ON A MAPPING POLYNOMIAL FOR GALOIS FIELDS*

By ARTHUR GILL AND JEAN-PAUL JACOB (*University of California, Berkeley*)

1. Introduction. A number of digital processes, such as the identification of two-tone patterns, the computation of multivalued Boolean functions, the decoding of binary block codes, the addressing of "files" in the memory of a computer, etc., may be described as a many-to-one mapping from an n-dimensional space S_n (over a binary field) onto itself. This mapping can be expressed by means of a polynomial whose coefficients, to a large extent, determine the "ease" with which any of the above processes can be carried out. In searching for the "easiest" such polynomial, a common task is that of computing sets of such coefficients for specified mappings, or of computing mappings to conform with specified sets of coefficients. The purpose of this note is to show how, by a suitable representation of S_n , the relationship between the mappings and the coefficients becomes especially simple, leading to considerable simplification in the computation procedures.

2. The mapping polynomial. Consider the Galois field

$$\mathrm{GF}\,(2^n) = \{a_0\ ,\ a_1\ ,\ \cdots\ ,\ a_{2^n-1}\} \qquad (a_0 = 0). \tag{1}$$

An element a of GF(2^n) can be represented by a polynomial in ξ with coefficients from GF(2), of degree $n - 1$ or less:

$$a = \alpha_0 + \alpha_1\xi + \cdots + \alpha_{n-1}\xi^{n-1} \qquad (\alpha_j \in \mathrm{GF}\,(2),\ j = 0,\ 1,\ \cdots\ ,n - 1). \tag{2}$$

Field operations are performed modulo 2 and modulo any fixed irreducible polynomial in ξ with coefficients from GF(2), of degree n:

$$p(\xi) = \pi_0 + \pi_1\xi + \cdots + \pi_{n-1}\xi^{n-1} + \xi^n; \tag{3}$$

$p(\xi)$ is called the *modulus polynomial* of GF(2^n).

The *characteristic polynomial* of a_i is a polynomial in x with coefficients from GF(2^n), of degree $2^n - 1$ or less, defined by:

$$f_i(x) = \prod_{\nu \neq i} (x - a_\nu) = \varphi_0^{(i)} + \varphi_1^{(i)}x + \cdots + \varphi_{2^n-1}^{(i)}x^{2^n-1} \qquad (\varphi_j \in \mathrm{GF}\,(2^n),\ j = 0,\ 1,\ \cdots\ ,\ 2^n - 1). \tag{4}$$

The following two theorems are taken from Dickson [1]:

THEOREM 1.

$$f_i(a_\nu) = \begin{cases} 1, & \nu = i, \qquad (5a) \\ 0, & \nu \neq i. \qquad (5b) \end{cases}$$

Proof. From the theory of Galois fields it is known that

$$\prod_{k \neq 0} (x + a_k) = x^{2^n-1} + 1; \tag{6}$$

*Received April 26, 1965. This study was supported by the Air Force Office of Scientific Research Grant No. AFOSR-639-64 and by the Joint Services Electronics Programs (U. S. Army, U. S. Navy and U. S. Air Force) under Grant No. AFOSR-139-64.

setting $x = 0$:

$$\prod_{k \neq 0} a_k = 1. \tag{7}$$

Now,

$$f_i(a_i) = \prod_{\nu \neq i} (a_i - a_\nu) = \prod_{k \neq 0} a_k \tag{8}$$

which, by (7), implies (5a). 5(b) follows from the definition (4).

Consider the many-to-one mapping f from GF(2^n) into GF(2^n), with a_i' denoting the image of a_i . Define:

$$f(x) = \sum_{i=0}^{2^n-1} f_i(x)a_i' = \varphi_0 + \varphi_1 x + \cdots + \varphi_{2^n-1}x^{2^n-1}. \tag{9}$$

THEOREM 2.

$$f(a_j) = a_j' . \tag{10}$$

Proof.

