$GF(3^m)$상에서 모든 항의 계수가 존재하는 기약다항식의 승산기 설계

이광희, 황종학, 박승용, 김흥수
인하대학교
전화 : 032-860-7413 / 핸드폰 : 016-283-3660

Design of a Multiplier for Irreducible Polynomial that all Coefficient over $GF(3^m)$

Kwang-Hee Lee, Jong-Hak Hwang, Seung-Yong Park, Hung-Soo Kim
Dept. of Electronic Engineering, Inha University
E-mail : g2011096@inhavision.inha.ac.kr

Abstract

In this paper, we proposed a multiplicative algorithm for two polynomials in existence coefficients over finite field $GF(3^m)$. Using the proposed multiplicative algorithm, we constructed the multiplier of modular architecture with parallel in-output. The proposed multiplier is composed of $(m+1)^2$ identical cells, each cell consists of single mod(3) additional gate and single mod(3) multiplicative gate. Proposed multiplier need single mod(3) multiplicative gate delay time and m mod(3) additional gate delay time not clock. Also, the proposed architecture is simple, regular and has the property of modularity, therefore well-suited for VLSI implementation.

I. 서론

유한체(Galois field)는 오류정정부호, 디지털 통신의 암호화 및 해독화를 요하는 보안 등에 많이 응용되고 있다. 이들 중 오류정정부호는 유한체 $GF(2^m)$상의 연산에서 실제로 부호기 및 복호기 설계시 전체시스템의 규모와 성능에 절대적인 영향을 미치므로 회로경로의 연결, 시스템 구조의 복잡성과 동시성 등의 문제점을 개선하기 위한 연구가 진행되어 왔다.[1] 유한체의 연산은 가산, 승산, 멱산, 제산 등인데, 가산은 매우 간단하여 유한체의 원소(field elements)들이 다항식 형태로 표현되는 경우 매우 간단한 회로로 수행될 수 있다.

본 논문에서는 C.Y. Lee 등[4]이 제시한 AOP를 기반으로 하는 유한체 $GF(2^m)$상에서의 승산 알고리즘을 $GF(3^m)$상으로 확장하여 모든 항이 존재하는 원시 기약다항식에 대한 승산 알고리즘을 제안하였다. 제안된 승산 알고리즘을 이용하여 병렬 입/출력 모듈구조의 승산기를 구성하였으며, 제안된 승산기는 $(m+1)^2$개의 동일한 셀로 구성되었으며, 1개의 셀은 1개의 2 입력 mod(3) 가산 게이트와 1개의 2 입력 mod(3) 승산 게이트로 구성되었다.

II. 유한체 $GF(3^m)$상의 알고리즘

본 절에서는 유한체 $GF(3^m)$상에서 모든 항의 계수가 존재하는 기약다항식의 두 원소에 대한 승산 알고리즘을 제안하였다.

경우 1. $GF(3^m)$상에서 m이 홀수인 경우

$GF(3^m)$은 m이 양의 정수인 3^m개의 원소를 갖는다. $GF(3^m)$상에서 모든 항이 존재하는 기약다항식은 식(1)과 같이 표현된다.

$$F(x)= f_0+f_1x+f_2x^2+\cdots+f_{m-1}x^{m-1}+2x^m \quad (1)$$

여기서 $F(x)$는 최고 차수가 m이고, $f_i \in GF(3)$이며, $0 \le i$

$\leq m-1$이다.

식(1)에서 최고차 항의 계수 2는 $GF(3^m)$상에서 식(3)을 성립시키기 위한 계수이다. α가 식(1)의 근이라고 하면, $F(\alpha)=0$이므로

$$F(\alpha) = f_0+f_1\alpha+f_2\alpha^2+\cdots+f_{m-1}\alpha^{m-1}+2\alpha^m=0 \quad (2)$$

로 표현된다. 식(2)으로부터 α^m은 식(3)과 같다.

$$\begin{aligned} -2\alpha^m &= f_0+f_1\alpha+f_2\alpha^2+\cdots+f_{m-1}\alpha^{m-1} \\ \alpha^m &= f_0+f_1\alpha+f_2\alpha^2+\cdots+f_{m-1}\alpha^{m-1} \end{aligned} \quad (3)$$

여기서, $f_i \in GF(3)$이다.

