상호상관관계 함숫값이 4개인 새로운 데시메이션

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

New Decimations with 4-Valued Cross-Correlations

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

요 약

본 논문에서는 주기 2^n-1인 m-수열에 새로운 데시메이션을 적용하여 얻은 Gold 계열의 이진수열을 제안하고, 제안된 이진수열의 상호상관관계 함숫값이 4개임을 보인다.

ABSTRACT

In this paper, we present a new decimated Gold-like m-sequence with a binary m-sequence of period 2^n-1. And we show that the cross-correlation function of the proposed sequence is four-valued.

키워드

decimation, pseudo-random sequences, trace function, cross-correlation, finite fields
데시메이션, 의사난수열, 트레이스 함수, 상호상관관계, 유한체

Ⅰ. 서 론

사용자의 이동성을 전제로 하는 무선통신인 이동통신 시스템의 목표는 언제, 어디서나, 누구에게나 시간과 공간을 초월하여 정보를 정확하게 주고받는 것이다. 다중화(multiplexing)와 다중 접속(multiple access)은 여러 사용자가 주파수와 시간 등을 공유하도록 하여 사용자의 수를 늘림으로써 이동통신 시스템의 목표에 부합하기 위해 사용하는 기술이다. CDMA 방식은 여러 사용자들의 신호를 처리하거나 여러 사용자들이 중앙통신장치에 접속할 때 부호를 분할하여 채널을 구분하는 방식이다[1]. 따라서 여러 사용자가 시간과 주파수를 공유하면서 각 사용자는 자신에게 할당된 부호만을 이용하여 대역확산(spread spectrum)하여 전송하고, 수신자는 송신측에서 사용된 부호를 사용하여 역확산(despreading)시켜 원하는 정보를 얻게 되므로 할당된 부호간의 상호상관관계(cross-correlation)는 낮으면서 자기상관관계(auto- correlation)는 높은 수열을 부호로 사용하는 것이 바람직하다[2,3]. 이러한 수열의 설계에 대한 연구도 이뤄지고 있다[4,5]. 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 있으

* 부경대학교 응용수학과(mjblack02@hanmail.net)
** 교신저자 : 부경대학교 응용수학과(sjcho@pknu.ac.kr)
*** 인제대학교 컴퓨터응용과학부
**** 동명대학교 자율전공학부
접수일자 : 2012. 06. 20 심사(수정)일자 : 2012. 07. 26 게재확정일자 : 2012. 08. 09

므로 완전히 랜덤한 부호를 이용할 수 없다. 따라서 이러한 시스템에서는 의사난수열(pseudo-random sequence)을 부호로 사용한다.

본 논문에서는 의사난수열인 두 개의 m-수열에 의해 생성되는 Gold 계열의 새로운 이진수열군을 생성하기 위한 d의 값을 제안하고, 그 수열의 상호상관관계 함숫값을 분석하여 제안된 수열은 상호상관관계 함숫값이 4개인 우수한 비선형 이진수열임을 보이고자 한다.

II. 배경 지식

이 절에서는 데시메이션(decimation)과 트레이스 함수를 이용하여 Gold 계열의 수열을 정의하고 두 수열의 상호상관관계 함수를 정의한다. 또한 상호상관관계 함수의 함숫값을 구하는 과정에서 유도되는 방정식에 대해 살펴보겠다.

원소의 개수가 2^n개인 유한체는 $GF(2^n)$으로 나타내고 곱셈에 대하여 닫혀있는 $GF(2^n)$의 부분군은 $GF(2^n)^* = GF(2^n) \setminus \{0\}$로 나타내자. $GF(2^n)$의 원시원소는 $GF(2^n)^*$의 모든 원소를 생성한다[6-8].

