최대 주기의 두 선형 순환 수열 사이의 4개의 값을 갖는 상호상관함수

최언숙* · 조성진** · 김한두***

Four-Valued Cross-Correlation Function between Two Maximal Linear Recursive Sequences

Un-Sook Choi* · Sung-Jin Kim* · Han-Doo Kim***

요 약

수열이론의 중요한 문제 중 하나는 두 수열사이의 상호 상관관계가 몇 개의 서로 다른 값을 가지며 또한 그 값의 발생횟수이다. 본 논문에서는 주기가 2^n-1인 m-수열 $u(t)$와 그 수열을 d만큼 데시메이션해서 얻은 수열 $u(dt)\,(0 \le t \le 2^n-2)$사이의 상호상관관계의 값과 그 값의 발생 횟수를 찾는다. 여기서 $n=2m,\ 2s|m$ 이고, $d=(2^{2m}+2^{2s+1}-2^{m+s+1}-1)/(2^s-1)$ 이다. 또한 제안된 데시메이션에 의해 생성된 수열이 4-값 상호상관관계를 가짐을 보인다.

ABSTRACT

One of important problems in the theory of sequences is to determine the values and number of occurrences of each value taken on by the cross-correlation. In this paper, we find the values and the number of occurrences of each value of cross-correlation between an m-sequence $u(t)$ of period 2^n-1 and its decimation $u(dt)\,(0 \le t \le 2^n-2)$ where $n=2m,\ 2s|m$ and $d=(2^{2m}+2^{2s+1}-2^{m+s+1}-1)/(2^s-1)$. Also we show that a family of decimations leads to a four-valued cross-correlation.

키워드

cross-correlation, m-sequence, Gold-like sequences, Niho type, decimation, finite field
상호상관관계, m-수열, Gold 계열 수열, Niho 형태, 데시메이션, 유한체

Ⅰ. 서 론

이진수열은 CDMA(Code Division Multiple Access) 시스템에서 여러 사용자가 시간과 주파수를 공유하면서 각 사용자에게 확산코드를 할당하는데 사용된다. 이러한 CDMA 시스템에서 신호를 변조하는데 사용되는 수열을 설계하는데 있어 중요한 요소 중 하나는 설계된 수열이 낮은 상호상관관계를 갖는가 하는 것이다. 왜냐하면 낮은 상호상관관계를 갖는 수열은 CDMA 시스템에서 사용자들 사이의 신호들의 간섭을 줄이고 신호를 잘 복호할 수 있기 때문이다. 이러한 최대주기 수열의 상호상관관계에 대한 연구는

* 동명대학교 자율전공학부(choies@tu.ac.kr)
** 교신저자 부경대학교 응용수학과(sjcho@pknu.ac.kr)
*** 인제대학교 컴퓨터응용과학부(mathkhd@inje.ac.kr)
접수일자 : 2012. 08. 06 심사(수정)일자 : 2012. 11. 21 게재확정일자 : 2012. 12. 10

지난 50여 년 동안 많은 연구자들에 의해 연구되어 왔다. Niho와 Rosendahl은 이 주제에 대한 우수한 연구결과를 발표하였다[1,2]. 이들은 품질이 우수한 이진 수열을 발생시키기 위해 최대 주기를 갖는 m-수열 $u(t)$와 $u(t)$에 데시메이션 d을 적용하여 얻은 수열 $v(t)=u(dt)$을 이용했다. 이러한 수열을 Gold 계열 수열이라 한다[3]. 이 때 두 수열 사이의 상호상관관계는 식 (1)과 같다.

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

Gold 계열 수열에서 낮은 상호상관관계를 갖는 수열을 발생하는 데시메이션에 대한 연구가 활발히 진행되었다. 표 1은 3값 상호상관관계를 갖는 수열을 발생시키는 데시메이션과 관련된 조건이다.

