상호상관 함숫값이 4개인 이진수열의 새로운 데시메이션

권숙희* · 조성진** · 권민정*** · 김한두**** · 최언숙***** · 김진경***

New Decimations of Binary Sequences with 4-Valued Cross-Correlations

Sook-Hee Kwon* · Sung-Jin Cho** · Min-Jeong Kwon*** · Han-Doo Kim**** ·
Un-Sook Choi***** · Jin-Gyoung Kim***

요 약

무선이동통신 시스템에서 두 수열의 상호상관 함숫값은 통화 품질과 사용자 수를 결정하는데 있어 큰 영향을 끼치고 있다. 본 논문에서는 주기 2^n-1인 m-수열에 새로운 데시메이션 $d=\frac{2^{m-st-1}}{2^s-1}(2^n+2^{st+s+1}-2^{m+st+1}-1)$를 적용하여 또 다른 m-수열을 생성하고 두 수열의 상호상관 함숫값과 그 값들의 발생횟수를 결정한다.

ABSTRACT

An important problem in the transmission performance and efficiency is to find the values and the number of the cross-correlation function between two different maximal sequences. In this paper, we present the new maximal sequences which are obtained by the new decimations $d=\frac{2^{m-st-1}}{2^s-1}(2^n+2^{st+s+1}-2^{m+st+1}-1)$ from some maximal sequences. We will also find the values and the number of occurrences of each value of the cross-correlation function from the proposed decimations.

키워드

데시메이션, m-수열, 트레이스 함수, 상호상관함수, 유한체

Key word

decimation, maximal sequences, trace function, cross-correlation function, finite fields

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

접수일자 : 2012. 10. 22
심사완료일자 : 2012. 11. 28

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.3.627

Ⅰ. 서 론

이동통신 방식 중 하나인 부호분할다중접속(CDMA) 방식은 다수의 사용자가 같은 시간대에 주파수를 공유하며 접속이 가능한 다중접속(Multiple Access) 방식으로 한 채널로 한 번에 한 통화밖에 하지 못하는 아날로그 방식의 한계를 극복하기 위해 개발되었다. 이 방식은 동일 주파수 대역의 여러 신호를 동시에 처리할 수 있는 장점이 있어 2세대 이동통신에 적용돼 왔고, 3세대 이동통신에도 핵심기술로 사용되고 있다. CDMA는 아날로그 형태인 음성을 디지털 신호로 전환한 후 여러 개의 디지털 코드로 변환하여 통신하는 것으로 통화자의 채널에 고유하게 부여된 부호만을 인식하기 때문에 통화 품질이 좋고 통신 비밀이 보장된다는 장점이 있다. 시간과 주파수를 공유하는 각 사용자에게 상호 상관관계 값이 작은 PN 부호를 할당하면 송신할 때는 각자에게 할당된 PN 부호를 이용하여 송신할 신호를 대역확산(spread spectrum)하여 전송하고, 수신할 때는 송신할 때 사용한 것과 같은 PN 부호를 발생시켜 동기를 맞추고 이를 이용하여 수신된 신호를 역확산(despreading)시켜 원하는 신호로 복원함으로써 정보가 전달된다. 신호를 복원할 때는 확산신호와 수신신호의 상호상관관계(cross-correlation)는 낮고 자기상관관계(auto-correlation)가 높은 수열을 부호로 사용하는 것이 바람직하며[1][2], 이러한 수열의 설계에 대한 연구도 지속적으로 이뤄지고 있다[3][4]. 상호상관관계가 낮으면 여러 사용자가 동시에 시스템에 접속할 때 발생할 수 있는 충돌을 최소화 할 수 있다.

본 논문에서는 의사난수열인 m-수열을 이용하여 새로운 이진수열군을 생성하기 위해 새로운 d의 값을 제안하고, 그 수열의 상호상관 함숫값을 분석함으로써 제안된 수열은 상호상관 함숫값이 4개인 우수한 이진 수열임을 보이고자 한다.

Ⅱ. 배경지식

먼저 트레이스 함수를 이용하여 두 m-수열의 상호상관함수를 정의한다.

