최적의 상호상관관계를 갖는 이진 수열의 설계

최언숙* · 조성진**

Design of Binary Sequences with Optimal Cross-correlation Values

Un-Sook Choi* · Sung-Jin Cho**

요 약

적당한 정수 $n(\geq 1)$에 대하여 2-valued 자기상관관계를 갖는 주기가 2^n-1인 균형 이진 수열(balanced binary sequences)은 대역확산 통신 시스템(spread-spectrum communication system)에서 많이 응용되고 있다. 본 논문에서는 르장드르 수열에 의해 구성되는 새로운 3-valued 비선형 이진 수열을 제안한다. 이 수열은 유한체 위에서 트레이스를 이용해 생성하는 가장 우수한 수열인 m-수열, GMW 수열, Kasami 수열, No 수열을 모두 포함한다. 제안된 수열은 Klapper에 의해 제안된 이차형식 수열보다 더 낮은 상호상관관계를 갖는다.

ABSTRACT

Balanced binary sequences of period $2^n-1(n \geq 1)$ having the two-valued autocorrelation function have many applications in spread-spectrum communications system. In this paper we propose new nonlinear binary sequences which are constructed from Legendre sequences with the same cross-correlation as the sequences proposed by Cho. These sequences include the m-sequences, GMW sequences, Kasami sequences and No sequences which are described in terms of the trace function over a finite field. Also the proposed sequences have more low cross-correlation distribution than the quadratic form sequences proposed by Klapper.

키워드

cross-correlation, auto-correlation, trace, binary sequences, Legendre sequences, pseudorandom sequence
상호상관관계, 자기상관관계, 트레이스, 이진수열, 르장드르 수열, 의사난수열

Ⅰ. 서 론

고속 통신을 위하여 현대의 무선통신은 점차 고주파 대역을 이용하는 방향으로 나아가고 있으며 고주파 대역의 특성상 셀의 크기는 점점 작아져 마이크로 셀룰러 환경이 되고 있다. 이러한 환경에 적합한 시스템으로 부호 분할 다원 접속(CDMA) 시스템에서 링크 상에서 지연 수를 칩 내로 제한한 준 동기 부호 분할 다원 접속(Quasi Synchronous CDMA : QS-CDMA) 시스템이 제안되었다. 이러한 준 동기 부호 분할 다원 접속 시스템이 효율적인 성능을 내기 위해서는 낮은 상관관계를 갖는 수열 군을 사용하는 것이 필수적이다[1,2].

적당한 정수 n에 대하여 자기상관관계(auto-correlation)값으로 -1또는 2^n-1을 갖는 주기가 2^n-1인 균형 이진수열(balanced binary sequences)[3]은 대역확산 통신 시스템(spread- spectrum communication system)에서 많이 응용되고 있다[4].

* 동명대학교 자율전공학부(choies@tu.ac.kr)
** 교신저자 : 부경대학교 응용수학과(sjcho@pknu.ac.kr)
접수일자 : 2011. 07. 07
심사(수정)일자 : 2011. 07. 28
게재확정일자 : 2011. 08. 12

이러한 수열로 잘 알려진 수열군은 m-수열, GMW 수열, Mersenne 소수를 이용한 Legendre 수열, Kasami 수열, No 수열, 이차형식 수열 등이 있다. 이 밖에도 트레이스를 이용한 여러 수열들이 연구되었다[5-10]. 또한 다양한 방법에 의해 생성되는 수열들이 소개되고, 분석되었다[11~14]. 본 논문에서는 Cho 등에 의해 제안된 이진수열[15]과 같은 상호상관관계를 가지며 Legendre 수열에 의해 구성되는 새로운 3-valued 비선형 이진 수열을 제안한다. 이 수열은 유한체 위에서 트레이스를 이용해 생성하는 가장 우수한 수열인 m-수열, GMW 수열, Kasami 수열, No 수열을 모두 포함한다. 제안된 수열은 Klapper에 의해 제안된 이차형식 수열보다 더 낮은 상호상관관계를 가지며 이는 최적의 상호상관관계를 갖는 이진수열이다.

