교 육 학 석 사 학 위 논 문

상호상관관계 함숫값이 4개인 Niho 타입의 새로운 데시메이션

2013년 2월

부경대학교교육대학원

수 학 교 육 전공

방 문 희

교 육 학 석 사 학 위 논 문

상호상관관계 함숫값이 4개인 Niho 타입의 새로운 데시메이션

지도교수 조 성 진

이 논문을 교육학석사 학위논문으로 제출함.

2013년 2월

부경대학교교육대학원

수 학 교 육 전공

방 문 희

방문희의 교육학석사 학위논문을 인준함.

2013년 2월 22일

주 심 이학 박사 표 용 수 (인)

위 원 교육학박사 서 종 진 (인)

위 원 이학 박사 조 성 진 (인)

목 차

표 목차

그림 목차

New Decimations with 4-Valued Cross-Correlations

Moon Hee Bang

Graduate School of Education

Pukyong National University

Abstract

In this thesis, we find the cross-correlation between a binary maximal length sequence and a special decimated sequence of that sequence by an integer d. We will be interested in the values and the number of occurrences of each value attained by such cross-correlation function $C_d(\tau)$. The decimation considered is the special decimation $d = \frac{1}{2^s - 1}(2^{k(i+1)} - 2^{ki} + 2^{s+1} - 2^k - 1)$, where $n = 2k$, k is even, s is an integer such that $\gcd(s, n) = 1$ and i is an odd integer such that s divides i. It is proved that the cross-correlation takes on four values and the distribution of the cross-correlation values is also completely determined.

Ⅰ. 서론

정보화 사회로의 발전과 더불어 이동통신에 대한 수요와 관심이 급속이 증대되고 이에 따라 제한된 주파수 대역에서 아날로그 방식의 이동통신 시스템이 제공할 수 있는 수용 용량은 포화 상태에 이르렀다. 새롭게 등장하는 다양한 형태의 무선통신 서비스를 수용하기 위해 고려되어야 하는 가장 중요한 문제 중의 하나가 '한정된 전파 자원을 어떻게 하면 효율적으로 이용할 수 있을까?'에 관한 것이다. 이동전화 시스템에서는 이렇게 부족한 주파수를 효율적으로 이용하기 위해 두 가지 기술을 채용하고 있다. 첫 번째가 주파수를 재사용하여 기지국의 수를 늘리는 셀룰러 기술이고 두 번째가 주파수를 동시에 여러 가입자가 사용할 수 있도록 하는 다중접속방식이다.

주파수를 많은 사용자가 사용할 수 있는 다중접속방식에는 주파수분할다중접속(FDMA), 시분할다중접속(TDMA), 코드분할다중접속(CDMA) 등이 있다[8]. 이중 디지털 신호 여러 개를 동시에 전송하는 방법으로 TDMA와 CDMA가 대표적인 방식이다. TDMA방식은 하나의 주파수 대역을 주기적인 일정한 시간 간격으로 나누어서 각 사용자가 차례차례로 자신에게 할당된 시간 간격에 자신의 신호를 실어 보내면 각 수신측에서 자기의 시간 간격에 있는 정보만을 골라 수집하는 방식이다[4]. CDMA방식은 여러 사용자들의 신호를 처리하거나 여러 사용자들이 중앙통신장치에 접속할 때 부호를 분할하여 채널을 구분하는 방식이다[24]. 따라서 여러 사용자가 시간과 주파수를 공유하면서 각 사용자는 자신에게 할당된 부호만을 이용하여 대역확산(spread spectrum)하여 전송하고, 수신자는 송신측에서 사

용된 부호를 사용하여 역확산(despreading)시켜 원하는 정보를 얻게 되므로 할당된 부호간의 상호상관관계(cross-correlation)는 낮으면서 자기상관관계(auto-correlation)는 높은 수열을 부호로 사용하는 것이 바람직하다([2], [10]). 이러한 수열의 설계에 대한 연구도 이루어지고 있다([5], [18]). 또한 대역확산 방식은 송신자의 입장에서 보면 대역의 다른 부분을 차지하는 부호와 변조된 부호를 동시에 송신하기 때문에 완전히 랜덤한 부호를 이용할 수 있으나 수신자의 입장에서는 수신된 부호를 축적하거나 재생시켜야 할 필요가 있으므로 완전히 랜덤한 부호를 이용할 수 없다. 따라서 이러한 시스템에서는 의사난수열(pseudo-random sequence)을 부호로 사용한다.

본 논문에서는 의사난수열인 두 개의 m-수열에 의해 생성되는 Gold 계열의 새로운 이진수열군을 생성하기 위한 d의 값을 제안하고, 그 수열의 상호상관관계 함숫값을 분석하여 제안된 수열은 상호상관관계 함숫값이 4개인 비선형 이진수열임을 보이고 그 값들의 발생횟수를 결정한다.

Ⅱ. 배경지식

2.1. 트레이스 함수

트레이스 함수는 유한체로부터 부분체로의 선형 매핑인데, 이 함수는 의사불규칙 수열의 설계와 분석을 위한 중요한 수학적 도구이다. 원소의 개수가 2^n개인 유한체를 $GF(2^n)$으로 나타내고, 곱셈에 대하여 닫혀있는 $GF(2^n)$의 부분군은 $GF(2^n)^* = GF(2^n) \setminus \{0\}$으로 나타내면, $GF(2^n)$의 원시원소는 $GF(2^n)^*$의 모든 원소를 생성한다([20], [21]).

<정의 2.1.1 ([20], [21])> 유한체 $GF(2^n)$에서 부분체 $GF(2^k)$으로의 트레이스 함수 $Tr_k^n(\cdot)$는 $GF(2^n)$의 임의의 원소 x에 대하여 다음과 같이 정의한다.

$$Tr_k^n(x) = \sum_{i=0}^{n/k-1} x^{2^{ki}} \tag{2.1}$$

<정리 2.1.2 [20]> $GF(2^n)$의 임의의 원소 x, y와 $GF(2^k)$의 임의의 원소 a, b에 대하여 트레이스 함수는 다음을 만족한다.

