論文99-36C-5-7

다치논리함수의 GRM상수 생성 방법

(A Production Method to GRM Coefficients of Multiple Valued Logic Function)

申 富 植 *, 沈 載 煥 *, 金 興 壽 *

(Boo Sik Shin, Jai Hwan Sim, and Heung Soo Kim)

요 약

GF(p)상의 n변수에 대한 p^n개의 극수를 갖는 GRM 상수를 구하는 방법을 제시하였다. 일반적인 GRM 상수의 생성방법은 RM (Reed-Muller) 전개식을 이용하여 극수(이하 P로 정의) 0의 RM상수를 구하고 이를 확장하여 모든 GRM상수를 구한다. 본 논문에서 제안된 GRM상수의 생성 방법은 2단계로 구성된다. 먼저 단변수에 대하여 최소의 연산자를 갖는 극수를 구하고 다음 극수의 순환성을 이용하여 동일한 변환 과정을 모든 GRM상수 생성과정에 적용한다. 제안된 방법은 극수의 순환성으로 인하여 생성과정이 간단하며 연산자의 개수를 줄일 수 있는 GRM상수 생성방법이다.

Abstract

This paper presents a production method to GRM coefficients which are consist of P^n polarities to n variables over GF(p). In general production method to GRM coefficients is derived from RM coefficients to polarity 0 using RM expansion and extended to GRM coefficients. The procedure of proposed production method to GRM coefficients is consists of 2 steps. First, obtain the optimal polarity which is contains a minimal operation to single variable and then apply the same process to all generation process of GRM coefficients using cyclic property of the polarity. Proposed method simplify the generation procedure and reduces a number of operators because of the cyclic property of polarity.

Ⅰ. 서 론

현재 사용되고 있는 논리회로 시스템은 부울함수를 기초로 한 2진 논리회로로 구성되어있다. 그러나 2진 논리회로가 갖는 회로 복잡성, 단자수 제한 문제등으로 인하여 부울체의 확장체인 유한체(Galois field)를 기초로 한 다치논리에 대한 연구가 활발히 진행중이다[1-2].

* 正會員, 仁荷大學校 電子工學科

(Department of electronics Engineering IN-HA University, Inchon, Korea)

接受日字:1998年12月1日, 수정완료일:1999年4月22日

$GF(p^m)$는 p를 소수 m을 양의 정수라 할 때 p^m개의 원소로 체를 구성한다. 다치논리함수는 일반적으로 입력값의 조합에의해 출력값이 주어지는 진리치 표를 일반화한 연산영역(operational domain)과 입력변수를 함수적으로 표현한 함수영역(functional domain)에서 해석이 가능하며 영역(domain)사이의 변환은 RM(Reed-Muller) 전개식을 이용한다. RM전개식을 사용하는 이점은 소자 수와 게이트의 상호 연결 수에 있어서 타 함수의 논리회로 실현보다 경제적이며 테스트가 용이하기 때문에 RM전개식의 계수들을 연산하는 여러 가지 방법들이 제안되었다[3-8]. RM상수를 구하는 방법은 변환행렬을 이용하여 구하는 방법[3]이 일반적이나 최근에는 그래프이론에 대한 관

심이 높아지면서 결정도를 이용하여 RM상수를 구하는 방법이 제시되었다[4]. RM상수를 이용한 GRM상수의 생성은 다치논리 함수 간략화 방법의 하나로서 GRM변환에 의하여 얻어진 최적의 변환방법을 사용하면 최적의 함수로 표현할 수 있으며 이러한 최적의 GRM상수를 생성하는 방법에 대한 연구가 행하여 지고 있다. D.H.Green[9,10]은 연속적으로 극수 생성이 가능하며 상수생성 연산식의 개수를 줄인 효과적인 GRM상수 생성 방법을 제안하였다. Q.H. Hong등[7]은 단변수에 대한 극수 변환 과정을 확장하여 n변수에 대한 GRM 상수를 구하였으며 B.J. Falkowski등[8]은 단변수에 대한 변환 과정을 4치 함수에 적용하여 GRM 상수를 구하였다. 그러나 제안된 논문[7,8]은 GRM상수를 구하는 논리적인 단계는 간단하나 극수에 따른 상수의 변환과정이 극수에 의하여 다르게 적용되며 모든 극수의 GRM상수 생성과정에 대한 흐름이 복잡하다는 단점이 있다. 따라서 본 논문에서는 GRM상수를 구함에 있어서 p치 단변수에 대한 p-1개의 GRM 상수변환식에서 최소의 변환형식을 갖는 극수를 선택하고 이를 극수에 따른 함수의 순환성을 이용하여 모든 극수의 GRM 상수 생성시에 동일한 방법을 적용하여 연산과정이 일관성이 있고 간단한 GRM 상수를 구하는 방법을 제안하였다.

