GF(2^m) 상의 누승 및 역원을 구하는 방법에 관한 연구

°박 용 준 강 성 수 김 흥 수
인하 대학교 전자 공학과

A Study on a Method for Computing the Powers and Inverses in GF(2^m)

Yong Joon Park Sung Su Kang Heung Soo Kim
Dept. of Electronics Inha University

Abstract

This paper presents a method for computing the powers and inverse of an element in GF(2^m). This method is based on the squaring algorithm $A^2=\sum_{i=0}^{2m-2} P_i$, where $P_i=a_{i/2}$ if i is even, $P_i=0$ otherwise, derived from the multiplication algorithm for two elements in GF(2^m).

The powers and inverses in GF(2^m) for m=2,3, 4,5 were obtained using computer program, and used in circuit realization of Galois switching funtion. The squaring and inverse generating circuits are also shown.

1. 서 론

유한체 GF(p^m)의 응용분야는 error-correcting code, 스위칭 이론, 디지털 신호 처리등이 있다. 이중 GF(2^m)은 2^m개의 원소로 이루어지며, 각 원소는 m개의 2진 비트로 표시될 수 있다. GF(2^m)상에서의 가산은 비트 독립적이고 수월하지만, 승산은 보다 복잡 하므로 GF(2^m)상의 두 원소를 곱하는 승산기를 실현시키는 연구가 여러사람에 의해 진행되어 왔다.[1-4]

특히 Yeh, Reed 와 Truong[3] 은 GF(2^m)상의 두 원소 A와 B의 곱셈을 P=AB+C인 형태로 계산한 후 이를 병렬 입출력 형태의 cell인 경우 cell의 내부는 shift register 와 세 원소 A,B,C 및 기약다항식 fi 등으로 구성하였으며, R.G.Gallager, B.A.Laws 와 C.K.Rushforth[4]등은 GF(2^m)상의 두 원소 A,B 와 기약다항식 fi로 구성된 cell 구조로써 승산기를 구성하였다. 또한 I.S.Reed[2] 등은 GF(2^m)상의 두 원소 A,B의 표시를 normal basis로 한 후 이를 자승하여 승산을 하고 shift register를 이용하여 승산기를 구성하였다.

본 논문에서는 GF(2^m)상의 한 원소의 누승을 구하는 방법과 누승을 통해 그 원소의 역원을 구하는 방법을 제시하였다. 여기에서 GF(2^m)상의 두 원소의 승산 알고리즘[1] 을 바탕으로 해서 자승 알고리즘을 유도하고 이를 이용하여 누승을 구한다.

누승 결과는 컴퓨터 프로그램을 사용하여 구하였고 이 결과를 Galois 스위칭 함수의 회로 실현에 이용하였다. 또한 자승기 및 역원 발생 회로를 보였다.

2. GF(2^m) 상의 자승 알고리즘

유한체 GF(2^m)은 2^m 개의 원소를 가지는데 이들 원소 중 0 이 아닌 원소들은 원시원소 α의 멱으로 표시할 수 있다. 즉,

$$GF(2^m)=\{0, \alpha, \alpha^2, \ldots\ldots, \alpha^{2^m-2}, \alpha^{2^m-1}=1\} \quad (1)$$

이때 α는 원시 기약 다항식

$$F(x)=x^m+f_{m-1}x^{m-1}+\cdots+f_1x+f_0 \quad (2)$$

의 한 근이다. 즉, $F(\alpha)=0$ 이므로

$$\alpha^m = f_{m-1}\alpha^{m-1} + \ldots + f_1\alpha + f_0 \quad (3)$$

이고, 따라서 GF(2^m)의 원소는 m보다 낮은 차수의 α의 다항식으로 표시할 수 있다. 즉,

$$GF(2^m)=\left\{a_{m-1}\alpha^{m-1}+\cdots+a_1\alpha+a_0 \;\middle|\; a_i\in GF(2) \text{ for } 0\le i\le m-1\right\} \quad (4)$$

