creative commons
COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

교 육 학 석 사 학 위 논 문

Niho 형태의 4개의 상호상관관계 함숫값을 갖는 함수

2013년 2 월

부경대학교 교육대학원

수 학 교 육 전 공

최 지 연

교 육 학 석 사 학 위 논 문

Niho 형태의 4개의 상호상관관계 함숫값을 갖는 함수

지도교수 조 성 진

이 논문을 교육학석사 학위논문으로 제출함.

2013년 2 월

부경대학교 교육대학원

수 학 교 육 전 공

최 지 연

최지연의 교육학석사 학위논문을 인준함.

2013년 2월 22일

주 심 이학박사 표 용 수 (인)

위 원 이학박사 박 진 한 (인)

위 원 이학박사 조 성 진 (인)

목 차

PUKYONG NATIONAL UNIVERSITY 부경대학교

표 목차

그림 목차

PUKYONG NATIONAL UNIVERSITY
부경대학교

Niho type four-valued cross-correlation function

Ji-Youn Choi

Graduate School of Education

Pukyong National University

Abstract

One of important problems in the theory of sequences is to determine the values and the number of occurrences of each value taken on by the cross-correlation function $C_d(\tau)$, where d is a decimation. To know the number of occurrence of values we need to solve the equation $x^d+(x+1)^d=1$. In this thesis, we find the values and the number of occurrences of each value of $C_d(\tau)$ where $d=(2^m-1)(2^{2m}+1)+2$, when m is an integer and we study the equation $x^d+(x+1)^d=1$.

PUKYONG NATIONAL UNIVERSITY 부경대학교

I. 서 론

코드분할다중접속(CDMA) 시스템에서 이진 수열은 많이 응용되고 있다. CDMA 시스템에서의 신호 디자인에 대한 가장 중요한 연구 영역 중의 하나는 좋은 상관관계 성질을 갖는 이진 수열을 만드는 것이다. 최대주기수열의 상호상관관계 함수들은 지난 50년간 연구되어 왔다. Niho [15], Helleseth [6] and Rosendahl [16]이 이 주제에 관한 놀라울 만한 논문들을 썼다. 유한체 이론에 의한, 일반적인 수열과 m-수열은 [5, 13, 14, 17]을 참조한다. q개의 원소를 갖는 유한체는 $GF(q)$로 나타낸다. q는 $m \geq 1$인 정수에 대하여 $q = 2^m$으로 표현된다.

$GF(q)$의 곱셈군은 $GF(q)^*$라 나타낸다. 즉, $GF(q)^* = GF(q) \setminus \{0\}$이다. $GF(q)^*$ 군은 순환적이고 $GF(q)^*$의 원시원소는 $GF(q)^*$의 생성자이다. 차수가 n인 기약다항식 $f(x) \in GF(2)[x]$가 $GF(q)$의 원시원소의 최소다항식이면 $GF(2)$ 위에서의 원시다항식(primitive polynomial)이라고 한다.

$v(t)=u(dt)$ $(1 \leq d \leq 2^n - 2)$인 수열 $u(t)$와 $v(t)$의 상호상관관계 함수 $C_d(\tau)$는 $\tau = 0, 1, \cdots, 2^n - 2$에 대하여

$$C_d(\tau) = \sum_{t=0}^{2^n-2} (-1)^{u(t+\tau)+v(t)}$$

로 정의된다.

수열 이론의 중요한 문제는 상호상관관계 함수 $C_d(\tau)$의 값들과 개수를 결정하는 것이다.

잘 알려진 3개의 상호상관관계 함숫값들을 갖는 경우는 다음과 같다.

(a) $d=2^k+1$, $n/\gcd(n, k)$이 홀수,

(b) $d=2^{2k}-2^k+1$, $n/\gcd(n, k)$이 홀수,

(c) $d=2^{n/2}+2^{(n+2)/4}+1$, $n\equiv 2 \pmod 4$,

(d) $d=2^{n/2+1}+3$, $n\equiv 2 \pmod 4$,

(e) $d=2^{(n-1)/2}+3$, n이 홀수,

(f) $d=2^{(n-1)/2}+2^{(n-1)/4}-1$, $n\equiv 1 \pmod 4$,

(g) $d=2^{(n-1)/2}+2^{(3n-1)/4}-1$, $n\equiv 3 \pmod 4$.

(a)는 Gold [4]에 의해 밝혀졌고 (b)는 Kasami [11]에 의해 밝혀졌으며, (c)와 (d)는 Cusick와 Dobbertin [2]에 의해 밝혀졌다. 그리고 (e)는 Canteaut 등 [1]에 의해 밝혀졌다. (f)와 (g)는 Hollmann 과 Xiang [7] 에 의해 밝혀졌다.

또한 잘 알려진 4개의 상호상관관계 함숫값들을 갖는 경우는 다음과 같다.

(h) $d=2^{n/2+1}-1$, $n\equiv 0 \pmod 4$,

(i) $d=(2^{n/2}+1)(2^{n/4}-1)+2$, $n\equiv 0 \pmod 4$,

(j) $d=\sum_{i=0}^{n/2} 2^{im}$, $n\equiv 0 \pmod 4$, $0<m<n$, $\gcd(m,n)=1$

(k) $d=\frac{2^{k-1}}{2^s-1}(2^{2k}+2^{s+1}-2^{k+1}-1)$, $n=2k$, $2s|k$.

(h)와 (i)는 Niho [15]에 의해 밝혀졌고, (j)는 Dobbertin [3]에 의해서 그리고 (k)는 Helleseth와 Rosendahl [8], 그리고 Rosendahl [16]에 의해 밝혀졌다.

2007년에 Helleseth 등 [9]은 상호상관관계 함숫값이 적어도 4가 되는 d를 제안하였다. 그리고 Johansen 과 Helleseth [10]은 m이 홀수이고 k=1일 때 5개의 상호상관관계 함숫값을 갖는 d, $d=\frac{2^{2k}+1}{2^k+1}$를 제안하였다.

위의 (i)가 4개의 상호상관관계 함숫값을 갖는다는 것을 Niho [15]가 밝혔다. 그러나 Niho의 증명은 매우 길고, Welch의 결과를 이용하여 증명을 하였으나 지금까지도 Welch의 결과는 알려져 있지 않다. 이러한 이유로 본 논문에서는 Niho의 방법과는 다른 방법을 이용하여 이 d가 4개의 상호상관관계 함숫값을 갖는다는 것을 밝히고 또한 이 d에 의한 상호상관관계 함숫값들의 발생 횟수도 밝힌다.