(1) $Tr_k^n(ax+by) = aTr_k^n(x) + bTr_k^n(y)$

(2) 음이 아닌 정수 i에 대하여

$Tr_k^n(x) = Tr_k^n\left(x^{2^{ki}}\right) = \left\{Tr_k^n(x)\right\}^{2^{ki}}$

(3) $Tr_1^n(x) = Tr_1^k\left[Tr_k^n(x)\right]$

(4) $GF(2^k)$의 임의의 원소 β에 대하여 방정식 $Tr_k^n(x) = \beta$를 만족하는 해의 개수는 2^{n-k} 이다.

트레이스 함수의 성질 (1)로부터 트레이스 함수가 선형임을 알 수 있고, (4)는 (2)로부터 쉽게 유도할 수 있다. 특히 성질 (3)은 m-수열의 확장된 형태인 GMW 수열을 생성하는데 중요한 역할을 한다.

<정의 2.1.3> 트레이스 함수는 유한체를 체로 가지는 벡터공간 $GF(2^n)$상에서의 선형함수가 된다. 이 트레이스 함수를 이용하여 m-수열을 다음과 같이 정의한다.

$$m(t) = Tr_1^n(\omega\alpha^t) \tag{2.2}$$

여기서, α는 $GF(2^n)$의 원시원소이며, $\omega \in GF(2^n)^*$가 존재한다. 역으로, $\omega \in GF(2^n)^*$이고, α가 $GF(2^n)$의 원시원소라 하면 (2.2)에 의해서 생성된 수열은 m-수열이다.

위에서 정의된 m-수열을 이용해서 많은 의사난수열군들이 제시되었는데, 특히 m-수열과 m-수열을 데시메이션하여 얻어지는 수열을 shift하여 더하는 방식으로 많은 수열군들이 만들어져 왔다.

<예제 2.1.4> 트레이스 함수(2.1)에서 $n=4$이고 $k=2$라 하자. 이때,

$f(x)=x^4+x+1$라 하고, α를 $\alpha^4=\alpha+1$을 만족하는 $GF(2^4)$의 원시원소라 하자. β를 $GF(2^2)$의 한 원시원소라 하면 $\beta^2=\beta+1$를 만족하고 α와 β는 $\beta=\alpha^{(2^4-1)/(2^2-1)}=\alpha^5$ 을 만족한다. 이 때, $GF(2^4)$의 원소에 대한 트레이스는 다음과 같다.

$$Tr_2^4(0)=0+0^{2^2}=0+0^4=0$$

$$Tr_2^4(1)=1+1^{2^2}=1+1^4=0$$

$$Tr_2^4(\alpha)=\alpha+\alpha^{2^2}=\alpha+\alpha^4=1$$

$$Tr_2^4(\alpha^2)=\alpha^2+(\alpha^2)^{2^2}=\alpha^2+\alpha^8=(\alpha+\alpha^4)^2=1$$

$$\begin{aligned}Tr_2^4(\alpha^3)&=\alpha^3+(\alpha^3)^{2^2}=\alpha^3+\alpha^{12}=\alpha^3+(\alpha^3+\alpha^2+\alpha+1)\\&=\alpha^2+\alpha+1=\alpha^{10}=\beta^2\end{aligned}$$

$$Tr_2^4(\alpha^4)=\alpha^4+(\alpha^4)^{2^2}=\alpha^4+\alpha^{16}=(\alpha+\alpha^4)^4=1$$

$$Tr_2^4(\alpha^5)=\alpha^5+(\alpha^5)^{2^2}=\alpha^5+\alpha^5=0$$

$$\begin{aligned}Tr_2^4(\alpha^6)&=\alpha^6+(\alpha^6)^{2^2}=\alpha^6+\alpha^9=(\alpha^2+\alpha^3)+(\alpha+\alpha^3)\\&=\alpha+\alpha^2=\alpha^5=\beta\end{aligned}$$

$$\begin{aligned}Tr_2^4(\alpha^7)&=\alpha^7+(\alpha^7)^{2^2}=\alpha^7+\alpha^{13}=(1+\alpha+\alpha^3)+(1+\alpha^2+\alpha^3)\\&=\alpha+\alpha^2=\alpha^5=\beta\end{aligned}$$

$$Tr_2^4(\alpha^8)=\alpha^8+(\alpha^8)^{2^2}=\alpha^8+\alpha^2=(\alpha+\alpha^4)^2=1$$

$$\begin{aligned}Tr_2^4(\alpha^9)&=\alpha^9+(\alpha^9)^{2^2}=\alpha^9+\alpha^6=(\alpha+\alpha^3)+(\alpha^2+\alpha^3)\\&=\alpha+\alpha^2=\alpha^5=\beta\end{aligned}$$

$$Tr_2^4(\alpha^{10})=\alpha^{10}+(\alpha^{10})^{2^2}=\alpha^{10}+\alpha^{10}=0$$

$$\begin{aligned}Tr_2^4(\alpha^{11})&=\alpha^{11}+(\alpha^{11})^{2^2}=\alpha^{11}+\alpha^{14}=(\alpha+\alpha^2+\alpha^3)+(1+\alpha^3)\\&=\alpha^2+\alpha+1=\alpha^{10}=\beta^2\end{aligned}$$

$$Tr_2^4(\alpha^{12}) = \alpha^{12} + (\alpha^{12})^{2^2} = \alpha^{12} + \alpha^3 = (1+\alpha+\alpha^2+\alpha^3) + \alpha^3$$
$$= \alpha^2 + \alpha + 1 = \alpha^{10} = \beta^2$$

$$Tr_2^4(\alpha^{13}) = \alpha^{13} + (\alpha^{13})^{2^2} = \alpha^{13} + \alpha^7 = (1+\alpha^2+\alpha^3) + (1+\alpha+\alpha^3)$$
$$= \alpha + \alpha^2 = \alpha^5 = \beta$$

$$Tr_2^4(\alpha^{14}) = \alpha^{14} + (\alpha^{14})^{2^2} = \alpha^{14} + \alpha^{11} = (1+\alpha^3) + (\alpha+\alpha^2+\alpha^3)$$
$$= \alpha^2 + \alpha + 1 = \alpha^{10} = \beta^2$$

즉 β에 대응되는 원소는 $\alpha^6, \alpha^7, \alpha^9, \alpha^{13}$로 2^2개이고 나머지 원소 $\beta^2, 1, 0$에 대해서도 2^2개씩 존재한다.