Ⅱ. GF(P)상에서 GRM상수 생성

RM전개식에 의하여 표현된 함수는 유일한 것이 아니다. GF(p)상에서 입력 변수 x를 $\bar{x}$ 인 $x+1$, $x+2, \cdots, x+(P-1)$로 대치한다면 다른 형태의 정규화된 형식으로 표현된다. 이와같이 GF(p)상에서의 n개의 입력 변수에 대한 p^n개의 서로다른 입력형태가 만들어지며 이에 대한 RM상수를 구하는 과정을 GRM변환이라한다. GRM상수값의 결정은 연산영역에서 극수에 대한 GRM상수를 구하는 방법이 있지만 극수가 0인 고정극수(fixed polarity)를 구하여 극수를 확장시켜 GRM상수를 구하는 것이 효과적이다. 본 장에서는 GF(p)상에서의 GRM상수를 생성하는 방법을 나타내었다.

1. 단변수에 대한 GRM 상수의 생성

p치 단변수(n=1)인 경우 일반적인 RM 전개식은 다음과 같다.

$$f(x) = a_0 + a_1 x' + a_2 x'^2 + \cdots + a_{P-1} x'^{P-1} \quad (1)$$

('+' 는 modulo-p 연산)

GRM 상수를 구하기 위해서는 x'는 x의 입력형태가 $x, x+1 \cdots, x+(P-1)$의 P가지 형태중에 하나를 의미한다. 각각은 극수 0,1,2, ..., P-1를 나타내며 x'를 극수 k에 대하여 x의 함수로 표현하면 다음과 같다.

$$x' = x + k \qquad (k = 0,1,2\cdots,P-1) \quad (2)$$

단변수에 대한 RM전개식이 식(1)과 같은 경우 x'에 대하여 식(2)를 대입하여 극수 k에 대한 함수식으로 표현하면 다음과 같다.

$$\begin{aligned} f(x) &= a_0 + a_1 x' + a_2 x'^2 + \cdots + a_{P-1} x'^{P-1} \\ &= a_0 + a_1 (x+k) + a_2 (x+k)^2 + \cdots + a_{P-1} (x+k)^{P-1} \\ &= a'_0 + a'_1 x + a'_2 x^2 + \cdots + a'_{P-1} x^{P-1} \end{aligned} \quad (3)$$

극수 k에 의해 생성된 상수 $a'_0, a'_1, \cdots, a'_{P-1}$는 x의 차수가 같은 항들에 대하여 P=0의 상수를 이용하여 극수 k에 해당하는 변환된 상수연산식을 구할 수 있다.

표 1. GF(3)상의 극수에 따른 상수의 변환
Table 1. Changes of coefficients to polarity over GF(3).

a_i	P=0($x' = x$)	$P=1(x' = x+1)$	$P=2(x' = x+2)$
a_0	a_0	$a_0 + a_1 + a_2$	$a_0 + 2a_1 + a_2$
a_1	a_1	$a_1 + 2a_2$	$a_1 + a_2$
a_2	a_2	a_2	a_2

[예제 1] 3치 1변수의 경우 P=0의 RM함수가 다음과 같은 경우 P=1, P=2의 함수를 구하여라.

$$f(x) = a_0 + a_1 x' + a_2 x'^2 \quad (4)$$

① $x' = x + 1$인 경우(P=1)

식(3)으로부터 $k=1$을 대입하면 다음과 같이 극수 1에 대한 변환식을 얻을 수 있다.

$$f(x) = (a_0 + a_1 + a_2) + (a_1 + 2a_2)x + a_2 x^2 \quad (5)$$

② $x' = x + 2$인 경우(P=2)

식(3)으로부터 $k=2$을 대입하면 다음과 같이 극수 2에 대한 변환식을 얻을 수 있다

$$f(x)=(a_0 + 2a_1 + a_2) + (a_1 + a_2)x + a_2x^2 \quad (6)$$

식(4)-(6)으로부터 3치 함수의 경우 극수에 따른 상수의 변환 관계를 나타내면 다음과 같다.

2. n변수에 대한 GRM 생성

P치 n변수에 대한 상수의 변환은 단변수에 대한 상수의 변환 과정을 n변수로 확장하여 이루어 진다. n변수에 대한 RM전개식의 일반식은 다음과 같이 표현된다.

[정의 1] $f^k(x)$는 $f(x)$ 함수에 대하여 극수 k변환에 의해 생성된 극수 k의 GRM함수를 나타낸다.

[정의 2] $f(X_n)$는 입력변수가 n개로 구성된 함수 $f(x)$를 의미한다.