원소의 개수가 2^n개인 유한체는 $GF(2^n)$이라 하고, $GF(2^n)^* = GF(2^n) \setminus \{0\}$으로 표현하자. 트레이스(trace) 함수 $Tr_m^n(\cdot)$는 $GF(2^n)$으로부터 부분체인 $GF(2^m)$으로 대응되는 선형함수이며

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

로 정의된다. 이 함수는 의사불규칙 수열의 설계와 분석을 위한 중요한 수학적 도구이다[3][4][5]. $GF(2^n)$의 임의의 원소 x, y와 $GF(2^m)$의 임의의 원소 a, b에 대하여 트레이스 함수는 다음을 만족한다[5][6][7].

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

(b) 임의의 자연수 i에 대하여

$$Tr_m^n(x) = Tr_m^n\left(x^{2^{mi}}\right) = \left\{Tr_m^n(x)\right\}^{2^{mi}}$$

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

(d) 임의의 $\beta \in GF(2^m)$에 대하여 $Tr_m^n(x) = \beta$를 만족하는 해의 개수는 2^{n-m}이다.

$q = 2^m$이라 하면 유한체 $GF(q)$에 대하여 $GF(q)$의 곱셈군은 $GF(q)^*$이다. $GF(q^2)$ 상에서의 방정식

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

에 대해 $d \equiv 1 \pmod{q-1}$를 만족하는 d를 Niho 형태라고 한다. 이러한 d에 대응하는 m-수열의 상호상관함수는 Niho의 학위 논문에서 처음 연구되었다[8]. 방정식 (1)에 대한 연구는 m-수열, 순환부호의 상호상관 함숫값과 밀접한 관련이 있다.

$GF(2^n)$의 원시원소 α에 대해 두 개의 m-수열을 $u(t) = Tr_1^n(\alpha^t)$, $v(t) = u(dt)(t = 0,1,\cdots,2^n-2)$라 정의하자. 위상이동차 $\tau = 0,1,\cdots,2^n-2$에 대하여 두 수열 $u(t)$와 $v(t)$의 상호상관함수 $C_d(\tau)$는 $C_d(\tau) = \sum_{t=0}^{2^n-2}(-1)^{u(t+\tau)+v(t)}$이고 $C_d(\tau)$ 값의 분포상태를 구하기 위해 다음 정리를 이용한다.

<정리 2.1> 상호상관함수 $C_d(\tau)$에 대하여 다음이 성립한다.

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

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

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

여기서 $b=|\{x\in GF(q^2)\,|\,(x+1)^d=x^d+1\}|$ 이다[9].

정리 2.1에서 알 수 있듯이 주어진 m-수열의 상호상관 함숫값과 방정식 (1)은 밀접한 관계가 있다. 본 논문에서는 Niho 형태의 d 만 다룬다.

이제 $GF(q^2)$ 에서 방정식 (1)의 해를 찾아보자.

Niho 형태의 d는 항상 $\gcd(d, q^2-1)=1$을 만족한다. $x\in GF(q^2)$ 의 켤레를 x^q 이라 정의하고 $\overline{x}=x^q$ 라 표기하자. 켤레에 대한 성질은 다음과 같으며 복소수상의 켤레복소수의 성질과 유사하다.

(a) $GF(q^2)$ 의 임의의 원소 x, y에 대하여
$\overline{x+y}=\overline{x}+\overline{y},\ \overline{xy}=\overline{x}\,\overline{y}$,

(b) $GF(q^2)$ 의 임의의 원소 x 에 대하여
$x+\overline{x}\in GF(q),\ x\overline{x}\in GF(q).$

$S=\{x\in GF(q^2)\,|\,x\overline{x}=1\}$ 라 정의하면 집합 S는 주기가 $q+1$ 인 순환군이다.

$$\begin{aligned}C_d(\tau) &= \sum_{t=0}^{q^2-2}(-1)^{u(t+\tau)+u(dt)}\\ &= \sum_{t=0}^{q^2-2}(-1)^{Tr_1^n(\alpha^{t+\tau}+\alpha^{dt})}\\ &= \sum_{t=0}^{q^2-2}(-1)^{Tr_1^n(\alpha^{\tau}\alpha^{t}+\alpha^{dt})}\end{aligned}$$

