Regular paper http://dx.doi.org/10.13067/JKIECS.2013.8.6.891

최대 주기를 갖는 이진 수열의 상호상관 함숫값의 분포

권민정* · 조성진**

The distribution of the values of the cross-correlation function between the maximal period binary sequences

Min-Jeong Kwon* · Sung-Jin Cho**

요 약

최대 주기를 갖는 이진 수열에 대한 상호상관 함숫값은 통신 분야에서 다양하게 응용되고 있기 때문에 그 값의 범위와 발생빈도에 대한 분석은 다양하게 연구되고 있다. 본 논문에서는 데시메이션 $d=2^{m-1}(3\cdot 2^m-1)$ 를 이용하여 새로운 수열군을 제안하고 그 수열의 상호상관 함숫값의 범위와 분포에 대하여 분석한다.

ABSTRACT

The spectrum and the number of the values of the cross-correlation function between the maximal period binary sequences have been extensively studied because of their importance in communications applications. In this paper, we propose the new family of the sequences using the decimation $d=2^{m-1}(3\cdot 2^m-1)$. And we find the spectrum of the cross-correlation function of the sequences and analyze the number of times each value occurs for $0\le\tau\le 2^n-2$.

키워드

Cross-Correlation, Auto-Correlation, Phase Shift, Decimation, Trace
상호상관함수, 자기상관함수, 위상이동차, 데시메이션, 트레이스

Ⅰ. 서 론

의사난수열은 대역확산통신 시스템 및 스트림 암호화 방식(RC4, A5, SEAL) 등에서 적은 양의 키를 가지고 긴 난수열을 생성하기 위해 많이 사용되고 있다[1]. 이때 사용되는 확산 코드는 송수신자 사이에서는 동기가 맞는 동일 코드를 사용하지만 다수의 사용자에게는 서로 다른 코드를 부여하여야 하고 암호학적으로도 안전해야 한다. 선형복잡도와 상관관계는 수열생성기의 안전성을 검증하는 대표적인 방법이다[2,3]. 선형복잡도가 클수록 대수적 공격에 의하여 해독되기 어려우며, 상호상관 관계가 낮을수록 여러 사용자가 동시에 사용하는 경우에도 다중접속 충돌이 낮아진다. 따라서 선형복잡도는 크고 상호상관관계는 낮은 수열생성에 관한 연구가 다양하게 진행되고 있다[1,4~6]. 특히 최대 주기를 갖는 이진 수열의 상호상관 함숫값은 통신 분야에서 중요하게 사용되기 때문에 Golomb[7]이 처음으로 연구한 이후부터 지금까지 꾸준히

* 부경대학교 응용수학과(mjblack02@hanmail.net)
** 교신저자(corresponding author) : 부경대학교 응용수학과(sjcho@pknu.ac.kr)
접수일자 : 2013. 04. 15 심사(수정)일자 : 2013. 05. 10 게재확정일자 : 2013. 06. 11

연구되고 있다[8~10]. 최대 주기를 갖는 이진 수열의 선택이 아니라 데시메이션의 값에 의해 상호상관 함숫값이 결정된다는 것은 잘 알려져 있으며, 상호상관 함숫값의 범위와 발생 빈도를 분석하는 것이 중요한 문제가 되었다[8,11,12]. 본 논문에서는 데시메이션 $d=2^{m-1}(3\cdot 2^m-1)$을 이용하여 새로운 수열군을 제안하고 수열의 상호상관 함숫값의 범위와 발생 빈도에 대하여 분석하겠다.

II. 사전지식

의사난수열 생성기를 설계하고 연구하기 위해 중요한 수학적 도구인 트레이스(trace) 함수는 유한체 $GF(2^n)$에서 그것의 부분체 $GF(2^m)$ 위로 대응되는 선형함수이다. 트레이스 함수는

$$Tr_m^n(x)=\sum_{i=0}^{\frac{n}{m}-1}x^{2^{m\cdot i}}=x+x^{2^m}+x^{2^{2m}}+\cdots+x^{2^{\left(\frac{n}{m}-1\right)m}}$$

로 정의되며 $a,b\in GF(2^n)$, $x,y\in GF(2^m)$에 대하여 다음과 같은 성질을 갖는다.

(a) $Tr_m^n(ax+by)=aTr_m^n(x)+bTr_m^n(y)$,

(b) $Tr_m^n\left(x^{2^m}\right)=Tr_m^n(x)$,

(c) $Tr_1^n(x)=Tr_1^m\left(Tr_m^n(x)\right)$,

(d) $Tr_m^n(x)=a$를 만족하는 $GF(2^m)$의 원소 x의 개수는 2^{n-m}.

