유한체 상에서의 효과적인 직렬 곱셈기의 설계

정회원 권 순 학*, 류 희 수**

Efficient Bit Serial Multipliers for a Class of Finite Fields

Soonhak Kwon*, Heuisu Ryu** *Regular Members*

요 약

최적의 정규기저의 자체 쌍대성을 이용하여 직렬형 곱셈기를 구현하였다. 이러한 직렬형 곱셈기의 설계는 [2]에서 질문되어진 문제인데 그 해답을 보였다. 본 논문에서 설계된 곱셈기는 쌍대기저 그리고 정규기저를 이용한 곱셈기가 가지는 좋은 성질을 모두 가지고 있음을 보였다.

ABSTRACT

Using the self duality of optimal normal basis of type II, we present a design of a bit serial multiplier, which gives an answer for the possible bit serial version asked in [2]. We show that our multiplier has good properties of both of dual and normal basis multipliers.

I. 서 론

유한 체(finite field) 상에서의 연산, 특히 유한 체 상에서의 곱셈은 부호론, 암호론 등의 여러 분야에 응용되고 있다. 그러므로 효율적인 유한 체 곱셈기의 설계가 필요하다. 곱셈 알고리즘의 효율성은 주어진 유한 체에서의 기저를 어떻게 선택하느냐에 따라 좌우된다. 널리 사용되고 있는 유한체 곱셈기 중의 하나로는 Berlekamp 가 제안한 직렬형 곱셈기가 있다[4],[6],[7]. Berlekamp 의 곱셈기는 하드웨어 복잡도가 상당히 낮으며 과거의 천체 탐사 계획 그리고 컴팩트 디스크 기술 등에 필수적인 Reed-Solomon encoder 의 설계에 이용되었다. Berlekamp 의 곱셈기에는 쌍대기저(dual basis)가 이용된다. 즉 유한체에서의 두 입력 값 x,y 의 곱셈을 계산하기 위하여 x 는 다항식 기저 그리고 y 는 쌍대기저로 표시한다. 그리고 그 결과인 두 수의 곱 xy 역시 쌍대기저로 표시한다. 따라서 Berlekamp 알고리즘의 구현에는 기저 변환 과정이 필요하다. 이러한 기저 변환 과정은 하드웨어 복잡도를 상당히 증가시킨다. 이러한 문제점은 필드 다항식을 잘 선택함으로서[6],[7] 부분적으로 해결될 수 있음이 알려져 있다. Berlekamp 곱셈기의 또 다른 결점은 제곱, 멱승(exponentiation) 그리고 역원 등을 구하는 과정이 Massey-Omura type 의 병렬 정규기저(normal basis) 곱셈기에 비해[1],[3],[8] 상당히 느리다는 것이다. 병렬 정규기저를 이용한 곱셈기는 제곱을 구하는 과정이 한번의 쉬프팅과 같기 때문에 역원이나 멱승을 구하는 과정이 비교적 간단하다. 그러므로 여러 종류의 병렬 정규기저 곱셈기가 연구되고 있다. 그 중에서 최적의 정규기저를 이용한 곱셈기가 다른 정규기저를 이용한 곱셈기에 비해 하드웨어 복잡도가 낮음이 잘 알려져 있다[1],[2],[8]. 최적의 정규기저에는 두 가지 종류가 있는데[1] 그 중 하나를 type I, 또 다른 하나를 type II 라 부른다. 본 논문에서 우리는 type II 최적의 정규기저를 이용한 직렬 정규기저 곱셈기를 제안하고자 한다. 그리고 본 곱셈기가 다음 세 가지의 좋은 성질을 가짐을 보이겠다. 첫째, 본 곱셈기는 Berlekamp 곱셈기에 비해 곱셈의 과정이 효율적이다. 둘째, 본 곱셈기에서의 제곱은 기저 원소들 사이의 순열(permutation)을 취함으로 구할 수 있다. 따라서 멱승이나 역원을 구하

* 성균관대학교 수학과 (shkwon@math.skku.ac.kr), ** 한국전자통신연구원 (hsryu@etri.re.kr)
※ 본 연구는 한국학술진흥재단 논문연구과제(KRF 2000-015-DP0005) 지원을 받아 수행되었습니다.
※ 본 논문은 2002년 4월 JCCI 학술대회에서 우수논문으로 선정되어 게재 추천된 논문입니다.

