通信情報保護學會誌
第1卷, 第2號, 1991. 8

유한체 GF(2^m)의 성질과 연산

원 동 호*

1. 서 언

유한체(finite field)의 연산은 스위칭 이론(switching theory)과 컴퓨터 연산 그리고 오류정정부호(error-correcting codes)에 이용되어 왔으며 최근 암호이론(cryptography)에도 활발히 응용되고 있다. 예를 들면 BCH 부호와 Reed-Soloman 부호의 복호화 과정과 공개키 암호방식의 암호화 복호화 과정에서는 GF(2^m)상의 연산을 이용하여 관련 알고리즘을 실현하고 있다. 그러므로 유한체 연산의 간소화는 이들 구성 회로의 복잡성에 매우 큰 영향을 미치게 된다.

유한체는 유한개의 원소로 구성되며 원소 사이에 사칙연산이 정의된다. 그 예로 소수 p를 법으로 하는 연산에서의 잉여류 집합(0, 1, 2, ···, p−1)은 체를 이룬다. 이를 galois field의 기초체(ground field)라 하며 GF(p)로 표시한다. 한편 GF(p)상의 원시다항식의 원시원소로 만들어지는 GF(p^m)도 체를 구성하게 되며 이를 기초체 GF(p)의 확대체(extension field)라 부른다.

유한체 연산의 복잡도는 유한체를 이루는 원소수와 원소를 표시하는 방법에 따라 크게 달라진다. 특히 암호계 구성에 필요한 유한체는 원소가 많기 때문에 연산속도가 개선된 새로운 연산 알고리즘과 연산회로 구성방법이 요구되고 있다.

유한체의 원소 표시방법은 크게 기저표현(basis representation)과 지수표현(exponent representation)의 두가지로 나눌 수 있다. 일반적으로 기저표현에 의한 유한체 연산에서는 가산(addition)과 감산(subtraction)이 용이한 반면 승산(multiplication) 및 제산(division)이 어렵고 지수표현에 의한 연산에서는 승산 및 제산이 비교적 간단한 반면 가산과 제산은 매우 복잡하다.

GF(2^m) 상의 연산방법의 복잡성과 동작의 신속성은 GF(2^m) 상의 원소를 바이너리로 표시하기 위한 기저 표현에 따라 달라진다.

Yeh, Reed와 Troung은 관용기저(conventional basis)로 원소를 표시하여 VLSI화가 가능한 GF(2^m) 상의 승산회로를 구성하였으며 다소 회로화가 복잡하기는 하지만 Bartee와 Schneider, Laws와 Rushforth 등도 관용기저로 GF(2^m) 상의 원소를 표시하여 승산회로를 구성하였다.

한편 Massey와 Omura는 정규기저(normal basis)로 원소를 표시하여 GF(2^m)상의 승산과 역원 계산을 보다 간편하고 신속하게 계산할 수 있는 연산회로를 구성하였다. 정규기저로 표시된 GF(2^m) 상의 원소의 자승은 벡터로 표시된 원소의 각 비트를 순회치환함으로써 역원 계산회로를 구성할 수 있다.

그러나 유한체 GF(2^m)의 구성은 GF(2)상의 m차

* 종신회원, 성균관대학교 정보공학과 부교수

원소 다항식에 따라 원소 값이 달라지며 특히 m 값에 따라 선택해야 할 원시다항식의 수가 많아진다. 이러한 원시다항식은 모두 관용기저를 갖고 있으나 모두 정규기저를 갖고 있지는 않다.

본고에서는 암호이론에 많이 이용되고 디지탈 회로응용에 적당한 유한체 GF(2^m)상의 연상방법과 GF(2^m) 구성에 근간이 되는 GF(2) 상의 m차 원시다항식(primitive polynomial)의 성질을 살펴보고 선택된 GF(2) 상의 원시다항식에 의한 GF(2^m)상의 원소 표시와 각 연산방식에 대하여 설명하고자 한다.

2. 유한체

2.1 유한체 성질

어떤 집합상에서 원소 사이에 2항 연산들이 정의되고 또 이 연산들이 특정한 공리계를 만족할 때 이 집합과 연산을 묶어 대수적 체계(algebraic system)라 하며 이 집합은 대수적 구조(algebraic structure)를 갖고 있다고 한다.

실수 전체의 집합은 사칙연산, 대소관계, 연속성 등 3가지 성질을 갖고 있으며 이중 사칙연산의 성질을 정리한 것이 다음의 7가지 공리(F1~F7)이다.

F1. 임의의 원소 x, y∈F에 대하여 가산과 승산이 정의된다.

$x+y \in F$

$x \cdot y \in F$

F2. 임의의 원소 x, y, z∈F에 대하여 결합법칙이 성립한다.

$x+(y+z)=(x+y)+z$

$(x \cdot y) \cdot z=x \cdot (y \cdot z)$

F3. 임의의 원소 x, y∈F에 대하여 교환법칙이 성립한다.

$x+y=y+x$

$x \cdot y=y \cdot x$

F4. 임의의 원소 x, y, z∈F에 대하여 분배법칙이 성립한다.

$x \cdot (y+z)=x \cdot y+x \cdot x$

F5. 임의의 원소 x∈F에 대하여 $x+0=x$를 만족하는 영원 0∈F가 단 하나 존재한다.

F6. 임의의 원소 x∈F에 대하여 $x \cdot y=x$가 만족하는 단위원 y∈F가 단 하나 존재한다.

F7. 임의의 원소 x∈F에 대하여 $x+y=0$을 만족하는 가산역원(음원) y∈F가 단 하나 존재하고, $x \cdot z=1$을 만족하는 승산역원(역원) z∈F가 단 하나 존재한다.

2개 이상의 원소를 갖는 집합 F가 공리 F1~F7을 만족할 때 체라고 한다.

실수 전체는 위의 공리를 만족하므로 체이지만 무한 집합이다. 원소가 p개인 유한집합으로 위의 공리를 만족시키는 것은 유한체, 혹은 galois field라고 하며 GF(p)로 표시한다.

