비선형수열의 상호상관함수 분석

조성진* · 임지미**

Analysis of cross-correlation functions of non-linear sequences

Sung-Jin Cho* · Ji-Mi Yim**

이 논문은 2012학년도 부경대학교의 지원을 받아 수행된 연구임(PK-2012-41)

요 약

최대주기를 갖는 수열들의 상호상관함수에 대한 연구는 수십년간 이루어져 왔다. 본 논문에서는 $n=2m$을 만족하고 최대주기 2^n-1을 가지면서 Niho type의 데시메이션 $d=2^{m-2}(2^m+3)$에 대하여 비선형수열 $S_a^r(t)=Tr_1^m\{[Tr_m^n(a\alpha^t+\alpha^{dt})]^r\}$의 상호상관함수 값을 구한다. 특히, $d\equiv 1(\mathrm{mod}\,2^m-1)$을 만족하는 d를 Niho type의 데시메이션 이라고 한다. 그리고 위상이동차 $\tau=(2^m+1)k\,(0\le k\le 2^m-2)$인 경우에 대하여 $S_a^r(t)$의 상호상관함수 값의 분포를 분석하고 실험 결과를 제시한다.

ABSTRACT

Cross-correlation functions of maximal period sequences have been studied for decades. In this paper, we find the cross-correlation values of non-linear sequences $S_a^r(t)=Tr_1^m\{[Tr_m^n(a\alpha^t+\alpha^{dt})]^r\}$ having the maximal period 2^n-1 for Niho type decimation $d=2^{m-2}(2^m+3)$, where $n=2m$. In particular, we call d Niho type decimation in case $d\equiv 1(\mathrm{mod}\,2^m-1)$. And we analyze the cross-correlation distributions of $S_a^r(t)$ when the phase shift $\tau=(2^m+1)k\,(0\le k\le 2^m-2)$ and provide experiment results.

키워드

상호상관함수, 데시메이션, 트레이스, 유한체

Key word

cross-correlation function, decimation, trace, finite fields

* 종신회원 : 부경대학교(교신저자, sjcho@pknu.ac.kr)

** 준회원 : 부경대학교

접수일자 : 2013. 01. 16

심사완료일자 : 2013. 03. 12

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.5.1138

Ⅰ. 서 론

낮은 상관함수를 갖는 이진 의사 난수열들은 통신과 암호분야에서 널리 사용 되어져 왔다[1-3]. 이 수열들은 다중 캐리어 확산대역 통신 시스템(Multi-carrier spread spectrum communication system), 직접방식의 코드 분할 다중접속(code-division multiple-access)통신 시스템과 같은 무선통신에 있어서 중요한 역할을 하고 있다[4, 5]. 수열들의 패밀리 크기는 시스템에서 사용자수를 결정한다. 사용자들에게 다른 수열을 할당하고 상관함수 탐지 방법을 적용하여 여러 명의 사용자들이 같은 채널에 동시에 접속하는 것을 가능하게 한다. 패밀리 크기가 클수록 그만큼 많은 사용자들의 접속이 가능하고 접속자들 간의 신호를 식별할 수 있다. 이진수열의 상호상관함수(Cross-Correlation)는 다중접속간섭(Multiple Access Interference)을 결정한다. 다중접속간섭(MAI)을 최소화하는 방법은 낮은 상관함수를 갖는 이진 수열을 적용하는 것이다. 최대 주기를 갖는 수열의 상호상관 함수에 대한 연구는 Niho[6], Helleseth[7], Rosendahl[8] 등에 의해서 이루어져 왔다. 특히 Niho는 주기가 $2^{2k}-1$인 수열에서 $d \equiv 1 (\mathrm{mod}\, 2^k-1)$을 만족하는 데시메이션(decimation) d값을 다루는 방법을 연구했다. Gold 수열[9], Kasami 수열[10], No 수열[11] 등은 최적의 상관함수를 갖는 수열들이다. 본 논문에서 사용되는 유한체에 관한 지식은 [12, 13]을 바탕으로 한다. 2장에서 배경지식을 소개하고 3장에서는 $d=2^{m-2}(2^m+3)$ 일 때 비선형 수열 $S_a^r(t)=Tr_1^m\{[Tr_m^n(a\alpha^t+\alpha^{dt})]^r\}$의 상호상관함수를 찾는다. 그리고 4장에서는 $\tau=(2^m+1)k$ $(0 \le k \le 2^m-2)$ 인 경우에 대하여 상호상관함수의 분포를 분석하고 실험결과를 제시한 후 5장에서는 결론을 맺는다.

