부울함수의 논리곱의 배타적 합 논리로의 간략화

이진홍*, 이상곤°*, 문상재**, 서용수*, 김태근***, 정원영***
* 동서대학교 전자기계공학부
**경북대학교 전자전기공학부
***한국통신 무선통신연구소

(The Minimization of Boolean functions to the Exclusive-OR sum of Products logic)

Jin-Hung Lee*, Sang-Gon Lee*, Sang-Jae Moon**, Yong-Soo Seo*, Tae-Geun Kim***, Won-Young Jeong***
* Division of Electronic and Mechanical Engr., Dongsoe Univ.
** School of Electronic and Electrical Engr., Kyungpook National Univ.
*** Korea Telecom Wireless Communication Research Lab.

요 약

본 논문에서는 임의의 부울함수(Boolean function)에 대한 진리표나 출력 시퀀스로부터 논리곱의 배타적 합(exclusive-or sum of products; ESOP)형의 부울함수를 구성하는 알고리듬을 제안한다. 기존에 알려진 카르노맵이나 Quine McClusky법에 의하여 구해지는 부울함수는 논리곱의 합(sum of product; SOP) 형으로 주어지며 이들 수식은 부정(NOT)논리를 포함하는 경우가 있다. 제안된 알고리듬에 의하여 구해지는 부울함수는 구조적인 등가성을 판별하는데 편리하므로 해쉬함수용 부울함수의 개발에 이용될 수 있다.

1. 서 론

부울함수는 컴퓨터 시스템의 논리회로 뿐만아니라 컴퓨터 시스템에서 사용자와 데이터의 인증과 데이터 무결성(data integrity)을 보장하기 위한 중요한 암호학적 도구로 사용되고 있는 일방성 해쉬함수(oneway hash function)에 이용된다. 그리고 해쉬함수에서 사용되는 부울함수의 암호학적 안전성 기준[1]으로는 0-1 balancedness, high nonlinearity, SAC(Strict Avalanche Criterion, 좌표축의 선형변환에 의한 함수의 비등가성, 상호 output-uncorrelated 등이 있다. 0-1 balancedness, high nonlinearity, SAC, 상호 output-uncorrelated 등은 부울함수의 출력시퀀스로 부터 조사할 수 있다. 그러나 좌표축의 선형변환에 의한 함수의 비등가성은 부울함수를 논리식으로 구성한 후 직접확인 해야 하므로 구조적 등가성을 조사하기가 쉬운 논리표현식이 요구된다. 일반적으로 해쉬함수의 부울함수는 ESOP 형으로 많이 표현되는데[1], 이러한 형태를 갖는 부울함수들은 구조적 등가성을 판별하기가 쉽다.

* 이 연구는 한국통신의 97년도 정보통신 기초연구비 지원에 의한 결과의 일부임.

부울함수의 진리표나 출력시퀀스로부터 논리수식을 구성하는 방법으로 지금까지는 카르노 맵을 사용하거나 독립변수가 많은 경우에는 Quine McClusky 법[2, 3]을 사용하였다. 이들 방법에 의하여 생성되는 부울함수는 SOP 형으로 표현되고 특히 NOT 논리를 포함할 수 도 있으므로 부울함수의 구조적 등가성판별에 좋지않다.

따라서 본 연구에서는 부울함수의 구조적 등가성 판별에 유리한 ESOP 형의 부울함수를 구하는 알고리듬을 제안한다. 그리고 전산 프로그램을 개발하여 실제 알고있는 부울함수로부터 출력시퀀스를 구하고, 이 시퀀스로부터 부울함수를 구하여 동일한 함수가 됨을 확인하였다.

2. 기존의 부울함수 구성 알고리듬[2-4]

Quine McClusky에 의한 부울함수의 간략화 방법은 체계적인 방법이므로 입력변수가 많아 지더라도 쉽게 간략화를 할 수있으며 컴퓨터 프로그램으로 실현하기에 적합하다. 간략화된 부울함수는 논리곱의 합의 형으로 나타난다. 아래에 예를 들어서 Quine McClusky 방법을 설명한다.

