유한체상에서의 선형디지털스위칭함수 구성

박춘명*

A Construction of the Linear Digital Switching Function over Finite Fields

Chun-Myoung Park*

요 약

본 논문에서는 유한체의 수학적 성질과 그래프이론을 바탕으로 GF(P)상의 선형디지털스위칭함수구성을 효과적으로 구성하는 한가지 방법을 제안하였다. 제안한 방법은 주어진 임의의 디지털스위칭함수의 입출력 사이의 연관관계특성으로 부터 DCG를 도출한 후에 노드의 개수를 인수분해한다. 이때 행렬방정식을 해당 차수보다 낮은 기약다항식으로 인수분해하여 그 결과를 부분회로실현한 다음 선형결합함으로써 최종 선형디지털스위칭함수를 구성하였다. 그 결과 기존의 방법에 비해 선형디지털스위칭함수구성을 상당히 간단화 할 수 있었으며 회로구성은 유한체 GF(P)내에서 정의된 가산기와 계수곱셈기를 사용하여 용이하게 실현 할 수 있다.

ABSTRACT

This paper presents a method of constructing the Linear Digital Switching Function(LDSF) over finite fields. The proposed method is as following. First of all, we extract the input/output relationship of linear characteristics for the given digital switching functions, Next, we convert the input/output relationship to Directed Cyclic Graph(DCG) using basic gates adder and coefficient multiplier that are defined by mathematical properties in finite fields. Also, we propose the new factorization method for matrix characteristics equation that represent the relationship of the input/output characteristics. The proposed method have properties of generalization and regularity. Also, the proposed method is possible to any prime number multiplication expression.

키워드

Graph Theory, Finite Fields, Linear Digital Switching Function, Circuit Design

Ⅰ. 서 론

최근의 집적회로기술의 비약적인 발전으로 인해 회로의 형태가 VLSI/ULSI화 되어 단일 칩상에 방대한 양의 회로가 집적될 수 있게 되었지만, 보다 복잡하고 다양한 기능을 실현하기 위해 더 많은 소자들이 더 적은 면적의 칩속에 집적되어야 하는 것이 현재 집적회로기술이 해결해야 할 과제로 떠오르고 있다. 이러한 문제들은 내부접속의 복잡성의 한계 때문에 기인하는 것이며 이를 해결하기 위한 많은 연구들이 계속되고 있다. 이러한 연구 중 현재 가장 주목받고 있는 분야로서 그래프 이론에 기초를 두고 구성하는 방법이 활발히 연구되고 있으며 점차 실용화 되어가고 있는 추세이다[1-3]. 이 중 방향성 사이클릭그래프는 시스템의 입출력 사이의 특정한 연

* 충주대학교 전기·전자 및 정보공학부 컴퓨터공학과

접수일자 2008. 06. 10

관관계를 도출하여 선형디지털스위칭함수를 구하는데 효과적이다.[4-7] 본 논문에서는 디지털스위칭함수의 특성방정식을 행렬기법에 기반을 두고 효과적으로 표현하는 알고리즘을 제안하였으며, 또한 최적의 코드할당 방법을 제안하여 선형디지털스위칭함수를 구성하는 알고리즘과 회로설계하는 방법을 제안하였다. 본 논문의 서술과정은 다음과 같다. Ⅱ장에서는 본 논문에서 적용되는 유한체의 수학적 성질과 그래프의 기본 성질에 대해 서술하였고, Ⅲ장에서는 선형디지털스위칭함수의 개념과 그에 대한 부분연산, 사이클릭연산의 해석 및 선형디지털스위칭함수회로설계에 필요한 기본 게이트에 대해 논의 하였다. Ⅳ장에서는 사이클의 특성을 갖는 행렬특성방정식, 행렬로 부터 직접적으로 선형스위칭함수회로설계하는 방법, 행렬특성방정식을 인수분해하여 선형스위칭함수회로설계하는 방법에 대해 논의 하였다. Ⅴ장에서는 선형다치논리디지털시스템의 특성을 표현하기 위한 행렬과 최적의 코드할당에 대해 논의하였으며 마지막 Ⅵ장은 결론으로 본 논문에서 제안한 선형스위칭함수구성방법의 특징 및 향후 연구 분야에 대해 서술하였다.