<보조정리 2.1.5> 원소의 개수가 q인 유한체 F의 모든 원소β는 방정식 $\beta^q - \beta = 0$을 만족하고 F^*의 모든 원소 β는 방정식 $\beta^{q-1} = 1$을 만족한다.

증명. $\beta = 0$이면 분명하다. $\beta \neq 0$라 하면 $F^* = \{\beta_1, \beta_2, \cdots, \beta_{q-1}\}$이다.

$$F^* = \{\beta\beta_1, \beta\beta_2, \cdots, \beta\beta_{q-1}\}$$

이므로

$$\beta_1\beta_2 \cdots \beta_{q-1} = (\beta\beta_1)(\beta\beta_2)\cdots(\beta\beta_{q-1}) = \beta^{q-1}(\beta_1\beta_2 \cdots \beta_{q-1})$$

이다. 따라서 $\beta^{q-1} = 1$이다. 그러므로 $\beta^q = \beta$이다.

<보조정리 2.1.6> F가 E의 부분체로서 $|F| = q$라 하고 $\beta \in E$라 하면,

$$\beta \in F \quad \Leftrightarrow \quad \beta^q = \beta$$

를 만족한다.

증명. 필요조건은 보조정리 2.1.5로부터 증명되었으므로, 충분조건만을 증명하기로 한다. 방정식 $x^q - x = 0$은 E에서 서로 다른 q개의 해를 갖는다. F의 모든 원소가 $x^q - x = 0$의 근이고 $|F| = q$이므로 $F = \{\alpha \in E | \alpha^q - \alpha = 0\}$이다. 그러므로 $\beta^q = \beta$이 성립하는 E의 원소 β는 F의 원소이다.

2.2 상호상관관계 함수

가. 자기상관관계(Auto-correlation)

주기가 $2^n - 1$이며, t가 0에서 $2^n - 2$까지 변할 때 0 또는 1의 값을 가지는 이진수열 $u(t)$의 주기적 상관관계 함수 $C_d(\tau)$를 $\tau = 0, 1, 2, \cdots, 2^n - 2$에 대하여 다음과 같이 정의한다.

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

이때 이상적인 상관관계 함수를 갖는 의사난수열의 주기적 상관관계 함수 $C_d(\tau)$는 다음을 만족한다.

$$C_d(\tau)=\begin{cases}2^n-1, & \tau=0 \bmod(2^n-1)\text{ 인 경우}\\ -1, & \text{그 밖의 경우}\end{cases}$$

나. 상호상관관계(Cross-correlation)

시프트 레지스터(shift register) n개에 의해 만들어진 최대주기 2^n-1인 m-수열 $u(t)$ $(t=0,1,2,\cdots,2^n-1)$는 한 주기 동안의 2^n-1개 수열 중 '0'은 $2^{n-1}-1$개가 있고 '1'은 2^{n-1}개가 존재한다. 즉, 항상 '0'의 개수가 '1'의 개수보다 하나 더 적음을 알 수 있다. 또한 '0'과 '1' 각각에 대해 연속하여 $n-i\,(i\geq 2)$번 반복되는 경우는 $i-1$번 발생한다. 최대주기수열 $u(t)$는 점화식에 의해 생성되고 주기가 있으므로 완전히 랜덤한 값을 갖지는 않지만 위와 같은 통계적 성질을 갖고 있으므로 의사난수열이다.

2.3 $GF(q^2)$의 부분집합

<정의 2.3.1> $GF(q^2)$은 $GF(q)$의 확장체이며 $GF(q^2)$의 모든 원소 x에 대하여 x^q은 x의 켤레(conjugate)라 하고 $\overline{x}=x^q$라고 표기한다.

$GF(q^2)$의 한 부분집합을 다음과 같이 정의한다.

$$S=\{x\in GF(q^2)\,|x\,\overline{x}=1\} \tag{2.3}$$

여기서 $k=$짝수, $n=2k$, $q=2^k$이다.

이때 S는 $GF(q^2)$의 원소 중에서 $x^{q+1}=1$을 만족하는 근들의 집합이고

2^k+1은 2^n-1의 약수이므로 $GF(q^2)^*$의 부분군이다.

<정리 2.3.2> 집합 S는 주기가 $q+1$인 순환군이다.

증명. α를 $GF(q^2)$의 원시원소라 하면 $GF(q^2)$의 임의의 원소 x는 $x=\alpha^t$, $t\in\{0, 1, \cdots, 2^n-2\}$로 나타낼 수 있다. 여기서 $Q=q+1$라 두고 $t=t_1Q+t_2$ $(0\le t_1\le q-2, 0\le t_2\le q)$로 나타내면

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

이다. $\alpha^{t_2}=\gamma$, $(\alpha^Q)^{t_1}=\delta$라 하면 $\delta^q=(\alpha^Q)^{t_1q}=(\alpha^{Qq})^{t_1}=(\alpha^{q^2-1+q+1})^{t_1}=(\alpha^{q+1})^{t_1}=\alpha^{Qt_1}=\delta$이 되므로 δ는 $GF(q)^*$의 원소이다. 따라서 $GF(q^2)$의 모든 원소 x는

$$x=\delta\gamma \tag{2.4}$$

$$(\delta\in GF(q)^*, \gamma\in\{1, \alpha, \alpha^2, \cdots, \alpha^q\})$$

이다. $q=2^k$인 경우 $q+1$과 $q-1$은 서로소이므로

$$\{1, \alpha, \alpha^2, \cdots, \alpha^q\}\cong S \tag{2.5}$$

이다.

