유한체 $GF(3^m)$상에서 역원생성 알고리즘에 관한 연구

박춘명*

*충주대학교 전기.전자 및 정보공학부 컴퓨터공학과

A Study on the Inverse Element Generation Algorithm over $GF(3^m)$

Chun-Myoung Park*

*Dept. of Computer Engineering, School of EEIE, Chungju National University

E-mail : cmpark@cjnu.ac.kr

요 약

본 논문에서는 유한체 $GF(3^m)$상에서의 역원을 효과적으로 생성할 수 있는 알고리즘을 제안하였으며, 이를 바탕으로 역원생성기를 구성하는 방법에 대해 논의하였다. 제안한 역원 생성기는 승산기, 출력레지스터 군, 승산 및 세제곱 선택 게이트와 순차선택기, 세제곱처리부, 내림차순 생성부 등으로 구성된다. 제안한 역원알고리즘과 역원생성기는 회로설계의 단순성, 규칙성, 확장성 및 모듈화 기능을 갖는다.

ABSTRACT

This paper presents an algorithm for generating inverse element over finite fields $GF(3^m)$, and constructing method of inverse element generator based on inverse element generating algorithm. The method need to compute inverse of an element over $GF(3^m)$ which corresponds to a polynomial over $GF(3^m)$ with order less than equal to m-1. Here, the computation is based on multiplication, square and cube method derived from the mathematics properties over finite fields.

키워드

Finite fields, polynomial, inverse element,

I. 서 론

최근에 대부분의 디지털논리시스템과 컴퓨터시스템은 방대한 데이터를 처리와 높은 효율성을 요구하고 있다.[1-5] 이를 위해 유한체상에서 연산과 관련한 해석을 하여 그 효율성을 높이고 있다.[6]

본 논문에서는 유한체상에서의 고효율 역원생성 알고리즘과 이를 바탕으로 역원생성기를 구성하는 방법을 제안하였다.

본 논문의 구성은 다음과 같다. 2장에서는 유한체의 수학적 성질을 근간으로 승산, 스퀘어(square), 큐브(cube) 알고리즘을 제안하였다. 3장에서는 $GF(3^m)$상에서의 역원 생성 알고리즘에 대해 논의하였다. 그리고, 4장에서는 3장의 내용을 바탕으로 역원생성기를 구성하였다. 마지막 5장의 결론에서는 본 논문에서 제안한 역원생성 알고리즘과 역원생성기의 특징을 요약하였으며, 향 후 연구과제에 대해 논의하였다.

II. 유한체상의 승산, 스퀘어 승산 및 큐브 승산

2-1. 유한체의 수학적 성질

본 장에서는 본 논문을 전개하는데 필요한 유한체상에서의 중요한 수학적 성질[6]에 대해 논의한다. 이외의 수학적 성질은 참고문헌[7-11]을 참조 하였다. 유한체는 임의의 소수 P와 양의 정수 m으로 정의되며 $GF(P^m)$으로 표현한다. 일반적으로, 유한체는 5-tuple $\{S,+,\bullet,0,1\}$으로 구성된다, 여기서 S는 원소의 집합이고 +와 $\bullet$는 집합 S상에서의 이항연산이며 0과 1은 각각 가산과 승산에 있어서 identity 원소이다. 또한, 유한체는 기초체 GF(P)와 이의 확장인 확대체 $GF(P^m)$로 분류하며, 기초체 GF(p)의 원소의 개수는 $\{0,1,2, \ldots\ldots, P-1\}$이다. 여기서 P는 1보다 큰 소수이다.중요한 유한체상의 수학적 성질은 다음과 같다.

[MP1] $\alpha \in GF(P^m)$에 대해, $\alpha \neq 1$인 경우에 $\alpha^{\Psi}=\alpha$이

고 $\alpha^{\psi-1}=1$ ($\psi=P^m$)이다.

[MP2] α, $\beta \in GF(P^m)$와 임의의 양의 정수 m에 대해, $(\alpha \pm \beta)^\mu = \alpha^\mu \pm \beta^\mu$ ($\mu=P^m$)이다.