이다. 이 식에서 $x=\alpha^t$, $y=\alpha^\tau$로 두면 $C_d(\tau)=\sum_{x\in GF(q^2)^*}(-1)^{Tr_1^n(yx+x^d)}$이다. 그런데 $GF(q^2)$ 의 모든 원소 x는 $x=\delta\gamma$ $(\delta\in GF(q)^*, \gamma\in S)$으로 나타낼 수 있으므로

$$\begin{aligned}Tr_1^n(yx+x^d) &= Tr_1^m\left[Tr_m^n\left(y\gamma\delta+\gamma^d\delta^d\right)\right]\\ &= Tr_1^m\left[\delta\left(y\gamma+\gamma^d+\overline{y}\gamma^{-1}+\gamma^{-d}\right)\right]\end{aligned}$$

이다. 따라서

$$\sum_{x\in GF(q^2)^*}(-1)^{Tr_1^n(yx+x^d)} = \sum_{\gamma\in S}\left[\sum_{\delta\in GF(q)}(-1)^{Tr_1^m[\delta(y\gamma+\gamma^d+\overline{y}\gamma^{-1}+\gamma^{-d})]}\right]-(q+1)$$

이고 $C_d(\tau)$ 의 함숫값은 식 (2)를 만족하는 $\gamma\in S$ 의 개수에 의해 결정된다.

$$y\gamma+\gamma^d+\overline{y}\gamma^{-1}+\gamma^{-d}=0 \qquad (2)$$

이와 같은 사실을 이용하여 Niho는 다음 정리를 증명하였다.

<정리 2.2> d는 $d\equiv 1 \pmod{2^m-1}$ 를 만족할 때, $GF(q^2)^*$의 임의의 원소 y와 위상이동차 $\tau=0,1,2,\cdots,2^n-2$ 에 대하여 $C_d(\tau)$의 함숫값은

$$C_d(\tau) = -1+2^m\,(N(y)-1)\ ,$$

단, $N(y)=|\{x\in S\mid x^{2d}+yx^{d+1}+\overline{y}x^{d-1}+1=0\}|$ 이다[8].

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

<정리 2.3> $GF(q^2)^*$의 임의의 원소 y에 대하여 방정식 $x^{2^s+1}+yx^{2^s}+\overline{y}x+1=0$를 만족하는 집합 S의 원소는 $0, 1, 2, 2^{\gcd(s,m)}+1$ 개 중 하나이다[9].

표 1은 $C_d(\tau)$ 값이 3 개인 것과 4 개인 d를 나타낸 것이다.

표 1. d와 상호상관함수
Table. 1 d and cross-correlation

상호상관 함숫값이 3 개인 d		
$d=2^m+1$	$n/\gcd(n,m)$: odd	Gold [10]
$d=2^{2m}-2^m+1$	$n/\gcd(n,m)$: odd	Kasami [11]
$d=2^{\frac{n}{2}}+2^{\frac{n+2}{4}}+1$	$n\equiv 2 \pmod 4$	Cusick & Dobbertin [12]
$d=2^{\frac{n}{2}+1}+3$	$n\equiv 2 \pmod 4$	
$d=2^{\frac{n-1}{2}}+3$	n: odd	Canteaut [13]
$d=2^{\frac{n-1}{2}}+2^{\frac{n-1}{4}}-1$	$n\equiv 1 \pmod 4$	Hollmann & Xiang [14]
$d=2^{\frac{n-1}{2}}+2^{\frac{3n-1}{4}}-1$	$n\equiv 3 \pmod 4$	

상호상관 함숫값이 4 개인 d		
$d=2^{\frac{n}{2}+1}-1$	$n\equiv 0(\mathrm{mod}\,4)$	Niho [8]
$d=(2^{\frac{n}{2}}+1)(2^{\frac{n}{4}}-1)+2$	$n\equiv 0(\mathrm{mod}\,4)$	
$d=\sum_{i=0}^{n/2}2^{im}$	$n\equiv 0(\mathrm{mod}\,4)$, $0<m<n$, $\gcd(n,m)=1$	Dobbertin [15]
$d=\frac{2^{k-1}}{2^s-1}(2^{2k}+2^{s+1}-2^{k+1}-1)$	$n=2k$, $2s\|k$	Rosendahl [16]

Ⅲ. 상호상관 함숫값이 4개인 새로운 이진수열

이 절에서는 $n=2m$를 만족하는 정수 m과 $\gcd(s,n)=1$을 만족하는 정수 s, 그리고 $2st<m$, $2s|m$ (t는 정수)일 때 주기가 2^n-1인 m-수열로부터 다음과 같이 정의된 새로운 d 를 이용하여 수열을 생성한다.

