論文 88-25-10-10

ROM 構造를 갖는 電流방식 CMOS 回路에 依한 GF(2^m)上의 演算器 설계

(A Design of Adder and Multiplier on GF (2^m) Using Current Mode CMOS Circuit with ROM Structure)

劉 仁 權*, 成 賢 慶*, 姜 聖 洙*, 金 興 壽*

(In Kweon Yoo, Hyeon Kyeong Seong, Sung Su Kang and Heung Soo Kim)

要 約

本 論文에서는 多値論理 函數를 계산하기 위해 GF(2^m)上의 元素生成, 加算, 乘算 및 除算에 대한 알고리듬을 제시하고 이 알고리듬에 의한 加算과 乘算의 결과를 ROM 構造의 電流방식 CMOS 回路로 設計하였다.

제시된 演算 알고리듬은 GF(2^m)上에서 多値論理 函數의 계산에 있어서 표조사방법이나 유클리드 알고리듬이 要하는 많은 양의 계산을 次數 m의 증가에 관계없이 범용 컴퓨터를 이용해 비교적 용이하게 처리할 수 있다.

또한 제시한 ROM 構造의 電流방식 CMOS 回路는 대칭적 多値眞理値表의 回路設計에 적합하고 GF(2^m)上의 加算 및 乘算을 동시에 실현할 수 있다.

Abstract

In this paper, it is presented element generation, addition, multiplication and division algorithm over GF (2^m) to calculate multiple-valued logic function. The results of addition and multiplication among these algorithms are applied to the current mode CMOS circuits with ROM structure to design of adder and multiplier on GF (2^m).

Table-lookup and Euclid's algorithm are required the computation in large quentities when multiple-valued logic functions are developed on GF (2^m). On the contrary the presented operation algorithms are prefered to the conventional methods since they are processed without relation to increasing degree m in the general purpose computer.

Also, the presented logic circuits are suited for the circuit design of the symmetric multiple-valued truth-tables and they can be implemented addition and multiplication on GF (2^m) simultaueously.

I. 序 論

현재의 2進論理를 수행하는 集積回路는 그동안 많은 발전을 이루어 왔지만 아직도 단자수 제한문제, 단자간 상호연결문제 그리고 보다 많은 정보 처리문

*正會員, 仁荷大學校 電子工學科
(Dept. of Elec. Eng., Inha Univ.)
接受日字 : 1988年 2月 24日

제 등의 解決策이 필요한 실정이다. 이러한 면에서 多値論理 理論의 연구가 대두되었고 지난 수 년간 여러 방법에 의해서 많은 발전을 이루어 왔다.[1]

그 중에서도 有限體는 2値 論理를 수행하는 Boolean體의 확장이라는 점에서 多値論理 理論의 주관심 분야가 되었다.[2]

즉, p가 素數, m이 陽의 整數인 GF(p^m)上에서 m의 확장에 따른 多値를 2進化하여 다루는 경우 有限體 GF(2^m)은 2개의 元素 0과 1로 이루어지는 GF(2)의 확대체로서 2^m개의 원소로 구성되며 모든 元素의 연산이 mod2로 행하여 진다. 그러므로 素數 p가 2인 경우에 있어 多値를 2進化하기가 용이하며 GF(2^m)上에서 m개의 비트 코드가 필요하다.[3]

이와 같이 GF(2^m)上의 모든 元素들을 2進 符號化하여 多値를 취급하는 例로는 Benjauthrit[2] 등과 Menger[3]에 의한 연구에서 볼 수 있다. 이들 연구에서 多値論理 函數를 구성하려면 공통적으로 GF(2^m)上의 加算 및 乘算을 표 조사 방법 또는 유클리드 알고리듬에 의하기 때문에 次數 m의 증가시 비교적 많은 계산을 要하게 된다.[4]

한편 多値論理 回路의 設計는 주로 電壓방식 쌍접합 트랜지스터 回路와 CMOS回路에 의해서 이루어져 왔고 지난 80년초 Intel 및 Motorola 등에 의한 多値 ROM의 출현으로 多値論理 回路를 긍정적으로 받아들이게 되었다.[5]

그러나 대부분의 電壓방식 回路는 回路의 복잡성과 傳達遲延 때문에 2進論理 回路와 경쟁이 못되어 새로운 기술인 電流방식 回路가 개발되었다.[6]

電流방식에 의한 回路동작은 電壓방식이 갖는 결점을 보완하고 임의의 절점에서 電流信號의 加, 減과 높은 電壓의 공급없이도 各 基底의 할당이 용이한 利點을 갖는다.[7]

Davio[8] 등과 Taniguchi[9] 등은 I²L에 의한 多値論理 回路의 設計를 제시하였고 최근에는 I²L과 유사한 동작을 하면서 VLSI 設計상 電力소모, 칩 점유率 및 동작특성 등에서 비교적 우수한 電流방식 CMOS 多値論理 回路가 Yamakawa,[7] Onneweer 등[10]과 Higuchi[11] 등에 의해 실현되고 있다.

本 論文에서는 GF(2^m)上의 多値論理 函數 계산에 있어서 次數 m이 증가할 때, 함수구성의 계산과정이 복잡하므로 m의 증가에 관계없이 入力된 旣約多項式을 이용하여 多値論理 函數를 2進符號化하는 알고리듬을 제시하였다.

또한 제시된 알고리듬에 의해 多値論理 函數의 加算, 乘算 및 除算 알고리듬도 제시하였다.

