情報保護學會論文誌
第14券 第3號, 2004. 6

Massey-Omura 승산기를 위한 최적 정규원소

김 창 규†
동의대학교

The Optimal Normal Elements for Massey-Omura Multiplier

Chang-Kyu, Kim†
Dong-Eui University

요 약

유한체의 곱셈과 나눗셈은 오류정정부호와 암호시스템에서 중요한 산술 연산이다. 유한체 $GF(2^m)$의 원소를 표현하기 위해 다양한 기저가 사용되며 차수가 m인 $GF(2)$상의 원시다항식으로 구성할 수 있다. 정규기저를 사용하면 곱셈이나 곱셈 역원의 연산을 쉽게 수행할 수 있다. 정규기저 표현을 이용하는 Massey-Omura 승산기는 동일한 2진함수를 사용하여 몇 번의 순회치환으로 곱셈 또는 나눗셈이 수행되며 논리함수의 곱셈항 수가 승산기의 복잡도를 결정한다. 유한체의 정규기저는 항상 존재한다. 그러나 주어진 원시다항식에 대해 최적의 정규원소를 구하는 것은 쉽지 않다. 본 논문에서는 정규기저의 생성 방법을 고찰하고, Massey-Omura 승산기를 이용한 곱셈 또는 곱셈 역원의 계산에서 연산의 복잡도를 최소화할 수 있는 정규기저를 각 원시다항식에 대해 구하여, 최적의 정규원소와 곱셈항의 개수를 제시한다.

ABSTRACT

Finite field multiplication and division are important arithmetic operation in error-correcting codes and cryptosystems. The elements of the finite field $GF(2^m)$ are represented by bases with a primitive polynomial of degree m over $GF(2)$. We can be easily realized for multiplication or computing multiplicative inverse in $GF(2^m)$ based on a normal basis representation. The number of product terms of logic function determines a complexity of the Messay-Omura multiplier. A normal basis exists for every finite field. It is not easy to find the optimal normal element for a given primitive polynomial. In this paper, the generating method of normal basis is investigated. The normal bases whose product terms are less than other bases for multiplication in $GF(2^m)$ are found. For each primitive polynomial, a list of normal elements and number of product terms are presented.

Keywords : *Finite field, Massey-Omura multiplier, Normal basis, Normal element*

Ⅰ. 서 론

유한체 $GF(2^m)$의 연산은 암호이론 및 오류정정부호(error-correcting code) 특히, BCH 부호와 Reed-Solomon 부호에서 응용되고 있다. $GF(2^m)$상의 연산을 얼마나 효율적으로 수행하느냐 하는 것이 유한체의 곱셈과 곱셈 역원의 연산 속도와 하드웨어의 크기에 직접적으로 영향을 미치는 매우 중요한 요소이다. $GF(2^m)$의 원소는 보통 표준기저(standard bases), 쌍대기저(dual basis), 정규기저(normal basis)로 표현되며, 덧셈은 간단하게

접수일 : 2003년 11월14일 ; 채택일 : 2004년 3월22일
* 본 연구는 동의대학교의 지원으로 수행되었습니다.
† ckkim@deu.ac.kr

수행되지만 곱셈과 곱셈 역원의 계산은 $GF(2^m)$의 m이 커지면 연산이 복잡해지고 고속처리도 어려워진다. 유한체 연산의 대표적인 것으로 쌍대기저를 이용한 Berlekamp의 비트직렬 곱셈 알고리즘[1]과, 정규기저를 사용한 Massey와 Omura의 알고리즘[2]을 들 수 있다.

유한체 $GF(2^m)$의 원소를 정규기저로 표현하면 연산을 효과적으로 수행할 수 있는 이점이 있다. Itoh[3]등은 정규기저를 이용하여 유한체 $GF(2^m)$ 상에서 곱셈 역원 계산에 필요한 곱셈 회수를 $O(\log m)$까지 감소시킬 수 있는 알고리즘을 제안하였으며, Fermat 정리를 기반으로 $m-1$을 두 개의 인수로 분해하거나 2^m-2를 분해하여 곱셈의 회수를 감소시킬 수 있는 알고리즘이 제안되기도 하였다[5,6]. 그리고 m이 특수한 형태일 때 곱셈의 회수를 최소화하여 고속의 역원 연산을 할 수 있는 정규기저에 대해서도 연구되었다[7,8]. Massey-Omura 승산기는 정규기저로 표현된 유한체 원소의 곱셈 연산을 동일한 2진함수를 사용하여 쉽게 수행할 수 있으며 2진함수의 곱셈항 개수가 승산기의 복잡도를 결정한다. 일반적으로 병렬 Massey-Omura 승산기는 $O(m^3)$의 AND 게이트가 필요하며[9] 최적 정규기저(optimal normal basis)의 경우는 2진함수의 곱셈항 개수가 $2m-1$이다[10]. 그리고 AND 게이트가 $O(m^2)$ 만큼 필요한 새로운 형태의 병렬 Massey-Omura 승산기가 제안되기도 하였다[11].

