GF(2^m)상의 승산기 구성에 관한 연구

○원 동 호* 김 명 찬**
성균관대학교 정보공학과* 성균관대학교 전자공학과**

A study on the multiplier for finite field GF(2^m)

D.H.Won B.C.Kim.
Dept. of Information Eng. Dept. of Electronic Eng.
Sung Kyun Kwan University

ABSTRACT

Finite field arithmetic logic is central in the implementation of Reed-Solomon coders and in some cryptographic algorithms.

There is a need for good multiplication and basis conversion algorithms.

In this paper, a new multiplication circuit is developed for the finite field GF(2^m) based on a conventional basis.

It is composed of AND gates and EXCLUSIVE-OR gates and is regular, simple, expandable and therefore, naturally suitable for VLSI implementations.

1. 서 론

최근 통신 분야에서는 현대 대수학의 정리와 기술들이 널리 이용되고 있다. 특히 유한체는 에러 검출 및 정정용 블럭 부호와 비밀 통신의 암호화, 복호화에 많이 사용됨에 따라 그 가산, 승산, 역수 계산, 멱수 계산 등의 간단한 계산 알고리즘 개발과 함께 계산회로 구성 방법이 요구되고 있다.[1,2]

유한체 GF(2^m)은 2^m개의 원소를 가지는 집합으로 회로 응용시, m비트 바이너리로 집합의 각 원소를 표기할 수 있어 에러검출 및 정정부호와 비밀통신의 암호화, 복호화 회로에 가장 널리 사용되고 있다. Reed-Solomon 부호의 부호기와 복호기, BCH 부호의 복호기, 비밀 통신에서 평문의 암호화, 복호화 등에 GF(2^m) 상의 연산이 이용되고 있다.[1,2,3,4]

Yeh, Reed 와 Truong 은 GF(2^m)상의 원소를 관용 기저(Conventional basis)로 표시하여 VLSI 화가 가능한 승산기를 구성하였으며, Massey, Omura 는 GF(2^m) 상의 원소를 정규 기저(Normal basis)로 표현하는 방법을 제안하여 그에 적당한 승산기를 구성하였다.[5,6] 정규기저로 표시된 원소의 승산은 비교적 VLSI 화에 용이하나 임의의 선택된 기약 다항식으로 구성된 승산 회로는 다른 기약 다항식의 근으로 표시된 원소 사이에 승산이 불가능하며, 정규 기저를 가지는 기약 다항식 선정의 어려운 단점이 있다.

본 연구에서는 관용 기저로 원소를 표시하여 임의의 기약 다항식에서도 승산이 가능한 보다 간단한 승산기를 제안하였으며 정규 기저로 표시된 GF(2^m) 상의 원소를 관용 기저로 변환하는 회로를 구성하였다.

2. Galois Field

2-1. 유한체

실수 전체의 집합은 1) 사칙연산 2) 대소관계 3) 연속성의 3가지 성질을 가지고 있으며 이 중 사칙연산의 성질을 정리한 것이 다음의 7가지 공리이다.[1,2]

2개 이상의 원소를 가지는 집합 F가 공리 F1 ~ F7을 만족할 때 체(Field)라고 부른다.

F1, 임의의 $x,y \in F$일때 가산과 승산이 정의 된다.

F2, 결합법칙 ; 임의의 $x,y,z \in F$일때 다음이 성립한다.

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

F3, 교환법칙 ; 임의의 $x,y \in F$일때 다음이 성립한다.

$$x+y=y+x, \quad x \cdot y = y \cdot x$$

F4, 분배법칙 ; 임의의 $x,y,z \in F$일때 다음이 성립한다.

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

F5, 0원의 존재 ; 임의의 $x \in F$일때 $x+0=x$를 만족하는 0원이 단 하나 존재한다.

F6, 단위원의 존재 ; 임의의 $x \in F$일때 $x \cdot 1 = x$를 만족하는 원소 $1 \in F$가 단 하나 존

재한다.

F7. 역원의 존재 : 임의의 $x \in F$ 임에 $x + y = 0$ 되는 $y \in F$가 단 하나 존재하고 $x \cdot z = 1$ 되는 $z \in F$가 단 하나 존재한다.