단변수에 대한 일반식을 표현하면 다음과 같다.

$$f(X_1) = a_0 + a_1x_i + a_2x_i^2 + \cdots + a_{p-1}x^{p-1} \quad (7)$$

2변수에 대한 일반식을 나타내면 다음과 같다.

$$\begin{aligned} f(X_2)=&(a_0+a_1x_1+\cdots+a_{P-1}x_1^{P-1}) \\ &+(a_P+a_{P+1}x_1+\cdots+a_{2P-1}x_1^{P-1})x_2 \\ &+\cdots+(a_{2P}+a_{2P+1}x_1+\cdots+a_{3P-1}x_1^{P-1})x_2^{P-1} \end{aligned} \quad (8)$$

x_1변수에 대한 부분 단변수에 대한 일반식으로 표현되며 식(8)을 x_2에 대하여 표현하면 다음과 같다.

$$f(X_2)=f(X_1)+f(X_1)x_2+\cdots+f(X_1)x_2^{P-1} \quad (9)$$

식(9)를 n변수로 확장하면 다음과 같다.

$$f(X_n)=f(X_{n-1})+f(X_{n-1})x_n+\cdots+f(X_{n-1})x_n^{P-1} \quad (10)$$

극수가 P인 GRM상수를 구하는 것은 각각의 변수에 따르는 극수 P의 단변수 변환 상수를 구하여 이를 n변수로 확장하면 극수 P에 대한 GRM 함수를 구할 수 있다.

[예제 2] 3치 2변수에 대한 P=0의 함수 식이 다음과 같은 경우 P=4의 GRM상수를 구하라.

$$f(X_2) = x_2+x_2^2+x_1+2x_1x_2+x_1x_2^2+x_1^2+2x_1^2x_2+x_1^2x_2^2$$

$$f(X_2) = (x_2+x_2^2)+(1+2x_2+x_2^2)x_1+(1+2x_2+x_2^2)x_1^2$$

x_2변수에 대한 P=1의 변환을 행하면 다음과 같다.

$$f^1(X_2)=(2+x_2^2)+(1+x_2+x_2^2)x_1+(1+x_2+x_2^2)x_1^2$$

위의 결과 식을 이용하여 x_1 변수에 대한 P=1의 변환을 행하면 P=4의 GRM 함수식을 구할 수 있으며 다음과 같다.

$$f^4(X_2)=(1+2x_2)+(1+x_2+x_2^2)x_1^2$$

위의 예제에서와 같이 n변수에 대한 GRM함수를 구하는 방법은 단변수에 대한 변환상수를 구하는 방법을 n변수로 확장하여 구하면 된다.

Ⅲ. 극수의 순환성

Ⅱ장의 경우에서 보면 P치 단변수의 경우 P=0을 제외한 모든 극수의 GRM상수생성은 극수에 따라서 P-1개의 서로다른 상수의 생성방법이 존재함을 알 수 있다. GF(3)의 경우 각각은 $a_0+a_1+a_2$, a_1+2a_2, a_2 와 $a_0+2a_1+a_2$, a_1+a_2, a_2로 극수 1과 극수 2에 대한 상수의 생성 방법이 다르다. 그러나 이와 같은 문제는 극수의 순환성을 이용하여 상수생성연산식이 가장 간단한 특정 극수를 이용하면 모든 GRM상수 생성시 특정극수의 연산식을 모두 적용하여 구할 수 있다.

[정의 3] $(f^k(x))^m$ 는 $f(x)$함수의 P=k의 GRM 함수 $f^k(x)$에 대한 P=m의 GRM 함수를 의미한다.

[정리 1] 단변수에 대하여 극수 k의 GRM 함수 $f^k(x)$에 대한 극수 m의 함수는 다음과 같이 표현된다.

$$(f^k(x))^m = f^{(k+m) \bmod p}(x)$$

(증명)

P치 단변수 x에 대한 P=0의 함수식이 식(11)와 같은 경우 P=k의 GRM함수식을 나타내면 식(12)와 같다.

$$f(x)= a_0+ a_1x+ a_2x^2+\cdots+a_{P-1}x^{P-1} \quad (11)$$

$$\begin{aligned} f^k(x)= &a_0+ a_1(x+k)+ a_2(x+k)^2 \\ &+\cdots+a_{P-1}(x+k)^{P-1} \end{aligned} \quad (12)$$

극수 k에 대한 전개식 식(12)를 P= m에 대한 전개식으로 나타내면 다음과 같다.

$$(f^k(x))^m = a_0 + a_1(x+k+m) + a_2(x+k+m)^2 + \cdots + a_{P-1}(x+k+m)^{P-1} \quad (13)$$

식(13)은 '+'는 mod$P$ 연산이므로 극수에 해당하는 부분에 mod$P$의 연산을 행하면 다음과 같이 표현이 가능하다.

$$\begin{aligned}(f^k(x))^m &= a_0 + a_1(x+(k+m) \bmod P) \\ &\quad + a_2(x+(k+m) \bmod P)^2 \\ &\quad + \cdots + a_{P-1}(x+(k+m) \bmod P)^{P-1} \\ &= f^{(k+m) \bmod P}(x)\end{aligned}$$

(증명 끝)

GF(P)에서 P=1의 변환을 이용하면 다음과 같이 연속적으로 GRM상수의 생성이 가능하다.

