論文 80-17-2-5

多値論理回路의 構成理論

(A Constructing Theory of Multiple-Valued Switching Functions)

高 瓊 植*, 金 興 壽**

(Koh, Kyung Shik and Kim, Heung Soo)

要 約

論文에서는 Galois 體를 이용한 多値論理函數의 構成方法을 제시하였다. 먼저 單一變數多値論理函數의 構成理論을 展開하고 그 結果를 多變數多値論理函數構成에 확장하였다. 本 論文의 理論을 展開하는데 있어서 가장 근원이 되는 數學的 根據는

(1) GF(N)의 모든 元素의 合은 零이다.

(2) GF(N)의 e_0을 除外한 모든 元素의 積은 N이 偶數일때는 e_1이고, N이 奇數일 때는 e_t ($\neq e_0, e_1$)이다. 라는 두 性質이다. 이 性質을 바탕으로 하여 비교적 간단하고 새로운 構成理論을 유도하고, 또 展開式의 各係數를 逐次的인 乘法을 거치지 않고 직접 결정하는 과정을 제시하였다. 또 例題를 들어 構成理論을 뒷받침하였다.

Abstract

This paper presents a method for constructing multiple-valued switching functions based on Galois fields. First the constructing method for single-variable switching functions is developed, and the results are extended to multiple-variable functions. The fundamental mathematical properties used in this paper are:

(1) The sum of all elements over GF (N) is zero.

(2) The product of nonzero elements over GF(N) is equal to e_1 for N even, and $e_t (\neq e_0, e_1)$ for N odd.

With these properties, a relatively simple constructing method is developed, and a process for determining the coefficients of the expanded forms of switching functions is also obtained without successive multiplication of the polynomials. Some examples are given to illustrate the method.

1. 序 論

集積回路技術의 비약적인 發展은 回路形態를 MSI나 LSI 化시켰다. 이렇게 大型化된 集積回路에서 가장 問題視되는 것 중의 하나는 端子數制限問題이며, 그 解決方法의 하나로 多値論理回路의 硏究가 대두되었다. 그 理由는 2進論理인 경우보다 多値論理인 경우에는 적은 端子數로 많은 情報量을 처리할 수 있기 때문이다. 例를 들면 3値論理回路에서는 4개의 端子로 81개의 情報를 다룰 수 있으나, 이 情報量을 2進論理回路에서 다루기 위해서는 7개의 端子가 필요하다. 3値論理素子는 이미 여러 사람에 의하여 개발

*, **正會員, 仁荷大學校 電子工學科

(Dept. of Electronics Engineering, Inha University)

接受日字: 1979年 12月 19日

(※ 이 논문은 1979년도 문교부 학술연구 조성비에 의하여 연구된 것임.)

되었으며 소련에서는 3値論理를 이용한 計算機도 제작한 바 있다고 한다. 이러한 3値計算機는 10進數를 나타내는데 있어서 2進系統인 경우보다 적은 빗트數로도 충분하므로 그 演算速度는 빨라진다.

이와 같은 多値理論의 槪念은 디지털系統의 設計, 소프트웨어의 設計, 人間行動調節等과 같은 여러 分野에서 매우 중요하게 다루어지고 있으며, 時間이 갈수록 이 개념의 應用은 더욱 넓어질 것으로 예상된다. 이러한 多値論理理論을 有限體上에서 解析하여 多値論理回路를 實現시키고저 하는 硏究는 이미 여러 사람에 의하여 시작되었으며 K.S. Menger[1]는 Boolean difference 를 有限體에 확장하며 Galois스윗칭函數를 多項式의 형태로 얻은 後 Fourier變換에 對應시켜 論理回路를 實現시켰다. 그 後 B. Benjauthrit와 I.S. Reed[2]는 Menger 가 求한 多項式을 多値多變數의 경우로 확장시켰다. 반면에 D.K. Pradhan[3]은 Galois 스윗칭函數를 一般化시킨 Reed-Muller展開式에서 係數를 결정짓는 새로운 數學的 結果를 얻었고, T.C. Wesselkamper[4]는 divided difference를 이용한 Newton의 補間法으로 有限體上의 多項式을 展開시켰다.

上述한 硏究以外에도 有限體上에서의 Galois 스윗칭函數의 構成을 다룬 硏究가 여러篇 發表되었으나, 그 多項式 展開에 막대한 計算을 要하는 共通點이 있다.

本 論文에서는 Galois體의 性質을 이용하여 Galois 스윗칭 函數를 構成할 수 있는 새로운 槪念을 제시하였다. 有限體上의 入力變數가 有限體上의 各要素에 서로 相異한 寫像을 일으키도록 하고, 이와 같은 相異한 寫像에 대응하는 函數를 각각 求하여 合成함으로써 Galois스윗칭 函數를 構成하였다. 그리고 이 개념을 多變數인 경우에 확장하여 多變數多値論理函數에 대한 構成理論을 제시하였다.