PUKYONG NATIONAL UNIVERSITY 부경대학교

Ⅱ. 예비지식

이 절에서는 3절과 4절의 이해에 필요한 내용을 소개한다.

2.1 m-수열의 성질

<정의 2.1.1> [16] n차 m-수열은 0-수열이 아니면서 n차 순환을 만족하는 n차 최대주기수열이다. m-수열의 특성다항식은 $GF(2)$위에서 원시다항식이다. 의사난수열 이라고도 한다.

m-수열은 다음과 같은 성질들을 가진다.

(a) The shift property : m-수열의 순환이동(cyclic shift)은 역시 m-수열이다.

(b) The recurrence property : m-수열 $\{a_n\}$은 다음의 선형점화관계식을 만족한다.

$$a_{n+i} = c_{n-1}a_{i+n-1} + c_{n-2}a_{i+n-2} + \cdots + c_1 a_{i+1} + a_i \pmod 2$$

(c) The window property : 차수가 n인 원시다항식에 의해서 생성된 m-수열에서 m-비트씩 읽으면 $1, 2, \cdots, 2^m - 1$이 모두 다 한 번씩만 나온다.

(d) The balance property : m-수열에서는 1의 개수가 0의 개수보다 하나 더 많다.

(e) The addition property : 두 개의 m-수열의 XOR은 여전히 m-수열이다.

(f) The shift and add property : m-수열과 그것의 순환이동의 합은 또 다른 m-수열이다. 즉, 수열 $\{S_t\}$를 길이가 2^n-1인 m-수열이라 하고 τ를 $\tau \not\equiv 0 \pmod{2^n-1}$라면, $\sigma(1 \le \sigma \le 2^n-2)$가 존재하여 다음 식을 만족한다.

$$s_t + s_{t+\tau} \equiv s_{t+\tau}\,(t \ge 0)$$

(g) The thumb and tack property : 자기상관함수(autocorrelation function)의 값은 1 또는 $-\frac{1}{N}$ (단, $N=2^n-1$)이다.

$$\rho(i) = \frac{1}{N}\sum_{j=0}^{N-1}(-1)^{c_j \oplus c_{i+j}}$$

(h) 0-run과 1-run

x^5+x^2+1에 의해서 생성된 m-수열

0001001011001111100011011101 01…

에서 0이 연이어 4개인 run을 길이가 4인 0-run이라 하며 중간에 11111과 같이 1이 연이어 5개인 run을 길이가 5인 1-run이라 한다. 그러므로 길이가 1인 o-run은 4개이며 길이가 2인 0-run은 2개이며 길이가 3인 0-run은 1개이며 길이가 4인 0-run은 1개가 있다. 또한 길이가 1인 1-run은 4개이며 길이가 2인 1-run은 2개이며 길이가 3인 1-run은 1개이며 길이가 4인

1-run은 없으며 길이가 5인 1-run은 1개이다.

(i) Characteristic phase : m-수열 $s=(s_i)$에 대하여 $(s_{2i})=s$인 m-수열은 단 하나 존재한다. 그러한 m-수열을 characteristic m-수열이라 한다.

(j) Decimation : 생성다항식이 $f(x)$인 m-수열 s에서 d칸씩 건너 뛰어 만든 수열을 $s[d]$라 쓰기로 한다. $s[d]=(0000000\cdots)$이 아닌 $s[d]$의 주기는 $\frac{2^n-1}{\gcd(2^n-1,d)}$이며 $s[d]$의 생성다항식은 $f(x^d)$이다.

(k) 주기가 2^{n-1}인 서로 다른 m-수열의 개수는 $\frac{\phi(2^n-1)}{n}$이다. 여기서 ϕ는 Euler 함수이다.

<정리 2.1.2> [12] 길이가 2^n-1인 m-수열의 run 분포는 다음과 같다.

[표 II-0] 길이가 2^n-1인 m-수열의 run 분포

길이	0-runs	1-runs
1	2^{n-3}	2^{n-3}
2	2^{n-4}	2^{n-4}
⋮	⋮	⋮
r	2^{n-r-2}	2^{n-r-2}
⋮	⋮	⋮
$n-2$	1	1
$n-1$	1	0
n	0	1
합계	2^{n-2}	2^{n-2}

2.2 트레이스 함수

<정의 2.2.1> $\alpha \in GF(2^n)$에 대하여 다음을 만족하는 함수 $Tr_k^n : GF(2^n) \rightarrow GF(2^k)$를 트레이스 함수(trace function)라 한다.

$$Tr_k^n(\alpha) = \alpha + \alpha^{2^k} + \alpha^{2^{2k}} + \cdots + \alpha^{2^{k(\frac{n}{k}-1)}}$$

<정리 2.2.1> [17] $GF(2^n)$에서 부분체 $GF(2^k)$ $(n = mk)$으로의 트레이스 함수 $Tr_k^n : GF(2^n) \rightarrow GF(2^k)$에 대하여 다음의 성질들이 만족된다.

(a) 모든 $\alpha \in GF(2^n)$에 대하여 $Tr_k^n(\alpha^{2^a}) = Tr_k^n(\alpha)$이다.

(b) Tr_k^n은 선형적이다.

(c) Tr_k^n은 전사함수이다.

(d) 모든 $a \in GF(2^k)$에 대하여 $Tr_k^n(a) = ma$이다.

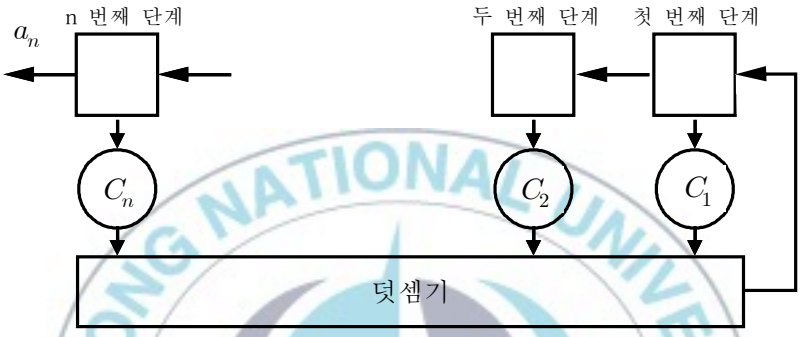
2.3 선형점화수열(linear recurring sequences)

<정의 2.3.1> 선형점화수열 $a_0, a_1, a_2, \cdots$ 은

$$a_{n+i} = \sum_{j=1}^{n} c_j a_{n+i-j} \qquad (i = 0, 1, 2, \cdots) \qquad (2.3.1)$$

의 선형점화관계를 만족하는 수열이다. 여기서 $a_i, c_j \in GF(2)$이고 $a_0, a_1, \cdots, a_{n-1}$은 이미 주어져 있다. 이러한 수열 $\{a_i\}$는 n 단계 쉬프트 레지스터와 덧셈기에 의해 생성될 수 있다.