이다. 여기서 GF(2^m)의 두 원소를 A,B라고 하면

$$A=\sum_{i=m-1}^{0} a_i\alpha^i \quad (5), \qquad B=\sum_{i=m-1}^{0} b_i\alpha^i \quad (6)$$

이고 두 원소의 승산은 다음과 같다.

$$\begin{array}{rccccccc} & a_{m-1} & a_{m-2} & \cdots & a_1 & a_0 \\ \times & b_{m-1} & b_{m-2} & \cdots & b_1 & b_0 \\ \hline & a_{m-1}b_0 & a_{m-2}b_0 & \cdots & a_1b_0 & a_0b_0 \\ & a_{m-1}b_1 & a_{m-2}b_1 & \cdots & a_0b_1 & \\ & \vdots & \vdots & & & \\ & a_{m-1}b_{m-2} & a_{m-2}b_{m-2} & \cdots & a_2b_{m-2} & a_1b_{m-2} \quad a_0b_{m-2} \\ a_{m-1}b_{m-1} & a_{m-2}b_{m-1} & \cdots & a_1b_{m-1} & a_0b_{m-1} & \\ \hline P_{2m-2} & P_{2m-3} & \cdots & P_m & P_{m-1} & P_{m-2}\cdots P_1 \quad P_0 \end{array} \quad (7)$$

$$A.B=\sum_{i=m-1}^{0} p_i\alpha^i + \sum_{i=2m-2}^{m} p_i\alpha^i \quad (8)$$

식 (3)에 의해서 GF(2^m)의 원소는 m보다 낮은 차수의 α의 다항식으로 표시되어야 하므로 식(8)은 최종적으로 다음 식과 같아야 한다.

$$A.B=\sum_{i=m-1}^{0} R_i\alpha^i \quad (9)$$

여기서 Ri 는 식 (8)의 둘째 항 $\sum_{i=2m-2}^{m} P_i\alpha^i$을 식 (3)에 의하여 변형시킨 후 첫째 항 $\sum_{i=m-1}^{0} P_i\alpha^i$과 합성시킨 것이다.

이때 자승은 B=A인 경우로서, 식(8)은 다음과 같이 된다.

$$A^2=\sum_{i=0}^{2m-2} P_i \text{ , where } P_i=\begin{cases} a_{i/2} & i=\text{even} \\ 0 & i=\text{odd} \end{cases} \quad (10)$$

마찬가지로 식 (3)에 의해 GF(2^m)의 원소는 m 보다 낮은 차수의 α의 다항식으로 표시되어야 하므로 식 (10)을 식(9)와 같이 합성시킨다.

예) GF(2^5)인 경우

$$A^2=a_2\alpha^4+(a_3\oplus a_4)\alpha^3+(a_1\oplus a_4)\alpha^2+a_3\alpha+(a_0\oplus a_4)$$

3. GF(2^m) 상의 누산 방법

GF(2^m)상의 한 원소 A의 N승을 구한다고 가정한다.

(1) N 을 2의 멱들의 합으로 표시한다. 이때 N 이 짝수일 때에는 2의 멱들의 합만으로 표시되고, N 이 홀수일 때에는 2의 멱들의 합 + 1 이 된다.

(2) 2의 멱들을 앞의 자승 알고리즘에 의해 구한 후, 이것들을 승산 알고리즘에 적용하여 승산을 행한다.