는 데 필요한 시간 복잡도가 Berlekamp 곱셈기에 비해 낮다. 셋째, Berlekamp 곱셈기에서 필요한 기저 변환 과정이 본 곱셈기에서는 필요하지 않다. Sunar 그리고 Koc 은 [2]에서 type II 최적의 정규기저를 이용한 병렬 곱셈기를 제안하였는데 그 논문에서 효과적인 직렬 곱셈기의 존재성에 대한 질문을 하였다. 따라서 본 논문은 그 질문에 대한 답이 되겠다.

Ⅱ. 정규기저와 type II 최적의 정규기저

$GF(2^m)$ 을 원소의 개수가 2^m 개인 유한체라 하자. $GF(2^m)$ 은 m차 $GF(2)$-벡터공간이 된다. $GF(2^m)$ 의 임의의 원소 α 에 대해 $Tr(\alpha)=\alpha+\alpha^2+\cdots+\alpha^{2^{m-1}}$ 라 하자.

정의 1. $GF(2^m)$ 상의 두 기저 $\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$와 $\{\beta_1,\beta_2,\cdots,\beta_m\}$ 이 모든 $1\le i,j\le m$ 에 대해 $Tr(\alpha)=\delta_{ij}$ 을 만족할 때 쌍대(dual) 관계에 있다고 한다. 여기서 δ_{ij} 는 $i=j$ 일 때는 1, $i\neq j$ 일 때는 0 으로 정의된다. 만약 $Tr(\alpha_i\alpha_j)=\delta_{ij}$ 를 만족하면 기저 $\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$ 은 자체 쌍대(self dual)라고 한다

정의 2. $GF(2^m)$ 상의 기저가 $\{\alpha,\alpha^2,\cdots,\alpha^{2^{m-1}}\}$와 같을 때 이를 정규기저라 한다.

임의의 $m\ge1$ 에 대해 $GF(2^m)$ 상에서 정규기저가 항상 존재한다는 것은 잘 알려져 있다[1]. 본 논문의 주된 관심은 다음과 같은 형태의 정규기저이다[1],[2].

정리 1. m 이 양의 정수이고 $2m+1=p$ 가 소수라 하자. 다음의 두 조건 중 하나는 반드시 만족된다고 가정하자.

(가) 2 는 모듈로 p 로 볼 때 원시근(primitive root)이다.

(나) -1 은 모듈로 p 로 볼 때 이차잉여(quadratic residue)가 아니고 모든 이차잉여는 2 의 멱승의 형태로 표시된다.

이 때 β 를 $GF(2^{2m})$ 안에 있는 정리 1의 p차 원시근이라 하고 $\alpha=\beta+\beta^{-1}$ 로 놓으면 α 는 $GF(2^m)$ 안에 있고 $\{\alpha,\alpha^2,\cdots,\alpha^{2^{m-1}}\}$ 은 기저가 된다.

정의 3. 정리 1 에서의 기저를 type II 최적의 정규기저라 한다.

최적의 정규기저는 트리 구조를 가지는 병렬 곱셈기의 설계에 널리 이용되고 있다. [1, p.100]의 테이블에 따르면 type II 최적의 정규기저가 type I 최적의 정규기저보다 세배 정도 많이 분포하고 있음을 알 수 있다. 예를 들면 $m=2, 3, 5, 6, 9, 11, 18, 23, \cdots$ 일 때 type II 최적의 정규기저가 존재한다. 정리 1 의 가정 하에서

$$\alpha^{2^s}=(\beta+\beta^{-1})^{2^s}=\beta^{2^s}+\beta^{-2^s}=\beta^t+\beta^{-t}$$

임을 알 수 있다. 여기서 t 는 $0<t<p$ 이며 $2^s\equiv t \pmod p$ 를 만족한다. $m+1\le t\le 2m$ 의 범위에 있는 t 를 $p-t$ 로 바꾸어 생각하면 다음의 두 기저, $\{\alpha,\alpha^2,\cdots,\alpha^{2^{m-1}}\}$ 와 $\{\beta+\beta^{-1},\ \beta^2+\beta^{-2},\cdots,\beta^m+\beta^{-m}\}$ 은 같은 집합임을 알 수 있다. 본 논문에서는 type II 최적의 정규기저가 가지는 다음의 자체 쌍대성의 성질을 이용하고자 한다.

