교 육 학 석 사 학 위 논 문

새로운 이진 의사난수열의 상호상관 함숫값과 발생 빈도수

2013년 8월

부경대학교 교육대학원

수 학 교 육 전 공

최 이 화

교 육 학 석 사 학 위 논 문

새로운 이진 의사난수열의 상호상관 함숫값과 발생 빈도수

지도교수 조 성 진

이 논문을 교육학석사 학위논문으로 제출함.

2013년 8월

부경대학교 교육대학원

수 학 교 육 전 공

최 이 화

최이화의 교육학석사 학위논문을 인준함.

2013년 8월 23일

주 심 이학박사 박 진 한 (인)

위 원 교육학박사 서 종 진 (인)

위 원 이학박사 조 성 진 (인)

목 차

표 목차

Binary pseudorandom sequences having optimal periodic correlation properties

Lee-Hwa Choi

Graduate School of Education

Pukyong National University

Abstract

In this thesis we will find a family of binary pseudorandom sequences having optimal periodic correlation properties. A special decimated sequence has an important part in Code Division Multiple Access system(CDMA). Also, we give the number of occurrence about the several sequences using the trace function. The cross-correlation value $C_{a,b}(\tau)$ of the two sequences $s_a^r(t)$ and $s_b^r(t)$ is $C_{a,b}(\tau) \in \{-1-2^m,\ -1,\ 2^m-1, 2^{m+1}-1, 3\cdot 2^m-1\}$ when $\tau \neq 0$ or $a \neq b$.

I. 서 론

대역확산통신은 디지털 CDMA 이동통신에서 사용하는 것으로 정보 데이터신호의 주파수대역폭보다 훨씬 넓은 대역폭을 갖는 확산코드(의사난수열 코드)를 사용해서 정보 데이터신호를 변조하여 주파수대역을 확인한 후에 전송하는 통신 방식이다[22]. CDMA방식은 여러 사용자들의 신호를 처리하거나 여러 사용자들이 중앙통신장치에 접속할 때 부호를 분할하여 채널을 구분하는 방식이다[4]. 따라서 여러 사용자가 시간과 주파수를 공유하면서 각 사용자는 자신에게 할당된 부호만을 이용하여 대역 확산하여 전송하고, 수신자는 송신측에서 사용된 부호를 사용하여 역확산시켜 원하는 정보를 얻게 되므로 할당된 부호간의 상호상관관계는 낮으면서 자기상관관계는 높은 수열을 부호로 사용하는 것이 바람직하다([2], [10], [22]). 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.

여러 가지 디지털통신 시스템에서 많이 사용되고 있는 의사난수열을 설계하는 데 있어 가장 중요한 문제는 생성된 수열들 사이의 상호상관관계가 좋은 수열을 생성하는 것이다. 지금까지의 대부분의 수열에 관한 연구는 이상적인 자기상관관계를 갖는 수열의 생성에 관한 연구이거나, 최적의 상호상관 함숫값을 갖는 수열에 관한 연구였다. 낮은 상관관계 함숫값을 갖는 의사난수열들은 통신과 암호에서 아주 중요하게

사용된다.

적당한 정수 n에 대하여 자기상관관계(auto-correlation) 함숫값으로 -1 또는 상호상관관계(cross-correlation) 함숫값으로 2^n-1을 갖는 주기가 2^n-1인 균형이 잡힌 이진수열(balanced binary sequences)은 대역확산 통신 시스템(spread-spectrum communication system)에서 많이 응용되고 있다([8], [12]). 이러한 이진수열은 1970년대부터 많은 연구자들에 의해 연구되어왔다([9], [13], [14], [5], [16]). 이러한 수열은 트레이스 함수를 사용하여 제안되었으며 잘 알려진 대표적인 수열군은 $m-$수열[10], GMW 수열[6], Kasami 수열[15], No 수열[7] 및 Gold 계열의 수열이 있다[9]. 이 밖에도 트레이스를 이용한 여러 수열들이 연구되었다[3].

본 논문에서는 CDMA 통신에서 중요한 역할을 하는 수열생성에 대하여 알아보고 생성된 수열의 상호상관 함숫값과 발생 빈도수에 대하여 살펴보기로 한다.

Ⅱ. 배경지식

2.1 트레이스 함수

정의 2-1 ([1], [11], [18])> $k|l$을 만족하는 $k, l \in N$에 대하여 다음과 같이 정의된 함수 $Tr_k^l : GF(2^l) \rightarrow GF(2^k)$을 트레이스(trace)라 한다:

$$Tr_k^l(x) = \sum_{j=0}^{l/k-1} x^{2^{kj}} \qquad (2\text{-}1\text{-}1)$$

임의의 $x, y \in GF(2^n)$, $a, b \in GF(2^k)$에 대하여 트레이스 함수는 다음과 같은 성질을 갖는다.

(i) $Tr_k^l(x) = Tr_k^l(x^{2^i}) = \{Tr_k^l(x)\}^{2^i}$

(ii) Tr_k^l은 선형적이다. 즉, $Tr_k^l(ax+by) = aTr_k^l(x) + bTr_k^l(y)$.

(iii) $Tr_1^l(x) = Tr_1^k[Tr_k^l(x)]$.

(iv) Tr_k^l은 전사 함수이다.

(v) $Tr_k^l(x) = a$ 를 만족하는 x는 2^{l-k}개다.