이러한 승산시, 동일 계수의 곱은 그 자신이란 사실과 GF(2^m)상의 가산은 mod 2 합이란 사실을 이용하여 많은 동일항을 소거할 수 있다. 이를 다시 쓰면,

① $(a_i)^n = a_i \quad (0\le i\le m-1)$

② $\sum_k a_i.a_j = \begin{cases} a_i.a_j & k=\text{odd (단, k는 } a_i.a_j\text{항의 갯수)} \\ 0 & k=\text{even} \end{cases}$

for R_i $(0\le i\le m-1)$ (11)

이 누산 방법의 예로서 GF(2^m)상의 한 원소 A 의 역원을 구해본다.

$$A^{-1}=A^{2^m-2} \tag{12}$$

이므로 $N = 2^m-2$ 인 경우이다. 따라서 N은 다음과 같이 쓸 수 있다.

$$N=2^m-2=2+2^2+2^3+\cdots+2^{(m-1)} \tag{13}$$

식 (13)을 식(12)에 대입하면

$$A^{-1}=(A^2)(A^{2^2})(A^{2^3})\cdots(A^{2^{(m-1)}}) \tag{14}$$

이다. 즉 A의 역원은 A의 자승을 자승 알고리즘에 의해 (m -1)번 까지 구한 후, 이것들의 승산을 행하여 구할 수 있다.

4. 적 용 예

GF(2^3)상에서 정의된 함수 Z가 표1과 같이 주어진다고 가정한다. 여기서 GF(2^3)의 원소는 표2와 같다.

Galois 스위칭 함수 구성 방법에 의해 함수 Z는 다음과 같다.

$$Z=e_2X^7+e_6X^3+e_6X^2+e_6X+e_5$$

이 함수를 논리 회로로 실현시키면 다음 그림 4.1과 같다.

누승 결과를 이용하여 그림 4.1의 블록소자의 실제 회로를 구성하면 그림 4.2와 같다.

X	Z
e_0	e_5
e_1	e_3
e_2	e_6
e_3	e_5
e_4	e_2
e_5	e_0
e_6	e_1
e7	e_4

표 1. GF(2^3)상의 함수 Z

Table 1.A function Z defined over GF(2^3)

a_2	a_1	a_0	
0	0	0	$0 = e_0$
0	0	1	$1 = e_1$
0	1	0	$\alpha = e_2$
1	0	0	$\alpha^2 = e_3$
1	1	0	$\alpha^2+\alpha = e_4$
1	0	1	$\alpha^2+1 = e_5$
0	1	1	$\alpha+1 = e_6$
1	1	1	$\alpha^2+\alpha+1 = e_7$

표 2. GF(2^3)의 원소 (단, $\alpha^3+\alpha+1=0$)

Table 2. Elements in GF(2^3)

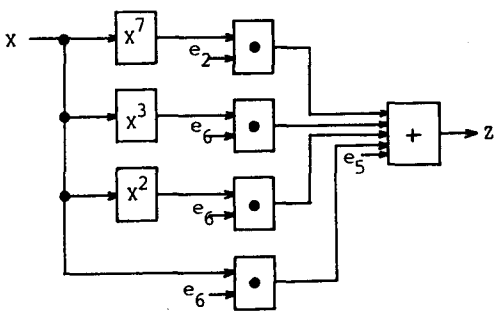
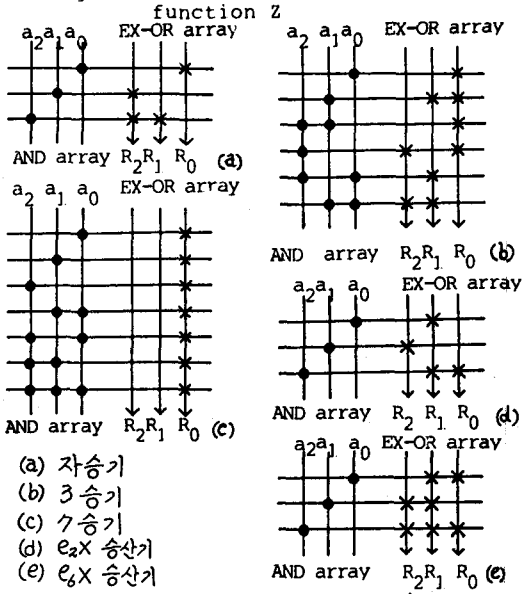