정리 2. $GF(2^m)$ 상에서 type II 최적의 정규기저가 만약 존재하면 이 기저는 자체 쌍대성의 성질을 가진다.

증명: 기저 원소들의 순열을 취하면 주어진 정규기저의 집합은 $\{\beta^s+\beta^{-s}|1\le s\le m\}$ 로 놓을 수 있다. $i=j$ 인 경우에는

$$Tr((\beta^i+\beta^{-i})(\beta^j+\beta^{-j}))=Tr(\beta^{2i}+\beta^{-2i})$$

이며 적당한 $1\le s\le m-1$ 에 대해

$$Tr(\beta^{2i}+\beta^{-2i})=Tr(\alpha^{2^s})$$

임으로 기저 원소들의 일차 독립성에 의해 $Tr(\alpha^{2^s})=1$ 이다. 그러므로 $i\neq j$ 인 경우를 생각하자. 이 경우에는 다음을 만족하는

$$Tr((\beta^i+\beta^{-i})(\beta^j+\beta^{-j}))=$$
$$Tr(\beta^u+\beta^{-u})+Tr(\beta^v+\beta^{-v})$$

$1\le u,v\le m$ 가 존재한다. $\beta^u+\beta^{-u}=\alpha^{2^s}$ 그리고 $\beta^v+\beta^{-v}=\alpha^{2^t}$ 로 쓸 수 있으므로

$$Tr(\beta^u+\beta^{-u})+Tr(\beta^v+\beta^{-v})=1+1=0$$

이다. 증명 끝.

Ⅲ. 곱셈 알고리즘

정리 2 의 증명과정을 살필 때 $\alpha_s=\beta^s+\beta^{-s}$ 로 정의하면 많은 기호들이 간단해 짐을 짐작할 수 있다. 그러므로 본 논문의 이 후 과정에서는 type II 최적의 정규기저 $\{\alpha^{2^s}|0\le s\le m-1\}$ 와 같은 집합인 $\{\alpha_s|\alpha_s=\beta^s+\beta^{-s},1\le s\le m\}$ 을 주로 생각하겠다. $GF(2^m)$ 상의 임의의 원소 $x=\sum_{i=1}^{m}x_i\alpha_i$, $x_i\in GF(2)$, 에 대하여 정리 2를 이용하면 모든

$1\le s\le m$ 에 대해

$$x_s = \sum_{i=1}^{m} x_i Tr(\alpha_s\alpha_i) = Tr(\alpha_s \sum_{i=1}^{m} x_i\alpha_i) = Tr(\alpha_s x)$$

임을 알 수 있다.

정의 4. $-m\le s\le 2m$ 의 범위에서 α_s, x_s 을 다음과 같이 정의하자.

$\alpha_s=\alpha_{-s}, x_s=x_{-s}$ if $-m\le s\le -1$

$\alpha_s=\alpha_{2m+1-s}, x_s=x_{2m+1-s}$ if $m+1\le s\le 2m$

$\alpha_0=x_0=0$

위 정의에 의하면 $-m\le j\le 2m$ 의 범위의 모든 j 에 대해 $x_j=Tr(\alpha_j x)$ 이며 또한 $1\le s,t\le m$ 인 s,t 에 대하여

$$\alpha_s\alpha_t=(\beta^s+\beta^{-s})(\beta^t+\beta^{-t})=\alpha_{s-t}+\alpha_{s+t}$$

의 $\alpha_{s-t},\alpha_{s+t}$ 가 잘 정의됨을 알 수 있다.

정리 3. $GF(2^m)$ 상의 두 원소 $x=\sum_{i=1}^{m} x_i\alpha_i$ 그리고 $y=\sum_{i=1}^{m} y_i\alpha_i$ 을 생각하자. 두 수의 곱 xy 을 $xy=\sum_{i=1}^{m}(xy)_i\alpha_i$ 로 표시할 때 계수 $(xy)_k$ 는 $(xy)_k=\sum_{i=1}^{2m} y_i x_{i-k}$ 을 만족한다.