부울함수가

$$f(A, B, C, D) = \sum(m_0, m_2, m_3, m_6, m_7, m_8, m_9, m_{10}, m_{13})$$

라고 하자. 여기서 우측항의 요소들은 최소항(min-term)들이다. 예를들어 m_3을 입력변수를 이용하여 논리식으로 표현하면 $\overline{A} \cdot \overline{B} \cdot C \cdot D$이며 이진수 형태로 표현하면 0011이다. 여기서 · 은 AND 논리연산자이다.

간략화 과정은 다음의 다섯단계로 이루어 진다.

단계 1 : 주어진 부울함수를 구성하는 최소항의 이진수 형태에서 1의 수를 세어 1의 개수가 0인 최소항의 집합을 그룹 0, 1의 개수가 1인 최소항의 집합을 그룹 1 등으로 하여 표 1 처럼 그룹을 형성한다. 부울함수의 이진 입력변수가 k개이면 그룹 k+1 까지 가능하다.

단계 2 : 표 1에서 그룹번호가 낮은 것에서 높은 것으로 내려가면서 아래의 그룹과 비교하여 하나의 자리수만 다르고 나머지 자리가 같은 것끼리 결합하여 표 2 처럼 제 1 감축표를 만든다. 표 2부터는 편의상 최소항을 번호만 표기한다. 표 2 에서 v 표시는 결합된 항목임을 나타내며 * 표시는 더 이상 결합이 이루어지지 않는 항이다. 이들 항은 주어진 부울함수를 구성하는 최소항의 후보가 되는 것으로 이를 주항(prime implicant)이라 한다[4].

단계 3 : 제 1 감축표에서 단계 2와 동일하게 위에서 아래 그룹으로 내려오면서 동일하게 한 비트만 다른 것끼리 결합시켜 표 3 처럼 제 2 감축표를 만든다.

단계 4 : 제 1 감축표와 제 2 감축표에 의하여 간소화된 자료에 의해서 표 4 처럼 주항표를 작성한다.

단계 5 : 주항표에서 각 주항 그룹의 요소들이 다른 주항 그룹에도 존재하는지 확인하여 만일 한 그룹의 모든 요소들이 다른 주항 그룹에도 있다면 그 그룹은 최종 주항이 되지 못한다. 이렇게하여 선정된 최종 주항들은 부울함수를 구성하는 최소항이 되고 이들을 진성주항

(essential prime implicant)이라 한다.

표 4에서 보면 주항그룹 3의 8번항과 9번항은 각각 주항그룹 1과 주항그룹 4에 포함되므로 진성주항이 되지 못한다. 표 4의 진성주항의 비트패턴을 이용하여 SOP 형의 간략화된 부울함수를 구하면 주항그룹 1은 $\overline{B}\cdot\overline{D}$, 주항그룹 2는 $\overline{A}\cdot C$, 주항그룹 4는 $A\cdot\overline{C}\cdot D$로 표기할 수 있므으로 간략화된 부울함수는 $\overline{B}\cdot\overline{D}+\overline{A}\cdot C+A\cdot\overline{C}\cdot D$가 된다. 여기서 + 는 OR 논리연산자이다.

표 1. 1의 수에 따라 재배열된 최소항표

그 룹	최 소 항	
0	m_0	0000
1	m_2	0010
	m_8	1000
2	m_3	0011
	m_6	0110
	m_9	1001
	m_{10}	1010
3	m_7	0111
	m_{13}	1101

표 2. 제 1 감축표

일치항	일치되는 비트형태
0, 2	00-0 v
0, 8	-000 v
2, 3	001- v
2, 6	0-10 v
2, 10	-010 v
* 8, 9	100-
8, 10	10-0 v
3, 7	0-11 v
6, 7	011- v
* 9, 13	1-01

표 3. 제 2 감축표

일치항	일치되는 비트형태
* 0, 2, 8, 10	-0-0
* 2, 3, 6, 7	0-1-

표 4. 주항표

주항그룹 번 호	최소항 / 주항	0	2	3	6	7	8	9	10	13	진성주항
1	0, 2, 8, 10 (-0-0)	v	v				v		v		*
2	2, 3, 6, 7 (0-10)		v	v	v	v					*
3	8, 9 (1)						v	v			
4	9, 13 (4)							v		v	*

