유한체상의 순차논리머시인 구성에 관한 연구

박춘명*

*충주대학교 전기.전자 및 정보공학부 컴퓨터공학전공

A Study on Constructing the Sequential Logic Machines over Finite Fields

Chun-Myoung Park*

*Major of Computer Engineering, School of EEIE, Chungju National University

E-mail : cmpark@chungju.ac.kr

요 약

본 논문에서는 유한체 GF(P)상의 순차논리머시인구성 방법의 한가지를 제안하였다.

제안한 순차논리머시인구성 방법은 먼저 GF(P)상에서의 순차논리머시인의 수학적 성질을 논의하였으며, 순차논리머시인 구성을 위하여 기본의 3가지 회로소자를 사용하여 선형궤환시프트레지스터와 이에 대한 행렬표현에 대해 논의하였다. 그리고, 제안한 방법을 제산연산처리에 적용하였다.

ABSTRACT

This paper presents a method of constructing the sequential logic machines over finite fields(or galois fields). The proposed the sequential logic machines is constructed by as following. First of all, we obtain the linear characteristics between present state and next state based on mathematical properties of finite fields and sequential logic machines. Next, we realize the sequential logic machines over finite field GF(P) using above linear characteristics and characteristic polynomial that expressed using by matrix.

키워드

Galois Fields, Sequential Logic Machines, Shift Register, Matrix, Division

Ⅰ. 서 론

일반적으로 대수학인 유한체에 근간을 두고 많은 학문이 발전해 왔으며, 소수인 P와 양의 정수인 m으로 표현되는 유한체를 Galois체 $GF(P^m)$으로 표현한다.

특히, P=2이고 m=1인 경우의 GF(2)는 현존의 2진 논리에 해당하는 디지털시스템의 근간인 부울대수(boolean algebra)에 귀착되며 오진정정코드(error correcting code) 분야를 비롯하여 디지털 스위칭이론, 디지털신호처리(DSP), 디지털정보처리(DIP), 디지털통신에서의 디지털정보에 대한 암호화(Encryption)와 복호화(Decryption), 고속산술연산기 구성 등과 같은 여러 분야에 걸쳐 적용 및 응용되고 있다.[1-6]

한편, 최근에는 멀티미디어 H/W와 S/W에 기반을 둔 여러 분야가 매우 급속도로 발전되고 있으며 21C에는 더욱 더 활용 및 적용이 요구될 것이다.

특히, 멀티미디어 H/W는 지금까지의 각종 데이터 처리보다는 훨씬 방대한 데이터 량, 최적의 데이터 압축 및 복원, 초고속 전송 등의 복합적이고 고기능의 기술이 요구되고 있으며, 최근에 각종 멀티미디어 H/W 시스템에기본적으로 필요로하는 산술연산을 효과적으로 수행 할 수 있는 산술연산기시스템 구성에 대한 연구들이 진행되고 있다.[7-8]

일반적으로 유한체는 기초체 GF(P)와 이의 확대인 확대체 $GF(P^m)$으로 분류되며, 본 논문에서는 기초체인 GF(P) 상에서의 순차논리머시인구성의 한가지 방법을 제안하다.

본 논문의 서술과정은 다음과 같다.

Ⅱ장에서는 순차논리머시인의 수학적 성질을 논

의하였으며, Ⅲ장에서는 GF(P)상의 순차논리머시인 구성에 사용되는 선형궤환시프트레지스터와 이에 대한 행렬표현에 대해 서술하였다.

그리고 Ⅳ장에서는 Ⅲ장에서 구성한 순차논리머시인을 GF(P)상의 제산처리(division arithmetic operation processing)에 적용하는 예를 들었다.

마지막 Ⅴ장에서는 본 논문에서 제안한 선형궤환시프트레지스터를 사용하여 구성한 순차논리머시인의 특징을 요약하였으며 향 후 연구과제에 대해 기술하였다.

Ⅱ. 순차논리머시인의 수학적 성질

유한체 GF(P)상에는 P개의 원소가 존재하고 이들 원소를 e_i(i=0,1,2, ... ,P-1)로 표시한다. 이외의 유한체에 대한 수학적 성질은 참고문헌[9-12]을 참조하였다.