[그림 Ⅱ-1] n 단계 쉬프트 레지스터와 덧셈기



상수 $c_1, c_2, \cdots, c_n$은 피드백 계수로서 c_i가 i번째 단계에서 연결이 되어있으면 1이고 연결이 되어있지 않으면 0이 된다. 식 (2.4.1)의 선형점화수열 a_i는 n번째 단계의 출력으로 생각할 수 있다.

선형점화수열 a_i는 점화식의 특성다항식

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$$

으로 정의되고 특성다항식 $f(x)$는 기약다항식이며 이 다항식은 유일하지 않다.

<정의 2.3.2> 선형점화수열 $\{a_i\}$의 주기(period)는 모든 i 에 대하여 $a_{i+p} = a_i$를 만족하는 가장 작은 양의 정수이다. 점화다항식 $f(x)$에서 주기

p는 $f(x)$를 (x^p+1)로 나누는 가장 작은 양의 정수이고 주기 $p=2^n-1$ 일 때, 다항식 $f(x)$를 기약다항식이라 한다. $f(x)$가 기약다항식이므로 선형점화수열 $\{a_i\}$의 주기 p는 2^n-1의 약수이다. $p=2^n-1$일 때 선형점화수열 $\{a_i\}$를 최대 선형점화수열 또는 최대길이 선형 쉬프트 레지스터 수열(linear shift register sequence, LFSR)이라 한다.

<정리 2.3.3> [17] u_t를 주기 2^n-1의 m-수열이라 하면 임의의 원시원소 $\gamma \in GF(2^n)$에 대하여 $u_t = Tr_1^n(y\gamma^t)$를 만족하는 $y \in GF(2^n)^*$가 존재한다. 역으로 $\gamma \in GF(2^n)$가 원시원소이고 $y \in GF(2^n)^*$이면 $u_t = Tr_1^n(y\gamma^t)$에 의한 수열은 m-수열이다.

<보조정리 2.3.4> [17] 주기가 2^n-1인 두 개의 m-수열 v_t, u_t에서

(a) $\gcd(d, 2^n-1)=1$이면 u_{dt} (d는 정수)는 m-수열이다.

(b) 모든 $t=0,1,\cdots$에 대하여 $v_{t+k}=u_{dt}$와 $\gcd(d, 2^n-1)=1$을 만족하는 정수 d, k가 존재한다.

<정의 2.3.5> [16] 모든 $t=0,1,\cdots$ 에 대하여 $v_{t+k}=u_t$를 만족하는 정수 k가 존재할 때 수열 v_t는 수열 u_t의 순환이동이라 한다

본 논문에서는 수열과 그것의 순환이동에 차이가 없는 것으로 간주한다.

<정의 2.3.6> [16] $\gcd(d, 2^n-1)=1$을 만족하는 정수 d를 데시메이션(decimation)이라 한다.

Ⅲ. 방정식 $(x+1)^d = x^d + 1$의 해의 개수

이 절에서는 방정식 $(x+1)^d = x^d + 1$의 해의 개수를 구하는 방법에 대하여 생각하기로 한다.

<보조정리 3.1> $q = 2^k$라 하고, $d \equiv 1 \pmod{q-1}$라 하자. 그러면 $x \in GF(q^2) \setminus \{0,1\}$이 방정식

$$(x+1)^d = x^d + 1 \tag{3.1.1}$$

의 해가 될 필요충분조건은 $x^{d-1} = (x+1)^{d-1} = 1$이거나 $x^{d-q} = (x+1)^{d-q} = 1$이다.

<증명> $(x+1)^d = x^d + 1$이기 때문에

$$\begin{aligned} (\bar{x}+1)^d &= (x^q+1)^d \\ &= (x+1)^{qd} \\ &= \{(x+1)^d\}^q \\ &= (x^d+1)^q = \overline{x^d}+1 \end{aligned} \tag{3.1.2}$$

이 성립한다. 그러므로

$$(x\bar{x}+x+\bar{x}+1)^d = (x\bar{x})^d + x^d + \bar{x}^d + 1 \tag{3.1.3}$$

이다. $x\bar{x} \in GF(q)$, $x+\bar{x} \in GF(q)$이고 $x\bar{x}+x+\bar{x}+1 \in GF(q)$이므로 $(x\bar{x}+x+\bar{x}+1)^d = x\bar{x}+x+\bar{x}+1$이고 $(x\bar{x})^d = x\bar{x}$이다. 따라서

$$x\bar{x}+x+\bar{x}+1 = x\bar{x}+x^d+\bar{x}^d+1 \tag{3.1.4}$$

이 성립한다. 즉,

$$x+\bar{x} = x^d+\bar{x}^d \tag{3.1.5}$$

이다. 식 (3.1.5)의 양변에 x^{d-q-1}을 곱하면

$$x^{d-q}+x^{d-1} = x^{2d-q-1}+x^{qd+d-q-1} \tag{3.1.6}$$

$d \equiv 1 \pmod{q-1}$이기 때문에 $d-1=(q-1)s$를 만족하는 $s \in \mathbb{N}$가 존재하므로

$$x^{qd+d-q-1} = x^{(q+1)(d-1)} = x^{(q+1)(q-1)s} = 1 \tag{3.1.7}$$

이 성립하고

$$x^{2d-q-1}-x^{d-q}-x^{d-1}+1 = (x^{d-1}-1)(x^{d-q}-1) = 0 \tag{3.1.8}$$

이다. 따라서 $x^d = x$ 또는 $x^d = x^q = \bar{x}$이다.

(i) $x^d = x$ 일 때 $(x+1)^d = x^d + 1 = x+1$이므로 $(x+1)^{d-1} = 1$이다.

(ii) $x^d = \bar{x}$ 일 때 $(x+1)^d = \bar{x}+1 = (x+1)^q$이므로 $(x+1)^{d-q} = 1$이다.

