論文2002-39SC-2-5

전류모드 CMOS를 사용한 병렬 3치 승산기 설계

(The Design of Parallel Ternary-Valued Multiplier Using Current Mode CMOS)

沈 載 煥 *, 卞 基 寧 *, 尹 炳 熙 *, 李 相 睦 *, 金 興 壽 *

(Jai-Hwan Sim, Gi-Young Byun, Byoung-Hee Yoon, Sang-Mok Lee, and Heung-Soo Kim)

요 약

본 논문에서는 전류모드 CMOS를 통한 GF(3^m)상의 표준기저 승산회로를 제안하였다. 먼저, GF(3)연산을 위해 필요한 가산 및 승산을 진리표를 통해 정의하고 이를 CMOS회로로 설계하였다. GF(3^m)상의 임의의 두 원소들간의 승산의 전개방식을 수식을 통해 보였으며, 정의된 3치 기본연산자를 조합하여 GF(3^m) 승산회로를 설계하였다. 제안된 수식과 회로를 m에 대하여 일반화하였고, 그 중 m=3에 대한 설계의 예를 보였다. 본 논문에서 제안된 승산회로는 그 구성이 블록의 형태로 이루어지므로 m에 대한 확장이 용이하며, VLSI에 유리하다. 또한 회로내부에 메모리소자를 사용하지 않고, 연산디지트들이 병렬로 연산되므로 빠른 연산이 가능하다. 제안된 회로의 논리연산동작을 시뮬레이션을 통해 검증하였다.

Abstract

In this paper, a new standard basis parallel ternary-valued multiplier circuit designed using current mode CMOS is presented. Prior to constructing the GF(3^m) multiplier circuit, we provide a GF(3) adder and a GF(3) multiplier with truth tables and symbolize them, and also design them using current mode CMOS circuit. Using the basic ternary operation concept, a ternary adder and a multiplier, we develop the equations to multiply arbitrary two elements over GF(3^m). Following these equations, we can design a multiplier generalized to GF(3^m). For the proposed circuit in this paper, we show the example in GF(3^3). In this paper, we assemble the operation blocks into a complete GF(3^m) multiplier. Therefore the proposed circuit is easy to generalize for m and advantageous for VLSI. Also, it need no memory element and the latency not less fewer than other circuit. We verify the proposed circuit by functional simulation and show its result.

Ⅰ. 서 론

유한체(finite field)는 Golois(1811~1832)에 의해 발견된 수학의 한 분야로 Galois체, 또는 간단히 GF라 하며 오류정정부호(error-correcting codes), 스위칭이론(switching theory)및 암호이론(cryptography)등의 분야에 널리 적용되고 있는 연산체계이다. 유한체에서 중요하게 다루어지는 연산으로는 가산(addition), 승산(multiplication), 제산(division), 승산에 대한 역원(multiplicative inversion)등이 있으며, 회로복잡도(complexity)와 처리속도(speed)를 고려한 최적의 연산 알고리즘을 찾기 위한 연구가 오랜 기간 지속되고 있다. 현재의 실용회로에 있어 GF(2^m)상의 회로가 주류를 이루

* 正會員, 仁荷大學校 電子工學科
(Dept. of Electronics Eng., Inha Univ.)

※ 본 연구는 인하대학교 2001년도 연구비 지원에 의하여 수행되었습니다.

接受日字:2001年11月9日, 수정완료일:2002年1月25日

고 있으며, 1971년, B.A. Laws등이 표준기저를 이용한 Cellular-Array 승산기[1]를 보인 이후, C.S.Yeh[2], Massey-Omura[3], C.C.Wang[4]등이 제안한 승산회로가 대표적으로 알려져 있다. 이후 Z.kiamal의 MUX를 적용한 승산기[5]와 C.Y.Lee의 AOP, ESP 조건에서 구현한 Bit-parallel systolic multipliers[6]에 이르기까지 최적의 연산알고리즘을 통한 최적화된 회로의 설계를 위한 많은 연구결과들이 최근까지 이루어지고 있다[7-12]. 이진논리(binary logic)회로는 다양한 장점을 가지고 있으나 VLSI chip 면적의 약 70%가 내부결선에 사용됨으로써 발생되는 chip면적의 효율성 저하 및 내부결선의 복잡성, 단자수의 제한과 같은 근본적 문제들을 안고 있다[13, 14]. 이러한 문제들에 대한 개선방법 중 하나로 1970년대 초부터 다치논리(Multiple-Valued Logic) 회로에 관한 연구가 활발히 진행되어 왔다. 1981년, 4치 Read Only Memory(ROM)형태를 갖는 최초의 상용가능한 다치논리회로가 제안된 이후, Motorola, General Instruments semicustom ICs등이 이를 적용한 CPU와 메모리소자를 개발하였다[15]. 이와 같이 최근 다치 VLSI회로구현에 대한 높은 관심과 함께 다양한 연구결과들이 속속 발표되고 있는 추세이다. N.Kamiura[16]등은 CMOS에 의한 다치 Cellular-Array회로를 제안하였으며 T.Hanyu[17]등은 전류원제어에 의한 저전력 다치논리 집적회로의 설계와 함께 칩제작을 통해 다치논리 회로의 실용가능성을 보였다. 이러한 연구결과들을 토대로 본 논문에서는 GF(3^m)상의 표준기저를 적용한 전류모드 CMOS를 사용한 3치 승산기를 제안하였다. 본 논문에서 제안한 3치 승산회로는 각 디지트(digit)들의 병렬연산에 의해 동작되며, 회로모듈 내에 별도의 메모리소자를 필요로 하지 않으므로, 시간지연이 적게 발생하여 고속의 동작특성을 갖는다. 또한, 회로구성을 모듈화, 블록화 함으로써 m에 대한 확장과 VLSI(Very Large Scale Integrate)에 유리하도록 하였다. 제안된 회로의 구성방법에 대하여 m에 대한 일반화된 수식과 이를 통한 회로의 구현을 보였다. 설계의 예로써 GF(3^3)상의 승산회로를 설계하였으며, 설계된 회로의 동작을 시뮬레이션을 통해 확인하였다.