II. 배경지식 및 기존 연구

주어진 크기의 의사불규칙(pseudorandom) 수열 군에 대한 바람직한 몇 가지 성질은 낮은 자기상관관계 값, 낮은 상호상관관계(cross- correlation) 값, 큰 선형복잡도(linear span), 균형성질(balanced property), 많은 서로 다른 수열군의 존재성, 구현의 용이성 등이다.

지금까지 발견된 주기가 2^n-1이고 이상적인 자기상관 특성을 갖는 의사불규칙 수열들 중 대표적인 것이 m-수열, GMW 수열, Kasami 수열, Gold 수열, Bent 수열, No 수열, Legendre 수열 등이 있다. 또한 낮은 상호상관관계 값은 부호 분할 다원 접속의 능력을 가지기 위해 중요하다. Welch[16]에 의해 유도된 최대 상관관계 값에 대한 하한은 의사불규칙 수열군의 상관관계 성질을 평가하는 데 자주 이용된다. m-수열, GMW 수열, 작은 집합의 Kasami 수열, Bent 수열, No 수열, Legendre 수열 등은 이러한 하한의 관점에서 최적인 상관관계 값을 갖는 수열 군들이다.

2.1 트레이스함수와 상호상관관계

트레이스(Trace)함수는 유한체로부터 부분체로의 선형매핑인데, 이 함수는 의사불규칙 수열의 설계와 분석을 위한 중요한 수학적 도구이다. 트레이스함수에 대한 정의와 그것들의 성질을 보면 대부분의 이진 의사불규칙 수열들은 트레이스 함수의 형태로 표현될 수 있다.

$GF(2^n)$를 2^n개의 원소를 가진 유한체라 하고, $GF(2^n)^* = GF(2^n)/\{0\}$ 라 하자. 1보다 큰 정수 k와 m에 대하여 $n = km$라 하자. 또한 $Q = \frac{2^n-1}{2^m-1}$ 라 하자. 차수가 n인 원시다항식 $f(x)$의 원시근을 $\alpha(\in GF(2^n))$라 하자. m이 n의 약수이므로 $GF(2^m) \subset GF(2^n)$ 이다. 임의의 자연수 l에 대하여 $\mathbb{Z}(l) = \{0, 1, \cdots, l\}$ 라 하자. 본 논문에서 수열의 생성을 위해 사용되는 트레이스 함수 $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$ 는 식(1)과 같이 정의된다.

$$Tr_m^n(x) = \sum_{i=0}^{k-1} x^{2^{mi}} \quad (1)$$

예를 들어 $n = 4$이고 $m = 2$이라 하자. 이 때, $f(x) = x^4 + x + 1$ 라 하고, α를 $\alpha^4 = \alpha + 1$ 을 만족하는 $GF(2^4)$의 원시원소라 하자. β를 $GF(2^2)$의 한 원시원소라 하면 $\beta^2 = \beta + 1$ 를 만족하고 α와 β는 $\beta = \alpha^{(2^4-1)/(2^2-1)} = \alpha^5$ 를 만족한다. 이 때, $Tr_2^4(x)$ $(x \in (GF(2^4))$ 를 구하면 표 1과 같다.