역으로, $x^{d-1} = (x+1)^{d-1} = 1$이라 하자. 그러면 $(x+1)^d = x+1$과 $x^d = x$가 만족되고 따라서 $(x+1)^d = x+1 = x^d+1$이 성립한다. 그러므로 x는 식 (3.1.1)의 해가 된다.

그리고 $x^{d-q} = (x+1)^{d-q} = 1$이라 하면 $(x+1)^d = (x+1)^q = x^q+1 = x^d+1$이 성립하므로 x는 식 (3.1.1)의 해가 된다.

<따름정리 3.2> $q = 2^k$이고 $d \equiv 1 \pmod{q-1}$이라 하자. 그리고 $x \in GF(q^2) \setminus \{0,1\}$ 가 방정식

$$(x+1)^d = x^d + 1 \tag{3.2.1}$$

의 해이면 $\left(\frac{x+1}{\bar{x}+1}\right)^{d-1} = 1$ 또는 $\left(\frac{x+1}{\bar{x}+1}\right)^{d+1} = 1$이다.

<증명> 보조정리 3.1에 의해 $x^d = x$ 또는 $x^d = \bar{x}$이다. 또한 식 (3.1.5)로부터 $x + \bar{x} = x^d + \overline{x^d}$가 된다.

(i) $x^d = x$일 때 식 (3.1.5)에 따라 $\bar{x}^d = \bar{x}$이기 때문에

$$\left(\frac{x+1}{\bar{x}+1}\right)^d = \frac{x^d+1}{\bar{x}^d+1} = \frac{x+1}{\bar{x}+1}$$

이고, 따라서 $\left(\frac{x+1}{\bar{x}+1}\right)^{d-1} = 1$이다.

(ii) $x^d = \bar{x}$일 때 식 (3.1.5)에 따라 $\bar{x}^d = x$이기 때문에

$$\left(\frac{x+1}{\bar{x}+1}\right)^d = \frac{x^d+1}{\bar{x}^d+1} = \frac{\bar{x}+1}{x+1}$$

이고, 따라서 $\left(\frac{x+1}{\bar{x}+1}\right)^{d+1} = 1$이다.

<보조정리 3.3> $d=(q-1)s+1$이고 $e=(q-1)t+1$이라 하자.

$$\begin{cases}\gcd(s,q+1)=\gcd(t,q+1)\\ \gcd(s-1,q+1)=\gcd(t-1,q+1)\end{cases} \tag{3.3.1}$$

이 성립한다고 가정하면 $x\in GF(q^2)$가 식 (3.1.1)의 해가 될 필요충분조건은 x가

$$(x+1)^e = x^e+1 \tag{3.3.2}$$

의 해 일 때다.

<증명> 모든 x는 식 (3.1.1)의 해이므로, $x \in GF(q^2) \setminus \{0,1\}$라 가정해도 무방하다. x를 식 (3.1.1)의 해라 하면 보조정리 3.1에 따라 $x^{d-1} = (x+1)^{d-1} = 1$ 또는 $x^{d-q} = (x+1)^{d-q} = 1$이 성립한다. $x^d = x$,이기 때문에 $x^d = x^{(q-1)s} \cdot x = x$이고 따라서 $x^{(q-1)s} = 1$이 성립한다.

$x^{q^2-1} = 1$이고

$$1 = x^{\gcd((q-1)s, q^2-1)} = \left(x^{(q-1)}\right)^{\gcd(s, q+1)} \tag{3.3.3}$$
$$= \left(x^{(q-1)}\right)^{\gcd(t, q+1)}$$
$$= x^{\gcd((q-1)t, q^2-1)}$$

이므로 $x^{(q-1)t} = 1$이다. 그러므로 $x^e = x^{(q-1)t+1} = x^{(q-1)t} \cdot x = x$이다. $x^d = \bar{x}$라 가정하면

$$1 = x^{d-q} = x^{(q-1)(s-1)} \tag{3.3.4}$$

이다.

$x^{q^2-1} = 1$이고 $x^{\gcd((q-1)s, q^2-1)} = x^{\gcd((q-1)t, q^2-1)}$이므로 $x^{e-q} = x^{(q-1)(t-1)} = 1$이다. 그러므로 $x^e = \bar{x}$이다. 마찬가지로 $(x+1)^e = x+1$ 과 $(x+1)^e = (x+1)^q$을 증명할 수 있다. 그러므로 $x^{e-1} = (x+1)^{e-1} = 1$이고 $x^{e-q} = (x+1)^{e-q} = 1$이다. 따라서 보조정리 3.1에 의해 x는 식 (3.3.2)의 해이다. d에 대한 역증명은 e에 대한 증명과 같다.

<보조정리 3.4> [17] $\mathbb{E} = GF(2^n)$이고 $k|n$, $\mathbb{F} = GF(2^k)$일 때 $\beta \in \mathbb{E}$라 하자.

$$\beta \in \mathbb{F} \quad \Leftrightarrow \quad \beta^{2^k} = \beta \tag{3.4.1}$$

이다.

<정리 3.5> $d \equiv 1 \pmod{2^k - 1}$이라 가정하자. 만약 $\gcd(d \pm 1, 2^k + 1) = 1$이면,

$$(x+1)^d = x^d + 1 \tag{3.5.1}$$

은 $GF(2^n)$안에서 정확하게 2^k개의 해를 갖는다.

<증명> $d \equiv 1 \pmod{2^k - 1}$이므로, 모든 $x \in GF(2^k)$는 식 (3.5.1)의 해이다. 그래서 식 (3.5.1)을 만족하는 $x \neq 0, 1$이라 가정해도 무방하다. x가 식 (3.5.1)의 해이므로, 보조정리 3.1에 의해 $x^d = x$ 또는 $x^d = \bar{x}$가 성립한다. $x^d = x$라 하면 따름정리 3.2에 의해 $\left(\frac{x+1}{\bar{x}+1}\right)^{d-1} = 1$이다. 그리고 $x^d = \bar{x}$이면 따름정리 3.2에 의해 $\left(\frac{x+1}{\bar{x}+1}\right)^{d+1} = 1$이다. $\gcd(d \pm 1, 2^k + 1) = 1$,

$$\frac{x+1}{\bar{x}+1} = 1 \tag{3.5.2}$$

이기 때문에 보조정리 3.4에 따라 $\bar{x} = x$이고 $x \in GF(2^k)$이 성립한다.

다음 정리는 잘 알려진 정리이다.