$GF(q^2)$의 원시원소 α에 대하여 두 m-수열 $u(t)=Tr_1^n(\alpha^t)$, $v(t)=u(dt)$의 상호상관관계 함수는

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

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

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

이고 $x = \alpha^t$, $y = \alpha^\tau$로 두면

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

이다. (2.4), (2.5)에 의해 $GF(q^2)$의 모든 원소 x는 $x = \delta\gamma$, $\delta \in GF(q)^*$, $\gamma \in S$ 이므로

$$Tr_1^n(yx+x^d) = Tr_1^k[Tr_k^n(y\delta\gamma+\delta^d\gamma^d)]$$

$$= Tr_1^k[(y\delta\gamma+\delta^d\gamma^d)+(y\delta\gamma+\delta^d\gamma^d)^q]$$

$$= Tr_1^k[y\delta\gamma+\delta^d\gamma^d+y^q\delta^q\gamma^q+\delta^{qd}\gamma^{qd}]$$

이다. 여기서 $d \equiv 1 \pmod{q-1}$라 하자. 그러면 $d-1 = (q-1)a$를 만족하는 정수 a가 존재한다. 따라서 $d = (q-1)a+1$이다. $\delta^d = \delta^{(q-1)a} \cdot \delta = \delta$이다. $\delta^q = \delta^{q-1} \cdot \delta = \delta$이다. 따라서

$$Tr_1^k[y\delta\gamma+\delta^d\gamma^d+y^q\delta^q\gamma^q+\delta^{qd}\gamma^{qd}]$$
$$= Tr_1^k[y\delta\gamma+\delta\gamma^d+\overline{y}\,\delta\gamma^{-1}+\delta\gamma^{-d}]$$
$$= Tr_1^k[\delta(y\gamma+\gamma^d+\overline{y}\,\gamma^{-1}+\gamma^{-d})]$$

이다. 그러므로

$$C_d(\tau)=\sum_{t=0}^{q^2-2}(-1)^{u(t+\tau)+v(t)}$$
$$=\sum_{x\in GF(q^2)^*}(-1)^{Tr_1^n(yx+x^d)}$$
$$= Tr_1^k[\delta(y\gamma+\gamma^d+\overline{y}\,\gamma^{-1}+\gamma^{-d})]$$
$$=\sum_{\gamma\in S}\Big[\sum_{\delta\in GF(q)^*}(-1)^{Tr_1^k[\delta(y\gamma+\gamma^d+\overline{y}\,\gamma^{-1}+\gamma^{-d})]}\Big]$$
$$=-(q+1)+\sum_{\gamma\in S}\Big[\sum_{\delta\in GF(q)}(-1)^{Tr_1^k[\delta(y\gamma+\gamma^d+\overline{y}\,\gamma^{-1}+\gamma^{-d})]}\Big]$$

이다. 따라서 $C_d(\tau)$의 함숫값은

$$y\gamma+\gamma^d+\overline{y}\gamma^{-1}+\gamma^{-d}=0$$

을 만족하는 $\gamma\in S$의 개수에 의해 결정된다. 이와 같은 사실을 이용하여 Niho는 다음 정리를 증명하였다.

<정리 2.3.3 [22]> $n=2k$이고 $d\equiv 1(\mathrm{mod}2^k-1)$을 만족하는 데시메이션 d와 $GF(q^2)^*$의 임의의 원소 y에 대하여 $C_d(\tau)$ $(\tau=0,1,2,\cdots,2^n-2)$의 값은

다음과 같다.

$$C_d(\tau) = -1 + (N(y) - 1) \cdot 2^k$$

여기서, $N(y)$는 $x^{2d} + yx^{d+1} + \bar{y}x^{d-1} + 1 = 0$을 만족하는 집합 S의 원소 x의 개수이다.

다음 정리는 $C_d(\tau)$ 값의 분포를 찾기 위해 널리 사용되고 있다.

<정리 2.3.4> $d(0 \le d \le 2^n - 2)$에 대하여

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

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

$$(c) \sum_{\tau=0}^{2^n-2} (C_d(\tau) + 1)^3 = 2^{2n} b$$

이다. 여기서 b는 $(x+1)^d = x^d + 1$을 만족하는 $GF(q^2)$의 원소인 x의 개수이다. (a), (b)는 트레이스 함수의 성질을 이용하여 증명할 수 있고[22], (c)는 Helleseth에 의하여 증명되었다[12].

<정의 2.3.5 [23]> 두 데시메이션 d와 e에 대하여

$$e \equiv p^i d (\mathrm{mod} p^n - 1)$$

또는

$$de \equiv p^i (\mathrm{mod} p^n - 1)$$

를 만족하는 양의 정수 i가 존재할 때 d와 e는 동치라고 한다.

어떤 정수 i에 대하여 두 데시메이션 d와 e가 $de \equiv p^i \pmod{p^n-1}$를 만족하면

$$\Delta_d(y) = \Delta_e(y^{-d}) \ (y \in GF(p^n))$$

이 성립한다. 여기서 $\Delta_d(\tau) = C_d(\tau)+1 (0 \le \tau \le 2^n-2)$이다. $\gcd(d,p^n-1)=1$이기 때문에 $\{y^{-d} \mid y \in GF(p^n)\} = GF(p^n)$이다. 따라서 두 데시메이션 d와 e가 동치이면 그 값과 발생 횟수 $C_d(\tau)$와 $C_e(\tau)$는 같다.

Ⅲ. 기존 상호상관관계 함숫값 연구 분석

3.1. 3값 상호상관관계 함수

최근 몇 년 동안 상호상관관계 함숫값의 분포는 m-수열의 이론에서 중요한 문제가 되어왔다. 상호상관관계 함숫값이 3개인 몇 가지의 수열군이 알려져 있고 이것들은 모두 발견되었다. 상호상관관계 함숫값이 3개인 데시메이션 d는 다음과 같다.