한편 GF(2^m)을 構成하는 2^m개의 元素들은 各各의 레벨로 볼 수 있으므로 電流에 의해 이들의 값을 할당하고, 제시된 알고리듬에 의해 얻은 加算과 乘算 결과를 ROM構造의 電流방식 CMOS 回路로 設計 방법을 제시하였다. 특히 GF(4)의 加算과 乘算 결과를 SPICE에 의해 시뮬레이션하여 回路의 타당성을 보였다.

Ⅱ. 數學的 배경과 電流방식 CMOS 基本回路

1. 有限體 GF(p^m)의 성질[2,12]

有限體 GF(p^m)上의 數學的 性質은 이미 발표된 내용을 증명없이 도입하여 사용하였다.

일반적으로 元素集合 {0, 1, 2, ⋯, p−1}로 표현되는 體 F가 있고 이 有限體 F의 m次 有限擴大體를 體 K라 하면 K는 陽의 整數 m에 대해서 p^m개의 元素를 갖는다. 이러한 有限體를 位數가 p^m인 Galois體라 하고 GF(p^m)로 표시한다.

GF(p^m)에서는 加算과 乘算이 唯一하게 성립하며 參考文獻[2]에 의한 이러한 GF(p^m)의 성질들 중 本 論文에서는 素數 p가 2인 경우에 대해서 적용한다.

2. 電流방식 CMOS 基本回路

電流방식 CMOS 基本回路는 여러 論文을 통해서 많은 종류가 발표되어 왔다.[7,10-11]

本 節에서는 이들 중 本 論文에 제시되는 回路를 구성할 基本回路를 그림 1에 들었다.

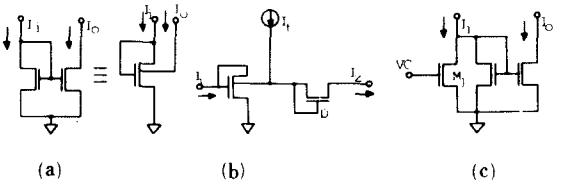


그림 1. 電流방식 CMOS 基本回路
(a) 電流 mirror　(b) 電流 difference
(c) 電流 switch

Fig. 1. Current mode CMOS basic circuits.
(a) current mirror. (b) current difference
(c) current switch.

그림 1(a)는 하나의 入力 電流源에서 多重 出力機能을 갖는 電流미러(current mirror)이다. 이는 일반적으로 電流방식 回路에서 팬-아웃(fanout) 수가 1이라는 결점을 보완해 주며 특히 電流이득에 관계되는 W(width)와 L(length)의 비율이 동일하다고 가정할 때, 出力電流는 入力電流와 같은 값을 갖게 된다.[7,13]

그림 1(b)는 電流差分回路로서, 정전류원으로 표시

되는 드래스홀드 電流 It가 공핍형 p채널 MOSFET로 구성되며 D는 다이오드를 나타낸다.[7] 이 回路에 대한 동작은 다음과 같다.

$$I_z=\begin{cases} I_t-I_x & \text{iff } I_t>I_x \\ 0 & \text{iff } I_t\le I_x \end{cases} \qquad (1)$$

그림 1(c)는 電流 스위치(switch)로서 패스 트랜지스터 M_1의 게이트 電壓이 높게되면 出力電流가 0이 되며 M_1의 VC가 낮게되면 電流 스위치는 電流미러로 동작한다.[10]

Ⅲ. GF(2^m)上에서 各 元素의 할당과 演算 알고리듬

本 章에서는 Ⅱ-1節에서 언급한 Galois體의 성질 중 素數 p가 2인 경우의 元素生成 알고리듬을 제시하고 이를 이용하여 多値論理 函數의 加算, 乘算, 除算에 대한 알고리듬도 제시하였다.

1. GF(2^m)上의 元素生成 알고리듬

有限體는 特性多項式 $X^{p^m}-X$가 p를 法으로 하는 整數體 Z_p의 分解體와 동형이 되어 다음式(2)와 같이 된다.

$$X^{p^m}-X=X\cdot(X-1)\cdot(X^{p^m-2}+\cdots+1) \qquad (2)$$

이때 式(2)로 부터 原始根을 갖는 최고차수 m인 既約多項式을 구하고 이 多項式의 한 根을 α라 할 때 式(3)과 같은 多項式이 生成된다.

$$F(\alpha)=\sum_{i=0}^{m-1}a_i\alpha^i$$
$$=a_0+a_1\alpha+a_2\alpha^2+\cdots+a_{m-1}\alpha^{m-1} \qquad (3)$$

여기서 α는 $Z_p=\{0,1,2,\cdots,p-1\}$의 元素를 係數로 하는 原始根을 갖는 m次 既約 多項式의 根이고 $a_i\in Z_p(i=0,1,2,\cdots,m-1)$이다.

本 論文에서는 素數 p가 2인 경우를 다루므로 式(3)의 係數 a_i는 0 또는 1로 표시된다. 즉, 이 경우 式(3)으로부터 GF(2^m)內의 모든 元素들은 m개의 2進符號로 표시할 수 있으나 本 論文에서는 한 비트를 추가하여, MSB(most significant bit)를 a_m이라 하고 式(3)의 最高次數係數 a_{m-1}, 最低次數係數 a_0를 各各 MSB-1번째 비트, LSB(least significant bit)가 되게 한다. 이때 既約多項式의 原如根을 α라 할 때 생성되는 元素 $\{0,1,\alpha,\cdots,\alpha^{2^m-2}\}$들 중에서 0은 m+1개의 비트로 처리되는 符號를 모두 0으로 하고 1은 LSB에 1을 入力시켜 처리하며 실제 기억장치에는 a_m비트를 제외하고 기억시킨다.