정규기저를 이용한 곱셈 역원의 연산에서 연산의 속도는 곱셈의 회수와 승산기의 구조에 의존하므로, Fermat 정리를 기반으로 곱셈회수를 줄이는 방법과 승산기의 구조를 변화시켜 승산기의 복잡도를 개선하는 연구가 계속되고 있다. 그러나 원시다항식에 대해 $GF(2^m)$의 모든 원소가 정규기저를 구성할 수 있는 정규원소(normal element)가 되는 것이 아니므로 논리함수의 곱셈항 수가 승산기의 복잡도와 밀접한 관계가 있는 Massey-Omura승산기를 곱셈이나 곱셈 역원의 계산에 적용할 때, 주어진 원시다항식에 대해 어떤 원소가 곱셈항을 최소화 할 수 있는 정규원소인지 알아야 할 필요가 있다. 본 논문에서는 유한체 $GF(2^m)$의 원소를 정규기저로 표현할 때 각 원시다항식에 대해 존재할 수 있는 모든 정규기저를 구하는 방법을 제안하고, 어떤 정규원소가 곱셈항을 최소로 할 수 있는 최적의 정규원소인지 제시한다.

II. 유한체 $GF(2^m)$의 기저

$p(x)$가 차수 m인 $GF(2)$ 상의 원시다항식이고 α가 $p(x)$의 근이면 $GF(2^m)$의 임의의 원소 β는 $m-1$차 이하의 $GF(2)$ 상의 다항식

$$\beta = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{m-1}\alpha^{m-1} \quad (1)$$

으로 유일하게 표현할 수 있다. 이때 집합 $S=\{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$를 $GF(2^m)$의 표준기저라 한다.

β가 $GF(2^m)$의 원소일 때 m개 원소의 집합 $N=\{\delta, \delta^2, \delta^{2^2}, \cdots, \delta^{2^{m-1}}\}$은 $GF(2^m)$의 기저가 될 수 있다. 즉, $GF(2^m)$의 모든 원소를 다음과 같이 유일하게 표현할 수 있다.

$$\beta = b_0\delta + b_1\delta^2 + b_2\delta^{2^2} + \cdots + b_{m-1}\delta^{2^{m-1}} \quad (2)$$

이 기저를 정규기저라 하며 δ를 정규원소라 한다. $GF(2^m)$의 원소를 정규기저로 표현하면 임의의 원소의 자승은 한번의 순회치환에 의해 수행할 수 있으며, 두 원소의 곱셈은 동일한 2진함수에 의해 얻을 수 있는 이점이 있다. 그리고 이를 응용하여 몇 번의 곱셈에 의해 곱셈 역원의 연산도 쉽게 할 수 있다.

$GF(2^m)$의 한 원소 β의 트레이스함수를

$$Tr(\beta) = \sum_{i=0}^{m-1} \beta^{2^i} \quad (3)$$

라 정의하면 두 기저 $\{x_0, x_1, \cdots, x_{m-1}\}$와 $\{y_0, y_1, \cdots, y_{m-1}\}$가

$$Tr(x_j y_k) = \begin{cases} 1, & j=k \\ 0, & j\neq k \end{cases} \quad (4)$$

를 만족할 경우 임의의 기저를 다른 기저의 쌍대기저(dual basis)라 한다.