유한체는 실수의 사칙연산 성질만을 가지며 구체적인 예로 p가 소수로 p를 법으로 하는 연산에서 얻어지는 잉여류 집합 $F=(0, 1, 2, \cdots, p-1)$가 있다.

p=5인 GF(5)의 원소 사이의 가산과 승산 그리고 0이 아닌 원소의 멱승은 표 1, 표 2, 표 3과 같다.

표 1. GF(5)상의 가산 x+y

x \ y	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

표 2. GF(5)상의 승산 x·y

x \ y	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

표 3. GF(5)상의 멱승 x^y

x \ y	0	1	2	3	4
1	1	1	1	1	1
2	2	4	3	1	2
3	3	4	2	1	3
4	4	1	4	1	4

한편 p가 소수이고 m이 양정수일 때 $GF(p^m)$도 유한체를 이루며 이를 기초체 GF(p)의 확대체라 한다. 이 확대체의 원소는 GF(p)상의 m차 원시 다항식의 근으로 표시된다.

특히 p=2인 $GF(2^m)$상의 원소는 2치 값을 나타내는 m비트 바이너리로 표시할 수 있어 여러 분야에 널리 응용되고 있다.

p=2, m=3, 원시다항식 $p(x)=x^3+x+1$로 만들어지는 $GF(2^3)$상의 원소사이의 가산과 승산, 그리고 0이 아닌 원소의 멱승은 표 4, 표 5, 표 6과 같다.

표 4. $GF(2^3)$상의 가산 x+y

x \ y	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	1	α	α^2	α^3	α^4	α^5	α^6
1	1	0	α^3	α^6	α	α^5	α^4	α^2
α	α	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^2	α^6	α^4	0	α^5	α	α^3	α
α^3	α^3	α	1	α^5	0	α^6	α^2	α^4
α^4	α^4	α^5	α^2	α	α^6	0	1	α^3
α^5	α^5	α^4	α^6	α^3	α^2	1	0	α
α^6	α^6	α^2	α^5	1	α^4	α^3	α	0

표 5. $GF(2^3)$상의 승산 x·y

x \ y	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	0	0	0	0	0	0	0
1	0	1	α	α^2	α^3	α^4	α^5	α^6
α	0	α	α^2	α^3	α^4	α^5	α^6	1
α^2	0	α^2	α^3	α^4	α^5	α^6	1	α
α^3	0	α^3	α^4	α^5	α^6	1	α	α^2
α^4	0	α^4	α^5	α^6	1	α	α^2	α^3
α^5	0	α^5	α^6	1	α	α^2	α^3	α^4
α^6	0	α^6	1	α	α^2	α^3	α^4	α^5

표 6. $GF(2^3)$상의 멱승 x^y

x \ y	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
α	α	α^2	α^3	α^4	α^5	α^6	1	α
α^2	α^2	α^4	α^6	α	α^3	α^5	1	α^2
α^3	α^3	α^6	α^2	α^5	α	α^4	1	α^3
α^4	α^4	α^1	α^5	α^2	α^6	α^3	1	α^4
α^5	α^5	α^3	α	α^6	α^4	α^2	1	α^5
α^6	α^6	α^5	α^4	α^3	α^2	α	1	α^6

표 4, 표 5, 표 6 상의 α는 원시다항식 $p(x)=x^3+x+1$의 근이다. 이러한 유한체 GF(p)와 $GF(p^m)$상의 원소는 다음과 같은 성질을 갖고 있다.

1) GF(p), $GF(p^m)$상의 임의의 원소 x를 p개 합한 것은 0이다.

$$p \cdot x = x+x+\cdots+x \equiv 0 \qquad (1)$$

2) GF(p), $GF(p^m)$상의 임의의 원소 x에 대하여 다음 식이 성립된다.

$$x^{p-1} \equiv 1 \qquad (2)$$

$$x^{p^m-1} \equiv 1 \qquad (3)$$

(Fermat 정리)

3) GF(p), $GF(p^m)$상의 임의의 원소 x, y에 대하여 다음 식이 성립된다.

$$(x+y)^p \equiv x^p + y^p \qquad (4)$$

$$(x+y)^{p^m} \equiv x^{p^m} + y^{p^m} \qquad (5)$$

4) GF(p), $GF(p^m)$상의 임의의 원소 x에 대하여 다음 식이 성립한다.

$$x^i \cdot x^j \equiv x^{i+j \pmod{p-1}} \qquad (6)$$

$$x^i \cdot x^j \equiv x^{i+j \pmod{p^m-1}} \quad (7)$$

2.2 원시다항식

기초체 GF(p)를 m차 확대한 확대체 GF(p^m)상의 원소는 GF(p)상의 m차 원시다항식의 원시근의 멱승으로 표시된다. m차 원시다항식은 단위다항식으로 m차 기약다항식 중에서 원시근을 갖는 다항식을 말하며 GF(p)상의 원시다항식을 p(x)라 하면

$$p(x)=x^m+f_{m-1}\cdot x^{m-1}+\cdots+f_1\cdot x+f_0 \quad (8)$$
$$f_i \in GF(p)$$

로 표시된다.

GF(p^m)상의 원소는 원시근 α를 식 (8)에 대입하여 α의 멱승으로 표시할 수 있으며 mod p(x)의 잉여다항식이므로 α의 (m−1)차 이하의 다항식으로 표시된다.

한편 확대체 GF(p^m)상의 원소는 특성방정식(characteristic equation) $x^{p^m}-x=0$의 근이므로 원시다항식 p(x)는 특성방정식의 인수다항식이다. 이러한 사실은 식 (3)의 Fermat 정리로부터 확인할 수 있다. 따라서 GF(p)상의 m차 원시다항식의 수는 ⌊p^m/m⌋보다 적으며 원시다항식은 특성방정식을 인수분해하여 기약인 다항식 중에서 원시근을 갖는 다항식을 선택하면 얻을 수 있다.

여기서 확대체 GF(2^m) 구성에 필요한 GF(2)상의 원시다항식을 구하는 방법을 생각해 본다. GF(2)상의 m차 원시다항식은 특성방정식 $x^{2^m}-x$를 인수분해하여 원시근을 갖는 m차 기약다항식을 구하면 얻을 수 있다.