본 논문의 구성을 간략히 소개하면 1장의 서론에 이어, 2장에서는 본 논문에서 제안한 승산회로 구성을 위해 필요한 GF(3^m)상의 승산전개방식과 승산회로설계에 필요한 행렬방정식을 수식을 통해 정립하였다. 3장에서는 2장의 수식을 바탕으로 GF(3^m)상의 일반화된 승산회로와 m=3의 적용 예를 보였다. 4장에서는 전류모드 CMOS를 사용한 승산회로구성과 시뮬레이션 결과를 첨부하였다. 그리고, 결론을 통해 본 논문의 끝맺음을 하였다.

Ⅱ. GF(3^m)상의 승산의 전개

1. 유한체 상의 승산

유한체를 개략적으로 정의하면 유한개의 원소로 이루어진 집합에 대하여 그 원소들간의 연산이 사칙연산에 대하여 닫혀있는 집합체를 말한다. 유한체는 기초체(ground field) GF(p)와 이를 확장한 확대체(extension field) GF(p^m)로 구분된다. 여기서 p와 m은 각각 소수와 양의 정수이며, p 또는 p^m은 유한체 구성원소의 수를 나타낸다. 예를 들어, 유한체 GF(2)는 0과 1의 두 원소로 구성되며, 이러한 기초체를 확장한 확장체 GF(2^m)은 2^m개의 원소를 갖는다. 현재의 실용회로는 GF(2^m)이 주류를 이루고 있으나, 본 논문에서 언급되는 유한체는 GF(3^m)에 국한하기로 한다.

GF(3^m)상의 0(zero element)이 아닌 (3^m-1)개의 원소들은 원시원(primitive element) α를 통하여 식(1)과 같이 나타낼 수 있다. GF(3^m)상의 원시다항식(primitive polynomial) $F(x)$를 식(2)와 같이 나타낼 때, α는 $F(x)$의 근이므로 $F(\alpha)=0$이 성립한다. 따라서, $F(x)$에 의해 GF(3^m)의 각 원소들은 식(3)과 같이 차수가 (m-1)이하의 α의 다항식으로 표현된다.

$$GF(3^m)=\{0, \alpha^0, \alpha^1, \cdots \alpha^{q-2} \mid q=3^m\} \quad (1)$$

$$F(x)=x^m+f_{m-1}x^{m-1}+\cdots+fx+f_0 \quad (2)$$

$$GF(3^m)=\{0, \alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{q-2}\}_{\bmod F(x)}$$
$$=\{x_{m-1}\alpha^{m-1}+\cdots+x_1\alpha+x_0 \mid x_i \in GF(3), \; 0 \le i \le m-1\} \quad (3)$$

식(3)과 같이 GF(3^m)의 모든 원소들에 대하여 α^{m-1}이하의 다항식으로 표현하는 방법을 다항식표현(polynomial representation)이라 하고, α^{m-1}, α^{m-2}, …, α^0=1의 기저들을 표준기저(standard basis)라 한다. 또한, 다항식의 계수만을 표현하는 방법을 벡터표현(vector representation)이라 한다. GF(3^m)상의 임의의 두 원소를 A, B에 대하여 표준기저에 의한 다항식 표현으로 나타내면 각각 식(4), (5)와 같다.

$$A = a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} = \sum_{i=0}^{m-1} a_i \alpha^i \quad (4)$$

$$B = b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{m-1} = \sum_{i=0}^{m-1} b_i \alpha^i \quad (5)$$

유한체는 모듈러연산에 의해 그 연산이 이루어진다. GF(3^m)의 두 원소 A, B의 가산은 각 디지트들간의 모듈러-3가산으로 이루어지며, 그 결과를 식(6)에 나타내었다.

$$S = S_0 + S_1\alpha + \cdots + S_{m-1}\alpha^{m-1} = \sum_{i=0}^{m-1} S_i \alpha^i \quad (6)$$

모듈러-3 가산을 ⊕기호로 나타낼 때 식(6)의 각 계수 $S_i = a_i \oplus b_i (0 \le i \le m-1)$와 같이 구할 수 있다. 모듈러 연산의 정의에 의해 가산 후 발생하는 캐리(carry)를 고려하지 않으므로 가산은 비교적 쉽게 구현되나, 승산은 매우 복잡하게 구현되며 그 전개방식에 따라 다양한 회로구현이 가능하다[1-12]. 본 논문에서는 두 원소 A와 B의 승산을 P라 하고 새로운 전개방식을 식(7)에 나타내었다.