Ⅱ. 배경지식

[정의 1] $k|l$을 만족하는 $k, l \in \mathbb{N}$에 대하여 함수 $Tr_k^l : GF(2^l) \rightarrow GF(2^k)$을 트레이스(trace)라 한다.

$$Tr_k^l(x) = x + x^{2^k} + x^{2^{2k}} + \cdots + x^{2^{(\frac{l}{k}-1)k}} \tag{1}$$

[예제 2] [정의 1]에서 $l=4$, $k=1$ 이라 하고 α를 $f(x)=x^4+x+1$의 원시근 이라고 하자. 트레이스 함수 (1)에 의해서 $Tr_1^4(\alpha)=\alpha+\alpha^2+\alpha^4+\alpha^8$ 이고 α는 $f(x)=x^4+x+1$의 원시근이므로 $\alpha^4=\alpha+1$ 와 $\alpha^8=(\alpha+1)^2=\alpha^2+1$ 를 만족한다.

따라서 $Tr_1^4(\alpha)=0$ 이다.

[정리 3] 함수 $Tr_k^l : GF(2^l) \rightarrow GF(2^k)$는 다음 성질을 만족한다.

(a) $Tr_k^l(\alpha^{2^k}) = Tr_k^l(\alpha)$ $(\alpha \in GF(2^l))$

(b) Tr_k^l은 선형적이다.

(c) $Tr_k^l(a) = \frac{l}{k} \cdot a$ $(a \in GF(2^k))$

【증명】 (a) $\alpha \in GF(2^l)$이므로 $\alpha^{2^l}=\alpha$이다. 그러면 아래와 같은 식이 성립한다.

$$\begin{aligned} Tr_k^l(\alpha^{2^k}) &= \alpha^{2^k} + (\alpha^{2^k})^{2^k} + \cdots + (\alpha^{2^k})^{2^{(\frac{l}{k}-1)k}} \\ &= \alpha^{2^k} + \alpha^{2^{2k}} + \cdots + \alpha^{2^l} \\ &= \alpha + \alpha^{2^{2k}} + \cdots + \alpha^{2^{(\frac{l}{k}-1)k}} \\ &= Tr_k^l(\alpha) \end{aligned} \tag{2}$$

(2)에 의해서 $Tr_k^l(\alpha^{2^k}) = Tr_k^l(\alpha)$이다.

(b) $\alpha, \beta \in GF(2^l)$에 대하여 다음 식이 성립한다.

$$\begin{aligned} & Tr_k^l(\alpha+\beta) \\ &= (\alpha+\beta) + (\alpha+\beta)^{2^k} + \cdots + (\alpha+\beta)^{2^{(\frac{l}{k}-1)k}} \\ &= (\alpha+\beta) + (\alpha^{2^k}+\beta^{2^k}) + \cdots + (\alpha^{2^{(\frac{l}{k}-1)k}} + \beta^{2^{(\frac{l}{k}-1)k}}) \\ &= (\alpha + \alpha^{2^k} + \cdots + \alpha^{2^{(\frac{l}{k}-1)k}}) + (\beta + \beta^{2^k} + \cdots + \beta^{2^{(\frac{l}{k}-1)k}}) \\ &= Tr_k^l(\alpha) + Tr_k^l(\beta) \end{aligned} \tag{3}$$

$c \in GF(2^l)$ 이면 $c^{2^l}=c$이므로

$c^{2^{l \cdot i}}=c$ $(0 \le i \le \frac{l}{k}-1)$이다. 따라서 $\alpha \in GF(2^l)$에 대하여 아래의 식이 성립한다.