本 論文의 서술과정은 다음과 같다. 即 2節에서 Galois體에 관한 性質을 要約하고 아울러 本 論文에 있어서의 理論的 根據가 될 定理를 들고 이를 證明하였으며, 3節에서 單一變數多値論理函數의 構成理論을 展開하고 이를 一般的인 多變數多値論理函數를 構成하는데 까지 확장시켰다. 4節에서는 3節의 構成理論을 바탕으로 하여 실제로 多値論理函數를 求하는 節次에 대해서 論하고, 5節에서는 多値論理函數의 最簡型의 展開式을 얻기까지의 복잡한 中間計算을 피하기 위한 合理的인 處理方法에 관해서 論하였다. 그리고 6節에서는 結論으로 本 方法을 지금까지 발표된 方法과 比較 檢討하였다.

2. Galois体의 諸性質

p를 素數로 하고 n을 陽의 整數라고 한다면, p개의 元素로 구성되는 有限體F의 n次 有限擴大體E의 元素 x는 E의 n개의 元素 $\alpha_1, \alpha_2, \cdots\cdots, \alpha_n$을 F上의 E의 基(basis)라 할때

$$x = a_1\alpha_1 + a_2\alpha_2 + \cdots\cdots + a_n\alpha_n$$
$$a_i \in F\ (i = 1, 2, \cdots\cdots, n)$$

와 같이 一義的으로 표시된다[15]. 따라서 E의 元素의 個數는 F의 p개의 元素를 n자리로 중복을 허용해서 配列하는 順列의 數와 같으므로 p^n개로 되며, 이 p^n개로 구성되는 有限體가 唯一하게 존재한다. 이 有限體를 一名 Galois體라고 하며 $GF(p^n)$으로 表記한다. 이러한 $GF(p^n)$의 元素사이에 定義된 加法과 乘法에 대하여

(1) 交換法則 : $a+b=b+a$, $ab=ba$

(2) 結合法則 : $a+(b+c)=(a+b)+c$
$$a\cdot(b\cdot c)=(a\cdot b)\cdot c$$

(3) 零元의 存在 : $a+o=o+a=a$인 零元 0이 存在한다.

(4) 單位元의 存在 : $a\cdot 1=1\cdot a=a$ 인 單位元 1이 存在한다.

(5) 逆元의 存在 : $a+(-a)=(-a)+a=0$인 a의 加法에 관한 逆元 $-a$가 存在한다. 또 $a\cdot a^{-1}=a^{-1}\cdot a=1$인 a의 乘法에 관한 逆元 a^{-1}이 存在한다.

(6) 分配法則 : $a\cdot(b+c)=a\cdot b+a\cdot c$ 等의 관계가 成立한다.

다음에 $GF(p^n)$의 중요한 基本性質을 들면 다음과 같다.[15]

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

P. 2 : $\underbrace{1+1+1+\cdots\cdots+1}_{p\text{ 개}}=0$

$$pa=0$$

P. 3 : $a^{p^n}=a$, $a^{p^n-1}=1$

P. 4 : $(a+b)^{p^n}=a^{p^n}+b^{p^n}$

P. 5 : $\alpha^i\alpha^j=\alpha^{i+j\,(mod\,p^n-1)}$

여기서 $i+j\equiv r\ (\mathrm{mod}\ p^n-1)$, $0\le r\le p^n-1$

P. 6 : $GF(p^n)$의 元素들은

$$f(\alpha)=\sum_{i=0}^{n-1} a_i\alpha^i$$

으로 一義的으로 표시된다. 但, α는 p를 法으로 하는 整數體 Zp의 元素를 係數로 하는 n次 旣約多項式의 根이고, $a_i \in Zp\ (i=0,1,2,\cdots\cdots, n-1)$이다. 여기서 n次 旣約多項式은 Zp의 元素를 係數로 하는 多項式

$X^{P^n}-X$ 의 既約因子를 말한다.

다음에 本 論文의 理論的 根據가 될 중요한 定理를 들고 이를 證明한다.

[定理 1] GF(N)의 元素사이에는 다음 관계가 成立한다.

(1) $\sum_{i=0}^{N-1} e_i = 0$

(2) $\prod_{i=1}^{N-1} e_i = \begin{cases} e_1 = 1 & ; \text{ N이 偶數일 때} \\ e_t (\neq e_0, e_1) & ; \text{ N이 奇數일 때} \end{cases}$

(證明) β 를 GF(N)의 原始元素(primitive element)즉 β 를 N-1 乘하면 1이 되는 元素라고 하면 GF(N)의 零이 아닌 모든 元素 $e_1, e_2, e_3, \cdots\cdots e_{N-1}$ 은 β 의 幕 $\beta, \beta^2, \beta^3, \cdots\cdots, \beta^{N-1}$ 로 표시된다. 따라서

(1) $\sum_{i=0}^{N-1} e_i = e_0 + \sum_{i=1}^{N-1} e_i = 0 + \sum_{i=1}^{N-1} \beta^i = \frac{\beta^{N-1}-1}{\beta-1}$

$= \frac{1-1}{\beta-1} = 0$

(2) $\prod_{i=1}^{N-1} e_i = \prod_{i=1}^{N-1} \beta^i = \beta^{N(N-1)/2}$ 이며

$N = 2t$ 라고 하면 $\beta^{N(N-1)/2} = \beta^{(N-1)t} = 1^t = 1$

$N = 2t+1$ 라고 하면 $\beta^{N(N-1)/2} = \beta^{(t+\frac{1}{2})(N-1)}$

$= \beta^{(N-1)t} \cdot \beta^{(N-1)/2} = \beta^{(N-1)/2} = \beta^t = e_t$

(證明끝)

