情報保護學會論文誌
第19卷 第2號, 2009. 4

회전대칭 이차 불함수의 해밍무게 및 비선형성

김 현 진,†‡ 정 창 호, 박 일 환
한국전자통신연구원 부설연구소

On the Weight and Nonlinearity of Quadratic Rotation Symmetric Boolean Functions

Hyeonjin Kim,†‡ Changho Jung, Ilhwan Park
The Attatched Institute of ETRI

요 약

회전대칭 불함수는 고속계산에 유리하고 암호학적으로 우수한 성질을 나타내어 최근 많은 주목을 받고 있다. 예를 들어, 부호이론에서 중요한 문제가 회전대칭 불함수를 이용하여 해결된 사례가 있고, 고속 해시함수 설계에 응용된 경우도 있다. 다른 한편으로, 매우 단순한 형태의 회전대칭 이차 불함수에 대한 비선형성 및 해밍무게의 정확한 공식이 발견되었으며[2,8], 더 넓은 범위의 함수들에 대한 보다 일반적인 공식들도 발견되었다[6]. 본 논문에서는 이들 공식들을 조금 더 확장하여 일차 항들이 포함된 회전대칭 이차 불함수에 대한 정확한 해밍무게 공식을 유도한다.

ABSTRACT

Recently, rotation symmetric Boolean functions have attracted attention since they are suitable for fast evaluation and show good cryptographic properties. For example, important problems in coding theory were settled by searching the desired functions in the rotation symmetric function space. Moreover, they are applied to designing fast hashing algorithms. On the other hand, for some homogeneous rotation symmetric quadratic functions of simple structure, the exact formulas for their Hamming weights and nonlinearity were found[2,8]. Very recently, more formulations were carried out for much broader class of the functions[6]. In this paper, we make a further improvement by deriving the formula for the Hamming weight of quadratic rotation symmetric functions containing linear terms.

Keywords: Boolean function, rotation symmetric, Hamming weight, nonlinearity

I. 서 론

불함수는 정보이론을 구성하는 중요한 한 분야로서 특히 암호학 및 부호이론에서 그 역할이 두드러진다. 스트림암호의 비선형 결합함수 및 필터로서 불함수가 사용되며, 블록암호에서 s-박스의 요소로 사용된다. 부호이론에서 Reed-Muller 부호는 불함수 공간의 부분집합으로 해석될 수 있다. 응용 분야에 따라 불함수의 다양한 특성이 정의되고 연구되었는데, 그 중에는 해밍무게 분포, 비선형성, 상관관계 면역도, 대수적 면역도 등이 포함된다.

최근 회전대칭 불함수가 많은 주목을 받고 있는데, 변수들의 회전 치환에 대하여 함수 값이 불변인 특성으로 인하여 고속 계산에 유리한 특성이 있으며, 또한 우수한 암호학적 특성을 나타내는 경우가 많다는 것이 밝혀지고 있기 때문이다. 회전대칭 불함수는 대수적 표현에서 진리표를 고속으로 구할 수 있고, 다시 이로부터 Walsh 변환을 고속으로 수행할 수 있다. 한편, 회전대칭 불함수 공간의 정확한 크기를 계산할 수 있으며[11], 그 값은 대략 $2^{2^n/n}$ 정도로서 전체 불함수 공간의 크기 2^{2^n}에 비하여 매우 작다. 이러한 특성을 이용

접수일(2008년 8월 14일), 게재확정일(2009년 2월 4일)
† 주저자, mikjh@ensec.re.kr
‡ 교신저자, mikjh@ensec.re.kr

하여 여러 가지 탐색이 수행되었다[3-5,10-12]. 특히, Kavut 등은 비선형성이 241인 9-변수 회전대칭 함수를 처음으로 발견하였고[4], 회전대칭 개념을 확장하여 비선형성이 242인 9-변수 함수를 찾는데 성공함으로서[5] 부호이론에서 오래된 문제를 해결하였다.

다른 한편으로, 회전대칭 불함수를 고속 해시함수 설계에 응용하면서, 가장 단순한 꼴의 회전대칭 이차 불함수들의 비선형성 및 해밍무게 값의 범위 또는 정확한 공식들이 발견되었다[8]. 이 결과를 개선하여, 약간 더 확장된 이차 불함수에 대한 정확한 공식과, 가장 단순한 회전대칭 삼차 불함수의 해밍무게의 생성함수가 발견되었다[2]. 아주 최근에, 회전대칭 이차 불함수에 대한 이전의 두 결과를 포함하는 일반화된 공식들이 발견되었는데[6], 이차 Reed-Muller 부호의 성질을 이용함으로서 매우 단순하고 일관적인 방법으로 공식들이 유도된다.

본 논문에서는 논문[6]의 결과를 약간 더 확장하여, 일차 항들이 포함된 회전대칭 이차 불함수에 대한 해밍무게 공식을 유도한다. 유도 과정은 논문[6]에서 제안된 방법과 거의 같아서, 아핀변환을 통하여 회전대칭 이차 불함수들을 해밍무게 계산이 쉬운 함수 꼴로 바꾸는 방법을 사용한다.

II. 기본 용어 및 정의

GF(2) 상의 n차원 벡터공간을 V_n으로 나타낸다. V_n에서 GF(2)로 매핑시키는 함수를 n-변수 불함수라고 하며, n-변수 불함수의 전체 공간을 B_n으로 표기한다. 별도의 언급이 없으면 함수는 불함수를 의미한다. 불함수는 대수적 다항식 또는 진리표를 이용하여 나타낼 수 있다. 간단한 예로서 3-변수 불함수 중 하나를 다항식 $f(x)=1+x_1+x_1x_2+x_2x_3$으로 나타낼 수 있으며, 이 함수를 진리표로 나타내면 다음 [표 1]과 같이 주어진다.