한편, 순차논리머시인의 출력은 조합논리와는 달리 현재입력 뿐만 아니라 과거의 입력에 의해서도 결정되는 특징을 갖고 있다.

따라서, 순차논리머시인에서 현재의 출력은 지연소자 또는 기억소자에 의해서 그 정보가 입력으로 궤환되어져야 한다.

일반적으로 순차논리머시인 M은 다음 식2-1과 같이 5-tuple로 표현된다.

$$M=(S, I, Z, \delta, \lambda) \quad (2\text{-}1)$$
$$S, I, Z=e_i \in GF(P)(i=0,1,2, \ldots\ldots ,P-1)$$

여기서, S는 상태, I는 입력, Z는 출력, δ는 차순상태함수, λ는 출력함수를 각각 의미한다.

또한, 위 식2-1은 다음 식2-2와 같은 사상(mapping) 관계를 갖는다.

$$S_t \times I_t \xrightarrow{\delta} S_{t+1} \quad (2\text{-}2)$$

여기서, S_t는 현재상태이며 S_{t+1}은 차순상태이다.

한편, λ는 Mealy model과 Moore model에 따라 다음 식2-3과 식2-4와 같다.

• Mealy model :

$$S_t \times I_t \xrightarrow{\lambda} S_{t+1} \quad (2\text{-}3)$$

• Moore model :

$$S_t \xrightarrow{\lambda} S_{t+1} \quad (2\text{-}4)$$

즉, Moore model에서의 출력은 오직 현재상태의 함수로만 이루어진다.

한편, GF(P)상의 행렬(Matrix)을 각각 *A*, *B*, *C*, *D* 라 하면 위 식2-2, 식2-3, 식2-4는 각각 다음 식2-5, 식2-6, 식2-7로 표현 할 수 있다.

$$\delta(S_t, I_t) = S_{t+1} = A \bullet S_t + B \bullet I_t \quad (2\text{-}5)$$
$$Z_t = C \bullet S_t + D \bullet I_t \quad (2\text{-}6)$$
$$Z_t = C \bullet S_t \quad (2\text{-}7)$$

Ⅲ. 순차논리머시인구성

3-1. 선형궤환시프트레지스터구성

Ⅱ장의 식(2-5)에서 살펴 본바와 같이 시간 t에서의 현재상태 S_t와 시간 (t+1)에서의 차순상태 S_{t+1}은 선형관계가 존재한다.

따라서, 위 내용과 다음의 그림3-1, 그림3-2, 그림3-3의 회로소자들을 사용하여 선형궤환시프트레지스터를 구성하면 다음 그림3-4와 같다.

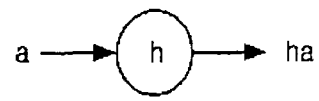

그림 3-1. modP 스칼라 곱 회로 심볼
Fig. 3-1. The circuit symbol modP scalar product.

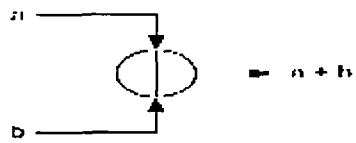

그림 3-2. modP 가산연산 심볼
Fig. 3-2. The circuit symbol of modP addition.

특히, P=2인 경우에 ⊕는 Exclusive-OR 게이트로 대체된다.

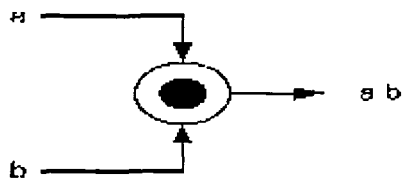

그림 3-3. modP 승산연산 심볼
Fig. 3-3. The circuit symbol of modP multiplication

특히, P=2인 경우는 ⊙는 AND 게이트로 대체된다.

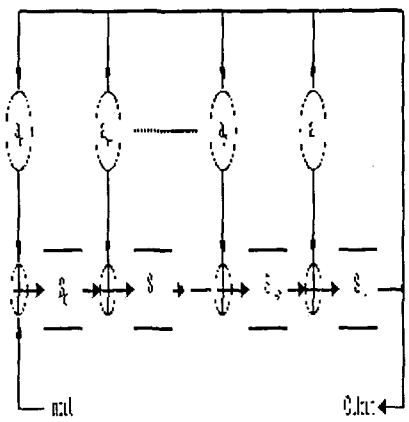

그림. 3-4. 선형궤환레지스터
Fig. 3-4. Linear feed-back shift register.