실수 전체는 위의 공리를 만족하므로 체이지만 무한집합이다. 유한 집합으로 위의 공리를 만족하는 것을 유한체 혹은 Galois Field라 하며 GF(p)로 표시한다. 유한체는 실수의 사칙연산 성질만 가지고 있으며 그 연속성이나 대소성 성질은 가지고 있지 않다. 유한체의 구체적인 예로는 GF(p)의 p가 소수로 mod p로 연이지는 $F = \{0, 1, 2, \cdots\cdots, p-1\}$가 있다. $p = 5$인 GF(5)의 원소 사이의 가산 및 승산은 표 1과 표 2와 같다.

표 1. GF(5)의 가산 $x + y$

Table 1. Addition for GF(5), $x + y$

y \ x	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)의 승산 $x \cdot y$

Table 2. Multiplication for GF(5), $x \cdot y$

y \ x	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

한편 p가 소수이고 m이 양의 정수인데 $GF(p^m)$도 유한체를 이루며 이를 기본체 GF(p)의 확대 Galois Field라고 한다. 그 확대체의 원소는 GF(p)상에서 기약인 다항식의 근으로 표현할 수 있다. 특히 $p = 2$인 경우 $GF(2^m)$의 원소는 2치 값을 나타내는 m비트 바이너리로 표시할 수 있어 편리하다.

이러한 유한체, Galois Field GF(p), $GF(p^m)$은 다음 성질을 가지고 있다.

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

$$px = x + x + \cdots\cdots + x \equiv 0 \quad (1)$$

2) GF(p), $GF(p^m)$의 임의의 원소 x에 대하여 다음식이 성립한다.

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

$$x^{p^m-1} \equiv 1 \quad (2')$$

(Fermat 정리)

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

$$(x + y)^p \equiv x^p + y^p \quad (3)$$

$$(x + y)^{p^m} \equiv x^{p^m} + y^{p^m} \quad (3')$$

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

$$x^i \cdot x^j \equiv x^{i+j} (\text{mod } p-1) \quad (4)$$

$$x^i \cdot x^j \equiv x^{i+j} (\text{mod } p^m - 1) \quad (4')$$

$GF(p^m)$의 원소를 관용기지와 정규 기지로 표기하고 그 상호 변환 회로를 생각해 보자.

2-2. 기지에 의한 $GF(p^m)$ 상의 원소 표현

$GF(p^m)$상의 원소는 p^m개로 GF(p) 상의 기약다항식 $P(x) = x^m + f_{m-1}x^{m-1} + \cdots\cdots + f_0$의 근으로 표시할 수 있으며 각 원소는 P개의 상태를 가지는 m디지트로 나타낼 수 있다. 이 방법을 기지에 의한 $GF(p^m)$상의 원소표현이라 하며 또 기지의 계수로 원소를 나타내는 방법을 원소의 벡터표시라 한다. 기지에 의한 원소 표시에는 관용 기지와 정규 기지가 있으며 각각 식(5)와 식(6)으로 표시된다.

$$F(\alpha) = \sum_{i=0}^{m-1} C_i \alpha^i \quad (5)$$

$$F(\alpha) = \sum_{i=0}^{m-1} \eta_i \alpha^{p^i} \quad (6)$$

단 $F(\alpha) \in GF(p^m)$

$C_i, \eta_i \in GF(p)$

본 연구에서는 바이너리로 표현이 가능한 $GF(2^m)$중에 계산을 간단하게 하기 위해 $m = 3$인 경우의 기지를 구하고, 관용 기지와 정규 기지의 변환 회로를 구성한다. $GF(2^3)$의 기약 다항식으로

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

을 선택하고 각 원소를 구하면 다음과 같다.

$\alpha^* = 0$ $\alpha^2 = \alpha^2$ $\alpha^5 \equiv \alpha + 1$

$\alpha^0 = 1$ $\alpha^3 \equiv \alpha^2 + 1$ $\alpha^6 \equiv \alpha^2 + \alpha$

$\alpha = \alpha$ $\alpha^4 \equiv \alpha^2 + \alpha + 1$ $\alpha^7 \equiv 1 \equiv \alpha^0$

단 α는 기약다항식 $P(x) = 0$의 근이다.

위의 GF(2^3) 원소를 관용 기저와 정규 기저로 표시한 것이 표 3과 표 4이다.