<보조정리 3.1> $n=2m$ 이고 정수 s,t에 대해 $2st<m$이고 $2s|m$일 때

$$d=\frac{2^{m-st-1}}{2^s-1}\left(2^n+2^{st+s+1}-2^{m+st+1}-1\right) \qquad (3)$$

라 하면 다음 성질을 만족한다.

(1) $d\equiv 1(\mathrm{mod}\ 2^m-1)$

(2) $d\equiv \frac{2^m-2^s}{2^s-1}\ (\mathrm{mod}\,2^m+1)$

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

증명. (1)

$$\begin{aligned} d&=\frac{2^{m-st-1}}{2^s-1}\left\{(2^m-1)^2+2(2^m-1)-2^{st+1}(2^m-2^s)\right\}\\ &=\frac{2^{m-st-1}}{2^s-1}\left\{(2^m-1)^2-2(2^{st}-1)(2^m-1)\right\}+2^m\\ &\equiv 2^m(\mathrm{mod}\,2^m-1)\end{aligned}$$

이므로 $d\equiv 1(\mathrm{mod}2^m-1)$ 이다.

(2)

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

이고 $2s\mid m$이므로 $\frac{2^m-2^s}{2^s-1}$은 정수이다. 따라서 $d\equiv \frac{2^m-2^s}{2^s-1}(\mathrm{mod}2^m+1)$ 이다.

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

그런데 $2^m+1=\frac{2^m-2^s}{2^s-1}(2^s-1)+2^s+1$이고 $\gcd(2^s-1,2^s+1)=1$이므로

$$\begin{aligned}\gcd\left(\frac{2^m-2^s}{2^s-1},2^m+1\right)&=\gcd\left(\frac{2^m-2^s}{2^s-1},2^s+1\right)\\ &=\gcd(2^m-2^s,2^s+1)\\ &=\gcd(2^m+1,2^s+1)\\ &=1\end{aligned}$$

이다. 여기서 마지막 등식은 $2s|m$이므로 성립한다. □

식 (3)의 d는 $t=0$이면 Rosendahl[16]의 d, $t=0$이면서 $m=2s$ 를 만족하면 Niho[8]의 d이다.

<보조정리 3.2> $q=2^m$, $d\equiv 1(\mathrm{mod}\,q-1)$이라 하자. 그러면 $GF(q^2)\setminus\{0,1\}$의 원소 x가 방정식

$$(x+1)^d=x^d+1 \qquad (4)$$

의 해가 될 필요충분조건은 $x^{d-1}=(x+1)^{d-1}=1$ 또는 $x^{d-q}=(x+1)^{d-q}=1$이다[17].

<정리 3.3> $n=2m$ 이고 정수 s,t 에 대해 $2st<m$이고 $2s|m$ 일 때 식(3)과 동치인 d를 다음과 같이 정의하자.

$$d=\frac{1}{2^s-1}\left(2^n+2^{st+s+1}-2^{m+st+1}-1\right) \qquad (5)$$

그러면 $GF(2^n)$에 존재하는 방정식 (4)의 해는 q개다.

증명. 보조정리 3.1 (1)에 의해 $d\equiv 1\ (\mathrm{mod}\,q-1)$이므로 $GF(q)$의 모든 원소는 식(4)의 해이다.

이제 $x(\neq 0,1)$)가 방정식 (4)를 만족한다고 가정하고 식 (4)의 양변을 2^s제곱하면 $(x+1)^{d2^s}=x^{d2^s}+1$이고, 다시 양변을 식 (4)로 나누면 $(x+1)^{(2^s-1)d}=\frac{x^{d2^s}+1}{x^d+1}$이다. 이를 정리하면

$$x^{2^{st+s+1}+d}+x^{2^{st+m+1}+d2^s}$$
$$=x^{2^{st+s+1}}+x^d+x^{2^{st+m+1}}+x^{d2^s} \quad (6)$$

이다. 그런데

$$\begin{aligned}&2^{st+s+1}+d-2^{st+m+1}-d2^s\\&=-(2^s-1)d+2^{st+s+1}-2^{st+m+1}\\&=-(2^n-1)\\&\equiv 0\,(\mathrm{mod}\,2^n-1)\end{aligned}$$

이므로 $x^{2^{st+s+1}}+x^d+x^{2^{st+m+1}}+x^{d2^s}=0$ 이다. 인수분해하면 $\left(x^{2^{m+st+1}}+x^d\right)\left(x^{(2^s-1)d}+1\right)=0$이다. 따라서 $x^{2^{m+st+1}}=x^d$ 또는 $\left(x^d\right)^{2^s-1}=1$이다.