$(3a)$ $d=2^k+1,\ \frac{n}{\gcd(n,k)}$:홀수,

$(3b)$ $d=2^{2k}-2^k+1,\ \frac{n}{\gcd(n,k)}$:홀수,

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

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

$(3e)$ $d=2^{(n-1)/2}+3,\ n$:홀수,

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

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

(3a)의 d는 Gold에 의해 연구되었고[9], (3b)의 d는 Kasami에 의해 연구되었다[17]. (3c)와 (3d)는 Ckusick와 Dobbertin에 의해 연구되었다[6]. (3e)는 Canteaut 등에 의해 연구되었다[3]. (3f)와 (3g)는 Hollmann와 Xiang에 의해 연구되었다[16].

3.2. 4값 상호상관관계 함수

기존에 알려진 4값 상호상관관계함수는 다음과 같다.

$(4a)\ d=2^{n/2+1}-1,\ n\equiv 0\ (\mathrm{mod}\ 4),$

$(4b)\ d=(2^{n/2}+1)(2^{n/4}-1)+2,\ n\equiv 0\ (\mathrm{mod}\ 4),$

$(4c)\ d=\sum_{i=0}^{n/2}2^{ik},\ n\equiv 0(\mathrm{mod}4),\ 0<k<n,\ \gcd(k,n)=1$

$(4d)\ d=\frac{2^{k-1}}{2^{s-1}}(2^{2k}+2^{s+1}-2^{k+1}-1),\ n=2k,\ 2s|k$

$(4e)\ d=\frac{1}{2^{s-1}}(2^{2k}+2^{2s+1}-2^{k+s+1}-1),\ n=2k,\ 2s|k$

(4c)의 d는 Dobbertin에 의해 연구되었고 이 데시메이션은 (4a)의 데시메이션을 포함한다[7]. (4a)와 (4b)는 (4d)의 특별한 경우이고 이것은 Rosendahl과 Helleseth에 의하여 얻어졌다([15], [23]). (4e)의 d는 2012년 Kim 등이 제안하였다[19].

다음은 4개의 상호상관관계 함숫값을 갖는 Niho의 데시메이션에 대해 살펴보겠다.

3.3. Niho의 데시메이션

$n\equiv 0(\mathrm{mod}\ 4)$이고 $n=2k$이고 $d=2^{n/2+1}-1$이면 4개의 상호상관관계함숫값을 갖는다. $\gcd(d,\ 2^n-1)=1$이고

$$d = 2(2^k - 1) + 1 \equiv 1 \pmod{2^k - 1}$$
$$d = 2(2^k + 1) - 3 \equiv -3 \pmod{2^k - 1}$$

이다. 그리고 상호상관관계 함수값 $C_d(\tau)$의 발생횟수는 다음과 같다.

[표 Ⅲ-1] Niho의 $C_d(\tau)$과 발생횟수

$C_d(\tau)$	발생횟수
$-1-2^k$	$\frac{2^{2k}-2^k}{3}$
-1	$2^{2k-1}-2^{k-1}$
$-1+2^k$	2^k
$-1+2^{k+1}$	$\frac{2^{2k-1}-2^{k-1}}{3}$

3.4 Helleseth의 데시메이션

$n = 2k$이고 $2s$가 k의 약수인 s에 대해 $d = \frac{2^{k-1}}{2^s - 1}(2^{2k} + 2^{s+1} - 2^{k+1} - 1)$이면 4개의 상호상관관계함숫값을 갖는다. $\gcd(d, 2^n - 1) = 1$이고

$$d \equiv 1 \pmod{2^k - 1}$$
$$d \equiv \frac{2^k - 2^s}{2^s - 1} \pmod{2^k - 1}$$

이다. 그리고 상호상관관계 함수값 $C_d(\tau)$의 발생횟수는 다음과 같다.

[표 Ⅲ-2] Helleseth의 $C_d(\tau)$과 발생횟수

$C_d(\tau)$	발생횟수
$-1-2^k$	$\frac{2^{2k+s-1}-2^{k+s-1}}{2^s+1}$
-1	$\frac{2^{2k}-2^k-2^s}{2^s}$
$-1+2^k$	$\frac{2^{2k+s-1}-2^{2k}+2^{k+s-1}}{2^s-1}$
$-1+2^{k+s}$	$\frac{2^{2k}-2^k}{2^{3s}-2^s}$

본 논문에서는 상호상관관계 함숫값이 4개가 되도록 하는 데시메이션을 제안하고 함숫값과 그 발생횟수를 구한다.

Ⅳ. 4값 상호상관관계 함숫값을 갖는 새로운 데시메이션

상호상관관계 함숫값이 4개인 데시메이션의 새로운 집합 d를 제안하고 m-수열과 d에 의해 생성된 수열의 상호상관관계 함숫값이 최대 4개임을 보이겠다.

2005년 Helleseth는 $x^{2^s+1}+yx^{2^s}+\bar{y}x+1=0$의 해의 개수에 관하여 다음 정리를 증명하였다[15].

<정리 4.1 [23]> $n=2k$이고 $y\in GF(q^2)^*$에 대하여 방정식

$$x^{2^s+1}+yx^{2^s}+\bar{y}x+1=0 \tag{4.1}$$

에서 S의 원소인 x의 개수는 0, 1, 2, $2^{\gcd(s,k)}+1$개 중 하나이다.

<보조정리 4.2> k가 짝수이고 s는 $\gcd(s,k)=1$를 만족하면

$$\gcd(2^k+1,2^s-1)=1$$

이다.

증명. $s/\gcd(k,s)=s$가 홀수이므로

$$\gcd(2^k+1, 2^s-1)=1$$

이다.

보조정리 4.2와 유클리드 알고리즘에 의하여 우리는 다음 보조정리 4.3을 얻는다.

<보조정리 4.3> 짝수 k와 $\gcd(s,k)=1$를 만족하는 s는

$$\gcd(2^k+1, 2^s+1)=1$$

를 만족한다.