Ⅱ. 유한체의 수학적 성질과 그래프의 성질

2-1. 유한체의 수학적 성질

유한체는 임의의 소수 P와 양의 정수 m에 대하여 Pm개의 원소를 가지는 유일한 체를 말하며 프랑스의 천재적 수학자 Galois가 발견하였으며, 일명 Galois체라고도 한다. 일반적으로 Galois체는 $GF(P^m)$으로 표시하며 Pm을 Galois체의 위수라고 하며 기초체 GF(P)와 이를 m차 확대한 확대체 $GF(P^m)$으로 나눌 수 있으며 GF(P)의 P는 1보다 큰 소수로써 GF(P)의 원소는 {0,1,2, ... ,P-1}이며, 확대체 $GF(P^m)$은 GF(P)상의 m차 벡터공간(vector space)으로 표시 할 수 있다. 한편, Galois체는 {S, +, •, 0, 1}의 5가지 요소로 표시되며 S는 원소들의 집합이고 +와 •는 S상의 이항연산이며 0과 1은 각각 가산과 승산에 대한 항등원이며 모든 산술연산은 modP로 처리된다. 이외에 Galois체의 유용한 성질은 참고문헌[8-9]을 참조하였다.

2-2. 그래프의 기본성질

일반적으로 그래프는 G(V,E)로 표현된다. 여기서, V는 유한개의 비공집합 노드(node)의 집합이고, E는 노드 집합에서의 2개의 부집합 에지의 집합이다. 또한, | V |는 그래프의 위수라 하며 노드의 개수를 나타내며, | E |는 그래프의 크기라 하며 에지의 개수를 나타낸다.

Ⅲ. 선형디지털스위칭함수

3-1. 디지털스위칭함수의 부분연산

디지털스위칭함수를 만족하는 선형조합회로의 특성은 각각의 함수행렬에 의하여 표현될 수 있으며 동일한 회로특성에 대한 임의의 함수행렬들은 유사함수행렬에 의해 다음 식(1)과 같은 하나의 부분대각함수행렬 δ로 변환할 수 있다.

$$\delta' = P\text{-}1\delta P = \begin{pmatrix} C_1 & & & \\ & C_2 & & \\ & & \ddots & \\ & & & C_s \end{pmatrix} \tag{1}$$

여기서, Ci는 다음 식(2)이며, P는 n×n의 유사함수행렬이다.

$$C_i = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & 0 & -a_2 \\ \vdots & & \ddots & & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & -a_{n\ i-2} \\ 0 & 0 & 0 & \cdots & 0 & 1 & -a_{n\ i-1} \end{pmatrix} \tag{2}$$

여기서, E는 n차 단위행렬이고 Ci는 δ-xE를 수행하는 수반행렬이다.

3-2. modP 변환연산자

선형디지털스위칭함수를 구성하기위해 먼저 주어진 디지털스위칭함수의 입출력 사이의 연관관계를 도식적으로 표현하는 방향성사이클릭그래프로 도시하고 그로부터 선형관계를 해석하여야한다. 이를 위해 본 절에서는 디지털논리시스템의 선형관계를 도출하기위해 다음과 같은 정의를 한다.

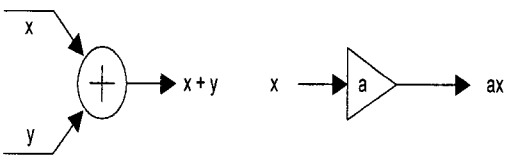
[정의 1] $S_i=\delta S_{i-1}$의 관계를 갖는 두개의 노드 S_i와 S_{i-1}에 대하여 S_{i-1}을 S_i의 부모라 하고 S_i를 S_{i-1}의 자식으로 가정한다. 그리고 Si와 Si-1의 연관관계를 도식적으로 표현할 때는 S_{i-1}에서 출발한 화살표가 S_i에 도착한 형태로 표현한다.

[정의 2] $S_k=\delta^m S_i$의 관계를 갖는 2개의 노드 S_k와 S_i에 대하여 S_i는 S_k의 m번째 부모가 되며 S_k는 S_i의 m번째 자식이 된다. 따라서 노드 S_i에서 출발하여 노드 S_k에 도착하기 위해서는 m번의 경로(path)가 필요하다.

[정의 3] 서로 독립적이며 경로 R을 형성하는 R+1개의 노드들인 $S_1, S_2, \ldots, S_{r+1}$에 대하여 $S_{R+1}=1$의 관계가 성립할때 이를 경로 R을 갖는 사이클이라 한다.