표 3. 관용기저에 의한 GF(2^3)상의 원소 표현

Table 3. Elements represented a conventional basis for GF(2^3)

	α^0 α^1 α^2	Vector 표시
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	α^2+1	1 0 1
α^4	$\alpha^2+\alpha+1$	1 1 1
α^5	$\alpha+1$	1 1 0
α^6	$\alpha^2+\alpha$	0 1 1

표 4. 정규 기저에 의한 GF(2^3)상의 원소표현

Table 4. Elements represented a normal basis for GF(2^3)

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

관용 기저와 정규 기저로 GF(2^m)상의 원소를 표시한 식이 식(7), (8)이다. 같은 원소를 관용 기저와 정규 기저로 표현하였으므로 기저를 상호 변환할 수 있다.

$$F(\alpha)=\sum_{i=0}^{m-1} C_i\alpha^i \qquad (7)$$

$$F(\alpha)=\sum_{i=0}^{m-1} n_i\alpha^{2^i} \qquad (8)$$

$$F(\alpha)\in GF(2^m)$$

$$C_i,\ n_i\in GF(2)$$

변환 과정은 행렬로 나타낼 수 있다. 즉 관용 기저의 계수 $C_0, C_1 \cdots\cdots C_{m-1}$은 정규 기저의 계수 $n_0, n_1 \cdots\cdots n_{m-1}$으로부터 구할 수 있다.

$$\begin{bmatrix} C_0 \\ C_1 \\ \vdots \\ C_{m-2} \\ C_{m-1} \end{bmatrix} = \begin{bmatrix} S_{11} & S_{12} & \cdots\cdots & S_{1m} \\ S_{21} & S_{22} & \cdots\cdots & S_{2m} \\ & & \ddots & \\ S_{m1} & S_{m2} & & S_{mm} \end{bmatrix} \begin{bmatrix} n_0 \\ n_1 \\ \vdots \\ n_{m-2} \\ n_{m-1} \end{bmatrix} \qquad (9)$$

$$C = SN \qquad (10)$$

위의 행렬 S는 m차 정방 행렬로 정규 기저를 관용 기저로 변환하는 변환 행렬이다. 행렬 S의 역행렬을 구하면 관용 기저로부터 정규 기저를 얻을 수 있다.

$$N = S^{-1}C \qquad (11)$$

일례로 GF(2^3)의 변환 행렬 S는 식(12)와 같다.

$$S=\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \qquad (12)$$

이러한 기저 변환 회로는 그림 1과 같이 PLA로 간단히 구성할 수 있다.

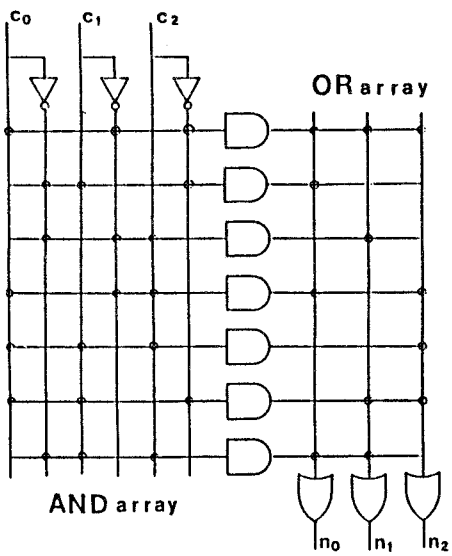

그림 1. GF(2^3)상의 기저 변환 회로

Fig 1. a basis conversion circuit for GF(2^3)

3. 연 산 회 로

본 절에서는 관용 기저로 표현된 GF(2^m) 상의 원소의 가산 및 승산 회로를 신형 논리를 근거로

구성한다.

3-1. 가산회로

가산 회로는 전용 기저나 정규 기저로 표시한 GF(2^m) 상의 원소에 대하여 공히 동일한 방법으로 구성할 수 있다.

여기서는 전용 기저로 표시된 경우의 가산 회로를 구성하도록 한다. GF(2^m) 상의 피가산 원소를 식(13), 가산 원소를 식(14)로 표시하고 두 원소의 가산후의 원소를 식(15)로 나타내면 계수 간의 관계식은 식(16)과 같다.

$$A(x) = a_0 + a_1x + a_2x^2 + \cdots\cdots + a_{m-1}x^{m-1} \quad (13)$$

$$B(x) = b_0 + b_1x + b_2x^2 + \cdots\cdots + b_{m-1}x^{m-1} \quad (14)$$

$$Z(x) = z_0 + z_1x + z_2x^2 + \cdots\cdots + z_{m-1}x^{m-1} \quad (15)$$

$$Z_i = a_i \oplus b_i \quad (16)$$

단 $A(x), B(x), Z(x) \in GF(2^m)$

$a_i, b_i, z_i \in GF(2)$

피가산 원소와 가산 원소의 x^i의 계수가 GF(2) 상의 원소이므로 x의 동일한 차수의 계수 사이에 합은 mod 2를 하여야 한다. 따라서 가산 후의 원소의 계수는 동일 차수 x^i의 계수의 배타적 논리합으로 표시된다. GF(2^m) 상의 가산회로는 그림 2와 같다.