2.2 m-수열, GMW 수열, Kasami 수열 및 No 수열

두 정수 m, n에 대하여 $N=2^n-1$, $n=2m(m>0)$, $\eta,\gamma\in GF(2^m)$, $Q=\frac{2^n-1}{2^m-1}=2^m+1$, $\gcd(r, 2^m-1)=1$이라 하자. 그리고 α를 $f(\alpha)=0$를 만족하는 $GF(2^n)$의 원시원소라 하고 $\beta=\alpha^Q$라 하자. 그러면 각각 같은 원시다항식 $f(x)$에 의해서 생성된 GMW 수열 $s_{G,r}(t)$, Kasami 수열 $s_{K,\eta}(t)$와 No 수열 $s_{N,\eta,r}(t)$은 다음 식과 같이 정의된다.

$$s_{G,r}(t)=Tr_1^m\left\{\left[Tr_m^n(\alpha^t)\right]^r\right\} \quad (2\text{-}2\text{-}1)$$

$$s_{K,\eta}(t)=Tr_1^m\left[Tr_m^n(\alpha^{2t})+\eta\beta^t\right] \quad (2\text{-}2\text{-}2)$$

$$s_{N,\gamma,r}(t)=Tr_1^m\left\{\left[Tr_m^n(\alpha^{2t})+\gamma\beta^t\right]^r\right\} \quad (2\text{-}2\text{-}3)$$

GMW 수열에서 $r=1$이면 m-수열이 되고, No 수열에서 $r=1$이면 Kasami 수열이 된다. 따라서 GMW 수열과 No 수열에서 $r>1$인 경우만 생각하기로 한다.

우수한 상호상관 함숫값을 갖는 이진 m-수열, GMW 수열, Kasami 수열 및 No 수열을 표로 나타내면 다음과 같다.

[표 II-1] 우수한 상호상관 함숫값을 갖는 이진수열

수열	함수	상호상관 함숫값
m-수열 $(s_{m,\eta}(t))$ [10]	$Tr_1^n(\eta\alpha^t)$	$-1,\ 2^m-1$
GMW 수열 $(s_{G,r}(t))$ [6]	$Tr_1^m\{[Tr_m^n(\alpha^t)]^r\}$ $n=2m,\ \gcd(r,2^m-1)=1$	$-1,\ 2^m-1$
Kasami 수열 $(s_{K,\eta}(t))$ [15]	$Tr_1^n(\alpha^{2t})+Tr_1^m(\eta_i\alpha^{Q\cdot t})$ $n=2m,\ Q=2^m+1,$ $\gamma_i\in GF(2^m)$	$-2^m-1,\ -1,\ 2^m-1$
No 수열 $(s_{N,\gamma,r}(t))$ [7]	$Tr_1^m\{[Tr_m^n(\alpha^{2t})+\gamma_i\alpha^{Q\cdot t}]^r\}$ $n=2m,\ \gcd(2^m-1,\ r)=1,$ $Q=2^m+1,\ \gamma_i\in GF(2^m)$	$-2^m-1,\ -1,\ 2^m-1$

2.3 Gold 계열 수열의 상호상관 함숫값

두 개의 m-수열 $u(t)$와 $v(t)$ $(t=0,1,2,\ ...)$는 주기가 2^{n-1}인 수열이라 하고 α는 $GF(2^n)$의 원시원소라 하자. 트레이스 함수를 이용하여 $u(t)=Tr_1^n(\alpha^t)$라 하고 $v(t)=u(dt)$라 할 때, $u(t)+v(t)$를 Gold 계열의 수열이라 하고 d를 데시메이션(decimation)이라 한다. 이 때 위상이동차 $\tau=0,\ 1,\ 2,\ \ ...\ ,\ 2^n-2$에 대하여 두 수열 $u(t)$와 $v(t)$의 상호상관 함숫값은 다음 식 (2.3.1)과 같이 정의된다.

$$C_d(\tau)=\sum_{i=0}^{2^n-2}(-1)^{u(t+\tau)+v(t)}=\sum_{i=0}^{2^n-2}(-1)^{u(t+\tau)+u(dt)} \qquad (2\text{-}3\text{-}1)$$

τ 에 대하여 두 수열 $u(t)$와 $v(t)$의 상호상관 함숫값을 수열의 정의와 트레이스 함수의 성질을 이용하면 다음 식 (2-3-2)와 같이 간단히 나타낼 수 있다.

$$C_d(\tau)=\sum_{t=0}^{2^n-2}(-1)^{Tr_1^n(\alpha^{t+\tau}+\alpha^{dt})} \qquad (2\text{-}3\text{-}2)$$

m-수열의 확장된 형태인 GMW 수열과 Kasami 수열을 포함하는 No 수열은 모두 Gold 계열의 수열로써 상호상관 함숫값이 낮고 GMW 수열은 m-수열로부터, No 수열은 Kasami 수열로부터 각각 데시메이션을 이용하여 생성할 수 있다.

2.4 $n=2m$인 경우의 수열

$n:=2m,\ q:=2^m$일 때 $y\in GF(q^2)$에 대하여 $\bar{y}:=y^q$라 정의하자. 그러면 $x,\ y\in GF(q^2)$에 대하여 다음이 성립한다.

(ⅰ) $\overline{x+y}=\bar{x}+\bar{y}$

(ⅱ) $x+\bar{x}\in GF(q),\ x\bar{x}=x^{q+1}\in GF(q)$

$GF(q^2)$의 단위원을

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

라 정의하자.

보조정리 2-4-1[20]> $n:=2m,\ q:=2^m$라 하자. 그러면 모든 $x\in GF(q^2)^*$는 다음과 같이 표현된다.

$$x=\delta\gamma$$

여기서 $\delta\in GF(q)^*$이고 $\gamma\in S$이다.

증명> $\gcd(q-1,\ q+1)=1$ 이므로 $u,\ v\in N$가 존재하여 $1=u(q-1)+v(q+1)$이다. 따라서

$$x = x^1 = x^{u(q-1)+v(q+1)} = x^{u(q-1)} \cdot x^{v(q+1)}$$

이다. $x^{v(q+1)} := \delta$, $x^{u(q-1)} := \gamma$라 정의하면 $x = \delta\gamma$이다. $\delta \neq 0$이고 $\delta^{q-1} = 1$이므로 $\delta \in GF(q)^*$이다. 또한 $\gamma^{q+1} = x^{u(q-1)(q+1)} = 1$이므로 $\gamma \in S$이다.

■

Ⅲ. 새로운 수열의 상호상관 함숫값

이 절에서는 CDMA 통신에서 중요한 역할을 하는 수열생성에 대하여 알아보고 생성된 수열의 상호상관 함숫값에 대하여 파악해 본다.