상관함수는 두 현상 사이의 유사성 또는 관계성을 측정하기 위해 사용되는 수학적 도구로써 함숫값이 0에 가까울수록 관계가 적음을 나타낸다. 위상이동차 τ에 대하여 주기가 2^n-1인 두 수열 $x(t)$와 $y(t)$의 상관함수 $C(\tau)$ ($\tau=0,1,\cdots,2^n-2$)는

$$C(\tau)=\sum_{t=0}^{2^n-2}(-1)^{x(t+\tau)+y(t)}$$

으로 정의된다. 이 때 두 수열 $x(t)$와 $y(t)$가 같으면 자기상관함수, 다르면 상호상관함수라 한다. 주기가 2^n-1이면서 자기상관 함숫값의 범위가 이상적인 수열로는 m-수열, GMW 수열, generalized GMW 수열이 있다[4,7,13]. 상관함수에 대한 내용은 [14]에 자세히 설명되어 있다.

보조정리 2.1.[15] $n=2m$을 만족하는 n,m에 대하여 $GF(2^n)$의 원시원소 α는 $\delta^{2^m}=\delta$, $\gamma^{2^m}=\gamma^{-1}$을 만족하는 δ, γ를 이용하여 다음과 같이 나타낼 수 있다.

$$\alpha=\delta\gamma$$

$n=2m$을 만족하는 n,m에 대하여, $x^{2^m}=\bar{x}$로 간단히 표기하고 $S=\{x\mid x\bar{x}=1,\ x\in GF(2^n)\}$로 정의하면 집합 S의 원소는 다음과 같은 성질을 갖는다.

보조정리 2.2. $n=2m$을 만족하는 n,m과 집합 S에 대하여, $x\in S$이면 $\bar{x}\in S$이다.

증명. $x\in S$이므로 $x\bar{x}=1$이고, $\bar{\bar{x}}=x$이므로 $x\bar{x}=\bar{x}x=\bar{x}\bar{\bar{x}}=1$을 만족한다. 따라서 $\bar{x}\in S$이다.

보조정리 2.3.[16] $n=2m$을 만족하는 n,m과 집합 S에 대하여

$$GF(2^m)\cap S=\{1\}$$

이다.

III. 이차방정식의 해의 개수

보조정리 3.1.[14] $m|n$을 만족하는 n,m과 $\alpha\in GF(2^n)$에 대하여 $Tr_m^n(\alpha)=0$일 필요충분조건은 $\alpha=\beta^{2^m}+\beta$를 만족하는 $\beta\in GF(2^n)$가 존재한다는 것이다.

예제 3.2. $n=4$, $m=1$일 때 $\alpha^4=\alpha+1$을 만족하는 $GF(2^n)$의 원시원소 α에 대하여 $Tr_1^4(\alpha^4)=0$이다. 이때 $\beta^2+\beta=\alpha^4$을 만족하는 $\beta=\alpha^6$이다.

보조정리 3.1과 트레이스 함수의 성질을 이용하면 이차방정식

$$ax^2+bx+c=0,\ a,b,c\in GF(2^n) \tag{1}$$

을 만족하는 해의 개수를 구할 수 있다.

(i) $b\neq 0$: $y=ab^{-1}x$, $\kappa=acb^{-2}$이라 두면 방정식 (1)

은 $y^2+y=\kappa$가 된다. 보조정리 2.1에 의하여 $y^2+y=\kappa$의 해가 존재할 필요충분조건은 $Tr_1^n(\kappa)=0$이다. 이차방정식 $y^2+y=\kappa$의 해가 존재할 경우 방정식 (1)의 해는 $x=ba^{-1}y, ba^{-1}(y+1)$이다.

(ii) $b=0$: $\kappa=\alpha a^{-1}$이라 두면 방정식 (1)은 $x^2=\kappa$가 되고 방정식 $x^2=\kappa$는 $x=\kappa^{2^{n-1}}$을 중근으로 갖는다.

예제 3.3. $\alpha^4=\alpha+1$을 만족하는 $GF(2^n)$의 원시원소 α에 대하여 이차방정식 $x^2+\alpha^4x+\alpha=0$의 해를 구해보자.

