Galois스윗칭函数의 構成理論
(A Constructing Theory of Galois Switching Functions)

金 興 壽*
(Kim, Heung Soo)

要 約

本 論文에서는 Galois스윗칭函數를 構成하기 위한 하나의 方法을 提示하였다. 먼저 單一變數에 대한 Lagrange 補間法을 多項式 形態로 展開시켜서 Galois 스윗칭函數를 構成한 다음 2變數에 대한 構成理論을 밝혔다. 이를 바탕으로 하여 多變數에 대한 Galois스윗칭函數를 構成하였다. 構成理論을 뒷받침하기 위한 例題를 他論文에서 引用하였으며 그 結果가 既存論文의 結果와 同一함을 보였다.

Abstract

In this paper, a method for constructing Galois switching functions is presented. Single variable Galois switching function is constructed at first by developing Lagrange's interpolating formula into polynomial forms and then the constructing theory for two variables is developed. With these developed theory, multiple variable Galois switching functions are constructed. Some examples for illustrating the theory are adopted from the existing papers and the results quite agree with the ones in the other papers.

1. 序 論

大型化된 集積回路에서 가장 重要하게 擡頭되는 問題中의 하나는 入·出力端子數의 制限問題이다. 이 問題는 集積回路의 密集化에 比例해서 또한 入·出力信號의 量에 比例해서 더욱 深刻해 진다. 이러한 2進論理回路의 制限性은 多値論理回路의 開發을 不可避하게 하였다. 더욱이 多値論理 理論을 論理設計에 導入한다면 進法間의 變換問題가 쉬어지며, 2進보다 적은 비트(bit)로도 10進數를 나타내므로 演算速度가 빨라 진다.[1],[2] 또한 디지털回路의 價格減少와 이들 價格의 계속적인 低下趨勢는 더욱 信賴性이 좋고 故障點 發見이 容易한 多値論理回路가 開發될 것으로 보인다.[2]

이러한 多値論理 理論을 Galois 體 上에서 解析하여 多値論理 回路로 實現시킨 것은 比較的 最近의 研究로서 K. S. Menger[3], B. Benjauthrit 와 I. S. Reed[4], D. K. Pradhan[5] 等은 Galois 스윗칭函數를 多項式 形態로 解析한바 있다. 以外에도 I. C. Wesselkamper[6]는 Newton의 補間法을 이용하여 解析하였으나 divided difference를 이용한 計算表를 따로 作成하여 多項式을 求하였다.

本 論文에서는 Lagrange의 補間法을 이용하여 多値 單一變數와 多値 2變數에 대한 Galois스윗칭函數의 構成理論을 먼저 展開하고 이 理論을 一般的인 多變數 Galois 스윗칭函數를 構成하는데 까지 擴張하였다. 本 論文의 理論을 展開시키는데 必要한 數學的 背景을 2節에서 略述하였고, 單一變數와 2變數에 대한 Galois 스윗칭函數를 構成한 後 이로부터 多變數에 대한 Galois스윗칭函數를 構成하는 節次를 3節에서 論하였다. 4節에서는 3節의 構成理論을 基礎로 하여 實際로 Galois 스윗칭函數를 求하는 過程을 例를 들어 자세히 밝혔다. 그리고 本 論文에서 다른 構成理論의 問題點을 5節에서 檢討하였다.

2. 數學的인 背景

이 節에서는 本 論文의 理論을 展開시키는데 必要한 Galois 體의 數學的인 性質을 列擧하였다.[3],[4],[9]

*正會員, 仁荷大學校 電子工學科
(Dept. of Electronics Engineering, InHa Univ.)
接受日字 ; 1980年 1月 31日

領域 D內의 모든 元素를 共域C內의 元素로 各各 對應시키는 法則을 D에서 C에로의 寫像 또는 函數라고 하며 $F : D \to C$ 또는 $D \xrightarrow{F} C$ 로 表記한다.[13]

지금 p를 素數 n을 陽의 整數라 할때 $P^n = N$ 인 有限個의 元素로 體를 形成하는 有限體를 一名 Galois 體라 하며 이와같은 Galois 體 GF(N)에는 + 와 ·演算이 唯一하게 存在한다.[4] 이러한 GF(N)의 元素사이에는 다음 性質이 成立한다.