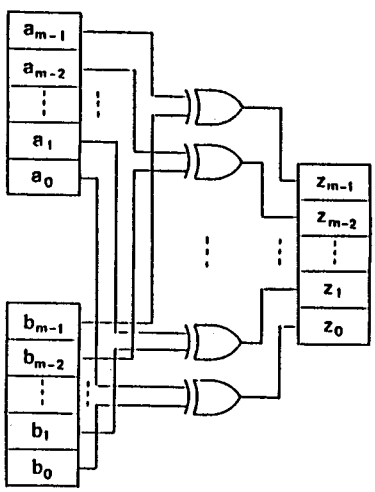

그림 2. GF(2^m) 상의 가산기

Fig 2. An adder for GF(2^m)

3-2. 승산회로

전용 기저로 표시된 피승산 원소의 승산 원소를 표시한 식(13),(14)를 승산 과정을 위기쉽게 하기 위해 식(17),(18)로 바꾸어 표기하자.

$$A(x) = \sum_{n=0}^{m-1} a_n x^n \quad (17)$$

$$B(x) = \sum_{k=0}^{m-1} b_k x^k \quad (18)$$

$A(x)$와 $B(x)$의 승산값을 $Y(x)$라 하면 그 값은 식(19)와 같이 표현된다.

$$\begin{aligned} Y(x) &= A(x)B(x) \\ &= \left(\sum_{n=0}^{m-1} a_n x^n\right)\left(\sum_{k=0}^{m-1} b_k x^k\right) \\ &= \sum_{k=0}^{m-1} (b_k A(x))x^k \\ &= P^{(m-1,m-1)} \end{aligned} \quad (19)$$

단 $P^{(i,0)}$는 $A(x)$에 $b_i(x^i)$를 곱하여 i번 left shift한 부분합이며 $P^{(m-1,j)}$는 j번째 right shift한 값을 $x^{(m-1-j)}P(x)$로 mod한 값이다. 이 과정을 회로화 하기 위하여 다음과 같이 승산부와 mod부로 나누어 생각할 수 있다.

수식에서 $\mathrm{mod}(x^{(m-1-j)}P(x))$는 x의 차수를 낮추어 m차 미만으로 줄이기 위한 것이며 기약다항식 $P(x)$가 모닉(monic) 다항식이므로 $x^{(m-1-j)}P(x)$도 모닉다항식이므로 다음단에 직접 대입시키는 것으로 생각할 수 있다.

먼저 승산과정을 살펴보자.

$$\begin{aligned} P^{(0,0)} &= b_0A(x) \\ P^{(1,0)} &= b_1xA(x) + b_0A(x) = b_1xA(x) + P^{(0,0)} \\ P^{(2,0)} &= b_2x^2A(x) + b_1xA(x) + b_0A(x) \\ &= b_2x^2A(x) + P^{(1,0)} \\ &\vdots \\ P^{(m-1,0)} &= b_{m-1}x^{m-1}A(x) + P^{(m-2,0)} \end{aligned} \quad (20)$$

(20)식은 x의 $2(m-1)$차의 다항식이므로 이를 mod부에 입력시키기 $m-1$차로 만들어야 한다. 이 과정은 다음과 같다.

$$\begin{aligned} P^{(m-1,1)} &= P^{(m-1,0)} \cdot \mathrm{mod}(x^{(m-1-1)}P(x)) \\ P^{(m-1,2)} &= P^{(m-1,1)} \cdot \mathrm{mod}(x^{(m-1-2)}P(x)) \\ &\vdots \\ P^{(m-1,m-1)} &= P^{(m-1,m-2)} \cdot \mathrm{mod}\,P(x) \end{aligned}$$

인발식으로 정리하면

$$P^{(m-1,m-1)} = ((((P^{(m-1,0)} \cdot \mathrm{mod}(x^{(m-1-1)}P(x))) \cdot \mathrm{mod}(x^{(m-1-2)}P(x))) \cdots\cdots)\ \mathrm{mod}\,P(x) \quad (21)$$

이다.