$n := 2m (m \in \mathbb{N})$, $N := 2^n - 1$, $Q := 2^m + 1$, $d = 3 \cdot 2^m - 1$라 하자.

$$S^r := \left\{ s_a^r(t) | 0 \le t \le N-1,\ a \in GF(2^m) \right\} \tag{3-1-1}$$

을 다음을 만족하는 2^n개의 이진수열들로 이루어진 모임이라 하자:

$$s_a^r(t) := Tr_1^m \left\{ \left[Tr_m^n \left(\alpha^{2t} + a\alpha^{(3 \cdot 2^m - 1)t} \right) \right]^r \right\} \tag{3-1-2}$$

여기서 α는 $GF(2^m)$의 한 원시원소이며 $r \left(1 \le r < 2^m - 1\right)$은 $\gcd(r, 2^m - 1) = 1$을 만족한다. 또한 $\gcd(d, 2^n - 1) = 1$이며 $d \equiv 2 \pmod{2^m - 1}$이다.

식 (3-1-2)에서 $a := 0$라 두면 새로운 수열들의 모임은 GMW 수열들의 모임이 된다.

$a, b \in GF(2^n)$에 대하여 $C_{a,b}(\bullet)$를 S^r의 $s_a^r(t)$와 $s_b^r(t)$ 사이의 상관함수(correlation function)라 하면 $C_{a,b}(\bullet)$는 다음과 같다[11].

$$C_{a,b}(\tau) := \sum_{t=0}^{N-1} (-1)^{s_a^r(t+\tau)+s_b^r(t)}, \quad 0 \le \tau \le N-1 \tag{3-1-3}$$

보조정리 3-1([19], [20], [21])> $n=2m$일 때 두 수열 $s_a^r(t)$와 $s_b^r(t)$의 상호상관 함숫값 $C_{a,b}(\tau)$은 다음과 같다. 여기서 $\tau \neq 0$이거나 $a \neq b$이다.

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

증명> $t=t_1Q+t_2$라 하면

$$\begin{aligned} s_a^r(t) &= Tr_1^m\left\{\left[Tr_m^n\left(\alpha^{2t}+a\alpha^{(3\cdot 2^m-1)t}\right)\right]^r\right\} \\ &= Tr_1^m\left\{\left[Tr_m^n\left(\alpha^{2(t_1Q+t_2)}+a\alpha^{(3\cdot 2^m-1)(t_1Q+t_2)}\right)\right]^r\right\} \\ &= Tr_1^m\left\{\beta^{2rt_1}\left[Tr_m^n\left(\alpha^{2t_2}+a\alpha^{(3\cdot 2^m-1)t_2}\right)\right]^r\right\} \end{aligned} \tag{3-1-4}$$

이므로

$$s_a^r(t+\tau)+s_b^r(t) = Tr_1^m\left\{\beta^{2rt_1}g(t_2,\tau)\right\} \tag{3-1-5}$$

이다. 여기서

$$\begin{aligned} &g(t_2,\tau) := \\ &\left[Tr_m^n\left(\alpha^{2(t_2+\tau)}+a\alpha^{(3\cdot 2^m-1)(t_2+\tau)}\right)\right]^r + \left[Tr_m^n\left(\alpha^{2t_2}+b\alpha^{(3\cdot 2^m-1)t_2}\right)\right]^r \end{aligned} \tag{3-1-6}$$

이다. 따라서

$$\begin{aligned} C_{a,b}(\tau) &= \sum_{t=0}^{N-1}(-1)^{s_a(t+\tau)+s_b(t)} \\ &= \sum_{t_2=0}^{Q-1}\sum_{t_1=0}^{2^m-2}(-1)^{Tr_1^m\left(\beta^{2^{n_1}}g(t_2,\tau)\right)} \\ &= \sum_{t_2=0}^{Q-1}\sum_{x\in GF(2^m)}(-1)^{Tr_1^m(xg(t_2,\tau))}-Q \\ &= 2^m U(\tau)-Q \\ &= -1+(U(\tau)-1)2^m \end{aligned} \tag{3-1-7}$$

이다. 여기서 $U(\tau):=\left|\{t_2|g(\tau,t_2)=0, 0\le t_2\le Q-1\}\right|$이다. $g(t_2,\tau)$에서 $x:=\alpha^{t_2}$라 하고 $g(t_2,\tau):=G(x)$라 하면

$$G(x)=\left[Tr_m^n\left(\alpha^{2\tau}x^2+a\alpha^{(3\cdot 2^m-1)\tau}x^{3\cdot 2^m-1}\right)\right]^r+\left[Tr_m^n\left(x^2+bx^{3\cdot 2^m-1}\right)\right]^r \tag{3-1-8}$$

이다. $\gcd(r,2^m-1)=1$이므로 $G(x)=0$일 필요충분조건은

$$Tr_m^n\left(\alpha^{2\tau}x^2+a\alpha^{(3\cdot 2^m-1)\tau}x^{3\cdot 2^m-1}\right)=Tr_m^n\left(x^2+bx^{3\cdot 2^m-1}\right) \tag{3-1-9}$$

이다. (3-1-9)로부터

$$Tr_m^n\left((\alpha^{2\tau}+1)x^2+\left(a\alpha^{(3\cdot 2^m-1)\tau}+b\right)x^{3\cdot 2^m-1}\right)=0 \tag{3-1-10}$$

이다. (3-1-10)에서 $A := \alpha^{2\tau}+1(\neq 0)$이고 $B := a\alpha^{(3\cdot 2^m-1)}+b$라 하면 (3-1-10)로부터

$$Ax^2+Bx^{3\cdot 2^m-1}+\overline{A}x^{2^{m+1}}+\overline{B}x^{-(2^m-3)}=0 \qquad (3\text{-}1\text{-}11)$$

을 얻는다. (3-1-11)의 양변에 x^{2^m-3}을 곱하여 정리하면

$$Bx^{4(2^m-1)}+\overline{A}x^{3(2^m-1)}+Ax^{2^m-1}+\overline{B}=0 \qquad (3\text{-}1\text{-}12)$$