3-3. 선형디지털스위칭함수의 회로실현시의 기본 게이트

디지털스위칭함수의 입력과 출력 사이의 관계를 방향성사이클릭그래프로 나타낸 후 입력과 출력의 연관관계를 규정하는 함수를 행렬로서 표현 할 수 있으며 본 논문에서는 선형특성을 갖는 디지털스위칭함수의 회로설계를 위해 Galois체 GF(P)내에서 정의된 가산기와 계수곱셈기를 사용한다. 이들 기본 게이트의 심볼과 그의 입출력 관계를 다음 그림1에 도시하였으며 이들 게이트들을 사용하여 선형특성을 갖는 디지털논리시스템의 회로를 구성 할 수 있다.



a) Adder b) Coefficient Multiplier

그림 1. GF(P)내에서 정의된 가산기와 계수곱셈기
Fig. 1. An adder and the coefficient multiplier which are defined in GF(P).

Ⅳ. 행렬방정식

디지털스위칭함수의 회로특성에 의해 주어진 행렬방정식을 이보다 낮은 차수의 기약다항식으로 인수분해하여 이를 각각 회로구성한 후 선형결합함으로써 다양하고 복잡한 경우에도 보다 간단히 처리하여 선형디지털논리시스템을 설계할 수 있으며 또한 검증할 수 있는 알고리즘을 제안한다.

4-1. 사이클특성을 갖는 행렬특성방정식

다음 표1과 같은 입출력 사이의 연관관계 특성을 갖는 디지털스위칭함수의 경우에서 4개의 입출력 사이의 연관관계는 소수 2의 곱인 2×2로 인수분해할 수 있으며 표1을 DCG로 도시하면 다음 그림2와 같다.

표 1. 4개의 입출력 사이의 연관관계 특성을 갖는 디지털스위칭함수
Table 1. The digital logic switching function which have four relationship characteristics of input/output

Input	B C D E
Output	C D E B

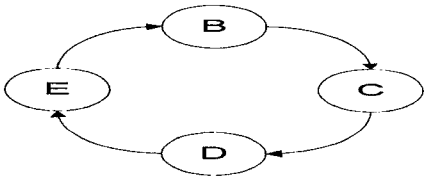


그림 2. 표4-1의 DCG.
Fig. 2. The DCG of table 1.

여기서, 위 그림2의 선형디지털스위칭함수의 입출력 사이의 관계계수를 갖는 회로를 설계하기 위해 다음과 같은 행렬특성방정식 성질에 대한 정리를 내린다.

[정리 1] 행렬특성방정식은 단위행렬(unit matrix)도 영행렬(zero matrix)도 아닌 정방행렬이다.

증명 : 위 그림2의 경우의 DCG에서 각 노드 B, C, D, E와 함수행렬δ 사이의 연관관계를 도출하면 $\delta B = C$, $\delta C = \delta^2 B = D$, $\delta D = \delta^3 B = E$, $\delta E = \delta^4 B = B$이다. 이때, 각각의 노드들은 독립적이며 열벡터(column vector)이다. 따라서, δ는 단위행렬도 영행렬도 아니다.

Q.E.D.

4-2. 행렬식으로 부터 디지털스위칭함수 회로설계

본 절에서는 도출해낸 행렬식으로 부터 직접 선형디지털논리시스템을 실현하는 방법을 제안한다. 예를 들

어 $\delta E=\delta^4 B=B$인 연관관계는 다음 식(3)과 같이 다시 표현 할 수 있다.

$$\delta^4 B = B \Leftrightarrow (\delta^4 - E)\, B = \phi \tag{3}$$

여기서, E는 단위행렬이고 ϕ는 영행렬이다. 또한 $\Leftrightarrow$는 좌항과 우항이 동치임을 나타내는 기호이다.

다음에 위 식(3)은 다음 식(4)와 같이 인수분해 할 수 있으며 δ는 단위행렬이 아니고, B도 역시 영행렬이 아니므로 다음 식(5)가 성립해야 한다.

$$(\delta^4 - E)B=(\delta - E)(\delta^3+\delta^2+\delta+E)B=\phi \tag{4}$$

$$\delta^3+\delta^2+\delta+E=\phi \tag{5}$$

위 식(5)에서 계수벡터 $[a_0,a_1,a_2]$는 [2,2,2]가 된다. 따라서 길이 4를 표현하는 수반행렬을 C_3라 하면 다음 식(6)을 도출 할 수 있다.

$$C_3 = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix} \tag{6}$$

그러므로 식(6)으로부터 표현행렬 ξ를 구하면 다음 식(7)과 같다.

$$\xi = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix} \tag{7}$$

최종적으로 위 식(7)의 표현행렬과 앞에서의 Ⅲ장의 3절에서 제안한 Galois체 내에서의 가산기와 계수곱셈기의 기본 게이트를 사용하여 선형디지털논리시스템을 실현하면 다음 그림3과 같다.