$y=\alpha^{-4}x=\alpha^{11}x$, $\gamma=\alpha\cdot\alpha^{-8}=\alpha^8$라 두면 이차방정식 $x^2+\alpha^4x+\alpha=0$는 $y^2+y=\alpha^8$가 된다. $Tr_1^8(\alpha^8)=0$이므로 방정식 $y^2+y=\alpha^8$의 해가 존재한다. $y=\alpha^{12}$은 $y^2+y=\alpha^8$을 만족하므로 해는 $y=\alpha^{12}$ 또는 $y=\alpha^{12}+1=\alpha^{11}$이다. $x=\alpha^4y$로부터 방정식 $x^2+\alpha^4x+\alpha=0$의 해는 $x=\alpha$ 또는 $x=1$이다.

정리 3.4. $n=2m$을 만족하는 n,m과 이차방정식의 해집합을 $R=\{x\in S\,|\,x^2+kx+1=0, k\in GF(2^m)^*\}$로 정의하면

$$|R|=0 \text{ or } 2$$

이다.

증명. $k\in GF(2^m)^*$일 때, 집합 S의 원소이면서 이차방정식

$$x^2+kx+1=0 \tag{2}$$

을 만족하는 x는 최대 2개까지 가능하다. $|R|=1$인 경우는 방정식 (2)가 중근을 가지면서 그것이 집합 S의 원소일 때, 방정식 (2)가 2개의 해를 갖지만 그 중 하나만 집합 S의 원소일 때이다.

(i) 방정식 (2)가 중근을 가지면서 그것이 집합 S의 원소인 경우 : $k\in GF(2^m)^*$이므로 방정식 (2)는 완전제곱식이 될 수 없다. 따라서 중근을 갖는 경우는 발생하지 않는다.

(ii) 방정식 (2)가 서로 다른 2개의 해를 갖지만 그 중 하나만 집합 S의 원소일 때 : 보조정리 3.1에 의하여 $n=2m$을 만족하는 n, m과 $k\in GF(2^m)^*$에 대하여 항상 $Tr_1^n\left(\frac{1}{k^2}\right)=0$이므로 방정식 (2)의 해는 모두 $GF(2^n)$에 존재한다. 방정식 (2)를 만족하는 $GF(2^n)$의 서로 다른 두 원소를 x_1, x_2라 하고 $x_1\in S$라 하자. $x_1\in S$이므로 보조정리 2.2에 의해 $\overline{x_1}\in S$이다. 근과 계수의 관계에 의해 $x_1x_2=1$이고 가정에 의해 $x_1\in S$이므로 $x_1\overline{x_1}=1$이다. 따라서 $x_2=\overline{x_1}$이므로 $x_2\in S$이다. 즉, x_1이 S의 원소이면 x_2도 S의 원소이다. 따라서 방정식 (2)가 서로 다른 2개의 해를 갖지만 그 중 하나만 집합 S의 원소인 경우는 발생하지 않는다.

(i), (ii)에 의하여 $|R|=1$ 인 경우는 발생하지 않으므로 $|R|=0$ or 2 이다. □

Ⅳ. 최대 주기를 갖는 이진 수열의 상호상관 함숫값의 분포

이제 $n=2m$을 만족하는 n,m과 $\gcd(r,2^m-1)=1$을 만족하는 r, $d=2^{m-1}(3\cdot 2^m-1)$에 대하여 새로운 수열군을 다음과 같이 정의한다.

$$S^r:=\left\{s_a^r(t)\,|\,a\in GF(2^m), 0\le t\le 2^n-2\right\},$$
$$s_a^r(t):=Tr_1^m\left(\left[Tr_n^m(a\alpha^t+\alpha^{dt})\right]^r\right).$$

수열군 S^r에서 위상이동차 $\tau(0\le\tau\le 2^n-2)$에 대하여 두 수열 $s_a^r(t)$, $s_b^r(t)$에 대한 상호상관함수는

$$C_{a,b}(\tau)=\sum_{t=0}^{2^n-2}(-1)^{s_a^r(t+\tau)+s_b^r(t)}$$

로 나타낸다. 제안된 수열군 S^r은 Choi 등의 연구결과와 같은 범위의 상호상관 함숫값을 갖는다[17].

정리 4.1. 수열군 S^r에서 $C_{a,b}(\tau)$는 5값 함수이며

$$C_{a,b}(\tau)\in\{-2^m-1,-1,2^m-1,2\cdot 2^m-1,3\cdot 2^m-1\}$$

이다.