표 1. 3값 상호상관관계 데시메이션
Table 1. 3-valued cross-correlation decimations

(a) $d=2^k+1$, $n/\gcd(n,k)$: 홀수
(b) $d=2^{2k}-2^k+1$, $n/\gcd(n,k)$: 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) $d=2^{(n-1)/2}+3$, n : 홀수
(f) $d=2^{(n-1)/2}+2^{(n-1)/4}-1$, $n\equiv 1 \pmod 4$
(g) $d=2^{(n-1)/2}+2^{(3n-1)/4}-1$, $n\equiv 3 \pmod 4$

표 1의 (a)는 Gold에 의해 증명되었고[3], (b)는 Kasami에 의해 증명되었다[4]. 이후 (c), (d)의 결과가 Cusick과 Dobbertin에 의해 증명되었고[5], Canteaut 등에 의해 (e)의 결과가 증명되었다[6]. Hollman과 Xiang에 의해 (f)와 (g)가 증명되었다[7]. 이 후 4값 상호상관관계를 갖는 수열을 발생시키는 데시메이션에 대한 연구가 Niho를 비롯한 많은 연구자들에 의해 진행되었다. 표 2는 잘 알려진 4값 상호상관관계를 갖는 수열을 발생시키는 데시메이션과 관련된 조건이다. 표2의 (a), (b)는 Niho에 의해 (c)는 Dobbertin에 의해 증명되었다[1,8]. (d)는 2005년에 Helleseth와 Rosendahl에 의해, (e)는 2008년에 Seo 등에 의해 증명되었다[9,10]. (f)은 권 등에 의해 증명되었다[11]. 그리고 계속해서 5값 상호상관관계를 갖는 수열을 발생시키는 데시메이션에 대한 연구가 계속 되고 있다[12].

본 논문에서는 4값 상호상관관계를 갖는 수열을 발생시키는 새로운 데시메이션을 제안하고 이것에 대한 각 상호상관관계 값의 발생 빈도를 분석한다.

표 2. 4값 상호상관관계 데시메이션
Table 2. 4-valued cross-correlation decimations

(a) $d=2^{n/2+1}-1$, $n\equiv 0 \pmod 4$
(b) $d=(2^{n/2}+1)(2^{n/4}-1)+2$, $n\equiv 0 \pmod 4$
(c) $d=\sum_{i=0}^{n/2} 2^{im}$, $n\equiv 0 \pmod 4$, $0<m<n$, $\gcd(m,n)=1$
(d) $d=2^{k-1}(2^{2k}+2^{s+1}-2^{k+1}-1)/(2^s-1)$, $n=2k$, $2s \mid k$
(e) $d=(p^{2k}+1)^2/4$, $n=4k$, $p(>2)$:소수
(f) $d=\dfrac{2^{k-1}(2^{k(i+1)}-2^{ki}+2^{s+1}-2^k-1)}{2^s-1}$, $n\equiv 0 \pmod 4$, $n=2k$, $\gcd(n,s)=1$, $(n,s)=1$ $s \mid i, i: odd$

II. 배경 지식

트레이스(Trace) 함수는 유한체로부터 부분체로의 선형매핑인데, 이 함수는 이진수열의 설계와 분석을 위한 중요한 수학적 도구이다. $GF(p^n)$를 p^n개의 원소를 가진 유한체라 하고, $GF(p^n)^*=GF(p^n)/\{0\}$라 하자. 차수가 n인 원시다항식 $f(x)$의 원시근을 $\alpha(\in GF(p^n))$라 하자.

트레이스함수 $Tr_m^n: GF(p^n)\rightarrow GF(p^m)$는 다음과 같이 정의한다[13].

$$Tr_m^n(x)=x+x^{2^m}+x^{2^{2m}}+\cdots+x^{2^{(k-1)m}}$$

여기서 x는 $GF(p^n)$의 원소이고 $k=n/m$이다. 트레이스함수 $Tr_m^n: GF(p^n)\rightarrow GF(p^m)$는 다음 성질을 만족한다[13].

ⓐ $Tr_m^n(x+y) = Tr_m^n(x) + Tr_m^n(y)\ \forall x,y \in GF(p^n)$.

ⓑ $Tr_m^n(cx) = c\,Tr_m^n(x),\ \forall c \in GF(p^m),\ x \in GF(p^n)$.

ⓒ Tr_m^n는 전사함수이다.

ⓓ $Tr_m^n(c) = kc,\ \forall c \in GF(p^m)$.