1. $a + b$ 나 $a \cdot b$ 는 GF(N)內에 存在한다. $(\forall a, b \in GF(N))$
2. 交換法則 : $a + b = b + a$, $a \cdot b = b \cdot a$ $(\forall a, b \in GF(N))$
3. 結合法則 : $a + (b + c) = (a + b) + c$ $(\forall a, b, c \in GF(N))$
4. 分配法則 : $a \cdot (b + c) = a \cdot b + a \cdot c$ $(\forall a, b, c \in GF(N))$
5. 零元의 存在 : $a + 0 = 0 + a$ 인 零元 0이 存在한다. $(\forall a \in GF(N))$
6. 單位元의 存在 : $a \cdot 1 = 1 \cdot a = a$인 單位元 1인 存在한다. $(\forall a \in GF(N))$
7. 逆元의 存在 : $a + (-a) = 0$인 a의 加法에 關한 逆元 $-a$가 存在한다. $(\forall a \in GF(N))$ ·

   $a \cdot a^{-1} = 1$ 인 a의 乘法에 關한 逆元 a^{-1} 이 存在한다. $(\forall a \neq 0 \in GF(N))$

以上에 列擧한 基本性質 以外에도 本 論文에서 使用된 GF(N)의 重要한 性質을 들면 다음과 같다.[3][4],[9]

P. 1 : $0 \cdot a = a \cdot 0 = 0$

P. 2 : a) $\underbrace{1 + 1 + \cdots\cdots + 1 = 0}_{P}$

b) $P \cdot a = 0$ $(\forall a \in GF(N))$

P. 3 : $\forall a \in GF(N)$ 이고 $a \neq 0$ 에 대하여

$a^N = a$, $a^{N-1} = 1$

P. 4 : $\forall a, b \in GF(P^n = N)$ 이고 陽의 整數 n 에 대하여 $(a + b)^N = a^N + b^N$

P. 5 : $\forall \alpha \in GF(N)$ 에 대하여

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

但 $i + j \,(\mathrm{mod}\ N-1)$ 은 $i + j = r \,(\mathrm{mod} N-1)$, $0 \leqslant r \leqslant N-1$ 을 表示한다.

P. 6 : GF(N)의 元素들은

$$F(\alpha) = \sum_{i=0}^{N-1} a_i \alpha^i$$

으로 一義的으로 表示된다. 但 α는 P를 法으로한 整數體 Z_P의 元素를 係數로 하는 n次 既約多項式의 根이고, $a_i \in Z_P$ $(i = 0, 1, 2, \cdots\cdots, N-1)$ 이다.

P. 6에서 말한 n次 既約多項式은 Z_P의 元素를 係數로한 多項式 $x^N - x$ 의 既約因子를 말하며 本 論文에서 다룬 $GF(2^2)$의 既約多項式은 $x^2 + x + 1$로 구해진다. 따라서 元素사이에는 附표1과 附표2와 같은 加法 및 乘法이 成立한다.

3. Galois 스윗칭函數의 構成理論

3－1. 單一變數 Galois 스윗칭函數

Lagrange 補間法에 根據를 두어 函數를 構成하였다. 먼저 單一變數에 대한 Galois 스윗칭函數를 構成하기 前에 〔10〕에서 解析한 Lagrange 補間法을 多項式 形態로 展開시키는데 必要한 定理를 다음에 든다.

［定理 1］; $F(x) = \prod_{j=1}^{N-1} (x - e_j)$

$= x^{N-1} - 1$ $(\forall e_j \in GF(N))$

［證明］; $F(x) = \prod_{j=1}^{N-1} (x - e_j)$

$= (x - e_1)(x - e_2) \cdots\cdots (x - e_{N-1})$

이式의 函數 $F(x)$는 GF(N)에서 e_0을 除外한 (N－1)個의 根 即 $e_1, e_2, \cdots\cdots, e_{N-1}$ 을 모두 포함하여야 한다. 한편 2節의 P. 3으로 부터 GF(N)에서 e_0를 除外한 N－1個의 元素는 $x^{N-1} - 1$인 多項式의 根이 되므로 $\prod_{j=1}^{N-1} (x - e_j) = x^{N-1} - 1$ 이 成立한다. (證明 끝)

［定理 2］; $i = 1, 2, \cdots\cdots, N-1$에 대하여

$$\prod_{\substack{j=1 \\ j \neq i}}^{N-1} (e_i - e_j) = \prod_{j=1}^{N-1} e_j$$

가 成立한다. 여기서 $\forall e_i \in GF(N)$이다.