다음으로 2進符號의 LSB를 레프트 쉬프트 시켜 a_m비트를 판별하며 이러한 과정을 반복 실행함으로써 α의 冪을 생성하게 된다. 여기서 a_m비트의 판별시 a_m비트가 0이면 a_m비트를 제외한 나머지를 기억시키고 그렇지 않으면 이때 入力된 原如根을 갖는 既約多項式의 係數와 a_m비트를 제외한 비트들 간의 mod2 加算을 실행하여 이를 기억시킨다. 또한 이들 생성된 2進符號들을 2進數順에 의해 배열하고 各各을 $e_i(i=0,1,2,\cdots,2^m-1)$로 표시함으로써 既約多項式의 原如根 α에 의해서 생성되는 모든 元素 $\{0,1,\alpha,\cdots,\alpha^{2^m-2}\}$와 2進符號 e_i를 1:1 대응되게 하였다.

이상의 내용을 종합한 GF(2^m)上에서 元素生成 알고리듬은 다음과 같다.

〔元素生成 알고리듬〕

(단계1) 値數(N), 次數(m) 및 原如根을 갖는 既約多項式의 정보를 入力한다.

여기에서 N과 m은 $N=2^m$의 관계를 갖으며 既約多項式의 原如根을 α라 할 때 入力되는 多項式의 정보는 상수항을 1로 $\alpha^i(i=1,2,\cdots,N-2)$는 i+1로 入力한다.

(단계2) 次數(m)에 의해서 생성되는 m개의 비트에 한 비트를 추가하고 이를 $(a_m,a_{m-1},\cdots,a_1,a_0)$라 표시하며 모든 비트에 대해 초기화하고 다음으로 m+1개의 비트중 a_0에 1을 入力하고 이를 기억시킨다.

(단계3) 前단계에 $a_i(i=m,m-1,\cdots,1,0)$ 정보를 한 비트씩 레프트 쉬프트 시킨다.

(단계4) 단계3의 정보 중 a_m의 값을 판별한다.

i) $a_m=0$이면 기억장치에 그 때의 정보를 기억시키고 단계3으로 진행한다.

ii) $a_m=1$이면 단계5로 진행한다.

(단계5) 이미 入力된 原如根을 갖는 既約多項式의 정보와 a_m만을 제외한 m-1비트간의 mod2 加算을 실행하여 결과를 기억시킨 후 단계3으로 진행한다.

(단계6) 이상의 과정에서 기억된 2進符號들을 2進數의 순서로 배열하고 이들을 e_i로 표시하며 임의의 기억장소에 저장한다. 이때 各 元素 $\{0,1,\alpha,\cdots,\alpha^{2^m-2}\}$는 2進符號 e_i에 1:1 대응관계를 갖는다.

2. GF(2^m)上에서의 加算 알고리듬

GF(2^m)上에서 2進符號化된 元素들 중 被加算元素를 $e_i(i=0,1,\cdots,2^m-1)$, 加算元素를 $e_j(j=0,1,\cdots,2^m-1)$라 하고 이들 두 元素간의 加算 실행 후 결과값을 $e_L(L=0,1,\cdots,2^m-1)$로 할 때 이는 入力된 元素 e_i와 e_j에 대응되는 2進符號의 LSB로부터 MSB까지의 mod2 加算을 실행함으로써 얻어지게 된다.

따라서 이는 다음과 같은 관계식으로 일반화될 수

있다.

i) 임의의 多項式 $A=\sum_{k=0}^{m-1}a_k\alpha^k$와 $B=\sum_{k=0}^{m-1}b_k\alpha^k$ 에서 各各의 係數는 $e_i:\rightarrow a_k$, $e_j:b_k$인 관계를 갖는다.

ii) 두 多項式을 mod2 加算하면 $A\oplus B=C$이고, $C=\sum_{k=0}^{m-1}(a_k\oplus b_k)\alpha^k=\sum_{k=0}^{m-1}C^k\alpha^k$이므로 $e_i\oplus e_j:\rightarrow a_k\oplus b_k$, $c_k:\rightarrow e_L$인 관계를 갖는다.

여기서 $a_k, b_k, c_k\in Z_2=\{0,1\}$, $k=m-1, m-2,\cdots, 2, 1, 0$, $i, j, L=0, 1, 2,\cdots, 2^{m-1}$, $\oplus$=mod2 加算

이상의 내용을 종합한 GF(2^m)上에서 加算 알고리듬은 다음과 같다.

〔加算 알고리듬〕

(단계1) 2進符號化된 元素들 중에서 加算元素를 e_i, 被加算元素를 e_j로 하여 入力한다. 여기서 $i, j=0, 1,\cdots, 2^{m-1}$이다.

(단계2) 두 元素 e_i, e_j에 대응되는 各 2進符號들에 대한 비트간의 mod2 加算을 LSB로부터 한 비트씩 실행하고 다음 단계로 진행한다.

(단계3) a_k, b_k ($k=m-1, m-2,\cdots, 1, 0$)에 대한k값을 판정한다.

i) $k<m$이면 단계2로 진행한다.

ii) $k\geq m$이면 단계4로 진행한다.

(단계4) 2進符號로 나타난 결과값에 대응되는 e_L($L=0, 1, 2,\cdots, 2^m-1$)를 추출하고 GF(2^m)上의 加算 과정을 끝낸다.