[MP3] $\alpha \in GF(P^m)$에 대해, $\alpha^i \bullet \alpha^j = \alpha^{i+j(\mathrm{mod}\,\psi-1)}$ ($\psi=P^m$)이다.

[MP4] $GF(P^m)$에서의 원소는 $F(\alpha)=\sum_{i=0}^{m-1} a_i\alpha^i$에 의해 표현 될 수 있으며, 여기서 α는 루트이다. 즉, m차 원시기약다항식인 $F(X)=X^m + f_{m-1}X^{m-1} + f_{m-2}X^{m-2} + \ldots\ldots + f_1X^1 + f_0$, 인 mosP를 갖는 양의 체인 Z_P에 대한 원소를 갖는 계수이다. 여기서, $a_i \in Z_P(i=0,1,2, \ldots\ldots, m-1)$이고 $f \neq 0$이다.

2-2. GF(3^m)상의 승산 및 스퀘어 알고리즘

유한체 GF(3^m)은 3^m개의 원소를 가지며, 다음 식(2-1)과 같이 표현 할 수 있다.

$$GF(3^m) = \{0, \alpha, \alpha^2, \ldots\ldots, \alpha^{\psi-2}=\alpha^{-1}, \alpha^{\psi-1}=1\} \qquad (2\text{-}1)$$

여기서, $\psi=3^m$이다.

이때,, m차 이상의 차수는 원시기약다항식 F(X)를 mod F(X) 연산으로 m-1 차수 이하로 표현 한다.

따라서, 임의의 GF(3^m)상의 원소는 다음 식(2-2)와 같이 표현 할 수 있다.

$$F(X) = a_{m-1}X^{m-1} + a_{m-2}X^{m-2} + \ldots\ldots + a_1X^1 + a_0$$
$$= \sum_{i=0}^{m-1} a_iX^i \qquad (2\text{-}2)$$

where, $a_i \in GF(3)$ and $i=0,1,2, \ldots\ldots, m-1$.

한편, 원시기약다항식의 근은 α이므로, m은 다음 식(2-3)과 같다. 여기서 +는 mod3이다.

$$\alpha^m + a_{m-1}\alpha^{m-1} + \ldots\ldots + a_1\alpha + a_0 = 0$$
$$\alpha^m = -a_{m-1}\alpha^{m-1} - a_{m-2}\alpha^{m-2} - \ldots\ldots - a_1\alpha - a_0$$
$$\alpha^m = (3-a_{m-1})\alpha^{m-1} + (3-a_{m-2})\alpha^{m-2} + \ldots\ldots + (3-a_1)\alpha + (3-a_0) \qquad (2\text{-}3)$$

그러므로, GF(3^m)상의 원소를 다음과 같이 m-1 차 이하로 표현 할 수 있다.

$$GF(3^m)=\{a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \ + a_1\alpha + a_0\}$$

where, $a_i \in GF(3)$ and $i=0,1,2, \ldots\ldots, m-1$.

GF(3^m)상의 임의의 2원소 $e_1=\sum_{i=0}^{m-1} a_i\alpha^i$ 과 $e_2=\sum_{j=0}^{m-1} b_j\alpha^j$ 에 대해서, $e_1 \bullet e_2$ 는 다음 식(2-4)와 같다.

$$e_1 \bullet e_2 = \sum_{i=m-1}^{0} P_i\alpha^i + \sum_{i=2m-2}^{m} P_i\alpha^i \qquad (2\text{-}4)$$

식(2-4)를 연속적인 승산에 의해, 최대 α^{2m-2} 까지 생성할 수 있으며, α^{2m-2}를 α^m로 mod F(X)으로 생성 할 수 있으며 다음 식(2-5)와 같이 표현 할 수 있다.

$$e_1 \bullet e_2 = \sum_{i=m-1}^{0} R_i\alpha^i \qquad (2\text{-}5)$$

여기서, 승산과 가산은 각각 mod3 승산과 mod3 가산이다.