$$\begin{aligned} P &= AB = P_0 + P_1\alpha + \cdots + P_{m-1}\alpha^{m-1} \\ &= A\left(\sum_{i=0}^{m-1} b_i \alpha^i\right) = \sum_{i=0}^{m-1} b_i (A\,\alpha^i) \\ &= \sum_{i=0}^{m-1} b_i \left(\sum_{k=0}^{m-1} a^{(i)}{}_k \alpha^k\right) \end{aligned} \quad (7)$$

식(2)와 같이 GF(3^m)의 원시다항식 $F(x)$에 의하여 α^k의 계수 $a^{(i)}k$는 식(8)과 같이 나타낼 수 있다.

$$\begin{aligned} a^{(i+1)}k &= a^{(i)}k-1 \oplus 2f_k a^{(i)}m-1 \quad (1 \le k \le m-1) \\ &= 2f_k a^{(i)}m-1 \quad (k=0) \end{aligned} \quad (8)$$

$F(\alpha)$=0이므로 $x^m + f_{m-1}x^{m-1} + \cdots + f_x + f_0 = 0$이 되며, GF(3)에서 -1=2이므로 $x^m = -f_{m-1}x^{m-1} - \cdots - f_x - f_0 = 2f_{m-1}x^{m-1} + \cdots + 2f_x + 2f_0$이 성립한다. 식(8)을 적용한 $A\alpha^i$의 연산은 i를 0에서 m-1까지 순차적으로 대입함으로써 반복적으로(recursively) 구할 수 있다.

2. 행렬방정식[18-20]

GF(3^m)상의 원소들은 $F(x)$를 통해 m개 기저들의 선형결합에 의해 벡터로 표현됨을 전술하였다. GF(3^m)상의 임의의 두 원소들의 벡터표현 x, y에 대하여, 이들이 일정한 규칙 T에 의해 각각 입출력의 관계를 가질 때 이를 $y = Tx$와 같이 표현할 수 있다. 여기서 x, y를 각각 $m\times1$구조를 갖는 m-튜플(tuple)벡터로 가정할 때, T는 $m\times m$ 구조를 가지며, 전달행렬(transfer matrix)이라 할 수 있다. 주어진 조건에 대한 전달행렬에 대하여 이를 상사변환(similar transformation)에 의해 식(9)와 같이 표현될 수 있다.

$$T' = P^{-1}TP = \begin{pmatrix} C_1 & & & 0 \\ & C_2 & & \\ & & \ddots & \\ 0 & & & C_s \end{pmatrix} \quad (9)$$

여기서, P는 상사변환행렬이라 하며 $m\times m$구조를 갖는다. 한편, T가 $m\times m$구조를 갖는 행렬이므로 T의 특성다항식(characteristic equation)의 차수는 m이 되고 특성다항식의 최고차항 λ^m의 계수는 1이 된다. 이 성질을 갖는 다항식을 모닉(monic)다항식이라 하며, 모든 모닉다항식은 어떤 행렬의 특성다항식임을 보여준다. 특성다항식 $c(\lambda) = c_0 + c_1\lambda + \cdots + c_{m-1}\lambda^{m-1} + \lambda^m$는 식(10)의 행렬로 나타낼 수 있으며, 이때의 행렬 C를 특성다항식 c(λ)의 동반행렬(companion matrix)라 한다.

$$C = \begin{pmatrix} 0 & 0 & 0 & \cdots & -c_0 \\ 1 & 0 & 0 & \cdots & -c_1 \\ 0 & 1 & 0 & \cdots & -c_2 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & -c_{n-1} \end{pmatrix} \quad (10)$$

GF(3^m)상의 원시다항식 $F(x)$를 통해 표준기저의 다항식표현으로 나타내어진 임의의 원소 $\alpha^i (0 \le i \le m-2)$로부터 α^{i+1}의 다항식표현을 구하면 식 (11)와 같다.

$$\begin{aligned} \alpha^{i+1} &= \alpha^i\alpha = (x_{m-1}\alpha^{m-1} + \cdots + x_1\alpha^1 + x_0)\alpha \\ &= x_{m-1}\alpha^m + \cdots + x_1\alpha^2 + x_0\alpha \\ &= x_{m-1}(2f_{m-1}\alpha^{m-1} + \cdots + 2f_1\alpha^1 + 2f_0) \\ &\quad + x_{m-2}\alpha^{m-1} + \cdots + x_1\alpha^2 + x_0\alpha \\ &= (x_{m-2} \oplus 2x_{m-1}f_{m-1})\alpha^{m-1} + \cdots \\ &\quad + (x_1 \oplus 2x_{m-1}f_2)\alpha^{02} \\ &\quad + (x_0 \oplus 2x_{m-1}f_1)\alpha + 2x_{m-1}f_0 \end{aligned} \quad (11)$$

원시다항식 $F(x)$는 모닉 다항식의 조건을 만족한다. 또한, 유한체의 성질에 의해 식 (12)와 같이 동반행렬

로 표현되며, 이에 따라 식(11)을 행렬표현형식으로 나타내면 식(13)와 같다.