$$f(a_j) = \sum_i f_i(a_j)a_i' = f_j(a_j)a_j' = a_j . \tag{11}$$

$f(x)$ is called the *mapping polynomial* of the mapping f. Any many-to-one mapping f from S_n into S_n may be regarded as mapping GF(2^n) into GF(2^n), and hence expressed as a mapping polynomial $f(x)$. Recognition of an element of S_n , therefore, can be performed by representing an n-tuple $(\alpha_0 , \alpha_1 , \cdots , \alpha_{n-1})$ as a polynomial $a = \alpha_0 + \alpha_1\xi + \cdots + \alpha_{n-1}\xi^{n-1}$ and computing $f(a) = a'$ as per rules of GF(2^n); the coefficients of a' are then the elements of the n-tuple which labels the class to which $(\alpha_0 , \alpha_1 , \cdots , \alpha_{n-1})$ belongs.

Clearly, any computing circuit or program devised for computing $f(x)$ requires complete information on the coefficients φ_i of $f(x)$. In general, this amounts to "remembering" all 2^n pairs (j, φ_j)—a requirement as severe as that of remembering all pairs of n-tuples which define the original mapping. In particular cases, however, it may happen that the coefficients of $f(x)$ exhibit some symmetry which obviate the requirement to remember all the (j, φ_j) pairs (for example, if φ_j is periodic with j, with the period τ, it is sufficient to remember the integer τ and the first τ pairs). These are the cases for which the mapping polynomial can be used to advantage in recognition processes where memory capacity is costlier than computation time. In searching for such cases, one has to pass repeatedly from sets of mappings to sets of polynomials, and conversely. The following section will show how this passage can be simplified.

3. Properties of coefficients of $f(x)$. For reasons which will become apparent presently, we shall always choose a maximum-period polynomial as a modulus polynomial for GF(2^n) (at least one such polynomial exists for every n). With this choice, ξ becomes a primitive element of GF(2^n), and we can write

$$a_i = \xi^{i-1} \qquad (i = 1, 2, \cdots , 2^n - 1). \tag{12}$$

In addition, the coefficients of the characteristic polynomials $f_i(x)$ assume a relatively simple structure:

THEOREM 3.

$$\varphi_j^{(0)} = \begin{cases} 1, & j = 0, 2^n - 1, \quad (13a) \\ 0, & \text{otherwise.} \quad (13b) \end{cases}$$

When $i \neq 0$:

$$\varphi_j^{(i)} = \begin{cases} \xi^{-j(i-1) \pmod{2^n-1}}, & j \neq 0, \quad (14a) \\ 0, & j = 0, \quad (14b) \end{cases}$$

Proof. (4) can be written as

$$f_i(x) = \frac{x + x^{2^n}}{x + a_i}. \quad (15)$$

When $i = 0$, $a_i = 0$ and (15) yields

$$f_0(x) = 1 + x^{2^n-1} \quad (16)$$

which implies (13a) and (13b). When $i \neq 0$, $a_i \neq 0$ and (15) can be written as

$$\frac{x + x^{2^n}}{x + a_i} = a_i^{2^n-2}x + a_i^{2^n-3}x^2 + \cdots + a_i x^{2^n-2} + x^{2^n-1} \quad (17)$$

(since $a_i^{2^n-1} = 1$). Hence $\varphi_0^{(i)} = 0$ and

$$\varphi_j^{(i)} = a_i^{2^n-1-j} = a_i^{2^n-1-j \pmod{2^n-1}} = a_i^{-j \pmod{2^n-1}}. \quad (18)$$

(14a) then follows from (12).

Let Φ be a $2^n \times 2^n$ matrix with rows $i = 0, 1, \cdots, 2^n - 1$, columns $j = 0, 1, \cdots, 2^n - 1$, and the (i, j) element $\varphi_j^{(i)}$. By Theorem 3, Φ has the general form shown in (19) (where the exponents are unique modulo $2^n - 1$). (19) places in evidence the simple structure of Φ: Row 0 has the form $10 \cdots 01$ and column 0 the form $10 \cdots 0$; from row 1 down, column $2^n - 1$ has successive powers (0 through $2^n - 2$) of ξ^0, column $2^n - 2$ successive powers of ξ^1, column $2^n - 3$ successive powers of ξ^2, $\cdots$, column 1 successive powers of ξ^{2^n-2}. The construction of Φ is simplified further by noting that the submatrix obtained by deleting row 0 and column 0 is symmetrical about the diagonal extending from the bottom left to the top right corners.