<정리 3.6> $n = 2k$, $q = 2^k$라 하고, $x \in GF(q^2)$에 대하여 $\bar{x} = x^q$라 정의하자.

그러면 다음이 성립한다.

(a) $\overline{x+y} = \bar{x}+\bar{y} \quad (x, y \in GF(q^2))$

(b) $\overline{xy} = \bar{x}\bar{y} \quad (x, y \in GF(q^2))$

(c) $x+\bar{x} \in GF(q) \quad (x, y \in GF(q^2))$

(d) $x\bar{x} \in GF(q) \quad (x, y \in GF(q^2))$

$$S = \{x \in GF(q^2) \mid x\bar{x} = x^{q+1} = 1\}$$

라 정의하자. 그러면 S는 원소의 개수가 $q+1$개인 군이다.

<보조정리 3.7> $x \in GF(q^2) \setminus GF(q)$라 하면 다음이 성립한다.

$$S \setminus \{1\} = \left\{ \frac{x+v}{\bar{x}+v} \mid v \in GF(q) \right\}$$

<증명> 어떤 $u, v \in GF(q)$에 대하여 $\frac{x+u}{\bar{x}+u} = \frac{x+v}{\bar{x}+v}$라 가정하자. 그러면

$$(x+u)(\bar{x}+v) = (x+v)(\bar{x}+u)$$

$$x\bar{x}+u\bar{x}+vx+uv = x\bar{x} + v\bar{x}+ux + uv$$

$$u\bar{x}+vx = v\bar{x}+ux$$

$$u\bar{x}+vx-v\bar{x}-ux = (x-\bar{x})(v-u) = 0$$

이다. 따라서 $x=\overline{x}$ 이거나 $u=v$이다. 그런데 가정에 의해 $x\neq\overline{x}$ 이므로 $u=v$이고, $u,v\in GF(q)$가 서로 다르면 $\frac{x+u}{\overline{x}+u}\neq\frac{x+v}{\overline{x}+v}$이다. 그러므로

$$\left|\left\{\frac{x+v}{\overline{x}+v}\mid v\in GF(q)\right\}\right|=q$$

이다. 그런데 $|S\setminus\{1\}|=q$이고

$$\left(\frac{x+v}{\overline{x}+v}\right)\overline{\left(\frac{x+v}{\overline{x}+v}\right)}=\left(\frac{x+v}{\overline{x}+v}\right)\left(\frac{\overline{x}+\overline{v}}{\overline{\overline{x}}+\overline{v}}\right)$$

$$=\left(\frac{x+v}{\overline{x}+v}\right)\left(\frac{\overline{x}+\overline{v}}{x+\overline{v}}\right)$$

$$=\left(\frac{x+v}{\overline{x}+v}\right)\left(\frac{\overline{x}+v}{x+v}\right)=1$$

이다. 그러므로 $\frac{x+v}{\overline{x}+v}\in S$이다.

<보조정리 3.8> $\beta\in S\setminus\{1\}$라 하면 다음이 성립한다.

$$S\setminus\{\beta\}=\left\{\frac{\alpha\beta+1}{\alpha+\beta}\mid\alpha\in GF(q)\right\}$$

<증명> 어떤 $\alpha,\alpha'\in GF(q)$에 대하여 $\frac{\alpha\beta+1}{\alpha+\beta}=\frac{\alpha'\beta+1}{\alpha'+\beta}$라 가정하자.

그러면

$$(\alpha+\beta)(\alpha'\beta+1)=(\alpha\beta+1)(\alpha'+\beta)$$

$$\alpha\alpha'\beta+\alpha+\alpha'\beta^2+\beta=\alpha\alpha'\beta+\alpha'+\alpha\beta^2+\beta$$

$$\alpha+\alpha'\beta^2=\alpha'+\alpha\beta^2$$

$$\alpha'\beta^2-\alpha\beta^2+\alpha-\alpha'=\alpha'\beta^2+\alpha\beta^2+\alpha+\alpha'$$

$$(\alpha'+\alpha)(\beta^2+1)=(\alpha'+\alpha)(\beta+1)=0$$

이다. 따라서 $\alpha'=\alpha$ 또는 $\beta=1$이다. 그런데 가정에 의해 $\beta\neq1$이므로 $\alpha'=\alpha$이다. 즉, $\alpha'\neq\alpha$이면 $\frac{\alpha\beta+1}{\alpha+\beta}\neq\frac{\alpha'\beta+1}{\alpha'+\beta}$이다. 그러므로

$$\left|\left\{\frac{\alpha\beta+1}{\alpha+\beta}\mid\alpha\in GF(q)\right\}\right|=q$$

이다. 그리고 $\frac{\alpha\beta+1}{\alpha+\beta}=\beta$이면

$$\alpha\beta+1=\beta(\alpha+\beta)$$

$$\alpha\beta+1=\alpha\beta+\beta^2$$

$$\beta^2=1$$

이고 가정에 의해 $\beta\neq1$이므로 $\frac{\alpha\beta+1}{\alpha+\beta}\neq\beta$이다. 또한

$$\left(\frac{\alpha\beta+1}{\alpha+\beta}\right)\overline{\left(\frac{\alpha\beta+1}{\alpha+\beta}\right)}=\left(\frac{\alpha\beta+1}{\alpha+\beta}\right)\left(\frac{\overline{\alpha}\overline{\beta}+1}{\overline{\alpha}+\overline{\beta}}\right)$$

$$=\left(\frac{\alpha\beta+1}{\alpha+\beta}\right)\left(\frac{\alpha\overline{\beta}+1}{\alpha+\overline{\beta}}\right)$$

$$=\frac{\alpha^2+\alpha(\beta+\overline{\beta})+1}{\alpha^2+\alpha(\beta+\overline{\beta})+\beta\overline{\beta}}=1$$

이고 $|S\setminus\{\beta\}|=q$이므로 $S\setminus\{\beta\}=\left\{\frac{\alpha\beta+1}{\alpha+\beta}\,|\,\alpha\in GF(q)\right\}$이다.

<보조정리 3.9> $q=2^k$라 가정하면 모든 $x\in GF(q^2)^*$는

$$x=\alpha\beta$$

로 표현할 수 있다. 여기서 $\alpha\in GF(q)^*$이고 $\beta\in S$이다.

<증명> $\gamma\in GF(q^2)$를 $GF(q^2)$의 원시원소라 하자. 그러면 $t(1\le t\le q^2-1)$가 존재하여 $x=r^t$이다.