증명. 수열군 S^r의 두 수열 $s_a^r(t)$, $s_b^r(t)$에 대한 상호상관함수는

$$C_{a,b}(\tau)=\sum_{t=0}^{2^n-2}(-1)^{s_a^r(t+\tau)+s_b^r(t)}$$

$$= \sum_{t=0}^{2^n-2} (-1)^{Tr_1^m\left(\left[Tr_m^n\left(a\alpha^{t+\tau}+\alpha^{d(t+\tau)}\right)\right]^r+\left[Tr_m^n\left(b\alpha^t+\alpha^{dt}\right)\right]^r\right)}$$

이다. 여기서 $Q=2^m+1$로 두고 $t=t_1Q+t_2(0\le t_1\le 2^m-2,\ 0\le t_2\le 2^m)$, $\alpha^Q=\beta$라 두면 $\beta\in GF(2^m)^*$이다. 그러면

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

이고 $\left\{\beta^{t_1r}\mid 0\le t_1\le 2^m-2, \gcd(r,2^m-1)=1\right\}=GF(2^m)^*$이므로 $s_a^r(t+\tau)+s_b^r(t)=Tr_1^m(\eta H(t_2,\tau,r))$이다. 여기서

$$H(t,\tau,r)=\left[Tr_m^n\left(a\alpha^{t+\tau}+\alpha^{d(t+\tau)}\right)\right]^r+\left[Tr_m^n\left(b\alpha^t+\alpha^{dt}\right)\right]^r$$

이다. 따라서

$$C_{a,b}(\tau)=\sum_{\eta\in GF(2^m)}\sum_{t_2=0}^{2^m}(-1)^{Tr_1^m(\eta H(t_2,\tau,r))}-(2^m+1)$$

이고 $N(t,\tau,r)=|\{t\mid H(t,\tau,r)=0,\ 0\le t\le 2^m\}|$ 라 두면 $C_{a,b}(\tau)=(N(t_2,\tau,r)-1)2^m-1$이다. 이제 $N(t_2,\tau,r)$의 값을 구하기 위해 $H(t_2,\tau,r)=0$을 만족시키는 t_2의 개수가 필요하다.

$$H(t_2,\tau,r)=0$$
$$\Leftrightarrow \left[Tr_m^n\left(a\alpha^{t_2+\tau}+\alpha^{d(t_2+\tau)}\right)\right]^r=\left[Tr_m^n\left(b\alpha^{t_2}+\alpha^{dt_2}\right)\right]^r$$

이고 $\gcd(r,2^m-1)=1$이므로

$$\Leftrightarrow Tr_m^n\left(a\alpha^{t_2+\tau}+\alpha^{d(t_2+\tau)}\right)=Tr_m^n\left(b\alpha^{t_2}+\alpha^{dt_2}\right)$$

이다. 따라서 $Tr_m^n\left(a\alpha^{t_2+\tau}+\alpha^{d(t_2+\tau)}+b\alpha^{t_2}+\alpha^{dt_2}\right)=0$을 만족하는 t_2의 개수를 구하면 된다.

$$Tr_m^n\left(a\alpha^{t_2+\tau}+\alpha^{d(t_2+\tau)}+b\alpha^{t_2}+\alpha^{dt_2}\right)$$
$$= Tr_m^n\left((a\alpha^\tau+b)\alpha^{t_2}+(\alpha^{d\tau}+1)\alpha^{dt_2}\right)$$

이다. 여기서 $A(\tau)=\alpha^{d\tau}+1$, $B(\tau)=a\alpha^\tau+b$로 두고 보조정리 2.1을 이용하여 $\alpha=\delta\gamma$로 표현하면 $d\equiv 1\pmod{2^m-1}$, $d\equiv 2\pmod{2^m+1}$ 이므로

$$Tr_m^n\left(B(\tau)\alpha^{t_2}+A(\tau)\alpha^{dt_2}\right)$$
$$= A(\tau)\alpha^{dt_2}+B(\tau)\alpha^{t_2}+\overline{A(\tau)}\alpha^{2^mdt_2}+\overline{B(\tau)}\alpha^{2^mt_2}$$
$$= A(\tau)\delta^{dt_2}\gamma^{dt_2}+B(\tau)\delta^{t_2}\gamma^{t_2}+\overline{A(\tau)}\delta^{2^mdt_2}\gamma^{2^mdt_2}+\overline{B(\tau)}\delta^{2^mt_2}\gamma^{2^mt_2}$$
$$= A(\tau)\delta^{t_2}\gamma^{2t_2}+B(\tau)\delta^{t_2}\gamma^{t_2}+\overline{A(\tau)}\delta^{t_2}\gamma^{-2t_2}+\overline{B(\tau)}\delta^{t_2}\gamma^{-t_2}$$
$$= 0$$