그림 4.1 함수 Z의 실현 구상 회로

Fig 4.1 Block circuit realizing a function Z



(a) 자승기
(b) 3승기
(c) 7승기
(d) e_2X 승산기
(e) e_6X 승산기

그림 4.2 그림 4.1 의 블록 소자의 실제 회로

Fig 4.2 Real circuits of Fig 4.1

5. 자승기 및 역원 발생 회로 구성

(1) GF(2^3)인 경우

$$A^2 = \sum_{i=1}^{0} R_i\alpha^i, \quad A^{-1}=A^2 = \sum_{i=1}^{0} R_i\alpha^i$$

$R_0=a_0\oplus a_1$

$R_1=a_1$

(2) $GF(2^3)$인 경우

$$A^2 = \sum_{i=2}^{0} R_i \alpha^i \quad , \quad A^{-1}=A^6 = \sum_{i=2}^{0} R_i \alpha^i$$

$R_0=a_0$ $\quad R_0=a_0 \oplus a_1 \oplus a_1 a_2 \oplus a_2$

$R_1=a_2$ $\quad R_1=a_0 a_1 \oplus a_2$

$R_2=a_1 \oplus a_2$ $\quad R_2=a_1 \oplus a_2 \oplus a_0 a_2$

(3) $GF(2^4)$인 경우

$$A^2 = \sum_{i=3}^{0} R_i \alpha^i$$

$R_0=a_0 \oplus a_2$

$R_1=a_2$

$R_2=a_1 \oplus a_3$

$R_3=a_3$

$$A^{-1}=A^{14} = \sum_{i=3}^{0} R_i \alpha^i$$

$R_0=a_0 \oplus a_1 \oplus a_1 a_2 a_3 \oplus a_1 a_2 \oplus a_0 a_1 a_2 \oplus a_0 a_2 \oplus a_2 \oplus a_3$

$R_1=a_0 a_1 \oplus a_0 a_1 a_3 \oplus a_1 a_2 \oplus a_0 a_2 \oplus a_3 \oplus a_1 a_3$

$R_2=a_0 a_1 \oplus a_0 a_2 \oplus a_0 a_2 a_3 \oplus a_0 a_3 \oplus a_2 \oplus a_3$

$R_3=a_1 \oplus a_2 \oplus a_2 a_3 \oplus a_1 a_3 \oplus a_0 a_3 \oplus a_1 a_2 a_3 \oplus a_3$

(4) $GF(2^5)$인 경우

$$A^2 = \sum_{i=4}^{0} R_i \alpha^i$$

$R_0=a_0 \oplus a_4$

$R_1=a_3$

$R_2=a_1 \oplus a_4$

$R_3=a_3 \oplus a_4$

$$A^{-1}=A^{30} = \sum_{i=4}^{0} R_i \alpha^i \quad R_4=a_2$$

$R_0=a_0 \oplus a_0 a_1 a_4 \oplus a_0 a_2 \oplus a_0 a_1 a_2 a_3 \oplus a_0 a_3 \oplus a_0 a_1 \oplus a_0 a_1 a_2 \oplus a_1 a_3 \oplus$
$a_1 a_2 \oplus a_2 \oplus a_0 a_2 a_3 \oplus a_1 a_2 a_3 \oplus a_0 a_3 a_4 \oplus a_1 a_4 \oplus a_4 \oplus a_0 a_1 a_3 a_4 \oplus$
$a_0 a_2 a_3 a_4 \oplus a_1 a_2 a_3 a_4 \oplus a_2 a_3 a_4$

$R_1=a_0 a_1 \oplus a_0 a_1 a_4 \oplus a_0 a_4 \oplus a_1 \oplus a_1 a_2 a_3 \oplus a_1 a_4 \oplus a_1 a_2 a_4 \oplus a_0 a_1 a_2 \oplus$
$a_0 a_1 a_2 a_3 \oplus a_0 a_2 \oplus a_0 a_1 a_2 a_4 \oplus a_1 a_2 a_3 a_4 \oplus a_2 a_3 a_4 \oplus a_3 \oplus a_0 a_3$
$\oplus a_0 a_3 a_4 \oplus a_4$