식(3)과 같이 유한체 $GF(3^m)$상의 각 원소들은 차수가 $m-1$이하의 α의 다항식으로 표현된다. 두 다항식을 승산 하였을 때, α^m보다 큰 차수들에 대하여 알아보기 위해 먼저 α^{m+1}에 대한 식을 구하면 식(4)과 같다.

$$\begin{aligned} \alpha^{m+1} &= \alpha^m \cdot \alpha \\ &= f_0\alpha+f_1\alpha^2+f_2\alpha^3+\cdots+f_{m-2}\alpha^{m-1}+f_{m-1}\alpha^m \end{aligned} \quad (4)$$

식(4)에 식(3)을 대입하면 식(5)과 같다.

$$\begin{aligned} \alpha^{m+1} &= f_0\alpha+f_1\alpha^2+f_2\alpha^3+\cdots+f_{m-2}\alpha^{m-1} \\ &\quad +f_{m-1}(f_0+f_1\alpha+f_2\alpha^2+\cdots+f_{m-1}\alpha^{m-1}) \\ &= f_0f_{m-1}+(f_0+f_1f_{m-1})\alpha+(f_1+f_2f_{m-1})\alpha^2 \\ &\quad +\cdots+(f_{m-2}+f_{m-1}f_{m-1})\alpha^{m-1} \end{aligned} \quad (5)$$

식(5)에서 $\alpha^{m+1}=1$이 되기 위하여 식(6)이 성립하여야 한다.

$$\begin{aligned} &f_0f_{m-1}+(f_0+f_1f_{m-1})\alpha+(f_1+f_2f_{m-1})\alpha^2+\cdots \\ &+(f_{m-2}+f_{m-1}f_{m-1})\alpha^{m-1} = 1 \end{aligned} \quad (6)$$

따라서, 식(6)을 만족하기 위한 각 항의 계수들을 나타내면 식(7)과 같다.

$$f_0f_{m-1}=1 \quad (7a)$$
$$f_0+f_1f_{m-1}=0 \quad (7b)$$
$$f_1+f_2f_{m-1}=0 \quad (7c)$$
$$\vdots$$
$$f_{m-2}+f_{m-1}f_{m-1}=0 \quad (7d)$$

식 (7)이 성립되기 위한 $f_i \in GF(3)$인 f_0부터 f_{m-1}까지의 계수들을 구하기 위해 다음의 과정을 이용한다.

[단계1] 식(7a)에서 $f_0f_{m-1}=1$이 만족되기 위해서 $f_0=1$, $f_{m-1}=1$이어야 한다.

[단계2] 식(7b)에서 $f_0+f_1f_{m-1}=0$이 되기 위해서 [단계 1]에서 구한 $f_0=1$, $f_{m-1}=1$을 대입하면 $f_1=2$이어야 한다.

[단계3] 식(7c)에서 $f_1+f_2f_{m-1}=0$이 되기 위해서 [단계 2]에서 구한 $f_1=2$를 대입하면 $f_2=1$이어야 한다.

[단계4] 식(7d)에서 $f_{m-2}+f_{m-1}f_{m-1}=0$이 되기 위해서[단계 1]에서 구한 $f_{m-1}=1$을 대입하면 $f_{m-2}=2$ 이어야 한다.

[단계1]~[단계4]에 의해서 α^{m+1}의 식(5)은 상수 항 f_0f_{m-1}만 1이 되고, 나머지 계수들은 모두 0이 되므로 α^{m+1}은 식(8)과 같이 된다.

$$\alpha^{m+1} = \alpha^m \cdot \alpha = 1 \quad (8)$$

식(8)을 이용하여 α^{m+2}, α^{m+3}, …, α^{m+i}, …, α^{2m}을 구하면 다음의 결과를 얻을 수 있다.

$$\alpha^{m+2} = \alpha^{m+1} \cdot \alpha = \alpha \quad (9a)$$
$$\alpha^{m+3} = \alpha^{m+2} \cdot \alpha = \alpha^2 \quad (9b)$$
$$\vdots$$
$$\alpha^{m+i} = \alpha^{i-1} \quad (9c)$$
$$\vdots$$
$$\alpha^{2m} = \alpha^{m-1} \quad (9d)$$

α가 유한체 $GF(3^m)$상에서 m차 기약 다항식의 근이라 할 때, $GF(3^m)$상의 두 원소인 승산 다항식 A와 피승산 다항식 B는 식(10)과 같이 표현된다.

$$\begin{aligned} A &= a_0+a_1\alpha+a_2\alpha^2+\cdots+a_m\alpha^m \\ B &= b_0+b_1\alpha+b_2\alpha^2+\cdots+b_m\alpha^m \end{aligned} \quad (10)$$

여기서, a_i, $b_i \in GF(3)$이며, $0 \leq i \leq m$이다.