$f^0(x) \dashrightarrow f^1(x) \dashrightarrow \cdots \dashrightarrow f^{P-1}(x) \dashrightarrow f^0(x)$

변환: P=1 P=1 P=1

[예제 3] 3치 1변수의 경우 P=0의 RM함수가 다음과 같은 경우 $f^2(x)$와 $(f^1(x))^1$의 함수식이 같음을 보여라.

$$f(x) = a_0 + a_1 x + a_2 x^2$$

표 1.로부터 P=2인 경우의 상수의 변환은 다음과 같이 표현된다.

$$f^2(x) = (a_0+2a_1+a_2) + (a_1+a_2)x + a_2x^2$$

표 1.로부터 P=1인 경우의 상수의 변환은 다음과 같이 표현된다.

$$f^1(x) = (a_0+a_1+a_2) + (a_1+2a_2)x + a_2x^2$$

$f^1(x)$의 함수식을 이용하여 $(f^1(x))^1$의 함수식을 표 1.을 이용하여 구하면 다음과 같다.

$$\begin{aligned}(f^1(x))^1 &= (a_0+a_1+a_2+a_1+2a_2+a_2) \\ &\quad + (a_1+2a_2+2a_2)x + a_2x^2 \\ &= (a_0+2a_1+a_2) + (a_1+a_2)x + a_2x^2 = f^2(x)\end{aligned}$$

Ⅳ. GF(3),GF(4)의 GRM상수 생성 방법

본 장에서는 단변수에 대한 극수에 따른 상수생성연산식과 극수의 순환성을 이용하여 GRM상수를 구하는 과정을 기술하였다. 제안된 GRM상수의 생성 방법은 먼저 단변수에 대하여 극수에 따른 상수생성연산식을 구하고 최소의 연산자를 필요로하는 극수를 선정한다. 극수에 따른 GRM 함수의 순환성을 이용하여 앞서 선정된 최적의 극수에 대한 상수생성연산식을 모든 GRM상수의 생성방법에 적용하여 구하며 그림 1.에 상수생성 흐름도를 나타내었다. 이와같은 방법을 적용하면 동일한 상수생성연산식을 사용하므로 연산과정이 간단하며 연산자의 개수를 줄일 수 있어 효과적으로 GRM상수를 생성할 수 있다. GF(3)과 GF(4)에 대한 GRM상수의 생성과정을 예로서 나타내었다.

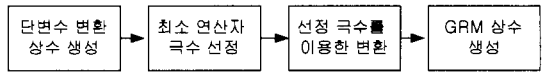

그림 1. 상수 생성 흐름도
fig. 1. Flow diagram for coefficient generation.

1. GF(3)상에서의 GRM 상수의 생성

단 변수에 대한 극수의 순환성을 이용하여 GF(3)상에서의 n=2 인 경우에 대하여 GRM 상수를 구하여 본다. n=2인 경우이므로 3^2개의 극수에 따라 서로 다른 GRM 함수식을 갖으며 이는 극수 0부터 극수 8에 해당하는 함수식을 의미한다. GF(3)에서의 입력원소에 대한 가산과 승산에 대한 연산은 표 2.와 같다.

표 2. GF(3)에서의 연산
Table 2. Operations of GF(3).

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

1.1. 최적의 극수 선정

GF(3)의 경우 단변수에 대한 극수의 상수생성연산식은 표 1.에 나타내었다. 표 1.에 의하여 P=1 또는 P=2의 상수의 변환 과정이 모두 3개의 가산과 1개의 승산으로 구성되므로 P=1 또는 P=2의 상수생성연산

식 중 어느것을 선택하여도 연산시의 복잡도는 서로 일치한다.

1.2. 순환성을 이용한 GRM 상수 생성

2개의 변수 x_1, x_2에 대하여 특정 극수의 변환을 이용한 모든 GRM상수의 생성 과정은 그림 2. ,그림 3. 과 같다. 그림 2.는 P=1에 대한 극수의 순환성을 이용하여 모든 GRM 상수를 구하는 것을 나타내었으며 그림 3.은 P=2에 대한 극수의 순환성을 이용하여 모든 GRM 상수를 구하는 것을 나타내었다.

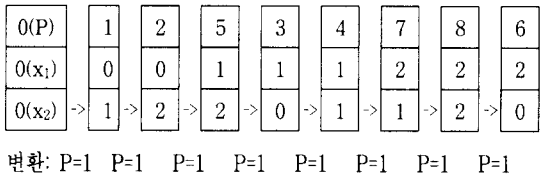

그림 2. 극수의 변환(P=1 경우)
Fig. 2. Changes of Polarity(case P=1).

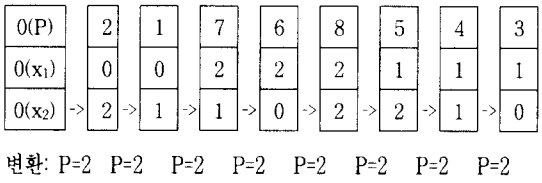

그림 3. 극수의 변환(P=2 경우)
Fig. 3. Changes of Polarity(case P=2).