표 1. $GF(2^4)$의 원소에 대한 트레이스
Table 1. Trace of elements in $GF(2^4)$

$Tr_2^4(1) = 1 + 1^{2^1} = 1 + 1^4 = 0$
$Tr_2^4(\alpha) = \alpha + \alpha^{2^1} = \alpha + \alpha^4 = 1$
$Tr_2^4(\alpha^2) = \alpha^2 + (\alpha^2)^{2^1} = \alpha^2 + \alpha^8 = (\alpha + \alpha^4)^2 = 1$
$Tr_2^4(\alpha^3) = \alpha^{3+}(\alpha^3)^{2^1} = \alpha^3 + \alpha^{12} = \alpha^3 + (\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^2 + \alpha + 1 = \alpha^{10} = \beta^2$
$Tr_2^4(\alpha^4) = \alpha^4 + (\alpha^4)^{2^1} = \alpha^4 + \alpha^{16} = (\alpha + \alpha^4)^4 = 1$
$Tr_2^4(\alpha^5) = \alpha^5 + (\alpha^5)^{2^1} = \alpha^5 + \alpha^5 = 0$
$Tr_2^4(\alpha^6) = \alpha^6 + (\alpha^6)^{2^1} = \alpha^6 + \alpha^9 = (\alpha^2 + \alpha^3) + (\alpha + \alpha^3) = \alpha + \alpha^2 = \alpha^5 = \beta$
$Tr_2^4(\alpha^7) = \alpha^7 + (\alpha^7)^{2^1} = \alpha^7 + \alpha^{13} = (1 + \alpha + \alpha^3) + (1 + \alpha^2 + \alpha^3) = \alpha + \alpha^2 = \alpha^5 = \beta$
$Tr_2^4(\alpha^8) = \alpha^8 + (\alpha^8)^{2^1} = \alpha^8 + \alpha^2 = (\alpha + \alpha^4)^2 = 1$
$Tr_2^4(\alpha^9) = \alpha^9 + (\alpha^9)^{2^1} = \alpha^9 + \alpha^6 = (\alpha + \alpha^3) + (\alpha^2 + \alpha^3) = \alpha + \alpha^2 = \alpha^5 = \beta$
$Tr_2^4(\alpha^{10}) = \alpha^{10} + (\alpha^{10})^{2^1} = \alpha^{10} + \alpha^{10} = 0$
$Tr_2^4(\alpha^{11}) = \alpha^{11+}(\alpha^{11})^{2^1} = \alpha^{11} + \alpha^{14} = (\alpha + \alpha^2 + \alpha^3) + (1 + \alpha^3) = \alpha^2 + \alpha + 1 = \alpha^{10} = \beta^2$
$Tr_2^4(\alpha^{12}) = \alpha^{12+}(\alpha^{12})^{2^1} = \alpha^{12} + \alpha^3 = (1 + \alpha + \alpha^2 + \alpha^3) + \alpha^3 = \alpha^2 + \alpha + 1 = \alpha^{10} = \beta^2$
$Tr_2^4(\alpha^{13}) = \alpha^{13} + (\alpha^{13})^{2^1} = \alpha^{13} + \alpha^7 = (1 + \alpha^2 + \alpha^3) + (1 + \alpha + \alpha^3) = \alpha + \alpha^2 = \alpha^5 = \beta$
$Tr_2^4(\alpha^{14}) = \alpha^{14+}(\alpha^{14})^{2^1} = \alpha^{14} + \alpha^{11} = (1 + \alpha^3) + (\alpha + \alpha^2 + \alpha^3) = \alpha^2 + \alpha + 1 = \alpha^{10} = \beta^2$

트레이스함수 $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$ 는 다음 성질을 만족한다[17].

(a) $Tr_m^n(x+y) = Tr_m^n(x) + Tr_m^n(y)\ \forall x,y \in GF(2^n)$.

(b) $Tr_m^n(cx) = c\,Tr_m^n(x),\ \forall c \in GF(2^m),\ x \in GF(2^n)$.

(c) Tr_m^n는 전사함수이다.

(d) $Tr_m^n(c) = kc,\ \forall c \in GF(2^m)$.

(e) $Tr_m^n(x^{2^m}) = Tr_m^n(x),\ \forall x \in GF(2^n)$.

(f) $Tr_1^n(x) = Tr_1^m(Tr_m^n(x)),\ \forall x \in GF(2^n)$.

(g) 임의의 고정된 $\beta \in GF(2^m)$에 대하여 방정식 $Tr_m^n(x) = \beta$를 만족하는 해 $x(\in GF(2^n))$가 2^{n-m}개 존재한다.

성질 (g)는 표 1에서 확인할 수 있다. 즉 β에 대응되는 원소는 $\alpha^6, \alpha^7, \alpha^9, \alpha^{13}$로 2^2개이고 나머지 원소 $\beta^2, 1, 0$에 대해서도 2^2개 씩 존재한다. 표 1에서 원소 0에 대응하는 원소 중 $Tr_2^4(0) = 0$가 생략되었다.