여기서, $S_0 = a_n S_{n-1}$
$S_t = a_{n-1} S_{n-1} + S_{t-1} (0 < t < n)$
$a_i \in GF(P)(i=0,1, \ldots\ldots, n-1)$

3-2. 선형궤환레지스터의 행렬 표현

선형궤환레지스터의 행렬 **A**에 대한 특성다항식(Characteristics polynomial)은 다름 식3-1로부터 구할 수 있다.

$$\det(\mathbf{X} \cdot \mathbf{I} - \mathbf{A}) \quad (3\text{-}1)$$

여기서 **I**는 Identity 행렬이다.

이제 식3-1로부터 선형궤환시프트레지스터의 특성다항식은 다음 식3-2에 의해 구할 수 있다.

$$P(X) = X^n - a_1 X^{n-1} - a_2 X^{n-2} - \ldots\ldots - a_n \quad (3\text{-}2)$$

여기서 $a_i (i=1,2, \ldots\ldots, n) \in GF(P)$

Ⅳ. 적용 예

이 장에서는 Ⅲ장의 내용이 어떻게 적용되는지 GF(P)상의 제산연산 처리에 적용하여 각각 몫과 나머지를 구하는 과정을 살펴보기로 한다.

[예1] GF(3)상의 순차논리머시인 구성

다음 그림4-1과 같은 GF(3)상의 임의의 상태천이도(State-transition diagram)가 주어졌다고 하면, 각각 차순상태함수는 다음 식4-1, 식4-2, 식4-2과 같다.

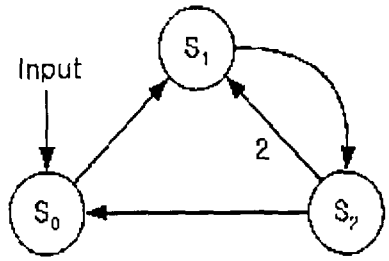

그림. 4-1. GF(3)상의 상태천이도
Fig. 4-1. State-transition diagram over GF(3)

$$[S_0]_{t+1} = [S_2]_t + \text{Input} \quad (4\text{-}1)$$
$$[S_1]_{t+1} = [S_0]_t + 2[S_2]_t \quad (4\text{-}2)$$
$$[S_2]_{t+1} = [S_1]_t \quad (4\text{-}3)$$

따라서 행렬 **A**는 다음 식4-4와 같다.

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 0 \end{bmatrix} \quad (4\text{-}4)$$

한편, 특성다항식을 구하면 다음 식4-5와 같다.

$$\det(\mathbf{XI-A}) = X^3 + X + 2 = (1012) \quad (4\text{-}5)$$

이제 식4-5와 Ⅲ장의 식3-2를 토대로 선형궤환시프트레지스터를 사용한 순차논리머시인을 구성하면 다음 그림4-2와 같다.

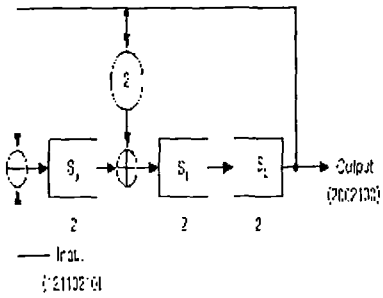

그림 4-2. 그림 4-1의 순차논리머시인
Fig. 4-2. Sequential logic machines of fig.4-1.

여기서, 입력 데이터 열이 $X^7 + 2X^6 + X^4 + 2X^2 + X = (12110210)$이라면, 이는 $(X^7 + 2X^6 + X^4 + 2X^2 + X)/(X^3 + X + 2)$와 같고 이를 수행하는 과정은 다음 표4-1과 같다.