3. 논리곱의 배타적 합(ESOP) 형의 부울함수 구성 알고리듬

부울함수에 기초한 해쉬함수에서는 입력변수들의 좌표변환에 의하여 동일함수가 되지 않는 함수들을 발굴하여 사용하여야 한다. 이때 부울함수가 ESOP 형으로 구성되면 구조적 동가성을 판별하기가 쉽다. 본 장에서는 주어진 부울함수의 진리표나 출력 시퀀스로부터 ESOP 형으로 간략화된

부울함수를 구하는 알고리듬을 제안한다.

3.1 ESOP 형 부울함수의 특성

GF(2)의 원소를 가지는 차원(dimension)이 n인 벡터공간을 V_n이라 할 때, V_n에서 GF(2)로 가는 함수를 부울함수이라 한다. V_n의 부울함수는 n개의 독립변수 χ_n, χ_{n-1}, ……, χ_1을 사용한 다항식 f(χ_n, χ_{n-1}, …… , χ_1)로 표시할 수 있다. χ_n, χ_{n-1}, ……, χ_1이 0, 0, …, 0에서 1, 1, …, 1까지 변할 때 함수 f의 2^n개 출력비트를 묶어서 f의 시퀀스(sequence)라 한다. 즉, 시퀀스는 (f(α_0), f (α_1), …, f(α_{2^n-1}))로 나타낼 수 있다. 여기서 α_0 = (0,0,…,0), …, $\alpha_{2^{n-1}-1}$ = (01…1), $\alpha_{2^{n-1}}$ = (10…0), …, α_{2^n-1} = (11…1) 이다.

부정논리를 포함하지 않는 최소항들이 배타적 논리합 형으로 표현된 함수를 본 논문에서는 "논리곱의 배타적 합형(exclusive-or sum of products)의 부울함수"로 부르기로 한다. 입력벡터를 부정논리가 포함되지 않는 최소항으로 표현할 경우에는 입력변수값이 1인 것만 논리곱으로 결합한다. 예를 들어 A, B, C, D 4개의 입력변수에 대하여 입력벡터 1011은 $A \cdot C \cdot D$가 된다. 간단한 ESOP형 함수의 예를들면 $f(A,B,C) = A \cdot C \oplus B \cdot C \oplus A \oplus C$ 와 같다. 여기서 ⊕는 Ex-OR 연산자이다.

ESOP 형의 부울함수는 다음과 같은 성질을 갖는다.

성질 1. 입력변수 값이 모두 1 일 때의 함수값 f(α_{2^n-1})이 1이면 Ex-OR로 연결되어 있는 최소항의 개수는 홀수이고, 0이면 최소항의 개수는 짝수이다. 즉, α_{2^n-1}= (11……1)이므로 어떠한 변수의 논리곱형태(부정논리를 포함하지않음)라 하더라도 그 최소항의 논리값은 1이므로 f (α_{2^n-1}) = 1 이면 부울함수를 구성하는 최소항의 개수는 홀수이고, f(α_{2^n-1}) = 0 이면 짝수임을 예측할 수 있다.

성질 2. f(α_0) = 0이면 부울함수는 상수항을 포함하니 않고, 1이면 상수항을 포함한다.

성질 3. f(α_0) = 0인 경우(상수항을 포함하지 않는 경우)

i) f(α_i) = 1인 α_i(i=1, …, 2^n-1) 중에서 α_i에 포함된 1의 개수가 최소인 것(들)은 해당 부울함수를 구성하는 최소개의 변수로 이루어진 최소항(들)이 된다.

ii) 부울함수를 구성하는 최소항들 중에서 임의의 α_i(i=1, …, 2^n-1)에 대하여 논리값이 1이 되는 항의 개수는 f(α_i) = 1이면 홀수, f(α_i) = 0이면 짝수이다. (모든 최소항의 값이 0인 경우는 짝수개인 것으로 취급한다.)