주기가 $2^n - 1$인 주어진 두 수열 $s_i(t)$와 $s_j(t)$의 상호 상관관계 $R_{ij}(\tau)$는 식 (2)와 같이 정의된다.

$$R_{ij}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_i(t)+s_j(t+\tau)} \tag{2}$$

예를 들어 $s_i(t) = 1001011$ 이고 ,
$s_j(t) = 0010111$이라 하면 $\tau = 1$일 때,
$s_j(t+1) = 0101110$이고,
$R_{ij}(1) = -1-1+1+1-1+1-1 = -1$이다.
또한 $\tau = 5$일 때, $s_j(t)$는 $s_j(t+5) = 1100101$이다.
따라서 $R_{ij}(5) = 1-1+1-1-1-1+1 = -1$ 이다.

2.2 기존 연구 분석

본 논문에서 언급되고 있는 최적의 상관관계를 갖는 수열들을 살펴보자.

m-수열 $m(t)$와 GMW 수열 $g(t)$은 다음 식 (3), (4)와 같다[5,6].

$$m(t) = Tr_1^n(\alpha^t) \tag{3}$$

$$g(t) = Tr_1^m([Tr_m^n(\alpha^t)]^r) \tag{4}$$

여기서 α는 $GF(2^n)$의 한 원시원소이고, $1 \le r < 2^m - 1$, $\gcd(r, 2^m - 1) = 1$을 만족한다. m-수열의 상호상관관계는 $\{2^n - 1, -1\}$의 원소 중 하나이다. 상호상관관계가 $2^n - 1$인 경우는 $s_i(t)$와 $s_j(t+\tau)$가 같은 수열일 때이다. 비선형 수열로 m-수열과 상호상관관계가 같은 수열은 GMW 수열이 유일하다. Welch bound에 의하면 $n = 2m$일 때, 상호상관관계가 $\{-2^m - 1, -1, 2^m - 1\}$의 원소 중 하나가 되는 수열을 적의 상관관계를 갖는 수열이라 한다. 다음에 소개 되는 수열들은 모두 최적의 상관관계를 갖는 비선형 수열들이다.

$n = 2m$이라 하고 $Q = \dfrac{2^n - 1}{2^m - 1} = 2^m + 1$ 이라 하자. 그러면 Kasami 수열 $K_i(t)$와 No 수열 $N_i(t)$는 식 (5)와 (6)과 같다[8,9].

$$K_i(t) = Tr_1^n(\alpha^{2t}) + Tr_1^m(\gamma_i \alpha^{Q \cdot t}) \tag{5}$$

$$N_i(t) = Tr_1^m\{[Tr_m^n(\alpha^{2t}) + \gamma_i \alpha^{Q \cdot t}]^r\} \tag{6}$$

여기서 α는 $GF(2^n)$의 한 원시원소이고, $\gamma_i \in GF(2^m)$이다. 그리고 정수 r에 대하여 $1 \le r < 2^m - 1$이고 $\gcd(2^m - 1, r) = 1$이다. 그림 1은 m-수열과 GMW 수열, Kasami 수열, No 수열 사이의 관계를 나타내고 있다.

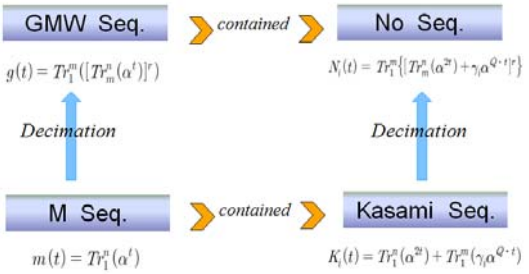

그림 1. 의사불규칙 수열 사이의 관계
Fig. 1 Relations between pseudo-random sequences

임의의 소수 p에 대하여 주기가 p인 Legendre 수열 $b(t)$는 식 (7)과 같이 정의된다[7].

$$b(t)=\begin{cases}0, & t\text{가 } \bmod p \text{에 대하여 이차잉여}\\ 1, & o/w\end{cases} \tag{7}$$

식 (7)의 $b(t)$가 이상적인 자기상관관계 값을 갖기 위한 필요충분조건은 $p\equiv 3(\bmod 4)$이다. 특히 $p=2^n-1$인 소수(Mersenne 소수, Mersenne prime)가 주기인 Legendre 수열은 유한체상에서 정의되는 트레이스함수를 이용하여 식 (8)과 같이 표현한다[7].

