

A Generalized Algorithm to Design Finite Field Normal Basis Multipliers

C. C. Wang

Communications Systems Research Section

Finite field arithmetic logic is central in the implementation of some error-correcting coders and some cryptographic devices. There is a need for good multiplication algorithms which can be easily realized. Massey and Omura recently developed a new multiplication algorithm for finite fields based on a normal basis representation. Using the normal basis representation, the design of the finite field multiplier is simple and regular. The fundamental design of the Massey-Omura multiplier is based on a design of a product function. In this article, a generalized algorithm to locate a normal basis in a field is first presented. Using this normal basis, an algorithm to construct the product function is then developed. This design does not depend on particular characteristics of the generator polynomial of the field.

I. Introduction

The finite field $GF(2^m)$ is a number system containing 2^m elements. Its attractiveness in practical applications stems from the fact that each element can be represented by m binary digits. The practical application of error-correcting codes makes considerable use of computation in $GF(2^m)$. Both the encoding and decoding devices for the important Reed-Solomon codes must perform computations in $GF(2^m)$ (Refs. 1, 2). The decoding device for the binary BCH codes also must perform computation in $GF(2^m)$ (Refs. 1, 2). On the other hand, recent advances in secret communications, such as encryption and decryption of digital messages, also require the use of computation in $GF(2^m)$ (Ref. 3). Hence, there is a need for good algorithms for doing multiplication in a finite field.

Yeh, Reed and Truong (Ref. 4) presented a design for performing multiplication in $GF(2^m)$ which is suitable for VLSI implementation. In their design, the elements in the field are represented by a canonical basis $\{1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{m-1}\}$ where α is a root of an irreducible polynomial of degree m over $GF(2)$. Some other previous work on multipliers in $GF(2^m)$ by Bartee and Schneider (Ref. 5), Gallager (Ref. 6), and Laws and Rushforth (Ref. 7) is also based on the canonical basis of $GF(2^m)$. However, these circuits are not as well suited for use in VLSI systems, due to irregular wire routing and complicated control problems as well as non-modular structure or lack of concurrency (Ref. 8).

Recently, Massey and Omura (Ref. 9) invented a multiplier which obtains the product of two elements in the finite field $GF(2^m)$. In their invention, they utilize a normal basis

of the form $\{\alpha, \alpha^2, \alpha^4, \dots, \alpha^{2^{m-1}}\}$ to represent elements of the field. In this basis, again, each element in the field $GF(2^m)$ can be represented by m binary digits.

In the normal-basis representation the squaring of an element in $GF(2^m)$ is readily shown (Ref. 10) to be a simple cyclic shift of its binary digits. In the normal basis representations, multiplication requires the same logic function for any one bit of the product as it does for any other (Ref. 10). The generation of adjacent product digits differs only in the inputs, which are cyclically shifted versions of one another, to this product function. Hence, designing a Massey-Omura multiplier is exactly the same as designing a product function. In Ref. 10, a pipeline architecture suitable for VLSI design has been developed for a Massey-Omura multiplier of $GF(2^m)$. In comparison with the multiplier designed in Ref. 4, the Massey-Omura multiplier is much simpler.

In Ref. 10, the design of a Massey-Omura multiplier is based on a normal basis

$$\{\alpha, \alpha^2, \alpha^{2^2}, \dots, \alpha^{2^{m-1}}\} \quad (1)$$

which is the set of roots of an irreducible polynomial

$$P(x) = x^m + c_1 x^{m-1} + \dots + c_m \quad (2)$$

over $GF(2)$.

In general, to verify the linear independence of the roots in Eq. (1) is difficult. A straightforward way to do this is to represent α^{2^i} , $i = 0, 1, \dots, m-1$, by m -dimensional vectors in canonical basis $\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$ and then to check whether the $m \times m$ matrix composed by the above m vectors is nonsingular. For large m , this method requires a great number of computations. Peterson and Weldon (Ref. 2) list a set of irreducible polynomials of degree $m \leq 34$ over $GF(2)$ for which the roots are linearly independent.

For the case of $m = 2^n$, Perlis (Ref. 11) has shown that a necessary and sufficient condition for the above set (Eq. [1]) to be a normal basis of $GF(2^m)$ is the trace of α obeying the relation

$$Tr(\alpha) \triangleq \alpha + \alpha^2 + \alpha^{2^2} + \dots + \alpha^{2^{m-1}} = 1$$

or, equivalently, the coefficient c_1 in Eq. (2) is 1. He also gave necessary and sufficient conditions for a normal basis of $GF(2^m)$ when $m = p^n$ with prime p . Berlekamp (Ref. 12, p. 254), and Lidl and Niederreiter (Ref. 13, p. 124) have also

given a formula to compute the number of elements which can generate a normal basis in $GF(2^m)$. Wah and Wang (Refs. 14, 16) have shown that the so-called all-one-polynomial of degree m is irreducible and its roots constitute a normal basis if and only if $m+1$ is a prime and 2 is primitive mod $(m+1)$. Pei, Wang and Omura (Ref. 15) have also presented necessary and sufficient conditions for an element to generate a normal basis in the field $GF(2^m)$ for the case that $m = 2^k p^n$ where p is an odd prime, k is a non-negative integer, n is a positive integer and p^n has 2 as one of its primitive roots. These conditions can be used to find a normal basis in $GF(2^m)$, if m is of the given form. Using this normal basis as the roots, one can construct an irreducible polynomial of degree m and, therefore, use the algorithm described in Ref. 10 to design the Massey-Omura multiplier.

In this article, a new algorithm to locate a normal basis in *any* field $GF(2^m)$ is presented. In this algorithm, a special $m \times m$ matrix needs to be set up and its nonsingularity needs to be verified. For large m , this algorithm also seems to be very time consuming. However, due to some special properties of this matrix, the matrix set up procedure only requires m , rather than $m \times m$ entry computations, and, the verification of the nonsingularity can be based on some quick check rules, resulting in a saving of a tremendous amount of computation time. Using this normal basis, a methodology to construct the product function of the Massey-Omura multiplier is also developed in this article. This approach uses the concept of dual basis. It is shown that the coefficients of the product function are the trace values of some particular elements in $GF(2^m)$. These particular elements can be computed by the normal basis used and its dual basis. Hence, the design of a Massey-Omura multiplier can be based on any arbitrary normal basis in $GF(2^m)$ which need not be the roots of the generator polynomial.