［證明］; 任意의 i에 대하여 集合 $\{(e_i - e_0), (e_i - e_1), \cdots, (e_i - e_{i-1}), (e_i - e_{i+1}), \cdots, (e_i - e_{N-1})\}$ 의 任意 두 元素 $(e_i - e_j)$와 $(e_i - e_k)$에 대하여 $(e_i - e_j) = (e_i - e_k)$ $(j \neq k)$라면

$e_j = e_k$ 이다.

그런데 GF(N)에서 $j \neq k$이면 $e_j \neq e_k$ 이므로 $e_j = e_k$ 는 모순이다. 그러므로

$(e_i - e_j) \neq (e_i - e_k)$

따라서 $GF(N) = \{(e_i - e_0), (e_i - e_1), \cdots, (e_i - e_{i-1}), (e_i - e_{i+1}), \cdots, (e_i - e_{N-1})\}$

$= \{e_1, e_2, \cdots\cdots, e_{N-1}\}$

이므로

$\prod_{\substack{j=1 \\ j \neq i}}^{N-1} (e_i - e_j) = \prod_{j=1}^{N-1} e_j$가 成立한다. (證明끝)

다음 두개의 補助定理는 他文獻에서 引用한 것으로 證明은 略한다.

補助定理 1[9] : $F(x)=x^{N-1}-1$ 일때 $F(x)/x-e_j$ 는 다음과 같다. 여기서 $\forall e_j \in GF(N)$이다.

$$\frac{F(x)}{x-e_j}=\frac{x^{N-1}}{x-e_j}$$
$$=x^{N-2}+e_j x^{N-3}+e_j^2 x^{N-4}+\cdots\cdots+e_j^{N-3}x+e_j^{N-2}$$

여기서 $e_j^{N-2}=e_j^{N-1}/e_j=1/e_j$ 이다.

補助定理 2[8] : a) $\prod_{j=1}^{N-1} e_j=e_t \qquad \forall e_j \in GF(N)$

여기서 $e_t \in GF(N)$로써 N이 偶數일 경우 e_1이고, N이 奇數일 때는 e_0, e_1을 除外한 GF(N) 內 餘他元素로 된다.

b) $\sum_{j=0}^{N-1} e_j=0 \qquad \forall e_j \in GF(N)$

單一變數에 대한 Lagrange 補間法[10]을 展開하여 整理하면 다음과 같다. 이의 展開過程은 附錄(Ⅱ)에 실었다.

$$F(x)=\sum_{i=0}^{N-1} y_i\left(\prod_{j\neq i}\frac{x-e_j}{e_i-e_j}\right) \quad \cdots\cdots\cdots\cdots\cdots\cdots(1)$$
$$=(e_t)^{-1}\prod_{j\neq 0}^{N-1}(x-e_j)\,y_0+(e_t)^{-1}x\prod_{j\neq 1}^{N-1}(x-e_j)\,y_1+\cdots+(e_t)^{-1}x\prod_{j\neq N-1}^{N-1}(x-e_j)\,y_{N-1} \quad \cdots\cdots\cdots\cdots\cdots(2)$$

여기서 $(e_t)^{-1}$은 e_t의 乘法에 關한 逆元이다.

定理 1을 이용하여 (2)式을 整理하면 다음과 같다.

$$F(x)=(e_t)^{-1}\left[(x^{N-1}-1)\,y_0+\frac{x\prod_{j=1}^{N-1}(x-e_j)}{x-e_1}y_1+\frac{x\prod_{j=1}^{N-1}(x-e_j)}{x-e_2}y_2+\cdots+\frac{x\prod_{j=1}^{N-1}(x-e_j)}{x-e_{N-1}}y_{N-1}\right] \quad \cdots\cdots(3)$$

(3)式의 第2項 以下를 補助定理 1에 의해서 整理하면 單一變數에 대한 Galois 스윗칭函數를 다음의 (4)式으로 構成할 수 있다.