[定理 2] 零이 아닌 GF(N)의 모든 元素의 積은 單位元의 加法에 관한 逆元이 된다. 즉

$$1 + \prod_{i=1}^{N-1} e_i = 0$$

(證明) $N = p^n$ 이 偶數일 때는 $p = 2$ 이며, 定理 1 (2)에 의하여 $\prod_{i=1}^{N-1} e_i = e_1 = 1$ 이므로

$$S = 1 + \prod_{i=1}^{N-1} e_i = 1 + 1 = 0$$

N이 奇數일 때는 定理 1(2)에 의하여

$\prod_{i=1}^{N-1} e_i = e_t = \beta^t = \beta^{(N-1)/2}$ 이므로

$S = 1 + \prod_{i=1}^{N-1} e_i = 1 + \beta^{(N-1)/2} = \beta^{N-1} + \beta^{(N-1)/2}$

$= \beta^{(N-1)/2}(1 + \beta^{(N-1)/2}) = \beta^{(N-1)/2} \cdot S$

여기서 $\beta \neq 1$ 이므로 $S = 0$ (證明끝)

3. 多値論理函数의 構成理論

3-1. 單一變數多値論理函數

그림 1과 같은 多値論理回路에 있어서 單一入力線 X에 $e_0, e_1, e_2, \cdots\cdots, e_{N-1}$ 인 N値의 入力이 들어와 出力線 Z에 역시 같은 N値의 出力이 나간다고 한다. 여기서

$$Z = F(X) \tag{1}$$

로 定義되는 F(X)를 單一變數多値論理函數라고 한다. 지금 어느 한 特定入力 e_i 에 대한 出力이 e_j 라고 할 때 $F_j(X)$를 다음과 같이 定義하면

$$F_j(X) = \begin{cases} e_j & ; X = e_i \text{ 일때} \\ 0 & ; X \neq e_i \text{ 일때} \end{cases} \tag{2}$$

(1)式의 F(X)는

$$F(X) = \sum_{j=1}^{N-1} F_j(X) \tag{3}$$

으로 構成된다. 따라서 F(X)의 構成問題는 $F_j(X)$의 構成問題로 歸着된다. 다음에 $F_j(X)$를 求하는 과정에 대해서 論하기로 한다. 지금 (2)式에 있어서

$$F_j(X)|_{X \neq e_j} = 0$$

을 만족시키는 部分函數를 $F_{j_0}(X)$라고 하면 $F_{j_0}(X)$는 다음과 같이 표시된다.

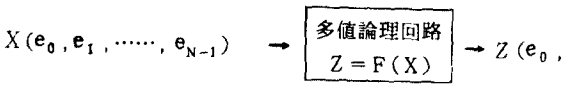

그림 1. 單一變數多値論理回路

Fig. 1. Single-variable multiple-valued switching circuit.

$$F_{jo}(X)=[(p-1)x+e_0][(p-1)x+e_1]\cdots\cdots\cdots\cdots [(p-1)x+e_{i-1}][(p-1)x+e_{i+1}]\cdots\cdots [(p-1)x+e_{N-1}] \quad (4)$$

그 理由는 e_i가 아닌 任意의 元素 e_k를 (4)式의 x에 代入하면 반드시 pe_k인 項이 나타나며, GF (N)에 관한 基本性質 P. 2에 의하여 $F_{jo}(e_k)=0$이 成立되기 때문이다.

다음에 $F_{jo}(X)$를 근거로 하여 $F_j(X)$를 求하는 節次를 생각한다. 지금 $F_{jo}(X)$의 X에 e_i를 代入하면

$$\begin{aligned}F_{jo}(e_i)&=[(p-1)e_i+e_0][(p-1)e_i+e_1]\cdots\cdots [(p-1)e_i+e_{i-1}][(p-1)e_i+e_{i+1}]\cdots\cdots [(p-1)e_i+e_{N-1}]\\&=[-e_i+e_0][-e_i+e_1]\cdots\cdots[-e_i+e_{i-1}] [-e_i+e_{i+1}]\cdots\cdots[-e_i+e_{N-1}]\\&=\prod_{m=1}^{N-1} e_m=\begin{cases}1\ ; & N=2t\text{일때}\\ e_t\ ; & N=2t+1\text{일때}\end{cases}\end{aligned} \quad (5)$$

그러므로 (2)式의 첫 部分이 成立하기 위해서는 (5)式에서 N이 偶數일 때는 $F_{jo}(e_i)=1$이므로 $F_{jo}(e_i)$에 e_j를 곱하면 되고, N이 奇數일 때는 $F_{jo}(e_i)=e_t$이므로 $F_{jo}(e_i)$에 e_t^{-1}을 곱하여 1로 만들고 그 결과에 e_j를 곱하면 된다. 따라서

$$F_j(X)=\begin{cases}e_j\cdot F_{jo}(X) & ;\ N\text{이 偶數일때}\\ e_j\cdot e_t^{-1}F_{jo}(X) & ;\ N\text{이 奇數일때}\end{cases} \quad (6)$$