$$\begin{aligned} Tr_k^l(c\alpha) &= (c\alpha)+(c\alpha)^{2^k}+\cdots+(c\alpha)^{2^{(\frac{l}{k}-1)k}} \\ &= c\alpha + c^{2^k}\alpha^{2^k}+\cdots+c^{2^{(\frac{l}{k}-1)k}}\alpha^{2^{(\frac{l}{k}-1)k}} \\ &= c\alpha + c\alpha^{2^k}+\cdots+c\alpha^{2^{(\frac{l}{k}-1)k}} \\ &= c(\alpha+\alpha^{2^k}+\cdots+\alpha^{2^{(\frac{l}{k}-1)k}}) \\ &= cTr_k^l(\alpha) \end{aligned} \quad (4)$$

(3)과 (4)에 의해서 Tr_k^l은 선형적이다.

(c) 임의의 $a\in GF(2^k)$에 대하여

$a^{2^{k\cdot i}} = a\,(0\le i\le \frac{l}{k}-1)$ 이므로 (5)가 성립한다.

$$Tr_k^l(a) = a+a^{2^k}+\cdots+a^{2^{(\frac{l}{k}-1)k}} = \frac{l}{k}\cdot a \quad (5)$$

(5)에 의해서 $Tr_k^l(a)=\frac{l}{k}\cdot a$ 이다. □

[정의 4] $f(x)$가 $GF(2)$위에서 n차 기약다항식이고 s가 양의 정수라 하자. 수열 $\boldsymbol{a}=\{a_i\}=\left\{Tr_k^l(\alpha^i)\right\}$ $(i\ge 0$인 정수, α는 $f(x)$의 원시근)와 $\boldsymbol{b}=\{a_{si}\}=\left\{Tr_k^l(\alpha^{si})\right\}$에 대하여 수열 $\boldsymbol{b}$는 수열 $\boldsymbol{a}$의 s-데시메이션(decimation)이라고 한다.

[예제 5] 기약다항식 $f(x)=x^4+x^3+1$에 대한 수열 $\boldsymbol{a}=(011110101100100)$이다. 그러면 [정의 4]에 의해서 $\boldsymbol{a}$의 3-데시메이션 $\boldsymbol{b}=(01111)$이고, $\boldsymbol{a}$의 7-데시메이션 $\boldsymbol{b}=(000100110101111)$이다.

[정의 6] 주기가 N인 두 수열 $u(t)$, $v(t)$에 대하여 상호상관함수는 다음과 같이 정의한다.

$$C(\tau)=\sum_{t=0}^{N-1}(-1)^{u(t+\tau)+v(t)}\,(0\le\tau\le N-1) \quad (6)$$

$n=2m$ $(m\in\mathbb{N})$, $N=2^n-1$, $Q=2^m+1$, α는 $GF(2^n)$의 원시원소라 하자.

주기가 N인 $s_i(t):=Tr_1^m\left\{[Tr_m^n(\alpha^{2t})+\eta_i\alpha^{Qt}]^r\right\}$ $(\eta_i\in GF(2^m)$, $\gcd(r,2^m-1)=1)$는 No 수열이며 $\eta_i=0$인 경우 GMW 수열이 되고 $r=1$인 경우 Kasami 수열이 된다. $\eta_i=0$이고 $r=1$이면 m-수열이 된다.

Ⅲ. $S_a^r(t)$의 상호상관함수

이번 장에서는 주기가 2^n-1인 비선형수열 $S_a^r(t)$의 상호상관함수를 구한다.

$n=2m$, $d=2^{m-2}(2^m+3)$, $\gcd(r,2^m-1)=1$, $S_r=\left\{S_a^r(t)\,|\,a\in GF(2^m),0\le t\le 2^n-2\right\}$라 두자.

비선형 수열 $S_a^r(t)$는 (7)과 같다.

$$S_a^r(t):=Tr_1^m\left\{[Tr_m^n(a\alpha^t+\alpha^{dt})]^r\right\} \quad (7)$$

(단, α는 $GF(2^n)$의 원시원소이다.)

[보조정리 7]의 (a)는 $d=2^{m-2}(2^m+3)$가 Niho type의 데시메이션 임을 보여준다.

[보조정리 7] $d=2^{m-2}(2^m+3)$에 대하여 다음을 만족한다.