3. GF(2^m)上에서 乘算 알고리듬

GF(p^m)內에 존재하는 各 元素 $0, 1, \alpha,\cdots, \alpha^{p^m-2}$ 에 대한 乘算 관계식은 參考文獻[2]의 성질12에 의한다.

本 論文에서는 素數 p가 2인 경우이고 주어진 元素 e_A, e_B ($A, B=0, 1, 2,\cdots 2^m-1$)는 Ⅲ-1節에 의해서 各各 $0, 1, \alpha,\cdots, \alpha^{2^m-2}$의 元素들에 1:1 대응관계를 갖는다.

한편 入力된 두 元素 중 어느 한 元素라도 0元素에 대응되면 乘算값은 e_0가 되고 $e_A(e_B)$ ($A, B=1, 2, \cdots, 2^m-1$)가 1元素에 대응되면 乘算값은 $e_B(e_A)$가 된다.

따라서 이들은 다음과 같은 관계식으로 일반화 될 수 있다.

i) $e_A\cdot e_B=e_0$ iff e_A or $e_B:\rightarrow 0$

$e_A\cdot e_B=e_B$ iff $e_A:\rightarrow 1$

$e_A\cdot e_B=e_A$ iff $e_B:\rightarrow 1$

ii) $e_A:\rightarrow\alpha^i$, $e_B:\rightarrow\alpha^j$

$e_A\cdot e_B:\rightarrow\alpha^i\cdot\alpha^j=\alpha^{i+j(\mathrm{mod}\,2^m-1)}$

$\alpha^{i+j(\mathrm{mod}\,2^m-1)}:\rightarrow e_M$

여기서 e_A, e_B, e_M은 各各 $(a_{m-1}, a_{m-2},\cdots, a_1, a_0)$, $(b_{m-1}, b_{m-2},\cdots, b_1, b_0)$, $(c_{m-1}, c_{m-2},\cdots, c_1, c_0)$로 표현되고 A, B, M은 $(0, 1, 2,\cdots, 2^m-1)$의 값을 갖는다.

이상의 내용을 종합한 GF(2^m)上의 乘算 알고리듬은 다음과 같다.

〔乘算 알고리듬〕

(단계1) 2進符號化된 元素들 중 乘數에 해당하는 e_A와 被乘數에 해당하는 元素 e_B를 入力한다.

(단계2) 乘數 또는 被乘數가 0元素에 대응되면 e_M은 e_0가 되고 乘數가 1元素에 대응되면 e_M은 被乘數 e_B가 된다. 또한 그 逆도 성립한다.

(단계3) 入力된 e_A, e_B 元素가 단계2 이외의 대응관계를 갖는 경우의 乘算은 各 元素에 대응되는 α의 $\exp(i+j)\ \mathrm{mod}(2^m-1)$ 연산을 실행한다.

(단계4) 단계3에서 얻은 α의 冪에 대응되는 e_M 값을 취하고 GF(2^m)上의 乘算을 끝낸다.

4. GF(2^m)上에서 除算 알고리듬

Galois 體內에서 加法과 乘法에 대한 逆元이 존재함은 參考文獻[2]에서 알 수 있다. 이때 乘法에 관한 逆元을 조사하면 式(4)로부터 式(5)를 유도할 수 있다.

$$\alpha^{p^m}=\alpha \tag{4}$$

$$\alpha^{-1}=\alpha^{p^m-2} \tag{5}$$

本 論文에서는 素數 p가 2인 경우를 다루고, 특히 乘法에 관한 逆元을 구하기 위해 다음 式을 사용한다.

$e_A:\rightarrow\alpha^i$일 때

$$(\alpha^i)^{-1}=\alpha^{2^m-1-i} \tag{6}$$

따라서 GF(2^m)上의 除算은 式(6)에 의해서 얻어진 결과를 乘數로 하고 임의의 入力된 元素에 대응되는 α의 冪을 被乘數로 한 乘算을 전개하여 얻을 수 있다.

이상의 내용을 종합한 GF(2^m)上의 除算알고리듬은 다음과 같다.

〔除算 알고리듬〕

(단계1) 2進符號化된 元素 e_i들 중 乘法에 관한 逆에 해당하는 元素(除數 : e_A)와 임의의 元素 (被除數 : e_B)를 入力한다. 여기서 $A=1, 2,\cdots, 2^{m-1}$, $B=0, 1, 2,\cdots, 2^m-1$ 이다.

(단계2) α를 旣約多項式의 原如根이라 할 때 $1, \alpha,\cdots, \alpha^{2^m-2}$ 중 入力된 원소 e_A가 1에 대응되면 e_1 값을 갖는다.

(단계3) 入力된 元素 e_A가 α의 冪에 대응되어지면 式 (6)에 의해서 해당하는 e_k ($k=2, 3,\cdots, 2^m-1$)값을 갖는다.

(단계 4) 단계 3에서 얻은 e_k 값을 乘數로 하고 入力된 임의의 元素(被除數 : e_B)를 被乘數로 하여 乘算을 실행한다.

Ⅳ. 電流방식 CMOS 多値論理回路

本 章에서는 電流방식 CMOS 基本回路를 이용하여 Ⅲ章에서 얻은 결과 중 加算과 乘算을 多値 ROM에 적용한다.

電流방식 CMOS 回路에 의한 多値 ROM의 構造는 그림 2와 같다.