유한체 $GF(2^n)$에서 부분체 $GF(2^k)$으로의 트레이스 함수 $Tr_k^n(\cdot)$는 $GF(2^n)$의 임의의 원소 x에 대하여

$$Tr_k^n(x) = \sum_{i=0}^{n/k-1} x^{2^i} = x + x^{2^1} + \cdots + x^{2^{(n/k-1)k}}$$

으로 정의된다. $GF(2^n)$의 임의의 원소 x, y와 $GF(2^k)$의 임의의 원소 a, b에 대하여 트레이스 함수는 다음을 만족한다[7, 8].

(a) $Tr_k^n(ax+by) = aTr_k^n(x) + bTr_k^n(y)$

(b) 음이 아닌 정수 i에 대하여
$Tr_k^n(x) = Tr_k^n(x^{2^{ki}}) = \{Tr_k^n(x)\}^{2^{ki}}$

(c) $Tr_1^n(x) = Tr_1^k[Tr_k^n(x)]$

(d) $GF(2^k)$의 임의의 원소 β에 대하여 방정식 $Tr_k^n(x) = \beta$를 만족하는 해의 개수는 2^{n-k}이다.

시프트 레지스터(shift register) n개에 의해 만들어진 최대주기 2^n-1인 m-수열 $u(t)$ $(t=0,1,2,\cdots,2^n-2)$는 한 주기 동안의 2^n-1개 수열 중 '0'은 $2^{n-1}-1$개가 있고 '1'은 2^{n-1}개가 존재한다. 즉, 항상 '0'의 개수가 '1'의 개수보다 하나 더 적음을 알 수 있다. 또한 '0'과 '1' 각각에 대해 연속하여 $n-i$ $(i \geq 2)$번 반복되는 경우는 $i-1$번 발생한다. 최대주기수열 $u(t)$는 점화식에 의해 생성되고 주기가 있으므로 완전히 랜덤한 값을 갖지는 않지만 위와 같은 통계적 성질을 갖고 있으므로 의사난수열이다[3, 7].

두 개의 m-수열 $u(t)$와 $v(t)$ $(t=0,1,2,\cdots)$는 주기가 2^n-1인 수열이라 하고 ω는 $GF(2^n)$의 원시원소라 하자. 트레이스 함수를 이용하여

$$u(t) = Tr_1^n(\omega^t),\ v(t) = u(dt) \tag{1}$$

라 할 때, $u(t)+v(t)$를 Gold 계열의 수열이라 하고 d를 데시메이션이라 한다[7,9]. 본 논문에서는 $d \equiv 1 \pmod{2^n-1}$ 인 경우로 제한한다.

위상이동차 $\tau = 0, 1, 2, \cdots, 2^n-2$ 에 대하여 두 수열 $u(t)$와 $v(t)$의 상호상관관계 함수는

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

으로 정의되고 (1)과 (2)를 이용하면

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

으로 간단히 나타낼 수 있다.

$q = 2^k$ 이라 하면 $GF(q^2)$은 $GF(q)$의 확장체이다. $GF(q^2)$의 모든 원소 x에 대하여 x^q을 $\overline{x}$라 정의하고 $x\overline{x}=1$을 만족하는 $GF(q^2)$의 원소들의 집합을 S라 하면 집합 S는

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

이다.

α를 $GF(q^2)$의 원시원소라 하면 $GF(q^2)$의 임의의 원소 x는 $x = \alpha^t$, $t \in \{0, 1, \cdots, 2^n-2\}$ 이다.

여기서 $Q=q+1$ 라 두고 $t=t_1Q+t_2$ $(0\le t_1\le q-2, 0\le t_2\le q)$로 나타내면

$$x=\alpha^t=\alpha^{t_1Q+t_2}=(\alpha^Q)^{t_1}\alpha^{t_2}$$

이다. $\alpha^{t_2}=\gamma$, $(\alpha^Q)^{t_1}=\delta$ 라 하면 $\delta^q=(\alpha^Q)^{t_1q}=(\alpha^{Qq})^{t_1}=(\alpha^{q^2-1+q+1})^{t_1}=(\alpha^{q+1})^{t_1}=\alpha^{Qt_1}=\delta$ 이 되므로 δ는 $GF(q)^*$의 원소이다. 따라서 $GF(q^2)$의 모든 원소 x는

$$x=\delta\gamma \tag{3}$$

$$(\delta\in GF(q)^*,\ \gamma\in\{1,\alpha,\alpha^2,\cdots,\alpha^q\})$$

이다. $q=2^k$ 인 경우 $q+1$과 $q-1$은 서로소이므로

$$\{1,\alpha,\alpha^2,\cdots,\alpha^q\}\cong S \tag{4}$$

이다.