$t=t_1Q+t_2$라 하자. 여기서 Q는 $q+1$이고, $0\le t_1\le q-2, 0\le t_2\le q$이다. 그러면

$$x=r^t=r^{t_1Q+t_2}=(r^Q)^{t_1}r^{t_2}$$

이다. $(\gamma^Q)^{t_1}=\alpha$라 하자. 그러면

$$((\gamma^Q)^{t_1})^q = (\gamma^{(q+1)q})^{t_1}$$
$$= (\gamma^{q^2-1+q+1})^{t_1}$$
$$= \gamma^{(q^2-1)t_1}\gamma^{(q+1)t_1}$$
$$= \gamma^{Qt_1}$$

이므로 $\alpha \in GF(q)^*$이다.

$\beta' = \gamma^{t_2} \in \{1, \gamma, \gamma^2, \cdots, \gamma^q\}$이고 $\beta = \beta'^{q-1}$라 하면

$$\beta\bar{\beta} = \beta^{q+1} = ((\gamma^{q-1})^{t_2})^{q+1}$$
$$= (\gamma^{q^2-1})^{t_2} = 1$$

이다. 따라서 $\beta \in S$이다.

<정리 3.10> 주어진 $d\,(0 \le d \le 2^n - 2)$에 대하여 다음이 성립한다.

(a) $\sum_{\tau=0}^{2^n-2} (C_d(\tau)+1) = 2^n$

(b) $\sum_{\tau=0}^{2^n-2} (C_d(\tau)+1)^2 = 2^{2n}$

(c) $\sum_{\tau=0}^{2^n-2} (C_d(\tau)+1)^3 = 2^{2n}c,\ c = \left|\{x \in GF(2^n) | (x+1)^d = x^d + 1\}\right|$이다.

<증명> (a) $GF(2^n)$의 원시원소 α에 대하여 $u(t) = Tr_1^n(\alpha^t)$, $v(t) = u(dt)$라

하고 $C_d(\tau)$의 값을 계산하면

$$C_d(\tau) = \sum_{t=0}^{2^n-2} (-1)^{u(t+\tau)+v(t)}$$

$$= \sum_{t=0}^{2^n-2} (-1)^{u(t+\tau)+u(dt)}$$

$$= \sum_{t=0}^{2^n-2} (-1)^{Tr_1^n(\alpha^{t+\tau})+Tr_1^n(\alpha^{dt})}$$

$$= \sum_{t=0}^{2^n-2} (-1)^{Tr_1^n(\alpha^{\tau}\alpha^{t})+Tr_1^n(\alpha^{dt})}$$

여기서 $x=\alpha^t$, $y=\alpha^\tau$로 두면 $0 \le t \le 2^n-2$이므로 $\alpha^t \neq 0$, 즉 $x \in GF(2^n)^*$이다. 따라서

$$C_d(\tau) = \sum_{x \in GF(2^n)^*} (-1)^{Tr_1^n(yx)+Tr_1^n(x^d)}$$

이고

PUKYONG NATIONAL UNIVERSITY 부경대학교

$$C_d(\tau)+1 = \sum_{x\in GF(2^n)^*} (-1)^{Tr_1^n(yx)+Tr_1^n(x^d)} + 1$$

$$= \sum_{x\in GF(2^n)^*} (-1)^{Tr_1^n(yx)+Tr_1^n(x^d)} + (-1)^{Tr_1^n(0)}$$

$$= \sum_{x\in GF(2^n)} (-1)^{Tr_1^n(yx)+Tr_1^n(x^d)}$$

$$= \sum_{x\in GF(2^n)} \sum_{y\in GF(2^n)} (-1)^{Tr_1^n(yx)+Tr_1^n(x^d)}$$

$$= \sum_{x\in GF(2^n)} (-1)^{Tr_1^n(x^d)} \sum_{y\in GF(2^n)} (-1)^{Tr_1^n(yx)}$$

여기서 $\sum_{y\in GF(2^n)} (-1)^{Tr_1^n(yx)} = \begin{cases} 0, & x\neq 0 \\ 2^n, & x=0 \end{cases}$ 이므로 $C_d(\tau)+1 = 2^n$이다.

(b) $\sum_{\tau=0}^{2^n-2} \left(C_d(\tau)+1\right)^2 = \sum_{x\in GF(2^n)} \left\{(-1)^{Tr_1^n(yx+x^d)}\right\}^2$

$$= \sum_{y\in GF(2^n)} \sum_{x\in GF(2^n)} (-1)^{Tr_1^n(yx+x^d)} \sum_{z\in GF(2^n)} (-1)^{Tr_1^n(yz+z^d)}$$

$$= \sum_{x,\,z\in GF(2^n)} (-1)^{Tr_1^n(x^d+z^d)} \sum_{y\in GF(2^n)} (-1)^{Tr_1^n\{y(x+z)\}}$$

(a)의 증명에서와 마찬가지로 $\sum_{y\in GF(2^n)} (-1)^{Tr_1^n\{y(x+z)\}} = \begin{cases} 0, & x\neq z \\ 2^n, & x=z \end{cases}$ 이므로

$$\sum_{\tau=0}^{2^n-2}\left(C_d(\tau)+1\right)^2 = \sum_{x,\,z\in GF(2^n)}(-1)^{Tr_1^n(x^d+z^d)}\sum_{y\in GF(2^n)}(-1)^{Tr_1^n\{y(x+z)\}}$$

$$= 2^n\left(\sum_{\substack{x,\,z\in GF(2^n)\\ x=z}}(-1)^{Tr_1^n(x^d+z^d)}\right)$$

$$= 2^n\left(\sum_{\substack{x,\,z\in GF(2^n)\\ x=z}}(-1)^{Tr_1^n(0)}\right)$$

$$= 2^n\left(\sum_{\substack{x,\,z\in GF(2^n)\\ x=z}}1\right)$$

$$= 2^{2n}$$

이다. 따라서 $\sum_{\tau=0}^{2^n-2}\left(C_d(\tau)+1\right)^2 = 2^{2n}$이다.