ⓔ $Tr_m^n(x^{p^m}) = Tr_m^n(x),\ \forall x \in GF(p^n)$.

ⓕ $Tr_1^n(x) = Tr_1^m(Tr_m^n(x)),\ \forall x \in GF(p^n)$.

ⓖ임의의 고정된 $\beta \in GF(p^m)$에 대하여 방정식 $Tr_m^n(x) = \beta$를 만족하는 해가 p^{n-m}개 존재한다.

하나의 m-수열 $u(t)$와 m-수열에 데시메이션을 적용한 수열을 $v(t)$라 할 때 주기 p^n-1인 두 m-수열의 합으로 생성되는 수열을 Gold 계열의 수열이라 한다[3]. $u(t)$와 $v(t)$는 식 (2)와 같다.

$$u(t) = Tr_1^n(\alpha^t),\ v(t) = u(dt) \tag{2}$$

여기서 α는 $GF(p^n)$의 한 원시원소이고, 데시메이션 $d(1 \le d \le p^n-2)$는 $\gcd(d, p^n-1) = 1$를 만족한다.

특히 소수인 p에 대하여 $n = km$일 때 $d \equiv 1 \pmod{p^m-1}$인 d를 Niho 형태의 데시메이션이라 한다.

$n = 2m$이고 m을 짝수라 하자. $q = 2^m$라 하면 임의의 $x \in GF(q^2)$에 대하여 $\overline{x} = x^q$라 정의하면 $GF(q^2)$의 모든 원소 x, y에 대하여 $\overline{x+y} = \overline{x} + \overline{y}$, $\overline{xy} = \overline{x}\,\overline{y}$, $x + \overline{x} \in GF(q)$, $x\overline{x} \in GF(q)$이 성립한다.

$GF(q^2)$의 단위원의 $q+1$제곱근의 집합을 S라 하자. 즉

$$S = \{x \in GF(q^2) \mid x\overline{x} = 1\} \tag{3}$$

이고, S는 주기가 $q+1$인 순환군이다.

$C_d(\tau)$를 계산하는 것은 $\sum_{x \in GF(p^n)^*} \chi(x + yx^d)$를 계산하는 것과 같다. 여기서 χ는 유한체 $GF(p^n)$의 canonical additive character이고, $y = \alpha^\tau$이다. 이것은 정리 1을 만족한다. $C_d(\tau)$의 값의 분포를 찾는데 있어 정리 1의 거듭제곱의 합에 관한 식을 사용한다.

<정리 1[1]> 소수 p에 대하여 상호상관관계 $C_d(\tau)$는 다음이 성립한다.

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

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

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

여기서 b는 $|\{x \in GF(q^2) \mid (x+1)^d = x^d+1\}|$이다.

p가 소수일 때 서로 다른 데시메이션 e와 d가 $e \equiv p^i d \pmod{p^n-1}$ 또는 $de \equiv p^i \pmod{p^n-1}$를 만족하는 정수 i가 존재하면 d와 i는 동치라 한다[2]. $\gcd(d, p^n-1) = 1$이므로, $\{y^{-d} \mid y \in GF(p^n)\} = GF(p^n)$이다. 그래서 d와 e가 동치이면 $C_d(\tau)$, $C_e(\tau)$의 값과 그것들이 발생 빈도도 같다[2].

III. 4값 상호상관관계 함수

이 절에서는 Niho 형태의 새로운 데시메이션 d를 제안하고 주어진 데시메이션에 의해 생성되는 수열이 4값 상호상관관계를 가짐을 보이고 그 상관관계 값의 발생 빈도를 구한다.

<정리 2[2]> $n = 2m$이고 $y \in GF(2^n)^*$에 대하여 방정식 (4)을 만족하는 S에 속한 x의 개수는 $0, 1, 2, 2^{\gcd(s,m)}+1$중 하나이다.

$$x^{2^s+1} + yx^{2^s} + \overline{y}\,x + 1 = 0 \tag{4}$$

$n = 2m$이고 $q = 2^m$라 하면 $GF(q^2)^*$의 임의의 원소 x에 대하여 $x = \delta\gamma$로 표현할 수 있다. 여기서 $\delta \in GF(q)^*$이고 $\gamma \in S$이다. $d \equiv 1 \pmod{2^m-1}$라 가정하고 $C_d(\tau)+1 = \Delta_d(\tau)$라 두면 $\Delta_d(\tau) = 2^m(N(y)-1)$이다[1]. 여기서 $N(y)$는 다음과 같다.