$P^{(i,j)}$에서 i는 $0\sim(m-1)$, j는 $1\sim(m-1)$이다.

식(21)은 $A(x)B(x)$인 $Y(x)$로 식(19)와 일치한다. 즉 $P^{(m-1,m-1)}\equiv A(x)B(x)$로 x의 최고 차수가 $m-1$인 관용 기저 표시의 $GF(2^m)$상의 원소가 된다. 이러한 과정을 회로화 한것이 그림 3이다.

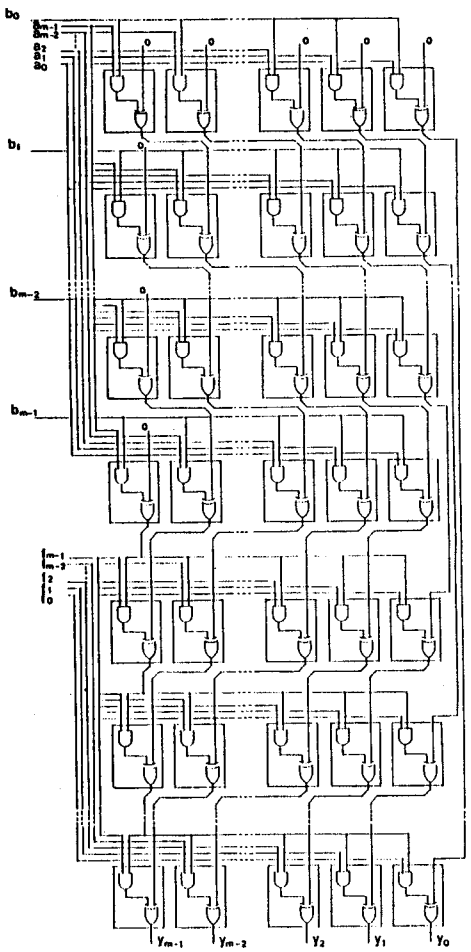

그림 3. $GF(2^m)$상의 승산기

Fig 3. A multiplier for $GF(2^m)$

4. 결 론

본 연구에서는 $GF(2^m)$상의 원소를 관용 기저로 표시하고 그 원소 사이의 승산을 용이하게 실행할수 있는 회로를 새로이 제안하였다. 이 승산기는 임의의 기약 다항식에도 그 승산이 가능하며 승산회로 각 Cell 을 AND gate와 Exclusive OR gate 각각 하나로 구성할 수 있어 회로가 간단하다.

따라서 VLSI 화가 용이하며 one-chip으로 구성할 경우에도 $m\geq r$에 대한 $GF(2^r)$ 승산이 가능하여 보다 보편적으로 사용할 수 있다. 또 관용기저와 정규기저 사이에 기저 변환 회로도 구성하였다. 이것은 정규 기저에서의 연산결과를 관용기저 연산회로에 입력시킬때 편리하게 사용될 수 있으리라 생각된다. 추후 관용 기저 상에서의 고속 역수 계산회로를 구성하는 것이 연구과제라 생각한다.

참 고 문 헌

1. R.E.Blahut, " Theory and Practice of Error Control Codes," Addison-weslely Publishing company, 1983.

2. P.J.Macwilliams and N.J.A.Skoane, " The Theory of Error-Correcting Codes ",Amsterdam : North-Holland 1978.

3. T.C.Bartee and D.I.Schneider, " Computation with finite field ", Inform. Contr, Vol.6, pp.79-98, Mar. 1963.

4. B.A.Laws and C.K.Rushforth, " A cellular-array multiplier for $GF(2^m)$ ", IEEE Trans : Comput., Vol. C-20, pp.1573-1578, Dec. 1971.

5. C.S.Yeh, Irving S.Reed, T.K. Truong, " Systolic multipliers for finite field $GF(2^m)$ ", IEEE Trans: Comput., Vol. C-33, No. 4, pp.357-360, 1984.

6. C.C.Wang, T.K.Truong, J.K.Omura, and Irving S. Reed, " VLSI Architectures for computing multiplications and inverse in $GF(2^m)$ ", IEEE Trans: Comput., Vol. C-34, No. 8, pp.709~716, August 1985.