(c) $\sum_{\tau=0}^{2^n-2}\left(C_d(\tau)+1\right)^3 = 2^{2n}c,\ \ c=\left|\{x\in GF(q)\mid (x+1)^d = x^d+1\}\right|$

$$\sum_{\tau=0}^{2^n-2}\left(C_d(\tau)+1\right)^3 = \sum_{w,\,x,\,z\in GF(2^n)}(-1)^{Tr_1^n(w^d+x^d+z^d)}\sum_{y\in GF(2^n)}(-1)^{Tr_1^n\{y(w+x+z)\}}$$

이고

$$\sum_{y\in GF(2^n)}(-1)^{Tr_1^n\{y(w+x+z)\}} = \begin{cases}1\,, & w+x+z=0\text{인 경우}\\ 0\,, & \text{그 밖의 경우}\end{cases}$$

이므로

$$\sum_{\tau=0}^{2^n-2}\left(C_d(\tau)+1\right)^3 = 2^n\left(\sum_{x,\,z\in GF(2^n)}\sum_{w=x+z}(-1)^{Tr_1^n(w^d+x^d+z^d)}\right)$$

$$= 2^n\left(\sum_{x,\,z\in GF(2^n)}\sum_{w=x+z}(-1)^{Tr_1^n((x+z)^d+x^d+z^d)}\right)$$

이다. 그런데 $z\in GF(2^n)$이므로 $GF(2^n)$의 어떤 원소 β를 이용하여 $z=\beta x$로 나타낼 수 있다. 따라서

$$\sum_{\tau=0}^{2^n-2}\left(C_d(\tau)+1\right)^3 = 2^n\left(\sum_{x\in GF(2^n)}\sum_{\beta\in GF(2^n)}(-1)^{Tr_1^n\{(x+\beta x)^d+x^d+(\beta x)^d\}}\right)$$

$$= 2^n\left(\sum_{x\in GF(2^n)}\sum_{\beta\in GF(2^n)}(-1)^{Tr_1^n\{x^d(1+\beta^d+(1+\beta)^d)\}}\right)$$

이다. 여기서 (a), (b)에서와 같이

$$\sum_{\beta\in GF(2^n)}(-1)^{Tr_1^n(x^d(1+\beta^d+(1+\beta)^d))} = \begin{cases}1\,, & 1+\beta^d+(1+\beta)^d=0\text{인 경우}\\ 0\,, & \text{그 밖의 경우}\end{cases}$$

이므로 $\sum_{\tau=0}^{2^n-2}\left(C_d(\tau)+1\right)^3 = 2^{2n}c,\ c=\left|\{x\in GF(2^n)\mid (x+1)^d=x^d+1\}\right|$이다.

IV. 4개의 상호상관관계 함숫값을 갖는 함수

이 절에서는 4개의 상호상관관계 함숫값을 갖는 함수에 대하여 생각한다.

보조정리 3.7과 3.8에 의해 다음의 정리가 주어진다.

<정리 4.1> [16] $n=2m$이고 $y\in GF(2^n)^*$라 하자. 다음 방정식

$$x^{2^s+1}+yx^{2^s}+\bar{y}x+1=0 \tag{4.1.1}$$

의 해는 0, 1, 2 또는 $2^{\gcd(s,m)}+1$ $(x\in S)$이다.

보조정리 3.9에 의해 다음의 정리가 주어진다.

<정리 4.2> [15] $n=2m$이고 $d\equiv 1(\mathrm{mod}\ 2^m-1)$, $C_d(\tau)+1=\Delta_d(\tau)$이면

$$\Delta_d(\tau)=2^m(N(y)-1) \tag{4.2.1}$$

이다. 여기서 $N(y)$는

$$x^d+yx+y^{2^m}x^{-1}+x^{-d}=0$$

과 $y \in GF(2^n)^*$를 만족하는 $x \in \{x \in GF(2^n) | x^{2^m+1} = 1\}$의 개수이다.

<보조정리 4.3> m이 정수이고 $n = 4m$일 때

$$d = 2^{m-1}\{(2^m - 1)(2^{2m} + 1) + 2\}$$

이면

(a) $d \equiv 1 \pmod{2^{2m} - 1}$,

(b) $d \equiv 2^m \pmod{2^{2m} + 1}$,

(c) $\gcd(d, 2^n - 1) = 1$

<증명> (a)

$$\begin{aligned} d &= 2^{m-1}\{(2^m - 1)(2^{2m} - 1) + 2(2^m - 1) + 2\} \\ &\equiv 2^{m-1} \cdot 2^{m+1} \pmod{2^m - 1} \\ &\equiv 2^{2m} \pmod{2^m - 1} \\ &\equiv 1 \pmod{2^m - 1} \end{aligned}$$

이므로 $d \equiv 1 \pmod{2^{2m} - 1}$이다.

(b) 명백히 $d \equiv 2^m \pmod{2^{2m} + 1}$이다.

(c) d가 짝수이므로 $\gcd(d, 2^n - 1) = 1$이다.

<정리 4.4> m이 정수이고 $n=4m$일 때 $d=2^{m-1}\{(2^m-1)(2^{2m}+1)+2\}$라 하면

$$(x+1)^d = x^d+1 \tag{4.4.1}$$

은 $GF(2^n)$ 안에서 정확하게 2^{2m}개의 해를 갖는다.

<증명> $d\equiv 1 \pmod{2^{2m}-1}$이므로 모든 $x\in GF(2^{2m})$는 식 (4.4.1)의 해이다. $x(\neq 0,1)$가 식 (4.4.1)의 해라 가정하면 $d-1\equiv 2^m-1 \pmod{2^{2m}+1}$이므로 $\gcd(d-1, 2^{2m}+1)=1$이다. 또한 $d+1\equiv 2^m+1 \pmod{2^{2m}+1}$이므로 $\gcd(d+1, 2^{2m}+1)=\gcd(2^{2m}+1, 2^m)=1$ 이다.

$$\frac{x+1}{\bar{x}+1}\in S$$

이기 때문에 따름정리 3.2에 따라

$$\frac{x+1}{\bar{x}+1}=1$$

이다. 그래서 $\bar{x}=x^{2^{2m}}$, 즉 $x\in GF(2^{2m})$이다.

<정리 4.5> m이 정수이고 $n=4m$일 때 $d=2^{m-1}\{(2^m-1)(2^{2m}+1)+2\}$라 하면 상호상관관계 함수 $C_d(\tau)$의 4개의 상호상관관계 함숫값과 발생 횟수

는 다음과 같다.