우선 $x^{2^{m+st+1}}=x^d$일 때 식 (6)을 이용하면 $x^{2^{m+st+1}(2^s-1)}=\left(x^{2^{m+st+1}}\right)^{2^s-1}=\left(x^d\right)^{2^s-1}$ $=x^{2^{st+s+1}-2^{m+st+1}}$이므로 $x^{2^{m+st+s+1}}=x^{2^{st+s+1}}$이다. 즉, $x^{2^{st+s+1}}=(x^{2^{st+s+1}})^{2^m}$이므로 $x^{2^{st+s+1}}\in GF(q)$이다. 따라서 $x^{2^m}=(x^{2^{st+s+1}})^{2^{m-st-s-1}}\in GF(q)$이고 $x=x^{2^n}$ $=(x^{2^m})^{2^m}$이므로 x는 $GF(q)$의 원소이다.

다음으로 $\left(x^d\right)^{2^s-1}=1$이면 $x^d\in GF(2^s)$이고 $2s|m$이므로 $x^d\in GF(q)$이다. 보조정리 3.2에 의하여 $x(\neq 0,1)$가 방정식 (4)를 만족하면 $x^d=x$ 또는 $x^d=x^q$이다.

$x^d=x$이면 분명히 $x\in GF(q)$이고, $x^d=x^q$이면 $x^q=x^d\in GF(q)$이므로 $x=\left(x^{2^m}\right)^{2^m}=\left(x^d\right)^{2^m}$이다. 그러므로 $x\in GF(q)$이다. 따라서 방정식 (4)의 해는 $GF(q)$의 원소이다. □

<정리 3.4> $n=2m$ 이고 정수 s, t에 대해 $2st<m$, $2s|m$을 만족하면

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

에 대하여 $C_d(\tau)$의 함숫값과 발생횟수는 다음과 같다.

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

증명. 보조정리 3.1과 식(2)에 의해 상호상관함수 $C_d(\tau)$는 $x^{\frac{2^m-2^s}{2^s-1}}+yx+\bar{y}x^{-1}+x^{-\frac{2^m-2^s}{2^s-1}}=0$가 되고 이 방정식은 $x^{2^s+1}+yx^{2^s}+\bar{y}x+1=0$이다. 정리 2.3에 의해 $C_d(\tau)$는 4개의 값을 가지고 정리 2.1과 정리 3.3에 의해 S에서 $i(i=0,1,2,2^s+1)$개의 해를 가지는 횟수를 N_i라 하면 다음 식을 따른다.

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

이 연립방정식을 풀면 각 N_i의 값을 구할 수 있다. 이제 정리 2.2를 이용하여 $C_d(\tau)$의 함숫값을 구하면 $C_d(\tau)\in\{-2^m-1,-1,\ 2^m-1,2^{m+s}+1\}$이다. □

<예제> 원시다항식 $f(x)=x^8+x^4+x^3+x^2+1$의 원시근 α에 대하여, $n=8$, $s=1$, $t=2$로 두면 $d=31$이다. $u(t)=Tr_1^8(\alpha^t)$ 와 $v(t)=u(31t)$는 각각 그림 1, 그림 2와 같다. 이제 그림 1에 나타난 수열에 0부터 2^8-2까지 위상이동차를 차례로 적용시켜 그림 2에 나타난 수열과의 상호상관 함숫값을 구해보자.

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, 0, 1, 1
0, 1, 1, 1, 1, 0, 1, 0, 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, 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 1. 수열 $u(t) = Tr_1^8(\alpha^t)$의 15×17배열
Fig. 1 15×17 array of $u(t) = Tr_1^8(\alpha^t)$

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, 1, 0, 1, 1, 1, 0, 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, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 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, 0, 1, 1, 1, 0, 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 2. 수열 $v(t) = u(31t)$의 15×17 배열
Fig. 2 15×17 array of $v(t) = u(31t)$

위상이동차를 0부터 254까지 순서대로 변화시켰을 때 $C_d(\tau) \in \{-17, -1, 15, 31\}$ 이다. 이 때 각 함숫값의 발생횟수는 표 2에 나타내었다.

