論文 78-15-5-6

Lagrange 補間法에 依한 Galois 스윗칭函數 構成

(Derivation of Galois Switching Functions by Lagrange's Interpolation Method)

金 興 壽
(Kim, Heung Soo)*

要 約

本 論文에서는 Galois 스윗칭函數를 구하기 위해서 任意의 有限體上에서 定義되는 Galois 體의 성질을 설명하였고, 任意의 有限體上에서의 演算方法을 밝혔다. 그리고 Lagrange 補間法에 依한 多項式이 有限體上에서 展開될 수 있음을 證明하였다. 이 結果를 適用하여 單一變數를 갖는 Galois 스윗칭 函數를 誘導하고 多値論理回路를 實現하였다.

Abstract

In this paper, the properties of Galois fields defined over any finite field are analyzed to derive Galois switching functions and the arithmetic operation methods over any finite field are showed. The polynomial expansions over finite fields by Lagrange's interpolation method are derived and proved. The results are applied to multivalued single variable logic networks.

1. 序 論

集積回路의 急進的인 發展은 組織的이고 간편한 論理設計를 要求하게 되었다. 특히 2進系統에서의 端子數制限問題, 進法間의 變換問題等은 多値論理를 導入함으로써 改善할 수 있는 것이다.[1] 더우기 多値論理理論을 論理設計에 이용한다면 decoding 過程이 경제적으로 되며 集積回路製作이 쉬워지고 모듈 代數에 의한 스윗칭函數의 實現이 容易하며 缺陷檢出이 또한 간편하고 많은 情報量을 다루는 通信回路에 有利한 利點[2]을 가지고 있다. 또한 디지털 回路의 가격감소와 앞으로 이들 가격의 계속적인 저하추세는 더욱 信賴性이 좋고 저렴한 多値論理回路의 開發이 예견 된다.

이러한 多値論理理論을 有限體上에서 解析하여 設計한 것은 비교적 最近의 硏究로써 K.S. Menger[3]는 Boolean difference 를 有限體로 擴張하여 Galois 스윗칭函數를 多項式형태로 얻은 후 Fourier 變換에 對應시켜 그 多項式의 論理回路實現을 이행하였다. 그 후 B. Benjauthrit 와 I.S. Reed[2]는 Menger 가 구한 多項式을 多値多變數인 경우로 擴張시켰다. 반면에 D.K. Pradhan[4]은 Galois 스윗칭函數를 一般化시킨 Reed Muller 展開式에서 係數를 결정짓는 새로운 數學的인 結果를 얻었고, T.C. Wesselkamper[5]는 divided difference 를 이용한 Newton 의 補間法으로 有限體上의 多項式을 展開시켰다.

本 論文에서는 Lagrange 의 補間法을 이용하여서 多値單一變數에 대한 Galois 스윗칭函數를 구하였다. Galois 體上에서 필요한 성질을 2節에서 略述하였고, 3節에서 Galois 스윗칭函數를 構成시킬 수 있는 多項式을 구하였다. 3節의 結果를 4節에서 多値論理回路實現에 適用시켰고 그 結果를 5節에서 檢討하였다.

2. Galois 體의 性質

體 E 를 p 개의 要素로 구성된 有限體 F 의 n 次有限擴張體라고 하면 體 E 는 陽의 整數 n 에 대하여 정확히 p^n 개의 要素를 갖는다. 다시 말하여 p 를 素數 n 를 陽의 整數라고 놓을때 p^n 개의 要素로 구성되는 有限體가 반드시 存在한다. 이 有限體를 임명 Galois 體라 하

* 正會員, 韓國航空大學 (Dept. of Electronics Engineering, Civil Aviation College)
接受日字 : 1978年 7月 25日

며 $GF(p^n)$으로 表記한다. 例로써 $GF(2)$라면 {0,1}인 2개의 要素로 구성되고, $GF(2^2)$는 {0,1}인 要素가 이룰 수 있는 集合 {00,10,01,11}인 4개의 要素로 구성된다. 반면에 $GF(3^2)$는 {00,10,01,12,22,20,02,21,11}인 9개의 要素로 구성된다. 이러한 $GF(p^n)$는 다음法則[4], 즉