$GF(q^2)$의 원시원소 α에 대하여 두 m-수열 $u(t)=Tr_1^n(\alpha^t)$, $v(t)=u(dt)$의 상호상관관계 함수는

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

이고 $x=\alpha^t$, $y=\alpha^\tau$로 두면

$$C_d(\tau)=\sum_{x\in GF(2^n)^*}(-1)^{Tr_1^n(yx+x^d)}$$

이다. (3), (4) 에 의해 $GF(q^2)$의 모든 원소 x는 $x=\delta\gamma$, $\delta\in GF(q)^*$, $\gamma\in S$ 이므로

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

이다. 그러므로

$$\begin{aligned}&\sum_{x\in GF(q^2)^*}(-1)^{Tr_1^n(yx+x^d)}\\&=-(q+1)+\\&\qquad\sum_{\gamma\in S}\left[\sum_{\delta\in GF(q)}(-1)^{Tr_1^k[\delta(y\gamma+\gamma^d+\bar{y}\gamma^{-1}+\gamma^{-d})]}\right]\end{aligned}$$

이다. 따라서 $C_d(\tau)$의 함숫값은

$$y\gamma+\gamma^d+\bar{y}\gamma^{-1}+\gamma^{-d}=0$$

을 만족하는 $\gamma\in S$의 개수에 의해 결정된다. 이와 같은 사실을 이용하여 Niho는 다음 정리를 증명하였다[11].

<정리 2.1> $d\equiv 1(\mathrm{mod}\,2^k-1)$ 을 만족하는 데시메이션 d와 $GF(q^2)^*$의 임의의 원소 y에 대하여 $C_d(\tau)$ $(\tau=0,1,2,\cdots,2^n-2)$의 값은

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

여기서 $N(y)$는 $x^{2d}+yx^{d+1}+\bar{y}x^{d-1}+1=0$을 만족하는 집합 S의 원소 x의 개수이다.

Helleseth는 2005년 $x^{2^s+1}+yx^{2^s}+\bar{y}x+1=0$ 의 해의 개수에 관하여 다음 정리를 증명하였다[12].

<정리 2.2> $y\in GF(q^2)^*$에 대하여 방정식

$$x^{2^s+1}+yx^{2^s}+\bar{y}x+1=0$$

에서 S에 존재하는 해 x의 개수는 0, 1, 2, $2^{\gcd(s,k)}+1$개 중 하나이다.

III. 상호상관관계 함숫값이 4개인 새로운 이진수열

이 절에서는 n은 4의 배수이면서 $n=2k$를 만족하는 k와 $\gcd(s,n)=1$을 만족하는 정수 s, 그리고 s의 배수이면서 홀수인 i에 대해 주기가 2^n-1인 m-수열로부터 다음과 같이 새로운 데시메이션 d를 정의하고 이를 이용하여 수열을 생성한다.

$$d=\frac{1}{2^s-1}\left(2^{k(i+1)}-2^{ki}+2^{s+1}-2^k-1\right) \quad (5)$$

정리 2.1과 정리 2.2에 의해 m-수열과 (5)를 이용하여 생성한 두 수열의 상호상관관계 함숫값이 4개가 됨을 보인다.