$R_2=a_1 a_3 \oplus a_0 a_2 \oplus a_0 a_1 \oplus a_0 a_1 a_3 \oplus a_1 a_2 \oplus a_0 a_2 a_3 \oplus a_2 a_4 \oplus a_3 a_4 \oplus$
$a_3 \oplus a_0 a_1 a_2 a_4 \oplus a_1 a_2 a_3 a_4 \oplus a_2 a_3 a_4$

$R_3=a_0 a_1 \oplus a_1 a_2 a_3 \oplus a_1 a_4 \oplus a_2 \oplus a_2 a_3 \oplus a_2 a_3 a_4 \oplus a_3 a_4 \oplus a_0 a_1 a_2 a_3 \oplus$
$a_0 a_2 \oplus a_1 a_3 \oplus a_0 a_3 a_4 \oplus a_4 \oplus a_0 a_1 a_3 a_4 \oplus a_0 a_2 a_4 \oplus a_1 a_2 a_4 \oplus$
$a_0 a_2 a_3 a_4 \oplus a_2 a_4$

$R_4=a_0 a_1 a_3 \oplus a_0 a_2 \oplus a_0 a_1 a_2 \oplus a_0 a_1 a_2 a_4 \oplus a_0 a_3 \oplus a_0 a_2 a_3 a_4 \oplus a_1 \oplus$
$a_1 a_2 \oplus a_1 a_2 a_3 a_4 \oplus a_2 a_3 \oplus a_2 a_3 a_4 \oplus a_1 a_3 \oplus a_1 a_2 a_3 \oplus a_3 \oplus a_1 a_4 \oplus$
$a_1 a_3 a_4 \oplus a_2 a_4 \oplus a_0 a_3 a_4 \oplus a_0 a_4$

6. 자승기 및 역원 발생 회로 실현

제 2 장에서 제시한 자승 알고리즘에 의해 구한 자승기와 제 3 장의 누산방법에 의해 구한 역원 발생 회로를 $GF(2^2)$ - $GF(2^5)$에 대해 PLA로 회로 실현하면 다음 그림과 같다.

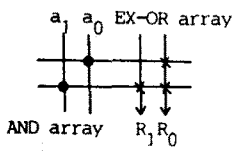


그림 6.1 $GF(2^2)$의 자승기 및 역원발생회로

Fig 6.1 Squaring and inverse generating circuits for $GF(2^2)$

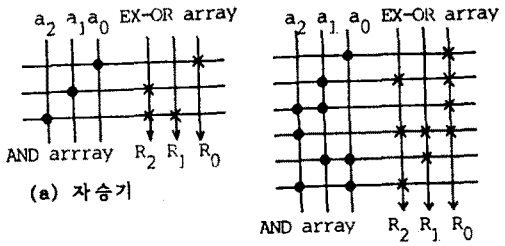
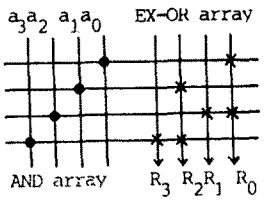