[표 1] 불함수 $f(x)=1+x_1+x_1x_2+x_2x_3$의 진리표 표현

(x_1,x_2,x_3)	(0,0,0)	(1,0,0)	(0,1,0)	(1,1,0)	(0,0,1)	(1,0,1)	(0,1,1)	(1,1,1)
$f(x)$	1	0	1	1	1	0	0	0

V_n에 속하는 벡터들의 순서를 일관성 있게 약속하면 n-변수 함수는 2^n비트 진리값 벡터로만 표현이 가능하다. 함수 f의 대수적 표현에서 하나의 항에 존재하는 변수 x_i들의 최대 개수를 f의 *대수적 차수*라고 한다. 위에서 예로 든 함수의 대수적 차수는 2이다. 대수적 차수가 1 이하인 함수를 *아핀함수*라고 하며, n-변수 아핀함수 공간을 A_n으로 나타낸다. 벡터 $x\in V_n$의 *해밍무게*는 x의 원소들 중 1의 개수를 말하며 $wt(x)$로 나타낸다. 함수 f의 무게 $wt(f)$는 $f(x)=1$인 $x\in V_n$의 개수로 정의한다. n-변수 함수의 무게가 2^{n-1}이면 *균형함수*라고 한다. 두 함수의 *거리*는 $wt(f+g)$로 정의하며 $d(f,g)$로 나타낸다. 이때 $f+g$는 GF(2) 상에서의 덧셈이다. 정수들의 집합은 $\mathbb{Z}$로 나타낸다.

정의 1. 함수 $f\in B_n$의 *비선형성*이란 f와 아핀함수들 사이의 최소 거리, 즉, f와 집합 A_n 사이의 거리로 정의하며, $NL(f)$로 나타낸다. 다시 말하면, $NL(f):=\min_{l\in A_n} d(f,l)$이다.

변수가 n인 함수의 비선형성은 $2^{n-1}-2^{n/2-1}$ 을 넘지 못한다. n이 짝수일 경우 이 최대값을 가지는 함수가 항상 존재하는 것이 잘 알려져 있으며[9], 이를 *bent* 함수라고 한다.

정의 2. n-변수 함수 f와 g가 GF(2) 상의 $n\times n$ 가역행렬 A와 벡터 $b\in V_n$에 대하여 다음 동치관계 $g(x)=f(xA+b)$을 만족하면 두 함수를 *아핀동치*라고 한다. 아핀동치 함수 f, g는 $f\equiv g$로 나타낸다.

함수의 해밍무게 및 비선형성은 아핀변환에 대하여 불변인 성질임은 쉽게 보일 수 있다. 즉, $f\equiv g$이면 $wt(f)=wt(g)$이고 $NL(f)=NL(g)$이다.

III. 회전대칭 불함수

회전대칭 불함수를 정의하기 위해서 우선 집합 $\{1,2,\cdots,n\}$에서 정의되는 회전 치환 ρ를 다음과 같이 정의한다.

$$\rho := \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}$$

치환 ρ의 역치환을 ρ^{-1}로 나타내며, 정수 k에 대하여 ρ^k는 치환 ρ를 k번 반복 적용하는 것을 의미한다. 치환 ρ^k는 다음과 같이 직접적으로 표현된다.

$$\rho^k(i)=\begin{cases} n & \text{if } i+k\equiv 0 \pmod n \\ i+k \pmod n & \text{otherwise} \end{cases}$$

치환 ρ^k로부터 벡터 $x=(x_1,\cdots,x_n)\in V_n$에 대한 작용(action)을 $\rho^k(x):=(x_{\rho^k(1)},\cdots,x_{\rho^k(n)})$로 정의한다.

정의 3. 임의의 $x\in V_n$에 대하여 $f(x)=f(\rho(x))$가 성립하면 함수 f를 *회전대칭*이라고 한다.

치환 ρ의 작용에 대한 벡터 x의 궤도(orbit)란 집합 $\{\rho^k(x)|k\in\mathbb{Z}\}$를 말한다. 따라서, 회전대칭 함수는 임의의 궤도상에서 함수값이 고정된다. 회전 치환의 작용을 단항식 $m(x)=x_{i_1}\cdots x_{i_d}\in B_n$에 확장하여 $\rho^k(m(x)):=x_{\rho^k(i_1)}\cdots x_{\rho^k(i_d)}$로 정의한다. 따라서 $m(x)$의 궤도는 $\{\rho^k(m(x))|k\in\mathbb{Z}\}$로 정의된다.

보조정리 4. 만약 단항식 $m(x)$가 회전대칭 함수의 항으로서 존재하면 $m(x)$의 궤도에 속하는 모든 단항식들도 그 함수에 항으로서 존재해야 한다.

