유한체상의 방정식과 m-수열의 상호상관관계 분석

최언숙* · 조성진**

Analysis of Cross-Correlation of m-sequences and Equation on Finite Fields

Un-Sook Choi* · Sung-Jin Cho**

요 약

주기가 p^n-1인 p진 수열은 부호이론, CDMA와 같은 통신시스템과 암호체계 등 많은 분야에서 폭넓게 응용되고 있다. 이러한 수열에 대한 상호상관관계에 대한 분석은 p진 수열의 연구에 있어 매우 중요한 문제이다. 본 논문에서는 유한체 위에서의 방정식 $(x+1)^d=x^d+1$의 해와 관련지어 p진 수열의 상호상관관계를 분석한다.

ABSTRACT

p-ary sequences of period $N=2^k-1$ are widely used in many areas of engineering and sciences. Some well-known applications include coding theory, code-division multiple-access (CDMA) communications, and stream cipher systems. The analysis of cross-correlations of these sequences is a very important problem in p-ary sequences research. In this paper, we analyze cross-correlations of p-ary sequences which is associated with the equation $(x+1)^d=x^d+1$ over finite fields.

키워드

p-ary sequence, cross-correlation, Niho type, decimation, finite field
p진 수열, 상호상관관계, Niho 형태, 데시메이션, 유한체

Ⅰ. 서 론

CDMA(Code Division Multiple Access)는 여러 사용자가 시간과 주파수를 공유하면서 각 사용자에게 확산코드라고 하는 서로 다른 의사난수열(pseudo-random sequence)을 할당한다. 각 사용자는 할당된 확산코드를 이용하여 송신할 신호를 변조한다. 신호를 변조하는데 사용하는 코드를 선택하는 것은 CDMA 시스템의 수행능력을 결정하는 데 있어 매우 중요하다. 왜냐하면 품질이 좋은 수열은 사용자들 사이의 신호들의 간섭을 줄이고 신호를 잘 복호할 수 있도록 하기 때문이다. 수신자는 데이터를 복호하기 위해 수신된 부호를 동기화한다. 서로 독립인 코드를 사용하는 것은 동시 다중접속을 가능하게 한다.

확산 스펙트럼 통신에서 다중접속 충돌을 최소화하고, 시스템의 보안을 증가시키고 사용자의 수를 늘이는데 도움을 주는 수열로 잘 알려진 수열군은 m-수열, GMW 수열, Kasami 수열, No 수열, m-수열에 데시메이션(decimation)을 적용하여 얻는 Gold 계열의 수열 등이 있다. 이 밖에도 트레이스를 이용한 여러 수열들이 연구되었다[1-6]. 제안되었던 많은 수열들이 좋은 수열인지를 판별하는 기준 가운데 가장 중요한 것 중 하나가 임의의 위상이동차에 대한 두 수열사이의 상호상관관계이다.

* 동명대학교 자율전공학부(choies@tu.ac.kr)
** 교신저자 : 부경대학교 응용수학과(sjcho@pknu.ac.kr)
접수일자 : 2012. 07. 03 심사(수정)일자 : 2012. 07. 26 게재확정일자 : 2012. 08. 09

본 논문에서는 두 개의 p진 m-수열에 의해 생성되는 Gold 계열의 수열에 대하여 상호상관관계를 분석하기 위하여 유한체 상의 방정식 $(x+1)^d = x^d + 1$의 해의 개수와 수열의 상호상관관계를 관련지어 생각한다.

II. 배경지식 및 기존 연구 분석

트레이스(Trace) 함수는 유한체로부터 부분체로의 선형매핑인데, 이 함수는 의사난수열의 설계와 분석을 위한 중요한 수학적 도구이다. $GF(p^n)$를 p^n개의 원소를 가진 유한체라 하고, $GF(p^n)^* = GF(p^n)/\{0\}$라 하자. 차수가 n인 원시다항식 $f(x)$의 원시근을 $\alpha(\in GF(p^n))$라 하자.