III. Massey-Omura 승산기

유한체 상에서의 연산에서 덧셈은 용이하지만 곱셈 또는 곱셈 역원의 연산은 구현이 복잡하다. 그러

나 (2)식과 같은 정규기저를 사용하면 구현의 복잡성을 줄일 수 있다. 정규기저를 사용하여 $GF(2)$상의 다항식으로 표현된 유한체 $GF(2^m)$의 원소 β를 자승하면,

$$\beta^2 = b_{m-1}\delta + b_0\delta^2 + b_1\delta^4 + \cdots + b_{m-2}\delta^{2^{m-1}} \quad (5)$$

로 나타난다. 그리고 β를 m차원벡터 $\beta = (b_0, b_1, b_2, \cdots, b_{m-1})$로 표현하면 그것의 자승은 $\beta^2 = (b_{m-1}, b_0, b_1, \cdots, b_{m-2})$로 된다. 즉, 정규기저 표현에서 β^2을 얻기 위해서는 β를 한번 순회치환하면 된다. 따라서 정규기저를 사용하면 $GF(2^m)$의 연산에서 임의의 원소의 자승은 간단한 논리회로에 의해 구현될 수 있다.

$\lambda = (c_0, c_1, \cdots, c_{m-1})$와 $\rho = (d_0, d_1, \cdots, d_{m-1})$가 정규기저로 표현된 $GF(2^m)$의 두 원소라 하면 두 원소의 곱 $\nu = (\phi_0, \phi_1, \cdots, \phi_{m-1})$의 마지막 요소 ϕ_{m-1}은 λ와 ρ의 요소들의 2진함수

$$\phi_{m-1} = f(c_0, c_1, \cdots, c_{m-1}; d_0, d_1, \cdots, d_{m-1}) \quad (6)$$

의 결과이다. 그리고 정규기저 표현에서 임의의 원소의 자승은 한번의 순회치환으로 이루어지므로 ν^2의 마지막 요소 ϕ_{m-2}는 λ^2와 ρ^2를 수행한 후에 나타나는 요소들을 사용하여 (6)식과 같은 2진함수에 의해 구해진다. 즉,

$$\phi_{m-2} = f(c_{m-1}, c_0, \cdots, c_{m-2}; d_{m-1}, d_0, \cdots, d_{m-2}) \quad (7)$$

가 된다. 따라서 λ와 μ를 순회치환하면서 그것의 요소를 논리함수 f의 입력으로 삼으면 두 원소의 곱을 구할 수 있으며 이를 Massey-Omura 승산기[2]라 한다.

유한체 $GF(2^m)$의 임의의 원소에 어떤 원소를 나눈다는 것은 그 원소의 역원을 곱하는 것과 같다. $GF(2^m)$의 원소 β에 대해 이것의 역원은 $\beta^{-1} = \beta^{2^m-2}$이며 2^m-2는 다음과 같이 쓸 수 있다.

$$2^m - 2 = 2 + 2^2 + 2^3 + \cdots + 2^{m-1} \quad (8)$$

그러므로, β의 역원 β^{-1}은 다음 식과 같이 표현할 수 있다.

$$\beta^{-1} = (\beta^2)(\beta^{2^2})(\beta^{2^3})\cdots(\beta^{2^{m-1}}) \quad (9)$$

따라서 β가 정규기저로 표현되면 한번의 순회치환에 의해 자승한 값을 얻을 수 있으므로 $GF(2^m)$의 임의의 원소에 대한 역원은 최대 m번의 연속적인 순회치환과 앞에서 언급한 Massey-Omura 승산기를 이용하여 구할 수 있다.

Ⅳ. 정규기저의 생성

4.1 정규기저

정규기저를 발견하기 위해 먼저 표준기저로 표현된 유한체 $GF(2^m)$를 사용하자. α를 원시원소(primitive element)라 하면 $GF(2^m)$의 임의의 원소 α^k는

$$\alpha^k = \sum_{j=0}^{m-1} a_{k,j}\alpha^j, \quad k = 0, 1, 2, \cdots, 2^m - 2 \quad (10)$$

으로 표현할 수 있다. 그리고 $GF(2^m)$의 원소인 기저 $\delta^{2^i}, i = 0, 1, \cdots, m-1$,는 표준기저를 사용하여 다음과 같이 유일하게 표현된다.

$$\delta^{2^i} = \sum_{j=0}^{m-1} b_{i,j}\alpha^j, \quad i = 0, 1, \cdots, m-1 \quad (11)$$