II. Dual Basis Approach of Designing Massey-Omura Finite Field Multiplier

Two bases $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ and $\{\beta_1, \beta_2, \dots, \beta_m\}$ are said to be dual, or complementary, if

$$Tr(\alpha_i \beta_j) = \delta_{ij} = \begin{cases} 0 & \text{for } i \neq j \\ 1 & \text{for } i = j \end{cases} \quad (3)$$

Seven useful properties of a finite field $GF(2^m)$ are stated here without proof (for proofs see Refs. 1 and 16). These properties are as follows:

- (1) Trace is a linear operation over $GF(2)$.

(2) For every $\alpha \in GF(2^m)$

$$Tr(\alpha^2) = [Tr(\alpha)]^2 = Tr(\alpha) \in GF(2)$$

(3) $Tr(1) = m \bmod 2$

(4) If $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ and $\{\beta_1, \beta_2, \dots, \beta_m\}$ are two bases and dual to each other, for any $x \in GF(2^m)$,

$$\begin{aligned} x &= \sum_{i=1}^m a_i \cdot \alpha_i \\ &= \sum_{i=1}^m Tr(x \cdot \beta_i) \cdot \alpha_i \end{aligned}$$

(5) Every basis has a dual basis.

(6) A normal basis exists in any field $GF(2^m)$.

(7) The dual basis of a normal basis is also a normal basis.

Suppose that $\{\alpha, \alpha^2, \alpha^{2^2}, \dots, \alpha^{2^{m-1}}\}$ is a normal basis of field $GF(2^m)$, and $\{\beta, \beta^2, \beta^{2^2}, \dots, \beta^{2^{m-1}}\}$ is its dual basis. For any two elements y and z in $GF(2^m)$, they can be expressed as

$$\begin{aligned} y &= y_0 \alpha + y_1 \alpha^2 + y_2 \alpha^{2^2} + \dots + y_{m-1} \alpha^{2^{m-1}} \\ &= \sum_{j=0}^{m-1} y_j \alpha^{2^j} \\ z &= z_0 \alpha + z_1 \alpha^2 + z_2 \alpha^{2^2} + \dots + z_{m-1} \alpha^{2^{m-1}} \\ &= \sum_{i=0}^{m-1} z_i \alpha^{2^i} \end{aligned}$$

Let

$$\begin{aligned} \omega &= y \cdot z \\ &= \omega_0 \alpha + \omega_1 \alpha^2 + \omega_2 \alpha^{2^2} + \dots + \omega_{m-1} \alpha^{2^{m-1}} \\ &= \sum_{k=0}^{m-1} \omega_k \alpha^{2^k} \end{aligned}$$

By property (4)

$$\begin{aligned} \omega_k &= Tr(\omega \beta^{2^k}) \\ &= Tr(yz \beta^{2^k}) \\ &= Tr\left(\sum_{i=0}^{m-1} y_i \alpha^{2^i} \sum_{j=0}^{m-1} z_j \alpha^{2^j} \cdot \beta^{2^k}\right) \\ &= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} y_i z_j Tr(\alpha^{2^i} \cdot \alpha^{2^j} \cdot \beta^{2^k}) \end{aligned} \quad (4)$$

Lemma 1

$$Tr(\alpha^{2^i} \cdot \alpha^{2^j} \cdot \beta^{2^k}) = Tr(\alpha^{2^{\bar{i}-1}} \cdot \alpha^{2^{\bar{j}-1}} \cdot \beta^{2^{\bar{k}-1}})$$

where

$$\bar{i} \triangleq i \bmod m$$

Proof: The lemma follows from the fact that $x^{2^m} = x$ and $Tr(x^2) = Tr(x)$ (Property 2) for any $x \in GF(2^m)$.

Theorem 2

$$\omega_{k-1} = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} y'_i z'_j Tr(\alpha^{2^i} \cdot \alpha^{2^j} \cdot \beta^{2^k})$$

where

$$y'_i = y_{\bar{i}-1}$$

Proof: From Eq. (4),

$$\begin{aligned} \omega_{k-1} &= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} y_i z_j Tr(\alpha^{2^i} \cdot \alpha^{2^j} \cdot \beta^{2^{k-1}}) \\ &= \sum_{i=1}^m \sum_{j=1}^m y_{i-1} z_{j-1} Tr(\alpha^{2^{i-1}} \cdot \alpha^{2^{j-1}} \cdot \beta^{2^{k-1}}) \\ &= \sum_{i=1}^m \sum_{j=1}^m y_{i-1} z_{j-1} Tr(\alpha^{2^i} \cdot \alpha^{2^j} \cdot \beta^{2^k}) \end{aligned}$$

Since

$$y'_0 = y_{m-1} \text{ and } z'_0 = z_{m-1}$$

$$\omega_{k-1} = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} y'_i z'_j \text{Tr}(\alpha^{2^i} \cdot \alpha^{2^j} \cdot \beta^{2^k})$$

Let f be a $2m$ -dimensional function such that

$$\begin{aligned} \omega_{m-1} &= f(y_0, y_1, \dots, y_{m-1}; z_0, z_1, \dots, z_{m-1}) \\ &\triangleq \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} y_i z_j \text{Tr}(\alpha^{2^i} \cdot \alpha^{2^j} \cdot \beta^{2^{m-1}}) \\ &= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \rho_{ij} y_i z_j \end{aligned}$$

where $\rho_{ij} \triangleq \text{Tr}(\alpha^{2^i} \cdot \alpha^{2^j} \cdot \beta^{2^{m-1}})$. Since $\{y'_i\}$ is the cyclically shifted version of $\{y_i\}$, by Theorem 2,

$$\begin{aligned} \omega_{m-2} &= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} y'_i z'_j \text{Tr}(\alpha^{2^i} \cdot \alpha^{2^j} \cdot \beta^{2^{m-1}}) \\ &= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \rho_{ij} y'_i z'_j \\ &= f(y_{m-1}, y_0, y_1, \dots, y_{m-2}; \\ &\quad z_{m-1}, z_0, z_1, \dots, z_{m-2}) \end{aligned}$$