트레이스함수 $Tr_m^n : GF(p^n) \rightarrow GF(p^m)$ 는 다음과 같이 정의한다[7].

$$Tr_m^n(x) = \sum_{i=0}^{k-1} x^{p^{m \cdot i}}$$

여기서 x는 $GF(p^n)$의 원소이고 $k = \frac{n}{m}$이다. 트레이스함수 $Tr_m^n : GF(p^n) \rightarrow GF(p^m)$ 는 다음 성질을 만족한다[7].

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

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

(c) Tr_m^n는 전사함수이다.

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

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

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

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

GMW수열, Kasami 수열, No 수열과 같은 부분체를 이용하여 제안된 수열과 다른 형태로 최적의 상호상관관계를 갖는 수열이 Gold를 비롯한 많은 연구자들에 의해 제안되었다[8-14]. 이러한 수열은 하나의 m-수열 $u(t)$와 m-수열에 데시메이션을 적용한 수열을 $v(t)$라 할 때 주기 p^n-1인 두 m-수열의 합으로 생성되는 수열을 Gold 계열의 수열이라 한다[13]. $u(t)$를 다음과 같이 정의하자.

$$u(t) = Tr_1^n(\alpha^t) \tag{1}$$

여기서 α는 $GF(p^n)$의 한 원시원소이다.

$\gcd(d, p^n-1) = 1$를 만족하는 데시메이션 d $(1 \le d \le p^n-2$)를 수열 $u(t)$에 적용하여 주기가 같은 또 하나의 m-수열 $v(t)$를 다음과 같이 생성할 수 있다.

$$v(t) = u(dt) \tag{2}$$

1, 0, 0, 0, 1, 0, 0, 1, 1, 0
1, 2, 1, 1, 0, 0, 2, 1, 0, 2
0, 1, 2, 2, 1, 0, 1, 0, 1, 1
1, 1, 2, 2, 2, 0, 1, 1, 2, 1
2, 0, 0, 0, 2, 0, 0, 2, 2, 0
2, 1, 2, 2, 0, 0, 1, 2, 0, 1
0, 2, 1, 1, 2, 0, 2, 0, 2, 2
2, 2, 1, 1, 1, 0, 2, 2, 1, 2

그림 1. $u(t) = Tr^4(\alpha^t)$
Fig. 1 $u(t) = Tr^4(\alpha^t)$

예를 들어 $n=4$이고 $p=3$, $d=13$라 하자. 그러면 $\gcd(d, p^n-1) = \gcd(13, 80) = 1$ 이다. $GF(3^4)$을 생성하는 4차 원시다항식 $f(x)$를 $f(x) = x^4 + 2x + 2$라 하고 $f(x)$의 원시근 α에 대하여 $u(t) = Tr^4(\alpha^t)$, $(t = 0,1,\cdots,3^4-2)$라 할 때 수열 $u(t)$의 주기는 $3^4-1 = 80$이고, 한 주기의 수열을 8×10 배열로 나타내면 그림 1과 같다. 이때 첫 번 째 열인 1, 1, 0, 1, 2, 2, 0, 2는 $GF(3^4)$의 부분체 $GF(3^2)$를 생성하는 2차 원시다항식 $f_1(x) = x^2 + x + 2$에 의해 생성된 주기가 8인 m-수열이고, 6번째 열 0-수열을 제외한 나머지 수열은 첫 번째 열과 같은 m-수열로 위상이 동차만 존재할 뿐이다. 수열 $u(t)$에 데시메이션 $d=13$을 적용한 수열 $v(t) = u(13t)$는 그림 2와 같다. 이 수열의 최소다항식은 $x^4 + 2x^3 + 2$이고 이 다항식은 원시다항식이다. 또한 그림 2의 수열의 배열에서 각 열 중 0-수열을 제외한 수열의 최소다항식은 $x^2 + 2x + 2$이다.