이다. $\gamma^{t_2}=x$로 치환하면 $x\in S$이고 $\delta^{t_2}\ne 0$이므로

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

이다. 방정식 (3)은 x에 관한 4차식이므로 최대 4개의 해가 존재할 수 있고 $N(t_2,\tau,r)=0,1,2,3,4$이므로 $C_{a,b}(\tau)\in\{-2^m-1,-1,2^m-1,2\cdot 2^m-1,3\cdot 2^m-1\}$이다. □

특별히 $a=0$, $b\ne 0$일 때, 위상이동차 $\tau=Q\tau_1(0\le\tau_1\le 2^m-2)$에 대한 $C_{0,b}(\tau)$의 분포는 다음과 같다.

정리 4.2. 수열군 S^r에서 위상이동차 $\tau=Q\tau_1$ $(0\le\tau_1\le 2^m-2)$, $b\ne 0$에 대하여 $C_{0,b}(\tau)$의 발생빈도는

$$Tr_1^m\left(\frac{1}{b}\right)=1:\begin{cases}C_{0,b}(\tau)=2\cdot 2^m-1, & 2^{m-1}-1\ times\\ C_{0,b}(\tau)=-1, & 2^{m-1}\ times\end{cases},$$
$$Tr_1^m\left(\frac{1}{b}\right)=0:\begin{cases}C_{0,b}(\tau)=2\cdot 2^m-1, & 2^{m-1}\ times\\ C_{0,b}(\tau)=-1, & 2^{m-1}-1\ times\end{cases}$$

이다.

증명. 첫 번째 단계로, 발생 가능한 상호상관 함숫값은 무엇인지 살펴보자. $a=0$, $b\ne 0$이므로 방정식 (3)에서 $B(\tau)=b$이고, $\tau=Qt_1(0\le\tau_1\le 2^m-2)$이므로 $\overline{A(\tau)}=A(\tau)$이다. 따라서 방정식 (3)은

$$A(\tau)x^4+bx^3+bx+A(\tau)=0 \quad (4)$$

이다. 방정식 (4)는 최대 4개의 해를 가질 수 있고 $A(\tau)x^4+bx^3+bx+A(\tau)=(x+1)^2(A(\tau)x^2+bx+A(\tau))=0$ 이므로 $x=1$ 이외의 다른 해의 개수는 방정식

$$A(\tau)x^2+bx+A(\tau)=0 \quad (5)$$

이 집합 S에서 몇 개의 해를 갖는지 확인하면 알 수 있다. $A(\tau)\in GF(2^m)$, $b\in GF(2^m)^*$이므로 정리 3.4에 의하여 방정식 (5)는 $GF(2^n)$에서 항상 2개의 해를 갖는다. 이제 2개의 해가 모두 집합 S의 원소인지 확인해야 한다.

(i) $Tr_1^m\left(\frac{A(\tau)^2}{b^2}\right)=0$이면 방정식 (5)의 해는 모두 $GF(2^m)$에 존재한다. 그러나 보조정리 2.3에 의해 $GF(2^m)\cap S=\{1\}$ 이므로 이 경우 방정식 (5)의 해는 모두 집합 S의 원소가 아니다. 중근 $x=1$을 고려하면 방정식 (4)의 해는 1개이므로 $C_{0,b}(\tau)=-1$이다.

(ii) $Tr_1^m\left(\frac{A(\tau)^2}{b^2}\right)=1$이면 방정식 (5)의 두 해는 모두 $GF(2^n)\setminus GF(2^m)$에 존재하고, 근과 계수의 관계 및 보조정리 2.2에 의해 두 해는 모두 집합 S의 원소이다.

따라서 중근 $x=1$을 포함하면 방정식 (4)의 해는 모두 3개, 즉 $N(t_2,\tau,r)=3$이므로 $C_{0,b}(\tau)=2\cdot 2^m-1$이다.

(i), (ii)에 의해 $\tau=Qt_1(0\le\tau_1\le 2^m-2)$일 때 $C_{0,b}(\tau)$의 값은 -1, $2\cdot 2^m-1$만 가능하다.

두 번째 단계로, $C_{0,b}(\tau)=-1$, $C_{0,b}(\tau)=2\cdot 2^m-1$의 발생빈도를 분석하겠다.