$$F(x)=(e_t)^{-1}[(x^{N-1}-1)\,y_0+(x^{N-1}+e_1x^{N-2}+e_1^2x^{N-3}+\cdots+e_1^{N-3}x^2+e_1^{N-2}x)\,y_1+(x^{N-1}+e_2x^{N-2}+e_2^2x^{N-3}+\cdots+e_2^{N-3}x^2+e_2^{N-2}x)\,y_2+\cdots+(x^{N-1}+e_{N-1}x^{N-2}+e_{N-1}^2x^{N-3}+\cdots+e_{N-1}^{N-3}x^2+e_{N-1}^{N-2}x)\,y_{N-1}]$$
$$F(x)=(e_t)^{-1}[(x^{N-1}-1)\,y_0+\sum_{j=1}^{N-1}(x^{N-1}+e_jx^{N-2}+e_j^2x^{N-3}+\cdots+e_j^{N-3}x^2+e_j^{N-2}x)y_j] \quad \cdots\cdots(4)$$

$F(x)$는 GF(N)의 元素를 係數로하는 x의 多項式으로 展開되는데 (4)式에서 x^0, x^{N-1}項을 除外한 x^i項은 實際로 $(e_t)^{-1}\sum_{j=1}^{N-1} e_j^{N-1-i}y_j$인 係數를 갖는다. 그런데 GF(N)에서 元素 e_j는 有限個이므로 이 元素들의 $(N-1-i)$ 乘은 乘積表에서 간단히 計算된다. 또한 e_j에 對應하는 y_j만을 이용하므로 이 係數計算은 比較的 組織的이다. 물론 x^0의 係數는 $(e_t)^{-1}(-y_0)$이며 x^{N-1}項의 係數는 $(e_t)^{-1}[y_0+\sum_{j=1}^{N-1}y_j]$이다.

3-2. 多變數 Galois 스윗칭函數

두變數 x_1, x_2로 構成되는 多項式 $F(x_1,x_2)$는 x_1, x_2가 다같이 2次라면

$$F(x_1,x_2)=a_0+a_1x_1+a_2x_2+a_3x_1^2+a_4x_1x_2+a_5x_1^2x_2+a_6x_1x_2^2+a_7x_2^2+a_8x_1^2x_2^2\cdots\cdots(5)$$

로 展開되어 係數 $a_0, a_1, \cdots, a_8$의 決定으로 $F(x_1, x_2)$를 구할 수 있다. 그러나 (5)式에서 $x_2=c_1$인 定數로 擇하면

$$F(x_1,x_2)\Big|_{x_2=c_1}=F(x_1,c_1)=b_0+b_1x_1+b_2x_1^2$$

마찬가지로 $x_2=c_2, c_3, \cdots$로 擇하면

$$F(x_1,c_2)=d_0+d_1x_1+d_2x_1^2$$
$$F(x_1,c_3)=g_0+g_1x_1+g_2x_1^2$$
$$\cdots\cdots \quad \cdots\cdots \quad \cdots\cdots$$

으로 되므로 주어진 眞値表에서 x_2가 $e_0, e_1, e_2, \cdots, e_{N-1}$인 値를 取할때 函數 $F(x_1,x_2)$는 $\sum_{j=0}^{N-1}(x_1,e_j)$로 構成할 수 있다.

지금 x_2가 $e_0, e_1, e_2, \cdots, e_{N-1}$인 値를 取할때 x_1變數에 대한 $F(x_1,x_2)$를 구하면 (1)式에 의하여 다음과 같다.

$$F(x_1,x_2)=\frac{(x_2-e_1)(x_2-e_2)(x_2-e_3)\cdots(x_2-e_{N-1})}{(e_0-e_1)(e_0-e_2)(e_0-e_3)\cdots(e_0-e_{N-1})}\bullet F(x_1,e_0)$$
$$+\frac{(x_2-e_0)(x_2-e_2)(x_2-e_3)\cdots(x_2-e_{N-1})}{(e_1-e_0)(e_1-e_2)(e_1-e_3)\cdots(e_1-e_{N-1})}\bullet F(x_1,e_1)$$
$$\cdots\cdots \quad \cdots\cdots \quad \cdots\cdots$$
$$+\frac{(x_2-e_0)(x_2-e_1)(x_2-e_2)\cdots\cdots}{(e_{N-1}-e_0)(e_{N-1}-e_1)(e_{N-1}-e_2)\cdots}\frac{(x_2-e_{N-2})}{(e_{N-1}-e_{N-2})}\bullet F(x_1,e_{N-1}) \cdots\cdots(6)$$

定理 1, 2와 補助定理를 이용하여 (6)式을 整理하면 다음 (7)式과 같은 2變數에 대한 Galois 스윗칭函數를 構成할 수 있으며 이를 m變數入力인 경우로 擴張하면 (8)式과 같은 結果를 얻는다.