$\gcd(s,n)=1$이고 짝수 k에 대하여 $\gcd(s,k)=1$이므로 s는 홀수다. 따라서 $\frac{s}{\gcd(s,k)}$가 홀수이므로 $\gcd(2^k+1,2^s-1)=1$이다. 또, $2^k+1=2^{k-s}(2^s+1)-2^{k-s}+1$ 이므로 $\gcd(2^k+1,2^s+1)=\gcd(2^s+1,2^{k-s}-1)$ 이다. 그런데 $\frac{k-s}{\gcd(s,k-s)}=\frac{k-s}{\gcd(s,k)}$ 도 홀수이므로 $\gcd(2^s+1,2^{k-s}-1)=1$ 이고, 따라서 $\gcd(2^k+1,\ 2^s+1)=1$ 이다. 이를 이용하여 다음을 증명한다.

<보조정리 3.1> n은 4의 배수이고 $n=2k$라 하자. 그리고 n과 서로소인 정수 s와 s의 배수인 홀수 i에 대하여

$$d=\frac{2^{k-1}}{2^s-1}\left(2^{k(i+1)}-2^{ki}+2^{s+1}-2^k-1\right)$$

는 다음 성질을 만족한다.

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

(2) $d\equiv \frac{2^{ki}-2^s}{2^s-1} \pmod{2^k+1}$

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

증명. (1)은 간단한 계산을 통하여 쉽게 알 수 있다.

(2) $d=2^{k-1}\left\{\frac{2^{ki}-2^s}{2^s-1}(2^k-1)+2^k+1\right\}$

$\equiv \frac{2^{ki}-2^s}{2^s-1} \pmod{2^k+1}$

(3) (1)과 (2)에 의해

$$\gcd(d,2^n-1)=\gcd(d,2^k+1)=\gcd\left(\frac{2^{ki}-2^s}{2^s-1},2^k+1\right)$$

이다. 그리고 $\gcd(2^s-1,2^k+1)=1$이므로

$$\gcd\left(\frac{2^{ki}-2^s}{2^s-1},2^k+1\right)=\gcd(2^{ki}-2^s,2^k+1)$$

이다. 또한 $2^{ki}-2^s\equiv -1-2^s \pmod{2^k+1}$ 이므로 $\gcd(2^{ki}-2^s,2^k+1)=\gcd(2^k+1,2^s+1)=1$이다. 따라서 $\gcd(d,2^n-1)=1$이다. □

<정의 3.2 [13]> 두 데시메이션 d와 e에 대하여

$$e\equiv p^i d \pmod{p^n-1}$$

를 만족하는 양의 정수 i가 존재할 때 d와 e는 동치(equivalent)라고 한다.

<보조정리 3.3 [11]> 두 데시메이션 d, e가 동치이면 각 $y\in GF(p^n)$에 대하여

$$\Delta_d(y)=\Delta_e(y^{-d})$$

이 성립한다. 여기서 $\Delta_d(\tau)=C_d(\tau)+1$, $\tau=0,1,2,\cdots$ 이다.

$\gcd(d,\ 2^n-1)=1$ 이므로 $\{y^{-d}\mid y\in GF(2^n)\}=GF(2^n)$이다. 따라서 보조정리 3.3에 의해 두 데시메이션 d와 e가 동치이면 $C_d(\tau)$와 $C_e(\tau)$가 같고 함숫값의 발생횟수도 같다.

보조정리 3.1과 3.3을 이용하여 다음 정리를 얻는다.

<정리 3.4> n은 4의 배수, $n=2k$라 하고 s는 n과 서로소인 정수, 홀수 i는 s의 배수일 때 데시메이션 $d=\frac{2^{k-1}}{2^s-1}\left(2^{k(i+1)}-2^{ki}+2^{s+1}-2^k-1\right)$에 대해 $C_d(\tau)$의 함숫값은 $\{-2^k-1,-1,2^k-1,2^{k+1}-1\}$에 포함된다.