〔交換法則〕; $a+b=b+a$, $a\cdot b=b\cdot a$ $\forall a,b\in GF(p^n)$

$a+0=0+a$ $\forall a\in GF(p^n)$

〔結合法則〕; $a+(b+c)=(a+b)+c$, $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ $\forall a,b,c\in GF(p^n)$

〔分配法則〕; $a\cdot(b+c)=a\cdot b+b\cdot c$ $\forall a,b,c\in GF(p^n)$

을 만족하는 Abel群 다시 말해서 交換的인 環이어야 하며 동시에

1) p^n개의 要素로 구성되고

2) 加算(+)과 乘算(·)이 성립하며

3) 0要素와 1인 要素가 存在할 수 있는 體이다.

다음에 本 論文의 結果를 얻기 위해서 사용되는 $GF(p^n)$의 중요한 성질을 든다.

성질 1 ; a) $\underbrace{1+1+\cdots+1}_{p}=0$

b) $pa=0$

성질 2 ; $\forall a\in GF(p^n)$이고, $a\neq 0$에 대하여

$$a^{p^n}=a,\quad a^{p^n-1}=1$$

성질 3 ; $\forall a,b\in GF(p^n)$이고, 陽의 整數 n에 대하여

$$(a+b)^{p^n}=a^{p^n}+b^{p^n}$$

성질 4 ; $\forall\alpha\in GF(p^n)$에 대하여

$$\alpha^i\alpha^j=\alpha^{i+j(\mathrm{mod}\,p^n-1)}$$여기서

mod는 모듈,

성질 5 ; $\forall a,b\in GF(p^n)$이고, 모듈 k일때

$a+b<k$라면 $a+b=a+b$

$a+b\geq k$라면 $a+b=a+b-k$

$$a\cdot b=\frac{a\cdot b}{k}$$

성질 6 ; $GF(p^n)$의 要素들은 $GF(p)$上에서 最高 $n-1$次인 多項式에 對應시킬 수 있으며 이런 多項式의 두 乘算은 $GF(p)$上에서 n次既約多項式에 모듈演算을 導入하여 계산한다.

$GF(2^n)$를 例로 든다면 $n=2$일때 $1+x+x^2$, $n=3$일때 $1+x+x^3$, $n=4$일때 $1+x+x^4$인 既約多項式이 各各 存在한다.[6]

앞에서 설명한 성질을 이용하여 $GF(2^2)$와 $GF(2^3)$에서 各要素들의 加算과 乘算을 행하면 표 1,2와 표 3,4와 같이 된다.

위의 표를 설명하기 위해서 몇개를 例로 든다면 표 1,2에서는 {($00=0=e_0$), ($10=1=e_1$), ($01=x=e_2$), (11

표 1. $GF(2^2)$에서 모든 要素의 加算
Table 1. Addition defined for the four elements in field $GF(2^2)$.

+	e_0	e_1	e_2	e_3
e_0	e_0	e_1	e_2	e_3
e_1	e_1	e_0	e_3	e_2
e_2	e_2	e_3	e_0	e_1
e_3	e_3	e_2	e_1	e_0

표 2. $GF(2^2)$에서 모든 要素의 乘算
Table 2. Multiplication defined for the four elements in field $GF(2^2)$.

·	e_0	e_1	e_2	e_3
e_0	e_0	e_0	e_0	e_0
e_1	e_0	e_1	e_2	e_3
e_2	e_0	e_2	e_3	e_1
e_3	e_0	e_3	e_1	e_2

표 3. $GF(2^3)$에서 모든 要素의 加算
Table 3. Addition defined for the eight elements in field $GF(2^3)$.