만일, e_1과 e2가 같은 경우에는 식(2-5)는 다음 식(2-6)과 같이 표현할 수 있다.

$$e_1^2 = e_1 \bullet e_1 = e_1 \bullet e_2 = \sum_{i=0}^{m-1} R_i\alpha^i \qquad (2\text{-}6)$$

따라서, 승산기를 사용하여 스퀘어를 구성할 수 있다.

2-3. GF(3^m)상의 큐브 승산 방법

수학적 성질 [MP2]에 의해, $(a+b)^3=a^3+b^3$, $a^3=a$과 $b^3=b$이다. 따라서, GF(3^m)상의 임의의 원소에 대한 큐브는 다음 식(2-7)과 같다.

$$e^3 = e = \sum_{i=3m-3}^{0} P_j\alpha^j \qquad (2\text{-}7)$$

여기서, j=3i인 경우에는 $P_j=a_j$이고, j=3i+1과 j=3i+2인 경우에는 Pj=0이다. 여기서, i=0,1, ..., m-1이다.

그 이유는 다음과 같다.

$$e^3=e=(a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \ldots\ldots + a_1\alpha + a_0)^3$$
$$=a_{m-1}^3\alpha^{3m-3} + a_{m-2}^3\alpha^{3m-6} + \ldots\ldots + a_1^3\alpha^3 + a_0^3$$
$$=a_{m-1}\alpha^{3m-3} + a_{m-2}\alpha^{3m-6} + \ldots\ldots + a_1\alpha^3 + a_0$$

예를 들어, GF(3^4)상의 임의의 원소에 대한 큐브를 구하는 내용은 다음과 같다. GF(3^4)상의 임의의 원소를 e라고 하면 다음과 같다.

$$e= a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$$

여기서 $a_i \in GF(3)$이고 i=0,1,2이다.

다음에 기약다항식F(X)로 $F(X)=X^4+X+2$를 선택한다. 그러면, 큐브를 다음과 같이 구할 수 있다.

$$e= (a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0)\alpha^3$$
$$= a_3\alpha^9 + a_2\alpha^6 + a_1\alpha^3 + a_0$$

한편, $F(\alpha)=\alpha^4+\alpha+2$이므로 $\alpha^4=\alpha+2$, $\alpha^6=2\alpha^3+\alpha^2$ 및 $\alpha^9=\alpha^3+\alpha^2+\alpha$이다. 따라서, e는 다음과 같이 구할 수 있다.

$$e= (a_3 + 2a_2 + a_1)\alpha^3 + (a_9 + a_2 + a_1)\alpha^2 + a_3\alpha + a_0$$

III. 역원 생성 알고리듬

이 장에서는 $GF(3^m)$상의 역원생성알고리즘에 대해 논의한다. $GF(3^m)$상의 임의의 원소를 e라고 하면, 이에 대한 역원 e^{-1}은 다음 식(3-1)과 같다.

$$e^{-1}=e^{\psi-2} \qquad (3-1)$$

where, $\psi=a^m$

또한, 앞의 역원은 다음과 같이 3을 triple 승산으로 표현 할 수 있다.

$$e^{-1}=e \bullet (e^2)^{\Omega 1} \bullet (e^2)^{\Omega 2} \bullet (e^2)^{\Omega 3} \bullet \ldots\ldots \bullet (e^2)^{\Omega m-1}$$

where, $\Omega 1=3$, $\Omega 2=3^2$, $\Omega 3=3^3$, ..., $\Omega m-1=3^{m-1}$

다음에 $GF(3^m)$상의 역원생성알고리즘을 서술하였으며 이에 대한 블록선도는 다음 그림 3-1에 나타내었다.