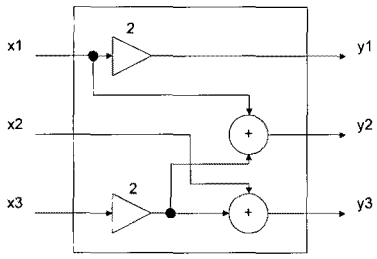


그림 3. 식(7)에 대한 선형디지털논리시스템의 회로설계
Fig. 3. The logic design of linear digital logic systems for expression (7)

4-3. 행렬특성방정식을 인수분해하여 디지털스 위칭함수 회로설계

항의 개수가 짝수개인 경우, 이를 다시 인수분해여 효과적으로 처리 할 수 있는 방법에 대해 논의한다. 예를 들어 식(5)는 다음 식(8)과 같이 다시 인수분해가 가능하다.

$$\delta^3+\delta^2+\delta+E=(\delta^2+E)(\delta+E)=\phi \tag{8}$$

위 식(8)은 $(\delta^2+E)=\phi$, $(\delta+E)=\phi$, 또는 (δ^2+E)와 $(\delta+E)$의 2개 항이 모두 ϕ인 조건을 만족해야함을 의미하며 이 내용을 집합으로 표현하면 다음 식(9)와 같다.

$$[\{(\delta^2+E)=\phi\} \cup \{(\delta+E)=\phi\} \cup \{(\delta^2+E) \cap (\delta+E)=\phi\}] \tag{9}$$

즉, 위 식(9)의 내용은 행렬의 중첩의 원리를 이용하여 선형디지털논리시스템을 설계할 수 있음을 의미한다. 여기서, $\delta+E=\phi$의 조건을 만족하는 행렬, $\delta^2+E=\phi$의 조건을 만족하는 행렬을 Galois체 GF(3)상의 최소행렬로 표현하면 $C_1=(2)$, $C0_2=\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$이다.

따라서, 표현행렬 $\xi=\begin{pmatrix} C_1 & \\ & C_{02} \end{pmatrix}$는 다음 식(10)과 같다.

$$\xi = \begin{pmatrix} 2 & & \\ & 0 & 2 \\ & 1 & 0 \end{pmatrix} \tag{10}$$

이에 대한 선형디지털스위칭함수회로설계는 다음 그림4와 같다.

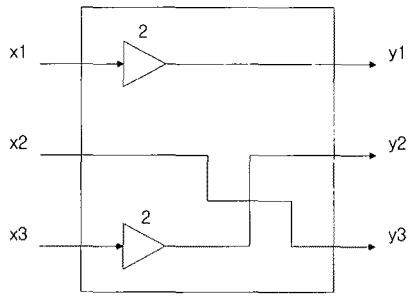


그림 4. 선형디지털논리시스템의 회로설계
Fig. 4. The logic design of linear digital logic systems

V. 행렬과 코드할당

본 장에서는 주어진 입출력 사이의 연관관계특성을 만족하는 행렬을 찾아내었을 때 각각의 노드들에 최적의 적합한 코드를 할당하는 방법의 한가지를 논의한다. 예를 들어 4개의 노드들을 갖는 디지털논리시스템은 함수행렬이 3×3 행렬이므로 각각의 노드들은 3×1의 열벡터가 된다.

즉, 각각의 노드들은 3디지트이며 주어진 입출력 사이의 연관관계는 4개의 노드를 가지고 있으며 그 각각의 신호들은 유일해야 하므로 각각의 벡터들은 서로 독립적이어야 한다.

Galois체 GF(3)上에서 3디지트를 갖는 3×1 열벡터들은 {(0,0,0), (0,0,1), (0,0,2), ... , (2,2,2)}의 27개이며 이들 중 주어진 입출력 사이의 연관관계특성을 만족하는 열벡터는 오직 (1,0,0), (0,1,0), (0,0,1), (2,2,2)의 4개뿐이며 입출력 사이의 연관관계특성이 사이클이므로 이들 4개의 코드들을 임의로 노드에 할당해 주면 된다.