$$F(x_1,x_2)=(e_t)^{-1}(x_2^{N-1}-1)\,F(x_1,e_0)+(e_t)^{-1}\sum_{j=1}^{N-1}(x_2^{N-1}+e_j\,x_2^{N-2}+e_j^2\,x_2^{N-3}+\cdots+e_j^{N-3}\,x_2^2+e_j^{N-2}\,x_2)\,F(x_1,e_j) \quad \cdots\cdots(7)$$

$$F(x_1,x_2,\cdots,x_m)=(e_t)^{-1}(x_m^{N-1}-1)\,F(x_1,x_2,\cdots,x_{m-1},e_0)+(e_t)^{-1}\sum_{j=1}^{N-1}(x_m^{N-1}+e_j\,x_m^{N-2}+e_j^2\,x_m^{N-3}+\cdots+e_j^{N-3}\,x_m^2+e_j^{N-2}\,x_m)\,F(x_1,x_2,\cdots,x_{m-1},e_j) \quad \cdots\cdots(8)$$

4. 適 用 例

Galois스윗칭函數를 構成하는데 지금까지 展開시킨 構成理論이 어떻게 適用되는지 그 計算過程을 밝히면서 例示함과 아울러 實現構想回路를 圖示하였다. 먼저 單一變數에 대한 例를 다음에 든다.

例 1.[6] 표1에서 $N=5$이므로 $-e_1=e_4$이고 $e_t=e_4$이므로 $(e_4)^{-1}=e_4$이다. 附표3과 4를 이용하여 (4)式의 $F(x)$를 구하면 다음과 같다.

표 1. 單一變數의 例

Table 1. An example of single variable.

x	$F(x)$
e_0	e_1
e_1	e_3
e_2	e_2
e_3	e_3
e_4	e_1

$$F(x)=e_4\,[(x^4-1)\,e_1+(x^4+x^3+x^2+x)\,e_3+(x^4+e_2\,x^3+e_4x^2+e_3x)e_2+(x^4+e_3\,x^3+e_4x^2+e_2x)e_3+(x^4+e_4\,x^3+e_1x^2+e_4x)e_1]$$
$$=x^2+x+e_1 \quad \cdots\cdots(9)$$

(9)式은 표1의 入·出力 關係를 모두 만족하는 Galois스윗칭函數로써 그의 實現 構想回路는 그림1과 같다. 그림1에서 各 게이트는 附표3과 4를 만족하는 Galois加算 및 乘算게이트이다.

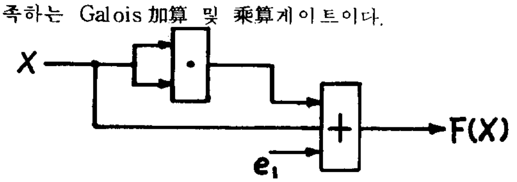

그림 1. 표1의 論理函數의 實現 構想回路

Fig. 1. Logic network realization of table 1.

다음의 例2와 例3은 多變數에 대한 適用例이다.

例2.[7] 주어진 眞値表 2에서 $N=2^2$이므로 $e_t=e_1=(e_t)^{-1}$이고 $-1=1$이다. 먼저 (7)式에서 $F(x_1,e_0)$, $F(x_1,e_j)$를 구하면 다음과 같다.

여기서 演算은 GF(4)에서 求한 元素사이의 加法및 乘法에 關한 附표1과 附표2에 의한 것이다.

표 2. 2變數의 例

Table 2. An example of two variables.

x_1	x_2	$F(x_1,x_2)$
e_1	e_0	e_0
e_1	e_1	e_1
e_1	e_2	e_3
e_1	e_3	e_2
e_0	e_0	e_0
e_0	e_1	e_0
e_0	e_2	e_1
e_0	e_3	e_1
e_3	e_0	e_1
e_3	e_1	e_3
e_3	e_2	e_3
e_3	e_3	e_1
e_2	e_0	e_1
e_2	e_1	e_2
e_2	e_2	e_1
e_2	e_3	e_2

$$F(x_1,e_0)=(x_1^3-1)\,e_0+(x_1^3+e_2\,x_1^2+e_3\,x_1)\,e_1+(x_1^3+e_3\,x_1^2+e_2\,x_1)\,e_1=e_1\,x_1^2+e_1\,x_1$$