$$T=\begin{pmatrix} 0 & 0 & \cdots & 0 & -f_0 \\ 1 & 0 & \cdots & 0 & -f_1 \\ 0 & 1 & \cdots & 0 & -f_2 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 1 & -f_{m-1} \end{pmatrix} \tag{12}$$

$$a^{i+1} = T\, a^{i}$$

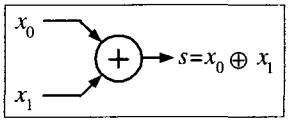
$$\begin{pmatrix} x_0^{(i+1)} \\ x_1^{(i+1)} \\ \vdots \\ x_{m-2}^{(i+1)} \\ x_{m-1}^{(i+1)} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 2f_0 \\ 1 & 0 & \cdots & 0 & 2f_1 \\ 0 & 1 & \cdots & 0 & 2f_2 \\ & \vdots & & & \vdots \\ 0 & 0 & \cdots & 1 & 2f_{m-1} \end{pmatrix} \begin{pmatrix} x_0^{(i)} \\ x_1^{(i)} \\ \vdots \\ x_{m-2}^{(i)} \\ x_{m-1}^{(i)} \end{pmatrix} \tag{13}$$

Ⅲ. GF(3^m)상의 승산회로의 구성

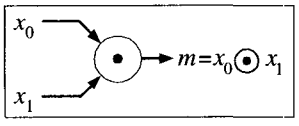
GF(3^m)상의 승산회로 구성에 앞서, 회로구성에 필요한 기본논리소자를 정의한다. GF(3)상의 가산 및 승산은 모듈러-3 연산으로 이루어지며, 이를 각각 ⊕와 ⊙ 기호로 나타내어 진리표를 통해 정의하면 표 1과 같다.

표 1. GF(3)상의 가산 및 승산 진리표
Table 1. Addition and multiplication table over GF(3).

GF(3)	가산 ⊕			승산 ⊙		
	0	1	2	0	1	2
0	0	1	2	0	0	0
1	1	2	0	0	1	2
2	2	0	1	0	2	1



(a) GF(3) 가산기



(b) GF(3) 승산기

그림 1. GF(3) 기본논리게이트
Fig. 1. Bisic logic gates over GF(3).

표 1의 성질을 만족하는 GF(3)상의 가산 및 승산게이트를 기호로 나타내면 그림 1과 같으며, 이를 각각 GF(3) 가산기(adder) 및 승산기(multiplier)라 명하기로 한다.

그림 1에서 x_0, x_1, s, $m \in$GF(3)이며, $s=(x_0 \oplus x_1)$, $m=(x_0 \odot x_1)$이다. 그림 1의 게이트를 통해 GF(3^m)상에서 주어진 원시다항식 $f(x)$에 대하여 식(8)과 이를 m비트로 확장한 식(13)을 회로로 설계하면 그림 2와 같다.

그림 2의 회로를 포함하여 식(7)의 GF(3^m)에 대한 일반화된 승산회로를 구성하면 그림 3과 같다.

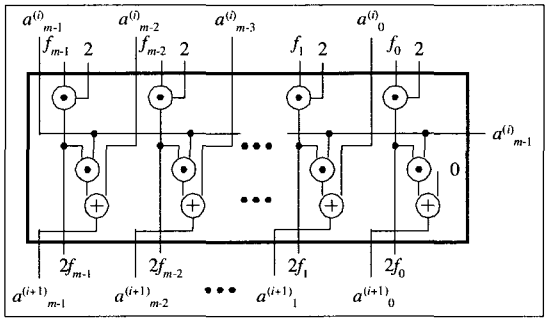


그림 2. 식(13)에 대한 회로설계
Fig. 2. Circuit design for Eq. (13)

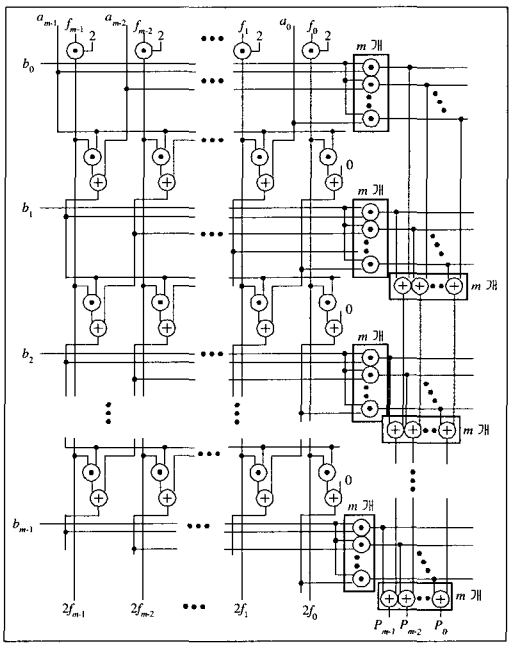


그림 3. 본 논문에서 제안한 GF(3^m)의 승산회로
Fig. 3. Multiplication circuit over GF(3^m) proposed in this paper.

본 논문에서 제안한 GF(3^m)의 승산회로로 부터 m=3에 대한 회로를 설계하기 위해 원시다항식을 다음과 같이 정의한다. $F(x)=x^3+2x+1$. F(x)를 통해 GF(3^3)의 모든 원소들은 α^2, α^1, α^0의 기저들로 표현될 수 있으며 이를 표 2에 정리하였다.