승산 알고리즘을 유도하기 위하여 다항식 A, B를 승산하면 식(11)과 같다.

$$\begin{aligned} A \cdot B &= (a_0+a_1\alpha+a_2\alpha^2+\cdots+a_m\alpha^m) \\ &\quad \cdot (b_0+b_1\alpha+b_2\alpha^2+\cdots+b_m\alpha^m) \\ &= \left(\sum_{i=0}^{m} a_i\alpha^i\right) \cdot \left(\sum_{i=0}^{m} b_i\alpha^i\right) \end{aligned} \quad (11)$$

두 다항식의 승산식인 식(11)을 D로 놓으면, 식(12)과 같이 표현된다.

$$\begin{aligned} D &= d_0+d_1\alpha+d_2\alpha^2+\cdots+d_{2m}\alpha^{2m} \\ &= \sum_{i=0}^{2m} d_i\alpha^i = \sum_{i=0}^{m} d_i\alpha^i + \sum_{i=m+1}^{2m} d_i\alpha^i \end{aligned} \quad (12)$$

식(12)의 두 번째 항 $\sum_{i=m+1}^{2m} d_i\alpha^i$ 는 식(9c)을 이용하여 식(13)과 같이 표현할 수 있다.

$$\begin{aligned} D &= \sum_{i=0}^{m} d_i\alpha^i + \sum_{i=0}^{m-1} d_{m+i+1}\alpha^i \\ &= \sum_{i=0}^{m-1} d_i\alpha^i + d_m\alpha^m + \sum_{i=0}^{m-1} d_{m+i+1}\alpha^i \\ &= \sum_{i=0}^{m-1} (d_i+d_{m+i+1})\alpha^i + d_m\alpha^m \end{aligned} \quad (13)$$

식(13)에서 $d_i+d_{m+i+1}=D_i$, $d_m=D_m$이라 놓으면 식(14)과 같이 표현된다.

$$D = \sum_{i=0}^{m-1} D_i\alpha_i + D_m\alpha^m = \sum_{i=0}^{m} D_i\alpha^i \quad (14)$$

경우 2. $GF(3^m)$상에서 m이 짝수인 경우

앞 절에서는 유한체 $GF(3^m)$상에서 m이 홀수일 경우에 대하여 모든 항의 계수가 존재하는 기약다항식에 대한 원소인 두 다항식의 승산 알고리즘을 제시하였다. 본 절에서는 $GF(3^m)$상에서 m이 짝수일 경우에 대한 승산 알고리즘을 제시한다.

두 다항식을 승산 하였을 때, α^m 보다 큰 차수들에 대해 알아보기 위하여 먼저 α^{m+1}에 대한 식을 구하면 식(5), (6)과 같다.

여기서 m이 짝수인 경우에 성립할 수 있는 조건을 구하기 위해$\alpha^{m+1}=2$로 놓으면, 식(6)은 식(15)과 같다.

$$f_0f_{m-1}+(f_0+f_1f_{m-1})\alpha+(f_1+f_2f_{m-1})\alpha^2 +\cdots+(f_{m-2}+f_{m-1}f_{m-1})\alpha^{m-1}=2 \quad (15)$$

따라서 식(15)을 만족하기 위하여 각 계수들은

$$f_0f_{m-1}=2 \quad (16a)$$
$$f_0+f_1f_{m-1}=0 \quad (16b)$$
$$f_1+f_2f_{m-1}=0 \quad (16c)$$
$$\vdots$$
$$f_{m-2}+f_{m-1}f_{m-1}=0 \quad (16d)$$

이 되어야 한다. 식(16)이 성립되기 위한 $f_i\in GF(3)$인 f_0부터 f_{m-1}까지의 계수들을 구하기 위해 다음의 과정을 이용한다.

[단계1] 식(16a)에서 f_0, $f_{m-1}=2$ 가 되기 위해서 $f_0=2$, $f_{m-1}=1$이어야한다.

[단계2] 식(16b)에서 $f_0+f_1f_{m-1}=0$이 되기 위해서 [단계1]에서 구한 $f_0=2$, $f_{m-1}=1$을 대입하면 $f_1=1$이어야 한다.

[단계3] 식(16c)에서 $f_1+f_2f_{m-1}=0$이 되기 위해서 [단계2]에서 구한 $f_1=1$을 대입하면 $f_2=2$이어야 한다.

[단계4] 같은 방법으로 대입하여 구하면 $f_{m-2}=2$ 이어야 한다.