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

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

【증명】 (a) $d=2^{m-2}(2^m+3)$는 (8)과 같은 등식이 성립한다.

$$\begin{aligned} d &= 2^{m-2}(2^m+3) \\ &= 2^{m-2}(2^m-1+4) \\ &= 2^{m-2}(2^m-1)+2^m \end{aligned} \quad (8)$$

(8)에 의해서 $d=2^{m-2}(2^m+3)$를 2^m-1로 나누면 나머지는 1이 된다. 따라서 $d\equiv 1\pmod{2^m-1}$이다.

(b) $d=2^{m-2}(2^m+3)$는 (9)과 같은 등식이 성립한다.

$$\begin{aligned} d &= 2^{m-2}(2^m+1+2) \\ &= 2^{m-2}(2^m+1)+2^{m-1} \end{aligned} \quad (9)$$

(9)에 의해서 $d=2^{m-2}(2^m+3)$를 2^m+1로 나누면 나머지는 2^{m-1}이 된다. 따라서 $d\equiv 2^{m-1}\pmod{2^m+1}$

이다. □

[정리 8] $S_a^r(t)$와 $S_b^r(t)$의 상호상관함수 $C_{ab}(\tau)$는 $-1-2^m$, -1, $-1+2^m$, $-1+2\cdot 2^m$, $-1+3\cdot 2^m$의 최대 5개의 함숫값을 갖는다.

【증명】 $C_{ab}(\tau)=\sum_{t=0}^{2^n-2}(-1)^{S_a^r(t+\tau)+S_b^r(t)}$에서

$S_a^r(t+\tau)+S_b^r(t)$는 아래와 같다.

$$Tr_1^m\left\{[Tr_m^n(a\alpha^{t+\tau}+\alpha^{d(t+\tau)})]^r+[Tr_m^n(b\alpha^t+\alpha^{dt})]^r\right\} \quad (10)$$

$Q=2^m+1$ 라 두면

$t=t_1Q+t_2(0\le t_1\le 2^m-2,\ 0\le t_2\le 2^m)$ 로 표현할 수 있다.

(10)에 $t=t_1Q+t_2$를 대입하면 (11)과 같다.

$$Tr_1^m\left\{[Tr_m^n(a\alpha^{t_1Q+t_2+\tau}+\alpha^{d(t_1Q+t_2+\tau)})]^r+[Tr_m^n(b\alpha^{t_1Q+t_2}+\alpha^{d(t_1Q+t_2)})]^r\right\} \quad (11)$$

$\alpha^Q=\beta$라 두면 $\beta\in GF(2^m)$이고 [보조정리 7]의 (a)에 의하여 $\beta^d=\beta$이다. 따라서 (11)은

$$Tr_1^m\left\{\beta^{t_1r}([Tr_m^n(a\alpha^{t_2+\tau}+\alpha^{d(t_2+\tau)})]^r+[Tr_m^n(b\alpha^{t_2}+\alpha^{dt_2})]^r)\right\} \quad (12)$$

이 된다. (12)에서

$$H(t_2,\tau,r)=[Tr_m^n(a\alpha^{t_2+\tau}+\alpha^{d(t_2+\tau)})]^r+[Tr_m^n(b\alpha^{t_2}+\alpha^{dt_2})]^r$$

라 두면 (12)는 $Tr_1^m\left\{\beta^{t_1r}H(t_2,\tau,r)\right\}$으로 나타낼 수 있다. 따라서

$$C_{ab}(\tau)=\sum_{t=0}^{2^n-2}(-1)^{S_a^r(t+\tau)+S_b^r(t)}=\sum_{t_2=0}^{2^m}\sum_{t_1=0}^{2^m-2}(-1)^{Tr_1^m\left\{\beta^{t_1r}H(t_2,\tau,r)\right\}}$$

이다.

집합 $\left\{t_2|H(t_2,\tau,r)=0,\ 0\le t_2\le 2^m\right\}$의 원소 개수를 $N(t_2,\tau,r)$라 두자. 그러면

$$C_{ab}(\tau)=N(t_2,\tau,r)(2^m-1)+(2^m+1-N(t_2,\tau,r))(-1)=-1+(N(t_2,\tau,r)-1)2^m$$

이다.