표 2. 표준기저에 의한 GF(33)상의 원소표시 $F(x)=x^3+2x+1$

Table 2. Elements representation over GF(33) based on the standard basis. $F(x)=x^3+2x+1$

원소	다항식표현	백터표현 $\alpha^2\alpha^1\alpha^0$
α^*	0	0 0 0
α^0	$\alpha^0=1$	0 0 1
α^1	α^1	0 1 0
α^2	α^2	1 0 0
α^3	$\alpha+2$	0 1 2
α^4	$\alpha^2+2\alpha$	1 2 0
α^5	$2\alpha^2+\alpha+2$	2 1 2
α^6	$\alpha^2+\alpha+1$	1 1 1
α^7	$\alpha^2+2\alpha+2$	1 2 2
α^8	$2\alpha^2+2$	2 0 2
α^9	$\alpha+1$	0 1 1
α^{10}	$\alpha^2+\alpha$	1 1 0
α^{11}	$\alpha^2+\alpha+2$	1 1 2
α^{12}	α^2+2	1 0 2
α^{13}	2	0 0 2
α^{14}	2α	0 2 0
α^{15}	$2\alpha^2$	2 0 0
α^{16}	$2\alpha+1$	0 2 1
α^{17}	$2\alpha^2+\alpha$	2 1 0
α^{18}	$\alpha^2+2\alpha+1$	1 2 1
α^{19}	$2\alpha^2+2\alpha+2$	2 2 2
α^{20}	$2\alpha^2+\alpha+1$	2 1 1
α^{21}	α^2+1	1 0 1
α^{22}	$2\alpha+2$	0 2 2
α^{23}	$2\alpha^2+2\alpha$	2 2 0
α^{24}	$2\alpha^2+2\alpha+1$	2 2 1
α^{25}	$2\alpha^2+1$	2 0 1

GF(3^3)상의 원시다항식 $F(x)=x^3+2x+1$을 식 (13)에 적용하면 식 (14)와 같다.

$$\alpha^{i+1} = T\,\alpha^{i}$$

$$\begin{pmatrix} x_0^{(i+1)} \\ x_1^{(i+1)} \\ \vdots \\ x_{m-2}^{(i+1)} \\ x_{m-1}^{(i+1)} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 2f_0 \\ 1 & 0 & \cdots & 0 & 2f_1 \\ 0 & 1 & \cdots & 0 & 2f_2 \\ & \vdots & & & \vdots \\ 0 & 0 & \cdots & 1 & 2f_{m-1} \end{pmatrix} \begin{pmatrix} x_0^{(i)} \\ x_1^{(i)} \\ \vdots \\ x_{m-2}^{(i)} \\ x_{m-1}^{(i)} \end{pmatrix} \quad (14)$$

이를 통해 그림 2와 같은 연산블럭을 구성한 후 GF(3^3) 상의 임의의 두 원소 $A(a_2a_1a_0)$와 $B(b_2b_1b_0)$의 승산회로를 완성하면 그림 4와 같다.

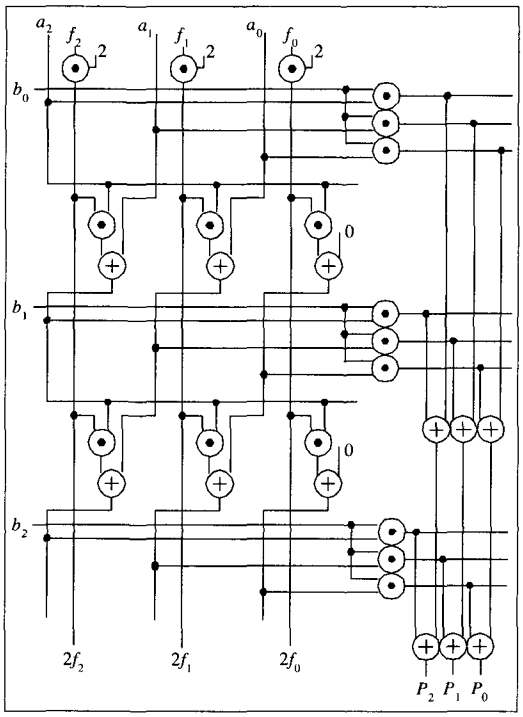


그림 4. 본 논문에서 제안한 GF(3^3)의 승산회로

Fig. 4. Multiplication circuit over GF(3^3) proposed in this paper.

Ⅳ. 전류모드 CMOS를 사용한 GF(3^m) 승산기 설계

본 논문에서 제한한 GF(3^m)상의 승산회로의 VLSI구현을 위해 그림 1(a)의 GF(3) 가산 게이트를 전류모드 CMOS를 통해 그림 5와 같이 설계하였다. 본 논문에서 사용한 설계 시뮬레이션 툴은 PSPICE의 Level 3 parameter 1.5μm 공정을 사용하였다.

회로의 단위전류(unit current) I_u는 15μA를 사용하였다. 그림 5의 M8, M9와 M10, M11은 각각 입력 x_0와 x_1에 대한 전류미러로 동작한다. M11은 입력된 두 전류 x_0와 x_1의 합에 의해 구동되며, M7은 이 전류값을 복제(미러)하여 출력에 나타낸다. 한편, 전류원 M4와 M5에 연결된 M12, 13, 14, 15, 17, 18은 전류비교기로써 흐르는 전류의 양을 조절하여 GF(3)상의 오버플로가 생김을 방지한다. 즉, 전류원 M2는 2.5I_u의 전류를

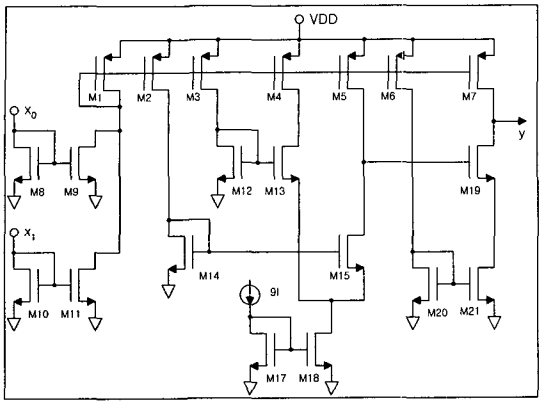


그림 5. GF(3)가산기에 대한 전류모드 CMOS 회로설계
Fig. 5. Current mode CMOS circuit design over GF(3) adder.