+	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_0	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	e_0	e_6	e_5	e_7	e_3	e_2	e_4
e_2	e_2	e_6	e_0	e_4	e_3	e_7	e_1	e_5
e_3	e_3	e_5	e_4	e_0	e_2	e_1	e_7	e_6
e_4	e_4	e_7	e_3	e_2	e_0	e_6	e_5	e_1
e_5	e_5	e_3	e_7	e_1	e_6	e_0	e_4	e_2
e_6	e_6	e_2	e_1	e_7	e_5	e_4	e_0	e_3
e_7	e_7	e_4	e_5	e_6	e_1	e_2	e_3	e_0

표 4. $GF(2^3)$에서 모든 要素의 乘算
Table 4. Multiplication defined for the eight elements in field $GF(2^3)$.

·	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_0	e_0	e_0	e_0	e_0	e_0	e_0	e_0	e_0
e_1	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_2	e_0	e_2	e_3	e_6	e_7	e_1	e_4	e_5
e_3	e_0	e_3	e_6	e_4	e_5	e_2	e_7	e_1
e_4	e_0	e_4	e_7	e_5	e_2	e_6	e_1	e_3
e_5	e_0	e_5	e_1	e_2	e_6	e_7	e_3	e_4
e_6	e_0	e_6	e_4	e_7	e_1	e_3	e_5	e_2
e_7	e_0	e_7	e_5	e_1	e_3	e_4	e_2	e_6

$=1+x=e_3)\}$로 $GF(2^2)$上 4개의 要素를 $GF(p)$上의 多項式 $P(x)=a_0+a_1x$에 各各 對應시켰다. 그러므로 표 1에서 $e_1+e_3=1+1+x=2+x=x=e_2$, 표 2에서는 $e_2\cdot e_3=x(x+1)=x^2+x$는 $\mathrm{mod}(x^2+x+1)$에서 1인 e_1으로 된다. 마찬가지로 표 3,4에서는 $GF(2^3)$上 8개의 要素를 $GF(p)$上의 多項式 $P(x)=a_0+a_1x+a_2x^2$에 $\{(000=0=e_0)$, $(100=1=e_1)$, $(010=x=e_2)$, $(001=x^2=e_3)$, $(011=x+x^2=e_4)$, $(101=1+x^2=e_5)$, $(110=1+x=e_6)$, $(111=1+x+x^2=e_7)\}$과 같이 各各 對應시켜서 계산한다. 즉, 표 3에서 $e_4+e_5=x+x^2+1+x^2=1+x+2x^2=1+x=e_6$, 표 4에서 $e_4\cdot e_5=(x+x^2)\cdot(1+x^2)=x+x^3+x^2+x^4$에 $\mathrm{mod}(1+x+x^2)$을 導入하면 $e_4\cdot e_5=x+(x+1)+x^2+x(x+1)=x+1=e_6$로 된다. 나머지 演算도 이와 마찬가지로 계산된 것이다. 다시 말하면 $GF(p^n)$에서의 모든 要素들을 $GF(p)$上의 多項式에 各各 對應시킨 후 n에 해당하는 既約多項式을 모듈로 택하여 계산해 주면 $GF(p^n)$에서 모든 要素들의 加算과 乘算이 이루어지는 것이다.

3. Lagrange 補間法에 依한 多項式의 展開

獨立變數$(x_0, x_1, \cdots, x_m)$가 從屬變數$(y_0, y_1, \cdots, y_m)$에 各各 對應되여 주어진 경우 이들 變數간에는 最高 m次인 1개의 多項式이 存在하며 이는 다음과 같은 Lagrange의 補間法으로 證明된다.[6]

定理(Lagrange의 補間法) : p를 素數, n를 陽의 整數로 놓을 때 $F(x):\{x_0, x_1, \cdots, x_m\}, (y_0, y_1, \cdots, y_m)\}\rightarrow GF(p^n)$시키는 函數 $F(x)$는

$$\begin{aligned} &F(x_0)=y_0\\ &F(x_1)=y_1\\ &\cdots\cdots\cdots\\ &F(x_m)=y_m \end{aligned} \qquad (1)$$

을 만족하는 最高 m次인 多項式 $F(x)$로 存在한다.

〔證明〕 : 다음과 같은 多項式을 생각하자. 즉

$P_i(x)=(x-x_0)(x-x_1)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_m)$

만일 $i\neq j$라면 $P_i(x_j)=0$이 되지만,

$i=j$라면 $P_i(x_j)\neq 0$이 된다.