3－2. 多變數多値論理函數

$$\begin{matrix}X_1(e_0,e_1,\cdots\cdots,e_{N-1})\rightarrow\\ X_2(e_0,e_1,\cdots\cdots,e_{N-1})\rightarrow\\ \vdots\\ X_m(e_0,e_1,\cdots\cdots,e_{N-1})\rightarrow\end{matrix}\boxed{\begin{matrix}\text{多 値 論 理 回 路}\\ Z=F(X_1,X_2,\cdots\cdots,X_m\end{matrix}}\rightarrow Z(e_0,e_1,\cdots,e_{N-1})$$

그림 2. 多變數多値論理回路

Fig. 2. Multiple-variable multiple-valued switching circuit.

그림 2와 같은 m개의 入力線을 통하여 N値의 入力이 들어와 出力線에 N値의 出力이 나가는 一般的인 多値論理回路를 생각할 때

$$Z=F(X_1,X_2,X_3,\cdots\cdots,X_m) \quad (7)$$

로 표시되는 $F(X_1,X_2,X_3,\cdots\cdots,X_m)$을 多變數多値論理函數라고 한다. 여기서 入力變數가 m개이고 各變數는 N値를 취하므로 一般的으로 N^m개의 入力組合이 존재한다. 지금 그 중의 한 入力組合($X_1=e_i$, $X_2=e_k$,……, $X_m=e_r$)에 대한 出力이 e_j가 되고 그 이외의 入力組合에 대해서는 零이 되는 論理式을 $F_j(X_1, X_2, \cdots\cdots, X_m)$이라고 하면

$$F_j(X_1,X_2,\cdots,X_m)=\begin{cases}e_j\ ;\ (X_1=e_i,\ X_2=e_k,\cdots\cdots,\\ \quad X_m=e_r)\text{일때}\\ 0\ ;\ \text{그 이외의 경우}\end{cases} \quad (8)$$

여기에 單一變數多値論理函數의 構成理論을 擴張適用하여

$$\begin{aligned}F_{io}(X_1)&=[(p-1)x_1+e_0][(p-1)x_1+e_1]\cdots\cdots [(p-1)x_1+e_{i-1}][(p-1)x_1+e_{i+1}]\cdots [(p-1)x_1+e_{N-1}]\\F_{ko}(X_2)&=[(p-1)x_2+e_0][(p-1)x_2+e_1]\cdots\cdots\\ &\vdots\qquad [(p-1)x_2+e_{k-1}][(p-1)x_2+e_{k+1}]\cdots\\ &\qquad [(p-1)x_2+e_{N-1}]\\F_{ro}(X_m)&=[(p-1)x_m+e_0][(p-1)x_m+e_1]\cdots\cdots [(p-1)x_m+e_{r-1}][(p-1)x_m+e_{r+1}]\cdots [(p-1)x_m+e_{N-1}]\end{aligned} \quad (9)$$

라고 하면

$$F_j(X_1,X_2,\cdots,X_m)=\begin{cases}e_jF_{io}(X_1)F_{ko}(X_2)\cdots F_{ro}(X_m);\\ \quad N\text{이 偶數일때}\\ e_j[e_t^{-1}F_{io}(X_1)][e_t^{-1}F_{ko}(X_2)]\cdots\\ \quad\cdots[e_t^{-1}F_{ro}(X_m)]\\ =e_j[e_t^{-1}]^mF_{io}(X_1)\ F_{ko}(X_2)\cdots\\ \quad\cdots F_{ro}(X_m);\ N\text{이 奇數일때}\end{cases} \quad (10)$$

그러므로 $F(X_1, X_2, \cdots, X_m)$은 다음과 같이 표시된다.

$$F(X_1,X_2,\cdots,X_m)=\sum_{j=1}^{N-1}F_j(X_1,X_2,\cdots,X_m) \quad (11)$$

4. 多値論理函數의 構成節次例示

本節에서는 前節의 構成理論을 기초로 하여 多値論理函數를 求하는 節次에 대해서 論한다. N의 값이 偶數일 때와 奇數일 때에는 약간의 差가 있으므로 이를 區分하여 고찰한다.

4－1. $N=p^n$이 偶數일 경우

$N=p^n$이 偶數가 되기 위해서는 p가 偶數이어야 하며, 또한 素數중에서 p가 偶數가 되는 경우는 $p=2$에 限한다. 따라서 N이 偶數가 되는 경우는 $N=2^n$의 경우이며 4値, 8値, 16値등이 이 범주에 속한다. 3節의 理論에 의하면 N의 값에 관계없이 그 構成節次는 同一하므로 本節에서는 $m=3$, $N=2^2$의

경우를 例로 들어 論하기로 한다. 지금 論理回路의 應動이 다음 표 1[3]로 주어진다고 한다. 물론 이 표에 적힌 入力組合以外의 入力組合에 대한 出力은 零이라고 생각하는 것이다.