그림 2., 그림 3.에서 3치 함수의 모든 극수를 구하는 것은 x_1, x_2변수의 P=1에 의한 상수의 변환 과정만을 적용하거나 또는 P=2의 상수의 변환 과정만을 적용하여 모든 극수에 해당하는 상수를 구할 수 있다. P=1 변환의 경우 $(a_1+a_2)+a_0, (a_1+a_2)+a_2$, P=2 변환의 경우 $a_0+a_1, a_1+a_2, (a_0+a_1)+(a_1+a_2)$를 사용하면 3개의 가산을 이용하여 상수를 구할 수 있다.

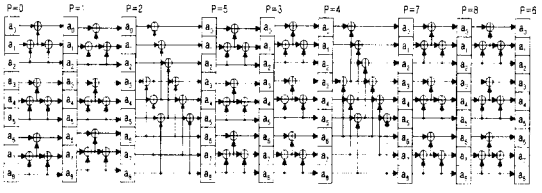

그림 4. GF(3)의 신호 흐름도
Fig. 4. Signal Flow Diagram over GF(3).

그림 4.는 P=1의 변환을 이용한 2변수에 대한 신호의 흐름도를 나타내었다.

[예제 4] 3치 2변수 P=0의 함수가 다음과 같은 경우 GRM상수를 구하여라.

$$f(x) = x_2 + x_2^2 + x_1 + 2x_1x_2 + x_1x_2^2 + x_1^2 + 2x_1^2x_2 + x_1^2x_2^2$$

위의 식을 다시 표현하면 다음과 같다.

$$f(x) = (x_2 + x_2^2) + (1 + 2x_2 + x_2^2)x_1 + (1 + 2x_2 + x_2^2)x_1^2$$

P=1의 변환을 적용하여 구하면 GRM상수는 다음과 같다.

P=0	011 121 121	
P=1	201 111 111	(P=0의 P=1변환)
P=2	021 001 001	(P=1의 P=1변환)
P=5	020 000 001	(P=2의 P=1변환)
P=3	220 000 121	(P=5의 P=1변환)
P=4	120 000 111	(P=3의 P=1변환)
P=7	201 222 111	(P=4의 P=1변환)
P=8	021 002 001	(P=7의 P=1변환)
P=6	011 212 121	(P=8의 P=1변환)

P=2의 변환과정을 적용하여도 같은 GRM상수를 구할 수 있으며 상수생성연산식이 일정하게 적용되어 일관성있게 GRM상수를 구할 수 있다.

2. GF(4)상에서의 GRM 상수의 생성

GF(4)는 GF(2)에 대한 확장체로서 $GF(2^2)$을 나타내며 4개의 원소로 구성되며 각 원소는 기약다항식의 근인 α의 다항식의 형태로 표현되며 일반적인 {0, 1, A, B}로 나타낸다. GF(3)에서는 원소간의 가산과 승산시에 Modulo-3의 연산을 행하지만 GF(4)는 GF(2)에 대한 확장체로서 기약다항식에 의한 Modulo 연산을 행하며 가산과 승산에 대한 연산을 나타내면 다음과 같다.

표 3. GF(4)상의 연산
Table 3. Operations of GF(4).

+	0	1	A	B
0	0	1	A	B
1	1	0	B	A
A	A	B	0	1
B	B	A	1	0

x	0	1	A	B
0	0	0	0	0
1	0	1	A	B
A	0	A	B	1
B	0	B	1	A

단 변수에 대한 극수의 순환성을 이용하여 GF(4)상에서의 n=2인 경우에 대하여 GRM 상수를 구하여 본다. n=2인 경우이므로 4^2개의 극수에 따른 서로 다른 GRM 함수식을 갖으며 이는 극수 0부터 극수 15에 해당하는 함수식을 의미한다.

2.1. 최적의 극수 선정

4치 단변수의 경우 P=0의 RM함수의 일반식은 식(14)과 같이 표현되며 극수 k에 대한 GRM 함수식은 식(15)와 같이 표현된다.

$$f(x)=a_0+a_1x+a_2x^2+a_3x^3 \quad (14)$$

$$\begin{aligned} f(x)&=a_0+a_1(x+k)+a_2(x+k)^2+a_3(x+k)^3 \\ &=(a_0+a_1k+a_2k^2+a_3k^3)+(a_1+2ka_2+3k^2a_3)x \\ &\quad +(a_2+3ka_3)x^2+a_3x^3 \end{aligned} \quad (15)$$

식(12)를 P=0($k=0$)부터 P=3($k=B$)에 대한 상수의 변환과정을 나타내면 표2.과 같다.