증명. 항의 차수에 대하여 귀납법을 이용한다. n-변수 함수 f가 회전대칭이라고 하자. 함수 f에서 k차 미만의 항들을 뺀 다항식을 f_k라고 하자. 그러면, $f(x)=a_0+\Sigma_{i=1}^{n}a_ix_i+f_2(x)$로 나타낼 수 있다. 벡터 $(1,0,\cdots,0)$의 궤도 상에서 함수 f_2는 항상 0이므로, $a_0+a_1=a_0+a_2=\cdots=a_0+a_n$임을 알 수 있다. 따라서 일차 단항식은 그 성질을 만족한다. $k-1$차 단항식까지 그 성질이 성립한다고 가정하자. 어떤 k차 단항식 $m(x)=x_{i_1}\cdots x_{i_k}$의 궤도의 크기가 t라고 하자. $g(x):=f(x)-f_k(x)$라 두고, $f_k(x)$에서 $m(x)$ 궤도의 모든 항들을 뺀 식을 $h_k(x)$라고 하면 $f(x)=g(x)+\Sigma_{i=1}^{t}b_i\rho^{i-1}(m(x))+h_k(x)$로 표현된다. 벡터 $e=(e_1,\cdots,e_n)$를, $i\in\{i_1,\cdots,i_k\}$이면 $e_i=1$ 그렇지 않으면 $e_i=0$으로 정의하면, f가 회전대칭이므로 e의 궤도에서 f의 함수 값은 고정되어 $g(e)+b_1=\cdots=g(\rho^{t-1}(e))+b_t$가 성립한다. 가정에서 g도 회전대칭이므로 $b_1=\cdots=b_t$이다. 따라서 k차 항들도 보조정리의 성질을 만족한다. □

다음은 4-변수 회전대칭 불함수의 예이다.

$x_1x_3+x_2x_4+x_1x_2x_3+x_2x_3x_4+x_3x_4x_1+x_4x_1x_2$

IV. 이차 불함수의 기본 성질

다음 보조정리 5는 참고문헌 [7]에서 찾아 볼 수 있다. 이를 임의화 보조정리(randomization lemma)라고도 하며 쉽게 증명이 가능하다.

보조정리 5. n-변수 함수가 $f(x_1,\cdots,x_{n-1})+x_n$ 꼴로 표현되면 이 함수는 균형함수이다.

다음 정리는 Dickson에 의하여 처음 증명되었고 [1], 정리의 완전한 꼴과 증명은 문헌 [7]을 참고한다.

정리 6. 임의의 n-변수 이차 함수 f는 다음 세 가지 종류의 함수들 중 하나와 아핀동치이다. 만약 f가 균형함수라면, 어떤 정수 $k\le(n-1)/2$에 대하여, $\Sigma_{i=1}^{k}x_{2i-1}x_{2i}+x_{2k+1}$과 아핀동치이다. 만약 f가 균형함수가 아니라면, 어떤 $k\le n/2$와 $b\in$GF(2)에 대하여, 함수 $\Sigma_{i=1}^{k}x_{2i-1}x_{2i}+b$와 아핀동치이다. 여기서 $wt(f)<2^{n-1}$이면 $b=0$이고 $wt(f)>2^{n-1}$이면 $b=1$이 된다.

어떤 이차 함수에 대하여, 정리 6에서 기술된 꼴의 아핀동치 함수가 결정되면 그것의 해밍무게와 비선형성을 쉽게 계산할 수 있다. 다음 보조정리 7은 참고문헌 [7]에서 찾을 수 있는데, 논문 [6]에서 기본도구로 사용되며 참고문헌 [7]과는 다른 방법으로서 직접 공식을 유도한다.

보조정리 7. n-변수 이차 함수가, 정수 $k\le n/2$에 대하여, $h(x)=\Sigma_{i=1}^{k}x_{2i-1}x_{2i}+\Sigma_{i=2k+1}^{n}a_ix_i$이면 비선형성은 $NL(h)=2^{n-1}-2^{n-k-1}$로 주어진다. 만약 일차항이 하나도 없으면 그것의 해밍무게는 비선형성과 같다. 그렇지 않으면 균형함수가 된다.

V. 회전대칭 동차 이차 불함수의 해밍무게 및 비선형성

논문 [2,8]에서는 가장 단순한 꼴의 회전대칭 이차 함수로서 이차단항식의 궤도 한 개로만 구성된 동차함수들을 주로 다루고 있다. 정수 $2\le s\le\lceil n/2\rceil$에 대하여 이 함수는 다음과 같이 정의된다.

$$\begin{aligned}f_{n,s}(x)&:=\Sigma_{i=0}^{n-1}\rho^i(x_1x_s)\\&=x_1x_s+x_2x_{s+1}+\cdots+x_nx_{s-1}\end{aligned}\quad(1)$$

짝수 n과 $s=n/2+1$에 대하여 함수 $f_{n,s}(x)$는 $\Sigma_{i=1}^{n/2}\rho^{i-1}(x_1x_s)$로 정의하는 것이 자연스러우며, 이 함수들은 Maiorana-McFarland 함수 클래스에 포함되어 최대의 비선형성을 가진다.

Pieprzyk[8] 등은 $f_{n,s}$가 고속 해시함수의 설계에 매우 적합하다고 논하면서, $s=2$인 경우의 해밍무게 및 비선형성이 다음 범위에 있다는 것을 밝혔다. 즉,

$$2^{n-2} \le wt(f_{n,2}) \le 2^n + 2^{n-2},$$
$$NL(f_{n,2}) \ge 2^{n-2}.$$

또한, n이 홀수이고 $s=2$인 경우, 해밍무게 및 비선형성 공식이 다음과 같이 주어진다는 것을 밝혔다.

$$wt(f_{n,2}) = 2^{n-1},$$
$$NL(f_{n,2}) = 2^{n-1} - 2^{(n-1)/2}. \quad (2)$$

Cusick[2] 등은 n이 짝수이고 $s=2$일 경우, 해밍무게와 비선형성의 공식을 다음과 같이 구했다.

$$wt(f_{n,2}) = NL(f_{n,2}) = 2^{n-1} - 2^{n/2} \quad (3)$$

또한, 궤도 한 개로 구성된 삼차 회전대칭 함수의 해밍무게를 기술하는 생성함수를 찾는데 성공하였다.