표 1. 3變數 4値論理回路의 應動

x_1	x_2	x_3	z
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

우선 (9), (10)式에 의하여 $F_1(x_1,x_2,x_3)$, $F_2(x_1,x_2,x_3)$, $F_3(x_1,x_2,x_3)$을 求한다.

$$\begin{aligned}F_1(x_1,x_2,x_3)&=e_1[(x_1+e_0)(x_1+e_1)(x_1+e_3)]\\&\quad[(x_2+e_0)(x_2+e_1)(x_2+e_2)]\\&\quad[(x_3+e_0)(x_3+e_2)(x_3+e_3)\\&\quad+(x_3+e_0)(x_3+e_1)(x_3+e_3)\\&\quad+(x_3+e_0)(x_3+e_1)(x_3+e_2)]\\&=e_1[x_1^3+(e_0+e_1+e_3)x_1^2+(e_0e_1+e_0e_3+e_1e_3)x_1+e_0e_1e_3]\cdot[x_2^3+(e_0+e_1+e_2)x_2^2+(e_0e_1+e_0e_2+e_1e_2)x_2+e_0e_1e_2]\cdot[3x_3^3+(3e_0+2e_1+2e_2+2e_3)x_3^2+(2e_0e_1+2e_0e_2+2e_0e_3+e_1e_2+e_2e_3+e_3e_1)x_3+e_0e_1e_2+e_0e_1e_3+e_0e_2e_3]\\&=e_1[x_1^3+e_2x_1^2+e_3x_1][x_2^3+e_3x_2^2+e_2x_2][x_3^3]\end{aligned}$$

같은 요령에 의하여

$$\begin{aligned}F_2(x_1,x_2,x_3)&=e_2[(x_1+e_0)(x_1+e_1)(x_1+e_3)]\\&\quad[(x_2+e_0)(x_2+e_1)(x_2+e_2)]\\&\quad[(x_3+e_1)(x_3+e_2)(x_3+e_3)]\\&=e_2[x_1^3+e_2x_1^2+e_3x_1][x_2^3+e_3x_2^2+e_2x_2][x_3^3+e_1]\\F_3(x_1,x_2,x_3)&=e_3[(x_1+e_1)(x_1+e_2)(x_1+e_3)+(x_1+e_0)(x_1+e_2)(x_1+e_3)+(x_1+e_0)(x_1+e_1)(x_1+e_2)]\\&\quad[(x_2+e_0)(x_2+e_1)(x_2+e_2)]\\&\quad[(x_3+e_1)(x_3+e_2)(x_3+e_3)]\\&=e_3[x_1^3+e_2x_1^2+e_3x_1+e_1][x_2^3+e_3x_2^2+e_2x_2][x_3^3+e_3x_3^2+e_2x_2]\\&\quad[x_3^3+e_1]\end{aligned}$$

따라서

$$\begin{aligned}F(x_1,x_2,x_3)&=F_1(x_1,x_2,x_3)+F_2(x_1,x_2,x_3)+F_3(x_1,x_2,x_3)\\&=[x_2^3+e_3x_2^2+e_2x_2][e_3x_3^3+e_1x_1^3+e_2x_1^2+e_3x_1+e_3]\end{aligned}$$

以上의 演算은 附錄의 GF(4)에 관한 加法表 및 乘法表를 참조한 것이며, 또 이 函數를 論理回路로 실현시키면 그림 3과 같다.

4－2. $N=p^n$이 奇數일 경우

$N=p^n$이 奇數가 되기 위해서는 p가 奇數이어야 하며, 素數중에서 p가 奇數인 경우는 3, 5, 7,…… 等이므로 3値, 5値, 7値……等이 이 범주에 속한다. N이 奇數인 限에 있어서는 論理函數를 求하는 節次는 역시 同一하므로 本節에서는 $m=2$, $N=3^1$, 즉 2變數 3値論理函數의 경우를 例로 들어 論한다. 지금 論理回路의 應動이 표 2[3]로 주어진다고 한다.

(9), (10) 式으로 規制되는 $F_1(x_1,x_2)$, $F_2(x_1,$

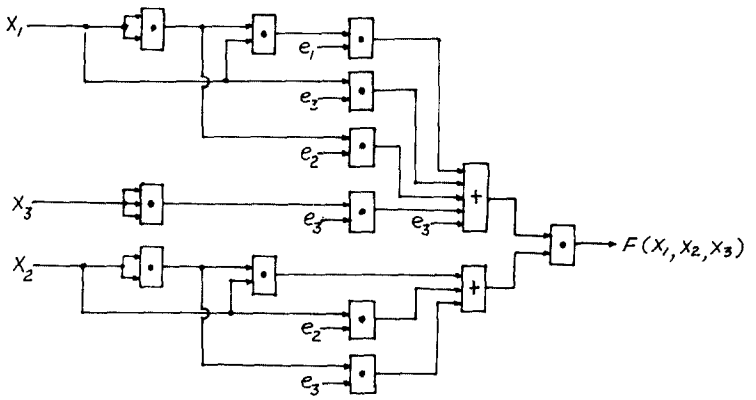

그림 3. 표 1의 論理函數의 實現構想回路

Fig. 3. Circuit inplementation of the switching function for table1.