예로 m=2, 3, 4, 5에 대하여 $x^{2^m}-x$를 인수분해 해보면 다음과 같다.

$$m=2,\ x^4-x=x(x+1)\underline{(x^2+x+1)} \quad (9)$$

$$m=3,\ x^8-x=x(x+1)\underline{(x^3+x+1)}\,\underline{(x^3+x^2+1)} \quad (10)$$

$$m=4,\ x^{16}-x=x(x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)\underline{(x^4+x+1)}\,\underline{(x^4+x^3+1)} \quad (11)$$

$$m=5,\ x^{32}-x=x(x+1)(x^5+x+1)\underline{(x^5+x^3+1)}\,\underline{(x^5+x^4+x^3+x^2+1)}\,\underline{(x^5+x^4+x^3+x+1)}\,\underline{(x^5+x^4+x^2+x+1)}\,\underline{(x^5+x^3+x^2+x+1)} \quad (12)$$

$x^{2^m}-x$를 인수분해하여 얻은 기약다항식에 대하여 원시근 유무를 확인하여 원시다항식을 구할 수 있으며 식(9), 식(10), 식(11), 식(12)의 밑줄 친 기약다항식이 원시근을 갖는 원시다항식이다.

일반적으로 특성다항식 $x^{2^m}-x$를 인수분해하여 원시근을 갖는 기약다항식을 선택하면 원시다항식을 구할 수 있으나 m이 클 때는 특성방정식 자체를 인수분해하는 것조차 복잡하고 어려운 문제가 된다.

따라서 m이 클 때는 특성방정식 $x^{2^m}-x$를 인수분해하지 않고 원시다항식의 다음과 같은 성질을 이용하여 직접 구한다.

1) GF(2)상의 원시다항식은 기수개의 항을 갖는다.

2) GF(2)상의 원시다항식은 x의 차수가 적어도 하나는 기수차를 갖는다.

3) GF(2)상의 m차 원시다항식은 특성다항식 $x^{2^m}-x$의 인수다항식이다.

4) GF(2)상의 m차 원시다항식의 근을 누승하면 2^m-1에서 처음 1이 된다.

2.3 기저에 의한 GF(2^m)상의 원소 표시

GF(2^m)상의 연산회로 구성은 원소 표시 방법에 따라 그 복잡성이 크게 좌우된다. GF(2^m)상의 원소를 GF(2)상의 원시다항식의 원시근의 멱승으로 표시하면 승산과 역원계산이 간단하나 디지탈 회로화가 불가능하다. 따라서 디지탈 회로화가 가능한 기저표시 방법으로 원소를 표시한다. 이러한 방법으로는 관용기저와 정규기저를 많이 이용한다.

2.3.1 GF(2^m)상의 관용 기저

GF(2^m)상의 원소는 2^m개로 GF(2)상의 m차 원시다항식 p(x)의 원시근의 멱승으로 표시되며 각각의 원소는 mod p(x)의 잉여다항식이므로 원시다항식의 원시근을 α라 하면 모든 원소는 α^0, α^1,

…, α^{m-1}의 선형결합으로 표시할 수 있다.

즉,

$$F(\alpha)=\sum_{i=0}^{m-1} c_i \cdot \alpha^i$$

$$= c_0+c_1\alpha+c_2\alpha^2+\cdots+c_{m-1}\alpha^{m-1} \quad (13)$$

$$c_i \in GF(2)$$

으로 $GF(2^m)$상의 모든 원소를 표시할 수 있다. 이것을 벡터로 표시하면 다음과 같다.

$$[c_0,\ c_1,\ c_2,\ \cdots,\ c_{m-1}] \quad (14)$$

이러한 원소 표시 방법을 관용기저에 의한 $GF(2^m)$상의 원소 표시 방법이라 하며 α^0, α^1, α^2, …, α^{m-1}은 모든 원시다항식에 대하여 선형독립이므로 모든 원시 다항식은 관용기저를 갖는다.

표 4, 표 5, 표 6의 $GF(2^3)$상의 원소를 관용기저로 표시하면 표 7과 같다.

표 7. 관용기저에 의한 $GF(2^3)$상의 원소 표시

원소	α^3 α^2 α^1 α^0	관용기저
α^*	0	0 0 0
α^0	1	1 0 0
α^1	α	0 1 0
α^2	α^2	0 0 1
α^3	$\alpha+1$	1 1 0
α^4	$\alpha^2+\alpha$	0 1 1
α^5	$\alpha^2+\alpha+1$	1 1 1
α^6	α^2+1	1 0 1

$p(x)=x^3+x+1$

2.3.2 $GF(2^m)$상의 정규기저

Massey, Omura는 정규기저로 $GF(2^m)$상의 원소를표시하여 자승회로, 역원회로 그리고 승산회로를 구성하였다. 정규기저로 표시된 $GF(2^m)$상의 원소의 자승과 역원계산은 정규기저 성질로부터 간단히 실행할 수 있다.

원시다항식의 원시근을 α라 할 때, $\alpha^{2^0}, \alpha^{2^1}, \alpha^{2^2}, \cdots, \alpha^{2^{m-1}}$이 선형독립이면 이 선형결합으로 $GF(2^m)$상의 모든 원소를 표시할 수 있다. 이러한 원소 표시 방법을 정규기저에 의한 $GF(2^m)$상의 원소 표시 방법이라 한다.

따라서 정규기저로 $GF(2^m)$상의 원소를 표시하면 다음과 같다.

$$F(\alpha)=\sum_{i=0}^{m-1} n_i \cdot \alpha^{2^i}$$

$$= n_0\alpha^{2^0}+n_1\alpha^{2^1}+n_2\alpha^{2^2}+\cdots+n_{m-1}\alpha^{2^{m-1}} \quad (15)$$

$$n_i \in GF(2)$$

윗식을 벡터로 표시하면 다음과 같다.

$$[n_0,\ n_1,\ n_2,\ \cdots,\ n_{m-1}] \quad (16)$$

그러나 GF(2)상의 m차의 원시다항식은 모두 정규기저를 갖지 못한다. 앞에서 설명한 표 4, 표 5, 표 6을 구성하는 원시다항식 $p(x)=x^3+x+1$은 정규기저를 갖지 못한다. GF(2)상의 3차 원시다항식 2개중 $p(x)=x^3+x^2+1$만이 정규기저를 갖는다.