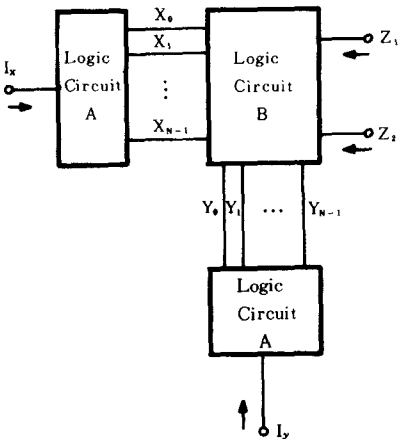


그림 2. 多値 ROM의 形態
Fig. 2. Configuration of multivalued ROM.

그림 2의 論理回路 A는 電流를 電壓으로 변환해 주는 전류/전압 변환기 이다.

이 변환기에서 入力電流 I_x(또는 I_y) ($I_x, I_y = 0,1, \cdots, N-1$)에 대한 出力電壓 x_i(또는 y_i) ($i = 0,1,2, \cdots, N-1$)는 다음과 같은 함수 관계를 갖는다.

$$x_i = \begin{cases} 0 & \text{iff} \quad I_x = i \\ 1 & \text{iff} \quad I_x \neq i \end{cases} \qquad (7)$$

여기에서 $i = 0,1,2,\cdots,N-1$ 이다.

論理回路 A는 Ⅱ-2節의 基本回路를 이용해 그림 3처럼 구성된다.

여기서 各 MOS 트랜지스터의 게이트 차원 (L×W)을 같게 해주고 단위전류를 15μA로 함으로써, 各 電流源에서의 數値는 자신의 값에 15μA를 곱한 電流값을 갖게 된다. 또한 I_x와 I_y의 入力電流에 대한 論理回路 A 부분은 論理回路 B 부분의 필요한 단위소자를 지정하는 역할을 한다.

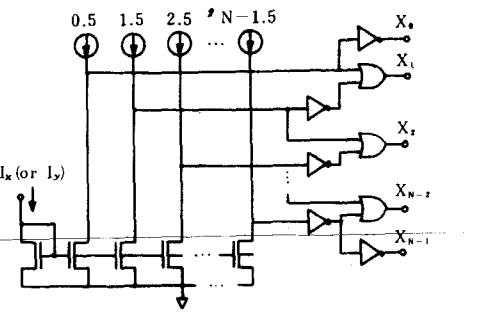


그림 3. N値에 대한 論理回路A의 設計
Fig. 3. Design of logic circuit A for N-valued.

즉, 入力電流 I_x(또는 I_y)에 대한 出力값으로 대각선에 眞理値 0을 갖게 한다. 이에 대한 入力電流와 出力電壓의 대응관계를 表 1로 나타낸다.

한편 論理回路 B는 그림 4(a)와 같은 2入力－2出力을 갖는 단위소자의 배열로 구성되며 그림 4(b)는 단위소자의 기호이다.

표 1. 入力電流와 出力電壓의 對應關係
Table 1. Mapping relation for current-to-voltage conversion.

I_x x_i	x_0	x_1	x_2	⋯	x_{N-2}	x_{N-1}
0	0	1	1	⋯	1	1
1	1	0	1	⋯	1	1
2	1	1	0	⋯	1	1
⋮	⋮	⋮	⋮	⋯	⋮	⋮
N − 2	1	1	1	⋯	0	1
N − 1	1	1	1	⋯	1	0

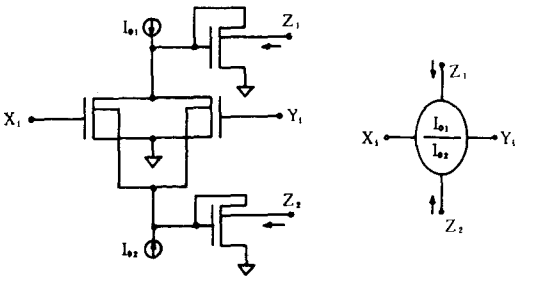


그림 4. 論理回路 B에서 2入力－2出力을 갖는 單位素子
Fig. 4. Two input-two output unit cell in logic circuit B.

그림 4(b)에서 단위원 內는 入力된 電流源의 크기를 나타내고 Z_1은 加算 Z_2는 乘算 出力을 나타낸다.

V. 適 用 例

本 章에서는 ROM構造를 갖는 電流방식 CMOS 多値論理回路의 設計를 Ⅲ章에서 얻은 GF(4)와 GF(8)의 多値眞理値表에 適用하는 例를 보였다. 특히 GF(4)의 加算과 乘算回路는 SPICE에 의해 시뮬레이션하여 回路의 타당성을 보였다.

〔例 1〕 原如根을 갖는 既約多項式 $F(x)=x^2+x+1$인 GF(4)의 加算 및 乘算回路

表 2는 Ⅲ章에서 얻은 GF(4)의 加算과 乘算에 대한 眞理値表로 2變數 4値眞理値를 나타낸다.

표 2. GF(4)의 多値眞理値表
Table 2. Multivalued truth table of GF(4).

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

(a) 가산표

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

(b) 승산표

여기서 各 數値는 GF(4)의 元素 $e_i(i=0,1,2,3)$의 i값에 해당하며 이는 各 電流레벨로 적용된다.

따라서 論理回路 A는 그림 5와 같으며 SPICE로 시뮬레이션한 결과는 그림 6과 같다.

그림 6의 결과에서 알 수 있듯이 I_x(또는 I_y)의 변화에 따라서 대각선으로 出力電壓 0이 나타나며 그 외의 부분에서는 眞理値 1(3V)이 出力된다.