생성하고, M3는 두 입력전류의 합을 복제한다. 두 입력의 합이 $2.5I_u$보다 낮을 때 M19는 OFF되며, 출력 $y=(x_0+x_1)$이 나타난다. 또한, 두 입력의 합이 $2.5I_u$보다 높을 때 M7의 전류는 M6의 $3I_u$에 의해 $y=(x_0+x_1)-3I_u$로 나타나게 된다. 따라서, 그림 5의 회로는 GF(3)상의 가산기, 즉 $y=(x_0+x_1)_{\mathrm{mod}(3)}=(x_0\oplus x_1)$로 동작하며 그 시뮬레이션 결과는 그림 6와 같다.

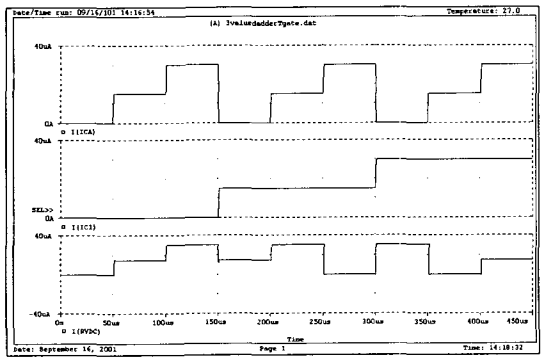


그림 6. 그림 5 회로의 시뮬레이션 결과
Fig. 6. Simulation result of Fig. 5

그림 6은 전류모드 CMOS에 의한 그림 5의 mod(3) 가산연산회로에 대한 시뮬레이션 결과이다. 입력 $x_0(I_x)$의 전류를 0μs에서 50μs간격으로 0μA에서 15μA씩 증가함으로써 GF(3)상의 세 신호레벨을 갖도록 하였다. 입력 x_0와 함께 연산을 이룰 또 다른 입력 x_1은 0μs에서 150μs간격으로 0μA에서 15μA씩 증가하는 신호레벨을 갖게 한후 그 출력을 M21의 드레인에서 보았다. 신호입력 x_0와 x_1의 변화에 따라 표 1의 연산결과를 가짐을 확인하였다. 또한, 그림 1(b)의 GF(3) 승산 게이트에 대한 전류모드 CMOS회로설계를 그림 7에 보였다.

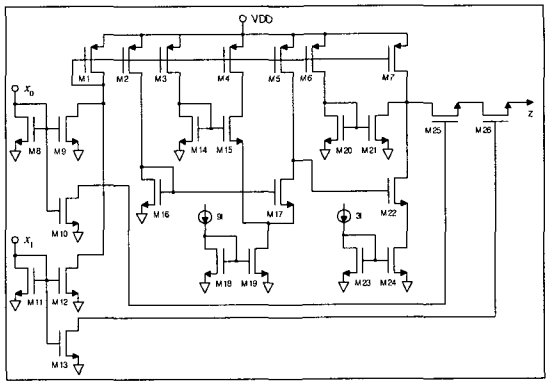


그림 7. GF(3)승산기에 대한 전류모드 CMOS 회로설계
Fig. 7. Current Mode CMOS circuit design over GF(3) multiplier.

그림 7의 트랜지스터 M8, M9와 M11, M12는 각각 입력 x_0와 x_1에 대한 전류미러로 동작한다. 이때, 전류원 M1은 x_0와 x_1의 합전류에 의해 구동되며, 이 전류값은 M7에 의해 복제된다. 전류원 M4와 M5에 연결된 M14, M15, M16, M17, M18과 M19는 전류비교기역할을 수행한다. 전류원 M2는 기준전류 $3.5I_u$를 생성하며, 전류원 M3는 두 입력 전류의 합을 복제한다. 복제된 전류가 기준전류 $4.5I_u$보다 작을 때 M22가 OFF동작이 되며, 이에 따라 M1에 대하여 M7에 의해 복제된 두 입력의 합전류는 M20과 M21에 의해 감소되도록 하였다. 즉, 출력 $y=(x_0+x_1)-Iu$가 얻어지도록 하였다. 이를 위해 M6의 W/L비를 20μm/2μm로 조정하였다. 또한, 복사된 전류가 기준전류 $3.5I_u$에 비해 보다 높을 때, M22가 ON되며 이때, M23과 M24에 의해 복사된 전류 $2I_u$만큼 M7의 전류가 감소된다. 따라서, 출력 $z=(a_i+b_i)-(I_u+2I_u)$로 나타나게 되며 GF(3)상의 승산이 구현된다. 그림 7의 회로에 대한 시뮬레이션결과를 그림 8에 나타내었다. 입력 x_0와 x_1은 각각 50μs와 150μs마다 15μA씩 증가하도록 하였다.