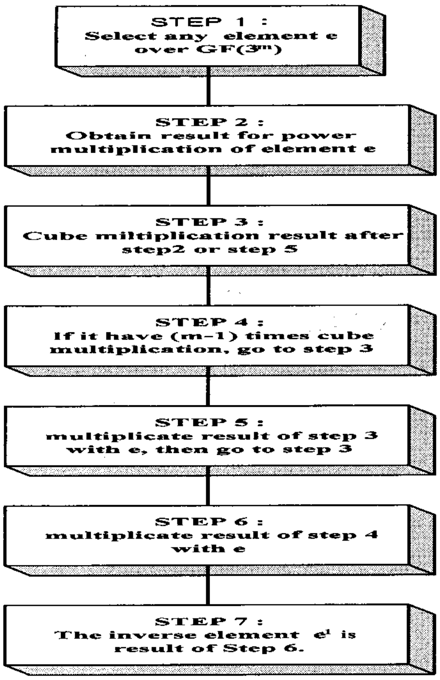


그림 3-1. $GF(3^m)$상의 역원생성알고리즘

[Algorithm]

STEP 1 : Accept any element e over $GF(3^m)$.
STEP 2 : Obtain result for power of element e.
STEP 3 : Cube product result after Step2 or Step 5.
STEP 4 : If it (m-1) times triple product do, go to Step 6.
STEP 5 : Product result of Step 3 with e, then go to Step 3.
STEP 6 : Product result of Step 4 with e.
STEP 7 : The inverse element e-1 is result of Step 6.

IV. 유니버설 역원 생성기

이 장에서는 (3^m)상의 유니버설 역원생성기에 대해 논의한다.

본 논문에서 제안한 (3^m)상의 유니버설 역원생성기는 다음 그림 4-1과 같다.

그림 4-1에서, 유니버설 역원생성기는 승산기, 스퀘어 승산기 및 큐브 승산기로 구성된다.

또한, 승산기, 스퀘어 승산기 및 큐브 승산기의 셀(cell)은 각각 다음 그림 4-2(a), 그림 4-4(b) 및 그림 4-2(c)와 같다.

승산기는 기약다항식의 변화나 m의 증가에 따라 변화하지 않는 특징이 있다. 또한, 승산기의 2개의 입력이 같다면, 스퀘어 승산기가 된다. 큐브 승산기의 기본 형태는 승산기와 같고, 승산 처리 없이 mod 처리로 원소가 입력된다.

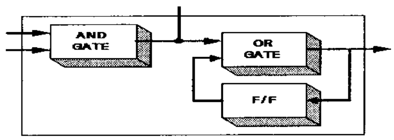
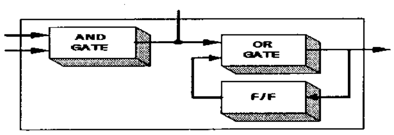
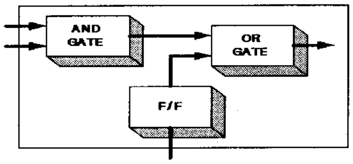


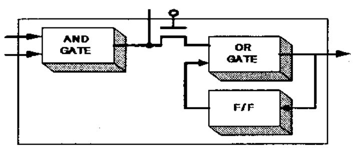
그림 4-1. $GF(3^m)$상의 유니버설 역원생성기 블록선도



(a) Cell of multiplier



(b) Cell of square multiplier



(c) Cell of cube multiplier

그림 4-2. $GF(3^m)$상의 유니버설 역원생성기의 각 셀

GF(3^m)상의 승산기는 다음 그림 4-3과 같다.

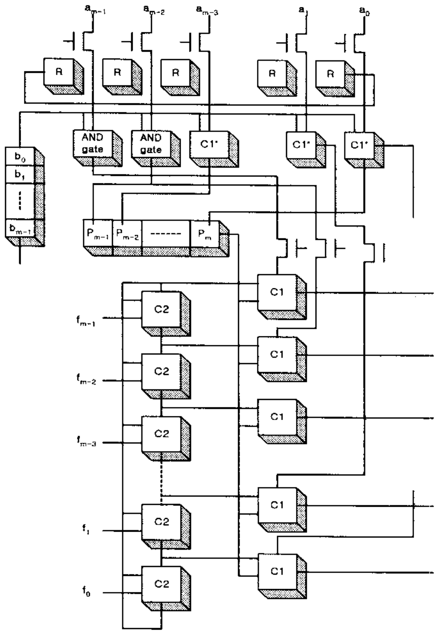


그림 4-3. GF(3^m)상의 승산기의 블록선도

GF(3^m)상의 큐브 승산기는 다음 그림 4-4와 같다.