이 식을 자승하면,

$$\begin{aligned}(\delta^{2^i})^2 &= \delta^{2^{i+1}} \\ &= \sum_{j=0}^{m-1}\sum_{k=0}^{m-1} b_{i,j}b_{i,k}\alpha^{j+k} \\ &= \sum_{j=0}^{m-1}\sum_{k=0}^{m-1} b_{i,j}b_{i,k}\sum_{l=0}^{m-1} a_{j+k,l}\alpha^l, i = 0, 1, \cdots, m-1\end{aligned} \quad (12)$$

로 된다. 그런데 $\alpha^{2^{i+1}}$을 표준기저로 표현했을 때는 아래 (13) 식의 형태임을 알고 있다.

$$\delta^{2^{i+1}} = \sum_{l=0}^{m-1} b_{i+1,l}\alpha^l, \quad i=0,1,\cdots,m-1 \qquad (13)$$

따라서 (12), (13)식을 보면 원소 $\delta^{2^{i+1}}$을 다항식으로 표현했을 때 그것의 계수는

$$b_{i+1,l} = \sum_{j=0}^{m-1}\sum_{k=0}^{m-1} b_{i,j}b_{j,k}a_{j+k,l}, \quad l=0,1,\cdots,m-1 \qquad (14)$$

와 같이 계산된다.

그러므로, 표준기저로 표현된 $GF(2^m)$의 원소 $\alpha^i, i=0,1,2,\cdots,2m-1$, 에 대한 다항식 표현을 알고 있으면 정규기저가 되는 $\delta^{2^\lambda}, \lambda=0,1,2,\cdots, m-1$, 에 대응하는 다항식의 각 계수가 식 (14)에 의해 계산 가능하다.

여기서, 정규기저에 대한 다항식표현을 구하고 각 계수를 행렬로 표현하여

$$\boldsymbol{B}=\begin{bmatrix} b_{0,0} & b_{0,1} & \cdots & b_{0,m-1} \\ b_{1,0} & b_{1,1} & \cdots & b_{1,m-1} \\ & b_{2,0} & b_{2,1} & \cdots & b_{2,m-1} \\ \vdots & \vdots & \vdots & \vdots & \\ & & & b_{m-1,0} & b_{m-1,1} \\ \cdots & b_{m-1,m-1} & & & \end{bmatrix} \qquad (15)$$

라 하면 정규기저는

$$\begin{bmatrix} \delta \\ \delta^2 \\ \delta^{2^2} \\ \vdots \\ \delta^{2^{m-1}} \end{bmatrix} = \boldsymbol{B}\cdot\begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \\ \vdots \\ \alpha^{m-1} \end{bmatrix} \qquad (16)$$

와 같이 표현 가능하다. 즉, $\boldsymbol{B}$의 역행렬이 존재한다면

$$\begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \\ \vdots \\ \alpha^{m-1} \end{bmatrix} = \boldsymbol{B}^{-1}\cdot\begin{bmatrix} \delta \\ \delta^2 \\ \delta^{2^2} \\ \vdots \\ \delta^{2^{m-1}} \end{bmatrix} \qquad (17)$$

이 되어 표준기저를 정규기저로 나타낼 수 있다.

유한체 $GF(2^m)$의 모든 원소를 정규기저로 표현하기 위해 (17)식의 $\boldsymbol{B}^{-1}$을 이용하자. 정규기저로 표현된 임의의 두 원소를

$$\begin{aligned} \lambda &= c_0\delta + c_1\delta^2 + c_2\delta^{2^2} + \cdots + c_{m-1}\delta^{2^{m-1}} \\ \rho &= d_0\delta + d_1\delta^2 + d_2\delta^{2^2} + \cdots + d_{m-1}\delta^{2^{m-1}} \end{aligned} \qquad (18)$$

라 하고, 이들의 곱을 구하면

$$\begin{aligned} \nu &= \lambda\cdot\rho \\ &= (c_0\delta + c_1\delta^2 c_2\delta^{2^2} + \cdots + c_{m-1}\delta^{2^{m-1}}) \\ &\quad (d_0\delta + d_1\delta^2 d_2\delta^{2^2} + \cdots + d_{m-1}\delta^{2^{m-1}}) \\ &= \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} c_i d_j \delta^{2^i}\delta^{2^j} \end{aligned} \qquad (19)$$