그러므로 $L_i=P_i(x_i)$라 놓는다면 $L_i\neq 0$이므로

$$F(x)=\sum_{i=0}^{m}\frac{y_i}{L^i}P_i(x)$$

$$=\sum_{i=0}^{m}y_i\left(\prod_{j\neq i}\frac{x-x_j}{x_i-x_j}\right) \qquad (2)$$

여기서 $P_i(x_j)=0$이므로 $i=0,1,\cdots,m$에 대해 $F(x_i)=y_i$로 된다. 따라서 $F(x_0)=y_0$, $F(x_1)=y_1$, $,F(x_m)=y_m$을 만족하는 多項式 $F(x)$가 存在한다. (證明끝)

앞의 多項式 (2)를 정리하면

$$\begin{aligned} F(x)=&\frac{(x-x_1)(x-x_2)(x-x_3)\cdots(x-x_m)}{(x_0-x_1)(x_0-x_2)(x_0-x_3)\cdots(x_0-x_m)}y_0\\ &+\frac{(x-x_0)(x-x_2)(x-x_3)\cdots(x-x_m)}{(x_1-x_0)(x_1-x_2)(x_1-x_3)\cdots(x_1-x_m)}y_1\\ &+\frac{(x-x_0)(x-x_1)(x-x_3)\cdots(x-x_m)}{(x_2-x_0)(x_2-x_1)(x_2-x_3)\cdots(x_2-x_m)}y_2\\ &+\cdots\cdots\cdots\cdots\cdots\cdots\\ &+\frac{(x-x_0)(x-x_1)(x-x_2)\cdots(x-x_{m-1})}{(x_m-x_0)(x_m-x_1)(x_m-x_2)\cdots(x_m-x_{m-1})}y_m \end{aligned} \qquad (3)$$

과 같은 Lagrange의 補間式을 얻게 된다.

이 式 (3)은 體 E를 구성할 수 있는 整數領域內에서 $\{(x_i, y_i)\}=\{(x_0, y_0), (x_1, y_1), \cdots, (x_m, y_m)\}$와 같은 對應關係를 갖는 變數集合 $\{(x_i, y_i)\}$를 Galois體에 對應시킬 때에는 반드시 整數領域內에 주어진 變數間의 對應關係를 모두 만족시키는 Galois스윗칭函數가 最高 m次인 1개의 多項式으로 存在함을 의미하는 것이다.

4. 多値論理回路에의 適用

3節에서 證明한 定理가 多値單一變數에 대한 Galois스윗칭函數를 구하기 위해서 어떻게 適用되는 가를 例를 들어서 설명하면 다음과 같다.

먼저 표 5[5]와 같이 入力變數 x가 5개의 서로 다른 信號레벨을 갖는 경우의 Galois스윗칭函數는 $GF(5)$에서 구한다. 표 5의 變數値를 式 (3)에 代入하면

표 5. $GF(5)$의 例
Table 5. An example of $GF(5)$.

x	$y(x)$
0	0
2	0
4	0
1	0
3	1

다음과 같이 된다.

$$\begin{aligned} F(x)&=\frac{(x-x_0)(x-x_1)(x-x_2)(x-x_3)}{(x_4-x_0)(x_4-x_1)(x_4-x_2)(x_4-x_3)}y_4\\ &=\frac{x(x-2)(x-4)(x-1)}{3\cdot(3-2)(3-4)(3-1)}\cdot 1 \end{aligned}$$

그런데 $GF(p^n)$에서 $p^n=5$가 되는 p나 n의 값은 有限體上에서 定할 수 없으므로 모듈 5를 導入하여 윗式을 계산하면 다음과 같다.