$Tr_1^m\left(\frac{A(\tau)^2}{b^2}\right)$에서 $A(\tau)\neq 1$이므로 $\frac{A(\tau)}{b}\neq\frac{1}{b}$이다. 따라서 $Tr_1^m\left(\frac{A(\tau)^2}{b^2}\right)$의 값 중 0과 1의 개수는 $Tr_1^m\left(\frac{1}{b^2}\right)$의 값에 따라 달라지고 트레이스 함수의 성질 (b)에 의하여 $Tr_1^m\left(\frac{1}{b^2}\right)=Tr_1^m\left(\frac{1}{b}\right)$이므로 간단히 $Tr_1^m\left(\frac{1}{b}\right)$의 값을 생각하면 된다.

(a) $Tr_1^m\left(\frac{1}{b}\right)=0$: $Tr_1^m\left(\frac{A(\tau)}{b}\right)$의 값 중 0인 것이 하나 빠지게 되므로 $Tr_1^m\left(\frac{A(\tau)}{b}\right)=\begin{cases}0\ ,\ 2^{m-1}-1\ times\\ 1\ ,\ 2^{m-1}\ times\end{cases}$ 이다. 따라서 $\tau=Q\tau_1(0\le\tau_1\le 2^m-2)$일 때, $C_{0,b}(\tau)=-1$은 $2^{m-1}-1$번, $C_{0,b}(\tau)=2\cdot 2^m-1$은 2^{m-1}번 나타난다.

(b) $Tr_1^m\left(\frac{1}{b}\right)=1$: $Tr_1^m\left(\frac{A(\tau)}{b}\right)$의 값 중 1인 것이 하나 빠지므로 $Tr_1^m\left(\frac{A(\tau)}{b}\right)=\begin{cases}0\ ,\ 2^{m-1}\ times\\ 1\ ,\ 2^{m-1}-1\ times\end{cases}$ 이다. 따라서 (a),(b)에 의하여 $\tau=Q\tau_1(0\le\tau_1\le 2^m-2)$일 때 $C_{0,b}(\tau)=-1$은 2^{m-1}번, $C_{0,b}(\tau)=2\cdot 2^m-1$은 $2^{m-1}-1$번 나타난다. □

예제 4.3. $n=8$, $m=4$이고 $a=0$, $b=\beta$일 때, $\tau=17\tau_1(0\le\tau_1\le 14)$에 대한 $C_{0,\beta}(\tau)$ 값의 분포를 살펴보자.

$Tr_1^m\left(\frac{1}{b}\right)=Tr_1^m(\beta^{14})=1$이어서 $Tr_1^m\left(\frac{A(\tau)}{b}\right)$의 값 중 1인 것이 하나 빠지게 되므로 $Tr_1^m\left(\frac{A(\tau)}{b}\right)=1$은 7번, $Tr_1^m\left(\frac{A(\tau)}{b}\right)=0$은 8번 발생한다. 따라서 해의 개수가 3개인 것은 7번, 해의 개수가 1개인 것은 8번 존재한다.

τ 값에 따른 $C_{0,\beta}(\tau)$ 값을 $(2^m-1)\times(2^m+1)$ 배열로 나타내면 $\tau=17\tau_1(0\le\tau_1\le 14)$일 때의 $C_{0,\beta}(\tau)$ 값은 그림 1과 같이 첫 열에 분포하고 $C_{0,\beta}(\tau)=31$이 7개, $C_{0,\beta}(\tau)=-1$이 8개 존재한다.

-1	-17	-17	15	-1	-1	15	-17	15	-17	-17	-1	-17	-17	-1	47	-17
31	-1	-1	-17	-1	-1	47	-17	-1	15	-1	-1	-17	-1	15	-17	-1
31	15	-17	-1	-1	-1	15	-17	-1	-1	-1	15	-1	-17	15	-1	15
31	-1	-17	-17	-17	15	-1	-17	-1	-17	-1	15	15	-1	-17	-17	-1
-1	-1	-17	-1	15	15	15	-1	-17	15	-17	15	-1	-1	-1	-17	-1
31	-1	-1	-1	-17	15	15	15	-17	-17	15	15	-1	-1	-17	-17	-1
31	-17	-17	-1	15	-17	47	-17	15	-1	-17	47	-1	-17	-1	-1	-17
-1	-17	-1	15	-17	-17	-1	47	-17	15	-17	15	15	15	-1	-17	-17
-1	15	-1	-17	15	-17	15	-1	-17	-1	-17	-1	15	-17	-1	-1	15
31	15	-1	-17	-1	-1	-1	-17	15	-1	-17	15	15	15	15	-1	15
-1	-17	15	-17	-17	-17	-1	-1	-1	-1	-1	15	-17	-17	-17	-1	-17
31	-17	-17	-17	15	-17	-1	-1	-17	-17	15	47	-17	15	-17	15	-17
-1	-1	-17	15	-17	-17	15	-1	15	-17	-17	-1	-17	-1	-17	-17	-1
-1	15	15	-1	-1	-1	15	-17	-17	15	47	15	-1	-17	-17	-17	15
-1	-17	47	15	-17	15	15	15	-1	-17	-1	-1	-17	15	15	15	-17