$$F(x_1,e_1)=(x_1^3+e_1\,x_1^2+e_1\,x_1)\,e_1+(x_1^3+e_2\,x_1^2+e_3\,x_1)\,e_2+(x_1^3+e_3\,x_1^2+e_2\,x_1)\,e_3=e_1\,x_1$$

$$F(x_1,e_2)=(x_1^3-1)\,e_1+(x_1^3+e_1\,x_1^2+e_1\,x_1)\,e_3+(x_1^3+e_2\,x_1^2+e_3\,x_1)\,e_1+(x_1^3+e_3\,x_1^2+e_2\,x_1)\,e_3=e_3\,x_1^2+e_1\,x_1+e_1$$

$$F(x_1,e_3)=(x_1^3-1)\,e_1+(x_1^3+e_1\,x_1^2+e_1\,x_1)\,e_2+(x_1^3+e_2\,x_1^2+e_3\,x_1)\,e_2+(x_1^3+e_3\,x_1^2+e_2\,x_1)\,e_1=e_2\,x_1^2+e_1\,x_1+e_1$$

따라서

$$F(x_1,x_2)=(x_1^3-1)\,(e_1x_1^2+e_1x_1)+$$

$$+(x_2^3+e_1x_2^2+e_1x_2)(e_1x_1)$$
$$+(x_2^3+e_2x_2^2+e_3x_2)(e_3x_1^2+e_1x_1+e_1)$$
$$+(x_2^3+e_3x_2^2+e_2x_2)(e_2x_1^2+e_1x_1+e_1)$$
$$=x_1^2+x_1+x_1^2x_2+x_2^2+x_2 \quad \cdots\cdots(10)$$

(10)式은 표 2를 만족하는 Galois 스윗칭函數로써 論理回路로의 實現構想回路는 그림 2와 같다.

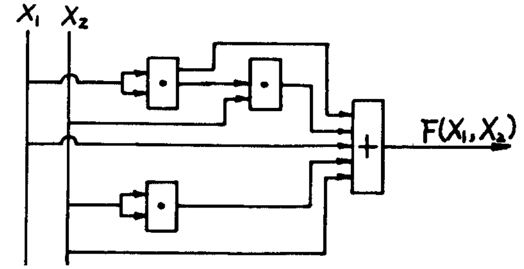

그림 2. 표 2의 論理函數의 實現構想回路
Fig. 2. Logic network realization of table 2.

例 3.[5] 주어진 眞値表 3에서 $N=2^2=4$ 이므로 $e_t=(e_t)^{-1}=e_1$ 이고 $-1\equiv1$ 이다.

표 3. 3變數의 例
Table 3. An example of 3-variables.

x_1	x_2	x_3	$F(x_1, x_2, x_3)$
e_0	e_3	e_0	e_3
e_1	e_3	e_0	e_3
e_2	e_3	e_0	e_2
e_2	e_3	e_1	e_1
e_2	e_3	e_2	e_1
e_2	e_3	e_3	e_1
e_3	e_3	e_0	e_3

(8)式으로부터 먼저 $F(x_1, x_2, e_0)$를 구하기 위하여 $F(x_1, e_0, e_0)$와 $F(x_1, e_j, e_0)$를 구하면 다음과 같다.

$$F(x_1, e_0, e_0)=0$$
$$F(x_1, e_1, e_0)=F(x_1, e_2, e_0)=0$$
$$F(x_1, x_3, e_0)=(x_1^3-1)e_3+(x_1^3+x_1^2+x_1)e_3$$
$$+(x_1^3+e_2x_1^2+e_3x_1)e_2$$
$$+(x_1^3+e_3x_1^2+e_3x_1)e_3$$
$$=x_1^3+e_2x_1^2+e_3x_1+e_3$$

따라서 $F(x_1, x_2, e_0)=(x_2^3-1)e_0$
$$+(x_2^3+e_3x_2^2+e_2x_2)$$
$$(x_1^3+e_2x_1^2+e_3x_1+e_3)$$

다음 $F(x_1, x_2, e_j)$를 구하면

$$F(x_1, e_0, e_j)=F(x_1, e_1, e_j)=F(x_1, e_2, e_j)=0$$

이고

$$F(x_1, e_3, e_1)=F(x_1, e_3, e_2)=F(x_1, e_3, e_3)$$
$$=x_1^3+e_2x_1^2+e_3x_1$$