Kim[6] 등은 앞의 두 공식 (2), (3)을 보다 일반화하여, 임의의 n과 $2 \le s \le \lceil n/2 \rceil$에 대하여 $f_{n,s}$의 해밍무게 및 비선형성 값의 공식을 발견하였다. $k := \gcd(n, s-1)$로 두고, 만약 n/k가 짝수일 경우 그 값들의 공식은 다음과 같이 주어진다.

$$wt(f_{n,s}) = NL(f_{n,s}) = 2^{n-1} - 2^{n/2+k-1} \quad (4)$$

만약 n/k가 홀수라면 해밍무게와 비선형성의 공식은 다음과 같이 주어진다.

$$wt(f_{n,s}) = 2^{n-1},$$
$$NL(f_{n,s}) = 2^{n-1} - 2^{(n+k)/2-1}. \quad (5)$$

VI. 회전대칭 이차 불함수의 해밍무게

본 절에서는 회전대칭 함수 $f_{n,s}$에 일차항이 포함된 함수 $g_{n,s}$의 해밍무게를 알아본다. 보조정리 4에 의해 일차항이 포함되면 그 항의 궤도가 모두 항으로 존재해야 하므로 함수 $g_{n,s}$는 다음과 같이 정의된다.

$$g_{n,s}(x) := f_{n,s}(x) + (x_1 + \cdots + x_n) \quad (6)$$

정의에 의해 $NL(f_{n,s}) = NL(g_{n,s})$임은 자명하다.

함수 $g_{n,s}$의 해밍무게를 구하기 위하여 논문 [6]의 방법을 동일하게 사용한다. 그 논문에서는 $s=2$인 경우, 즉, $f_{n,2}$의 아핀동치 함수로서 보조정리 7의 꼴이 되는 것을 우선 찾는다. 이것은 결국 Pieprzyk[8] 등과 Cusick[2] 등의 결과를 매우 간결하고 일관된 방법으로 얻는 것을 의미한다. 다음으로 함수 $f_{n,s}$의 아핀동치 함수를 $f_{n,2}$ 꼴의 함수를 이용하여 표현함으로서 $f_{n,s}$의 해밍무게와 비선형성을 계산한다. 이들의 방법이 함수 $g_{n,s}$에 대해서도 비슷하게 적용이 가능하다는 점을 본 논문에서 사용한다.

보조정리 8. 변수의 개수가 $n \ge 6$이면 아핀동치 $g_{n,2} \equiv u_1u_2 + u_3u_4 + 1 + g_{n-4,2}$가 성립한다. 여기서 변수 u_1, u_2, u_3, u_4는 함수 $g_{n-4,2}$의 변수들과는 독립된 변수들이다.

증명. 식 $x_1 + x_3 + 1$과 $x_2 + x_n + 1$을 새로운 변수 u_1과 u_2로 각각 치환하면 주어진 함수 $g_{n,2}$가 다음과 같이 표현된다.

$$g_{n,2} = u_1u_2 + 1 + (x_3x_4 + \cdots + x_{n-1}x_n + x_nx_3) + (x_4 + \cdots + x_{n-1})$$

다시 식 $x_3 + x_5 + 1$과 $x_4 + x_n$을 각각 u_3, u_4로 치환하면 함수 $g_{n,2}$는 다음과 같이 표현된다.

$$g_{n,2} = u_1u_2 + u_3u_4 + 1 + (x_5x_6 + \cdots + x_{n-1}x_n + x_nx_5) + (x_5 + \cdots + x_n)$$

바로 위의 식에서 변수 x_i로 표현되는 부분은 함수 $g_{n-4,2}$와 아핀동치임을 알 수 있다. 그리고 앞의 변수 치환에서 변수 $u_1, \cdots, u_4$는 변수 $x_5, \cdots, x_n$과 독립임을 알 수 있다. □

이제 $g_{n,2}$의 해밍무게를 알아본다. 우선 작은 n에 대하여, $g_{n,2}$의 아핀동치 함수로서 해밍무게 계산이 쉬운 함수를 직접 계산에 의하여 찾는다. 편의상 $g_{2,2} := x_1 + x_2 (\equiv x_1)$로 정의한다. 함수 $g_{3,2}$는 다음의 관계식을 만족한다. 즉,

$$g_{3,2} = x_1x_2 + x_2x_3 + x_3x_1 + x_1 + x_2 + x_3 = (x_1 + x_3 + 1)(x_2 + x_3 + 1) + 1$$

따라서 $g_{3,2} \equiv x_1x_2 + 1$임을 알 수 있다. 함수 $g_{4,2}$와 $g_{5,2}$에 대해서도 같은 방법으로 계산할 수 있다. 한편, 함수 $g_{6,2}$의 아핀동치는 보조정리 8을 적용하면 $g_{6,2} \equiv x_1x_2 + x_3x_4 + x_5$임을 바로 알 수 있다. 같은 방법으로, 보조정리 8과 $g_{3,2}$, $g_{4,2}$, $g_{5,2}$의 아핀동치 함수들을 이용하면, 함수 $g_{7,2}$, $g_{8,2}$, $g_{9,2}$들의 아핀 동치함수를 얻을 수 있다. 이상의 결과를 정리하면 다음과 같다.