증명: 정리 2의 자체 쌍대성을 이용하면

$$\begin{aligned}(xy)_k &= Tr(\alpha_k xy) = Tr(\alpha_k x \sum_{i=1}^{m} y_i\alpha_i)\\ &= \sum_{i=1}^{m} y_i Tr(\alpha_k\alpha_i x)\\ &= \sum_{i=1}^{m} y_i Tr(\alpha_{i-k}x+\alpha_{i+k}x)\\ &= \sum_{i=1}^{m} y_i(Tr(\alpha_{i-k}x)+Tr(\alpha_{i+k}x))\\ &= \sum_{i=1}^{m} y_i(x_{i-k}+x_{i+k}).\end{aligned}$$

정의 4를 이용하면

$$\begin{aligned}\sum_{i=1}^{m} y_i x_{i+k} &= \sum_{i=1}^{m} y_{m+1-i}x_{m+1-i+k}\\ &= \sum_{i=1}^{m} y_{m+i}x_{m+i-k}\\ &= \sum_{i=m+1}^{2m} y_i x_{i-k}.\end{aligned}$$

그러므로

$$\begin{aligned}(xy)_k &= \sum_{i=1}^{m} y_i x_{i-k}+\sum_{i=1}^{m} y_i x_{i+k}\\ &= \sum_{i=1}^{2m} y_i x_{i-k}.\end{aligned}$$

증명 끝.

이제 정리 3에 의하면 $(xy)_k$ 을 행 벡터 와 열 벡터의 곱으로 다음과 같이 표시할 수 있다.

$$(xy)_k=(x_{1-k},x_{2-k},\cdots,x_{2m-k})\times(y_1,y_2,\cdots,y_{2m})^T.$$

여기서 열 벡터 $(y_1,y_2,\cdots,y_{2m})^T$ 은 행 벡터 $(y_1,y_2,\cdots,y_{2m})$ 의 전치행렬이다. 이제 정의 4에 있는 대로 $y_0=0$ 을 이용하면

$$(xy)_k=(x_{1-k},x_{2-k},\cdots,x_{2m-k},x_{2m+1-k})\times(y_1,y_2,\cdots,y_{2m},y_0)^T.$$

이 때 $(xy)_{k+1}$ 은

$$(xy)_{k+1}=(x_{-k},x_{1-k},\cdots,x_{2m-1-k},x_{2m-k})\times(y_1,y_2,\cdots,y_{2m},y_0)^T.$$

정의 4에 의하면 $x_{-k}=x_{2m+1-k}$ 이다. 그러므로 행 벡터 $(x_{-k},x_{1-k},\cdots,x_{2m-1-k},x_{2m-k})$ 은 $(x_{1-k},x_{2-k},\cdots,x_{2m-k},x_{2m+1-k})$을 오른 쪽으로 한 번 쉬프팅한 벡터가 된다. 이와 같은 특성을 이용하면 $(xy)_k$ 의 계산을 쉬프트 리지스터를 이용한 회로도로 그림 1 과 같이 구현할 수 있다. 그림 1의 쉬프트 리지스터의 초기 값은 $(x_0, x_1,\cdots, x_{2m})$이다. 실제로 이 값은 $(0, x_0, \cdots, x_m, x_m, \cdots, x_1)$ 이다. k-클럭 사이클 뒤에 결과 값 $(xy)_k$ 을 얻게 된다.

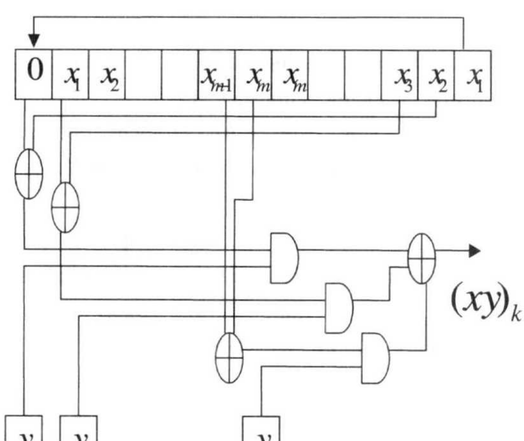

그림 1. type II 최적의 정규기저를 이용한 직렬 곱셈기

IV. 결 론

Berlekamp 의 곱셈기와 비교할 때 본 논문의 곱셈기는 m+1 개의 플립-플롭을 더 필요로 한다. 하지만 Berlekamp 곱셈기에서는 쉬프팅을 하기 전에 x_i 을 계산하기 위해 XOR 연산이 필요하지만 본 곱셈기에서는 그 과정이 불필요하므로 보다 빠르게 연산을 수행할 수 있다. 또한 본 곱셈기는 정규기저