$$\Phi = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ \vdots \\ 2^n - 1 \end{array} \begin{array}{c} \begin{array}{ccccccc} 0 & 1 & \cdots & 2^n - 4 & 2^n - 3 & 2^n - 2 & 2^n - 1 \end{array} \\ \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 & 1 \\ 0 & 1 & \cdots & 1 & 1 & 1 & 1 \\ 0 & \xi^{2^n-2} & \cdots & \xi^3 & \xi^2 & \xi & 1 \\ 0 & \xi^{(2^n-2)2} & \cdots & \xi^6 & \xi^4 & \xi^2 & 1 \\ 0 & \xi^{(2^n-2)3} & \cdots & \xi^9 & \xi^6 & \xi^3 & 1 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ 0 & \xi^{(2^n-2)(2^n-2)} & \cdots & \xi^{3(2^n-2)} & \xi^{2(2^n-2)} & \xi^{2^n-2} & 1 \end{bmatrix} \end{array} \quad (19)$$

Example 1. Let $n = 3$ and $p(\xi) = 1 + \xi + \xi^3$. GF(2^3) consists of the elements

$$a_0 = 0,$$

$$\begin{aligned} a_1 &= \xi^0 = 1, \\ a_2 &= \xi^1 = \xi, \\ a_3 &= \xi^2 = \xi^2, \\ a_4 &= \xi^3 = 1 + \xi, \\ a_5 &= \xi^4 = \xi + \xi^2, \\ a_6 &= \xi^5 = 1 + \xi + \xi^2, \\ a_7 &= \xi^6 = 1 + \xi^2 \qquad (\xi^7 = 1). \end{aligned} \tag{20}$$

In this case:

$$\boldsymbol{\Phi} = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{array} \begin{array}{c} \begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \xi^6 & \xi^5 & \xi^4 & \xi^3 & \xi^2 & \xi & 1 \\ 0 & \xi^5 & \xi^3 & \xi & \xi^6 & \xi^4 & \xi^2 & 1 \\ 0 & \xi^4 & \xi & \xi^5 & \xi^2 & \xi^6 & \xi^3 & 1 \\ 0 & \xi^3 & \xi^6 & \xi^2 & \xi^5 & \xi & \xi^4 & 1 \\ 0 & \xi^2 & \xi^4 & \xi^6 & \xi & \xi^3 & \xi^5 & 1 \\ 0 & \xi & \xi^2 & \xi^3 & \xi^4 & \xi^5 & \xi^6 & 1 \end{bmatrix} \end{array} \tag{21}$$

Define the following vectors:

$$\boldsymbol{\varphi} = (\phi_0, \phi_1, \cdots, \phi_{2^n-1}), \tag{22}$$

$$\mathbf{a}' = (a'_0, a'_1, \cdots, a'_{2^n-1}). \tag{23}$$

THEOREM 4.

$$\boldsymbol{\varphi} = \mathbf{a}'\boldsymbol{\Phi}. \tag{24}$$

Proof. The jth element ($j = 0, 1, \cdots, 2^n - 1$) of $\mathbf{a}'\boldsymbol{\Phi}$ is

$$\varphi_j^{(0)} a'_0 + \varphi_j^{(1)} a'_1 + \cdots + \varphi_j^{(2^n-1)} a'_{2^n-1} \tag{25}$$

which, by (9), is the coefficient of x^j in $f(x)$.