지금부터 $N(t_2,\tau,r)$을 구하기 위해서 $H(t_2,\tau,r)=0$라 두자. 그러면

$[Tr_m^n(a\alpha^{t_2+\tau}+\alpha^{d(t_2+\tau)})]^r=[Tr_m^n(b\alpha^{t_2}+\alpha^{dt_2})]^r$ 이고

$\gcd(r,2^m-1)=1$ 이므로

$Tr_m^n(a\alpha^{t_2+\tau}+\alpha^{d(t_2+\tau)})=Tr_m^n(b\alpha^{t_2}+\alpha^{dt_2})$ 가 된다.

이 등식을 정리하면 (13)과 같다.

$$(a\alpha^\tau+b)\alpha^{t_2}+(\alpha^{d\tau}+1)\alpha^{dt_2}+(a\alpha^\tau+b)^{2^m}\alpha^{2^mt_2}+(a\alpha^\tau+1)^{2^m}\alpha^{2^mdt_2}=0 \quad (13)$$

(13)에서 $a\alpha^\tau+b=A(\tau)$, $\alpha^{d\tau}+1=B(\tau)$ 라 두면

(13)은 다음과 같다.

$$A(\tau)\alpha^{t_2}+B(\tau)\alpha^{dt_2}+\overline{A(\tau)}\alpha^{2^mt_2}+\overline{B(\tau)}\alpha^{2^mdt_2}=0 \quad (14)$$

집합 $S=\left\{x\,|\,x\overline{x}=1,\ \overline{x}=x^{2^m},\ x\in GF(2^n)\right\}$라 두면

$\alpha=\delta\gamma$ ($\delta\in GF(2^m)$, $\gamma\in S$)로 나타낼 수 있다.

그러면 (14)는

$$A(\tau)\delta^{t_2}\gamma^{t_2}+B(\tau)\delta^{dt_2}\gamma^{dt_2}+\overline{A(\tau)}\delta^{2^mt_2}\gamma^{2^mt_2}+\overline{B(\tau)}\delta^{2^mdt_2}\gamma^{2^mdt_2}=0 \quad (15)$$

이다. $\delta\in GF(2^m)$, $\gamma\in S$ 이므로 $\delta^{2^m}=\delta$, $\gamma^{2^m}=\gamma^{-1}$ 이고

[보조정리 7]에 의해서

$\delta^d=\delta$, $\delta^{2^md}=\delta$, $\gamma^d=\gamma^{2^{m-1}}$, $\gamma^{2^md}=\gamma^{-2^{m-1}}$가 성립하므로

(15)는

$$A(\tau)\delta^{t_2}\gamma^{t_2}+B(\tau)\delta^{t_2}\gamma^{2^{m-1}t_2}+\overline{A(\tau)}\delta^{t_2}\gamma^{-t_2}+\overline{B(\tau)}\delta^{t_2}\gamma^{-2^{m-1}t_2}=0 \quad (16)$$

이다.

(16)에서 $\gamma^{t_2}=x$라 두면 $x\in S$이고 (16)은

$A(\tau)\delta^{t_2}x+B(\tau)\delta^{t_2}x^{2^{m-1}}+\overline{A(\tau)}\delta^{t_2}x^{-1}+\overline{B(\tau)}\delta^{t_2}x^{-2^{m-1}}=0$

이고 (17)과 같다.

$$\delta^{t_2}x^{-2^{m-1}}(A(\tau)x^{2^{m-1}+1}+B(\tau)x^{2\cdot 2^{m-1}}+\overline{A(\tau)}x^{2^{m-1}-1}+\overline{B(\tau)})=0 \quad (17)$$

$x^{2^{m-1}+1}=y$라 두면 $y\in S$이고 $y^2=x$이다.