을 얻는다. (3-1-12)에서 $x^{2^m-1} := y$라 하면 $y\in S$이며 (3-1-12)는

$$By^4+\overline{A}y^3+Ay+\overline{B}=0 \qquad (3\text{-}1\text{-}13)$$

이 된다. (3-1-13)은 4차방정식이므로 최대 4개의 해를 갖는다. ■

보조정리 3-2 [17]> (3-1-13)에서 $a := 0$이고 $b\in GF(2^m)$일 때 $(N_3 = |\{\tau | U(\tau)=3\}|)$

$$N_3=\begin{cases}2^{m-1}, & Tr_1^m(b)=0\\ 2^{m-1}-1, & Tr_1^m(b)=1\end{cases} \qquad (3\text{-}2\text{-}1)$$

증명> $a=0$이고 $b\in GF(2^m)$인 경우에 $A=\alpha^{2\tau}+1$이고 $B=b=\overline{B}$이다. 따라서 (3-1-13)은 다음과 같다.

$$by^4 + \overline{A}y^3 + Ay + b = 0 \qquad (3\text{-}2\text{-}2)$$

(3-2-2)가 정확하게 세 개의 서로 다른 근들을 S에서 가질 필요충분조건은 하나의 중근과 서로 다른 두 근을 가져야 한다. 이때는 당연히 $b \neq 0$, $A \neq 0$이다. (3-2-2)의 양변을 미분하여 정리하면 $\overline{A}y^2 + A = 0$가 된다. $y \neq 0$이므로 $y^2 = \dfrac{A}{\overline{A}}$이다. 이를 (3-2-2)에 대입하여 정리하면 $bA^2 = b\overline{A}^2$이 된다. 즉, $A \in GF(2^m)$이다. 그러므로 (3-2-2)는 다음과 같다.

$$by^4 + Ay^3 + Ay + b = 0 \qquad (3\text{-}2\text{-}3)$$

(3-2-3)을 정리하면

$$b(y^2+1)\left(y^2 + \frac{A}{b}y + 1\right) = 0 \qquad (3\text{-}2\text{-}4)$$

가 된다. 따라서 두 근은 γ, γ^{-1} 형태이다. $Tr_1^m\left(\dfrac{b^2}{A^2}\right) = Tr_1^m\left(\dfrac{b}{A}\right) = 0$이면 $\gamma \in GF(2^m)$이다. 그런데 $\gamma \in S$여야 하므로 $Tr_1^m\left(\dfrac{b}{A}\right) = 1$이 되어야 한다. 따라서 γ의 개수는 $\dfrac{(2^m+1)-1}{2} = 2^{m-1}$이다. 그런데 $A \neq 1$이므로 $Tr_1^m(b) = 1$인 경우는 제외되어야 한다. 이때의 γ의 개수는 $2^{m-1}-1$이 되어야 한다. ■

IV. 발생 빈도수

이 절에서는 트레이스를 이용한 여러 수열들의 발생 빈도수에 대하여 알아보도록 한다.

보조정리 4-1> $n=2m$, $q:=2^m$이고 $d\equiv 2 \pmod{2^m-1}$이라 하자. $x\in GF(2^n)/\{0,1\}$가 다음 방정식의 해가 될 필요충분조건은 $x^{d-2}=(x+1)^{d-2}=1$이거나 $x^{d-2q}=(x+1)^{d-2q}=1$이다.

$$(x+1)^d = x^d+1 \tag{4-1-1}$$

증명> $x\in GF(2^n)/\{0,1\}$가 (4-1-1)의 해이므로

$$\begin{aligned}(\overline{x}+1)^d &= (x^q+1)^d \\ &= (x+1)^{qd} \\ &= \{(x+1)^d\}^q \\ &= (x^d+1)^q = \overline{x}^d+1\end{aligned} \tag{4-1-2}$$

이다. $x+\overline{x}\in GF(2^q)$이고 $x\overline{x}\in GF(2^q)$이므로 $x\overline{x}+x+\overline{x}+1\in GF(2^q)$이다. 따라서

$$(x\overline{x}+x+\overline{x}+1)^d = (x\overline{x}+x+\overline{x}+1)^2 \tag{4-1-3}$$

이다.

$$\{(x+1)(\bar{x}+1)\}^d = (x\bar{x}+x+\bar{x}+1)^d \tag{4-1-4}$$

이고

$$(x+1)^d(\bar{x}+1)^d = (x^d+1)(\bar{x}^d+1) = x^d\bar{x}^d + x^d + \bar{x}^d + 1 \tag{4-1-5}$$

이며 $(x\bar{x})^d = (x\bar{x})^2$이므로

$$(x\bar{x}+x+\bar{x}+1)^d = (x\bar{x})^2 + x^d + \bar{x}^d + 1 \tag{4-1-6}$$

이다. 그러므로 (4-1-3)과 (4-1-6)에 의하여

$$x^2 + \bar{x}^2 = x^d + \bar{x}^d \tag{4-1-7}$$

이다. 양변에 x^{d-2q-2}을 곱하면

$$x^{d-2q} + x^{d-2} = x^{2d-2q-2} + x^{qd+d-2q-2} \tag{4-1-8}$$

이 된다. $d \equiv 2 \pmod{q-1}$이므로 $s \in \mathbb{N}$가 존재하여 $d-2 = (q-1)s$가 성립한다. 따라서

$$x^{qd+d-2q-2} = x^{(q+1)(d-2)} = x^{(q+1)(q-1)s} = 1 \tag{4-1-9}$$

이므로

$$x^{2d-2q-2}-x^{d-2q}-x^{d-2}+1=(x^{d-2}-1)(x^{d-2q}-1)=0 \qquad (4\text{-}1\text{-}10)$$

이 성립한다. 즉,

$$x^d=x^2 \text{ 혹은 } x^d=x^{2q}=\overline{x}^2 \qquad (4\text{-}1\text{-}11)$$

이다. 그러므로

(ⅰ) $x^d=x^2$인 경우는 $(x+1)^d=x^d+1=x^2+1=(x+1)^2$이 되어 $(x+1)^{d-1}=1$이다.