x_2)를 求하기에 앞서 우선 GF(3)의 零元e_0을 除外한 모든 元素의 積을 求하면

$$e_t = e_1 e_2 = e_2$$

이므로 이것의 逆元素는 $e_2^{-1} = e_2$ 가 된다. 그러므로

$$\begin{aligned} F_1(x_1, x_2) &= e_1 e_2^2[(2x_1+e_0)(2x_1+e_1)][(2x_2+e_1)(2x_2+e_2)] + e_1 e_2^2[(2x_1+e_0)][(2x_2+e_0)(2x_2+e_1)] \\ &= 2x_1^2 x_2^2 + e_2 x_1^2 x_2 + e_2 x_1^2 + e_2 x_1 x_2 + x_1 \end{aligned}$$

$$\begin{aligned} F_2(x_1, x_2) &= e_2 e_2^2[(2x_1+e_0)(2x_1+e_2)][(2x_2+e_1)(2x_2+e_2)] + e_2 e_2^2[(2x_1+e_0)(2x_1+e_2)][(2x_2+e_0)(2x_2+e_2)] + e_2 e_2^2[(2x_1+e_0)(2x_1+e_1)][(2x_2+e_0)(2x_2+e_2)] \\ &\quad + e_2 e_2^2[(2x_1+e_0)(2x_1+e_1)][(2x_2+e_0)(2x_2+e_1)] = e_2 x_1^2 x_2^2 + e_2 x_1^2 x_2 + e_2 x_1 x_2 + x_1^2 + x_1 \end{aligned}$$

표 2. 2變數 3値論理回路의 應動

x_1	x_2	z
e_0	e_0	e_0
e_1	e_0	e_2
e_2	e_0	e_1
e_0	e_1	e_0
e_1	e_1	e_2
e_2	e_1	e_2
e_0	e_2	e_0
e_1	e_2	e_1
e_2	e_2	e_2

따라서

$$\begin{aligned} F(x_1, x_2) &= F_1(x_1, x_2) + F_2(x_1, x_2) \\ &= x_1^2 x_2^2 + x_1^2 x_2 + x_1 x_2 + e_2 x_1 \end{aligned}$$

以上의 演算에 있어서는 附錄의 GF(3)에 관한 加法表 및 乘法表를 참조하였으며, 또 이 函數를 論理回路로 실현시키면 그림 4와 같이 된다.

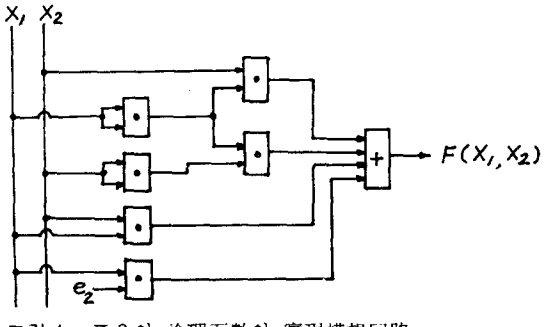

그림 4. 표 2의 論理函數의 實現構想回路

Fig. 4. Circuit implementation of the switching function for table 2.

5. 多値論理函数의 展開式에 대한 考察

3節의 (6)式 및 (10)式으로 規制되는 多項式의 積을 展開하여 이를 簡單化하고, 다시 이들을 (3)式 및 (11)式에 의하여 統合하여 最簡型의 論理式을 얻는데는 一般的으로 N의 값이 增加함에 따라 그 展開過程의 計算이 방대해진다. 따라서 展開過程의 복잡한 計算을 생략하고 最簡型의 展開式을 求할 수 있다면 多値論理函數의 構成은 容易해질 것이다. 本節에서는 이와 같은 意圖下에서 직접 展開式을 求하는 方法에 대해 論하기로 한다.

一般的으로 (6)式으로 規制되는 論理式은 變數 x에 대한 次數가 最高 $(N-1)$次이다. 따라서 $F_{jO}(x)$ 도 最高$(N-1)$次이며 다음과 같은 一般式을 갖는다.

$$F_{jO}(x) = a_{N-1}x^{N-1} + a_{N-2}x^{N-2} + a_{N-3}x^{N-3} + \cdots\cdots + a_1 x + a_0 \qquad (12)$$

따라서 $F_{jO}(x)$, 나아가서 $F_j(x)$ 의 展開式을 求하는 문제는 (12)式의 各係數를 定하는 문제로 歸着되며, 그 중 x^{N-1}은 반드시 e_1이 된다. 그리고 (12)式의 $F_{jO}(x)$의 x에 e_i를 代入하면 (5)式에서 표시되는 바와 같이 N이 偶數일 경우에는 1을 취하고 N이 奇數일 경우에는 e_t를 취하여야 하며, e_i以外의 元素를 代入하면 零을 취하여야 한다. 따라서 이와 같은 條件을 만족시키기 위해서는 (12)式의 各係數는 다음과 같은 값을 취하여야 한다.