그러면 (17)은 $A(\tau)y+B(\tau)y^{-2}+\overline{A(\tau)}y^{-3}+\overline{B(\tau)}=0$이 되고 따라서 (18)과 같다.

$$A(\tau)y^4+\overline{B(\tau)}y^3+B(\tau)y+\overline{A(\tau)}=0 \quad (18)$$

$\gcd(2^{m-1}+1, 2^m+1)=1$이므로 (17)을 만족하는 x의 개수와 (18)를 만족하는 y의 개수는 일치한다. 따라서 $N(t_2,\tau,r)$는 0, 1, 2, 3, 4 중의 하나이다. 따라서 $C_{ab}(\tau)\in\{-1-2^m, -1, -1+2^m, -1+2\cdot 2^m, -1+3\cdot 2^m\}$인 최대 5개의 함숫값을 갖는다. □

Ⅳ. $\tau=(2^m+1)k$ $(0\le k\le 2^m-2)$인 경우에 대한 상호상관함수 분석 및 실험

위상이동차 $\tau=(2^m+1)k$ $(0\le k\le 2^m-2)$인 경우에 대하여 $C_{ab}(\tau)$의 분포를 조사해보자.

$a\alpha^{\tau}+b=A(\tau)$, $\alpha^{d\tau}+1=B(\tau)$ 에서 $\tau=(2^m+1)k$ $(0\le k\le 2^m-2)$ 이면 $\alpha^{\tau}\in GF(2^m)$이고 따라서 $A(\tau)\in GF(2^m)$, $B(\tau)\in GF(2^m)$이다.

따라서 (18)은 $A(\tau)y^4+B(\tau)y^3+B(\tau)y+A(\tau)=0$이고 인수분해하면

$$(y^2+1)\{A(\tau)y^2+B(\tau)y+A(\tau)\}=0 \quad (19)$$

이다.

(i) $B(\tau)=0$이면 $k=\tau=0$이고 (19)는 $y=1$을 4중근으로 갖는다.

(ii) $B(\tau)\neq 0$, $Tr_1^n\left(\frac{A(\tau)^2}{B(\tau)^2}\right)=0$ 이면 (19)는 $(y+1)^2=0$ 에서 $y=1$을 중근으로 갖고 $A(\tau)y^2+B(\tau)y+A(\tau)=0$ 에서 1이 아닌 서로 다른 두 근을 갖는다.

(iii) $B(\tau)\neq 0$, $Tr_1^n\left(\frac{A(\tau)^2}{B(\tau)^2}\right)=1$ 이면 (19)는 $(y+1)^2=0$ 에서 $y=1$을 중근으로 갖고 $A(\tau)y^2+B(\tau)y+A(\tau)=0$ 에서는 근을 갖지 않는다.

(i), (ii), (iii)에 의해서 (19)는 근을 1개 또는 3개를 갖게 되므로 $C_{ab}(\tau)=\{-1, -1+2\cdot 2^m\}$의 두 값만 갖게 된다.

지금부터 3개의 근을 갖는 τ의 개수를 조사해 보자.

$Tr_1^n\left(\frac{A(\tau)^2}{B(\tau)^2}\right)=0$은 $Tr_1^m\left(\frac{A(\tau)}{B(\tau)}\right)=1$과 동치이고 다음과 같은 식이 성립한다.

$$\frac{A(\tau)}{B(\tau)}=\frac{a\alpha^{\tau}+b}{\alpha^{d\tau}+1}=\frac{a\alpha^{(2^m+1)k}+b}{\alpha^{d(2^m+1)k}+1}=\frac{a\beta^k+b}{\beta^k+1}$$
$$=\frac{a\beta^k+a+a+b}{\beta^k+1}=a+\frac{a+b}{\beta^k+1}$$

그리고 아래 식이 성립한다.

$$\left\{\frac{a+b}{\beta^k+1}\mid 1\le k\le 2^m-2\right\}=GF(2^m)\backslash\{0, a+b\} \quad (20)$$

$Tr_1^m\left(a+\frac{a+b}{\beta^k+1}\right)=1$인 k의 개수가 상호상관함수가 $-1+2\cdot 2^m$인 개수이다.

(a) $Tr_1^m(a)=0$, $Tr_1^m(b)=0$인 경우

$Tr_1^m\left(a+\frac{a+b}{\beta^k+1}\right)=1$이기 위해서는 $Tr_1^m\left(\frac{a+b}{\beta^k+1}\right)=1$이다.

$Tr_1^m(a+b)=0$ 이므로 (20)에 의해서 $Tr_1^m\left(\frac{a+b}{\beta^k+1}\right)=1$이 되는 k의 개수는 2^{m-1} 개 이다.