(ⅱ) $x^d=\overline{x}^2$인 경우는 $(x+1)^d=\overline{x}^2+1=(x^2+1)^q=(x+1)^{2q}$이므로 $(x+1)^{d-2q}=1$이다.

역으로 $x^{d-2}=(x+1)^{d-2}=1$이라 하자. 그러면 $(x+1)^d=x^2+1$이고 $x^d=x^2$이다. 따라서 $(x+1)^d=x^d+1$이다. $x^{d-2q}=(x+1)^{d-2q}=1$이라 하자. 그러면 $(x+1)^d=(x+1)^{2q}=\overline{x}^2+1$이다. 또한 $x^d=\overline{x}^2$이므로

$$(x+1)^d=(x+1)^{2q}=\overline{x}^2+1=x^d+1 \qquad (4\text{-}1\text{-}12)$$

이 되어 x는 (4-1-1)의 해가 된다. ■

따름정리 4-2> $n=2m$, $q:=2^m$이고 $d\equiv 2 \pmod{2^m-1}$이라 하자. $x\in GF(2^n)\setminus\{0,1\}$가 다음 방정식의 해라 하자.

$$(x+1)^d = x^d + 1 \qquad (4\text{-}2\text{-}1)$$

그러면 $\left(\frac{x+1}{\bar{x}+1}\right)^{d-2} = 1$ 혹은 $\left(\frac{x+1}{\bar{x}+1}\right)^{d+2} = 1$이다.

증명> 보조정리 4-1에 의하여 $x^d = x^2$ 혹은 $x^d = \bar{x}^2$이다. 또한 (4-1-7)에 의하여 $x^2 + \bar{x}^2 = x^d + \bar{x}^d$이다.

(i) $x^d = x^2$인 경우는 $\bar{x}^d = \bar{x}^2$이므로

$$\left(\frac{x+1}{\bar{x}+1}\right)^d = \frac{x^{2d}+1}{\bar{x}^{2d}+1} = \frac{x^2+1}{\bar{x}^2+1} = \left(\frac{x+1}{\bar{x}+1}\right)^2$$

이므로 $\left(\frac{x+1}{\bar{x}+1}\right)^{d-2} = 1$이다.

(ii) $x^d = \bar{x}^2$인 경우는 (4-1-7)로부터 $\bar{x}^d = x^2$이므로

$$\left(\frac{x+1}{\bar{x}+1}\right)^d = \frac{x^{2d}+1}{\bar{x}^{2d}+1} = \frac{\bar{x}^2+1}{x^2+1} = \left(\frac{\bar{x}+1}{x+1}\right)^2$$

이므로 $\left(\frac{x+1}{\bar{x}+1}\right)^{d+2} = 1$이다. ■

정리 4-3> $n = 2m$, $q := 2^m$이고 $d \equiv 2 \pmod{2^m - 1}$이라 하자. 만일 $\gcd(d \pm 2, q+1) = 1$라면 방정식 (4-1-1)은 $GF(2^n)$에서 정확하게 2^m개의 해를 갖는다.

증명> $d \equiv 2 \pmod{q-1}$이므로 모든 $x \in GF(2^m)$는 (4-1-1)의 해가 된다. 따라서 $x \neq 0, 1$이 (4-1-1)의 해라 하자. x가 (4-1-1)의 해이므로 보조정리 4-1에 의하여 $x^d = x^2$ 혹은 $x^d = \bar{x}^2$을 만족한다. $x^d = x^2$라 하면 따름정리 4-1-2에 의하여 $\left(\frac{x+1}{\bar{x}+1}\right)^{d-2} = 1$이며 $x^d = \bar{x}^2$라면 따름정리 4-1-2에 의하여 $\left(\frac{x+1}{\bar{x}+1}\right)^{d+2} = 1$이다. $\gcd(d \pm 2, q+1) = 1$이므로

$$\frac{x+1}{\bar{x}+1} = 1 \tag{4-3-1}$$

이 성립한다. 따라서 $x = \bar{x}$이다. 즉, $x \in GF(2^m)$이다. ■

보조정리 4-4> $n = 2m$, $d := 3 \cdot 2^m - 1$, $b \in GF(2^m)^*$

$$\sum_{x \in GF(2^n)} (-1)^{Tr_1^n(x^2 + bx^d)} = \begin{cases} 0, & Tr_1^m(b) = 0 \\ 2^{m+1}, & Tr_1^m(b) = 1 \end{cases} \tag{4-4-1}$$

증명> $d := 3 \cdot 2^m - 1$이면 $d \equiv 2 \pmod{2^m - 1}$이고 $d \equiv -4 \pmod{2^m + 1}$이다. $A := \sum_{t=0}^{2^n - 2} (-1)^{Tr_1^n(\alpha^{2t} + b\alpha^{dt})}$라 하자. $t := t_1 Q + t_2$라 하면

$$\begin{aligned} Tr_1^n(\alpha^{2t}+b\alpha^{dt}) &= Tr_1^m\{Tr_m^n(\alpha^{2t}+b\alpha^{dt})\} \\ &= Tr_1^m\{\beta^{2t_1}Tr_m^n(\alpha^{2t_2}+b\alpha^{dt_2})\} \end{aligned} \tag{4-4-2}$$

가 된다. $\alpha^{t_2} := x$라 두면 $\alpha^{2t_2}+b\alpha^{dt_2} = x^2+bx^d$이 되어

$$Tr_m^n(x^2+bx^d) = x^2+bx^d+\overline{x^2}+b\overline{x}^d \tag{4-4-3}$$

$\alpha := \delta\gamma\left(\delta^{2^m}=\delta,\ \gamma^{2^m}=\gamma^{-1}\right)$라 두면 $x^d = \delta^{2t_2}\gamma^{-4t_2}$, $\overline{x^2} = \delta^{2t_2}\gamma^{-2t_2}$이며 $\overline{x^d} = \delta^{2t_2}\gamma^{4t_2}$가 된다. 따라서 $\gamma^{t_2} := z(\neq 0)$라 두면 (4-4-3)은

$$Tr_m^n(x^2+bx^d) = \delta^{2t_2}(z^2+bz^{-4}+z^{-2}+bz^4) \tag{4-4-4}$$

이 된다. 따라서

$$\sum_{x\in GF(2^m)}(-1)^{Tr_1^n(x^2+bx^d)} = A+1 = (N-1)2^m \tag{4-4-5}$$

이 된다. 여기서 $N = \left|\{z\in S \mid z^2+bz^{-4}+z^{-2}+bz^4=0\}\right|$이다.