그림 1. $C_{0,\beta}(\tau)(0\le\tau\le 2^n-2)$의 배열
Fig. 1 The array of the value $C_{0,\beta}(\tau)$ for $0\le\tau\le 2^n-2$

예제 4.4. $n=8$, $m=4$일 때, $a=0$, $b=\beta^7$인 경우 $\tau=17\tau_1(0\le\tau_1\le 14)$에 대한 $C_{0,\beta^7}(\tau)$ 값의 분포를 살펴보자.

$Tr_1^m\left(\frac{1}{b}\right)=Tr_1^m\left(\frac{1}{\beta^7}\right)=Tr_1^m(\beta^8)=0$이므로 $Tr_1^m\left(\frac{A(\tau)}{b}\right)$의 값 중 0인 것이 하나 빠지게 되어 $Tr_1^m\left(\frac{A(\tau)}{b}\right)=1$은 8번, $Tr_1^m\left(\frac{A(\tau)}{b}\right)=0$은 7번 발생하게 된다. 따라서 해의 개수가 3개인 것은 8번, 해의 개수가 1개인 것은 7번 존재한다.

τ의 값에 따른 $C_{0,\beta^7}(\tau)$를 $(2^m-1)\times(2^m+1)$ 배열로 나타내면 $\tau=17\tau_1(0\le\tau_1\le 14)$일 때 $C_{0,\beta^7}(\tau)$ 값은 그림 2의 첫 열에 분포하고 $C_{0,b}(\tau)=31$인 것은 8개, $C_{0,b}(\tau)=-1$인 것은 7개 발생한다.

-1	-17	-1	-17	-1	-1	-1	15	15	-1	-17	15	15	-17	-17	-1	-17
31	-17	-17	15	-17	-17	-1	-1	-1	-1	-1	-17	15	-17	15	-1	-17
-1	-17	15	-17	-17	15	-1	-1	-17	15	15	-17	-17	15	-17	-17	-17
31	-1	-17	15	47	47	-17	-1	-17	15	15	-1	-17	-1	15	15	-1
31	15	-17	-1	-1	-1	-17	15	-17	15	-17	-17	-1	-17	-17	-17	15
31	15	47	15	15	-17	15	-17	-1	15	-1	-1	-17	-17	15	-17	15
31	-17	-17	-17	-1	-1	-17	-17	-17	-17	15	-1	15	47	-1	47	-17
-1	-1	-1	-17	-1	-1	47	15	-1	15	-1	-1	47	-1	15	-17	-1
-1	-17	-17	-1	-1	-1	15	-17	-1	-1	-1	-17	-1	15	-17	-1	-17
-1	-1	15	15	15	-17	-1	-17	-1	-17	-1	-17	-17	-1	-17	-17	-1
31	-1	-17	-1	-17	-17	15	-1	15	-17	15	15	-1	-1	-1	15	-1
-1	-1	-1	-1	-17	15	-17	15	15	-17	-17	-17	-1	-1	15	-17	-1
-1	15	15	-1	-17	15	-17	15	15	-1	-17	47	-1	15	-1	-1	15
31	15	-1	-17	-17	-17	-1	-17	15	-17	15	15	-17	-17	-1	15	15
31	15	-1	15	15	-17	-17	-1	-17	-1	-17	-1	-17	-17	-1	-1	15

그림 2. $C_{0,\beta^7}(\tau)(0\le\tau\le 2^n-2)$의 배열
Fig. 2 The array of the value $C_{0,\beta^7}(\tau)$ for $0\le\tau\le 2^n-2$

예제 4.5. $n=8$, $m=4$일 때 $a=0$으로 두고 b를 변

화시켰을 때 $\tau = Q\tau_1\ (0 \le \tau_1 \le 14)$에 대한 $C_{0,b}(\tau)$ 값의 분포는 다음과 같다.