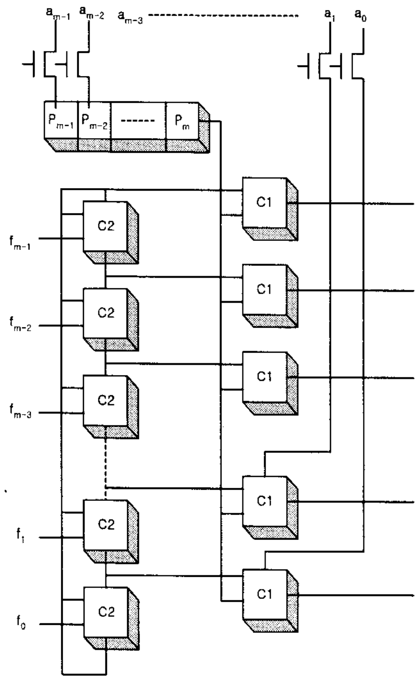


그림 4-4. GF(3^m)상의 큐브 승산기의 블럭선도

V. 결론

본 논문에서는 유한체 GF(3^m)상의 역원생성 알고리즘과 역원생성기를 구성하는 방법을 제안하였다.

제안한 역원생성기는 직렬 처리 승상기 형태로 구성된다. 승산, 스퀘어 승산 및 큐브 승산은 유한체의 수학적 성질로부터 구할 수 있다. 향 후 연구과제로서는 진보된 역원생성기와 유한체상의 제산기 구성이 요구되며,또한, 유한체상의 기본산술연산기시스템(AOUS)의 구성이 요구된다. 그리고, 시프트, 로테이트 및 보수 등과 같은 논리연산을 수행하는 LU 부분에 대한 연구도 요구된다. 만일, 위의 연구가 진행된다면임베디드시스템의 기반이되는 고효율 컴퓨터의 ALU 아키텍쳐를 구성 할 수 있을 것으로 기대되며 현재 연구 진행 중에 있다.

참고문헌

[1] D.L.Dietmeyer, *Logic Design of Digital Systems*, Allyn and Bacon, 1979.

[2] K. Hwang, *Comptuer Arithmetic principles, architecture, and design*, John Wiley & Sons,1979

[3] M.D.Ercegovac and T.Lang, *Digital Systems and* Hardware/Firmware Algorithms, Wiley, 1985.

[3] E.J.McClusky, *Logic Design Principles*, Prentice-Hall, 1986.

[5] D.Green, *Modern Logic Design*, Electronic Systems Engineering Series, 1986.

[6] R.J.McEliece, *Finite Fields for Computer Science and Engineers*, Kluer Academic Publishers, 1987.

[7] G.Drolet,"A New Representation of Elements of Finite Fields GF(2^m) Yielding Small Complexity Arithmetic Circuits," IEEE Trans. Comput., vol. 47, no.9, pp.938-946, Sep. 1988.

[8] H.Wu and M.A.Hassn,"Low Complexity Bit-Parallel Multipliers for a Class of Finite Fields," IEEE Trans. Comput.,vol.47, no.8, pp.883-887, Aug. 1988.

[9] C.Ling and J.Lung,"Systolic array implementation of multipliers for finite fields GF(2^m)", IEEE Trans. Cir. & Sys.,vol.38,no.7, pp.796 -800,Jul.1991.

[10] S.T.J.Fenn, M.Benaissa and D.Taylor,"GF(2^m) multiplication and Division over dual basis",IEEE Trans. Comput., vol.45,no.3, pp. 319 - 327, Mar.1996.

[11] K.Z.Pekmastzi,"multiplxer-based array multipliers", IEEE Trans. Comput., vol.48, no.1, pp.15-23,Jan.1999.