$z^2 := w$라 두면 $z^2+bz^{-4}+z^{-2}+bz^4 = w+bw^{-2}+w^{-1}+bw^2 = 0$이다. 양변에 w^2을 곱하면

$$bw^4+w^3+w+b=0 \tag{4-4-6}$$

이 된다. $w \in S$이므로 (4-4-6)의 S에서의 근의 개수가 곧 N이다. (4-4-6)은 다음과 같다.

$$(w+1)^2(bw^2+w+b)=0 \tag{4-4-7}$$

$Tr_1^m(b)=0$이면 $w \notin S$이므로 $w \in S$이기 위하여

$$Tr_1^m(b^2)=Tr_1^m(b)=1 \tag{4-4-8}$$

이 되어야 한다. 따라서 이 경우는 $N=3$이고 그렇지 않은 경우 즉, $Tr_1^m(b)=0$인 경우는 $N=1$이다. 따라서 (4-4-5)에 의하여

$$A+1=\begin{cases}2^{m+1}, & Tr_1^m(b)=1\\ 0, & Tr_1^m(b)=0\end{cases} \tag{4-4-9}$$

이다. 그러므로 (4-4-1)을 얻는다. ■

정리 4-5> $b \in GF(2^m)^*$일 때 다음이 성립한다.

(a) $$\sum_{\tau=0}^{2^n-2}\{C_{0,b}(\tau)+1\}=\begin{cases}2^n, & Tr_1^m(b)=0\\ 2^n-2^{m+1}, & Tr_1^m(b)=1\end{cases}$$

(b) $$\sum_{\tau=0}^{2^n-2}\{C_{0,b}(\tau)+1\}^2=\begin{cases}2^{2n}, & Tr_1^m(b)=0\\ 2^{2n}-2^{n+2}, & Tr_1^m(b)=1\end{cases}$$

(c) $$\sum_{\tau=0}^{2^n-2}\{C_{0,b}(\tau)+1\}^3=\begin{cases}2^{2n}\cdot 2^m, & Tr_1^m(b)=0\\ 2^{2n}\cdot 2^m-2^{n+m+3}, & Tr_1^m(b)=1\end{cases}$$

증명> (a) $A(\tau)=\alpha^{2\tau}+1$이고 $d=3\cdot 2^m-1$이라 하면 보조정리 4-4에 의하여

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

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

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

$$=\begin{cases}\sum_{z\in GF(2^n)}\sum_{x\in GF(2^n)}(-1)^{Tr_1^n(zx^2+bx^d)}-2^{m+1}, & Tr_1^m(b)=1\\ \sum_{z\in GF(2^n)}\sum_{x\in GF(2^n)}(-1)^{Tr_1^n(zx^2+bx^d)}, & Tr_1^m(b)=0\end{cases} \qquad (4\text{-}5\text{-}1)$$

$$=\begin{cases}\sum_{z\in GF(2^n)}(-1)^{Tr_1^n(zx^2)}\sum_{x\in GF(2^n)}(-1)^{Tr_1^n(bx^d)}-2^{m+1}, & Tr_1^m(b)=1\\ \sum_{z\in GF(2^n)}(-1)^{Tr_1^n(zx^2)}\sum_{x\in GF(2^n)}(-1)^{Tr_1^n(bx^d)}, & Tr_1^m(b)=0\end{cases}$$

$$=\begin{cases}2^n-2^{m+1}, & Tr_1^m(b)=1\\ 2^n, & Tr_1^m(b)=0\end{cases}$$

(b) 보조정리 4-4에 의하여

$$\left(\sum_{x\in GF(2^n)}(-1)^{Tr_1^n(x^2+bx^d)}\right)^2=\begin{cases}2^{n+2}, & Tr_1^m(b)=1\\ 0, & Tr_1^m(b)=0\end{cases}$$

이다. 따라서

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

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

$$=\begin{cases}\sum_{u\in GF(2^n)}(-1)^{Tr_1^n(u(x^2+y^2))}\sum_{x,y\in GF(2^n)}(-1)^{Tr_1^n b(x^d+y^d)}-2^{n+2}, & Tr_1^m(b)=1\\ \sum_{u\in GF(2^n)}(-1)^{Tr_1^n(u(x^2+y^2))}\sum_{x,y\in GF(2^n)}(-1)^{Tr_1^n b(x^d+y^d)}, & Tr_1^m(b)=0\end{cases} \quad (4\text{-}5\text{-}2)$$

$$=\begin{cases}2^{2n}-2^{n+2}, & Tr_1^m(b)=1\\ 2^{2n}, & Tr_1^m(b)=0\end{cases}$$

(c) 우선

$$\sum_{\tau=0}^{2^n-2}\{C_{0,b}(\tau)+1\}^3=\sum_{\tau=0}^{2^n-2}\left(\sum_{x\in GF(2^n)}(-1)^{Tr_1^n(A(\tau)x^2+bx^d)}\right)^3$$
$$=\sum_{u\neq 1}\left(\sum_{x\in GF(2^n)}(-1)^{Tr_1^n(ux^2+bx^d)}\right)^3 \quad (4\text{-}5\text{-}3)$$

이므로 (4-5-3)의 왼쪽 식을 S_3라 하면

$$S_3=\sum_{u\neq 1}\sum_{x,y,z\in GF(2^n)}(-1)^{Tr_1^n\{u(x^2+y^2+z^2)+b(x^d+y^d+z^d)\}} \quad (4\text{-}5\text{-}4)$$

이다. 보조정리 4-4에 의하여

$$\left(\sum_{x\in GF(2^n)}(-1)^{Tr_1^n(x^2+x^d)}\right)^3=\begin{cases}2^{n+m+3}, & Tr_1^m(b)=1\\ 0, & Tr_1^m(b)=0\end{cases}$$