증명. $2^k+1=2^{k-s}(2^s+1)-2^{k-s}+1$이고 $\frac{k-s}{\gcd(k-s,s)}=k-s$이며 $k-s$가 홀수이므로 $\gcd(2^k+1,2^s+1)=\gcd(2^{k-s}+1,2^s+1)=1$이다.

<보조정리 4.4> $n=2k$, $d\equiv 1 \pmod{q-1}$ 라 하면 $x\in GF(q^2)\backslash\{0,1\}$ 가 $(x+1)^d=x^d+1$의 해가 될 필요충분조건은 $x^{d-1}=(x+1)^{d-1}=1$ 또는 $x^{d-q}=(x+1)^{d-q}=1$ 이다.

보조정리 4.4를 사용하여 우리는 아래와 같은 보조정리 4.5를 얻는다.

<보조정리 4.5> $n=2^k$, $d\equiv 1 \pmod{q-1}$라 하고 $x\in GF(q^2)^*$가

$(x+1)^d = x^d + 1$를 만족하면 또는 $\left(\frac{x+1}{\bar{x}+1}\right)^{d+1} = 1$이다.

증명. $x \neq 1$인 $GF(q)$의 모든 원소가 $(x+1)^d = x^d + 1$의 해이면, 보조정리 4.4에 의해 $x^d = x$ 또는 $x^d = \bar{x}$이다. 그러면 $(x+1)^d = x^d + 1$이고, $(\bar{x}+1)^d = \bar{x}^d + 1$이다. $(x+1)^d(\bar{x}+1)^d = (x^d+1)(\bar{x}^d+1)$이므로 $(x\bar{x}+x+\bar{x}+1)^d$ $= (x\bar{x})^d + x^d + \bar{x}^d + 1$ 이다.

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

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

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

보조정리 4.4와 보조정리 4.5로부터 아래와 같은 정리를 얻는다.

<정리 4.6> $d \equiv 1 \pmod{q-1}$에 대해 $\gcd(d \pm 1, 2^k+1) = 1$이면 방정식 $(x+1)^d = x^d + 1$는 $GF(2^n)$에서 정확히 2^k개의 해를 가진다.

증명. 보조정리 4.2에서 $d \equiv 1 \pmod{q-1}$이므로 $GF(q)$의 모든 원소는 $(x+1)^d = x^d + 1$의 해이다. 이제 $x(\neq 0,1)$을 $(x+1)^d = x^d + 1$의 해라고 가정하면 x는 $(x+1)^d = x^d + 1$의 해이므로 보조정리 4.4에 의하여 $x^d = x$ 또는 $x^d = \bar{x}$이다. 보조정리 4.5에 의하여 $x^d = x$이면 $\left(\frac{x+1}{\bar{x}+1}\right)^{d-1} = 1$이고 $x^d = \bar{x}$

이면 $\left(\frac{x+1}{\bar{x}+1}\right)^{d+1}=1$이다. 그런데 $\gcd(d\pm1,2^k+1)=1$이므로 $\frac{x+1}{\bar{x}+1}=1$이다. 따라서 $\bar{x}=x$이다. 즉, $x\in GF(2^k)$이다.

n은 4의 배수이면서 $n=2k$를 만족하는 k와 $\gcd(s,n)=1$을 만족하는 정수 s, 그리고 s의 배수이면서 홀수인 i에 대해 주기가 2^n-1인 m-수열로부터 다음과 같이 정의된 새로운 데시메이션 d를 이용하여 수열을 생성한다.

$$d=\frac{2^{k-1}}{2^s-1}\left(2^{k(i+1)}-2^{ki}+2^{s+1}-2^k-1\right) \tag{4.2}$$

$\gcd(s,n)=1$이고 짝수 k에 대하여 $\gcd(s,k)=1$이므로 s는 홀수이다. 따라서 $\gcd(2^k+1,2^s-1)=1$이고, $\gcd(2^k+1,2^s+1)=1$가 성립한다. 또, $\frac{s}{\gcd(s,k)}$가 홀수이므로 $\gcd(2^k+1,2^s-1)=1$이다.

$2^k+1=2^{k-s}(2^s+1)-2^{k-s}+1$로 표현할 수 있고 $\gcd(2^k+1,2^s+1)=\gcd(2^s+1,2^{k-s}-1)$이다.

그런데 $\frac{k-s}{\gcd(s,k-s)}=\frac{k-s}{\gcd(s,k)}$도 홀수이므로 $\gcd(2^s+1,2^{k-s}-1)=1$이고, 따라서 $\gcd(2^k+1,2^s+1)=1$이다. 이 사실들을 이용하여 다음을 증명한다.

<보조정리 4.7> 짝수 k에 대하여 $n=2k$, s는 $\gcd(s,n)=1$를 만족하고 홀수 i의 약수이면

$$d=\frac{2^{k-1}}{2^s-1}\left(2^{k(i+1)}-2^{ki}+2^{s+1}-2^k-1\right) \tag{4.3}$$

는 다음 성질을 만족한다.

(1) $d\equiv 1 \pmod{2^k-1}$

(2) $d\equiv \dfrac{2^{ki}-2^s}{2^s-1} \pmod{2^k+1}$

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

증명. (1)은 간단한 계산을 통하여 쉽게 알 수 있다.

(2) $d=2^{k-1}\left\{\dfrac{2^{ki}-2^s}{2^s-1}(2^k-1)+2^k+1\right\}$

$\equiv \dfrac{2^{ki}-2^s}{2^s-1}\pmod{2^k+1}$

(3) (1)과 (2)에 의해

$$\gcd(d,2^n-1)=\gcd(d,2^k+1)=\gcd\left(\frac{2^{ki}-2^s}{2^s-1},2^k+1\right)$$

이다. 그리고 $\gcd(2^s-1,2^k+1)=1$이므로

$$\gcd\left(\frac{2^{ki}-2^s}{2^s-1},2^k+1\right)=\gcd(2^{ki}-2^s,2^k+1)$$

이다. 또한 $2^{ki}-2^s\equiv -1-2^s\pmod{2^k+1}$이므로 $\gcd(2^{ki}-2^s,2^k+1)=\gcd(2^k+1,2^s+1)=1$이다. 따라서 $\gcd(d,2^n-1)=1$이다.