Applying this technique repeatedly, one can obtain

$$\left. \begin{aligned} \omega_{m-1} &= f(y_0, y_1, y_2, \dots, y_{m-1}; \\ &\quad z_0, z_1, z_2, \dots, z_{m-1}) \\ \omega_{m-2} &= f(y_{m-1}, y_0, y_1, \dots, y_{m-2}; \\ &\quad z_{m-1}, z_0, z_1, \dots, z_{m-2}) \\ &\vdots \\ \omega_1 &= f(y_2, y_3, \dots, y_{m-1}, y_0, y_1; \\ &\quad z_2, z_3, \dots, z_{m-1}, z_0, z_1) \\ \omega_0 &= f(y_1, y_2, \dots, y_{m-1}, y_0; \\ &\quad z_1, z_2, \dots, z_{m-1}, z_0) \end{aligned} \right\} (5)$$

where

$$f(a_0, a_1, \dots, a_{m-1}; b_0, b_1, \dots, b_{m-1}) = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \rho_{ij} a_i b_j \quad (5a)$$

with

$$\rho_{ij} = \text{Tr}(\alpha^{2^i} \cdot \alpha^{2^j} \cdot \beta^{2^{m-1}}) \quad (5b)$$

In Eq. (5), it is shown that the product components ω_i , $i = 0, 1, \dots, m-1$, can be obtained by the same logic function f operating on the cyclically shifted versions of the components of multiplicand and multiplier. This function f , the so-called product function, defines the Massey-Omura multiplier (Refs. 9, 10). It is illustrated from Eqs. (5), (5a) and (5b) that the product function f only depends on the normal basis $\{\alpha, \alpha^2, \dots, \alpha^{2^{m-1}}\}$ used since β also depends on α and that its coefficients are the trace values of some elements in $GF(2^m)$. These elements can be computed by multiplying the components of the normal basis and the last component $\beta^{2^{m-1}}$ of its dual basis. Unlike the method described in Ref. 10, the construction of the product function f in this article is independent of the characteristic of the generating polynomial of $GF(2^m)$. Hence, this method gives an advantage that one can use any *arbitrary* irreducible polynomial of degree m to generate the field $GF(2^m)$.

III. Properties of the Associated Boolean Matrix

An equivalent way to represent the product function f of Eq. (5) is by means of a Boolean matrix

$$\Omega \triangleq [\rho_{ij}]_{i,j=0}^{m-1} \quad (6)$$

where

$$\rho_{ij} = \text{Tr}(\alpha^{2^i} \cdot \alpha^{2^j} \cdot \beta^{2^{m-1}}) \quad (6a)$$

is the coefficient of $a_i b_j$ in Eq. (5a).

Since to design a Massey-Omura multiplier is essentially to design a product function, the construction of the Boolean matrix Ω in Eq. (6) becomes the central issue of the design. The following theorems show some properties of the Boolean matrix.

Theorem 3. The matrix Ω is symmetric, that is, $\rho_{ij} = \rho_{ji}$.

Proof. This is obvious from the definition of ρ_{ij} in Eq. (6a).

Theorem 4

$$\rho_{ii} = \begin{cases} 0, & \text{if } i \neq m-2 \\ 1, & \text{if } i = m-2 \end{cases}$$

Proof

$$\begin{aligned} \rho_{ii} &= Tr(\alpha^{2^i} \cdot \alpha^{2^i} \cdot \beta^{2^{m-1}}) \\ &= Tr(\alpha^{2^{i+1}} \cdot \beta^{2^{m-1}}) \\ &= \delta_{i(m-2)} \\ &= \begin{cases} 0, & \text{if } i \neq m-2 \\ 1, & \text{if } i = m-2 \end{cases} \end{aligned}$$

Theorem 5

$$\sum_{i=0}^{m-1} \rho_{ij} = \begin{cases} 0, & j \neq m-1 \\ 1, & j = m-1 \end{cases}$$

Proof

$$\begin{aligned} \sum_{i=0}^{m-1} \rho_{ij} &= Tr\left(\sum_{i=0}^{m-1} \alpha^{2^i} \cdot \alpha^{2^j} \cdot \beta^{2^{m-1}}\right) \\ &= Tr(\alpha^{2^j} \cdot \beta^{2^{m-1}}) \\ &= \delta_{j(m-1)} \\ &= \begin{cases} 0, & j \neq m-1; \\ 1, & j = m-1 \end{cases} \end{aligned}$$

From theorems 3 and 4, one can conclude that in the Boolean matrix Ω only the $(m^2 - m)/2$ entry values in the upper-right triangular portion must be computed, with the diagonal values being fixed. Theorem 5 shows that there are an odd number of 1's in the last row and last column, and, an even number of 1's in the remaining rows and columns. This gives a very simple check on the correctness of the Boolean matrix.

Once the Boolean matrix is formed, the design of the Massey-Omura multiplier can proceed as described in Ref. 10. However, there are two important issues which must be addressed.

- (1) How can one find a normal basis in $GF(2^m)$ if the generating irreducible polynomial of this field does not provide linearly independent roots?
- (2) How can one find the dual basis of a normal basis in $GF(2^m)$? In the next section we will address these two issues.