이다. S_3의 안쪽 합을 $A(u)$라 하면

$$S_3=\begin{cases}\sum_{u\in GF(2^n)}A(u)-2^{n+m+3}, & Tr_1^m(b)=1\\ \sum_{u\in GF(2^n)}A(u), & Tr_1^m(b)=0\end{cases} \tag{4-5-5}$$

$S_A:=\sum_{u\in GF(2^n)}A(u)$라 하자. 그러면

$$S_A:=\sum_{x,y,z\in GF(2^n)}(-1)^{Tr_1^n\{b(x^d+y^d+z^d)\}}\sum_{u\in GF(2^n)}(-1)^{Tr_1^n\{u(x^2+y^2+z^2)\}} \tag{4-5-6}$$

S_A의 안 쪽의 합은 $x+y+z=0$일 때는 2^n이며 그렇지 않을 때는 0이 된다. 따라서 S_A는 다음과 같다.

$$\begin{aligned}S_A&=2^n\sum_{x+y+z=0}(-1)^{Tr_1^n\{(u+1)(x^d+y^d+z^d)\}}\\&=2^n\sum_{x,y}\sum_{z=x+y}(-1)^{Tr_1^n\{b(x^d+y^d+z^d)\}}\\&=2^n\sum_{x,y}(-1)^{Tr_1^n\{b(x^d+y^d+(x+y)^d)\}}\\&=2^n\left(2^n+\sum_{x\neq 0}\sum_{y\in GF(2^n)}(-1)^{Tr_1^n\{b(x^d+y^d+(x+y)^d)\}}\right)\end{aligned} \tag{4-5-7}$$

$y := ax(a \in GF(2^n))$라 두면

$$\begin{aligned} S_A &= 2^n\left(2^n + \sum_{x \neq 0}\sum_{a \in GF(2^n)} (-1)^{Tr_1^n\{b(x^d + (ax)^d + (x+ax)^d)\}}\right) \\ &= 2^n\left(2^n + \sum_{x \neq 0}\sum_{a \in GF(2^n)} (-1)^{Tr_1^n\{bx^d(1 + a^d + (1+a)^d)\}}\right) \\ &= 2^{2n} \cdot w \end{aligned} \tag{4-5-8}$$

여기서 $k := |\{x \in GF(2^n) : (x+1)^d = x^d + 1\}|$이다. 따라서

$$S_3 = \begin{cases} 2^{2n} \cdot k - 2^{n+m+3}, & Tr_1^m(b) = 1 \\ 2^{2n} \cdot k, & Tr_1^m(b) = 0 \end{cases} \tag{4-5-9}$$

이다. 정리 4-3에 의하여 $k = 2^m$이다. 그러므로

$$S_3 = \begin{cases} 2^{2n} \cdot 2^m - 2^{n+m+3}, & Tr_1^m(b) = 1 \\ 2^{2n} \cdot 2^m, & Tr_1^m(b) = 0 \end{cases} \tag{4-5-10}$$

이다. ■

정리 4-6> $a:=0$이고 $b\in GF(2^m)$일 때 새로운 수열의 발생 빈도수는 다음과 같다. $(N_i=|\{\tau|U(\tau)=i\}|)$

$$N_0=3\cdot 2^{n-3}-2^{m-1}$$

$$N_1=\begin{cases}\dfrac{2^n+2^{m-1}}{3}-1, & Tr_1^m(b)=0\\ \dfrac{2^n+2^{m-1}}{3}, & Tr_1^m(b)=1\end{cases}$$

$$N_2=2^{n-2}$$

$$N_3=\begin{cases}2^{m-1}, & Tr_1^m(b)=0\\ 2^{m-1}-1, & Tr_1^m(b)=1\end{cases}$$

$$N_4=\frac{2^{n-3}-2^{m-1}}{3}$$

증명> 보조정리 3-2에 의하여

$$N_3=\begin{cases}2^{m-1}, & Tr_1^m(b)=0\\ 2^{m-1}-1, & Tr_1^m(b)=1\end{cases} \qquad (4\text{-}6\text{-}1)$$

이므로 두 가지 경우로 나누어서 구한다. 정리 4-5에 의하여

(i) $Tr_1^m(b)=0$: (4-6-1)에 의하여

$$\begin{aligned} N_0+N_1+N_2+2^{m-1}+N_4 &= 2^n-1\\ -2^mN_0+2^mN_2+2^{m-1}N_3+3\cdot 2^mN_4 &= 2^{2n}\\ 2^nN_0+2^nN_2+2^{n-2}N_3+9\cdot 2^nN_4 &= 2^{2n}\\ -2^{n+m}N_0+2^{n+m}N_2+2^{n+m-3}N_3+27\cdot 2^{n+m}N_4 &= 2^{2n}\cdot 2^m \end{aligned} \qquad (4\text{-}6\text{-}2)$$

을 얻는다.

(ii) $Tr_1^m(b)=1$: (4-6-1)에 의하여

$$\begin{aligned} N_0+N_1+N_2+(2^{m-1}-1)+N_4 &= 2^n-1 \\ -2^{2m}N_0+2^mN_2+(2^{m-1}-1)N_3+3\cdot 2^mN_4 &= 2^n-2^{m+1} \\ 2^nN_0+2^nN_2+(2^{m-1}-1)^2N_3+9\cdot 2^nN_4 &= 2^{2n}-2^{n+2} \\ -2^{n+m}N_0+2^{n+m}N_2+(2^{m-1}-1)^3N_3+27\cdot 2^{n+m}N_4 &= 2^{2n}\cdot 2^m-2^{n+m+3} \end{aligned} \tag{4-6-3}$$

를 얻는다. (4-6-2)와 (4-6-3)을 풀면 다음을 얻는다.

$$N_0=3\cdot 2^{n-3}-2^{m-1}$$

$$N_1=\begin{cases}\dfrac{2^n+2^{m-1}}{3}-1, & Tr_1^m(b)=0\\ \dfrac{2^n+2^{m-1}}{3}, & Tr_1^m(b)=1\end{cases}$$

$$N_2=2^{n-2}$$

$$N_3=\begin{cases}2^{m-1}, & Tr_1^m(b)=0\\ 2^{m-1}-1, & Tr_1^m(b)=1\end{cases}$$

$$N_4=\frac{2^{n-3}-2^{m-1}}{3}$$

.