1, 1, 1, 1, 2, 0, 1, 2, 1, 1
2, 1, 2, 0, 2, 0, 2, 2, 1, 1
0, 2, 0, 1, 1, 0, 0, 1, 2, 2
2, 0, 2, 1, 0, 0, 2, 0, 0, 0
2, 2, 2, 2, 1, 0, 2, 1, 2, 2
1, 2, 1, 0, 1, 0, 1, 1, 2, 2
0, 1, 0, 2, 2, 0, 0, 2, 1, 1
1, 0, 1, 2, 0, 0, 1, 0, 0, 0

그림 2. $v(t)=u(13t)$
Fig. 2 $v(t)=u(13t)$

소수인 p에 대하여 주기가 $q=p^k$인 유한체 $GF(q)$에 대하여 $GF(q)$의 곱셈군은 $GF(q)^*$이다. $GF(q^2)$상에서의 방정식

$$(x+1)^d = x^d + 1 \tag{3}$$

의 해에 대해 생각해 보자. 이때 d는 식 (2)에서 정의된 d이다. 특히, $d \equiv 1 \pmod{q-1}$ 인 Niho 형태의 d에 대응하는 m수열의 상호상관관계함수는 Niho의 학위 논문에서 처음 연구되었다[15]. Niho 등은 상호상관관계가 3값 혹은 4값이 되는 수열을 발생시키는 Gold 계열의 수열에 대하여 연구하였다. 최근 이런 종류의 데시메이션이 큰 관심의 대상이 되고 있다. 이러한 수열의 상호상관관계를 분석하는 데 있어 방정식 (3)에 대한 연구는 매우 중요한 역할을 한다.

앞의 예에서 $d=17$이라 두면 $d \equiv 1 \pmod 8$이므로 주어진 데시메이션은 Niho 형태이고 그림 3은 $v_1(t)=u(17t)$이다.

주기가 p^n-1인 두 p진 m-수열 $u(t)$와 $v(t)=u(dt), t=0,1,\cdots,p^n-2$ 의 상호상관관계 함수를 $C_d(\tau), \tau=0,1,\cdots,p^n-2$ 라 할 때 $C_d(\tau)$는 다음과 같다.

$$C_d(\tau) = \sum_{t=0}^{p^n-2} w^{u(t+\tau)-u(dt)} \tag{4}$$

여기서 w는 단위원의 p제곱근 복소원시근이다. 임의의 $\delta \in GF(p^n)$에 대하여 식 (5)는 이미 잘 알려져 있다[16].

$$\sum_{x \in GF(p^n)^*} w^{Tr_1^n(\delta x)} = \begin{cases} -1 & , \delta \neq 0 \\ p^n - 1 & , \delta = 0 \end{cases} \tag{5}$$

$C_d(\tau)$를 계산하는 것은 $\sum_{x \in GF(p^n)^*} \chi(x+yx^d)$를 계산하는 것과 같다. 여기서 χ는 유한체 $GF(p^n)$의 canonical additive character이고, $y=\alpha^\tau$이다. 이것은 정리 1을 만족한다. $C_d(\tau)$의 값의 분포를 찾는데 있어 정리 1의 거듭제곱의 합에 관한 식을 사용한다.

1, 1, 2, 1, 2, 0, 2, 1, 1, 1
1, 0, 2, 2, 1, 0, 2, 0, 2, 0
0, 1, 0, 2, 1, 0, 0, 1, 2, 1
1, 2, 2, 0, 0, 0, 2, 2, 0, 2
2, 2, 1, 2, 1, 0, 1, 2, 2, 2
2, 0, 1, 1, 2, 0, 1, 0, 1, 0
0, 2, 0, 1, 2, 0, 0, 2, 1, 2
2, 1, 1, 0, 0, 0, 1, 1, 0, 1

그림 3. $v_1(t)=u(17t)$
Fig. 3 $v_1(t)=u(17t)$

<정리 1[14]> 소수 p에 대하여 상호상관관계 $C_d(\tau)$는 다음이 성립한다.