IV. Locating a Normal Basis in $GF(2^m)$

Suppose that $\{\alpha, \alpha^2, \alpha^4, \dots, \alpha^{2^{m-1}}\}$ is a normal basis in $GF(2^m)$. From properties (5) and (7) of section II, its dual basis $\{\beta, \beta^2, \dots, \beta^{2^{m-1}}\}$, which is also normal, must exist in $GF(2^m)$. Since $\{\beta, \beta^2, \dots, \beta^{2^{m-1}}\}$ is a basis of $GF(2^m)$, element α can be expressed as

$$\alpha = a_0 \beta + a_1 \beta^2 + \dots + a_{m-1} \beta^{2^{m-1}} \quad (7)$$

where $a_j \in GF(2)$ for $j = 0, 1, \dots, m-1$. By squaring Eq. (7) repeatedly and applying the property that $\beta^{2^m} = \beta$, one can write

$$\begin{bmatrix} \alpha \\ \alpha^2 \\ \alpha^4 \\ \cdot \\ \cdot \\ \cdot \\ \alpha^{2^{m-1}} \end{bmatrix} = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{m-1} \\ a_{m-1} & a_0 & a_1 & \cdots & a_{m-2} \\ a_{m-2} & a_{m-1} & a_0 & \cdots & a_{m-3} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{bmatrix} \begin{bmatrix} \beta \\ \beta^2 \\ \beta^4 \\ \cdot \\ \cdot \\ \cdot \\ \beta^{2^{m-1}} \end{bmatrix} \quad (8)$$

$$\triangleq A \cdot \begin{bmatrix} \beta \\ \beta^2 \\ \beta^4 \\ \cdot \\ \cdot \\ \cdot \\ \beta^{2^{m-1}} \end{bmatrix}$$

Multiplying both sides of Eq. (8) by a row vector $[\alpha \alpha^2 \alpha^4 \cdots \alpha^{2^{m-1}}]$, we have

$$\begin{bmatrix} \alpha^2 & \alpha^3 & \alpha^5 & \dots & \alpha^{(2^{m-1}+1)} \\ \alpha^3 & \alpha^4 & \alpha^6 & \dots & \alpha^{(2^{m-1}+2)} \\ \alpha^5 & \alpha^6 & \alpha^8 & \dots & \alpha^{(2^{m-1}+4)} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \alpha^{(2^{m-1}+1)} & \alpha^{(2^{m-1}+2)} & \alpha^{(2^{m-1}+4)} & \dots & \alpha^{2^m} \end{bmatrix}$$

$$= \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{m-1} \\ a_{m-1} & a_0 & a_1 & \dots & a_{m-1} \\ a_{m-2} & a_{m-1} & a_0 & \dots & a_{m-3} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1 & a_2 & a_3 & \dots & a_0 \end{bmatrix}$$

$$\cdot \begin{bmatrix} \beta\alpha & \beta\alpha^2 & \beta\alpha^4 & \dots & \beta\alpha^{2^{m-1}} \\ \beta^2\alpha & \beta^2\alpha^2 & \beta^2\alpha^4 & \dots & \beta^2\alpha^{2^{m-1}} \\ \beta^4\alpha & \beta^4\alpha^2 & \beta^4\alpha^4 & \dots & \beta^4\alpha^{2^{m-1}} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \beta^{2^{m-1}}\alpha & \beta^{2^{m-1}}\alpha^2 & \beta^{2^{m-1}}\alpha^4 & \dots & \beta^{2^{m-1}}\alpha^{2^{m-1}} \end{bmatrix} \quad (9)$$

Since the trace function is linear over $GF(2)$, applying the trace function to both sides of Eq. (9) results in

$$\mathbf{F} = \mathbf{A} \cdot \mathbf{I} = \mathbf{A} \quad (10)$$

where \mathbf{F} is an m by m matrix with (i, j) entry

$$F_{ij} = \text{Tr}(\alpha^{2^i} \cdot \alpha^{2^j}) \quad (11)$$

for $i, j = 0, 1, 2, \dots, m-1$. Notice that \mathbf{F} depends only on α . Hence Eq. (8) can be written as

$$\begin{bmatrix} \alpha \\ \alpha^2 \\ \alpha^4 \\ \cdot \\ \cdot \\ \cdot \\ \alpha^{2^{m-1}} \end{bmatrix} = \mathbf{F}(\alpha) \cdot \begin{bmatrix} \beta \\ \beta^2 \\ \beta^4 \\ \cdot \\ \cdot \\ \cdot \\ \beta^{2^{m-1}} \end{bmatrix} \quad (12)$$

Theorem 6. For $\alpha \in GF(2^m)$, $\alpha, \alpha^2, \alpha^4, \dots, \alpha^{2^{m-1}}$ are linearly independent if and only if $\mathbf{F}(\alpha)$ is invertible.

Proof. Only the proof of the sufficient condition is necessary since the proof of the necessary condition is trivial and well known. If $\alpha, \alpha^2, \alpha^4, \dots, \alpha^{2^{m-1}}$ are linearly dependent, there exist c'_i 's, $i = 0, 1, \dots, m-1$ in $GF(2)$ which are not all zeros such that

$$\sum_{i=0}^{m-1} c'_i \alpha^{2^i} = 0$$

Multiplying both sides by α^{2^j} for $j = 0, 1, \dots, m-1$,

$$\sum_{i=0}^{m-1} c'_i \alpha^{2^i} \cdot \alpha^{2^j} = 0$$

Taking the trace values on both sides, one has

$$\sum_{i=0}^{m-1} c'_i \text{Tr}(\alpha^{2^i} \cdot \alpha^{2^j}) = \sum_{i=0}^{m-1} c'_i F_{ij} = 0$$

for all $j = 0, 1, 2, \dots, m-1$. Thus, \mathbf{F} is not invertible and the theorem is proved.

From Eq. (12), if \mathbf{F} is invertible, the dual basis $\{\beta, \beta^2, \dots, \beta^{2^{m-1}}\}$ of the normal basis $\{\alpha, \alpha^2, \dots, \alpha^{2^{m-1}}\}$ can be computed by

$$\begin{bmatrix} \beta \\ \beta^2 \\ \vdots \\ \beta^{2^{m-1}} \end{bmatrix} = \mathbf{F}^{-1}(\alpha) \cdot \begin{bmatrix} \alpha \\ \alpha^2 \\ \vdots \\ \alpha^{2^{m-1}} \end{bmatrix} \quad (13)$$

V. Construction of the Boolean Matrix

Now, an algorithm to construct the Boolean matrix Ω for the multiplication in $GF(2^m)$ can be developed. Starting with an arbitrary element α in $GF(2^m)$ (for example, a root of the generating polynomial), one can set up the matrix $\mathbf{F}(\alpha)$ as given by Eq. (11) and then check whether $\mathbf{F}(\alpha)$ is invertible. If it is, $\{\alpha, \alpha^2, \dots, \alpha^{2^{m-1}}\}$ is a normal basis; otherwise, repeat the process with another element α in $GF(2^m)$ until the corresponding $\mathbf{F}(\alpha)$ is invertible. The dual basis $\{\beta, \beta^2, \beta^4, \dots, \beta^{2^{m-1}}\}$ of $\{\alpha, \alpha^2, \alpha^4, \dots, \alpha^{2^{m-1}}\}$ then can be formed by Eq. (13). Finally, using Eq. (6) together with the Theorems 3 and 4 in Section III, we can construct the Boolean matrix Ω . Figure 1 shows the flow chart of constructing the Boolean matrix Ω for the multiplication in $GF(2^m)$.