표 4. GF(4)상의 극수에 따른 상수의 변환
Table 4. Changes of coefficients to polarity over GF(4).

a_i	P=0(x=x)	P=1(x=x+1)
a_0	a_0	$a_0+a_1+a_2+a_3$
a_1	a_1	a_1+a_3
a_2	a_2	a_2+a_3
a_3	a_3	a_3

a_i	P=2(x=x+A)	P=3(x=x+B)
a_0	$a_0+Aa_1+Ba_2+a_3$	$a_0+Ba_1+Aa_2+a_3$
a_1	a_1+Ba_3	a_1+Aa_3
a_2	a_2+Aa_3	a_2+Ba_3
a_3	a_3	a_3

표 4.에서 보면 4치 단변수의 경우에 P=1의 상수생성연산식이 GRM 상수를 구함에 있어서 가장 적은 연산이 필요함을 알 수 있다. 그러므로 P=1의 경우를 최적의 극수로 선정한다.

2.2 순환성을 이용한 GRM 상수 생성

GF(4)의 경우는 P=1을 적용하여 모든 극수를 구할 수 없으며 이는 다항식에 대한 모듈러의 성질을 갖기 때문이다. 표 3.의 입력변수의 덧셈에 대한 연산을 이용하여 $(f^k(x))^m$에 대한 극수의 변환을 보면 다음과 같다.

$$(f^0(x))^1=f^1(x) \quad (0+1=1)$$
$$(f^1(x))^3=f^2(x) \quad (1+B=A)$$
$$(f^2(x))^1=f^3(x) \quad (A+1=B)$$
$$(f^3(x))^3=f^0(x) \quad (B+B=0)$$

이와 같이 GF(4)에서 모든 극수를 구하기 위해서는 P=1 ($k=1$)과정과 P=3 ($k=B$)의 2가지의 변환 과정을 조합하면 모든 극수의 GRM 상수를 구할 수 있다. 위의 극수의 변환 과정은 역으로도 성립하며 이를 표현하면 다음과 같다.

P=1변환 P=3변환 P=1번환 P=3변환

$$f^0(x)<-->f^1(x)<-->f^2(x)<-->f^3(x)<-->f^0(x)$$

P=1의 변환은 4개의 가산으로 가능하지만 P=3의 변환은 4개의 승산과 5개의 가산을 필요로 하기 때문에 연산시의 간편성을 위하여 변환 과정을 다음과 같이 행한다.

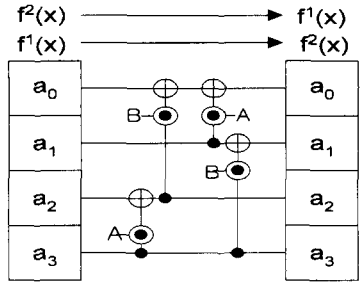

그림 5. 신호흐름도(P=0)
Fig. 5. Signal flow Diagram(P=3).

위와 같은 변환을 행하면 P=3의 변환과정은 각 4개의 승산, 가산을 행하면 된다. 4치 2변수의 P=0의 함수 $f(x_1,x_2)$에 대한 GRM 상수의 생성 과정을 나타내면 다음과 같다.

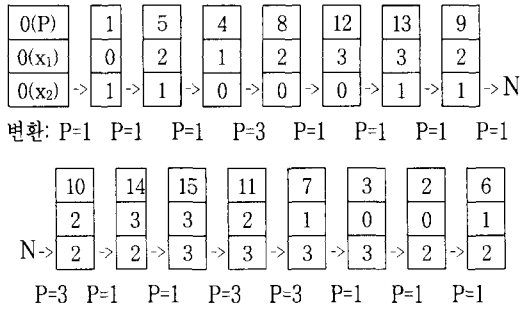

그림 6. GF(4)상의 극수의 변환
Fig. 6. Changes of Polarity over GF(4).

그림 6.에서와 같이 16개의 GRM상수를 생성하는 데는 P=1에 대한 변환과정이 12개, P=3에 대한 변환 과정이 3개가 필요하며 2변수에 대한 신호의 흐름도를 나타내면 그림 7.과 같다.

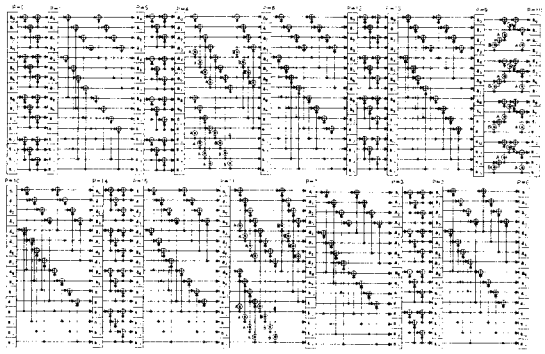

그림. 7. GF(4)의 흐름도
Fig. 7. Signal Flow Diagram over GF(4).

[예제 5] 4치 2변수의 P=0의 상수가 [0AAB A011 10AB A1BA] 인 경우 GRM상수를 구하라.