만일 (1,0,0)을 B에, (0,1,0)을 C에, (0,0,1)을 D에, (2,2,2)를 E에 할당해 주면 다음 식(11)과 같다.

$$\delta B = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = C,$$

$$\delta C = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = D$$

$$\delta D = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix} = E$$

$$\delta E = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = C \qquad (11)$$

따라서, 위 식(11)을 만족하는 코드할당은 다음 식(12)와 같다.

$$\delta = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix} \qquad (12)$$

즉, 입출력 사이의 연관관계특성을 만족하는 행렬 δ을 구한뒤 행렬 δ의 각각의 열들을 노드들에 대한 코드로 활용할 수 있다.

따라서 4번째 노드에 대한 코드는 3번째 열을 함수행렬과 연산하여 구할 수 있다. 위 내용을 토대로 각각 코드할당을 수행하면 다음 표2와 표3과 같다.

표 2. 식(6)에 대한 코드할당
Table 2. The code assignment of expression (6)

Xi	B C D E
X1	1 0 1 2
X2	0 1 0 2
X3	0 0 1 2

표 3. 식(11)에 대한 코드할당
Table 3. The code assignment of expression (11)

Xi	B C D E
X1	0 0 0 0
X2	0 2 0 1
X3	1 0 2 0

Ⅶ. 결론

본 논문에서는 유한체의 수학적 성질과 그래프이론을 바탕으로 GF(P)상의 선형디지털논리스위칭함수구성을 효과적으로 구성하는 한가지 방법을 제안하였다. 제안한 방법은 기존 연구의 방법에서 다룰 수 없었던 동일한 소수값의 곱으로 표현되는 시스템에도 적용할 수 있는 방법으로써 다음과 같은 특징이 있다. 주어진 임의의 디지털논리시스템의 입출력 사이의 연관관계에 대한 특성을 도식적인 표현인 DCG로 도시 한 후 이로부터 노드의 개수를 인수분해한다. 이때 행렬방정식을 해당 차수보다 낮은 기약다항식으로 인수분해하여 그 결과를 부분회로실현한 다음 선형결합함으로써 최종 선형디지털논리스위칭함수를 효율적으로 구성할 수 있으며, 그 결과 기존의 방법에 비해 선형디지털논리시스템의 회로구성을 상당히 간단화할 수 있다. 또한, 선형디지털논리시스템의 회로구성은 Galois체 GF(P)내에서 정의된 가산기와 계수곱셈기를 사용하여 용이하게 실현 할

수 있다. 본 논문에서 제안한 방법에 대한 예들은 Galois 체 GF(3)상에서 수행하였지만 임의의 소수 P인 GF(P)상에서도 쉽게 적용될 수 있으리라 사료된다. 향후 연구과제로서는, 좀 더 일반적인 경우인 다중입력/다중출력의 선형디지털논리스위칭함수에 대한 K-ary 연산에 대한 연구가 요구된다. 이 외에 트리(tree) 형태의 선형디지털 논리스위칭함수구성에 대한 연구가 요구된다.

참고문헌

[1] S.Mitra, N.R.Saxena, and E.J.McCluskey,"Efficient Design diversity Estimation for Combinational Circuits," IEEE Trans. on Computers, pp.1483-1492, Vol.53, No.11, Nov. 2004.

[2] Lathi, Linear Systems and Signals, 2/E, Oxford, 2004.

[3] Kleitz, Digital Electronics: A Practical Approach, 8/E, Prentice-Hall, 2005.

[4] R.E.Bryant,"Graph-Based Algorithms for Boolean Function manipulations," IEEE Trans. Comput., vol.C-35, no.8, pp.677-691, Aug. 1986.

[5] Yung-Te Lai and Sarma Sastry, "Edge-Valued Binary Decision Diagrams for Multi-Level Hierarchical Verification" 29th ACM/IEEE Design Automation Conference, pp.608-613, 1992.

[6] Chun-Myoung, Park etc,"A Study on the Circuit Minimization Technique using Edge-Valued Decision Diagram," ITC-CSCC'97, vol.2 pp.943-946, Naha, Okinawa, Japan, 14~16 July, 1997.

[7] M.Nakajima and M.Kameyama,"Design of Highly Parallel Linear Digital System for ULSI Processors", IEICE Trans, Vol.E76-C, No.7, pp.1119-1125, July, 1993.

[8] R.Gould, *Graph Theory*, The Bejamin/Cummings Publishing Company, Inc., 1988.

[9] D.B.West, *Introduction to Graph Theory*, Prentice-hall, 1996.

저자소개

제12권 10호 참조