이다. 여기서 $\delta^{2^i}\delta^{2^j}$가 정규기저로 표현되기만 하면 ν의 정규기저 표현이 가능하다. δ^{2^i}와 δ^{2^j}의 표준기저 표현으로부터

$$\delta^{2^i}\delta^{2^j} = \sum_{k=0}^{m-1}\sum_{l=0}^{m-1} b_{i,k}b_{j,l}\alpha^{k+l} \qquad (20)$$

이며 (12)식과 같이 α^{k+l}을 다항식으로 표현하고 표준기저를 정규기저로 나타내면

$$\begin{aligned} \delta^{2^i}\delta^{2^j} &= \sum_{k=0}^{m-1}\sum_{l=0}^{m-1} b_{i,k}b_{j,l}\sum_{t=0}^{m-1} a_{k+l,t}\alpha^t \\ &= \sum_{k=0}^{m-1}\sum_{l=0}^{m-1}\sum_{t=0}^{m-1} b_{i,k}b_{j,l}a_{k+l,t}\sum_{u=0}^{m-1} e_{t,u}\delta^{2^u} \end{aligned} \qquad (21)$$

와 같이 $\delta^{2^i}\delta^{2^j}$를 정규기저로 표현할 수 있다. (21)식을 (19)식에 대입하면

$$\nu = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} c_i d_j \sum_{k=0}^{m-1}\sum_{l=0}^{m-1}\sum_{t=0}^{m-1} b_{i,k}b_{j,l}a_{k+l,t}\sum_{u=0}^{m-1} e_{t,u}\delta^{2^u} \qquad (22)$$

이다. 그런데 ν를 정규기저로 표현한 형태는

$$\nu = \sum_{n=0}^{m-1} \phi_n \delta^{2^n} \tag{23}$$

이므로 (22)식과 (23)식을 비교하면

$$\begin{aligned} \phi_n &= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} c_i d_j \mu_{i,j} \\ \mu_{i,j} &= \sum_{k=0}^{m-1} \sum_{l=0}^{m-1} b_{i,k} b_{j,l} \xi_{k,l} \\ \xi_{k,l} &= \sum_{t=0}^{m-1} a_{k+l,t} \sum_{u=0}^{m-1} e_{t,u} \end{aligned} \tag{24}$$

라 쓸 수 있다.

따라서 (24)식에서 정규기저로 표현된 두 원소가 주어지면 c_i, d_j를 알 수 있으므로 $\mu_{i,j}$만 얻을 수 있으면 정규기저로 표현된 두 원소의 곱을 정규기저로 표현할 수 있다. 이 방법을 이용하여 (16)식의 결과 얻어지는 원소들의 정규기저 표현을 이용하여 순차적으로 모든 원소의 정규기저 표현을 구할 수 있다. 식 (24)에서 $\mu_{i,j}$의 $b_{i,k}$와 $b_{j,l}$은 (15)식에서 얻어지는 정규기저들의 다항식 표현에서 그 값을 알 수 있고, $\xi_{k,l}$의 $a_{k+l,t}$는 표준기저 표현에서 얻을 수 있으며, $e_{t,u}$는 (16)식의 결과이므로 구할 수 있다. 따라서 $\mu_{i,j}$가 구해지고 유한체 $GF(2^m)$의 원소를 정규기저로 표현할 수 있다.

4.2 최적 정규원소

(23), (24)식을 보면 정규기저를 사용한 유한체 원소의 다항식 표현에서 계수 ϕ_n은 곱하는 두 원소 λ와 μ의 계수들의 곱셈항의 2원합이며 어떤 곱셈항을 합할 것인가 하는 것을 $\mu_{i,j}$가 결정한다. 그리고 (6), (7)식에서 보듯이 계수 ϕ_n, $n=0,1,2,\cdots,m-1$은 같은 2진함수에 의해 구해진다. 즉, i와 j가 0에서 $m-1$까지 변할 때, $\mu_{i,j}$의 값이 1인 경우가 2진함수의 곱셈항으로 나타난다. 식 (24)에서 정규기저를 생성하기 위해 필요한 $\mu_{i,j}$를 구하고 이를 행렬로 나타내면

$$\boldsymbol{M} = \begin{bmatrix} \mu_{0,0} & \mu_{0,1} & \cdots & \mu_{0,m-1} \\ \mu_{1,0} & \mu_{1,1} & \cdots & \mu_{1,m-1} \\ \mu_{2,0} & \mu_{2,1} & \cdots & \mu_{2,m-1} \\ \vdots & \vdots & \vdots & \vdots \\ \mu_{m-1,0} & \mu_{m-1,1} & \cdots & \mu_{m-1,m-1} \end{bmatrix} \tag{25}$$

와 같다. 그러므로 이것을 구하면 정규기저로 표현된 유한체 $GF(2^m)$를 구성할 수 있으며 곱셈에서 곱셈항의 개수가 몇 개인지 알 수 있다. 1의 개수가 $2m-1$인 경우를 최적 정규기저라 한다.