원시다항식 $p(x)=x^3+x^2+1$로 만들어지는 $GF(2^3)$상의 원소를 정규기저를 이용하여 표시하면 표 8과 같다.

표 8. 정규기저에 의한 $GF(2^3)$상의 원소 표시

원소	α^{2^0} α^{2^1} α^{2^2}	정규기저
α^*	0	0 0 0
α^0	$\alpha^{2^0}+\alpha^{2^1}+\alpha^{2^2}$	1 1 1
α^1	α^{2^0}	1 0 0
α^2	α^{2^1}	0 1 0
α^3	$\alpha^{2^0}+\alpha^{2^2}$	1 0 1
α^4	α^{2^2}	0 0 1
α^5	$\alpha^{2^1}+\alpha^{2^2}$	0 1 1
α^6	$\alpha^{2^0}+\alpha^{2^1}$	1 1 0

$p(x)=x^3+x^2+1$

따라서, 정규기저를 이용하여 $GF(2^m)$상의 원시원소를 표시하려면 먼저 GF(2)상의 m차 원시다항식이 정규기저를 갖는가를 확인해야 한다.

정규기저를 갖고 있는 원시다항식의 확인은 관용기저를 정규기저로 변환시키는 변환행렬을 구하여 각 행과 열의 선형독립성을 조사하여 한다. 즉 행렬의 원소로 이루어지는 행렬식의 값이 1일 때만 원시다항식이 정규기저를 갖는다.

필자가 GF(2)상에서 m=15차까지의 원시다항식에 대하여 정규기저를 갖는 것을 확인한 결과 표 9와 같다. 따라서 원시다항식의 정규기저 유무를 반드시 확인 후 사용해야 한다.

표 9. 정규기저를 갖는 원시다항식 수

m	PP	NP	비고
2	1	1	50%
3	2	1	50%
4	2	1	50%
5	6	3	50%
6	6	3	50%
7	18	7	39%
8	16	7	43%
9	48	19	39%
10	60	29	48%
11	176	86	48%
12	144	48	33%
13	630	299	47%
14	756	265	35%
15	1800	497	27%

PP : 원시다항식

NP : 정규기저를 갖는 원시다항식

2.4 유한체의 원시원소

표 3의 멱승표에서 알 수 있는 바와 같이 유한체 GF(5)상의 모든 원소의 4승은 모두 1이다. 즉 크기가 p인 기초체의 모든 원소의 (p−1)승은 1이 된다. 또 표 3의 멱승표에서 원소 2, 3은 각각 멱승을 증가시켜가면 유한체 GF(5)상의 모든 원소가 나타난다. 이와 같은 원소를 원시원소(primitive element)라 하며 (p−1)보다 작은 0이 아닌 수로 (p−1)과 서로소인 i를 찾아 원시원소를 i승하여도 원시원소가 된다. 따라서 유한체 GF(p)상의 원시원소의 수는 Euler 함수 $\varphi(p-1)$가 되며 GF(5)상의 원시원소의 수는 $\varphi(4)=2$가 된다. 처음 1이 되는 멱승을 그 원소의 위수(order)라 하며 원시원소의 위수는 (p−1)임을 알 수 있다.

마찬가지로 표 6의 멱승표에서 GF(2^3)상의 원시원소는 GF(5)상의 경우와 같이 임의의 원소를 멱승시켜 감에 따라 GF(2^3)상의 모든 원소가 나타나는 α, α^2, α^3, α^4, α^5, α^6이다. GF(2^3)상의 원시원소의 경우도 (2^3-1)보다 작은 0이 아닌 수로 (2^3-1)과 서로 소인 i를 찾아 원시원소를 i승하여도 원시원소가 된다. 그러므로 GF(p^m)상의 원시원소의 수도 $\varphi(p^m-1)$개이며 GF(2^3)상의 원시원소의 수는 $\varphi(2^3-1)=6$개 임을 확인할 수 있다.

원시원소는 암호학이론 분야에서 중요한 역할을 한다. 즉 유한체상에서의 멱승관계인 이산 대수 문제(discrete logarithm problem)가 Diffie-Hellman의 공개키 분배방식과 ID를 기반으로 하는 키 분배 방식에 이용되고 있다. 이산대수는 유한체상에서의 대수를 말하며 유한체 상에서 이산적 대수를 계산하는 문제를 이산 대수 문제라 한다. 실수체의 대수를 계산하는 문제는 매우 큰 수의 경우에도 간단하나 유한체 연산체계에서 대수 문제를 계산하는 것은 매우 어려운 NP문제로 알려져 있다.

이산 대수 문제는 유한체 상의 멱승관계이므로 다음 관계가 있다. GF(p)상의 임의의 원소 g, z에 대하여

$$y=g^z \bmod p \qquad (17)$$

이 성립할 때 y와 g를 알고 z를 구하는 경우 z를 y의 이산 대수 문제라 하며 z는 다음 식으로 표시된다.

$$z=\log_g y \qquad (18)$$

이 때 g가 GF(p)상의 원시원소이면 z값에 따라 서로 다른 y값을 갖게 된다. 물론 확대체 GF(p^m)상에서도 위 이산 대수 문제가 정의된다.

3. 유한체 GF(2^m)상의 연산

GF(2^m)상의 원소의 표시를 지수형태로 표시하는 경우와 기저 표현에 의한 방법이 있으나 지수 형태의 표시 경우 디지탈 회로화가 불편하여 기저 표시 원소의 연산만을 설명한다. 기저로 표시된 유한체 GF(2^m)상의 연산은 원소 상호간의 가감승제산을 모두 고려해야 하나 일반적으로 감산과 제산을 제외시킨다. 왜냐하면 감산은 피감산원소에 감산원소의 음원(가산역원)을 더하는 과정으로 생각하고 제산은 피제산원소에 제산원소의 역원을 곱하는 것으로 대신한다. 특히 GF(2^m)상의 원소의 음원은 원소 자신이므로 가산과 감산은 동일하다. 그러므로 승산에 대한 역원만 구할 수 있으면 가산과 승산으로 가감승제산이 모두 가능하게 된다. 따라서 기저로 표시된 GF(2^m)승의 가산과 승산 그리고 역원 계산 방식과 멱승 계산을 위한 자승 계산 방식에 대하여 알아 본다.

