# 효율적인 기저 변환

박춘명*

*한국교통대학교

# Efficiency Base Conversion

Chun-Myoung Park*

*Korea National University of Transportation

E-mail : cmpark@ut.ac.kr

## 요 약

본 논문에서는 최근 21세기의 지식정보화 시대의 ICT 분야에서 그 중요성과 응용 부분이 극대화 되고 있는 유한체상에서의 기저 변환에 대한 한 가지 방법을 제안하였다.

제안한 방법은 기존의 방법에 비해 규칙적이고 확장성의 용이하고, 각종 IT 분야에 적용 및 응용이 가능하다.

## ABSTRACT

This paper present a method of base conversion over finite fields which is the important and its application fields are maximization in the 21C knowledge based information society.

The proposed method is more regularity and extensibility compare with previous relational method recently.

## 키워드

Base, base conversion, finite fields, ICT

## Ⅰ. 서 론

최근 급격히 발전하고 있는 디지털통신 및 저장매체의 개발에 있어 유한체 연산은 매우 중요한 분야로 대두되고 있다. 유한체 연산은 통신 채널 및 저장매체에서 발생하는 오류를 정정하기 위한 오류정정 회로로 부터 컴퓨터 메모리, 디지털 레이더 신호처리, 이동통신, 위성통신, 패킷 스위칭 시스템, CD(Compact Disk), DAT(Digital Audio Tape) 등의 분야에 활용된다. 또한 차세대의 성장 동력 산업으로 손꼽히는 디지털 보안 및 서명, 디지털 워터마킹, 가정용 보안시스템, RF용 스마트 카드 등 유한체 연산에 대한 응용할 수 있는 영역이 날로 확장되고 있다[1-5].

## Ⅱ. 트레이스 함수

트레이스 함수는 선형함수의 대표적인 예이면서 유한체 승산기를 설계하는데 매우 적합하고, 유한체 상에서 2차 방정식의 해에 관련된 결과를 얻는데 이용한다.

[정의1]

임의의 선형 함수 F(z)는 다음 식(1)의 형태로 표현된다.

$$F(z)=Tr(\beta z) \quad \forall\ z\in GF(p^m), \beta \in GF(2^m) \qquad (1)$$

따라서, $p^m$ 개의 선형 함수 F(z)가 존재한다.

[정의2]

$\{\mu i\}$를 GF($p^m$)에 대한 기저라 하고 GF($p^m$)상의 임의의 원소 Z($\alpha$)∈GF($p^m$)를 표현하면 다항식의 표현인 식(2)로 표현할 수 있다.

$$Z(a)=\sum_{i=0}^{m-1} z_i u_i, \quad z_i \in GF(p) \qquad (2)$$

이 원소들로 이루어진 $p^m$ 개의 선형 함수 F(z)는 다시 식(3)과 같이 계수 ai를 갖는 함수 형태로 표현이 가능하다.

$$F(z)=\sum_{i=0}^{m-1} a_i z_i \qquad \forall_z \in GF(p^m) \qquad (3)$$

여기서 $a_i \in GF(p)$이고 가산은 모듈러 p이다

식(3)에서 정의한 함수들은 분명히 선형이고 함수들은 $p^m$개의 원소들로 구성된다. 정의 3.2로부터 $p^m$개의 선형함수들 F(z)가 존재하므로 식(3.3)에서 정의한 함수 F(z)도 $p^m$개의 선형함수 F(z)가 존재하여야 한다. 선형함수들은 기저 $\{\mu i\}$를 다항식 기저(polynomial basis, 표준기저) $\{a^0, a^1, ..., a^{m-1}\}$로 표현하는 것이 일반적이다. 여기서 a는 GF($p^m$)에 대해서 정의하는 다항식의 근이다.

## Ⅲ. 기저 변환

본 절에서는 표준기저상의 원소 표현이 쌍대기저로 변환되기 위해서 트레이스 함수를 정의한다.