$$N(y) = |\{x \in S \mid x^d + yx + \overline{y}x^{-1} + x^{-d} = 0,\ y \in GF(2^n)^*\}| \tag{5}$$

$n = 2m$, $2s \mid m$일 때 데시메이션 d를 식 (6)과 같이 정의하자.

$$d = (2^{2m} + 2^{2s+1} - 2^{m+s+1} - 1)/(2^s - 1) \tag{6}$$

다음 정리는 식 (6)에 정의된 데시메이션 d와 동치인 데시메이션에 대한 결과이며 이는 주어진 식 (6)의 데시메이션에 대하여도 같은 결과를 만족하며 제안된 d가 Niho 형태의 데시메이션임을 의미한다.

<정리 3> $n=2m$이고, $2s \mid m$일 때

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

라 하면 다음을 만족한다.

① $d \equiv 1 \pmod{2^m-1}$

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

③ $\gcd(d, 2^n-1)=1$

(증명) ① 주어진 d에 대하여 다음을 만족한다.

$$\begin{aligned} d &= \frac{2^{m-s-1}}{2^s-1}\{(2^m-1)(2^m-1)+2(2^m-1)-2^{s+1}(2^m-2^s)\} \\ &= \frac{2^{m-s-1}}{2^s-1}\{(2^m-1)(2^m-1)+2(2^m-1)-2^{s+1}(2^m-1)\}+2^m \\ &= \frac{2^{m-s-1}}{2^s-1}\{(2^m-1)(2^m-1)+2(2^m-1)(2^s-1)\}+2^m \end{aligned}$$

그러므로 $d \equiv 1 \pmod{2^m-1}$이다.

② 주어진 d에 대하여 다음을 만족한다.

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

그러므로 $d \equiv \frac{2^m-2^s}{2^s-1} \pmod{2^m+1}$이다.

③ ①에 의해 $\gcd(d, 2^m-1)=1$이므로 $\gcd(d, 2^n-1)=\gcd(d, 2^m+1)$이다. ②에 의해 $\gcd(d, 2^n-1)=\gcd\left(\frac{2^m-2^s}{2^s-1}, 2^m+1\right)$이다.

$2^m+1=(2^s-1)\frac{2^m-2^s}{2^s-1}+2^s+1$이므로 $\gcd\left(\frac{2^m-2^s}{2^s-1}, 2^m+1\right)=\gcd\left(\frac{2^m-2^s}{2^s-1}, 2^s+1\right)$이고, 따라서 $\gcd(d, 2^n-1)=\gcd\left(\frac{2^m-2^s}{2^s-1}, 2^s+1\right)$이다. $2s \mid m$이므로 정수 a에 대하여 $m=2as$라 할 수 있다. $2a-2$가 짝수이므로 다음을 만족한다.

$$\begin{aligned} \frac{2^m-2^s}{2^s-1} &\equiv \frac{2^{2as}-2^s}{2^s-1} \\ &\equiv 2^s\{(2^s)^{2a-2}+(2^s)^{2a-3}+\cdots+2^s+1\} \\ &\equiv 2^s \pmod{2^s+1} \end{aligned}$$

그러므로 $\gcd\left(\frac{2^m-2^s}{2^s-1}, 2^s+1\right)=\gcd(2^s, 2^s+1)=1$이다. 따라서 $\gcd(d, 2^n-1)=1$이다.

주어진 데시메이션에 의해 생성된 수열의 상호상관관계 $C_d(\tau)$를 구하기 위해 정리 1의 식 (c)을 구하기 위해 방정식 $(x+1)^d=x^d+1$의 해의 개수를 구해야 한다.

<보조정리 4[14]> $q=2^m$이고 $d \equiv 1 \pmod{q-1}$이라 하자. $x \in GF(q^2) \setminus \{0,1\}$가 $(x+1)^d=x^d+1$의 해일 필요충분조건은 $x^{d-1}=(x+1)^{d-1}=1$ 또는 $x^{d-q}=(x+1)^{d-q}=1$이다.