In the procedure of Fig. 1, setting up the matrix $\mathbf{F}(\alpha)$ seems to be very time consuming since it requires trace computations for m^2 elements. However, it should be pointed out that, since $Tr(\alpha^2) = Tr(\alpha)$ and $\alpha^2 = \alpha$ for any α in $GF(2^m)$, $F_{\bar{i}+1, \bar{j}+1}(\alpha) = F_{ij}(\alpha)$ where $\bar{i} = i \bmod m$. This implies that the $(i+1)$ th row or column of $\mathbf{F}(\alpha)$ is the cyclically shifted version of the i th row or column. Hence, only the first row or column of $\mathbf{F}(\alpha)$ must be computed. Appendix A illustrates a way to compute the trace value for any element in $GF(2^m)$.

Traditionally, a Gaussian elimination algorithm can be used to verify whether $\mathbf{F}(\alpha)$ is invertible or not. However, a few conditions for $\mathbf{F}(\alpha)$ to be invertible can be checked before actually performing the Gaussian elimination algorithm,

resulting in a saving of a significant amount of computation time. The following theorems describe these conditions.

Theorem 7. If $Tr(\alpha) = 0$, $\mathbf{F}(\alpha)$ is not invertible.

Proof. This is obvious because $Tr(\alpha) = 0$ implies that $\{\alpha, \alpha^2, \alpha^4, \dots, \alpha^{2^{m-1}}\}$ are linearly dependent.

Theorem 8. If $Tr(\alpha \alpha^{2^i}) = 1$ for all $i = 0, 1, \dots, m-1$, $\mathbf{F}(\alpha)$ is not invertible.

Proof. Since $F_{\bar{i}+1, \bar{i}+1}(\alpha) = F_{ij}(\alpha)$, the condition of $Tr(\alpha \alpha^{2^i}) = 1$ for all i results in an all-one matrix $\mathbf{F}(\alpha)$ which is not invertible.

Theorem 9. If m is even and $Tr(\alpha) = Tr(\alpha^{2^{m/2} + 1})$, $\mathbf{F}(\alpha)$ is not invertible. The following two lemmas are required to prove this theorem.

Lemma 10. If the first row of matrix $\mathbf{F}(\alpha)$ has an even number of 1's, $\mathbf{F}(\alpha)$ is not invertible.

Proof. Since the $(i+1)$ th row of $\mathbf{F}(\alpha)$ is the cyclically shifted version of the i th row, this condition means that $\mathbf{F}(\alpha)$ has an even number of 1's in all rows. Adding up all column vectors results in an all-zero vector. Hence $\mathbf{F}(\alpha)$ is not invertible.

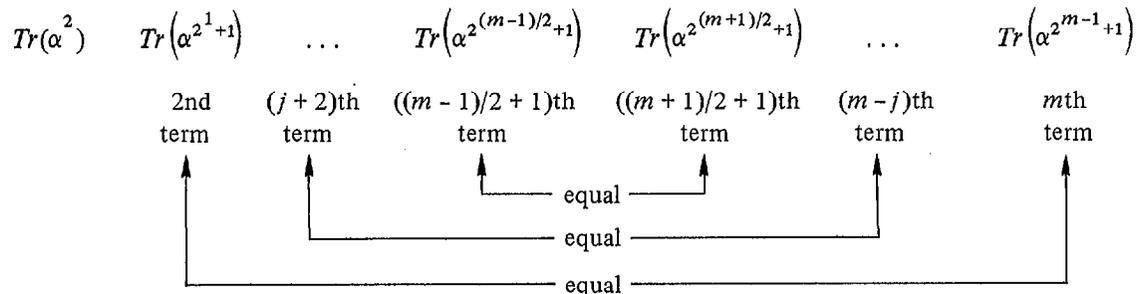
Lemma 11. $Tr(\alpha^{2^j+1}) = Tr(\alpha^{2^{m-j}+1})$ for $1 \leq j < m/2$.

Proof

$$\begin{aligned} Tr(\alpha^{2^{m-j}+1}) &= Tr\left[\left(\alpha^{2^{m-j}+1}\right) 2^j\right] = Tr(\alpha^{2^m+2^j}) \\ &= Tr(\alpha^{2^j+1}) \end{aligned}$$

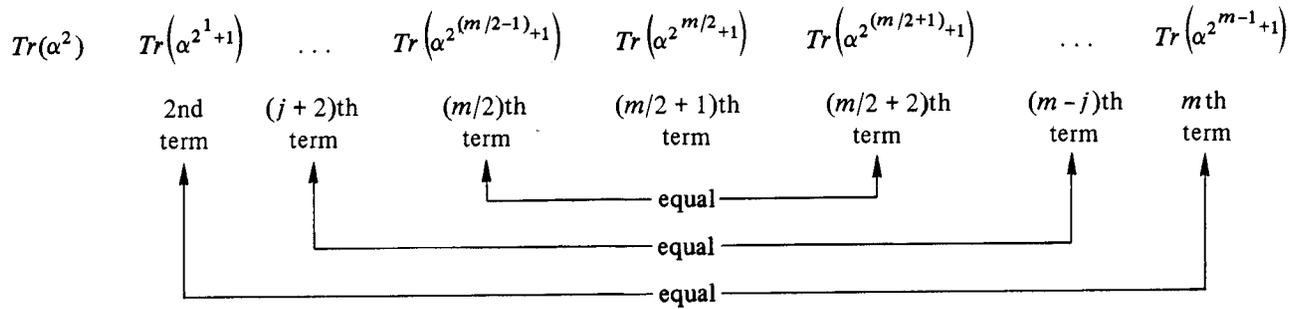
Lemma 11 implies that the $(j+1)$ th element from the left of the first row vector of $\mathbf{F}(\alpha)$ is equal to the j th element from the right. Lemma 10 and Lemma 11 lead to the following two properties.