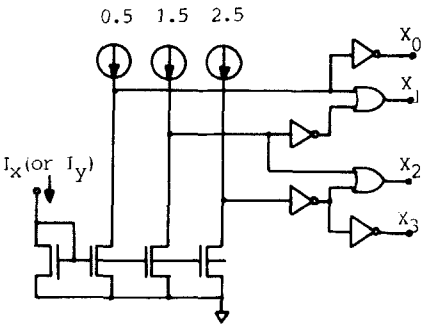


그림 5. GF(4)에 대한 論理回路A의 設計
Fig. 5. Design of logic circuit A for GF(4).

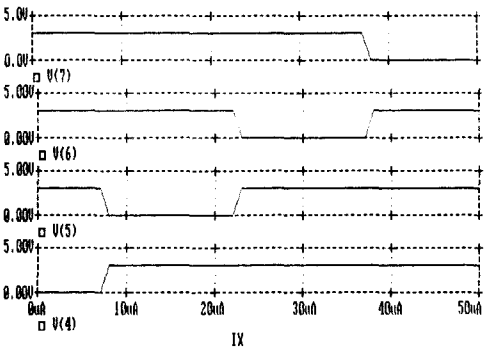


그림 6. GF(4)의 논리회로 A 부분을 SPICE로 시뮬레이션한 결과
Fig. 6. The results of logic circuit A of GF(4) to be simulated by SPICE.

또한 論理回路 B는 그림 7으로 구성된다. 여기서 各 單位素子의 원내값은 表 2의 값에 대응된다.

특히 Galois 體의 加算과 乘算은 Abelian群을 이루므로 대각선을 중심으로 좌우 대칭을 이룬다. 이것은 N×N 單位素子의 배열에서 素子數를 〔$(N^2-N)/2$〕$+N$으로 감소시킨다.

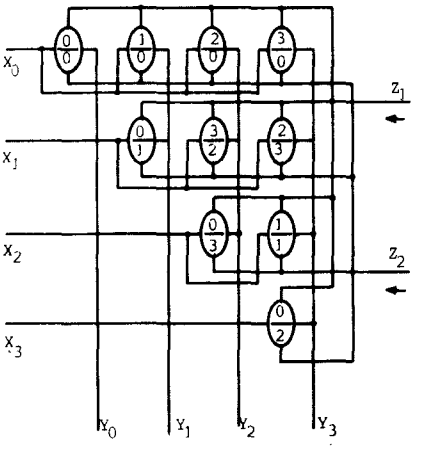
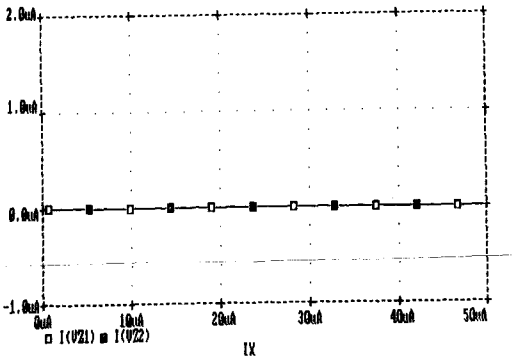


그림 7. GF(4)에 대한 論理回路B의 設計
Fig. 7. Design of logic circuit B for GF(4).

한편 이상의 論理回路 A와 B로 구조적 設計된 GF(4)의 加算, 乘算回路를 SPICE에 의해 시뮬레이션한 결과는 그림 8~11과 같다.

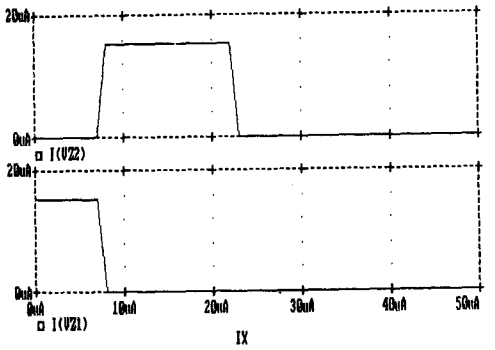
〔例 2〕 原如根을 갖는 既約多項式을 x^3+x+1로 선택한 경우의 GF(8)의 加算 및 乘算回路



여기서 I (VZ₁)은 加算 I (VZ₂)는 乘算出力이다.

그림 8. I_x를 증가시키고 I_y는 0μA를 入力했을때 GF(4)의 加算과 乘算出力

Fig. 8. Addition and multiplication output of GF(4) when incresing I_x, and $I_y=0\mu A$.



여기서 I (VZ₁)은 加算, I (VZ₂)는 乘算出力이다.

그림 9. I_x를 증가시키고 I_y는 15μA를 入力했을때 GF(4)의 加算과 乘算出力

Fig. 9. Addition and multiplication output of GF(4) when incresing I_x, and $I_y=15\mu A$.

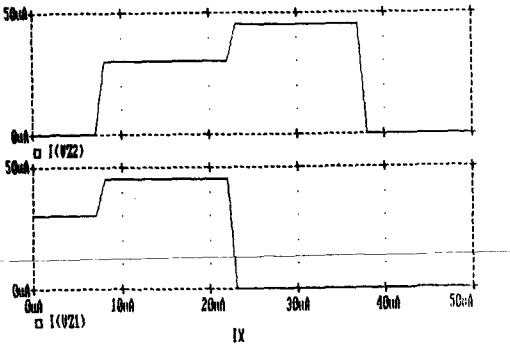
表 3은 Ⅲ章에서 얻은 GF(8)의 加算과 乘算에 대한 眞理値表로서 2變數 8値眞理値를 나타낸다.

여기서 各 數値는 GF(8)의 元素 e_i (i=0,1,2,…,7)의 i값에 해당하며 이는 各 電流레벨로 적용된다.