$$
\begin{aligned}
g_{2,2} &\equiv x_1\\
g_{3,2} &\equiv x_1x_2+1\\
g_{4,2} &\equiv x_1x_2+1\\
g_{5,2} &\equiv x_1x_2+x_3x_4+1\\
g_{6,2} &\equiv x_1x_2+x_3x_4+x_5\\
g_{7,2} &\equiv x_1x_2+x_3x_4+x_5x_6\\
g_{8,2} &\equiv x_1x_2+x_3x_4+x_5x_6\\
g_{9,2} &\equiv x_1x_2+x_3x_4+x_5x_6+x_7x_8
\end{aligned} \tag{7}
$$

위의 동치함수들은 보조정리 7을 적용하여 해밍무게를 바로 계산할 수 있는 꼴이다. 이들 동치관계를 이용하면 일반적인 n에 대하여 $g_{n,2}$의 아핀동치 함수를 얻을 수 있다. 예를 들어, 만약 $n\equiv 3 \pmod 8$인 경우, 보조정리 8을 $(n-3)/4$번 반복적으로 적용하고 관계식 (7)을 적용하면 다음 아핀동치 함수를 얻을 수 있다.

$$
\begin{aligned}
g_{n,2} &\equiv x_1x_2+\cdots+x_{n-4}x_{n-3}+g_{3,2}\\
&\equiv x_1x_2+\cdots+x_{n-2}x_{n-1}+1
\end{aligned}
$$

나머지 경우에 대해서도 같은 방법으로 유도하면 $n \pmod 8$에 대하여 $g_{n,2}$의 아핀동치 함수들을 다음과 같이 얻을 수 있다.

$$
g_{n,2} \equiv \begin{cases}
\Sigma_{i=1}^{n/2-1} x_{2i-1}x_{2i}, & n\equiv 0\\
\Sigma_{i=1}^{(n-1)/2} x_{2i-1}x_{2i}, & n\equiv 1,7\\
\Sigma_{i=1}^{n/2-1} x_{2i-1}x_{2i}+x_{n-1}, & n\equiv 2,6\\
\Sigma_{i=1}^{(n-1)/2} x_{2i-1}x_{2i}+1, & n\equiv 3,5\\
\Sigma_{i=1}^{n/2-1} x_{2i-1}x_{2i}+1, & n\equiv 4
\end{cases} \tag{8}
$$

따라서 보조정리 7을 이용하여 $g_{n,2}$의 해밍무게를 바로 계산할 수 있다. 예를 들어, $n\equiv 3 \pmod 8$인 경우 $k=(n-1)/2$로 적용하면 다음을 얻는다.

$$
\begin{aligned}
wt(g_{n,2}) &= 2^n-(2^{n-1}-2^{n-(n-1)/2-1})\\
&= 2^{n-1}+2^{(n-1)/2}
\end{aligned}
$$

나머지의 경우에 대해서도 마찬가지로 계산하면 다음 보조정리 9의 공식을 얻을 수 있다.

보조정리 9. 불함수 $g_{n,2}(x)=\Sigma_{i=0}^{n-1}\rho^i(x_1x_2+x_1)$의 해밍무게는 $n \pmod 8$에 대하여 다음과 같다.

$$
wt(g_{n,2}) = \begin{cases}
2^{n-1}-2^{n/2}, & n\equiv 0\\
2^{n-1}-2^{(n-1)/2}, & n\equiv 1,7\\
2^{n-1}, & n\equiv 2,6\\
2^{n-1}+2^{(n-1)/2}, & n\equiv 3,5\\
2^{n-1}+2^{n/2}, & n\equiv 4
\end{cases}
$$

이제 일반적인 s에 대하여 $g_{n,s}$의 해밍무게를 알아본다. 우선 함수 $f_{n,s}$의 구조적 특성에 대하여 기술한다[6]. 회전 치환 ρ에 대하여 치환 $\rho_s=\rho^{s-1}$로 나타내자. 식 (1)에 의한 정의와 ρ_s로부터 함수 $f_{n,s}$는 $x_1x_{\rho_s(1)}+x_2x_{\rho_s(2)}+\cdots+x_nx_{\rho_s(n)}$으로 표현된다.

치환 ρ_s는 분리된 순환치환(disjoint cycle)의 곱으로 유일하게 나타낼 수 있는데, 이를 $\rho_s=\tau_1\cdots\tau_k$라고 하자. 순환치환 τ_i는 $\tau_i=(j,\rho_s(j),\cdots,\rho_s^{t-1}(j))$로 나타낼 수 있다. 이때 t를 이 순환치환의 길이라고 한다. 즉 τ_i는 $\{1,2,\cdots,n\}$를 $j\to\rho_s(j)\to\cdots\to\rho_s^{t-1}(j)\to j$ 구조로 대응시킨다. 따라서 τ_i는 불함수 $f_{\tau_i}(x)=x_jx_{\rho_s(j)}+x_{\rho_s(j)}x_{\rho_s^2(j)}+\cdots+x_{\rho_s^{t-1}(j)}x_j$와 대응된다. 따라서 관계식 $f_{n,s}=f_{\tau_1}+f_{\tau_2}+\cdots+f_{\tau_k}$가 성립한다. 논문 [6]에 의하면 ρ_s의 분리된 순환치환 τ_i들의 길이는 모두 같으며 $t=n/\gcd(n,s-1)$로 주어진다. 또한 순환치환의 개수는 $k=\gcd(n,s-1)$로 주어진다. 한편, 순환치환 τ_i에 의한 함수 $f_{\tau_i}(x)$에서 변수들을 $x_j\to x_1$, $x_{\rho_s(j)}\to x_2$, $\cdots$, $x_{\rho_s^{t-1}(j)}\to x_t$로 바꾸어 표현하면 결국 f_{τ_i}와 $f_{t,2}$는 아핀동치임을 알 수 있다. 따라서 아핀동치 $f_{n,s}\equiv f_{t,2}^{(1)}+f_{t,2}^{(2)}+\cdots+f_{t,2}^{(k)}$가 성립한다. 여기서 $f_{t,2}^{(i)}$는 f_{τ_i}로부터 유도된, $f_{t,2}$ 꼴의 아핀동치 함수를 나타낸다.