- (1) When m is odd, the first row vector of the matrix $\mathbf{F}(\alpha)$ has the structure



Therefore if the first element $Tr(\alpha^2) = 0$, $F(\alpha)$ is not invertible. This is equivalent to the Theorem 7 since $Tr(\alpha) = Tr(\alpha^2)$.

(2) When m is even, the structure of the first row of $F(\alpha)$ becomes



This implies that if $Tr(\alpha) = Tr(\alpha^{2^{m/2+1}})$, $F(\alpha)$ is not invertible since there are an even number of 1's in the first row. Hence, Theorem 9 is proved.

VI. Example and Results

This section gives an example of designing the Massey-Omura multiplier for $GF(2^7)$. Let $P(x) = x^7 + x^3 + 1$ be the generating polynomial of $GF(2^7)$. Suppose that θ is a root of $P(x)$. Note that the roots $\{\theta, \theta^2, \theta^4, \theta^2^3, \theta^2^4, \theta^2^5, \theta^2^6\}$ are not linearly independent. By Eq. (A-3), the trace values of the canonical basis, $\{Tr(\theta^i) | i=0, 1, \dots, 6\}$ are $\{1, 0, 0, 0, 0, 0, 0\}$.

- (1) Let $\alpha = \theta$. By Theorem 7, $F(\alpha)$ is not invertible since $Tr(\alpha) = 0$.
- (2) Let $\alpha = 1 + \theta$. Then $Tr(\alpha \alpha^{2^i}) = 1$ for all $i = 0, 1, \dots, m - 1$. By Theorem 8, $F(\alpha)$ is not invertible.
- (3) Let $\alpha = \theta^2$. $Tr(\alpha) = 0$ and $F(\alpha)$ is not invertible.
- (4) Let $\alpha = 1 + \theta^2$. $Tr(\alpha \alpha^{2^i}) = 1$ for all $i = 0, \dots, m - 1$. The matrix $F(\alpha)$ is not invertible.
- (5) Let $\alpha = \theta + \theta^2$. $Tr(\alpha) = 0$. The matrix $F(\alpha)$ is not invertible.
- (6) Let $\alpha = 1 + \theta + \theta^2$. $Tr(\alpha \cdot \alpha^{2^i}) = 1$ for all $i = 0, \dots, m - 1$. The matrix $F(\alpha)$ is not invertible.
- (7) Let $\alpha = \theta^3$. $Tr(\alpha) = 0$. The matrix $F(\alpha)$ is not invertible.
- (8) Let $\alpha = 1 + \theta^3$.

$$F(\alpha) = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

is invertible and its inverse is given by

$$F^{-1}(\alpha) = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Hence $\{\alpha, \alpha^2, \dots, \alpha^{2^{m-1}}\}$ is a normal basis

(9) The dual basis $\{\beta\}$ of $\{\alpha\}$ is given by

$$\begin{bmatrix} \beta \\ \beta^2 \\ \beta^4 \\ \cdot \\ \cdot \\ \beta^{2^6} \end{bmatrix} = F^{-1}(\alpha) \cdot \begin{bmatrix} \alpha \\ \alpha^2 \\ \alpha^4 \\ \cdot \\ \cdot \\ \alpha^{2^6} \end{bmatrix}$$

Therefore

$$\begin{aligned} \beta &= \alpha + \alpha^2 + \alpha^8 + \alpha^{16} + \alpha^{64} \\ &= 1 + \theta + \theta^3 + \theta^6 \end{aligned}$$

(10) Finally,

$$\Omega = [Tr(\alpha^{2^i} \cdot \alpha^{2^j} \cdot \beta^{2^{m-1}})]_{i,j=0}^{m-1}$$

$$= \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Once the Boolean matrix is constructed, the product function is defined. Then the implementation of the Massey-Omura multiplier of $GF(2^7)$ can be designed as described in Ref. 10. Figures 2-4 give Boolean matrices for $m = 8, 17$ and 30 , respectively. Reference 16 also gives a Boolean matrix for $m = 127$. It should be pointed out that, in our experience of searching the Boolean matrix, the above-mentioned three quick ways as to verifying the invertibility of $F(\alpha)$ given in Theorems 7 through 9 are the primary verification rules that the procedure has gone through. In other words, our experience indicates that, in the process of constructing the Boolean matrix shown in Fig. 1, the most time-consuming matrix inversion procedure in the Gaussian elimination method is unlikely to be needed to rule out the candidate α , resulting in

a saving of a great deal of time. Figure 5 illustrates the CPU time required to construct the Boolean matrix for $GF(2^m)$ on a VAX-11/750. The capital delta (Δ) in the figure indicates the actual time required by using a arbitrarily selected irreducible polynomial of degree m . For example, the construction of the Boolean matrix for $GF(2^{127})$ takes only 40 minutes. The solid line shows that the trend of the required time increases exponentially as m increases. For large m , the computation time is mainly for forming the Boolean matrix, while, for small m , the computation time is dominated by the pre-matrix computation including the initial program set up and the trace computations of canonical basis which is required for forming matrix $F(\alpha)$. The most vertical part of the line in Fig. 5 shows the transition between these two kinds of computation.

VII. Conclusion

Although for some Galois field $GF(2^m)$ the roots of a generating polynomial can be easily verified to be linearly independent and then used as a normal basis, it is generally very difficult to locate a normal basis in a field. This makes the Massey-Omura multiplication less attractive since its design is based on a normal basis. A generalized algorithm to locate a normal basis of $GF(2^m)$ has been presented. Using this normal basis, an algorithm to construct a product function has also been developed. After a product function is defined, the design of the Massey-Omura multiplier is straightforward.