$C_{0,b}(\tau)=31$이 8개(또는 $C_{0,b}(\tau)=-1$이 7개)인 경우 : $b=1, \beta^5, \beta^7, \beta^{10}, \beta^{11}, \beta^{13}, \beta^{14}$ (7번)

$C_{0,b}(\tau)=31$이 7개(또는 $C_{0,b}(\tau)=-1$이 8개)인 경우 : $b=\beta, \beta^2, \beta^3, \beta^4, \beta^6, \beta^8, \beta^9, \beta^{12}$ (8번)

Ⅴ. 결 론

본 논문에서는 $n=2m$을 만족하는 n, m과 $\gcd(r, 2^m-1)=1$을 만족하는 r, $d=2^{m-1}(3\cdot 2^m-1)$에 대하여 새롭게 정의된 수열군은 5개의 상호상관 함숫값을 가진다는 것을 보였고 $a=0$, $b\in GF(2^m)^*$인 경우 위상이동차 $\tau = Q\tau_1 (0 \le \tau_1 \le 2^m-2)$에 대한 $C_{0,b}(\tau)$ 값의 분포에 대하여 살펴보았다. 이 연구를 바탕으로 일반적인 τ에 대한 상호상관 함숫값의 분포에 관한 연구가 이루어질 수 있을 것이라 생각된다.

감사의 글

이 논문은 부경대학교 자율창의학술연구비(2013년)에 의하여 연구되었음

참고 문헌

[1] M.K. Simon, J.K. Omura, R.A. Scholtz and B.K. Levitt, “Spread Spectrum Communications”, Vol. 1, Computer Science Press, Rockville, MD, 1985.

[2] R.A. Rueppel, “Analysis and Design of Stream Ciphers”, Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, In Communications and Control Engineering Series, 1996.

[3] W. Meier and O. Staffelbach, “Fast Correlation Attacks on Certain Stream Ciphers”, Journal of Cryptology, Vol. 1, No. 3, pp. 159-176, 1989.

[4] R.A. Scholtz and R. Welch, “GMW sequences”, IEEE Trans. Infom. Theory, Vol. 30, No. 3, pp. 548-553, 1984.

[5] G. Gong, “New design for signal sets with low cross correlation, balance property, and large linear span: $GF(p)$ case”, IEEE Trans. Infom. Theory, Vol. 4, No. 11, pp. 2847-2867, 2002.

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

[7] S.W. Golomb, "Shift Register Sequences", Holden Day, pp. 190-193, 1967.

[8] D.V. Sarwate, M.B. Pursley, “Crosscorrelation properties of pseudorandom and related sequences”, Proc. IEEE. Vol. 68, No. 5, pp. 593-619, 1980.

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

[10] 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.

[11] M.J. Kwon, S.J. Cho, S.H. Kwon, J.G. Kim, H.D. Kim, U.S. Choi, “New Decimations with 4-Valued Cross-Correlations”, The Journal of The Korea Institute of Electronic Communication Sciences, Vol. 7, No. 4, pp. 827-832, 2012.

[12] J.G. Kim, S.J. Cho, H.D. Kim, U.S. Choi, “New decimations with 5-level cross-correlation and large linear span”, The Journal of The Korea Institute of Electronic Communication Sciences, Vol. 8, No. 2, pp. 263-269, 2013.

[13] J.S. No, “Generalization of GMW sequences and No sequences”, IEEE Trans. Infom. Theory, Vol. 42, No. 1, pp. 260-262, 1996.

[14] R.J. McEliece, “Finite Fields for Computer Scientists and Engineers”, Kluwer Academic Pub., pp. 103-110, 1987.

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

[16] M.J. Kwon, S.J. Cho, “Analysis of The Sequences with Optimal Cross-correlation Propery”, submitted.

[17] U.S. Choi, S.J. Cho, H.D. Kim, “Design and

Analysis of Linear Span of A New Family of Non-linear Binary Sequences with 5-Valued Cross-Correlation Functions", submitted.

저자 소개

권민정(Min-Jeong Kwon)

1997년 2월 부산대학교 수학교육과 졸업(이학사)
2002년 8월 부산대학교 교육대학원 수학과 졸업(교육학석사)
2007년~현재 부경대학교 응용수학과 박사과정
※ 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