유한체 P=3인 경우의 GRM에 관한 연구

박춘명*

*한국교통대학교

A Study on the GRM in case of P=3 over Finite Fields

Chun-Myoung Park*

*Korea National University of Transportation

E-mail : cmpark@ut.ac.kr

요 약

본 논문에서는 유한체 P=3에서 GRM 상수의 극수가 가진 순환적인 성질을 이용하여 새로운 GRM 상수 생성에 대한 방법을 제안하였으며, 또한, 극수들을 비교하여 최적의 GRM 상수를 생성하는 방법에 대해서 논의하였다.

ABSTRACT

This paper present a method of GRM constant generation in case of prime number P=3 over finite fields. Also we discuss the method which is the optimal GRM generation compare with polarity. The proposed method is the efficiency and optimization compare with earlier method.

키워드

Finite fields, GRM, polarity, optimal method

Ⅰ. 서 론

최근의 초고도화 정보화 시대에는 그 이전에 비해 방대하고 다양한 정보를 취합하여 분석하고 이를 종합하여 새로운 정보를 생성하는 새로운 형태의 정보화 시대가 요구되고 있다.[1-3]

본 논문에서는 유한체 P=3에서 GRM 상수의 극수가 가진 순환적인 성질[4-6]을 이용하여 새로운 GRM 상수 생성에 대한 방법을 제안하였으며, 또한, 극수들을 비교하여 최적의 GRM 상수를 생성하는 방법에 대해서 논의하였다.

Ⅱ. GF(3)에서의 극수의 순환성

단일변수에 대한 GRM 함수는 식(1)과 같이 표현 할 수 있다.

$$f(x) = c_0 + c_1 x' + c_2{}'^2 \tag{1}$$

GF(3)상에서 입력변수 x의 보수에 해당하는 $\overline{x}$는 x+1, x+2의 두 가지 경우이며 각각 극수 p=1)과 p=2를 의미한다.

식(1)의 x에 보수인 x+k(k=1 또는 2)를 대입하여 x' 항을 표현하면 다음 식(2)와 같다.

$$\begin{aligned} f(x) &= c_0 + c_1(x+k) + c_2(x+k)^2 \\ &= (c_0 + c_1 k = c_2 k^2) + (c_1 + c_2)x + c_2 x^2 \end{aligned} \tag{2}$$

식(2)를 행렬로 표현하면 식(3)과 같이 표현 할 수 있다.

$$[1\ x'\ x'^2] = [1\ x\ x^2]\begin{bmatrix} 1 & k & k^2 \\ 0 & 1 & 2k \\ 0 & 0 & 1 \end{bmatrix} \tag{3}$$

식(3)에 역변환을 행하면 식(4)와 같다.

$$[1\,x\,x^2]=[1\,x'\,x'^2]\begin{bmatrix}1&2k&k^2\\0&1&k\\0&0&1\end{bmatrix} \quad (4)$$

식(4)를 식(1)에 대입하면 다음 식(5)와 같다.

$$f(x)=c'_0+c'_1x+c'_2x^2 =[1\,x'\,x'^2]\begin{bmatrix}1&2k&k^2\\0&1&k\\0&0&1\end{bmatrix}\begin{bmatrix}c_0\\c_1\\c_2\end{bmatrix} \quad (5)$$

III. 극수의 순한성을 이용한 GRM 상수 생성

본 장에서는 극수의 순환성을 이용하여 GRM 상수를 구하는 방법에 있어서 상수의 연산과정이 일관성을 갖는 방법을 적용하여 GRM 상수를 구할 수 있는 직렬형의 방법에 대하여 나타내었다. 단일 변수에 대한 상수 GRM 상수를 구하여 본다.

3.1 변환 회로 설계

GF(3)의 경우 단일 변수에 대한 극수의 상수 생성은 다음 식(6)과 같은 식에 의하여 p=1 또는 p=2 상수의 변환 과정은 다음과 같다.

$$c^{(1)}=c_0+2c_1+c_2,\ c^{(1)}=c_1+c_2,\ c^{(1)}=c_2$$
$$c^{(2)}=c_0+c_1+c_2,\ \ c^{(2)}=c_1+2c_2,\ c^{(2)}=c_2 \quad (6)$$

위의 식에서 보면 극수 p=1과 p=2를 구하기 위한 연산자의 개수는 모두 3개의 가산과 1개의 승산으로 구성되므로 p=1 또는 p=2의 상수 생성 연산식 중 어느 것을 선택하여도 연산의 복잡도는 서로 동일하다. 하지만 회로구현 측면에서 볼 때, 승산기의 사용은 가산기보다 더 복잡도가 커지므로 승산기를 사용하지 않고 가산기만을 사용할 수 있다. 극수 p=1의 상수 $c_0^{(1)}$를 구하는데 있어서 c_0+c_1과 c_1+c_2의 가산을 하면 3개의 가산기로만 원하는 상수를 구할 수 있게 되고 p=2의 경우에도 마찬가지로 3개의 가산기로 원하는 상수를 구할 수 있으며 이런 변환들을 각각 p=1, p=2 변환이라 한다.

IV. 극수 변환회로를 이용한 GRM 상수 생성

GF(p)에서 p=k 변환을 p-1회 반복하게 되면 모든 극수의 GRM 상수를 구할 수 있었다. 2변수 함수에서 변수x_1,x_2에 대하여 특정 극수의 변환을 이용한 모든 GRM상수의 생성 과정을 변수 x_1,x_2에 대하여 p=0의 상수로부터 p=6까지 변수 x_1,x_2에 대한 극수의 변환 과정을 나타내었다. p=0에서 p=1의 변환은 변수x_1에 대해 p=1변환을 적용하였고, p=2에서 p=5까지 극수의 변환은 변수x_2에 p=1변환이 적용되었다. 모든 극수를 구하는 과정은 x_1 또는 x_2 변수에 대하여 p=1 변환 과정을 적용하면 모든 극수의 상수를 구할 수 있다.

V. 결론

본 논문에서는 유한체 P=3에서 GRM 상수의 극수가 가진 순환적인 성질을 이용하여 새로운 GRM 상수 생성에 대한 방법을 제안하였으며, 또한, 극수들을 비교하여 최적의 GRM 상수를 생성하는 방법에 대해서 논의하였다.

참고문헌

[1] Sasao. T., Debnath, D., “An exact minimization algorithm for generalized Reed-Muller expressions“, Proc. Asia-Pacic Conference on Circuits and Systems, APCCAS 2010, pp. 460-465, 2010.

[2] R.J. McEliece, “Finite Fields for Computer Scientists and Engineers“, Kluwer Academic Publishers, 2009.

[3] Xu, L., Almaini, A.E.A., Miller, J.F., McKenzie, L., “Reed-Muller universal logic module networks“, IEE Proc. Computers and Digital Techniques, Part E, Vol. 140, No. 2, pp.105-108, 2010.

[4] Wu., H., Perkowski, M.A., Zeng, X., Zhuang., N., “Generalized partially-mixed-polaty Reed-Muller expansion and its fast computation“, IEEE Trans. On Computers, vol. 45, No. 9, pp.1084-1088, 2012.

[5] Stankovic, R.S., Moraga, C., Astola, J.T., “Reed-Muller expressions in the Previous Decade“, Proc. 5th GRM Conference, pp., 2011.

[6] X.Wu, X.Chen, S.L.Hurst, “Mapping of Reed-Muller coefficients and the minimisation of exclusive OR-switching functions“, IEE Proceedings, vol. 129, Pt. E, No. 1, pp.101-105, Jan. 2011.