이므로

$$F(x_1, x_2, e_1)=F(x_1, x_2, e_2)=F(x_1, x_2, e_3)$$
$$=(x_2^3+e_3x_2^2+e_2x_2)$$
$$(x_1^3+e_2x_1^2+e_3x_1)$$

그러므로 표 3을 만족하는 Galois 스윗칭函數는 다음 (11)式으로 構成되며 그의 論理回路實現 構想回路는 그림 3과 같다.

$$F(x_1, x_2, x_3)=(x_3^3+1)(x_2^3+e_3x_2^2+e_2x_2)$$
$$(x_1^3+e_2x_1^2+e_3x_1+e_3)$$
$$+(x_3^3+x_3^2+x_3)(x_2^3+e_3x_2^2+e_2$$
$$x_2)(x_1^3+e_2x_1^2+e_3x_1)$$

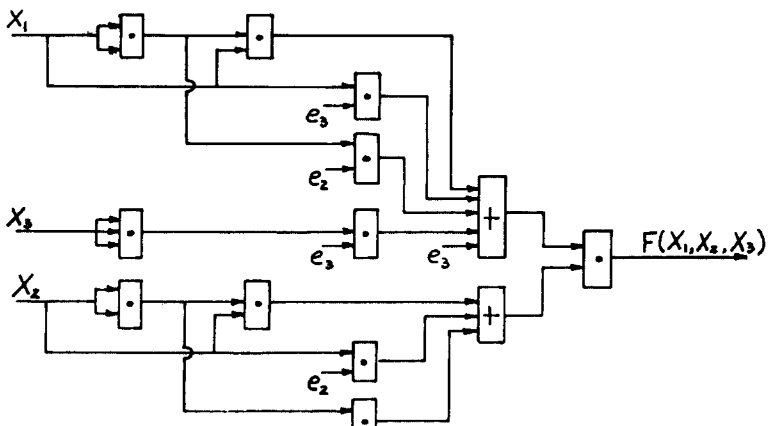

그림 3. 표 3의 論理函數의 實現 構想回路
Fig. 3. Logic network realization of table 3.

$$+(x_3^3+e_2x_3^2+e_3x_3)(x_2^3+e_3x_2^2+e_2x_2)(x_1^3+e_2x_1^2+e_3x_1)$$
$$+(x_3^3+e_3x_3^2+e_2x_3)(x_2^3+e_3x_2^2+e_2x_2)(x_1^3+e_2x_1^2+e_3x_1)$$
$$=(x_2^3+e_3x_2^2+e_2x_2)(e_3x_3^3+x_1^3+e_2x_1^2+e_3x_1+e_3)$$
$$=e_3x_2^3x_3^3+e_2x_2^2x_3^3+x_2x_3^3+x_1^3x_2^3+e_2x_1^2x_2^3+e_3x_1x_2^3+e_3x_2^3+e_3x_1^3x_2^2+x_1^2x_2^2+e_2x_1x_2^2+e_2x_2^2+e_2x_1^3x_2+e_3x_1^2x_2+x_1x_2+x_2 \quad \cdots\cdots\cdots\cdots (11)$$

5. 結 論

Boole代數를 이용한 現存의 2進論理는 元素數가 두個인 Galois 體 GF(2)인 경우에 지나지 않는다는 點을 考慮할때 多値論理函數 構成의 한 方法을 Galois體에서 찾는 것은 當然한 일이다. 뿐만 아니라 Galois 體의 算法을 만족하는 게이트의 開發이 活潑히 進行中이므로 不遠間 Galois 스윗칭函數의 構成理論은 多値論理에서 重要한 役割을 할 것으로 보인다.

本 論文에서 다룬 Galois 스윗칭函數의 構成理論은 多項式의 複雜한 係數處理 過程을 줄이려는 方向으로 設定되었던바 複雜한 數學的 處理없이 1變數와 2變數인 경우에 대하여 比較的 容易하게 多項式의 係數를 決定할 수 있는 函數式을 構成하였다. 그러나 3變數 以上의 多變數인 경우에는 函數式의 遂條過程이 길어질 수도 있으므로 計算機 프로그래밍을 비롯한 다른 演算에 의한 係數處理 方法이 要求된다.

附 錄 (I)

P=2, n=2인 N=4일때의 既約多項式은 x^2+x+1이다. 이러한 $GF(4)=\{e_0, e_1, e_2, e_3\}$元素들의 加法表 및 乘積表는 附표 1과 附표 2와 같다.