$$c(t)=\sum_{i=0}^{\frac{2^m-2}{2m}-1} Tr_1^m(\alpha^{u^{2i}}t) \tag{8}$$

여기서 u는 $\mathbb{Z}_p=\{0,1,2,\cdots,p-1\}$ 의 원시원소이다. 이상적인 자기상관 특성을 갖는 짧은 주기 2^m-1의 의사불규칙 수열로부터 이상적인 자기상관 특성을 갖는 긴 주기 2^n-1의 의사 불규칙 수열을 만들 수 있다. 이를 트레이스 함수를 이용하여 나타내면 식 (9)와 같다.

$$c(t)=\sum_{i=0}^{\frac{2^m-2}{2m}-1} Tr_1^m\left\{[Tr_m^n(\alpha^t)]^{u^{2i}\cdot r}\right\} \tag{9}$$

여기서 α는 $GF(2^n)$의 한 원시원소이고, $\gcd(2^m-1,r)=1$이다.

III. 3-valued 비선형 이진 수열

본 논문에서는 상호 상관관계 값으로 3개를 갖는 Legendre 수열을 트레이스로 표현한 비선형 이진 수열을 제안한다.

<정리 1[18]> 지수집합 I에 대하여 주기가 2^m-1인 이진 수열 $b(t)$가

$$b(t)=\sum_{a\in I} Tr_1^m(\beta^{at}) \tag{10}$$

이고 이상적인 자기상관 성질을 가진다고 하자. 정수 $r(1\le r\le M-1)$ 에 대하여 $\gcd(r,M)=1$이라 하면, 주기가 2^n-1인 비선형 수열 $s(t)$가

$$s(t)=\sum_{a\in I} Tr_1^m\left\{[Tr_m^n(\alpha^t)]^{ar}\right\} \tag{11}$$

과 같이 정의될 때, $s(t)$도 이상적인 자기상관관계를 갖는다. □

n과 m이 양의 정수이고 $n=2m$이라 하자. α가 $GF(2^n)$의 원시원소이고, β는 $GF(2^m)$의 원시원소라 하자. 두 원소 α,β 사이의 관계는 $\alpha^Q=\beta$를 만족한다고 하자. 여기서 $Q=\dfrac{2^n-1}{2^m-1}=2^m+1$이다. I가 식 (10)에서 정의된 집합이라 하자. 비선형 수열 S가 다음과 같이 정의된다고 하자.

$$S=\left\{s_i(t)\,|\,0\le t\le N-1,\ 1\le i\le 2^m\right\} \tag{12}$$

여기에서 $s_i(t)$는 식 (13)을 만족한다.

$$s_i(t)=\sum_{a\in I} Tr_1^m\left\{\left[Tr_m^n\left(\alpha^{2t}+u_i\alpha^{2^{m+1}t}\right)+v_i\beta^t\right]^{ar}\right\} \tag{13}$$

여기서 $u_i\in GF(2^n)$이고, $v_i\in GF(2^m)$이다. 식 (13)에서 $Tr_m^n\left(\alpha^{2t}+u_i\alpha^{2^{m+1}t}\right)+v_i\beta^t\ (:=G_i(\alpha^t))$라 두면 $s_i(t)$는 $G(\alpha^t)$를 이용하여 다음과 같이 나타낼 수 있다.

$$s_i(t)=\sum_{a\in I} Tr_1^m\left\{\left[G_i(\alpha^t)\right]^{ar}\right\} \tag{14}$$

식 (9)을 이용하여 식 (14)의 지수집합을 식 (15)와 같이 구체화 시킨다.

$$s_i(t)=\sum_{i=0}^{\frac{2^m-2}{2m}-1} Tr_1^m\left\{G_i(\alpha^t)\right]^{k^{2i}\cdot r}\right\} \tag{15}$$

여기서 k는 $\mathbb{Z}_p=\{0,1,2,\cdots,p-1\}$ 의 원시원소이며 $p=2^m-1$를 만족한다.