를 이용하기 때문에 제곱의 연산을 한 번의 치환(permutation)으로 구할 수 있다. 그러므로 주어진 수의 멱승 그리고 역원 등의 계산이 Berlekamp 의 경우보다 훨씬 간단해진다. 그리고 본 곱셈기에서 사용하는 기저가 자체 쌍대기저(self dual basis)이므로 기저 변환 과정이 필요 없다. 하지만 Berlekamp 곱셈기와 같이 쌍대기저를 이용한 곱셈기들은 반드시 기저 변환 과정이 필요하고 이 때 추가로 시간 및 공간 복잡도가 증가하게 된다. 지금까지 우리는 $GF(2^m)$ 상에서 type II 최적의 정규기저가 존재할 때 효과적인 직렬 곱셈기의 설계를 구현할 수 있음을 보였다. 본 논문의 아이디어는 $GF(2^{mn})$, 여기서 $GF(2^m)$ 는 type II 최적의 정규기저가 존재하는 유한체, 와 같은 확장 필드에도 적용될 수 있으나 그 내용은 여기서 생략하겠다. 또한 정리 3의 결과를 이용하면 type II 최적의 정규기저를 이용한 효과적인 병렬 시스톨릭 곱셈기의 설계가 가능하다는 것도 언급하겠다. 마지막으로 type I 최적의 정규기저를 이용한 직렬 곱셈기의 구현이 [9],[10]에서 다루어졌음을 밝힌다.

참 고 문 헌

[1] A.J. Menezes, "Applications of finite fields," Kluwer Academic Publisher, 1993.

[2] B. Sunar, C.K. Koc, "An efficient optimal normal basis type II multiplier," IEEE Trans. Computers, 50, pp. 83-87, 2001.

[3] C.K. Koc, B. Sunar, "Low complexity bit parallel canonical and normal basis multipliers for a class of finite fields," IEEE Trans. Computers, 47, pp. 353-356, 1998.

[4] E.R. Berlekamp, "Bit serial Reed-Solomon encoders," IEEE Trans. Inform. Theory, 28, pp.869-874, 1982.

[5] I.S. Hsu, T.K. Troung, L.J. Deutch, I.S. Reed, "A comparison of VLSI architecture of finite field multipliers using dual, normal or standard bases," IEEE Trans. Computers, 37, 1988.

[6] M. Wang, I.F. Blake, "Bit serial multiplication in finite fields," SIAM J. Disc. Math., 3, pp. 140-148, 1990.

[7] M. Morii, M. Kasahara, D.L. Whiting, "Efficient bit serial multiplication and discrete-time Wiener-Hopf equation over finite fields," IEEE Trans. Inform. Theory, 35, pp. 1177-1183, 1989.

[8] M.A. Hasan, M.Z. Wang, V.K. Bhargava, "A modified Massey-Omura parallel multiplier for a class of finite fields," IEEE Trans. Computers, 42, pp. 1278-1280, 1993.

[9] G. Drolet, "A new representation of elements of finite fields $GF(2^m)$ yielding small complexity of arithmetic circuits," IEEE Trans. Computers, 47, pp. 938-946, 1998.

[10] C.H. Lee, J.I. Lim, "A new aspect of dual basis for efficient field arithmetic," PKC, Lecture Notes in Computer Science, 1560, pp. 12-28, 1999.

권 순 학(Soonhak Kwon) 정회원

1990년 2월 : KAIST 수학과 학사

1992년 2월 : 서울대학교 수학과 석사

1997년 5월 : Johns Hopkins University Ph. D.

1998년 3월~현재 : 성균관대학교 수학과 전임강사, 조교수.

<주관심 분야> 정수론, 암호론, 회로 이론

류 희 수(Heuisu Ryu) 정회원

1990년 : 고려대학교 수학과 학사

1992년 : 고려대학교 수학과 석사

1999년 : Johns Hopkins University Ph. D.

1999년~2000년 : 홍익대학교 전자과 post-doc

2000년~현재 : 한국전자통신연구원 선임연구원 (팀장)

<주관심 분야> 암호이론, 통신망 정보보호, 정수론