<예제 3.5> 8차 원시다항식 $f(x)$가 $f(x)=x^8+x^4+x^3+x^2+1$일 때 $f(x)$의 원시근 α에 대하여 주기가 2^8-1인 두 m-수열 $u(t)$, $v(t)$에 대한 상호상관관계의 함숫값을 분석해보자.

$n=8$이므로 $k=4$이다. $s=1$, $i=3$으로 두면

$d=227$이다. $u(t)=Tr_1^n(\alpha^t)$는 그림 1과 같고, $v(t)=u(227t)$는 그림 2와 같다. $\tau=201$일 때, $u(201+t)$는 그림 3과 같다. 따라서 $C_{227}(201)=-2^4-1=-17$이다. 같은 방법으로 0부터 254까지 τ의 값을 차례대로 변화시키면서 $C_d(\tau)$의 값을 구하면 $\{-17,-1,15,31\}=\{-2^4-1,-1,2^4-1,2^{4+1}-1\}$으로 4개의 값 중 하나가 된다.

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, 1, 0, 1, 1
0, 1, 1, 1, 1, 0, 1, 0, 1, 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, 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, 0, 1, 1, 1, 0, 1, 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, 1, 0, 1, 0, 1, 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 $v(t)=u(227t)$의 15×17 배열
Fig. 2 15×17 array of $v(t)=u(227t)$

0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 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, 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
1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 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

그림 3. 수열 $u(201+t)$의 15×17배열
Fig. 3 15×17 array of $v(t)=u(227t)$

IV. 결 론

본 논문에서는 CDMA 통신에서 부호 분할을 위해 사용되는 의사난수열에 대해 d의 값을 이용하여 주기가 같은 새로운 수열을 생성하고 두 수열의 상호상관 관계 함숫값이 4개임을 보였다.

참고 문헌

[1] M.K. Simon, J. K. Omura, R.A. Sholtz, and B. K. Levitt, “Spread Spectrum Communications”, Rockville, MD : Computer Sci., Vol. 1, pp. 45-65, 1985.

[2] L.D. Baumert, “Cyclic Difference Sets”, Lecture Notes in Mathematics, New York : Springer-Verlag, Vol. 182, 1971.

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

[4] 최언숙, 조성진, “최적의 상호상관관계를 갖는 이진 수열의 설계”, 한국전자통신학회논문지, 6권, 4호, pp. 539-544, 2011.

[5] 김한두, 조성진, 권민정, 안현주, “확장 Zeng 수열의 상호상관 함숫값에 대한 연구”, 한국전자통신학회논문지, 7권, 1호, pp. 69-80, 2012.

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

[7] R. McEliece, Finite fields for computer scientists and engineers, Kluwer Academic

Publisher, Boston, 1987.
[8] 조성진, “유한체 및 그 응용”, 교우사, pp. 65-75, 2012.
[9] R. Gold, "Maximal recursive sequences with 3-values cross-correlation functions", IEEE Trans. Inform. Theory, Vol. 14, pp. 154-156, 1967.
[10] J. Lahtonen, "On the odd and aperiodic correlation properties of the Kasami sequences", IEEE Trans. Inf. Theory, Vol. 41, No. 5, pp. 369-394, 1971.
[11] Y. Niho, "Multi-valued Cross-Correlation functions between two maximal linear recursive sequences", Ph.D. thesis, University of Southern California, 1972.
[12] 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.
[13] P. Rosendahl, “Niho Type Cross-Correlation Functions and Related Equations”, Ph.D. thesis, University of Turku, 2004.

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 수리과학부 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호

권숙희(Sook-Hee Kwon)

1989년 2월 경북대학교 조경학과 졸업(이학사)
2011년 2월 부경대학교 응용수학과 졸업(이학석사)
※ 관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론, 컴퓨터 구조론

김진경(Jin-Gyoung Kim)

2008년 2월 부경대학교 대학원 응용수학과 졸업 (이학석사)
2008년~현재 부경대학교 대학원 응용수학과 박사과정
※ 관심분야 : 셀룰라 오토마타론, 유한체

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

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