[정의3]

GF($p^m$) 내의 임의의 원소 $\beta$ 에 대한 trace, Tr($\beta$)는 식(4)와 같이 정의되며 다음의 성질을 갖는다.

$$Tr(\beta) = \sum_{i=0}^{m-1} b^{p^i} \quad (4)$$

1) $[Tr(B)]^p = Tr(b)$=Tr($\beta$)
   (즉 Tr($\beta$)는 GF(p)상의 원소이다.)
2) Tr($\beta$+r)=Tr($\beta$)+Tr(r)
3) Tr(c$\beta$)=c•Tr($\beta$) (c∈GF(p) )
4) Tr(1)=m(mod p)

[정의4]

GF($p^m$)내의 m개의 선형독립인 원소들의 집합을 GF($p^m$)의 기저라 하고, 모든 기저는 GF($p^m$)상의 '0' 이 아닌 어떠한 함수나 '0' 이 아닌 어떠한 원소 $\beta$ 에 대해서도 하나의 쌍대기저를 갖는다.

[정의5]

$\{\mu_i\}$, $\{\lambda_k\}$를 GF($p^m$)상의 모든 Trace 함수와 임의의 원소 $\beta(\beta \neq 0)$ 에 대한 기저들이라 하고, 다음과 같은 조건을 만족할 때 이 두 개의 기저를 각각에 대한 쌍대기저라 한다.

$$f(\beta \mu_i, \lambda_j) = Tr(\mu_i \lambda_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \quad (5)$$

여기서, $\{\mu_i\}$는 표준기저이고 $\{\lambda_j\}$는 쌍대기저이다.

[정의6]

$\{\mu_i\}$, $\{\lambda_k\}$를 각각 Trace 함수와 $\beta$에 대한 GF($p^m$)상의 쌍대기저가 되게 한다. 이때 $z_k \in$ GF($p^m$)(0≤k≤m-1)는 식(6)처럼 쌍대기저에서 표현된다.

$$Z = \sum_{i=0}^{m-1} f(z_i B u_i) \lambda_i \quad (6)$$

GF($p^m$)상의 임의의 원소 Z를 쌍대기저 $\{\lambda_i\}$로 표현하면 식(7)과 같다.

$$Z(a) = z_0\lambda_0 + z_1\lambda_1 + ... + z_{m-1}\lambda_{m-1} = \sum_{i=0}^{m-1} z_i\lambda_i \quad (7)$$

식(7)의 양변에 표준기저 $\{a^k\}$를 곱하여 Trace를 취하면 다음과 같다.

$$Z(\alpha) \cdot \alpha^k = \left(\sum_{i=0}^{m-1} z_i\lambda_i\right) \cdot \alpha^k$$

$$Tr(Z(\alpha) \cdot \alpha^k) = Tr\left(\sum_{i=o}^{m-1} z_i\lambda_i a^k\right)$$

그러므로 식(7)은 식(8)와 같이 표현된다.

$$Z(a) = \sum_{i=0}^{m-1} z_k\lambda_k = \sum_{k=0}^{m-1} Tr(za^k)\lambda_k \quad (8)$$

## Ⅳ. 결 론

본 논문에서는 최근 21세기의 지식정보화 시대의 IT 분야에서 그 중요성과 응용 부분이 극대화되고 있는 유한체상에서의 기저 변환에 대한 한 가지 방법을 제안하였다. 제안한 방법에서는 효율적으로 기저 변환을 수행할 수 있는 트레이스 변환 과정을 제안하였으며, 이를 바탕으로 기저 변환을 용이하게 할 수 있는 알고리즘을 제안하였다.

## 참고문헌


[1] R.W. Hamming, "Error Detecting and Error Correcting Codes," Bell Syst. Thch. J., 29, pp. 147-160, 2016.

[2] I.S. Reed and G. Solomon, "Polynomial Codes over Certain Finite Field," J. Soc, Ind. Appl. Math., 8, pp. 300-304, 2015.

[3] E. Artin, Galois Theory, NAPCO Graphic arts, Inc., Wilconsin. 2013.

[4] R.J. McEliece, Finite Fields for Computer Scientists and Engineers, KluwerAcademic Pub., 2012.

[5] C. K. Koc, and B. Sunar, "Low-Complexity Bit Parallel Canonical and Normal Basis Multipliers for a Class of Finite Fields," IEEE Trans. Comp., vol. 47, no.3, pp. 353-356, March 2015.