<보조정리 4.8> 짝수 k에 대하여 $n=2k$, s는 $\gcd(s,n)=1$를 만족하고 홀

수 i의 약수라 하면

$$d=\frac{2^{k-1}}{2^s-1}\left(2^{k(i+1)}-2^{ki}+2^{s+1}-2^k-1\right) \tag{4.4}$$

는 다음 성질을 만족한다.

(1) $\gcd(d+1,2^k+1)=1$

(2) $\gcd(d-1,2^k+1)=1$

증명. (1) 보조정리 4.2에 의해 $\gcd(2^s-1,2^k+1)=1$이므로

$$\gcd(d+1,2^k+1)=\gcd((2^s-1)(d+1),2^k+1)$$

이다.

$$\begin{aligned}&(2^s-1)(d+1)\\&=2^{k-1}(2^{k(i+1)}-2^{ki}+2^{s+1}-2^k-1)+(2^s-1)\\&\equiv -2 \pmod{2^k+1}\end{aligned}$$

이고

$$\gcd((2^s-1)(d+1),2^k+1)=\gcd(2,2^k+1)=1$$

이므로

$$\gcd(d+1,2^k+1)=1$$

이다.

(2) 보조정리 4.2에서 $\gcd(2^s-1,2^k+1)=1$이므로

$$\gcd(d-1,2^k+1)=\gcd((2^s-1)(d-1),2^k+1)$$

이다.

$$\begin{aligned}&(2^s-1)(d-1)\\&=2^{k-1}(2^{k(i+1)}-2^{ki}+2^{s+1}-2^k-1)-(2^s-1)\\&\equiv-2^{s+1}\pmod{2^k+1}\end{aligned}$$

이므로

$$\gcd((2^s-1)(d-1),2^k+1)=\gcd(2^{s+1},2^k+1)$$

이다. 따라서

$$\gcd(d-1,2^k+1)=1$$

이다.

보조정리 4.7에 의하여 $d\equiv1\pmod{2^k-1}$이다. 정리 4.6과 보조정리 4.8에 의하여 아래의 정리를 얻는다.

<정리 4.9> 짝수 k에 대하여 $n=2k$, s는 $\gcd(s,n)=1$를 만족하고 홀수 i의 약수이다. 그리고 d를 다음과 같다고 하자.

$$d=\frac{2^{k-1}}{2^s-1}\left(2^{k(i+1)}-2^{ki}+2^{s+1}-2^k-1\right) \tag{4.5}$$

이때 i는 홀수이고 s는 i의 약수이다. 그러면 두 개의 m수열사이의 상호 상관관계 함수값 $C_d(\tau)$의 발생횟수는 다음과 같다.

[표 Ⅳ-1] 새로운 수열의 $C_d(\tau)$과 발생횟수

$C_d(\tau)$	발생횟수
$-1-2^k$	$\frac{2^{2k}-2^k}{3}$
-1	$\frac{2^{2k}-2^k-2}{2}$
$-1+2^k$	2^k
$-1+2^{k+1}$	$\frac{2^{2k}-2^k}{6}$

증명. 보조정리 4.7에서 $d\equiv 1 \pmod{2^k-1}$, $d\equiv\frac{2^{ki}-2^s}{2^s-1} \pmod{2^k+1}$ 그리고 $\gcd(d, 2^n-1)=1$이다. 그러므로 정리 2.3.3에 의하여 우리는 아래의 식을 얻는다.

$$yx+x^{\frac{2^{ki}-2^s}{2^s-1}}+y^{2^k}x^{-1}+x^{-\frac{2^{ki}-2^s}{2^s-1}}=0 \tag{4.6}$$

$$x^{2^k+1}=1$$

보조정리 4.2 에 의하여 $\gcd(2^k+1, 2^s-1)=1$이므로 식 (4.6)의 해의 개수는 식 (4.6)에서의 x 대신 x^{2^k-1}로 대체하여 얻은 아래 식 (4.7)의 해의 개수와 같다.

$$yx^{2^s-1}+x^{2^{ki}-2^s}+\bar{y}x^{1-2^s}+x^{-2^{ki}+2^s}=0 \tag{4.7}$$

식 (4.7)의 양변에 $x^{2^{ki}-2^s}$을 곱하면 아래의 방정식을 얻는다.

$$yx^{2^s-1}+x^{2(2^{ki}-2^s)}+\bar{y}x^{2^{ki}-2^{s+1}+1}+1=0 \tag{4.8}$$

그리고 $2^k \equiv -1 \pmod{2^k+1}$에 의하여 식 (4.8)은 아래의 식과 같다.

$$x^{2(-1-2^s)}+yx^{-2}+\bar{y}x^{-2^{s+1}}+1=0 \tag{4.9}$$

식 (4.9)의 해의 개수는 아래 식 (4.10)의 해의 개수와 같다.

$$x^{-1-2^s}+yx^{-1}+\bar{y}x^{-2^s}+1=0 \tag{4.10}$$

그러므로 식 (4.10)의 해의 개수는 아래 식 (4.11)의 해의 개수와 같다.

$$x^{2^s+1}+yx^{2s}+\bar{y}x+1=0 \tag{4.11}$$

그리고 정리 4.1의 $C_d(\tau)$는 4개의 값을 가진다.

정리 2.3.4와 정리 4.6에 의하여

$$\sum_{\tau=0}^{2^n-2}(C_d(\tau)+1)^3 = 2^{2n}2^k$$

이다.