이 GF(8)에 대한 論理回路 A와 B부분은 例 1에서와 같은 방법으로 구조적 設計를 할 수 있으며 이들을 그림 12와 13으로 구성할 수 있다.

Ⅵ. 比較 및 檢討

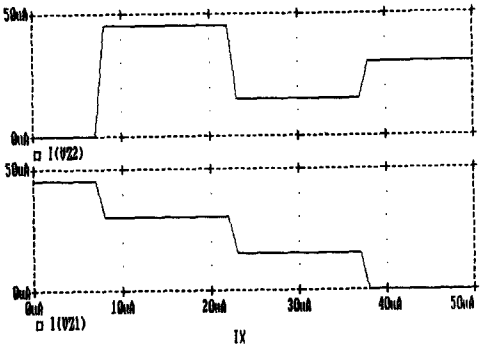
本 章에서는 제시된 回路의 타당성을 조사하기 위



여기서 I(VZ₁)은 加算, I(VZ₂)는 乘算出力이다.

그림10. I_x를 증가시키고 I_y는 30μA를 入力했을때 GF(4)의 加算과 乘算出力

Fig. 10. Addition and multiplication output of GF(4) when incresing I_x, and $I_y=30\mu A$.



여기에서 I(VZ₁)은 加算, I(VZ₂)는 乘算出力이다.

그림11. I_x를 증가시키고 I_y는 45μA를 入力했을때 GF(4)의 加算과 乘算出力

Fig. 11. Addition and multiplication output of GF(4) when incresing I_x, and $I_y=45\mu A$.

표 3. GF(8)의 多値眞理値表

Table 3. Multivalued truth table of GF(8).

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	4	7	2	6	5	3
2	2	4	0	5	1	3	7	6
3	3	7	5	0	6	2	4	1
4	4	2	1	6	0	7	3	5
5	5	6	3	2	7	0	1	4
6	6	5	7	4	3	1	0	2
7	7	3	6	1	5	4	2	0

(a) 가 산 표

•	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	3	4	5	6	7	1
3	0	3	4	5	6	7	1	2
4	0	4	5	6	7	1	2	3
5	0	5	6	7	1	2	3	4
6	0	6	7	1	2	3	4	5
7	0	7	1	2	3	4	5	6

(b) 승 산 표

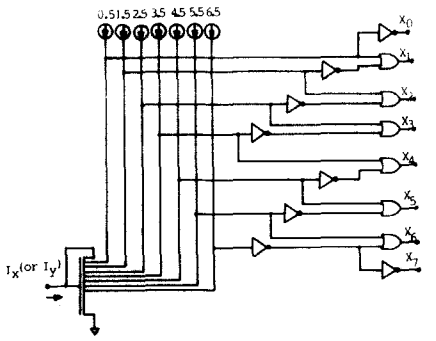


그림12. GF(8)에 대한 論理回路A 의 設計
Fig. 12. Design of logic circuit A for GF(8).

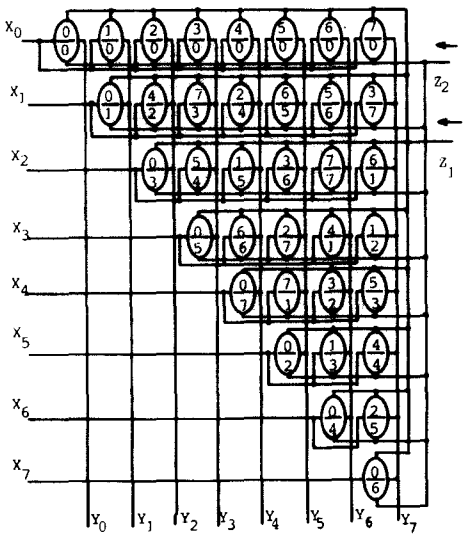


그림13. GF(8)에 대한 論理回路B 의 設計
Fig. 13. Design of logic circuit B for GF(8).

해 Taniguchi[9] 등의 論文에서 설명된 多値回路에 대해서 고찰해 보았다.

Taniguchi 등의 多値回路는 論理回路 A부분을 I^2L에 의한 電流미러, 금지회로 그리고 정전류원의 조합으로 구성하였고, 論理回路 B 부분을 지정하기 위해 論理回路 A의 出力電流와 論理回路 B 부분의 入力단 정전류원과의 차성분에 의해 구동되도록 하였다.

그러나 本 論文에 제시된 多値回路는 論理回路 A에 있어서 電流방식 CMOS에 의한 電流差分回路와 몇 개의 論理게이트를 조합시킴으로써 論理回路 B의 入力단 패스 트랜지스터를 구동시키게 하였다. 즉, 비교적 간단하고 안정된 동작에 의해서 Taniguchi 등이 실현하였던 多値回路와 같은 결과를 얻었다.

또한 Taniguchi 등의 論文에 적용된 素子와 本 論文에 적용한 素子가 各各 동등하다 가정하고 GF(4)와 GF(8)에 대한 加算, 乘算回路의 素子數 비교를 表 4에 나타냈다.

표 4. 비 교 표
Table 4. Comparis on table.

	사용된 t·r 의갯수		정전류원의 갯수		Logic gate 수	
	GF(4)	GF(8)	GF(4)	GF(8)	GF(4)	GF(8)
Taniguchi 논문	110 개	390 개	60 개	188 개	0	0
본 논 문	88 개	304 개	26 개	86 개	OR gate 4 개 inverter 8 개	ORgate 12개 inverter 16개

그러나 表 4에 제시한 자료는 1983년도에 발표된 Taniguchi 등의 論文결과와 비교한 것으로 구성 소자수에서 큰 차이를 보인 것은 사실이지만 Taniguchi 등이 다룬 감도문제는 고려하지 않은 결과이다.