성질 4. f(α_0) = 1인 경우(상수항을 포함하는 경우)

i) f(α_i) = 0인 α_i(i=1, …, 2^n-1) 중에서 α_i에 포함된 1의 개수가 최소인 것(들)은 해당 부울함수를 구성하는 최소개의 변수로 이루어진 최소항(들)이 된다.

ii) 부울함수를 구성하는 최소항들 중에서 임의의 α_i(i=1, …, 2^n-1)에 대하여 논리값이 1인

항의 개수는 $f(\alpha_i) = 1$이면 짝수, $f(\alpha_i) = 0$이면 홀수이다. (모든 최소항의 값이 0인 경우는 짝수개인 것으로 취급한다.)

3.2 ESOP 형 부울함수의 구성 알고리듬

부울함수를 간략화하는 알고리듬으로는 입력변수가 4개 이하인 경우이는 카르노 맵, 5개 이상인 경우에는 Quine McClusky 방법이 널리 사용되고 있다. 이들 방법에 의하여 간략화된 부울함수는 SOP 형이되므로 이것을 다시 ESOP 형으로 변환하기 위해서는 SOP 형 논리식의 변수들을

$$\overline{x} = x \oplus 1$$

$$x + y = xy \oplus x \oplus y$$

으로 치환함으로써 최종적인 부울함수를 구할 수 있다. 입력변수가 많아지면 치환작업이 복잡해진다. 함수의 출력시퀀스로부터 바로 논리곱의 배타적 논리합 형으로 간략화하는 방법을 제안한다.

단계 1. 입력벡터에 포함되어있는 1의 개수별로 그룹화

Vn 상의 입력벡터를 부울함수의 진리표나 출력 시퀀스로부터 부울함수값에 따라 0인 그룹(group 0)과 1인 그룹(group 1)으로 나누고, 각 그룹에 대하여 Quine McClasky 법의 단계 1에서와 같이 입력벡터에 포함되어 있는 1의 개수별로 부그룹을 나눈다. 예를 들어 출력 시퀀스가 $\{f(\alpha_0), f(\alpha_1), \cdots, f(\alpha_{2^5-1})\}$ = {00000000000001010001100111100011 0}이면 표 5와 같이 된다.

단계 2. 진성주항 색출

1. 단계 1에서 $f(\alpha_{2^n-1}) = 0$ 이므로 부울함수를 구성하는 최소항은 짝수개임을 알 수 있다.
2. 표 5의 그룹 1에서 1의 개수가 최소개인 그룹의 입력벡터들을 주항표에 등록한다. 이들은 부울함수를 구성하는 진성주항이 된다. 표 5에서 처음 색출된 진성주항을 표 6에 나타내었다.
3. 표 5의 그룹 0 와 그룹 1의 입력벡터가 진성주항의 1패턴을 포함하는지를 검사한다. 포함의 의미는 다음과 같이 설명할 수 있다. 예를 들어, 입력변수가 A, B, C, D, E 이고 진성주항이 01100, 입력벡터 01101이면 진성주항은 BC로 입력벡터는 BCE로 표현되므로 진성주항은 입력벡터에 포함된다. 이러한 검사는 그룹 1의 최소 부그룹 보다 높은 부그룹을 대상으로 낮은 부그룹에서 높은 부그룹으로 차례로 검색한다. 검색 결과 포함되는 진성주항의 개수가 3.1절에 정의된 성질(성질 3-ii 또는 성질 4-ii)에 맞지 않으면 그 입력벡터를 진성주항으로 등록시켜 바라는 성질을 만족시키도록 한다.

   표 6의 진성주항이 부그룹 2의 요소들이므로 부그룹 3의 요소들에 대하여 진성주항 포함여부를 조사하여 표 7에 나타내었다. 그룹 0의 부그룹 3에 있는 01101이 포함하는 진성주항의 개수는 짝수이어서 성질 3-ii를 만족하지 않으므로 주항표에 시킨다. 표 7의 입력벡터중 진성주항을 포함하는 나머지 것들은 성질 3-ii을 만족하므로 진성주항이 되지못한다. 이렇게

하여 진성주항표를 갱신시킨다.