$e_i \neq 0$ 일 경우:

$$\left.\begin{aligned} &a_{N-1} = (e_i^{N-1})^{-1},\ a_{N-2} = (e_i^{N-2})^{-1},\ a_{N-3} = (e_i^{N-3})^{-1}, \cdots\cdots,\ a_1 = e_i^{-1},\ a_0 = 0 \\ &e_i = 0 \text{ 일 경우}: \\ &a_{N-1} = -a_0,\ a_{N-2} = a_{N-3} = \cdots\cdots = a_1 = 0 \\ &a_0 = \begin{cases} 1 & ; N \text{이 偶數일때} \\ 0 & ; N \text{이 奇數일때} \end{cases} \end{aligned}\right\} \qquad (13)$$

다음에 그 理由를 고찰한다. 지금 편의상 e_i를 GF(N)의 原始元素β $(\neq 0)$라고 하면, (13)式으로 표시되는 各係數는 다음과 같이 된다.

$$a_{N-1} = (\beta^{N-1})^{-1} = 1,\ a_{N-2} = (\beta^{N-2})^{-1} = \beta,\ a_{N-3} = (\beta^{N-3})^{-1} = \beta^2,\ \cdots\cdots,\ a_1 = \beta^{N-2},\ a_0 = 0$$

따라서 (12)式의 $F_{jO}(x)$는 다음과 같이 표시된다.

$$F_{jO}(x) = x^{N-1} + \beta x^{N-2} + \beta^2 x^{N-3} + \cdots\cdots + \beta^{N-2} x \qquad (14)$$

上式의 x에 $e_i = \beta$를 代入하면

$$F_{jO}(e_i) = \beta^{N-1} + \beta^{N-1} + \cdots\cdots + \beta^{N-1} = \underbrace{1 + 1 + \cdots\cdots + 1}_{N-1} = p^n - 1 = -1 \qquad (15)$$

그런데 定理 2에 의하여 單位元의 加法에 관한 逆元

은 零이 아닌 GF(N)의 모든 元素의 積이며, 또 이 積은 定理1에 의하여 N이 偶數일 때는 1이 되고 N이 奇數일 때는 e_t가 되므로 (5)式을 만족시킨다. 일방 (12)式의 x에 e_i가 아닌 任意의 다른 元素 $e_k = \beta^k$ 를 代入하면

$$F_{j0}(e_k)=\beta^{k(N-1)}+\beta^{k(N-2)+1}+\beta^{k(N-3)+2}+\cdots\cdots$$
$$+\beta^{(N-2)+k}=\beta^{k(N-1)}[\beta^{1-k}+\beta^{2(1-k)}+$$
$$\beta^{3(1-k)}+\cdots\cdots+\beta^{(N-1)(1-k)}]$$
$$=\beta^{kN-1}\cdot\sum_{i=1}^{N-1}e_i=0$$

다음에 $e_i = 0$라고 하면 (12)式은 (13)式의 條件을 이용하여 다음과 같이 표시된다.

$$F_{j0}(x)=a_{N-1}x^{N-1}+a_0 \qquad (16)$$

上式의 x에 0을 代入하면

$$F_{j0}(0)=a_0=\begin{cases}1 ; & N\text{이 偶數일때}\\ e_t ; & N\text{이 奇數일때}\end{cases}$$

따라서 (5)式을 만족시킴을 알 수 있다. 또 (16)式의 x에 0이 아닌 任意의 다른 元素e_k를 代入하면

$$F_{j0}(e_k)=a_{N-1}e_k^{N-1}+a_0=-a_0+a_0=0$$

以上으로 (12)式의 各係數사이에는 (13)式의 관계가 成立해야 함이 確認된다.

(例1) 單一入力 8値論理回路에 있어서 $x=e_6$에 대한 出力이 e_1이고, 其他의 入力에 대해서는 出力이 零이 되는 論理式을 求한다.

$GF(2^3)$에 있어서는 $e_6^1=e_6$, $e_6^2=e_5$, $e_6^3=e_3$, $e_6^4=e_7$, $e_6^5=e_2$, $e_6^6=e_4$, $e_6^7=e_1$이므로

$a_1=e_6^{-1}=e_4$, $a_2=e_5^{-1}=e_2$, $a_3=e_3^{-1}=e_7$, $a_4=e_7^{-1}=e_3$, $a_5=e_2^{-1}=e_5$, $a_6=e_4^{-1}=e_6$, $a_7=e_1^{-1}=e_1$이다.

따라서

$$F_1(x)=x^7+e_6x^6+e_5x^5+e_3x^4+e_7x^3+e_2x^2+e_4x$$

(例2) 單一入力 5値論理回路에 있어서 $x=e_2$일때의 出力이 e_3이고, 其他의 入力에 대해서는 出力이 零이 되는 論理式을 求한다.

GF(5)에 있어서 e_0를 제외한 모든 元素의 積e_t를 求하면 $e_t=e_1\cdot e_2\cdot e_3\cdot e_4=e_4$이며 또 $e_t^{-1}=e_4$이다. 일방 GF(5)에 있어서는 $e_2^1=e_2$, $e_2^2=e_4$, $e_2^3=e_3$, $e_2^4=e_1$이며, $a_1=e_2^{-1}=e_3$, $a_2=e_4^{-1}=e_4$, $a_3=e_3^{-1}=e_2$, $a_4=e_1^{-1}=e_1$이므로

$$F_{30}(x)=x^4+e_2x^3+e_4x^2+e_3x$$

따라서

$$F_3(x)=e_3\cdot e_4\cdot F_{30}(x)=e_2\cdot F_{30}(x)$$
$$=e_2[x^4+e_2x^3+e_4x^2+e_3x]$$
$$=e_2x^4+e_4x^3+e_3x^2+x$$

