyōritsu Press, Tokyo.

POSTONIKOV, M. (1964) "Galois Theory." Book translated into Japanese by K. Hino, Tokyo Press, Tokyo.