표준기저를 사용하는 유한체 $GF(2^m)$에서 (15)식과 같은 행렬을 구하여 그것의 역행렬이 존재하는지 판단한다. 역행렬이 존재하면 정규기저가 될 수 있고 그렇지 못하면 정규기저가 될 수 없는 것이다. (15), (16), (17)식을 이용하여 δ를 α에서 α^{2^m-2}까지 변화시키면서 역행렬의 존재를 확인하면 정규기저가 될 수 있는지 판단할 수 있다. 또 정규기저가 될 수 있는 경우, (25)식을 계산하여 영이 아닌 요소의 개수를 계산함으로서 정규기저를 사용한 $GF(2^m)$상의 두 원소 곱셈에서 곱셈항이 몇 개인지 알 수 있는 것이다. 표 1은 유한체 $GF(2^m)$를 구성할 수 있는 각 원시다항식 중에서 최소의 항을 가지는 원시다항식을 택하여 이상에서 기술한 바를 적용할 경우 존재할 수 있는 정규기저 중에서 최적인 것을 찾아 정규원소와 Massey-Omura 승산기에서의 곱셈항 수를 수록한 것이다. 여기서 원시다항식은 그것의 계수가 1인 멱승으로 표현하였으며, 정규원소는 원시원소의 멱승으로 표시하였다. 표에서 *는 최적 정규기저가 존재하는 유한체이며 곱셈항의 수가 $2m-1$임을 확인할 수 있다.

표 1. 유한체 $GF(2^m)$의 최적정규원소($3 \le m \le 20$)

원시다항식	정규원소의 멱승	곱셈항의 수
(3,1,0)*	3	5
(4,1,0)*	3	7
(5,2,0)*	5	9
(6,1,0)*	23	11
(7,3,0)	21	19
(8,4,3,2,0)	47	21
(9,4,0)*	41	17
(10,3,0)*	93	19
(11,2,0)*	439	21
(12,6,4,1,0)*	315	23
(13,4,3,1,0)	401	45
(14,10,6,1,0)*	725	27
(15,1,0)	1359	45
(16,12,3,2,0)	7897	85
(17,3,0)	615	81
(18,7,0)*	13797	35
(19,5,2,1,0)	10873	117
(20,3,0)	12883	73

표 2. 유한체 $GF(2^m)$ 의 모든 원시다항식에 대한 최적의 정규원소($3 \le m \le 10$)

원시다항식	정규원소의 멱승	곱셈항의 수
(3,1,0)	3	5
(3,2,0)	1	
(4,1,0)	3	7
(4,3,0)	3	
(5,2,0)	5	9
(5,3,0)	11	
(5,3,2,1,0)	7	
(5,4,2,1,0)	1	
(5,4,3,1,0)	15	
(5,4,3,2,0)	3	
(6,1,0)	23	11
(6,4,3,1,0)	13	
(6,5,0)	5	
(6,5,2,1,0)	31	
(6,5,3,2,0)	11	
(6,5,4,1,0)	1	
(7,1,0)	13	19
(7,3,0)	21	
(7,3,2,1,0)	7	
(7,4,0)	43	
(7,4,3,2,0)	55	
(7,5,2,1,0)	63	
(7,5,3,1,0)	27	
(7,5,4,3,0)	9	
(7,5,4,3,2,1,0)	47	
(7,6,0)	23	
(7,6,3,1,0)	11	
(7,6,4,1,0)	29	
(7,6,4,2,0)	19	
(7,6,5,2,0)	1	
(7,6,5,3,2,1,0)	31	
(7,6,5,4,0)	15	
(7,6,5,4,2,1,0)	3	
(7,6,5,4,3,2,0)	5	
(8,4,3,2,0)	47	21
(8,5,3,1,0)	127	
(8,5,3,2,0)	23	
(8,6,3,2,0)	43	
(8,6,4,3,2,1,0)	37	
(8,6,5,1,0)	31	
(8,6,5,2,0)	53	
(8,6,5,3,0)	29	
(8,6,5,4,0)	13	
(8,7,2,1,0)	19	
(8,7,3,2,0)	7	
(8,7,5,3,0)	1	
(8,7,6,4,2,1,0)	61	
(8,7,6,5,2,1,0)	11	
(8,7,6,5,4,2,0)	91	