$$F(x)=\frac{x(x+3)(x+1)(x+4)}{3\cdot1\cdot4\cdot2}$$

$$=4x(x+1)(x+3)(x+4) \quad (4)$$

式 (4)는 표 5에 주어진 모든 變數간의 對應關係를 모두 만족하는 4次 多項式이다. 즉 $x=x_4=3$인 경우 $F(3)=4\cdot3(3+1)(3+3)(3+4)=12\cdot4\cdot6\cdot7=2\cdot4\cdot1\cdot2=1$ (모듈 5)로 되고 나머지 變數에 대한 出力函數는 모두 0이 되여 표 5를 만족하는 Galois 스윗칭函數를 式 (4)로 얻게된다. 그리고 2節에 실은 有限體上의 성질을 만족하는 Galois 加算 및 乘算게이트를 이용한다면 그림과 같은 多値論理回路로 實現시킬 수 있다.

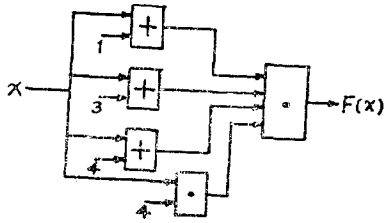

그림 1. 표 5의 論理回路實現
Fig. 1. Logic network realization of Table 5.

다음은 표 6[5]에서와 같이 4개의 要素로 구성되는 $GF(4)$인 경우로써 표 1,2의 要素를 {0→e_0, 1→e_1, 2→e_2, 3→e_3}로 各各 對應시킨 후 式 (3)을 계산하면 다음과 같다.

$$F(x)=\frac{(x-x_0)(x-x_1)(x-x_3)}{(x_2-x_0)(x_2-x_1)(x_2-x_3)}y_2$$

$$=\frac{(x-e_0)(x-e_1)(x-e_3)}{(e_2-e_0)(e_2-e_1)(e_2-e_3)}e_1$$

표 6. $GF(2^2)$의 例
Table 6. An example of $GF(2^2)$.

x	$y(x)$
0	0
1	0
2	1
3	0

이 式에 표 1,2의 演算結果를 適用시키고, 또 $GF(4)=GF(2^2)$에서 $-1\equiv1$이므로 윗式을 정리하면 다음과 같이된다.

$$F(x)=e_1x(x+e_1)(x+e_3)$$

$$=x^3+2x^2+3x \quad (5)$$

이 結果式은 표 6을 만족하는 Galois 스윗칭函數로써 이 式의 論理回路實現은 그림 2과 같다.

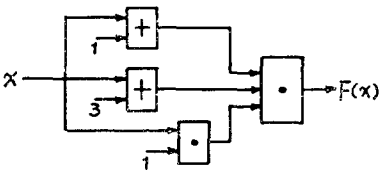

그림 2. 표 6의 論理回路實現
Fig. 2. Logic network realization of Table 6.

다음 표 7[3]은 8개의 入力信號레벨을 變數値로 사용할 수 있는 $GF(2^3)$에서의 Galois 스윗칭函數 구성을 例示키 위한 것으로 式 (3)에 이 표의 값을 代入하여 정리하면 다음과 같다.

$$F(x)=(x+e_1)(x+e_5)[e_7x^4+e_5x^3+e_4x^2+e_1]$$

$$=(x+e_1)(x+e_5)[e_7x^2(x+e_3)(x+e_4)+e_1] \quad (6)$$

표 7. $GF(2^3)$의 例
Table 7. An example of $GF(2^3)$

x	$y(x)$
e_0	e_5
e_1	e_0
e_2	e_6
e_3	e_5
e_4	e_2
e_5	e_0
e_6	e_2
e_7	e_6

표 7의 모든 條件을 만족하는 이 結果式을 論理回路로 實現한 것이 그림 3이다.

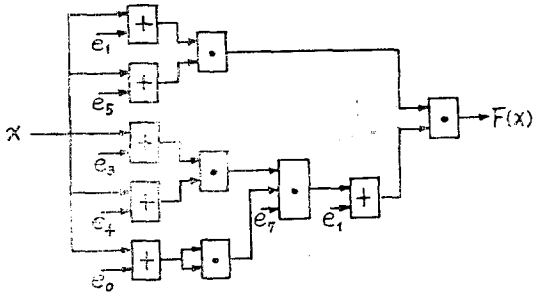

그림 3. 표 7의 論理回路實現
Fig. 3. Logic network realization of Table 7.