그림 9은 두 입력 $A(a_2a_1a_0)$와 $B(b_2b_1b_0)$를 갖는 그림 4의 GF(33) 승산기에 대한 논리시뮬레이션 결과 중 그 일부를 보였다. 시뮬레이션 조건은 그림 6, 8과 동일한 조건에서 실행하였다. GF(3^3)상의 임의의 두 원소의 승산이 이루어지는 모든 경우의 수는 36=729가지이며

하나의 신호를 50μs에 표현하고자 할 때, 총 36.45ms에 걸쳐 모든 동작을 확인할 수 있다.

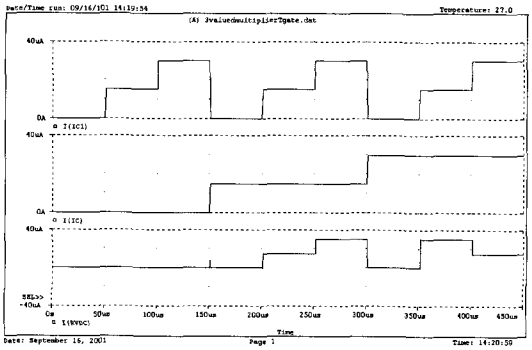


그림 8. 그림 7회로의 시뮬레이션결과
Fig. 8. Simulation result of Fig. 7

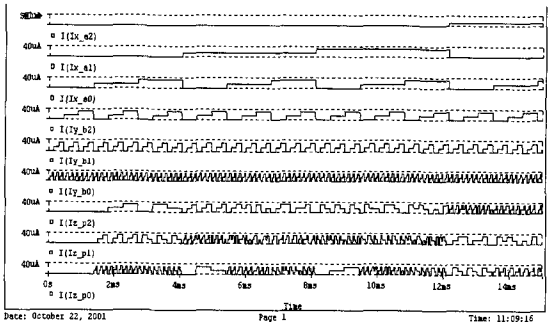


그림 9. GF(33) 승산회로의 시뮬레이션 결과
Fig. 9. Simulation result of GF(33) multiplication circuit.

그림 9에서 첫 번째부터 세 번째 줄까지는 GF(3^3)상의 임의의 한 원소 $A(a_2a_1a_0)$를 가정한 것이며, 네 번째부터 여섯 번째 줄까지는 또 다른 한 원소 $B(b_2b_1b_0)$의 각 디지트들의 값을 가정한 것이다. 이들 두 원소들의 각 디지트들로 부터의 승산결과가 일곱째부터 아홉째 줄을 통해 보여지고 있다. 구간 0~1.35ms까지는 A의 각 디지트들이 000이며 이에 임의의 B를 승산한 결과는 항상 000이 나타남을 확인할 수 있다. 또한, 1.35ms~2.7ms까지의 A의 각 디지트들은 001로서 이에 임의의 B를 승산한 결과는 곧 B로서 나타나며, 2.7ms~4.05ms까지는 B의 각 디지트들에 모듈러 2승산을 취한 결과가 나타난다. 이후, 각 연산의 결과는 모두 GF(3^3)상의 연산을 만족함을 확인할 수 있다.

V. 결 론

기존의 이진논리의 경우, GF(2)상의 가산과 승산은 각각 EX-OR 게이트와 AND 게이트로써 구현하고 있으나, GF(3)의 경우 이에 적합한 새로운 연산자를 정의할 필요가 있다. 본 논문에서는 GF(3)상의 가산 및 승산연산자를 진리표로써 정의하였고 이를 전류모드 CMOS에 의해 회로로 설계하였으며 그 연산결과를 시뮬레이션하였다. 이를 위해 GF(3^m)상의 원소들의 승산에 대한 전개방식을 수식을 통해 보였고, 본 논문에서 정의한 3치 기본 연산자를 사용하여 GF(3^m)상의 병렬 승산회로를 설계하였다. 본문에서 설계한 3치 기본 연산회로는 비교적 손쉬운 설계방식인 전류미러의 조합으로 회로를 설계하였고, 흐르는 전류의 양과 쓰레숄드 값을 조정하여 그 기능을 구현하도록 하였으나, MUX나 T-Gate 등을 이용하여 구현할 수도 있겠다. 또한, 다양한 CMOS 회로설계기법에 따라 보다 개선된 형태의 회로가 제안될 수 있다.

GF(p^m)상의 유한체 연산기에서 데이터 처리량은 2치에 비해 3치의 경우 $(3/2)^m=1.5^m$으로 m의 증가에 따라 비약적으로 증가되며, 특히 실용회로가 m=8이상인 점을 감안하면 대단히 큰 차이라 할 수 있다. 따라서, 다양한 3치연산회로의 개발은 차세대 VLSI 회로에 매우 중요한 가치를 갖으리라 사료된다.

참 고 문 헌

[1] B. A. Laws and C. K. Rushford, "A Cellular-Array Multiplier for GF(2^m)" *IEEE Trans. Comp.*, vol. C-20, no. 12, pp. 1573~1578, Dec. 1971.

[2] C. S. Yeh, I. S. Reed, and T. K. Trung. "Systolic multipliers for finite field GF(2^m)," *IEEE Trans.* Computer, vol. C-33, pp. 357~360, Apr. 1984.

[3] J. Omura and J. Massey, "Computational Method and Apparatus for Finite Fields," *U.S. Patent* no. 4,587,627, May 1986.

[4] C. C. Wang, T. K. Trung, H. M. Shao, L. J. Deutsch, J. K. Omura, and I. S. Reed., "VLSI Architecture for Computing Multiplications and

Inverses in GF(2^m)," *IEEE Trans. Comp.*, vol. C-34, pp. 709~717, Aug. 1985.