위에서 살펴본 사실들은 일차항이 포함된 함수 $g_{n,s}(x)=f_{n,s}(x)+(x_1+\cdots+x_n)$에 대해서도 그대로 적용된다. 즉, ρ_s의 분리된 순환치환 τ_i들에 대하여 아핀동치 $g_{n,s}\equiv g_{t,2}^{(1)}+g_{t,2}^{(2)}+\cdots+g_{t,2}^{(k)}$가 성립하며, 이때 $g_{t,2}^{(i)}(x)=f_{t,2}^{(i)}(x)+(x_1^{(i)}+x_2^{(i)}+\cdots+x_t^{(i)})$이고 위첨자 (i)는 각각의 대상들이 τ_i와 관계있음을 나타낸다. 식 (8)로 주어진 아핀동치를 이용하면 $g_{n,s}$의 아핀동치 함수들은 $t \pmod 8$에 대하여 다음과 같이 주어진다.

$$
g_{n,s} \equiv \begin{cases}
\Sigma_{i=1}^{k}\left(\Sigma_{j=1}^{t/2-1}x_{2j-1}^{(i)}x_{2j}^{(i)}\right), & t\equiv 0\\
\Sigma_{i=1}^{k}\left(\Sigma_{j=1}^{(t-1)/2}x_{2j-1}^{(i)}x_{2j}^{(i)}\right), & t\equiv 1,7\\
\Sigma_{i=1}^{k}\left(\Sigma_{j=1}^{t/2-1}x_{2j-1}^{(i)}x_{2j}^{(i)}+x_{t-1}^{(i)}\right), & t\equiv 2,6\\
\Sigma_{i=1}^{k}\left(\Sigma_{j=1}^{(t-1)/2}x_{2j-1}^{(i)}x_{2j}^{(i)}+1\right), & t\equiv 3,5\\
\Sigma_{i=1}^{k}\left(\Sigma_{j=1}^{t/2-1}x_{2j-1}^{(i)}x_{2j}^{(i)}+1\right), & t\equiv 4
\end{cases} \tag{9}
$$

보조정리 7을 이용하여 (9)에서 제시된 $g_{n,s}$의 아핀동치 함수들의 해밍무게를 계산할 수 있다. 예를 들어 $t\equiv 2,6 \pmod 8$인 경우 $g_{n,s}$는 균형함수가 됨을 알 수 있다. 또한 $t\equiv 1,7 \pmod 8$인 경우, (9)의 두 번째 동치식에서 분리된 이차항들이 $(n-k)/2$개로서 $g_{n,s}(x)\equiv x_1x_2+x_3x_4+\cdots+x_{n-k-1}x_{n-k}$임을 알 수 있다. 여기서 t가 홀수일 때 n과 k는 같은 패리티

(parity)를 가진다. 보조정리 7을 이용하면 $g_{n,s}$의 해밍무게는 $2^{n-1}-2^{n-(n-k)/2-1}=2^{n-1}-2^{(n+k)/2-1}$임을 알 수 있다. 나머지 경우도 같은 방법으로 계산하면 함수 $g_{n,s}$의 해밍무게는 다음 정리 10에서와 같이 얻을 수 있다.

정리 10. 양의 정수 n과 $2 \le s \le \lceil n/2 \rceil$에 대하여 회전대칭 불함수 $g_{n,s}(x)=\Sigma_{i=0}^{n-1}\rho^i(x_1x_s+x_1)$의 해밍무게는, $k=\gcd(n,s-1)$와 $n/k \pmod 8$에 대하여 다음과 같다.

$$wt(g_{n,s})=\begin{cases}2^{n-1}-2^{n/2+k-1}, & n/k\equiv 0\\ 2^{n-1}-2^{(n+k)/2-1}, & n/k\equiv 1,7\\ 2^{n-1}, & n/k\equiv 2,6\\ 2^{n-1}-(-1)^k2^{(n+k)/2-1}, & n/k\equiv 3,5\\ 2^{n-1}-(-1)^k2^{n/2+k-1}, & n/k\equiv 4\end{cases}$$

VII. 실험적 고찰

궤도가 두 개 이상인 회전대칭 이차함수에 대해서는 해밍무게 및 비선형성에 대해서 아직 알려진 바가 없는 것으로 보인다. 앞에서 기술한 방법 또한 잘 적용이 되지 않는다. Cusick[2] 등은 삼차 함수의 해밍무게에 대해서 약간의 결과를 얻었다. 그들이 고려한 회전대칭 함수는 다음과 같다.

$$f_{n,2,3}(x)=x_1x_2x_3+x_2x_3x_4+\cdots+x_nx_1x_2$$

그들은 함수 $f_{n,2,3}$의 해밍무게에 대한 닫힌 공식(closed formula)을 얻지는 못하고, 그 값들의 재귀적 성질 및 생성함수를 얻는데 성공하였다. 함수 $f_{n,2,3}$의 해밍무게는 다음의 재귀적 관계를 만족한다.