<정리 5> $n=2m$이고 $2s \mid m$이라 하자. 데시메이션 d가 $d=\frac{1}{2^s-1}(2^{2m}+2^{2s+1}-2^{m+s+1}-1)$라 할 때 방정식 (7)을 만족하는 해의 개수는 $GF(2^n)$에서 정확히 2^m이다.

$$(x+1)^d=x^d+1 \tag{7}$$

(증명) 주어진 d는 $d \equiv 2^{-m+s+1} \pmod{2^m-1}$이므로 $GF(2^m)$의 모든 원소는 방정식 (7)의 해이다. $x(\neq 0, 1)$를 방정식 (7)의 해라고 가정하자. 식 (7)을 양변 2^s-1 거듭제곱을 하면 다음과 같다.

$$(x+1)^{(2^s-1)d}=\frac{x^{2^sd}+1}{x^d+1} \tag{8}$$

가정으로부터 $(2^s-1)d=2^{2m}+2^{2s+1}-2^{m+s+1}-1$ 이므로 식 (8)은 다음과 같다.

$$\frac{x^{2^2}+1}{x^{2^{m+s+1}}+1}=\frac{x^{2^sd}+1}{x^d+1} \tag{9}$$

그러므로 $(x^{2^2}+1)(x^d+1)=(x^{2^sd}+1)(x^{2^{m+s+1}}+1)$이고 전개하여 정리하면

$x^{2^{2s+1}+d}+x^{2^sd+2^{m+s+1}}=x^{2^{2s+1}}+x^{2^sd}+x^{2^{m+s+1}}+x^d$이다.

$$\begin{aligned} 2^{2s+1}+d-2^sd-2^{m+s+1} &= -(2^s-1)d+(2^{2s+1}-2^{m+s+1}) \\ &\equiv 0 \pmod{2^n-1} \end{aligned}$$

이므로 $x^{2^{2s+1}}+x^{2^sd}+x^{2^{m+s+1}}+x^d=0$이다. 그리고

$x^{(2^s-1)d}=x^{2^{2s+1}-2^{m+s+1}}$이므로 $(x^{2^{m+s+1}}+x^d)(x^{(2^s-1)d}+1)=0$이다. 그러므로 $x^{2^{m+s+1}}=x^d$ 또는 $(x^d)^{2^s-1}=1$이다.

(a) $x^{2^{m+s+1}}=x^d$인 경우: $x^{2^{m+s+1}(2^s-1)}=x^{2^{2s+1}-2^{m+s+1}}$이므로 $x^{2^{m+2s+1}}=x^{2^{2s+1}}$이고, $\left(x^{2^{2s+1}}\right)^{2^m}=x^{2^{2s+1}}$이다. 그러면 $x^{2^{2s+1}}\in GF(2^m)$이다. $m=2as$라 하자. 그러면 $x^{2^m}=\left(x^{2^{2s+1}}\right)^{2^{2(a-1)s-1}}\in GF(2^m)$이고, $x=\left(x^{2^m}\right)^{2^m}=x^{2^m}\in GF(2^m)$ 그러므로 $x\in GF(2^m)$이다.

(b) $(x^d)^{2^s-1}=1$인 경우 : $x\in GF(q^2)\backslash\{0,1\}$가 방정식 (7)의 해 이므로 보조정리 4에 의하여 $x^{d-1}=1$ 또는 $x^{d-q}=1$이다. $x^{d-1}=1$이면 $x=x^d\in GF(2^m)$이고 $x^{d-q}=1$이면 $x^q=x^d\in GF(2^m)$이라서 $x=\left(x^{2^m}\right)^{2^m}=x^{2^m}$이다. 그러므로 $x\in GF(2^m)$이다.

정리 3과 정리 5에서 정의된 데시메이션은 서로 동치이다. 따라서 두 데시메이션에 의해 생성된 수열이 가지고 있는 상호상관관계 값과 발생 빈도는 같다. 다음 정리는 이 논문의 주요 정리로 주어진 데시메이션에 의해 생성된 수열의 상호상관관계와 발생 빈도에 대한 분석결과이다.