附표 1. GF(4)內 元素들의 加法表

+	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

附표 2. GF(4)內 元素들의 乘積表

•	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

다음 GF(5)內 元素들의 加法 및 乘積表는 附표 3과 附표 4와 같다.

附표 3. GF(5)內 元素들의 加法表

+	e_0	e_1	e_2	e_3	e_4
e_0	e_0	e_1	e_2	e_3	e_4
e_1	e_1	e_2	e_3	e_4	e_0
e_2	e_2	e_3	e_4	e_0	e_1
e_3	e_3	e_4	e_0	e_1	e_2
e_4	e_4	e_0	e_1	e_2	e_3

附표 4. GF(5)內 元素들의 乘積表

•	e_0	e_1	e_2	e_3	e_4
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_2	e_0	e_2	e_4	e_1	e_3
e_3	e_0	e_3	e_1	e_4	e_2
e_4	e_0	e_4	e_3	e_2	e_1

附 錄 (II)

本文의 (1)式에서 (2)式으로의 展開過程은 다음과 같다.

$$F(x)=\sum_{i=0}^{N-1} y_i \left(\prod_{j\neq i} \frac{x-e_j}{e_i-e_j}\right) \qquad (1)$$

$$\left.\begin{aligned}
&=\frac{(x-e_1)(x-e_2)(x-e_3)\cdots(x-e_{N-1})}{(e_0-e_1)(e_0-e_2)(e_0-e_3)\cdots(e_0-e_{N-1})}\,y_0\\
&+\frac{(x-e_0)(x-e_2)(x-e_3)\cdots(x-e_{N-1})}{(e_1-e_0)(e_1-e_2)(e_1-e_3)\cdots(e_1-e_{N-1})}\,y_1\\
&\qquad\cdots\cdots\qquad\cdots\cdots\qquad\cdots\cdots\\
&+\frac{(x-e_0)(x-e_1)(x-e_2)\cdots\cdots(x-e_{N-2})}{(e_{N-1}-e_0)(e_{N-1}-e_1)(e_{N-1}-e_2)\cdots(e_{N-1}-e_{N-2})}\,y_{N-1}
\end{aligned}\right\}(2)$$

定理 1, 2와 補助定理 2에 의하여 (2)式을 整理하면 本文의 (2)式을 얻는다.

※ 追記 ; 本 硏究는 韓國科學財團의 1979年度 定着硏究奬勵金 支援에 依해서 이루어진 것으로 韓國科學財團에 謝意를 表한다.

參 考 文 獻

1. I. Halpern and M. yoeli : "Ternary arithmetic unit," Proc. IEE, vol. 115, No. 10, pp. 1385-1388, Oct. 1968.
2. S. S. H. Su and A. A. Sarris : "The relationship between multivalued switching algebra and Boolean algebra under different definitions of complements," IEEE Trans. Compt., vol C-21, No. 5, pp. 479-485, May, 1972.
3. K. S. Menger : "A transform for logic net-works", IEEE Trans. Compt., vol. C-18, pp. 241-250, Mar. 1969.
4. B. Benjauthrit and I. S. Reed : "Galois switching functions and their applications," IEEE Trans. Compt., vol. C-25, pp. 78-86, Jan. 1976.
5. D. K. Pradhan : "A theory of Galois switching functions," IEEE Trans. Compt., vol. C-27, pp. 239-248, Mar. 1978.

6. T. C. Wesselkamper : "Divided difference methods for Galois switching functions," IEEE Trans. Compt., vol. C-27, pp. 232-238, Mar. 1978.
7. D. K. Pradhan and A. M. Patel : "Reed-Muller like canonic forms for multivalued functions," IEEE Trans. Compt., pp. 206-210, Feb. 1975.
8. 高瓊植, 金興壽 : "多値論理回路의 構成理論," 大韓電子工學會誌, 2號誌, 4月, 1980.
9. J. B. Fraleigh : "A first course in abstract algebra," Addison-Wesley, 1974.
10. G. Birkhoff and T. C. Bartee : "Modern applied algebra," New-York, McGraw-Hill, 1970.
11. C. F. Gerald ; "Applied numerical analysis," g^{nd} ed. Addison-Wesley, 1970.
12. David C Rine : "Computer science and multiple-valued logic," New-York, North-Holland, 1977.
13. 朴元善 : "抽象代數學," 서울, 螢雪出版社, 1974.