Acknowledgment

The author thanks Mr. D. Y. Pei for his contribution in helping with the Appendix.

References

1. MacWilliams, F. J., and Sloane, N. J. A., *The Theory of Error-Correcting Codes*, North-Holland Publishing, New York, 1977.
2. Peterson, W. W., and Weldon, Jr., E. J., *Error-Correcting Codes*, MIT Press, Cambridge, 1972.
3. Berkovits, S., Kowalchuk, J., and Schanning, B., "Implementing Public Key Scheme," *IEEE Communications Magazine* 17, pp. 2-3, May 1979.
4. Yeh, C. S., Reed, I. S., and Troung, T. K., "Systolic Multipliers for Finite Fields $GF(2^m)$," *IEEE Transactions on Computers C-33*, No. 4, pp. 357-360, April 1984.
5. Bartee, T. C., and Schneider, D. I., "Computation with Finite Fields," *Inform. Contr.* 6, pp. 79-98, Mar. 1963.
6. Gallagert, R. G., *Information Theory and Reliable Communication*, New York: Wiley, 1968.
7. Laws, B. A., and Rushforth, C. K., "A Cellular-array Multiplier for $GF(2^m)$," *IEEE Transactions on Computers C-20*, pp. 1573-1578, Dec. 1971.
8. Kung, H. T., "Why Systolic Architectures?" *IEEE Computer* 15, pp. 37-46, Jan. 1982.
9. Massey, J. L., and Omura, J. K., U. S. Patent Application of "Computational Method and Apparatus for Finite Field Arithmetic," submitted in 1981.
10. Wang, C. C., et al., "VLSI Architectures for Computing Multiplications and Inverses in $GF(2^m)$," *IEEE Transactions on Computers C-34*, No. 8, pp. 709-717, August 1985.
11. Perlis, S., "Normal Basis of Cyclic Fields of Prime-Power Degree," *Duke Math. J.* 9, pp. 507-517, 1942.
12. Berlekamp, E. R., *Algebraic Coding Theory*, McGraw-Hill Book Company, 1968.
13. Lidl, R., and Niederreiter, H., *Finite Fields*, Addison-Wesley Publishing Company, 1983.
14. Wah, P. K. S., and Wang, M. Z., "Realization and Application of the Massey-Omura Lock," *Proceedings of International Zurich Seminar*, IEEE press, pp. 175-182, March 1984.
15. Pei, D. Y., Wang, C. C., and Omura, J. K., "Normal Basis of Finite Field $GF(2^m)$," *IEEE Transactions on Information Theory IT-32*, No. 2, pp. 285-287, March 1986.
16. Wang, C. C., "Exponentiation in Finite Field $GF(2^m)$," Ph.D. dissertation, School of Engineering and Applied Sciences, UCLA, February 1985.

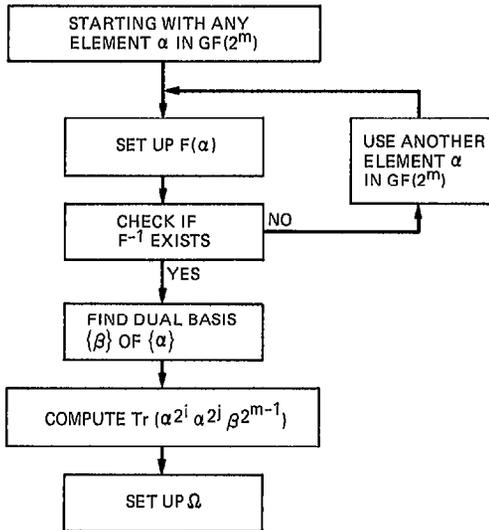


Fig. 1. Algorithm of constructing the Boolean matrix for the multiplication in $GF(2^m)$

	0	1	2	3	4	5	6	7
0	0	1	0	0	1	1	1	0
1	1	0	1	1	0	0	0	1
2	0	1	0	1	1	1	0	0
3	0	1	1	0	0	0	0	0
4	1	0	1	0	0	1	0	1
5	1	0	1	0	1	0	0	1
6	1	0	0	0	0	0	1	0
7	0	1	0	0	1	1	0	0

NUMBER OF 1 IN BOOLEAN MATRIX = 27

Fig. 2. Boolean matrix for $GF(2^8)$

	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
0	0	1	1	1	0	0	1	1	1	0	0	1	1	1	1	0	0
1	1	0	1	1	0	0	0	0	1	0	0	1	0	1	1	0	1
2	1	1	0	1	0	0	0	1	0	0	1	1	1	1	1	1	0
3	1	1	1	0	0	0	0	1	0	0	1	1	1	0	1	0	0
4	0	0	0	0	0	0	0	1	1	0	1	0	1	1	1	0	0
5	0	0	0	0	0	0	0	1	1	1	1	0	0	1	1	1	1
6	1	0	0	0	0	0	0	1	1	1	0	0	0	1	0	0	1
7	1	0	1	1	1	1	1	0	1	1	0	0	0	1	1	1	1
8	1	1	0	0	1	1	1	1	0	1	0	0	0	1	0	1	1
9	0	0	0	0	0	1	1	1	1	0	1	0	0	0	1	0	0
10	0	0	1	1	1	1	0	0	0	1	0	1	1	0	0	0	1
11	1	1	1	1	0	0	0	0	0	0	1	0	1	1	0	0	1
12	1	0	1	1	1	0	0	0	0	0	1	1	0	0	0	0	0
13	1	1	1	0	1	1	1	1	1	0	0	1	0	0	0	1	0
14	1	1	1	1	1	1	0	1	0	1	0	0	0	0	0	0	0
15	0	0	1	0	0	1	0	1	1	0	0	0	0	1	0	1	0
16	0	1	0	0	0	1	1	1	1	0	1	1	0	0	0	0	0