■

예제> (ⅰ) $n=8$, $a=0$, $b=\beta^5$이면 $Tr_1^4(b)=0$이므로 $N_3=2^{m-1}=8$으로 31값이 8개이다.

[표 Ⅳ-1] $n=8$, $a=0$, $b=\beta^5$ 일 때 상호상관 함숫값

−1	−1	15	−17	−1	−1	15	−1	15	−1	−17	15	−17	−1	15	−17	−1
31	15	15	−1	−1	−17	−1	15	47	15	−17	−1	−17	−1	−17	15	15
−1	−1	−1	−17	15	−1	−17	−1	15	−17	15	−17	−17	−1	−17	15	−1
31	−1	−17	−17	−17	15	15	−1	−1	−17	−17	−1	15	−1	−1	−1	−1
31	−1	47	−17	15	−17	−1	−17	15	−17	15	−17	−1	−1	−17	−17	−1
−1	−17	−17	−17	−17	−1	−1	−1	−17	−17	−1	15	−17	15	−17	47	−17
31	−17	15	−1	15	15	−17	−1	−1	−17	−1	−1	−1	−17	−17	−17	−17
−1	−1	−17	47	−1	−17	−1	15	−17	15	15	−17	15	15	−17	15	−1
−1	15	15	−17	−1	−17	−1	−1	47	−1	15	15	−17	−17	−1	−17	15
31	15	−1	−1	−17	47	15	−17	15	15	−1	−1	−1	15	47	15	15
−1	−17	−17	15	−17	15	15	−17	−17	−1	−17	−1	15	−1	−17	−1	−17
31	−1	−17	15	15	−17	−1	15	−17	15	−1	−17	−17	−1	−1	−17	−1
31	−17	−1	15	−1	−17	−17	−17	−17	−17	−1	−1	−17	−17	15	−17	−17
−1	−1	−17	15	−1	−17	−1	15	−17	−1	15	−1	47	−17	15	−1	−1
31	15	−17	−17	−1	15	−17	−1	−17	−17	−1	15	15	15	15	−17	15

(ⅱ) $n=8$, $a=0$, $b=\beta^3$이면 $Tr_1^4(b)=1$이므로 $N_3=2^{m-1}-1=7$으로 31값이 7개이다.

[표 Ⅳ-2] $n=8$, $a=0$, $b=\beta^3$ 일 때 상호상관 함숫값

−1	−1	−17	15	47	15	−17	15	−1	−17	−17	−1	−1	−1	−17	15	−1
−1	−1	−17	−17	15	−17	47	47	−17	15	−17	−17	15	15	−1	−17	−1
−1	−1	−17	−1	15	−1	−1	−17	−1	−1	15	−17	−1	−1	15	−17	−1
−1	−17	−17	−1	15	−1	−1	−17	−1	−1	−17	−1	−17	47	−17	−17	−17
−1	−17	−17	−1	15	−17	−1	−1	−1	15	−17	15	15	15	−1	−17	−17
31	47	15	−17	15	−17	15	−1	−17	−17	−1	−17	−17	15	−1	−17	47
31	−17	−1	−1	15	−17	−17	15	−1	−1	15	47	−1	15	−1	15	−17
−1	−17	15	−17	15	15	−17	−17	−1	−1	47	−1	−1	15	−17	−1	−17
31	−17	15	15	−1	−17	−17	−17	−17	−17	−17	−1	−17	15	−1	15	−17
−1	−1	−1	−17	15	15	−17	−17	15	−1	−17	−1	−17	15	−17	15	−1
−1	−17	−17	−1	15	−1	−1	−17	−1	−1	−1	15	−17	15	15	−1	−17
31	−1	−17	15	15	−1	−17	15	−1	−1	−1	−17	15	−1	−17	−17	−1
31	15	−1	−1	−1	15	−17	−17	15	−17	15	−17	−17	15	−1	−17	15
31	15	15	−17	15	−1	−1	−17	−17	−1	−17	−17	15	15	15	−1	15
31	−17	15	−1	−1	−17	15	−1	−1	−1	−17	−17	−1	15	−1	15	−17

Ⅴ. 결론

본 논문에서는 CDMA 통신에서 수열생성에 대하여 알아보고 생성된 수열의 상호상관 함숫값과 발생 빈도수에 대하여 살펴보았다.

$n=2m$일 때 두 수열 $s_a^r(t)$와 $s_b^r(t)$의 상호상관 함숫값 $C_{a,b}(\tau)$은 다음과 같다. 여기서 $\tau \neq 0$이거나 $a \neq b$이다.

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

$a:=0$이고 $b \in GF(2^m)$일 때 새로운 수열의 발생 빈도수는 다음과 같다. $(N_i = |\{\tau | U(\tau)=i\}|)$

$$N_0 = 3\cdot 2^{n-3} - 2^{m-1}$$

$$N_1 = \begin{cases} \dfrac{2^n+2^{m-1}}{3}-1, & Tr_1^m(b)=0 \\ \dfrac{2^n+2^{m-1}}{3}, & Tr_1^m(b)=1 \end{cases}$$

$$N_2 = 2^{n-2}$$

$$N_3 = \begin{cases} 2^{m-1}, & Tr_1^m(b)=0 \\ 2^{m-1}-1, & Tr_1^m(b)=1 \end{cases}$$

$$N_4 = \frac{2^{n-3}-2^{m-1}}{3}$$

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 and 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] R.A. Schotz and L. Welch, GMW sequences, IEEE Trans. Inform. Theory Vol. IT-30, No. 3, pp. 548-553, 1984.

[7] J.S. No and D.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. 37-379, 1989

[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 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] M.J. Kwon and S.J. Cho, The distribution of the values of the cross-correlation function between the maximal period binary

sequences., The Korea Institute of Electronic Communication Science, Submitted.

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

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

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

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

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