$$wt(f_{n,2,3})=2(wt(f_{n-2,2,3})+wt(f_{n-3,2,3}))+2^{n-3}$$

또한 해밍무게의 생성함수는 다음과 같다.

$$\frac{8z^6/(1-2z)+z^3+4z^4+4z^5}{1-2z^2-2z^3}$$

한편, 실험적 계산으로 $n=9$까지 $f_{n,2,3}$의 해밍무게와 비선형성이 같다는 것을 확인하고 이것이 일반적으로 성립할 것으로 추측하였다. 우리는 $n=14$까지 실험적으로 계산하였는데, 그 추측이 여전히 성립함을 확인할 수 있었다. 한 개의 궤도로 구성되는 회전대칭 삼차함수의 가장 일반적인 꼴은 다음과 같다.

$$f_{n,s,t}(x)=x_1x_sx_t+x_2x_{s+1}x_{t+1}+\cdots+x_nx_{s-1}x_{t-1}$$

우리는 $6 \le n \le 14$, $2 \le s < t \le n$에 대하여 해밍무게와 비선형을 실험적으로 계산하였으며 그 결과는 다음 [표 2]와 같다.

두 개의 궤도로 정의되는 회전대칭 이차 동차함수는 $f_{n,s}+f_{n,t}$로 정의되며, $n=16$ 까지 해밍무게와 비선형

[표 2] 회전대칭 삼차 함수 $f_{n,s,t}$의 해밍무게 및 비선형성 ($6 \le n \le 14$, $2 \le s < t \le n$). 중복된 함수들은 생략됨

	n = 6		n = 7		n = 8		n = 9		n = 10		n = 11		n = 12		n = 13		n = 14	
s,t	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL
2,3	18	18	36	36	80	80	172	172	360	360	760	760	1576	1576	3264	3264	6720	6720
2,4	24	24	36	36	112	104	184	184	440	440	848	848	1792	1792	3680	3680	7392	7392
3,4	24	24	36	36	112	104	184	184	440	440	848	848	1792	1792	3680	3680	7392	7392
2,5			36	36	112	104	184	184	440	440	848	848	1792	1792	3680	3680	7392	7392
3,5	14	14	36	36	96	96	172	172	312	312	760	760	1656	1656	3264	3264	6624	6624
4,5					112	104	184	184	440	440	848	848	1792	1792	3680	3680	7392	7392
2,6							172	172	480	448	848	848	1768	1768	3680	3680	7392	7392
3,6					80	80	184	184	480	448	848	848	1792	1792	3680	3680	7392	7392
4,6							184	184	480	448	848	848	1792	1792	3680	3680	7392	7392
5,6									480	448	848	848	1768	1768	3680	3680	7392	7392
2,7											760	760	1984	1888	3680	3680	7392	7392
3,7									312	312	848	848	1920	1920	3680	3680	6624	6624
4,7							148	148	360	360	760	760	1792	1792	3264	3264	6720	6720
5,7											848	848	1920	1920	3680	3680	6624	6624
6,7													1984	1888	3680	3680	7392	7392
2,8															3264	3264	8064	7808
3,8													1576	1576	3680	3680	8064	7808
4,8											760	760	1792	1792	3680	3680	8064	7808
5,8													1792	1792	3680	3680	8064	7808
6,8															3680	3680	8064	7808
7,8																	8064	7808
3,9																	6624	6624
4,9															3264	3264	7392	7392
5,9													1400	1400	3264	3264	6624	6624
6,9																	7392	7392
5,10																	6720	6720

〔표 3〕 회전대칭 이차 함수 $f_{n,s}+f_{n,t}$의 해밍무게 및 비선형성 ($6 \le n \le 16$, $2 \le s < t \le \lceil (n+1)/2 \rceil$)

	n = 6		n = 7		n = 8		n = 9		n = 10		n = 11		n = 12		n = 13		n = 14		n = 15		n = 16	
s,t	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL	wt	NL
2,3	32	16	56	56	144	112	288	224	512	480	1056	992	2176	1920	4160	4032	8192	8064	16640	16128	33024	32512
2,4	16	16	56	56	64	64	240	240	480	480	1056	992	1920	1920	4160	4032	8064	8064	16256	16256	31744	31744
3,4	24	bent	56	56	144	112	240	240	512	384	1056	992	1984	1984	4160	4032	8192	8064	16896	15872	33024	32512
2,5					136	bent	288	224	512	384	1056	992	1920	1920	4160	4032	8192	8064	15360	15360	32512	32512
3,5					120	bent	288	224	480	480	1056	992	2048	1536	4160	4032	8064	8064	16640	16128	32256	32256
4,5					136	bent	240	240	512	480	1056	992	2112	1984	4160	4032	8192	7168	16256	16256	32512	32512
2,6									496	bent	1056	992	1536	1536	4160	4032	8064	8064	16640	16128	31744	31744
3,6									528	bent	1056	992	2176	1920	4160	4032	8192	7168	16640	16128	33024	32512
4,6									496	bent	1056	992	1920	1920	4160	4032	8064	8064	16256	16256	28672	28672
5,6									528	bent	1056	992	1920	1920	4160	4032	8192	8064	16640	16128	32512	32512
2,7													1984	1984	4160	4032	8192	7168	16896	15872	33024	32512
3,7													1536	1536	4160	4032	8064	8064	16256	16256	24576	24576
4,7													2080	bent	4160	4032	8192	8064	16640	16128	33024	32512
5,7													1920	1920	4160	4032	8064	8064	16896	15872	32256	32256
6,7													1984	1984	4160	4032	8192	8064	16256	16256	33024	32512
2,8																	8128	bent	16640	16128	28672	28672
3,8																	8256	bent	15360	15360	33024	32512
4,8																	8128	bent	16896	15872	31744	31744
5,8																	8256	bent	16640	16128	32512	32512
6,8																	8128	bent	16640	16128	31744	31744
7,8																	8256	bent	16256	16256	33024	32512
2,9																					32896	bent
3,9																					32640	bent
4,9																					32896	bent
5,9																					32640	bent
6,9																					32896	bent
7,9																					32640	bent
8,9																					32896	bent