[5] K. Z. Pekmestzi, "Multiplexer-Based Array Multipliers," *IEEE Trans. Computer*, vol. 48, no. 1, pp. 15~23. Jan. 1999.

[6] C. Y. Lee, E. H. Lu, and J. Y. Lee, "Bit-Parallel Systolic Multipliers for GF(2^m) Fields Defined by All-One and Equally Spaced Polynomials," *IEEE Trans. Comp.*, vol. 50, no. 5, pp. 385~393, May. 2001.

[7] E. R. Berlekamp, "Bit-Serial Reed-Solomon Encoders," *IEEE Trans. Information Theory*, vol. 28, pp. 869~874, Nov. 1982.

[8] S. T. J. Fenn, M. Benaissa, and D. Taylor, "GF (2^m) Multiplication and Division Over the Dual Basis," *IEEE Trans. Comp.*, vol. 45, no. 3, pp. 37~46, Jan. 1982.

[9] I. S. Hsu, T. K. Troung, L. J. Deutsch, and I. S. Reed, "A Comparision of VLSI Architecture of Multipliers using Dual, Normal, or Standard Bases," *IEEE Trans. Computer*, vol. C-37, pp. 735~739, 1988.

[10] E. D. Mastrovito, "VLSI Design for Multiplication over Finite Fields," *LNCS-357, Proc. AAECC-6*, pp. 297~309, Rome, July 1988, Spring-Verlag.

[11] G. L. Feng, "A VLSI Architecture for Fast Inversion in GF(2^m)," *IEEE Trans. Computer*, vol. 38, no. 10, Oct. 1989.

[12] C. K. Koc, and B. Sunar, "Low-Complexity Bit Parallel Canonical and Normal Basis Multipliers for a Class of Finite Fields," *IEEE Trans. Computer*, vol. 47, no. 3, pp. 353~356. Mar. 1998.

[13] J. T. Butler, "Multiple-valued logic :guest editor's introduction and bibliography," *IEEE Computer, Mag.*, vol. 21, pp. 13~15, Apr. 1988.

[14] J. C. Muzio, "Introduction multiple-valued logic," *IEEE Trans. Computer*, vol. 35, pp. 97~98. Feb. 1986.

[15] Y. Hata, N. Kamiura and K. Yamato, "Design of Multiple-Valued Programmable Logic Array with Unary Function Generators", *IEICE Trans. INF. & SYST.* vol. E82-D, no. 9, pp. 1254~1260, Sep. 1999.

[16] N. Kamiura, Y. Hata and K. Yamato, "Design of a Multiple-Valued Cellular Array", *IEICE Trans. Electron.*, vol. E76-C, no. 3, pp. 412~418, Mar. 1993.

[17] T. Hanyu, S. Kazama, M. Kameyama, "Design and implementation of a Low-Power Multiple-Valued Current Mode Integrated Circuit with Current-Source Control", *IEICE Trans. Electron* vol. E80-C, no. 7, pp. 941~947, July 1997.

[18] A. Gill, *Linear Sequential Circuits*, McGraw-Hill Book Co., Newyork. 1966.

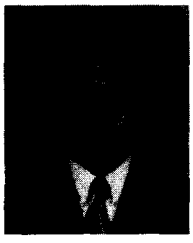
[19] H. Anton, Elementary Linear Algebra, John Wiley & Sons, Inc., Newyork. 1994.

[20] E. Kreyszig, *Advanced Engineering Mathematics 8/e*, John Wiley & Sons, Inc., Newyork. 1999.

저 자 소 개

沈 載 煥(正會員)

1976년 2월 : 인하대학교 전자공학과 졸업(공학사). 1982년 2월 : 숭실대학교 대학원 전자공학과 졸업(공학석사). 1996년 8월~1999년 8월 : 인하대학교 전자공학과 박사과정 수료. 현재 : 시립 인천 전문대학 통신과 교수. <주관심분야 : 부호이론, 다치논리시스템, VLSI 등>



尹 炳 熙(正會員)

1997년 2월 : 원광대학교 전자공학과 졸업(공학사). 1999년 2월 : 인하대학교 대학원 전자공학과 졸업(공학석사). 1999년 3월~현재 : 인하대학교 대학원 전자공학과 박사과정. <주관심분야 : 다치논리시스템, VLSI설계, FPGA 등임>

卞 基 寧(正會員)
1994년 2월 : 인하대학교 전자공학과 졸업(공학사). 1998년 8월 : 인하대학교 대학원 전자공학과 졸업(공학석사). 1999년 3월~현재 : 인하대학교 대학원 전자공학과 박사과정. 1994년 1월~1996년 8월 : ㈜LG전자 VCR사업부 회로설계연구원 근무. <주관심분야 : 정보이론, 부호이론, 다치논리시스템, VLSI설계, 유한체 이론의 응용 및 회로구현 등임>

李 相 睦(正會員)
1984년 2월 : 한국항공대학교 항공전자공학과 졸업(공학사). 1986년 2월 : 한국항공대학교 항공전자공학과 대학원 졸업(공학석사). 1996년 8월~현재 : 인하대학교 전자공학과 박사과정 수료. 1990년 3월~현재 : 재능대학 정보통신과 부교수. <주관심분야 : 안테나 설계, 통신망, 통신이론>

金 興 壽(正會員) 第37卷 SC編 第6號 參照
현재 : 인하대학교 전자공학과 교수