주기가 2^n-1 인 주어진 수열 $s_i(t)$를 $(2^m-1)\times(2^m+1)$ 배열로 나타내기 위하여 t를 $t=Q\cdot t_1+t_2(0\le t_1<2^m-1\ ,\ 0\le t_2<2^m+1)$ 로 두면 $G_i(\alpha^t)=\beta^{2t_1}G_i(\alpha^{t_2})$를 만족한다. 따라서 식 (15)는 다음과 같이 나타낼 수 있다.

$$s_i(t)=\sum_{i=0}^{\frac{2^m-2}{2m}-1} Tr_1^m\left\{\beta^{2rtk^{2i}}\left[G_i(\alpha^{t_2})\right]^{rk^{2i}}\right\} \tag{16}$$

고정된 α , r , m에 대하여 이동 양 τ에 대하여 $s_i(t)+s_j(t+\tau)$는

$$s_i(t)+s_j(t+\tau)=\sum_{i=0}^{\frac{2^m-2}{2m}-1} Tr_1^m\left\{\beta^{2rt_ik^{2i}}\cdot g(\tau,t_2)\right\} \tag{17}$$

이고, 여기서 $g(\tau,t_2)$는 다음과 같다.

$$g(\tau,t_2)=[G_i(\alpha^{t_2})]^{rk^{2i}}+[G_j(\alpha^{t_2+\tau})]^{rk^{2i}} \tag{18}$$

식 (2)에서 정의된 두 수열 $s_i(t)$과 $s_j(t+\tau)$사이의 상호상관관계를 $R_{ij}(\tau)$는 식 (19)를 만족한다.

$$\begin{aligned}R_{ij}(\tau)&=\sum_{t=0}^{2^n-2}(-1)^{s_i(t)+s_j(t+\tau)}\\&=\sum_{t_2=0}^{2^m}\sum_{t_1=0}^{2^m-2}(-1)^{\sum_{\alpha\in F}Tr_1^m[\beta^{2rt_1}k^{2i}g(\tau,t_2)]}\end{aligned} \tag{19}$$

식 (19)에서

$$\sum_{t_1=0}^{2^m-2}(-1)^{\sum_{\alpha\in F}Tr_1^m[\beta^{2rt_1}k^{2i}g(\tau,t_2)]}$$

은 이상적인 자기상관 성질을 가지므로 $g(\tau,t_2)=0$이면 0-수열로 2^m-1이고, $g(\tau,t_2)\neq 0$이면 이상적인 자기상관 성질에 의하여 -1이 된다. 따라서 전체 수열에 대한 $R_{ij}(\tau)$는 다음을 만족한다.

$$\begin{aligned}R_{ij}(\tau)&=-1\cdot(Q-z)+(2^m-1)\cdot z\\&=2^m\cdot z-Q\end{aligned} \tag{20}$$

여기서 $z=|\{t_2\mid g(\tau,t_2)=0,\ 0\le t_2<Q\}|$ 이다.

$x:=\alpha^t(0\le t<2^n-1)$라 하면 x는 0을 제외한 모든 $GF(2^n)$ 원소 중 하나이다.

$$\begin{aligned}G_S(x)=\ &Tr_n^m(x^2+u_ix^{2^{m+1}})+v_ix^Q\\&+Tr_n^m(x^2\alpha^{2\tau}+u_jx^{2^{m+1}}\alpha^{2^{m+1}\tau})+v_jx^Q\beta^\tau\end{aligned} \tag{21}$$

이라 하면 식 (18)은 $\left[G_S(x)\right]^{rk^{2i}}$이라 할 수 있다. $\gcd(r,2^m-1)=1$이므로 $\left[G_S(x)\right]^{rk^{2i}}=0$일 필요충분조건은 $G_S(x)=0$ 이다. 그리고 $G_S(x)=0$을 만족하는 해의 개수는 0 , 1, 2이다. 그러므로 식 (20)에서 $R_{ij}(\tau)=\{-2^m-1,\ -1,\ 2^m-1\}$ 이다.

Ⅳ. 결 론

본 논문에서는 Cho 등에 의해 제안된 이진수열과 같은 상호상관관계를 가지며 Legendre 수열에 의해 구성되는 새로운 3-valued 비선형 이진수열을 제안하였다. 이 수열은 유한체위에서 트레이스를 이용해 생성하는 가장 우수한 수열인 m-수열, GMW 수열, Kasami 수열, No 수열을 모두 포함하며, Klapper에 의해 제안된 이차형식 수열보다 더 낮은 상호상관관계를 갖는다. 본 논문에서 제안한 비선형 이진수열은 지금까지 제안되었던 우수한 수열들을 모두 포함하는 일반화된 형태이며 상관관계 3가지의 값만을 가지므로 최적의 상호상관관계를 갖는다.