[단계1]~[단계4]에 의해서 α^{m+1}의 식(15)은 상수 항 f_0f_{m-1}만 2이고, 나머지 계수들은 모두 0이 되어 α^{m+1}은 식(20)과 같이 된다.

$$\alpha^{m+1}=\alpha^m\cdot\alpha=2 \quad (17)$$

식(17)을 이용하여 α^{m+2}, α^{m+3}, $\cdots$, α^{m+i}, $\cdots$, α^{2m}을 구하면 다음의 결과를 얻을 수 있다.

$$\alpha^{m+2}=\alpha^{m+1}\cdot\alpha=2\alpha \quad (18a)$$
$$\alpha^{m+3}=\alpha^{m+2}\cdot\alpha=2\alpha^2 \quad (18b)$$
$$\vdots$$
$$\alpha^{m+i}=2\alpha^{i-1} \quad (18c)$$
$$\vdots$$
$$\alpha^{2m}=\alpha^{m-1} \quad (18d)$$

식(10)의 두 다항식의 승산식인 식(12)의 두 번째 항 $\sum_{i=m+1}^{2m} d_i\alpha^i$ 는 식(18c)을 이용하여 식(19)과 같이 표현할 수 있다.

$$\begin{aligned} D &= \sum_{i=0}^{m} d_i\alpha^i+\sum_{i=0}^{m-1}2d_{m+i+1}\alpha^i \\ &= \sum_{i=0}^{m-1} d_i\alpha^i+d_m\alpha^m+\sum_{i=0}^{m-1}2d_{m+i+1}\alpha^i \\ &= \sum_{i=0}^{m-1}(d_i+2d_{m+i+1})\alpha^i+d_m\alpha^m \end{aligned} \quad (19)$$

식(19)에서 $d_i+2d_{m+i+1}=D_i$, $d_m=D_m$이라 놓으면 식(20)과 같이 표현된다.

$$D=\sum_{i=0}^{m-1}D_i+D_m\alpha^m=\sum_{i=0}^{m}D_i\alpha^i \quad (20)$$

III. $GF(3^m)$상에서의 승산기 구성

본 절에서는 $GF(3^m)$상에서의 승산 알고리즘에 대한 승산기를 구성한다. $GF(3^m)$상에서 승산기는 mod(3) 게이트로 변경하여 나타내면 그림 1.과 같이 나타낼 수 있다.

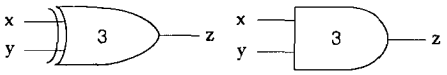

그림 1. mod(3) 가산/승산 게이트

그림 1.을 이용하여 $GF(3^m)$상의 승산기에서 m이 홀수일 때 사용되는 기본모듈 그림 2.에 나타내었다. 3치 승산에 사용된 셀에서 mod(3) 가산 게이트와 mod(3) 승산 게이트는 두 원소를 mod(3) 가산 및 승산하기 위한 게이트를 말하며, a_i와 b_i는 각각 승산 다항식 A와 피승산 다항식 B의 계수를 의미한다.

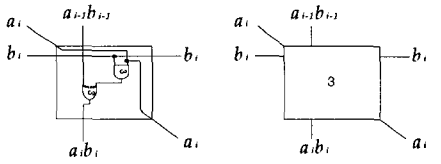

그림 2. $GF(3^m)$상에서 m이 홀수인 승산기에 사용된 기본 셀

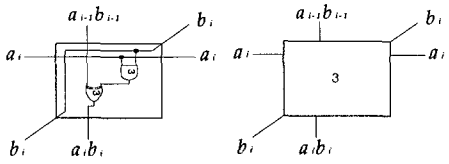

그림 3. $GF(3^m)$상에서 m이 짝수인 승산기에 사용된 기본 셀

또한, 식(19)의 두 번째 항에서 나타나는 2를 포함하기 위해 $GF(3^m)$상에서 m이 짝수일 때 사용되는 기본 셀을 그림 3.에 다르게 나타내었다.