앞으로 2節에서 설명한 有限體의 성질을 만족하면서 信賴性이 좋고, 妥當한 演算速度를 갖는 多値信號레벨素子[3]가 開發된다면 틀림없이 앞에서 설명한 多値論理回路實現方法은 效果的인 方法이 될 것이다.

그러나 Galois스윗칭函數式의 簡略化 表現은 論理回路設計나 製作에 큰 영향을 미치므로 效果的인 因數分解方法이 硏究되어야 한다.

5. 檢討 및 結論

p가 素數이고 n가 陽의 整數인 有限體 $GF(p^n)$에서 모든 論變變數와 論理函數와의 관계를 만족시키는 函數 즉 $F: GF(p^n)\rightarrow GF(p^n)$인 $F(x)$를 Menger[3]와 Benjauthrit, Reed[2]는

$$f(0)=F(0)$$

$$f(i)=\sum_{r=0}[F(0)-F(r)]r^{-i} \quad 0<i<k \qquad (7)$$

인 係數函數를 만족하는 多項式

$$F(x)=\sum_{i=0}^{p^n-1} f(i)x^i \qquad (8)$$

으로 구하였다. 이들의 方法에 의하면 式 (7)의 係數函數를 구하는데 많은 시간과 노력이 必要하게 되며 多變數로 擴張하였을 경우[5] 엄청난 계산을 하여야 한다. 또한 從屬變數가 divided difference에 포함되어 계산되는 Newton 補簡法에 依한 Wesselkamper[5]의 多項式 展開는 divided difference를 계산하기 위해서 표를 따로이 작성하고 이 표로부터 多項式을 구하여야 한다.

이와같이 Galois스윗칭函數를 구하는 방법은 最近 여러 編의 論文에 發表되였지만[2),3),4),5)] 本 論文에서는 Lagrange 補簡法에 의해서도 單一變數에 대한 Galois스윗칭函數를 구할 수 있음을 提示함과 동시에 이 方法에 의하면 從屬變數 자체가 式 (2)에 포함되므로 式 (2)의 계산만으로 多項式을 구할 수 있음을 보였다 다시 말하면 係數函數式을 따로이 設定한다든가 또는 divided difference 표를 작성해야 하는等의 手苦없이 비교적 간단하게 그 결과를 얻을 수 있음을 提示하였다.

本 論文에서 취급한 多値 單一變數인 경우에 대한 解析方法을 앞으로는 多値 2變數인 경우로 擴張시킬 계획이며 아울러 Galois스윗칭 函數를 가장 效果的으로 因數分解시킬 수 있는 技法도 또한 硏究할 계획이다.

參 考 文 獻

1. I.G. Rosenberg: "Some algebraic and combinatorial aspects of multiple-valued circuits," Proc. of the sixth Int. Symp. on Multiple-Valued Logic, 1976.
2. B. Benjauthrit and I.S. Reed: "Galois switching functions and their applications," IEEE Trans. Compt., vol. C-25, pp. 78-86, Jan., 1976.
3. K.S. Menger: "A transform for logic networks," IEEE Trans. Compt., vol. C-18, pp. 241-250, Mar., 1969.
4. D.K. Pradhan: "A theory of Galois switching functions," IEEE Trans. Compt., vol. C-27, pp. 239-248, Mar., 1978,
5. T.C. Wesselkamper: "Divided difference methods for Galois switching functions," IEEE Trans. Compt., vol. C-27, pp. 232-238, Mar., 1978.
6. G. Birkhoff and T.C. Bartee:"Modern applied algebra," New York, McGraw-Hill, 1970.
7. J.B. Fraleigh: "A first course in abstract algebra," Addison-Wesley, 1974.
8. F.J. Scheid: "Elements of finite Mathematics," Addison-Wesley, 1962.
9. M.L. Keedy: "Number system: A modern introduction." Addison-Wesley, 1965.
10. J.B. Scarborough: "Numerical Mathematical Analysis," John Hopkins press, 1962.