6. 結 論

多値論理函數를 構成하는데 있어서 論理合 및 論理積을 단순히

$x+y=\max(x,y)$

$x\cdot y=\min(x,y)$

로 규정하는 2値의 Boole代數算法을 그대로 多値에 적용하는 方法은 현재 3値論理게이트가 어느 정도 實用化되고, 또 앞으로 開發이 기대되는 多値論理게이트가 현재의 2値게이트와 類似性을 지닌다는 假定下에서는 그 타당성이 인정되지만, Boole代數가 元素數가 2인 Galois體GF(2)의 경우에 지나지 않는다는 점을 생각하면 多値論理函數의 構成理論의 한 근거를 Galois體에 찾는다는 것은 당연한 일이다.

Galois體를 이용한 多値論理函數構成에 관한 論文은 序論에서도 言及한 바와 같이 지금까지 몇篇 있지만 多變數에 관한 構成理論이 발표된 것은 비교적 最近의 일이다. 本 論文에서 제시한 方法은 Galois 體를 이용한 점에 있어서는 이들 論文과 그 類를 같이 하지만, 方法論에 있어서는 相異하다. 本論文에서는 2節에서 證明된 定理에 理論的根據를 두어 構成理論을 展開한 것이 특이하다. 旣存論文들이 有限體에 관한 數學的理論에 置重하는 나머지 論理函數인 構成過程이 대단히 복잡한데 반하여, 本 論文의 方法은 4節에서도 아는 바와 같이 他論文의 例題를 대상으로 하였는데도 그 處理過程이 單純하고 容易함을 짐작할 수 있다. 또 5節에서는 3節의 理論에 근거를 두고 직접적으로 展開式의 各項의 係數를 결정하는 節次를 설명하였는데 이 과정은 Pradhan[3]의 係數決定方法과 비교할 때 많은 計算이 생략되는 장점이 있다.

附 錄

本文의 4節 및 5節에 있어서의 演算에 引用되는 GF(3), GF(4), GF(5) 및 GF(8)에 관한 加法表 및 乘法表를 여기에 싣는다. 이와 같은 加法表 및 乘法表는 2節의 p.6에서 말한 n次旣約多項式을 근거로 하여 얻어지는 것이다.

표 3. GF(3)의 加法表

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

표 4. GF(3)의 乘法表

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

표 5. GF(4)의 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

표 6. GF(4)의 乘法表

•	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

표 7. GF(5)의 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

표 8. GF(5)의 乘法表

•	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

표 9. GF(8)의 加法表

+	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 10. GF(8)의 乘法表

•	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

參 考 文 獻

1. K. S. Menger, "A transform for logic networks", IEEE Trans. Compt., vol. C-18, pp. 241-250, Mar. 1969.
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. D. K. Pradhan, "A theory of Galois switching functions", IEEE Trans. Compt., vol. C-27, pp. 239-248, Mar. 1978.
4. T. C. Wesselkamper, "Divided difference methods for Galois switching functions", IEEE Trans. Compt., vol. C-27, pp 232-238, Mar. 1978.
5. I. G. Rosenberg, "Some algebraic and combinatorial aspects of multiple-valued circuits", 1976 Int. Symp. on Multivalued Logic, pp. 9-23, May 25-28, 1976, Utah.
6. M. Kameyama and T. Higuchi, "Synthesis of multiple-valued logic networks based on tree-type universal logic module", IEEE Trans. Compt., C-26, No. 12, pp. 1297-1302, Dec. 1977.
7. S. Y. H. Su and P. T. Chen, "Cubical notation for Computer-aided processing of multiple-valued switching function", in 1976 Int. Symp. on Mutiple Logic, pp. 24-29, May 1976, Utah.
8. C. M. Allen and D. D Givone, "A minimization technique for multiple-valued logic systems", IEEE Trans. Compt., pp. 182-184, Feb. 1968.
9. D. K. Pradhan and A. M. Patel, "Reed-Muller like canonic forms for multivalued functions", IEEE Trans. Compt., vol. C-24, pp. 206-210, Feb. 1975.
10. K. L. Kodandapani and V. Setlur, "Reed-Muller canonical forms in multivalued logic", IEEE Trans. Compt., vol. C-24, pp. 628-635, June 1975.
11. S. Y. H. Su and P. T. Cheng, "Computer minimization of multivalued switching functions", IEEE Trans. Compt., vol. C-21, pp. 995-1003, Sept. 1972.
12. K. C. Smith, "Circuits for multiple-valued logic", in 1976 Int. Symp. on Multivalued Logic, pp. 30-43, May 1976 Utah.
13. H. T. Mouth, "A study on implementation of three-valued logic," in 1976 Int. Symp on Multivalued Logic, pp. 123-126, May 1976 Utah.
14. S. Y. H. Su and A. A. Sarris, "The relationship between multivalued switching algebra under different definitions of complement", IEEE Trans. Compt., vol. C-21, pp 479-485, May 1972.
15. J. B. Fraleigh, A first course in abstract algebra, Addison-Wesley, 1974.