<정리 6> $n=2m$이고 $2s|m$이라 하자. 데시메이션 d가 $d=\dfrac{1}{2^s-1}(2^{2m}+2^{2s+1}-2^{m+s+1}-1)$라 하자. 그러면 주어진 데시메이션에 의해 생성된 수열의 상호상관관계 $C_d(\tau)$ 값과 발생 빈도는 다음과 같다.

$C_d(\tau)$	발생 빈도
$-1-2^m$	$(2^{2m+s-1}-2^{m+s-1})/(2^s+1)$
-1	$(2^{2m}-2^m-2^s)/2^s$
$-1+2^m$	$(2^{2m+s-1}-2^{2m}-2^{m+s-1})/(2^s-1)$
$-1+2^{m+s}$	$(2^{2m}-2^m)/(2^{3s}-2^s)$

(증명) 정리 3에 의해 $d\equiv 1\pmod{2^m-1}$, $d\equiv\dfrac{2^m-2^s}{2^s-1}\pmod{2^m+1}$이고, $\gcd(d,2^n-1)=1$이므로 식 (5)의 $N(y)$는 다음 방정식을 만족하는 해의 개수이다.

$$yx+x^{\frac{2^m-2^s}{2^s-1}}+\bar{y}x^{-1}+x^{-\frac{2^m-2^s}{2^s-1}}=0 \tag{10}$$

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

$\gcd(2^s-1,2^m+1)=1$이므로 식 (10)에서 x를 x^{2^s-1}로 바꿀 수 있으며 그 결과는 $yx^{2^s-1}+x^{2^m-2^s}+\bar{y}\,x^{-2^s+1}+x^{-2^m+2^s}=0$이고 $x^{2(2^m-2^s)}+yx^{2^m-1}+\bar{y}\,x^{2^m-2^{s+1}+1}+1=0$와 동치이다. $2^m\equiv-1\pmod{2^m+1}$이므로

$x^{2(-1-2^s)}+yx^{-2}+\bar{y}\,x^{-2^{s+1}}+1=0$와 동치이고,

$\left(x^{-1-2^s}+y^{1/2}x^{-1}+(\bar{y})^{1/2}x^{-2^s}+1\right)^2=0$이므로 식 (10)의 해의 개수는 식 (11)의 해의 개수와 같다.

$$x^{-1-2^s}+y^{1/2}x^{-1}+(\bar{y})^{1/2}x^{-2^s}+1=0 \tag{11}$$

또한 식 (11)를 변형하여 얻은 $x^{2^s+1}+yx^{2^s}+\bar{y}x+1=0$의 해의 개수와도 같다. 따라서 정리 2에 의해 $C_d(\tau)$는 4값을 갖는다. 그러므로 정리 1과 정리 5에 의하여 $\sum_{\tau=0}^{2^n-2}(\Delta_d(\tau))^3=2^{2n}2^m$이다. N_i를 집합 S에서 방정식 (4)의 해의 개수가 i인 경우가 나타나는 발생 빈도수라 하면 다음과 같은 연립방정식을 얻는다.

$$\begin{cases} N_0+N_1+N_2+N_{2^s+1} & =2^n-1\\ -2^mN_0+0\cdot N_1+2^mN_2+2^{m+s}N_{2^s+1} & =2^n\\ 2^nN_0+0\cdot N_1+2^nN_2+2^{n+2s}N_{2^s+1} & =2^{2n}\\ -2^{n+m}N_0+0\cdot N_1+2^{n+m}N_2+2^{n+m+3s}N_{2^s+1} & =2^{2n+m}\end{cases}$$

이 연립방정식을 풀면

$$N_0=\frac{2^{2m+s-1}-2^{m+s-1}}{2^s+1},\ N_1=\frac{2^{2m}-2^m-2^s}{2^s},$$

$$N_2=\frac{2^{2m+s-1}-2^{2m}-2^{m+s-1}}{2^s-1},\ N_{2^s+1}=\frac{2^{2m}-2^m}{2^{3s}-2^s}$$

이다. 그러므로 $C_d(\tau)\in\{-1-2^m,-1,-1+2^m,-1+2^{m+s}\}$이고 발생 빈도는 N_0, N_1, N_2, N_{2^s+1}이다.