참고 문헌

[1] T. Helleseth and P.V. Kumar, "Sequences with low correlation," in Handbook of Coding Theory, V.S. Pless and W.C. Huffman, Eds., Amsterdam, The Vetherland: North-Holland, Vol. II, pp. 1765-1853, 1998.

[2] G. Gong, "New designs for signal sets with low cross correlation, balance property, and large linear span: GF(p) case," IEEE Trans. Inform. Theory, Vol. 4, pp. 2847-2867, 2002.

[3] S.W. Golomb, "On the classification of balanced binary sequences of period 2^n-1," IEEE trans. Inform. Theory, Vol. IT-26, No.6, pp. 730-732, 1980.
[4] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, Spread Spectrum Communications, Vol. 1, Rockville, MD: Computer Science Press, 1985.
[5] S.W. Golomb, "Shift Register Sequences," Holden Day, 1967.
[6] R.A. Scholtz and R. Welch, "GMW sequences," IEEE Trans. Inform. Theory, Vol. IT-30, pp. 548-553, 1984.
[7] J.S. No, H.K. Lee, H. Chuang, H.Y. Song, and K. Yang, "Trace representation of Legendre Sequences of Mersenne prime period," IEEE Trans. Inform. Theory, Vol. 42, No. 6, pp. 2254-2255, 1996.
[8] 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. IT-35, No. 2, pp. 371-379, 1989.
[9] T. Kasami, "Weight distribution of Bose-Chaudhuri-Hocquenghem codes," in Combinatorial Mathematics and Its Applications. Chapel Hill, NC: Univ. North Carolina Press, 1969.
[10] A. Klapper, "Large Families of Sequences with Near-Optimal Correlations and Large Linear Span," IEEE Trans. Inform. Theory, Vol. 42, No. 4, pp. 1241-1248, 1996.
[11] U.S. Choi, S.J. Cho, H.D. Kim, "Attack using Phase Shifts of Shrunken Sequence", J. The Korea Institute of Electronic Communication Sciences, Vol. 6, No. 1, pp. 97-104, 2011.
[12] J.G. Kim, S.J. Cho, U.S. Choi, Y.H. Hwang, " Crosscorrelation of Kasami sequences and No sequences", J. The Korea Institute of Electronic Communication Sciences, Vol. 6, No. 1, pp. 13-19, 2011.
[13] U.S. Choi, S.J. Cho, J.G. Kim, " Analysis of Shrunken Sequences using LFSR and CA on $GF(2^p)$", J. The Korea Institute of Electronic Communication Sciences, Vol. 5, No. 4, pp. 418-424, 2010.
[14] S.J. Cho, U.S. Choi, H.D. Kim, H.J. An, " Analysis of nonlinear sequences based on shrinking generator", J. The Korea Institute of Electronic Communication Sciences, Vol. 5, No. 4, pp. 412-417, 2011.
[15] S.J. Cho, S.H. Kwon, "A new family binary sequences with low correlation," (submitted).
[16] L.R. Welch, "Lower bounds on the maximum cross-correlation of signals," IEEE Trans. Inform. Theory, Vol. IT-20, pp. 397-399, 1974.
[17] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press 1997.
[18] J.S. No, "p-ary unified sequences : p-ary extended d-form sequences with ideal autocorrelation property," IEEE Trans. Inform. Theory, Vol. 48, No. 9, pp. 2540-2546, 2002.

저자 소개

최언숙(Un-Sook Choi)

1992년 2월 성균관대학교 산업공학과 졸업 (이학사)
2000년 2월 부경대학교 대학원 응용수학과 졸업(이학석사)
2004년 2월 부경대학교 대학원 응용수학과 졸업(이학박사)
2006년~현재 : 동명대학교 자율전공학부 교수
※ 주 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
※ 주 관심분야 : 셀룰라 오토마타론, 정보보호