표 2. 상호상관 함숫값의 발생횟수
Table. 2 number of the cross-correlation value

상호상관 함숫값	-17	-1	15	31
발생횟수	80	119	16	40

Ⅳ. 결 론

본 논문에서는 의사난수열인 m-수열로부터 또다른 m-수열을 생성하기 위해 Rosendahl과 Niho의 d를 포함하는 새로운 d의 값을 제안하였다. 또한 제안된 d를 이용하여 생성된 수열의 상호상관 함숫값과 그 값의 발생횟수를 구하였다. 생성된 수열은 4 개의 상호상관 함숫값을 갖기 때문에 CDMA와 같은 통신 시스템에서 사용자가 많음으로써 발생할 수 있는 충돌을 최소화하기 위해 신호를 변조할 때 응용될 수 있는 우수한 수열이라고 생각된다.

참고문헌

[1] S.W. Golomb, “Shift-Register Sequences”, Laguna Hills, CA : Aegean Park, 1982.

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

[3] 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.

[4] 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.

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

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

[7] S.J. Cho, 유한체 및 그 응용, 교우사, 2007.

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

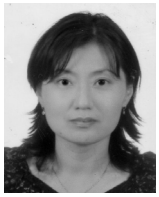
[9] T. Helleseth and P. Rosendahl, “New pairs of m -sequences with 4-level cross-correlation”, Finite Fields and Their Applications, vol. 11, no. 4, pp. 674-683, 2005.

[10] R. Gold, “Maximal recursive sequences with 3-valued cross-correlation functions”, IEEE Trans. Inf. Theory, vol. 14, pp. 154-156, 1967.

[11] T. Kasami, “The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes”, IEEE Inf. Control, vol. 18, pp. 369-394, 1971.

[12] 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.
[13] A. Canteaut, P. Charpin and H. Dobbertin, “Binary m -sequence with three-valued cross-correlation ; a proof of Welch’s”, IEEE Trans. Inf. Theory, vol. 46, pp. 4-8, 2000.
[14] H.D. Hollmann and Q. Xiang, “A proof of Welch and Niho conjectures on cross-correlation of binary m -sequences”, Finite Fields and Their Applications, vol. 7, pp. 253-286, 1976.
[15] H. Dobbertin, “One-to-one highly nonlinear power functions on $GF(2^n)$”, Applicable Algebra in Engineering, Communication and Computing, vol. 9, pp. 139-152, 1998.
[16] P. Rosendahl, “Niho Type Cross-Correlation Functions and Related Equations”, Ph.D. thesis, University of Turku, 2004.
[17] 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.

저자소개



권숙희 (Sook-Hee Kwon)

1989년 경북대학교 조경학과 졸업(농학사)
2011년 부경대학교 응용수학과 졸업(이학석사)
2011년～현재 부경대학교 응용수학과 박사과정
※ 관심분야 : 정보보호, 부호이론

조성진 (Sung-Jin Cho)

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

권민정(Min-Jeong Kwon)

1997년 부산대학교 수학교육과 졸업(이학사)
2002년 부산대학교 교육대학원 수학과 졸업(교육학석사)
2007년～현재 부경대학교 응용수학과 박사과정
※ 관심분야 : 셀룰라 오토마타론, 정보보호

김한두(Han-Doo Kim)

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

최언숙(Un-Sook Choi)

1992년 성균관대학교 산업공학과 졸업(공학사)
2000년 부경대학교 대학원 응용수학과 졸업(이학석사)
2004년 부경대학교 대학원 응용수학과 졸업 (이학박사)
2009년 부경대학교 대학원 정보보호학과 졸업 (공학박사)
2006년～현재: 동명대학교 자율전공학부 교수
※관심분야 : 셀룰라 오토마타론, 정보보호, 암호이론

김진경(Jin-Gyoung Kim)

2008년 부경대학교 응용수학과 졸업(이학석사)
2013년 부경대학교 응용수학과 졸업(이학박사)
※ 관심분야 : 셀룰라 오토마타론, 유한체