3.1 GF(2^m)상의 가산

GF(2^m)상의 가산은 각 원소를 나타내는 다항식의 차수가 동일한 α의 계수 사이의 합이므로 기저나 원시다항식에 관계없이 동일하다. 관용기저로 표시된 GF(2^m)상의 피가산 원소와 가산원소를 식 (19), 식 (20)으로 표시하고 가산 후의 원소를 식 (21)으로 표시하면 각 $\alpha^i(0\leq i\leq m-1)$의 계수 사이의 관계식은 식 (22)의 배타적 논리로 표시된다.

$$A(\alpha)=a_0+a_1\alpha+a_2\alpha^2+\cdots+a_{m-1}\alpha^{m-1} \quad (19)$$

$$B(\alpha)=b_0+b_1\alpha+b_2\alpha^2+\cdots+b_{m-1}\alpha^{m-1} \quad (20)$$

$$Y(\alpha)=y_0+y_1\alpha+y_2\alpha^2+\cdots+y_{m-1}\alpha^{m-1} \quad (21)$$

$$a_i+b_j=y_i \quad (22)$$

단, $A(\alpha)$, $B(\alpha)$, $Y(\alpha)$ GF(2^m)

a_i, b_i, y_i GF(2)

따라서, 관용기저로 표시된 GF(2^m)상의 가산회로는 그림 1과 같다.

한편 정규기저로 표시된 GF(2^m)상의 피가산원소와 가산원소를 식 (23), 식 (24)로 표시하고 가산 후의 원소를 식 (25)로 표시하면 $\alpha^{2^i}(0\leq i\leq m-1)$의 계수 사이의 관계는 식 (26)과 같으며 가산회로는 그림 2와 같다.

$$G(\alpha)=g_0\alpha^{2^0}+g_1\alpha^{2^1}+g_2\alpha^{2^2}+\cdots+g_{m-1}\alpha^{2^{m-1}} \quad (23)$$

$$H(\alpha)=h_0\alpha^{2^0}+h_1\alpha^{2^1}+h_2\alpha^{2^2}+\cdots+h_{m-1}\alpha^{2^{m-1}} \quad (24)$$

$$Z(\alpha)=z_0\alpha^{2^0}+z_1\alpha^{2^1}+z_2\alpha^{2^2}+\cdots+z_{m-1}\alpha^{2^{m-1}} \quad (25)$$

$$g_i+h_j=z_i \quad (26)$$

단, $G(\alpha)$, $H(\alpha)$, $Z(\alpha)$ GF(2^m)

g_i, h_i, z_i GF(2)

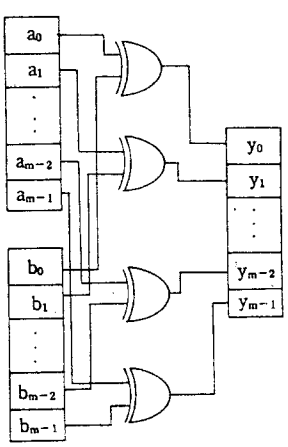

그림 1. 관용기저로 표시된 GF(2^m)상의 가산회로

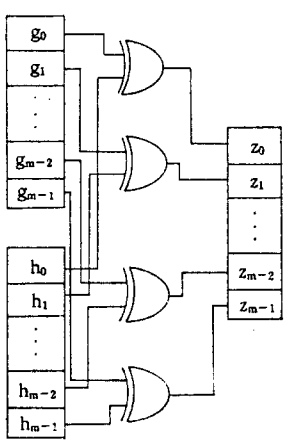

그림 2. 정규기저로 표시된 GF(2^m)상의 가산회로

3.2 GF(2^m)상의 승산

먼저 관용기저상에서의 GF(2^m)상의 원소의 승산회로 구성에 대하여 알아보자. 관용기저로 표시된 승산 원소와 피승산원소를 식 (27), 식 (28)로 표시하면 A(α)와 B(α)의 승산 값 Y(α)는 식 (29)로 표시된다.

$$A(\alpha)=\sum_{i=0}^{m-1} a_i\alpha^i \tag{27}$$

$$B(\alpha)=\sum_{k=0}^{m-1} b_k\alpha^k \tag{28}$$

$$\begin{aligned} Y(\alpha)&=A(\alpha)\cdot B(\alpha)\\ &=\{\sum_{k=0}^{m-1} a_i\cdot\alpha^i\}\{\sum_{k=0}^{m-1} b_k\cdot\alpha^k\}\\ &=\sum_{k=0}^{m-1}(b_k\cdot A(\alpha))\alpha^k\\ &=p^{(m-1,m-1)} \end{aligned} \tag{29}$$

여기서 $p^{(1,0)}$는 $A(\alpha)b_g\alpha^g$를 곱한 다음 $p^{(g-1,0)}$와 합한 값이며 $p^{(m-1,j)}$는 $p^{(m-1,j-1)}$를 mod $(\alpha^{(m-1-j)}p(\alpha))$한 값이다. 이러한 과정은 승산부와 mod부로 나누어 계산된다. 앞에서 mod$(\alpha^{(m-1-j)}p(\alpha))$는 α의 차수를 낮추어 (m−1)차 이하로 줄이기 위한 것이며, 원시다항식 p(α)가 단위 다항식이므로 $\alpha^{(m-1-j)}p(\alpha)$도 단위 다항식이다.