성을 실험적으로 계산하였다. 그 결과는 위의 〔표 3〕과 같다.

VIII. 결 론

본 논문에서는 회전대칭 동차 이차 불함수에 대한 해밍무게와 비선형성에 대한 최근의 연구결과를 기술하고, 이를 약간 더 개선하여 일차 항이 포함된 함수꼴에 대하여 해밍무게 공식을 계산하는 방법을 보였다. 논문 〔6〕에서 제안한 방법으로서 회전대칭 이차 함수와 자연스럽게 연관되는 치환을 분해하여 분리된 순환치환의 곱으로 단순하게 변형하는 방법을 써서 해밍무게를 쉽게 계산할 수 있었다. 그 논문에서 제기한, 궤도가 두 개 이상인 이차함수 또는 가장 단순한 회전대칭 삼차 함수 등에 적용하는 방법에 대해서는 아직 결과가 없는 것으로 추정되며 흥미로운 주제로 보인다.

참 고 문 헌

〔1〕 C. Carlet, "Boolean Functions for Cryptography and Error Correcting Codes," in: Y. Crama, P. Hammer, (Eds.), Boolean Methods and Models, Cambridge Univ. Press, (in press). Available at http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html.

〔2〕 T.W. Cusick and P. Stanica, "Fast evaluation, weights and nonlinearity of rotation-symmetric functions," Disc. Math., vol. 258, no. 1-3, pp. 289-301, Dec. 2002.

〔3〕 S. Kavut, S. Maitra, S. Sarkar, and M.D. Yücel, "Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity > 240," IndoCrypt 2006, LNCS 4329, pp. 266-279, 2006.

〔4〕 S. Kavut, S. Maitra, and M.D. Yücel, "Search for Boolean functions with excellent profiles in the rotation symmetric class," IEEE Trans. Inform. Theory, vol. 53, no. 5, pp. 1743-1751, May 2007.

〔5〕 S. Kavut and M.D. Yücel, "Generalized rotation symmetric and dihedral symmetric Boolean functions - 9 variable Boolean functions with nonlinearity 242," AAECC 2007, LNCS 4851, pp. 321-329,

2007.
[6] H. Kim, S.M. Park, and S.G. Hahn, "On the weight and nonlinearity of homogeneous rotation symmetric Boolean functions of degree 2," Disc. Appl. Math., vol. 157, no. 2, pp. 428-432, Jan. 2009.
[7] F.J. MacWilliams and N.J. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, The Netherlands, 1977.
[8] J. Pieprzyk and C.X. Qu, "Fast hashing and rotation-symmetric functions," J. of Universal Computer Science, vol. 5, no. 1, pp. 20-31, Jan. 1999.
[9] O.S. Rothaus, "On "bent" functions," J. Combinatorial Theory (A), vol. 20, no. 3, pp. 300-305, May 1976.
[10] S. Sarkar and S. Maitra, "Idempotents in the neighbourhood of Patterson-Wiedemann functions having Walsh spectra zeros," Designs, Codes and Cryptography, vol. 49, no. 1-3, pp. 95-103, Dec. 2008.
[11] P. Stanica and S. Maitra, "Rotation symmetric functions - count and cryptographic properties," Disc. Appl. Math., vol. 156, no. 10, pp. 1567-1580, May 2008.
[12] P. Stanica, S. Maitra, and J.A. Clark, "Results on rotation symmetric bent and correlation immune Boolean functions," FSE 2004, LNCS 3017, pp. 161-177, 2004.

〈著者紹介〉

사 진

김 현 진 (Hyeonjin Kim) 정회원
1992년 2월: 서울대학교 수학과 졸업
1994년 2월: 포항공과대학교 수학과 석사
2008년 8월: 한국과학기술원 수리과학과 박사
1994년 2월~1999년 9월: 한국전자통신연구원
1999년 10월~현재: 한국전자통신연구원 부설연구소 선임연구원
〈관심분야〉 정보보호, 암호분석, 불함수이론

사 진

정 창 호 (Changho Jung) 정회원
2002년 2월: 고려대학교 응용생명환경화학과 학사
2004년 8월: 고려대학교 정보보호대학원 석사
2005년 3월~현재: 한국전자통신연구원 부설연구소 연구원
〈관심분야〉 정보보호, 암호분석, 컴퓨터 포렌식

사 진

박 일 환 (Ilhwan Park) 정회원
1988년 2월: 고려대학교 수학과 졸업
1990년 2월: 고려대학교 수학과 석사
1996년 2월: 고려대학교 수학과 박사
1996년 5월~1999년 12월: 한국전자통신연구원
2000년 1월~현재: 한국전자통신연구원 부설연구소 책임연구원
〈관심분야〉 정보보호이론