NUMBER OF 1 IN BOOLEAN MATRIX = 137

Fig. 3. Boolean matrix for $GF(2^{17})$

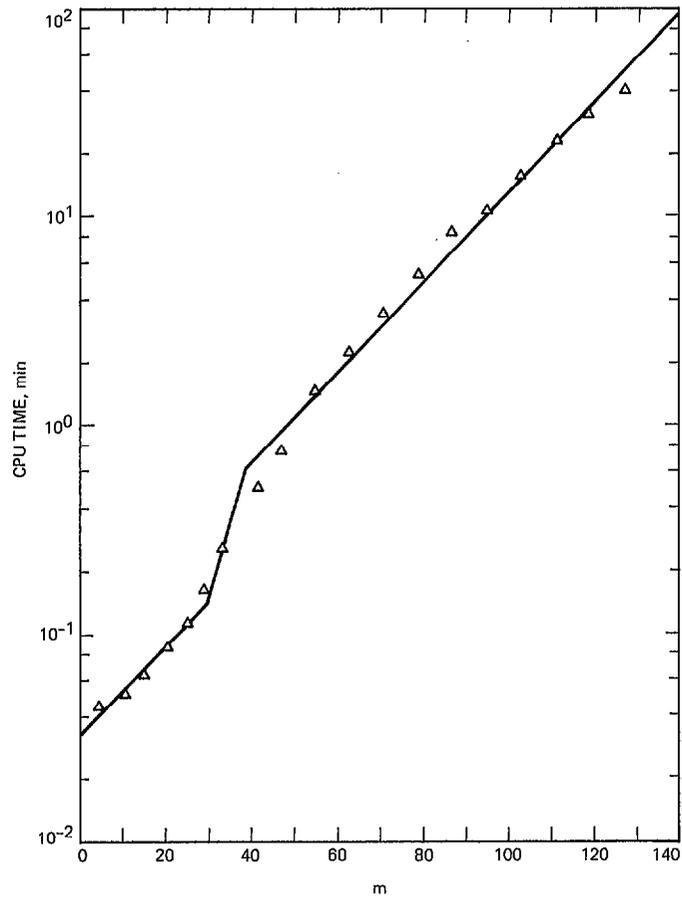


Fig. 5. CPU time required to construct Boolean matrix for $GF(2^m)$

Appendix A

Trace Computation for $GF(2^m)$

Although the trace value of an element θ in $GF(2^m)$ can be computed directly by its definition

$$Tr(\theta) = \sum_{i=0}^{m-1} \theta^{2^i}$$

this appendix provides a much simpler approach to compute the trace value.

Let ϵ be a root of the generating irreducible polynomial $P(x)$ of $GF(2^m)$. For any element θ of $GF(2^m)$,

$$\begin{aligned} \theta &= a_0 + a_1 \epsilon + a_2 \epsilon^2 + \dots + a_{m-1} \epsilon^{m-1} \\ &= \sum_{i=0}^{m-1} a_i \epsilon^i \end{aligned} \quad (A-1)$$

Since trace is a linear operator in $GF(2^m)$,

$$Tr(\theta) = \sum_{i=0}^{m-1} a_i Tr(\epsilon^i) \quad (A-2)$$

Hence, our problem becomes how to find the trace values of the canonical basis $\{1, \epsilon, \epsilon^2, \dots, \epsilon^{m-1}\}$ of $GF(2^m)$. The set of Newton formulae (Ref. A-1) demonstrates a very easy and quick way to accomplish it.

Let the generating polynomial be

$$P(X) = X^m + c_1 X^{m-1} + c_2 X^{m-2} + \dots + c_{m-1} X + c_m$$

and $\{\epsilon, \epsilon^2, \epsilon^4, \dots, \epsilon^{2^{m-1}}\}$ be the set of its roots. By Newton formulae, it can be shown that

$$\left. \begin{aligned} Tr(1) &= m \pmod{2} \\ Tr(\epsilon) + c_1 &= 0 \\ Tr(\epsilon^2) + c_1 Tr(\epsilon) &= 0 \\ &\dots \\ Tr(\epsilon^j) + c_1 Tr(\epsilon^{j-1}) + \dots \\ &\quad + c_{j-1} Tr(\epsilon) + [j \pmod{2}] c_j = 0 \\ &\dots \\ Tr(\epsilon^{m-1}) + c_1 Tr(\epsilon^{m-2}) + \dots + c_{m-2} Tr(\epsilon) \\ &\quad + [(m-1) \pmod{2}] c_{m-1} = 0 \end{aligned} \right\} \quad (A-3)$$

Therefore, the trace values of the canonical basis $\{1, \epsilon, \epsilon^2, \dots, \epsilon^{m-1}\}$ can be easily computed.

An interesting case is that when a trinomial is used to generate a field $GF(2^m)$. References A-2, A-3, and A-4 give a list of trinomials which are irreducible for $m < 1000$. In this case, the way of computing the trace values of the canonical basis $\{1, \epsilon, \epsilon^2, \dots, \epsilon^{m-1}\}$ can be further simplified from Eq. (A-3) to the following:

Suppose that $P(X) = X^m + X^k + 1$. Let $j \triangleq m - k$.

- (1) $Tr(1) = m \pmod{2}$.
- (2) When j is even, $Tr(\epsilon^i) = 0$ for $0 < i \leq m - 1$.
- (3) When j is odd, for $0 < i \leq m - 1$,

$$Tr(\epsilon^i) = \begin{cases} 1, & \text{if } i = nj \text{ (} n \text{ is an integer)} \\ 0, & \text{otherwise} \end{cases} \quad (A-4)$$

Note that if $P(X)$ is irreducible and m is even, k and j must be odd.

References

- A-1. Redei, L., *Algebra*, Volume I, Pergammon Press, London, 1967.
- A-2. Zierler, N., and Brillhart, J., "On Primitive Trinomials (Mod 2)," *Information and Control* 13, pp. 541-554, 1968.
- A-3. Zierler, N., and Brillhart, J., "On Primitive Trinomials (Mod 2), II," *Information and Control* 14, pp. 566-569, 1969.
- A-4. Zierler, N., "On $X^n + X + 1$ over $GF(2)$," *Information and Control* 16, pp. 502-505, 1970.