N_i를 식 (4.11)에서 S에서 i개의 해를 갖는 횟수라 하자.

$$\begin{aligned} N_0+N_1+N_2+N_3 &= 2^n-1 \\ -2^kN_0+0\cdot N_1+2^kN_2+2^{k+1}N_3 &= 2^n \\ -2^nN_0+0\cdot N_1+2^nN_2+2^{n+2}N_3 &= 2^{2n} \\ -2^{n+k}N_0+0\cdot N_1+2^{n+k}N_2+2^{n+k+3}N_3 &= 2^{2n+k} \end{aligned}$$

이 연립방정식을 풀면 $N_0=\frac{2^{2k}-2^k}{3}, N_1=\frac{2^{2k}-2^k-2}{2}$, $N_2=2^k$, $N_3=\frac{2^{2k}-2^k}{6}$을 얻는다.

정리 2.3.3에 의해 $C_d(\tau)\in\{-1-2^k, -1, -1+2^k, -1+2^{k+1}\}$이다.

<예제 4.10> 8차 원시다항식 $f(x)$가 $f(x)=x^8+x^4+x^3+x^2+1$일 때 $f(x)$의 원시근 α에 대하여 주기가 2^8-1인 두 m-수열 $u(t)$, $v(t)$에 대한 상호상관관계의 함숫값을 분석해보자.

$n=8$이므로 $k=4$이다. $s=1$, $i=3$으로 두면 $d=227$이다. $u(t)=Tr_1^n(\alpha^t)$는 그림 1과 같고, $v(t)=u(227t)$는 그림 2와 같다. $\tau=201$일 때, $u(201+t)$는 그림 3과 같다. 따라서 $C_{227}(201)=-2^4-1=-17$이다. 같은 방법으로 0부터 254까지 τ의 값을 차례대로 변화시키면서 $C_d(\tau)$의 값을 구

하면 $\{-17, -1, 15, 31\} = \{-2^4-1, -1, 2^4-1, 2^{4+1}-1\}$로 4개의 값 중 하나가 된다.

0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0
0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1
0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0
0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0
0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1
0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1
0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0
0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1
0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0
0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1
0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1
0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1
0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1
0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0
0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0

[그림 Ⅳ-1] 수열 $u(t) = Tr_1^8(\alpha^t)$의 15×17배열

0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0
0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0
0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1
0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0
0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0
0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1
0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1
0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0
0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1
0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0
0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1
0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1
0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1
0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1
0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0

[그림 Ⅳ-2] 수열 $v(t) = u(227t)$의 15×17 배열

0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0
0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1
1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1
0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0
0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1
1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0
1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1
0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1
1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1
0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1
1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0
1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0
1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0
1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1
0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0

[그림 Ⅳ-3] 수열 $u(201+t)$의 15×17배열

그리고 두 m-수열 $u(t)$, $v(t)$에 대한 상호상관관계 함수값 $C_d(\tau)$의 발생 횟수는 다음과 같다.

[표 Ⅳ-2] 두 m-수열 $u(t)$, $v(t)$에 대한 $C_d(\tau)$과 발생횟수

$C_d(\tau)$	발생횟수
-17	80
-1	119
15	16
31	40

Ⅴ. 결론

본 논문에서는 아래의 d에 대하여 $C_d(\tau)$의 4값의 상호상관관계의 분포를 구하였다.

$$d=\frac{1}{2^s-1}\left(2^{k(i+1)}-2^{ki}+2^{s+1}-2^k-1\right)$$

여기서, $n=2k$이고, k는 짝수이며, s는 홀수 i의 약수이며 $\gcd(s,n)=1$이다.

그리고 CDMA 통신에서 부호 분할을 위해 사용되는 의사난수열에 대해 d의 값을 이용하여 주기가 같은 새로운 수열을 생성하고 두 수열의 상호상관관계 함숫값이 4개임을 보였고 그 값들의 발생횟수를 구하였다.

참 고 문 헌

[1] 조성진, “유한체 및 그 응용”, 교우사, 2007.

[2] L.D. Baumert, “Cyclic Difference Sets”, Lecture Notes in Mathematics, New York : Springer-Verlag, Vol. 182, 1971.

[3] 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.

[4] G. Chakraborty, “Genetic algorithm to solve optimum TDMA transmission schedule in broadcast packet radio networks”, IEEE Trans. Commun., Vol. 52(5), pp. 765-777, 2004.

[5] U.S. Choi, S.J. Cho, “Design of Binary Sequences with Optimal Cross-Correlation Values”, J. The Korea Institute of Electronic Communication Science, Vol. 6, No. 4, pp. 539-544, 2011.

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

[7] 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.

[8] K. Fazel and S. Kaiser, “Multi-carrier and Spread Spectrum System”, John Wiley and Sons Ltd., 2003.

[9] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, IEEE Trans. Inf. Theory, Vol. 14, No.

1, pp. 154-156, 1968.

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

[11] S.W. Golomb and G. Gong, Signal Design for Good Correlation-For Wireless Communication, Cryptography, and Radar. Cambridge, U.K. : Cambridge Univ. Press, 2005.

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

[13] T. Helleseth and P. V. Kumar, Sequences with low correlation, in Handbook in Coding Theory, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science B. V., Vol. 2, ch. 21, pp. 1765-1853, 1998.

[14] 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.

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

[16] 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.

[17] 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.

[18] H.D. Kim, S.J. Cho, M.J. Kwon and H.J. An, “A Study on the cross-correlation function of extended Zeng sequences”, J. The Korea Institute of Electronic Communication Science, Vol. 7, No. 1, pp. 263-269, 2012.

[19] H.D. Kim, S.J. Cho, S.T. Kim and U.S. Choi, Four-valued cross-correlation function between two maximal linear recursive sequences, Submitted.

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

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

[22] Y. Niho, Multi-valued cross-correlation functions between two maximal linear recursive sequences, Ph.D. thesis, University of Southern California, 1972.

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

[24] M.K. Simon, J. K. Omura, R.A. Sholtz, and B. K. Levitt, “Spread Spectrum Communications”, Rockville, MD : Computer Sci., Vol. 1, 1985.