승산부의 $p^{(m-1,0)}$의 계산 과정은 다음과 같다.

$$\begin{aligned} p^{(0,0)}&=b_0\cdot A(\alpha)\\ p^{(1,0)}&=b_1\cdot\alpha\cdot A(\alpha)+b_0\cdot A(\alpha)\\ &=b_1\cdot\alpha\cdot A(\alpha)+p^{(0,0)}\\ p^{(2,0)}&=b_2\cdot\alpha^2\cdot A(\alpha)+b_1\cdot\alpha\cdot A(\alpha)+b_0\cdot A(\alpha)\\ &=b_2\cdot\alpha^2\cdot A(\alpha)+p^{(1,0)}\\ &\vdots\\ p^{(m-1,0)}&=b_{m-1}\cdot\alpha^{m-1}\cdot A(\alpha)+p^{(m-2,0)} \end{aligned} \tag{30}$$

식 (30)은 A(α)와 B(α)의 곱으로 α의 2(m−1)차 다항식이므로 이를 mod부에 입력시켜 (m−1)차 이하로 만들어야 한다.

이 과정은 다음과 같다.

$$\begin{aligned} p^{(m-1,1)}&=p^{(m-1,0)} \bmod (\alpha^{(m-1-1)}\cdot p(\alpha))\\ p^{(m-1,2)}&=p^{(m-1,1)} \bmod (\alpha^{(m-1-2)}\cdot p(\alpha))\\ &\vdots \end{aligned}$$

$$p^{(m-1,m-1)}=p^{(m-1,m-2)} \bmod p(x) \tag{31}$$

일반식으로 정리하면

$$\begin{aligned} p^{(m-1,m-1)}=((((p^{(m-1,0)} &\bmod (\alpha^{(m-1-1)}\cdot p(\alpha))\\ &\cdot \bmod (p^{(m-1-2)}\cdot p(\alpha)))\cdots) \bmod p(\alpha) \end{aligned} \tag{32}$$

이다. $p^{(g,j)}$에서 g는 0~(m−1), j는 1~(m−1) 값을 갖는다. 식 (32)는 A(α)와 B(α)의 곱인 Y(α)로 식 (29)와 일치한다. 즉, $p^{(m-1,m-1)}=A(\alpha)\cdot B(\alpha)$로 α의 최고 차수가 m−1인 관용기저표시의 GF(2^m)상의 원소가 된다. 이 과정을 m=3인 GF(2^3)상의 승산회로를 구성하면 그림 3과 같다.

Massey와 Omura는 정규기저의 성질상 승산하려는 두 원소의 계수와 승산 후의 원소의 계수 사이에 관계식이 각 원소 계수에 대하여 동일함에 착안하여 승산회로를 구성하였다.

GF(2^m)상의 두 원소와 승산 후의 원소를 정규기저로 표시하면

$$G(\alpha)\Rightarrow[g_0,g_1,g_2,\cdots,g_{m-1}] \tag{33}$$

$$H(\alpha)\Rightarrow[h_0,h_1,h_2,\cdots,h_{m-1}] \tag{34}$$

$$Z(\alpha)=G(\alpha)\cdot H(\alpha)\Rightarrow[z_0,z_1,z_2,\cdots,z_{m-1}] \tag{35}$$

이다. 승산 후의 원소 Z(α)의 계수 $z_i(0\leq i\leq m-1)$는 피승산원소 G(α), 승산원소 H(α)의 계수 함수 f로 표시할 수 있으며 이를 승산함수라 한다.

i=m−1일 때의 승산함수를

$$z_{m-1}=f(g_0,g_1,g_2,\cdots,g_{m-1};\ h_0,h_1,h_2,\cdots,h_{m-1}) \tag{36}$$

라 하면 정규기저로 표시된 원소의 자승 성질로부터

$$Z^2(\alpha)=G^2(\alpha)\cdot H^2(\alpha) \tag{37}$$

$z_{m-2},z_{m-3},\cdots,z_0$의 승산 함수는 다음과 같이 표시된다.

$$z_{m-2}=f(g_{m-1},g_0,g_1,\cdots,g_{m-2};\ h_{m-1},h_0,h_1,\cdots,h_{m-2}) \tag{38}$$

$$z_{m-3}=f(g_{m-2},g_{m-1},g_0,\cdots,g_{m-3};\ h_{m-2},h_{m-1},h_0,\cdots,h_{m-3}) \tag{39}$$

$$\vdots$$

$$z_0 = f(g_1, g_2, g_3, \cdots, g_0 ; h_1, h_2, h_3, \cdots, h_0) \quad (40)$$

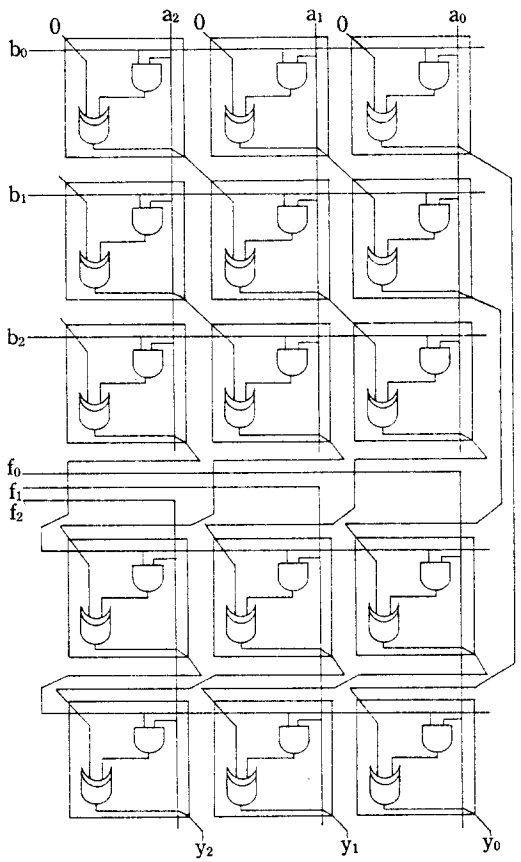

그림 3. 관용기저로 구성된 GF(2^3)상의 승산회로

앞에서 설명한 $p(x)=x^3+x^2+1$로 구성되는 GF(2^3)상의 원소 G(α), H(α)의 곱인 Z(α)의 계수를 구해보면 다음과 같다.

$$Z_2 = g_1h_0 + g_1h_1 + g_0h_1 + g_0h_2 + g_2h_0 \quad (41)$$

$$Z_1 = g_0h_2 + g_0h_0 + g_2h_0 + g_2h_1 + g_1h_2 \quad (42)$$

$$Z_0 = g_2h_1 + g_2h_2 + g_1h_2 + g_1h_0 + g_0h_1 \quad (43)$$

G(2^3)의 승산 함수는 5개의 AND gate와 4개의 EX-OR gate로 실현할 수 있으며 GF(2^3)상의 승산회로는 3개의 승산 함수 회로로 구성되며 승산 함수 회로와 승산 회로는 그림 4와 그림 5와 같다.