4. 3의 과정을 새로이 진성주항표에 등록되는 입력벡터가 속한 부그룹 보다 한단계 위의 부그룹에 대하여 반복한다. 표 8은 표 7의 주항들의 포함여부를 검색한 결과이다.
5. 마지막 부그룹까지 위의 과정을 반복하여 나온 진성주항들을 최소항으로하여 ESOP 형 부울함수를 구성한다.

표 8의 진성주항으로부터 $m_{12}, m_{18}, m_{24}, m_{13}$은 각각 BC, AD, AB, BCE이므로 ESOP 형 부울함수는 F(x)=AB⊕AD⊕BC⊕BCE 가 된다. 이 부울함수로부터 출력시퀀스를 구해보면 위에서 도입한 예제의 출력시퀀스인 {00000000000010100011001111000110}가 나옴을 확인할 수 있다.

표 5. 1의 수에 따라 재배열된 최소항표

그룹명 / 부그룹명	그룹 0	그룹 1
부그룹 0	00000	
부그룹 1	00001 00010 00100 01000 10000	
부그룹 2	00011 00101 00110 01001 01010 10001 10100	01100 10010 11000
부그룹 3	00111 01011 01101 10101 11010 11100	01110 10011 10110 11001
부그룹 4	01111 11011	10111 11101 11110
부그룹 5	11111	

표 6. 표 5에서 색출된 진성주항

진성주항
01100 (m_{12})
10010 (m_{18})
11000 (m_{24})

표 7. 제 1 감축표

진성주항	부그룹명	그룹 0		그룹 1	
		입력벡터	포함되는 항	입력벡터	포함되는 항
01100 m_{12} 10010 m_{18} 11000 m_{24}	부그룹 3	00111 01011 01101 10101 11010 11100	 m_{12} * m_{18}, m_{24} m_{12}, m_{24}	01110 10011 10110 11001	m_{12} m_{18} m_{18} m_{24}

표 8. 제 2 감축표

진성주항	부그룹명	group 0		group 1	
		입력벡터	포함되는 항	입력벡터	포함되는 항
01100 m_{12} 10010 m_{18} 11000 m_{24} 01101 m_{13}	subgroup 4	01111 11011	m_{12}, m_{13} m_{18}, m_{24}	10111 11101 11110	m_{18} m_{12}, m_{24}, m_{13} m_{12}, m_{18}, m_{13}

4. 결 론

부울함수는 중요한 암호학적 도구로 사용되고 있는 일방성 해쉬함수(oneway hash function)에 이용된다. 해쉬함수에서 사용되는 부울함수들은 좌표축을 선형변환하여도 동일한 함수가 되지 않아야 암호학적으로 안전하다. 해쉬함수에 사용될 부울함수를 개발할 때 이러한 구조적 비등가성은 부울함수를 논리식으로 구성한 후 직접확인 해야 하므로 구조적 등가성을 조사하기가 쉬운 논리표현식이 요구된다. 본 논문에서는 부울함수의 구조적 등가성 판별에 유리한 ESOP 형의 부울함수를 구하는 알고리듬을 제안하였다. 그리고 전산 프로그램을 개발하여 실제 알고있는 부울함수로부터 출력시퀀스를 구하고, 이 시퀀스로부터 부울함수를 구하여 동일한 함수가 됨을 확인하였다.

참고문헌

[1] Y. Zhang, J. Pieprzyk, and J. Seberry, "HAVAL - A One-way Hashing Algorithm with Variable Length of Output", *Auscrypt'92 Abstract*, 1992.

[2] Quine, W.V., "The Problem of Simplying Truth Functions," *Am. Math. Monthly*, 59:8, Oct. 1952, pp.521-531

[3] McClusky, E.J., Minimization of Boolean Functions," *Bell System Tech. J.*, 35:5, Nov. 1956, pp.1417-1444

[4] 이두성외 2인, *디지틀공학*, 청문각, 1993, pp.104-107