원시다항식	정규원소의 멱승	곱셈항의 수
(9,4,0)	41	17
(9,4,3,1,0)	93	
(9,5,0)	183	
(9,5,3,2,0)	59	
(9,5,4,1,0)	47	
(9,6,4,3,0)	23	
(9,6,4,3,2,1,0)	127	
(9,6,5,3,0)	61	
(9,6,5,3,2,1,0)	187	
(9,6,5,4,2,1,0)	239	
(9,6,5,4,3,2,0)	15	
(9,7,2,1,0)	171	
(9,7,4,2,0)	117	
(9,7,5,1,0)	103	
(9,7,5,2,0)	43	
(9,7,5,3,2,1,0)	107	
(9,7,5,4,2,1,0)	19	
(9,7,5,4,3,2,0)	57	
(9,7,6,3,2,1,0)	11	
(9,7,6,4,0)	39	
(9,7,6,4,3,1,0)	95	
(9,7,6,5,4,2,0)	55	
(9,7,6,5,4,3,0)	31	
(9,8,4,1,0)	75	
(9,8,4,2,0)	51	
(9,84,3,2,1,0)	79	
(9,8,5,1,0)	109	
(9,8,5,4,0)	29	
(9,8,5,4,3,1,0)	255	
(9,8,6,3,2,1,0)	53	
(9,8,6,4,3,1,0)	191	
(9,86,5,0)	45	
(9,8,6,5,3,1,0)	5	
(9,8,6,5,3,2,0)	13	
(9,8,6,5,4,1,0)	1	
(9,8,6,5,4,3,2,1,0)	223	
(9,8,7,2,0)	85	
(9,8,7,3,2,1,0)	25	
(9,8,7,5,4,2,0)	123	
(9,8,7,5,4,3,0)	17	
(9,8,7,6,2,1,0)	111	
(9,8,7,6,3,1,0)	87	
(9,8,7,6,3,2,0)	125	
(9,8,7,6,4,2,0)	83	
(9,8,7,6,4,3,0)	37	
(9,8,7,6,5,1,0)	27	
(9,8,7,6,5,3,0)	3	
(9,8,7,6,5,4,3,1,0)	9	
10차 원시다항식	93	19

예를 들어, 원시다항식 $p(x)=x^6+x+1$을 사용하여 $GF(2^6)$을 구성할 경우, α가 원시다항식의 근이면 $\delta=\alpha^{23}$일 때 최적의 정규기저가 된다. 정규기저로 표현된 임의의 두 원소를

$$\lambda=c_0\delta+c_1\delta^2+a_2\delta^4+c_3\delta^8+c_4\delta^{16}+c_5\delta^{32}$$
$$\rho=d_0\delta+d_1\delta^2+d_2\delta^4+d_3\delta^8+d_4\delta^{16}+d_5\delta^{32}$$

라 하면, 정규기저를 생성하기 위한 행렬은

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

로 구해지며, 두 원소의 곱인 $\nu=\lambda\rho$의 마지막요소 ϕ_5를 계산할 수 있는 2진함수는

$$\phi_5=\begin{array}{l}c_0d_3+c_0d_5+c_1d_2+c_1d_3+c_2d_1+c_2d_4\\+c_3d_0+c_3d_1+c_4d_2+c_4d_4+c_5d_0\end{array}$$

이며 곱셈항은 11개이다. $p(x)=x^6+x+1$를 원시다항식으로 사용하여 확대체를 구성하면 $\delta=\alpha^5$일 때와 $\delta=\alpha^{15}$일 때도 정규기저를 구성할 수 있지만 이 때의 곱셈항의 수는 각각 17, 15이다.

표 2는 10차 이하의 모든 원시다항식에 대한 정규원소와 그 때의 곱셈항의 수를 수록한 것이다. 표를 살펴보면 어떤 원시다항식을 사용하더라도 같은 확대체일 때, 정규원소는 다르지만 최적의 곱셈항 수는 같음을 알 수 있다. 그러나 $GF(2^{10})$의 경우는 모든 원시다항식에 대한 최적 정규원소가 동일하게 나타났다.