관용기저와 정규기저로 표시된 GF(2^m)상의 승

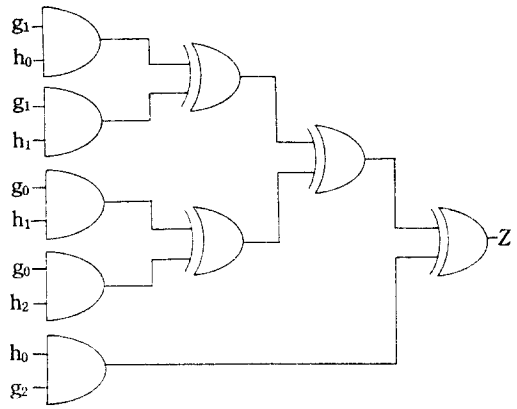

그림 4. GF(2^3)상의 승산 함수

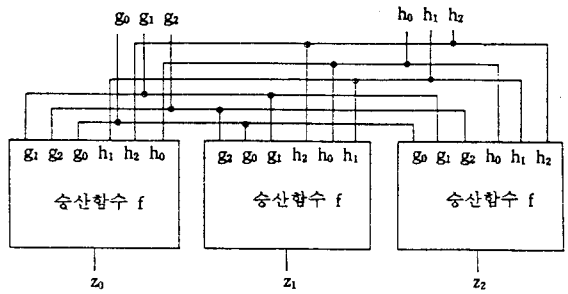

그림 5. 정규기저상의 GF(2^3)상의 승산 회로

산회로를 비교하면 관용기저로 구성된 승산회로 구조가 간단하며 원시다항식의 변화에도 연산이 가능하다. 반면 정규기저로 구성된 승산회로는 원시다항식의 변화에 따라 회로가 달라지는 단점이 있다.

3.3 GF(2^m)상의 자승

GF(2^m)상의 승산회로에 피승산원소와 승산원소를 동일하게 입력시키면 간단히 GF(2^m)상의 원소를 자승할 수 있으나, 자승회로는 멱승회로, 특히 역원회로의 일부로 사용되고 있어 승산회로보다 구성이 간단한 자승계산만 실행하는 회로를 생각해 보자.

관용기저 상에서 GF(2^m)상의 원소의 자승은 조

합논리를 사용해야 한다. $Y(\alpha)=A^2(\alpha)$는 α의 우수차 항만 갖게 되며 m차 이상은 원시다항식으로 (m−1)차 이하로 낮추어서 $A^2(\alpha)$를 구한다.

$$Y(\alpha)=\sum_{k=0}^{m-1} y_k \cdot \alpha^k \equiv \sum_{n=0}^{m-1} a_n \cdot \alpha^{2n} \bmod P(\alpha) \quad (44)$$

$Y(\alpha)$의 계수를 $A(\alpha)$의 계수로 나타내어 GF(2^3)상의 자승회로를 PLA로 구성하면 그림 6과 같다.

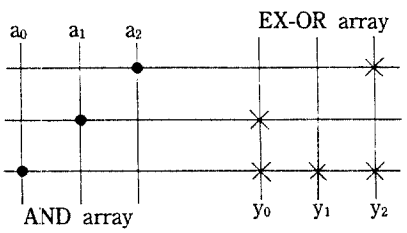

그림 6. 조합논리로 구성한 GF(2^3)상의 역원 회로

$$P(x)=x^3+x^2+1 \quad (45)$$

$$Y(\alpha)=\sum_{k=0}^{2} y_k \cdot \alpha^k \equiv \sum_{n=0}^{2} a_n \cdot \alpha^{2n} \bmod P(\alpha) \quad (46)$$

$$y_0=a_0+a_2 \quad (47)$$

$$y_1=a_2 \quad (48)$$

$$y_2=a_1+a_2 \quad (49)$$

정규기저상에서 GF(2^m)상의 원소를 자승하는 것은 대단히 간단하다. 정규기저 성질에 의하면 원소 G(α)의 계수를 순회치환하면 간단히 자승계산이 된다.

$$G(\alpha)=g_0\alpha^{2^0}+g_1\alpha^{2^1}+g_2\alpha^{2^2}+\cdots+g_{m-1}\alpha^{2^{m-1}} \quad (50)$$

$$G^2(\alpha)=g_{m-2}\alpha^{2^0}+g_0\alpha^{2^1}+g_1\alpha^{2^2}+\cdots+g_{m-2}\alpha^{2^{m-1}} \quad (51)$$

즉 $\alpha^{2^m}\rightarrow\alpha$이므로 식 (50)을 자승하면 $g_{m-1}\cdot\alpha^{2^m}$이 $g_{m-1}\cdot\alpha$가 되어 식 (51)과 같이 표현된다. 그러므로 우측 순회치환으로 자승을 간단히 할 수 있다.

3.4 GF(2^m)상의 역원 계산

GF(2^m)상의 원소 $A(\alpha)$의 역원은 GF(2^m)의 성질에 의해 다음 식으로 표시된다.

$$A^{-1}(\alpha)=A^{2^m-2}(\alpha) \quad (52)$$

관용기저상에서의 역원 계산 회로는 원소를 직접 2^m-2 승하여 원시다항식으로 (m−1)차 이하로 차수를 낮추어 조합논리를 구성한다. GF(2^3)상의 역원 계산 회로를 구성하면 그림 7과 같다.