그림 6.2 $GF(2^3)$의 자승기 및 역원발생회로

Fig 6.2 Squaring and inverse generating circuits for $GF(2^3)$



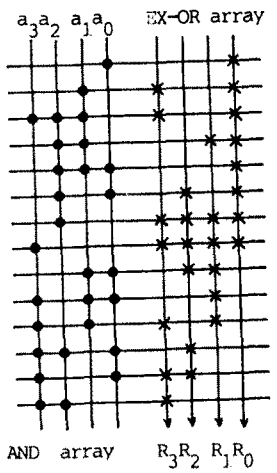
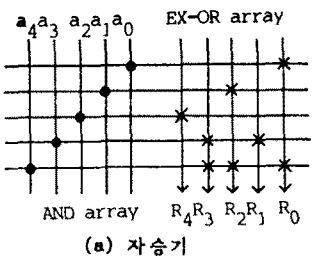
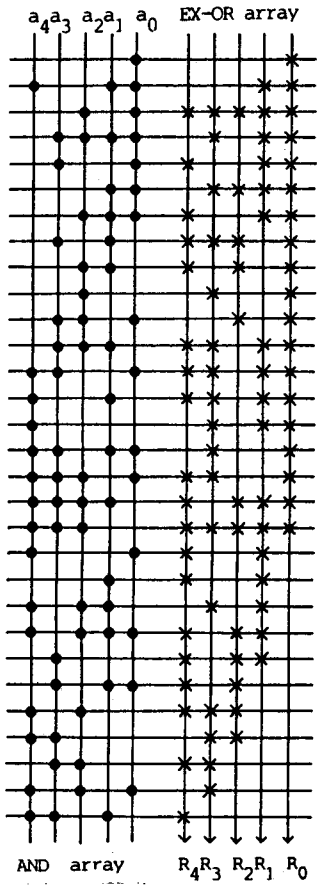


그림 6.3 $GF(2^4)$의 자승기 및 역원발생회로

Fig 6.3 Squaring and inverse generating circuits for $GF(2^4)$





(b) 역원발생회로

그림 6.4 GF(2^5)의 자승기 및 역원발생회로

Fig 6.4 Squaring and inverse generating circuits for GF(2^5)

7. 결 론

GF(2^m) 상의 임의의 한 원소를 $A=\sum_{i=0}^{m-1} a_i\alpha^i$ 로 표시하여 이 원소의 누승을 자승 알고리즘을 바탕으로 구하였다. 여기에 쓰인 자승은 $A^2=\sum_{i=0}^{m-1} P_i$ 로서 Pi 는 i가 짝수일 때 $a_{i/2}$ 이고, i가 홀수일 때 0 이 되며 기약다항식을 이용 m 보다 낮은 차수의 다항식으로 변환하면 되므로, 계산과정이 거의 없이 직접 결과를 산출할 수 있는 장점이 있다. 구한 결과는 GF(2^m) 상에 정의된 어떤 Galois 스위칭 함수라도 이의 회로 실현에 적용할 수 있고, A의 역원도 누승을 통해 얻을 수 있다. 여기서 구한 역원은 그대로 계산에 적용할 수 있는 것이다.

또한 누승중 2^m-1승은 영원이 아닌 경우는 1이 명백하지만 여기서는 영원까지 포함한 임의의 원소의 누승을 구하였으므로 상수항만의 결과를 얻었는데 이는 다항식의 모든 계수의 OR 임을 알았다.

m 이 커질수록 회로가 복잡하지만 NOT 게이트는 전혀 사용하지 않고 구성할 수 있었다.

참고 문헌

1. 성현경, 강성수,김홍수, "Bit code 연산에 의한 GF(2) 상의 승산기 구성," 대한전자공학회 창립 40주년 기념 학술대회 논문집, Vol.9,No.2,1986.
2. Charles C.Wang,T.K.Truong,Howard M.Shao,L.J. Deutch,J.K.Omura and I.S.Reed,"VLSI Architecture for Computing Multiplications and Inverses in GF(2)," IEEE Trans.Comput.,Vol.c-34, pp.709-717, Aug.1985.
3. C.S.Yeh,I.S.Reed and T.K.Truong,"Systolic Multipliers for Finite Fields GF(2), "IEEE Trans.Comput.,Vol.c-33,pp.357-360,Apr.1984.
4. B.A.Laws and C.K.Rushforth,"A Cellular Array Multiplier GF(2)," IEEE Trans.Comput.,short notes,pp.1573-1578,Dec.1971.