(b) $Tr_1^m(a)=0$, $Tr_1^m(b)=1$인 경우

$Tr_1^m\left(a+\frac{a+b}{\beta^k+1}\right)=1$이기 위해서는 $Tr_1^m\left(\frac{a+b}{\beta^k+1}\right)=1$이다.

$Tr_1^m(a+b)=1$이므로 (20)에 의해서 $Tr_1^m\left(\frac{a+b}{\beta^k+1}\right)=1$이 되는 k의 개수는 $2^{m-1}-1$ 개 이다.

(c) $Tr_1^m(a)=1$, $Tr_1^m(b)=0$인 경우

$Tr_1^m\left(a+\frac{a+b}{\beta^k+1}\right)=1$이기 위해서는 $Tr_1^m\left(\frac{a+b}{\beta^k+1}\right)=0$이다.

$Tr_1^m(a+b)=1$이므로 (20)에 의해서 $Tr_1^m\left(\frac{a+b}{\beta^k+1}\right)=0$이 되는 k의 개수는 $2^{m-1}-1$ 개 이다.

(d) $Tr_1^m(a)=1$, $Tr_1^m(b)=1$인 경우

$Tr_1^m\left(a+\frac{a+b}{\beta^k+1}\right)=1$이기 위해서는 $Tr_1^m\left(\frac{a+b}{\beta^k+1}\right)=0$이다. $Tr_1^m(a+b)=0$이므로 (20)에 의해서 $Tr_1^m\left(\frac{a+b}{\beta^k+1}\right)=0$이 되는 k의 개수는 $2^{m-1}-2$ 개 이다.

아래의 표는 α가 $x^8+x^4+x^3+x^2+1$의 원시근 이고 β가 x^4+x+1의 원시근인 경우 a, b값에 따라서 위상이동차 $\tau=(2^4+1)k$ $(0\le k\le 2^4-2)$인 경우에 대한 $C_{ab}(\tau)$를 계산한 것이다.

표 1. $\tau=(2^4+1)k$ $(0\le k\le 2^4-2)$인 경우의 $C_{ab}(\tau)$
Table. 1 $C_{ab}(\tau)$ when phase shift $\tau=(2^4+1)k$ $(0\le k\le 2^4-2)$

$A(\tau)$ / τ	(1) $a=\beta^2$ $b=\beta^5$	(2) $a=\beta$ $b=\beta^4$	(3) $a=\beta^1$ $b=\beta^3$	(4) $a=\beta^5$ $b=\beta^{11}$	(5) $a=\beta^{12}$ $b=\beta^5$	(6) $a=\beta^9$ $b=\beta^8$	(7) $a=\beta^7$ $b=\beta^{13}$	(8) $a=\beta^{11}$ $b=\beta^{14}$
0	-1	-1	-1	-1	-1	-1	-1	-1
17	31	31	31	31	31	31	31	-1
34	-1	31	31	-1	-1	31	-1	31
51	-1	-1	-1	-1	31	-1	-1	-1
68	-1	31	31	-1	-1	-1	31	-1
85	31	-1	31	-1	31	31	31	31
102	31	-1	31	-1	31	-1	-1	-1
119	31	31	31	31	31	-1	-1	31
136	31	31	-1	-1	-1	31	-1	31
153	31	-1	-1	31	-1	31	-1	-1
170	31	-1	-1	31	-1	-1	31	31
187	-1	31	-1	31	31	31	31	-1
204	-1	-1	31	31	-1	31	-1	-1
221	-1	31	-1	31	31	-1	-1	31
238	31	31	-1	-1	-1	-1	31	-1

(1),(2)의 경우 $Tr_1^4(a)=0$, $Tr_1^4(b)=0$이므로 $C_{ab}(\tau)=-1+2\cdot 2^4$가 되는 τ가 2^{4-1}개 발생하고 $C_{ab}(\tau)=-1$인 τ가 $2^{4-1}-1$개 발생한다.

(3),(4)의 경우 $Tr_1^4(a)=0$, $Tr_1^4(b)=1$이므로 $C_{ab}(\tau)=-1+2\cdot 2^4$가 되는 τ가 $2^{4-1}-1$개 발생하고 $C_{ab}(\tau)=-1$인 τ가 2^{4-1}개 발생한다.