V. 결 론

유한체 $GF(2^m)$에서 정규기저가 존재하려면 정규기저의 원소들을 표준기저로 표현했을 때 나타나는 행렬의 역행렬이 존재하여야 한다. 이러한 정규기저를 이용한 Massey-Omura 승산기에서 논리회로의 복잡도는 곱셈항의 수에 비례한다. 본 논문에서는 곱셈항의 수가 최소인 최적 정규원소를 구하는 방법을 해석하고, 확대체를 구성할 수 있는 원시다항식 중에서 항의 수가 최소인 것을 선택하여, 존재할 수 있는 정규기저 중 곱셈항의 수가 최소인 것에 대해 정규기저와 곱셈항의 수를 수록하였다. 그리고 10차 이하의 모든 원시다항식에 대해서 최적의 정규기저와 곱셈항의 수를 구하여 수록하였다. 어떤 원시다항식을 사용하던 최적의 경우는 Massey-Omura 승산기의 곱셈항 수는 동일하며, 곱셈 연산을 수행하는 논리회로의 구현에서 보통의 정규기저보다 복잡도가 2/3정도로 줄어든다.

참 고 문 헌

[1] E. R. Berlekamp, "Bit-Serial Reed-Solomon Encoder," *IEEE Trans. Information Theory*, Vol. 28, pp. 869-874, 1982.

[2] C. C Wang, T. K. Truong, H. M. Shao, J. K. Omura and I. S. Reed, "VLSI Architectures for Computing Multiplications and Inverses in GF(2^m)", *IEEE Trans. Computers*, vol. C-34, pp. 709-716, 1985.

[3] T. Itoh, O. Teechai, and S. Tsujii, "A Fast Algorithm for Computing Multiplicative Inverses in GF(2^m) Using Normal Bases," *J. Soc. Electro. Comm.*, pp. 31-36, 1986.

[4] 박정식, 안금혁, 김영길, 장청룔, "유한체 GF(2^m) 상에서의 빠른 역원계산 기법," 한국통신정보보호학회 종합학술발표회 논문집, 제6권 1호, pp. 145-150, 1996.

[5] 장용희, 권용진, "GF(2^m)에서 정규기저를 이용한 고속 곱셈 역원 연산 방법," 정보보호논문지, 제 13권 2호, pp. 127-132, 2003

[6] S. M. Ten, "Improved Normal Basis Inversion in GF(2^m)," *Electronics Letters*, vol. 33, no.3, pp. 196-197, 1997.

[7] M. Wang and F. Blake, "Normal Basis of the Finite Field $F_{2^{(p-1)p}}$ over F_2," *IEEE Trans. on Inform. Theory*, vol. 43, no. 2, pp. 737-739, 1997.

[8] J. H. Jeng, "Normal Basis Inversion in Some Finite Fields," *ISSPA '99*, pp. 701-703, Brisbane, Australia, August, 1999.

[9] M. A. Hansan, M. wang, and V. K. Bhargava, "Modular Construction of Low Complexity Parallel Multipliers for a Class of Finite Fields GF(2^m)," *IEEE Trans. Computers*, vol. 41, no. 8, pp. 962-971, 1993.
[10] S. Gao, "Normal Bases over Finite Fields," thesis for Ph. D. in Combinatorics and Optimization, the University of Waterloo, Waterloo, Ontario, Canada, 1993.
[11] C. H. Kim, S. Oh, and J. Lim, "A New Hardware Architecture for Operation in GF(2^m)," *IEEE Trans. Computers*, vol. 51, no. 1, pp. 90-92, 2002.
[12] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice-Hall, Englewood Cliffs, New Jersey, 1995.

〈著者紹介〉

김 창 규 (Chang-Kyu Kim) 정회원
1981년 2월 : 한양대학교 전자통신공학과 학사
1984년 8월 : 한양대학교 전자통신공학과 석사
1989년 2월 : 한양대학교 전자통신공학과 박사
1999년 1월~2000년 12월 : 동의대학교 정보통신연구소장
1988년 3월~현재 : 동의대학교 정보통신공학과 교수
〈관심분야〉 암호이론, 부호이론