P=0 0AAB A011 10AB A1BA
P=1 B11B A101 0B1B AB1A
(P=0의 P=1변환)
P=5 B01B 0A1B A001 AB1A
(P=1의 P=1변환)
P=4 1BAB 01AB B111 A1BA
(P=5의 P=1변환)
P=8 ABA1 BBB0 AAB0 A1BA
(P=4의 P=2변환)
P=12 1B1B 1A0A 0B0A A1BA
(P=8의 P=1변환)
P=13 00AB 10AA 11AA AB1A
(P=12의 P=1변환)
P=9 AAB1 BBB0 BAB0 AB1A
(P=13의 P=1변환)
P=10 B001 0BB0 AAB0 AAAA
(P=9의 P=2변환)
P=14 010B 0BBA BABA 000A
(P=10의 P=1변환)
P=15 AABB A11A 001A AAAA
(P=14의 P=1변환)
P=11 A111 0BB0 AAB0 AAAA
(P=15의 P=1변환)
P=7 BA0B B00B BBA1 AAAA
(P=11의 P=2변환)
P=3 1B0B 1AA1 110B AAAA
(P=7의 P=1변환)
P=2 10BB 0BB1 BABB 000A
(P=3의 P=1변환)
P=6 A1BB 0BBB BAB1 000A
(P=2의 P=1변환)

F_n, B_n을 n개의 변수에 대한 극수변환의 순방향과 역방향을 의미하면 F_2의 순방향은 그림 5.에 의하여 P=1 -> P=6, B_2는 P=6 -> P=1의 방향을 의미한다. 2변수의 극수 배열을 이용하여 3변수인 대한 극수의 배열은 다음과 같이한다.

0000000000000000 1111111111111111
0011233223321001 1001233223321100
0110001122333322 2233332211000110
2222222222222222 3333333333333333
0011233223321001 1001233223321100
0110001122333322 2233332211000110

이를 간단히 표현하면 $0F_2$ $1B_2$ $2F_2$ $3B_2$로 표현할 수 있으며 n개의 변수로 확장하면 $0F_{n-1}$ $1B_{n-1}$ $2F_{n-1}$ $3B_{n-1}$로 표현할 수 있다.

V. 비교 및 검토

GRM상수를 구하는 방법은 일반적으로 단변수에 대한 상수의 변환 행렬을 이용하여 이를 kronecker곱을 이용한 변수로 확장하여 행렬연산을 이용하여 구하는 방법[3]이 일반적으로 사용되고 있다. 이러한 방법은 변수의 개수가 증가하면서 행렬의 차수가 증가하는 문제점이 있다. 3치 함수에서 Q.H.Hong[7]이 제안한 Fast 알고리듬과 B.J.Falkowski등[8]이 4치 함수에 적용한 알고리즘의 경우는 연산자의 개수를 감소하였으나 P치의 경우 P-1개의 서로 다른 GRM 상수생성연산식을 적용하였고 상수 생성과정에서 서로 다른 극수의 상수를 참조해야 하며 또한 극수의 연속적 성질을 갖고있지 않기 때문에 상수 생성시 복잡성이 따른다. D.H Green[9,10]은 direct, fast, Gray-Code 알고리즘의 3가지의 방법을 제안하였는데 이러한 방법

은 상당히 효과적으로 GRM상수를 구할 수 있는 방법으로 소개되었다[7]. D.H.Green은 변환행렬에 의한 극수의 변환 관계식을 이용하여 직렬형의 GRM상수를 구하였으며 제안된 논문은 극수의 순환성을 이용하여 직렬형의 GRM상수 생성 과정을 나타내었다. 또한 D.H.Green의 방법보다 연산자의 개수를 줄일 수 있으며 Q.H.Hong과 B.J.Falkowski의 병렬형의 방법보다 연산자의 개수는 상대적으로 많지만 직렬형의 장점인 상수 생성 과정이 간단한 GRM 상수의 생성 방법에 관하여 제안하였다. 제안된 방법은 상수생성연산식의 연산자의 개수를 최소로 하는 극수의 변환을 선택하고 이를 극수의 순환성을 이용하여 모든 GRM상수를 구함에 있어 현재의 극수의 결과를 이용하여 다음의 극수를 구하는 방법을 제안하여 연속적으로 극수를 구하는 경우를 나타내었다. 표 5.는 제안된 방법과 직렬형의 D.H.Green의 Gray-Code알고리즘과 병렬형의 Q.H.Hong,B.J.Falkowski의 GF(3), GF(4)의 경우에 대하여 비교를 나타내었다.