Ⅳ. 결 론

본 논문에서는 최대주기를 갖는 m-수열과 데시메

이션을 적용한 수열을 발생시키는 Gold 계열의 수열 중 새로운 Niho 형태의 데시메이션을 적용하여 얻은 수열에 대하여 상호상관관계와 각 상호상관관계 값에 대한 빈도를 분석하였다. 제안된 데시메이션에 의해 생성된 수열의 상호상관관계값은 $-1-2^m, -1, -1+2^m, -1+2^{m+s}$중 하나가 됨을 보임으로 4값 상호상관관계를 갖는 새로운 Niho 형태의 데시메이션을 제안하였다. 이러한 수열은 CDMA 시스템에서 신호를 변조하는데 사용되는 수열로 응용될 수 있는 품질이 우수한 비선형 이진수열군이라 사료된다.

참고 문헌

[1] Y. Niho, "Multi-valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences", Ph.D. thesis, University of Southern California, 1972.

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

[3] R. Gold, "Maximal recursive sequences with 3-valued cross-correlation functions," IEEE Trans. Inf. Theory, Vol. 14, No. 1, pp. 154-156, 1967.

[4] T. Kasami, "The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes," Inform. Control, Vol. 18, No. , pp. 369-394, 1971.

[5] T.W. Cusick and H. Dobbertin, "Some new three-valued cross-correlation functions for binary m-sequences," IEEE Trans. Inf. Theory, Vol. 42, No. 4, pp. 1238-1240, 1996.

[6] A. Canteaut, P. Charpin and H. Dobbertin, "Binary m-sequences with three-valued cross-correlation: a proof of Welch's conjecture," IEEE Trans. Inf. Theory, Vol. 46, No. 1, pp. 4-8, 2000.

[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, No. 2, pp. 253-286, 2001.

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

[9] T. Helleseth and P. Rosendahl, "New pairs of m-sequences with 4-level cross-correlation," Finite Fields and Their Applications, Vol. 11, No. 4, pp. 647-683, 2005.

[10] E.Y. Seo, Y.S. Kim, J.S. No and D.J. Shin, "Cross-correlation distribution of p-ary m-sequence of period $p^{4k}-1$ and its decimated sequences by $\left(\frac{p^{2k}+1}{2}\right)^2$," IEEE Trans. Inf. Theory, Vol. 54, No. 7, pp. 3140-3149, 2008.

[11] 권민정, 조성진, 권숙희, 김진경, 김한두, 최언숙, "상호상관관계 함숫값이 4개인 새로운 데시메이션," 한국전자통신학회논문지, 7권, 4호, pp. 827-832, 2012.

[12] 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.

[13] 조성진, "유한체 및 그 응용", 교우사, 2007.

[14] 최언숙, 조성진, "유한체상의 방정식과 m-수열의 상호상관관계 분석," 한국전자통신학회논문지, 7권, 4호, pp. 821-826, 2012.

저자 소개

최언숙(Un-Sook Choi)

1992년 2월 성균관대학교 산업공학과 졸업 (공학사)

2000년 2월 부경대학교 대학원 응용수학과 졸업(이학석사)

2004년 2월 부경대학교 대학원 응용수학과 졸업(이학박사)

2008년 8월 부경대학교 정보보호협동과정 졸업(공학박사)

2006년~현재 동명대학교 자율전공학부 교수

※ 관심분야 : 셀룰라 오토마타론, 정보보호

조성진(Sung-Jin Cho)

1979년 2월 강원대학교 수학교육과 졸업(이학사)
1981년 2월 고려대학교 대학원 수학과 졸업(이학석사)
1988년 2월 고려대학교 대학원 수학과 졸업(이학박사)
1988년~현재 부경대학교 응용수학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호

김한두(Han-Doo Kim)

1982년 2월 고려대학교 수학과 졸업(이학사)
1984년 2월 고려대학교 대학원 수학과 졸업(이학석사)
1988년 2월 고려대학교 대학원 수학과 졸업(이학박사)
1989년~현재 인제대학교 컴퓨터응용과학부 교수
※ 관심분야 : 전산수학, 셀룰라 오토마타론