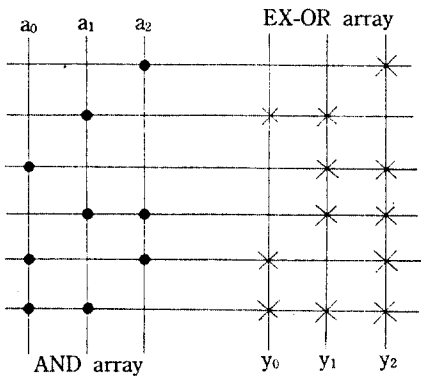

그림 7. 조합논리로 구성한 GF(2^3)상의 역원 계산 회로

$$P(x)=x^3+x^2+1 \quad (53)$$

$$Y(\alpha)=\sum_{n=0}^{2} y_n \cdot \alpha^n \equiv A^6(\alpha) \bmod P(\alpha) \equiv A^{-1}(\alpha) \quad (54)$$

$$y_0=a_0+a_2+a_0\cdot a_1+a_0\cdot a_2+a_1\cdot a_2 \quad (55)$$

$$y_1=a_1+a_2+a_0\cdot a_1+a_1\cdot a_2 \quad (56)$$

$$y_2=a_1+a_0\cdot a_2+a_1\cdot a_2 \quad (57)$$

정규기저로 역원회로를 계산하는 경우는

$$2^m-2=2^1+2^2+2^3+\cdots+2^{m-1} \quad (58)$$

이므로

$$A^{-1}(\alpha)=(A^2(\alpha))\,(A^{2^2}(\alpha))\cdots(A^{2^{m-1}}(\alpha)) \quad (59)$$

와 같이 표시된다. 따라서 앞에서 설명한 자승회로와 승산회로를 이용하여 역원 계산회로를 구성할 수 있다. 이때 역원 계산에 걸리는 시간이 많이 소요되는 것이 단점이다.

4. 결 언

유한체 GF(2^m)은 디지탈 회로에 응용이 용이하므로 여러 분야에서 이용되고 있다. 특히 암호학 이론 분야에서는 m 값이 수십 내지 수백으로 원소의 수가 많은 GF(2^m)이 이용되고 있다.

GF(2^m)상의 원소의 연산은 원소의 표시방법에 따라 연산절차의 복잡성이 다르다. 원소를 지수로 표현하면 승·제산이 용이하고 가·감산이 복잡하며, 더우기 디지탈 회로에 적용시킬 수 없어 불편하다. 기저로 원소를 표시한 경우는 가·감산이 간단하나 승·제산이 복잡하며 또한 기저에 따라 연산회로의 복잡도가 다르다.

관용기저로 표시된 GF(2^m)상의 연산에서 승산회로 구성은 간단하나 자승, 역원 계산회로 구성은 복잡하다. 정규기저의 경우는 승산회로 구성은 복잡하나 자승회로나 역원 계산 회로는 비교적 간단하다. 그러나 정규기저는 원시다항식 선택의 폭이 좁다. 모든 원시다항식은 관용기저가 정의되나 정규기저가 정의되지 않는 것이 많다. 따라서, 유한체 GF(2^m) 상의 연산은 응용분야에 따라 연산회로를 적당히 선택해야 한다.

앞으로 유한체 GF(2^m)연산이 여러 분야에 이용될 전망이 크며 특히 m 값이 큰 경우의 연산이 요구되고 있어, 보다 연산 알고리즘이 간단하고 연산속도가 개선된 방식의 개발이 요구되고 있다.

참 고 문 헌

1. W.W. Peterson, "Error-Correcting Codes," New York, Wiley, 1961.

2. R.E. Blahut, "Theory and Practice of Error Control Codes," California Addison-Wesley, 1983.

3. C.C. Wang, T.K. Troung, H.M. Mao, L.T. Deutsch, T.K. Omura and I.S. Reed, "VLSI Trans. comput. Vol. C-34, No. 8, pp.709-716, Aug. 1985.

4. T.C. Bartee and D.I. Schneider, "Computation with Finite Field," Inform. Contr. Vol. 6, pp.79-98, Mar. 1963.

5. 高橋碧郎, "組み合わせ理論とその應用," 東京岩波全書, 1979.

6. 원동호, "GF(2)상의 정규기저를 갖는 원시다항식 분류에 관한 연구," 정보보호와 암호에 관한 워크% 논문집, pp.219-227, 1989.

7. B.A. Laws and C.K. Rushforth, "A Cellular-array multiplier for GF(2^m)," IEEE Trans. Comput. Vol. c-20, pp.1953-1978, Dec. 1971.

8. B. Benjauthrit and I.S. Reed, "Galois switching function and their application," IEEE Trans. Comput, Vol. C-25, pp.78-86, Jun. 1976.

9. 吉田浩, 今村恭己, "GF(2)上の原始多項式の分布," 情報理論とその應用研究會 第8回シンポジウム資料, pp.1-3, 日本, 1985.

10. W. Stahnke, "Primitive binary polynomials," Mathematics of Computation, Vol. 27, No. 124, p. 977-980, Oct. 1973.

11. N. Zierler and J. Brillhart, "On primitive trinomials (Mod 2)," Inform, Contr. Vol. 13, pp.541-554, 1968.

12. N. Zierler and Brillhart, "On primitive trinomials (Mod 2) II," Inform, Contr. Vol. 14, pp.566-569, 1969.

13. 박용준, 강성수, 김홍수, "GF(2^m)상의 누승 및 역원을 구하는 방법에 관한 연구," 전기전자공학 학술대회 논문집, pp.1191-1194, 1987.

14. 원동호, 김병찬, "GF(2^m)상의 승산기 구성에 관한 연구," 전기전자공학학술대회 논문집, pp.845-849. 1987.

□ 著者紹介

원 동 호(종신회원)

1949年生

1976年 成均館大學校 電子工學科 卒業(學士)
1978年 成均館大學校 大學院 電子工學科 卒業(碩士)
1988年 成均館大學校 大學院 電子工學科(博士)
1978年～1980年 韓國電子通信研究所 專任研究員
1985年～1986年 日本 東京工大 客員研究員
現 成均館大學校 情報工學科 副教授
관심분야 : 정보이론, 암호이론