표 5. GF(3), GF(4)상의 비교 표
Table 5. Comparison Table over GF(3), GF(4).

n		D.H.Green		Q.H.Hong
		GF(3)	GF(4)	GF(3)
1	가산	6	12	4
	승산	2	4	0
2	가산	72	240	40
	승산	24	80	0
n≥3	가산	$3^n x(3^n-1)$	$(4^n-1)4^n$	(7^n-3^n)
	승산	가산/3	$(4^n-1)4^n/3$	0
사용연산식		1	2	2
상수생성		직렬형	직렬형	병렬형
상수참조		간단	간단	복잡

n		B.J.Falkowski	제안된 알고리듬	
		GF(4)	GF(3)	GF(4)
1	가산	12	6	12
	승산	4	0	4
2	가산	204	72	240
	승산	48	0	48
n≥3	가산	$\frac{4}{3}(13^n-4^n)$	$(4^n-1)4^n$	$(4^n-1)4^n$
	승산	$\frac{3}{8}(3^n-1)4^n$	0	$(4^{n-3}\times 12+\sum_{n=3}^{n}4^{n-3})4^n$
사용연산식		3	1	2
상수생성		병렬형	직렬형	직렬형
상수참조		복잡	간단	간단

Ⅵ. 결 론

본 논문은 GF(p)상의 다치논리함수의 GRM상수 생성방법에 관한 방법을 제안하였다. GRM상수 생성시 단 변수에 대한 극수에 따른 상수생성식을 이용하여 이를 n변수로 확장하였다. P치 함수의 경우 상수생성연산식 가장 적은 연산자를 갖는 극수의 변환 1개를 선택하여 모든 GRM상수를 구하는 과정에 적용하였으며 확장체($p=q^m$)인 경우는 1개 이상의 극수의 변환 과정을 적용해야한다. 제안된 논문은 기 발표된 논문에 비하여 동일한 상수생성연산식을 최소로하는 극수의 연산식을 선정하여 모든 GRM상수 생성시에 적용함으로서 연산과정의 효율을 높일 수 있으며, 극수에 따른 상수 생성시에 연속성을 유지할 수 있고 연산자의 수를 줄일 수 있는 방법으로 사료된다. $GF(q^m)$으로 확장시 연속성을 유지하기 위한 극수의 배열에 관한 방법이 계속 되어야할 연구 과제이다.

참 고 문 헌

[1] K. C. Sith, "Multiple-valued logic : a tutorial and appreciation, "computers, pp. 17-27, Apr, 1988.

[2] D. Etiemble, "On the Performance of the Multivalued intergrated Circuits : Past, Present and future," ISMVL 92, pp.154-164, Sendai japan, May, 1992.

[3] Davio Green "Modern Logic Design", Addision-Wesley publishing co, 1986.

[4] T.Sasao, "Calculation of Reed-Muller-Fourier Coefficients of Multiple-Valued Functions through Multiple-Place Decision", IEEE Proc. of International Symposium on Multiple-Valued Logic, Boston, Massachusetts, USA, pp.82-88, May 1994.

[5] B. Harking and C. Moraga, "Efficient Derivation of Reed-Muller Expansions in Multiple-Valued Logic System", IEEE Proc. of International Symposium on Multiple-Valued Logic, Sendai Japan,. pp.436-441, May. 1992.

[6] Z.Zilic and Z.G. Vranesic, "New Interpolation Algorithms for Multiple-

Valued Reed-Muller Forms", IEEE Proc. of International Symposium on Multiple -Valued Logic, SANTIAGO de COMPOSTELA, Spain, pp.16-23, May. 1996.

[7] Q. H. hong, B. C. Fei, H. M .Wu, M. A. Perkowski, N. Zhaung "Fast Synthesis for Ternary Reed-Muller Expansion", ,IEEE Proc. of International Symposium on Multiple-Valued Logic, Sacramento, California, USA, pp.14-16, May 1993.

[8] B, J, Falkowski, S. Rahardja, "Efficient Algorithm for Generation of Fixed Polarity Quaternary Reed-Muller Expansions", ,IEEE Proc. of International Symposium on Multiple -Valued Logic, Bloomington, Indiana, USA, pp.158-161 May, 1995.

[9] D. H. Green, "Ternary Reed-Muller switching functions with fixed and mixed polarity", Int. J. Electronics, vol.67, no.5, pp.761-775 Nov.1989.

[10] D. H. Green, "Reed-Muller expansions with fixed and mixed polarits over GF(4)", IEE. Porc., Part E, vol. 137, no. 5, Sept. 1990.

저 자 소 개

申 富 植(正會員)

1965년 1월 14일생. 1987년 인하대학교 전자공학과 졸업(학사). 1989년 인하대학교 대학원 전자공학과 졸업(석사). 1989 ~ 1995년 LG산전 선임연구원. 1995 ~ 현재 인하대학교 전자공학과 박사과정

沈 載 煥(正會員)

1947년 3월 19일생. 1976년 인하대학교 전자공학과 졸업. 1982년 숭실대학교 전자공학과 졸업(석사)(현재). 1996~인하대학교 대학원 전자공학과 박사과정. 1978년~시립인천전문대학 통신과 교수

金 興 壽(正會員) 第 34卷 C編 第 6號 參照