(5),(6)의 경우 $Tr_1^4(a)=1$, $Tr_1^4(b)=0$이므로 $C_{ab}(\tau)=-1+2\cdot 2^4$가 되는 τ가 $2^{4-1}-1$개 발생하고 $C_{ab}(\tau)=-1$인 τ가 2^{4-1}개 발생한다.

(7),(8)의 경우 $Tr_1^4(a)=1$, $Tr_1^4(b)=1$이므로 $C_{ab}(\tau)=-1+2\cdot 2^4$가 되는 τ가 $2^{4-1}-2$개 발생하고 $C_{ab}(\tau)=-1$인 τ가 $2^{4-1}+1$개 발생한다.

V. 결 론

본 논문에서는 유한체 지식을 바탕으로 하여 4차 방정식을 유도하는 방식으로 Niho type의 데시메이션 $d=2^{m-2}(2^m+3)$인 경우의 비선형수열 $S_a^r(t)=Tr_1^m\{[Tr_m^n(a\alpha^t+\alpha^{dt})]^r\}$에서 나타날 수 있는 상호상관함수가 최대 5값을 갖는다는 것을 보였다. 그리고 $\tau=(2^m+1)k$ $(0\le k\le 2^m-2)$인 경우에는 상호상관함수가 -1, $-1+2\cdot 2^m$의 두 가지 값만 나타나는 $S_a^r(t)$의 상호상관함수의 분포를 분석하고 몇 가지 경우의 실험을 통하여 분석결과를 확인하였다. 앞으로 다양한 데시메이션 값에 대한 비선형수열의 상호상관함수 분석에 대한 연구가 계속되어야 하겠다.

참고문헌

[1] T. Helleseth and P.V. Kumar, “Sequences with low correlation,” in Handbook of Coding Theory, ed. V. Pless and C. Huffman, Elsevier, Amsterdam, The Netherlands, 1998.

[2] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, “Spread spectrum communication,” vol.I, Computer Science Press, Rockville, MD, 1985.

[3] J. Foerster, “The performance of a direct-sequences spread ultra wideband system in the presence of multipath, narrowband, interference, and multiuser interference,” Proc. IEEE Int. Conf. on Ultra Wideband Systems and Technologies, pp.87-91, 2002.

[4] K. Fazel and S. Kaiser, “Multi-carrier and spread spectrum system,” John Wiley and Sons Ltd., 2003.

[5] M. K. Simon, J. K. Omura, R. K. Scholtz and B. K.

Levitt, “Spread spectrum communications handbook,” McGraw-Hill, Inc., 1994.

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

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

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

[9] R. Gold, “Maximal recursive sequences with 3-valued recursive cross-correlation functions,” IEEE Trans. Inf. Theory, vol. IT-14, no. 1, pp. 154-156, Jan. 1968.

[10] T. Kasami, “Weight distribution formula for some class of cyclic codes,” Coordinated Science Laboratory, University of Illinois, Urbana, Tech. Rep. R-285(AD632574), 1966.

[11] J. S. No and P. V. Kumar, “A New Family of Binary Pseudorandom Sequences Having Optimal Periodic Correlation Properties and Large Linear Span,” IEEE Trans. Inform. Theory, vol. 35, no. 2, pp. 371-379, Mar. 1989.

[12] S.W. Golomb, “Shift register sequences,” Holden-Day, Inc, 1967.

[13] 조성진 외 2인, “알기 쉬운 유한체론,” 경문사, 2005.

저자소개

조성진(Sung-Jin Cho)

1979년 2월: 강원대학교 수학교육과 학사
1981년 2월: 고려대학교 수학과 석사
1988년 2월: 고려대학교 수학과 박사
1988년 ~ 현재: 부경대학교 응용수학과 정교수
※관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론

임지미(Ji-Mi Yim)

1997년 2월: 부산대학교 수학교육과 학사
2008년 8월: 부경대학교 교육대학원 수학과 석사
2008년 ~ 현재: 부경대학교 응용수학과 박사과정
※관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론