Ⅶ. 結　　論

GF(2ᵐ)上에서 多値論理函數를 계산할 때 표조사 방법이나 유클리드 알고리듬은 次數 m이 5이상이 되면 元素生成, 加算, 乘算 및 除算의 실행에 있어서 비교적 많은 계산을 要해 왔다.

本 論文에서는 제시한 알고리듬이 GF(2ᵐ) 上에서 多値論理函數를 계산할 때, 次數 m의 증가에 따라 요구되는 많은 양의 계산을 컴퓨터 프로그램에 적용함으로써 용이하게 하였다.

한편 ROM 構造를 갖는 電流방식 CMOS 回路에 의해 GF(2ᵐ) 上의 加算과 乘算을 실행한 결과, 제시된 回路는 Taniguchi 등이 제시한 回路보다 소요된 소자의 갯수에서 유리하였다. 또한 Galois體 연산에 적용함으로써 서로 독립된 기능을 갖는 함수를 동시에 얻을 수 있었다.

그러나 本 論文에 제시된 回路는 물리적 設計시 要하는 구체적인 파라메터 값 및 연산속도, 하자드 발생문제 등은 고려하지 않았다. 이러한 문제는 더 많은 연구를 요구하며 아울러 GF(2ᵐ)에 대하여 마스크 프로그램어블한 기법을 개발함이 요망된다.

參 考 文 獻

[1] Stanley L. Hurst, "Multiple-valued logic-its status and its future," *IEEE Trans. |Compt.*, vol. C-30, pp. 619-634, Sep. 1981.

[2] Boonsieng Benjauthr it and Irving S. Reed, "Galois switching functions and their application," *IEEE Trans. Compt.*, vol. C-25, pp. 78-86, Jan. 1976.

[3] Karl S. Menger, "A transform logic networks," *IEEE Trans. Compt.*, vol. C-18, pp. 241-250, Mar. 1969.

[4] Charles C. Wang, T.K. Truong, Howard M. Shao, Leslie J. Deutsch, Jim K. Omura and Irving S. Reed, "VLSI architectures for computing multiplications and inverses in GF (2^m), " *IEEE Trans. Compt.*, vol. C-34, pp. 709-717. Aug. 1985.

[5] Jon T. Butler, James H. Pugsley and Charles B. Silio, Jr., "High-speed multiplier uses 50 percent less chip area and power," *IEEE Computer*, vol. 20, pp. 109-110, August, 1987.

[6] Edward I. McCluskey, *Logic design principles with emphasis on testable semicustom circuit*, Prentice-Hall, New Jersey, 1986.

[7] Takeshi Vamakawa, Tustomu Miki and Fumio Ueno, "The design and fabrication of the current mode Fuzzy logic Semicustom IC in the standard CMOS IC technology," Proc. 15th ISMVL., Canada, pp. 76-82, May 1985.

[8] M. Davio and J.P. Deschamp, "Synthesis of discrete functions using IIL technology," *IEEE Trans. Compt.*, vol. C-30, pp. 653-661, Sept. 1981.

[9] Kazutaka Taiguchi, Takahiro Inoue and Fumio Ueno, "Realization and analysis of a mask-programmable IIL multivalued logic circuit," *Proc. 13th ISMVL.*, Kyoto, Japan, pp. 196-200, May. 1983.

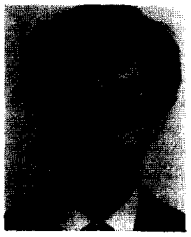
[10] S.P. Onneweer, H.G. Kerkhoff, "Current-mode CMOS high-radix circuits," *Proc. 16th ISMVL.*, Virginia, USA., pp. 60-69. May 1986.

[11] Shoji Kawahito, Michitaka Kameyama and tatsuo Higuchi, "VLSI-oriented bidirectional current-mode arithmetic circuits based on the radix-4 signed digit number system," *Proc. 16th ISMVL.*, Virginia, USA., pp. 70-77. May 1986.

[12] Rudolf Lidl, Gunter Pilz, *Applied Abstract Algebra*, Springer-Verlag, New York, 1984.

[13] Nell Weste, Kamran Eshraghian, *Principles of CMOS VLSI Design, A Systems Perspective*, AT&T Bell Laboratories, 1985 *

著 者 紹 介

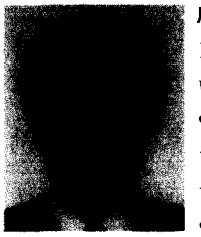


劉 仁 權 (正會員)

1959年 10月 11日生. 1986年 2月 인하대학교 전자공학과 졸업. 1988年 2月 인하대학교 대학원 전자공학과 졸업 공학석사학위 취득. 주관심분야는 VLSI 설계, 논리회로 설계 등임.

●

姜 聖 洙 (正會員) 第25卷 第5號 參照
현재 부천공업전문대학 전자계산학과 전임강사



成 賢 慶 (正會員)

1955年 12月 21日生. 1982年 인하대학교 전자공학과 졸업. 1984年 인하대학교 대학원 전자공학과 공학석사학위 취득. 1985年 인하대학교 대학원 전자공학과 박사과정 입학. 주관심분야는 이론 및 회로 설계, VLSI 설계, Coding theory 등임.

●

金 興 壽 (正會員) 第24卷 第5卷 參照
현재 인하대학교 전자공학과 교수