표 4-1. 입력 데이터 (12110210)에 대한 수행과정
Table. 4-1. Procedure of input data (12110210)

		S_0	S_1	S_2	Output	
	Initial	0	0	0		
Input data stream	1	1	0	0	0	Quotient
	2	2	1	0	0	
	1	1	2	1	1	
	1	2	0	2	2	
	0	2	0	0	0	
	2	2	2	2	0	
	1	1	2	2	2	
	0	2	2	1		

Remainder

[예2] GF(2)상의 순차논리머시인 구성

다음 그림4-3과 같은 GF(2)상의 임의의 상태천이도가 주어졌다고 하면, 각각 차순상태함수는 다음 식4-6, 식4-7, 식4-8과 같으며 이를 시프트레지스터를 사용한 순차논리머시인을 구성하면 다음 그림 4-4와 같다.

$$[S_0]_{t+1} = [S_2]_t + \text{Input} \quad (4\text{-}6)$$

$$[S_1]_{t+1} = [S_0]_t \quad (4\text{-}7)$$

$$[S_2]_{t+1} = [S_1]_t + [S_2]_t \quad (4\text{-}8)$$

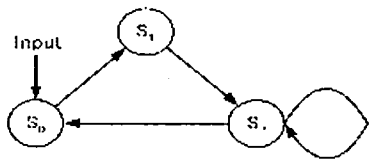

그림. 4-3. GF(2)상의 상태천이도
Fig. 4-3. State-transition diagram over GF(2)

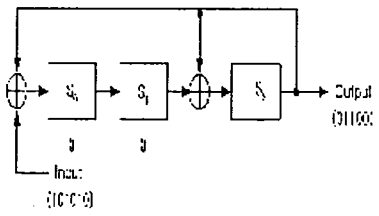

그림 4-4. 그림4-3의 순차논리머시인
Fig. 4-4. Sequential logic machine of fig.4-3.

V. 결 론

본 논문에서는 유한체 GF(P)상의 순차논리머시인구성 방법의 한가지를 제안하였다.

제안한 순차논리머시인구성 방법은 먼저 GF(P)상에서의 순차논리머시인의 수학적 성질을 논의하였으며, 순차논리머시인 구성을 위하여 기본의 3가지 회로소자를 사용하여 선형궤환시프트레지스터와 이에 대한 행렬표현에 대해 논의하였다.

그리고, 제안한 방법을 제산연산처리에 적용하였다.

제안한 방법은 기존의 방법에 비해 다소 개선된 점을 알 수 있었다.

향 후 연구과제로는 제산연산처리 이외의 분야에 적용하는 연구가 요구되며, 또한 GF(P)의 확대체인 $GF(P^m)$(P는 소수, m은 양의 정수)상에서 대해서도 본 논문에서 제안한 순차논리머시인을 확장할 수 있으리라 전망된다

참고문헌

[1] I.F. Blake, *Algebraic Coding Theory : History and Development*, Down, Hutchinson & Ross, Inc., Stroudburg, Pennsylvania, 1973.

[2] R. Lidi and G. Pilz, *Applied Abstract Algebra* ,Spring-Verlg, Inc., N.Y., 1984.

[3] R.E. Blahut, *Fast Algorithms for Digital Signal Processing*, Addison-Wesley Publishing Company, Inc., 1985.

[4] M.D. Ercegovac and T. Lang, *Digital Systems and Hardware/Firmware Algorithms*, John Wiley & Sons, Inc., Canadea, 1985.

[5] David Green, *Modern Logic Design*, Addison-Wesley Publishing Company, 1986.

[6] E.J. McClusky, *Logic Design Principles*, Prentice-Hall, 1986.

[7] S. baktir and B. Sunar,"Optimal Tower Fields," IEEE Trans. Computer. VOL. 53, NO. 10, pp.1231-1243, Oct. 2004.

[8] C.K. Koc and B. Sunar,"Low-Compexity Bit Parallel canonical and Normal Nultipliers for Claa of Finite Fields," IEEE Trans. Computer, VOL. 47, NO. 3, pp.353-356, Mar. 1998.

[9] E.Artin, *Galois Theory*, NAPCO Graphic arts,Inc.,Wisconsin.1971.

[10] R.J.McEliece, *Finite Fields for Computer Science and Engineers*, Kluer Academic Publishers, 1987.

[11] A.J. Menezes, *Application of Finite Fields*, Kluwer academic Pub. 1993.

[12] T. sasso, *switching Theory for Logic Synthesis*, Kluwer academic Pub. 1999.