[표 IV-1] 4개의 상호상관관계 함숫값과 발생 횟수

상호상관관계 함숫값	발생 횟수
$-1-2^{2m}$	$2^{4m-1}-2^{3m-1}$
-1	$2^{3m}-2^{m}-1$
$-1+2^{2m}$	$2^{4m-1}-2^{3m-1}$
$-1-2^{3m}$	2^{m}

<증명> 보조정리 4.3에 의해 $d \equiv 1 \pmod{2^{2m}-1}$, $d \equiv 2^m \pmod{2^{2m}+1}$, $\gcd(d, 2^n-1)=1$이다. 따라서 정리 4.2에 의해 아래의 식을 얻을 수 있다.

$$yx + x^{2^m} + \bar{y}x^{-1} + x^{-2^m} = 0 \tag{4.5.1}$$

$\gcd(2^m-1, 2^{2m}+1)=1$이므로 식 (4.5.1)의 x를 x^{2^m-1}로 바꿀 수 있다.

$$yx^{2^m-1} + (x^{2^m-1})^{2^m} + \bar{y}x^{-(2^m-1)} + (x^{-(2^m-1)})^{2^m} = 0 \tag{4.5.2}$$

식 (4.5.2)는 다음과 같고

$$x^{2(2^{2m}-2^m)} + yx^{2^m-1} + \bar{y}x^{2^{2m}-2^{m+1}+1} + 1 = 0 \tag{4.5.3}$$

$x^{2^{2m}} = x^{-1}$이므로 식 (4.5.3)은 다음과 같이 된다.

$$x^{2(-1-2^m)} + yx^{-2} + \bar{y}x^{-2^{m+1}} + 1 = 0 \tag{4.5.4}$$

$$(x^{-1-2^m} + y^{1/2}x^{-1} + \bar{y}^{1/2}x^{-2^m} + 1)^2 = 0 \tag{4.5.5}$$

이기 때문에 식 (4.5.5)의 해의 개수는 식 (4.5.6)의 해의 개수와 같다.

$$x^{-1-2^m} + yx^{-1} + \bar{y}x^{-2^m} + 1 = 0 \tag{4.5.6}$$

따라서 식 (4.5.6)의 해의 개수는 다음의 식 (4.5.7)의 해의 개수와 같다.

$$x^{2^m+1} + yx^{2m} + \bar{y}x + 1 = 0 \tag{4.5.7}$$

따라서 정리 4.1에 의해 $C_d(\tau)$는 4개의 값을 갖는다. 정리 3.10과 정리 4.4에 의해

$$\sum_{\tau=0}^{2^n-2} (\Delta_d(\tau))^3 = 2^{2n}2^{2m}$$

이다. N_i로 나타내는 식 (4.5.7)의 반복 횟수는 S에서 정확히 i개의 해를 가지고 다음과 같다.

$$
\begin{aligned}
N_0 + N_1 + N_2 + N_{2^m+1} &= 2^n - 1,\\
-2^{2m}N_0 + 0\cdot N_1 + 2^{2m}N_2 + 2^{3m}N_{2^m+1} &= 2^n,\\
2^n N_0 + 0\cdot N_1 + 2^n N_2 + 2^{n+2m}N_{2^m+1} &= 2^{2n},\\
-2^{n+2m}N_0 + 0\cdot N_1 + 2^{n+2m}N_2 + 2^{2n+m}N_{2^m+1} &= 2^{2n+2m}.
\end{aligned}
$$

그러므로 다음이 얻어진다.

$$
\begin{aligned}
N_0 &= 2^{4m-1} - 2^{3m-1},\\
N_1 &= 2^{3m} - 2^m - 1,\\
N_2 &= 2^{4m-1} - 2^{3m-1},\\
N_{2^m+1} &= 2^m.
\end{aligned}
$$

정리 4.2에 의해 $C_d(\tau) \in \{-1-2^{2m}, -1, -1+2^{2m}, -1+2^{3m}\}$이다.

PUKYONG NATIONAL UNIVERSITY 부경대학교

참 고 문 헌

[1] A. Canteaut, P. Charpin and H. Dobbertin, Binary m-sequences with three-valued cross-correlation: a proof of Welch's conjecture, IEEE Trans. Inf., Vol. 46, pp. 4-8, 2000.

[2] T.W. Cusick and H. Dobbertin, Some new three-valued cross-correlation functions for binary m-sequences, IEEE Trans. Inf. Theory, Vol. 42, pp. 1238-1240, 1996.

[3] H. Dobbertin, One-to-one highly nonlinear power functions on $GF(2^n)$, AAECC Applicable Algebra in Engineering, Communication and Computing, Vol. 9, pp. 139-152, 1998.

[4] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, IEEE Trans. Inf. Theory, Vol. 14, No. 1, pp. 154-156, 1968.

[5] S.W. Golomb, Shift register sequences, Holden Day, 1967.

[6] T. Helleseth, Some results about the cross-correlation function between two maximal linear sequences, Discrete Mathemetics, Vol. 16, No. 3, pp. 209-232, 1976.

[7] H.D. Hollmann and Q. Xiang, A proof of the Welch and Niho conjectures on cross-correlation of binary m-sequences, Finite Fields and Their Applications, Vol. 7, pp. 253-286, 2001.

[8] T. Helleseth and P. Rosendahl, New pairs of m-sequences with 4-level cross-correlation, Finite Fields and Their Applications, Vol. 11, pp. 647-683, 2005.

[9] T. Helleseth, J. Lahtonen and P. Rosendahl, On Niho type cross-correlation functions of m-sequences, Finite Fields and Their Applications, Vol. 13, No. 2, pp. 305-317, 2007.

[10] A. Johansen and T. Helleseth, A family of m-sequences with five-valued cross-correlation, IEEE Trans. Inf. Theory, Vol. 55, No. 2, pp. 880-887, 2009.

[11] T. Kasami, The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes, Inform. Control, Vol. 18, pp. 369-394, 1971.

[12] J. Lahtonen, On the odd and the aperiodic correlation properties of the Kasami sequences, IEEE Trans. Inf. Theory, Vol. 41, No. 5, pp. 1506-1508, 1995.

[13] R. Lidl and H. Niederreiter, Finite fields, Cambridge University Press, 1997.

[14] R. McEliece, Finite fields for computer scientists and engineers, Kluwer Academic Publishers, Boston, 1987.

[15] Y. Niho, Multi-valued cross-correlation functions between two maximal linear recursive sequences, Ph.D. thesis, University of

Southern California, 1972.

[16] P. Rosendhal, Niho type cross-correlation functions and related equations, Ph.D. thesis, Turku center for computer science, 2004.

[17] 조성진, 유한체 및 그 응용, 교우사, 2007.