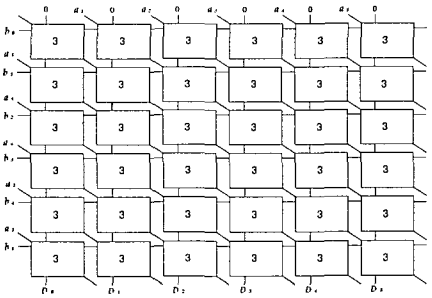

그림 4. $GF(3^5)$상의 제안된 승산기

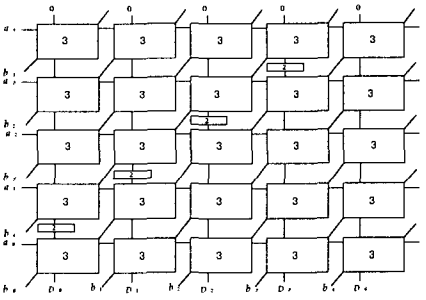

그림 7. $GF(3^4)$상의 제안된 승산기

그림 4.는 $GF(3^m)$상에서 m이 홀수인 승산기 구성도에서 $GF(3^5)$상에서의 승산기 구성도를 예로 보였다. 그림 4.에서 $a_0 \sim a_5$는 승산 다항식 A에 대한 각 항의 계수를 의미하며, $b_0 \sim b_5$는 피승산 다항식 B에 대한 각 항의 계수를 의미한다. 최 상단에 위치한 셀에 입력되는 0은 $a_{i-1}b_{i-1}$에 대한 초기값이다. 최 하단의 $D_0 \sim D_5$는 승산 결과에 대한 각 항의 계수이다. 또한 그림 5.는 $GF(3^m)$상에서 m이 짝수인 승산기 구성도에서 $GF(3^4)$상에서의 승산기 구성도를 예로 보였다. 승산기에서 4개의 "2"블럭은 m이 짝수일 경우에 대한 승산 알고리즘을 구현할 때 식(19)의 두 번째 항에서 나타나는 "2"를 나타낸다.

IV. 결 론

본 논문에서는 유한체 $GF(3^m)$상에서 모든 항이 존재하는 원시 기약 다항식에 대한 승산 알고리즘을 제안하였으며, 제안된 승산 알고리즘을 이용하여 병렬 입/출력 모듈구조의 승산기를 구성하였다.

제시된 승산기는 $(m+1)^2$개의 동일한 셀로 구성되었으며, 1개의 셀은 1개의 mod(3) 가산 게이트와 1개의 mod(3) 승산 게이트로 구성되었다.

제안된 승산기는 기억소자를 사용하지 않으므로 클럭이 필요하지 않고, m개의 mod(3) 가산 게이트 지연시간과 1개의 mod(3) 승산 게이트 소자 지연시간 만을 필요로 한다.

표 5 기존 승산기와의 비교

항목 \ 승산기		Yeh[2]	Wei[3]	Lee[4]	본 논문
Function		AB+C	AB^2+C	AB+C	AB+C
셀당 사용된 게이트 수	2 입력 AND	2	3	1	1
	2 입력 XOR	2	1	1	1
	3 입력 XOR	0	1	0	0
	1 비트 latch	7	10	3	0
전체 게이트 수	2 입력 AND	$2m^2$	$3m^2$	$(m+1)^2$	$(m+1)^2$
	2 입력 XOR	$2m^2$	m^2	$(m+1)^2$	$(m+1)^2$
	3 입력 XOR	0	m^2	0	0
	1 비트 latch	$7m^2$	$10m^2$	$\approx 4(m+1)^2$	0
최소 클럭 주기		$T_A+T_X+2T_L$	$T_A+T_{3X}+2T_L$	T_A+T_X	T_A+T_X
지 연 시 간		3m	3m	m+1	m+1

또한, 기존 승산기와의 게이트 수를 비교한 표 1에서 본 논문의 승산기가 게이트수가 가장 적은 것으로 회로의 간단함을 알 수 있다. 따라서 제안된 승산기의 간단성, 규칙성 그리고 셀 배열에 의한 모듈성을 VLSI회로 실현에 적합할 것이다. 향후 연구과제는 3치 게이트 회로를 구현하고 알고리즘에 따른 집적회로를 구현하는 것이다.

참고문헌

[1] S.L. Hurst, "Multiple-valued logic-its future," *IEEE Trans. Computers*, vol 30, pp. 1161-1179, Dec. 1984.

[2] C.S. Yeh, I.S. Reed, and T.K. Truong, "Systolic Multipliers for Finite Fields $GF(2^m)$," *IEEE Trans. Computers*, vol. 33, no. 4, pp. 357-360, Apr. 1984.

[3] S.W. Wei, "A Systolic Power-Sum Circuit for $GF(2^m)$," *IEEE Trans. Computers*, vol. 43, no. 2, pp. 226-229, Feb. 1994.

[4] C.Y. Lee, E.H. Lu, and J.Y. Lee, "Bit Parallel Systolic Multipliers for $GF(2^m)$ Fields Defined by All-One and Equally Spaced Polynomials," *IEEE Trans. Computers*, vol. 50, no. 5, pp. 385-392, May 2001.

[5] 황종학, 박승용, 신부식, 김홍수 "멀티플렉서를 이용한 $GF(2^m)$상의 승산기," *전자공학회 논문지*,제37권, SC편, 제7호, pp. 35-41, 2000년 7월.