THEOREM 5. *$\boldsymbol{\Phi}$ is nonsingular. Let its inverse $\boldsymbol{\Psi}$ have the (i, j) elements ψ_{ij} ($i, j = 0, 1, \cdots, 2^n - 1$). Then*:

$$\psi_{i0} = \begin{cases} 1, & i = 0, \qquad (26a) \\ 0, & i \neq 0. \qquad (26b) \end{cases}$$

When $j \neq 0$:

$$\psi_{ij} = \xi^{i(j-1) \pmod{2^n-1}}. \tag{27}$$

Proof. Let $\boldsymbol{\Phi}\boldsymbol{\Psi} = \mathbf{M}$, with the (i, j) elements μ_{ij}. Then, by (13a)-(14b) and (26a)-(27), we have:

$$\mu_{00} = 1, \tag{28}$$

$$\mu_{0j} = 1 + \xi^{(2^n-1)(j-1) \pmod{2^n-1}} = 0 \qquad (j \neq 0), \tag{29}$$

$$\mu_{i0} = 0 \qquad (i \neq 0). \tag{30}$$

For all $i \neq 0$, $j \neq 0$:

$$\begin{aligned}\mu_{ij} &= \sum_{\nu=0}^{2^n-1} \phi_\nu^{(i)} \psi_{\nu j} \\ &= \sum_{\nu=1}^{2^n-1} \xi^{-\nu(i-1) \pmod{2^n-1}} \xi^{\nu(j-1) \pmod{2^n-1}} \\ &= \sum_{\nu=1}^{2^n-1} \xi^{\nu(j-i) \pmod{2^n-1}}.\end{aligned}$$

When $i = j$, μ_{ij} is the sum of an odd number of 1's, and hence 1. When $i \neq j$, let $\xi^{(j-i)} = \eta$. Then

$$\begin{aligned}\mu_{ij} &= 1 + \eta + \eta^2 + \cdots + \eta^{2^n-2} \\ &= (1 + \eta^{2^n-1})/(1 + \eta) = 0.\end{aligned} \tag{31}$$

Thus, $\Phi\Psi$ is the identity matrix and $\Psi = \Phi^{-1}$.

$$\Psi = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ \vdots \\ 2^n-2 \\ 2^n-1 \end{array} \begin{array}{c} \begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & \cdots & 2^n-1 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \xi^3 & \cdots & \xi^{2^n-2} \\ 0 & 1 & \xi^2 & \xi^4 & \xi^6 & \cdots & \xi^{(2^n-2)2} \\ 0 & 1 & \xi^3 & \xi^6 & \xi^9 & \cdots & \xi^{(2^n-2)3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & \xi^{2^n-2} & \xi^{2(2^n-1)} & \xi^{3(2^n-1)} & \cdots & \xi^{(2^n-2)(2^n-2)} \\ 0 & 1 & 1 & 1 & 1 & \cdots & 1 \end{bmatrix} \end{array} \tag{32}$$

Theorem 5 implies that Ψ has the general form shown in (32) (where the exponents are unique modulo $2^n - 1$). Note that Φ with row 0 and column 0 omitted and Ψ with row $2^n - 1$ and column 0 omitted are identical except for reversal in the order of columns. For example, if Φ is as given in (21), Ψ is the matrix shown in (33).

$$\Psi = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{array} \begin{array}{c} \begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & \xi & \xi^2 & \xi^3 & \xi^4 & \xi^5 & \xi^6 \\ 0 & 1 & \xi^2 & \xi^4 & \xi^6 & \xi & \xi^3 & \xi^5 \\ 0 & 1 & \xi^3 & \xi^6 & \xi^2 & \xi^5 & \xi & \xi^4 \\ 0 & 1 & \xi^4 & \xi & \xi^5 & \xi^2 & \xi^6 & \xi^3 \\ 0 & 1 & \xi^5 & \xi^3 & \xi & \xi^6 & \xi^4 & \xi^2 \\ 0 & 1 & \xi^6 & \xi^5 & \xi^4 & \xi^3 & \xi^2 & \xi \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \end{array} \tag{33}$$

Thus, we can write

$$\mathbf{a}' = \varphi\Psi^{r}. \tag{34}$$

By means of (24), the mapping polynomial $f(x)$ can be readily computed for any specified mapping $a \rightarrow a'$. By means of (34), one can compute the mapping $a \rightarrow a'$ corresponding to any specified mapping polynomial $f(x)$ (for example, a polynomial whose coefficients exhibit some symmetry or periodicity).

Reference

1. L. E. Dickson, *Linear groups with an exposition of the Galois field theory*, pp. 53–55, Dover Publications, Inc., New York, 1958