(1) $\sum_{\tau=0}^{p^n-2} (C_d(\tau)+1) = p^n$

(2) $\sum_{\tau=0}^{p^n-2} (C_d(\tau)+1)^2 = p^{2n}$

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

여기서 b는 $|\{x \in GF(q^2) | (x+1)^d = x^d+1\}|$ 이다.

정리 1에서 나타난 바와 같이 주어진 $m-$수열의 상호상관관계와 방정식 $(x+1)^d = x^d+1$은 밀접한 관계가 있다. 본 논문에서 방정식 $(x+1)^d = x^d+1$의 d는 Niho 형태의 d에 대해서만 다룬다. 즉, $d \equiv 1 \pmod{q-1}$이다. $GF(q^2)$에서 방정식을 만족하는 해 x를 찾아보자. 여기서 p는 소수이다. 조건 $\gcd(d, q^2-1)=1$은 Niho 형태를 만족하는 d에 대해 항상 성립하므로 고려하지 않아도 된다. $GF(q)$상에

서 $x \in GF(q^2)$에 대하여 $\overline{x}$를 식 (6)과 같이 정의한다.

$$\overline{x} = x^q \tag{6}$$

$\overline{x}$에 대한 성질은 일반적인 복소수의 켤레와 유사하다. 예를 들어 $\overline{x+y} = \overline{x}+\overline{y}$ 이다.

주기가 $q+1$인 순환군 S를 식 (7) 같이 정의한다.

$$S = \{x \in GF(q^2) \mid x\overline{x} = 1\} \tag{7}$$

III. Niho형태의 지수에 대한 유한체 방정식

Niho 형태의 데시메이션 d는 $d \equiv 1 \pmod{q-1}$ 이므로 $d = (q-1)s+1$라 하자. $x \in GF(q)$라 하면 $x+1 \in GF(q)$이므로 $x^{q-1} = 1$, $(x+1)^{q-1} = 1$이다. 그러므로 다음이 성립한다.

$$\begin{aligned} \text{①}: \quad (x+1)^d &= (x+1)^{(q-1)s+1} \\ &= \left((x+1)^{q-1}\right)^s (x+1) \\ &= x+1 \\ \text{②}: \quad x^d+1 &= x^{(q-1)s+1}+1 \\ &= (x^{q-1})^s x+1 \\ &= x+1 \end{aligned}$$

①과 ②에 의해 $(x+1)^d = x^d+1$이다. 이것은 $GF(q)$의 모든 원소가 분명히 $(x+1)^d = x^d+1$의 해가 됨을 의미한다.

<정리 2> $q = p^k$이고 $d \equiv 1 \pmod{q-1}$이라 하자. $x \in GF(q^2) \setminus \{0,-1\}$가 $(x+1)^d = x^d+1$의 해일 필요충분조건은 $x^{d-1} = (x+1)^{d-1} = 1$ 또는 $x^{d-q} = (x+1)^{d-q} = 1$이다.

(증명)

$(\overline{x}+1)^d = (x^q+1)^d = \{(x+1)^q\}^d = (x+1)^{qd}$ 이다. 그런데 x가 $(x+1)^d = x^d+1$의 해이므로

$(x+1)^{qd} = \overline{x^d}+1$ 이다. 따라서 $(\overline{x}+1)^d = \overline{x^d}+1$이므로 $\overline{x}$ 또한 방정식 $(x+1)^d = x^d+1$의 해이다. 또한 $(x+1)^d(\overline{x}+1)^d = (x^d+1)((\overline{x})^d+1)$ 이고 식 (8)을 만족한다.

$$(x\overline{x}+x+\overline{x}+1)^d = (x\overline{x})^d + x^d + (\overline{x})^d + 1 \tag{8}$$

그런데 $x\overline{x}, x+\overline{x} \in GF(q)$이고 $1 \in GF(q)$이므로 $x\overline{x}+x+\overline{x}+1 \in GF(q)$이다.

$(x\overline{x}+x+\overline{x}+1)^d = x\overline{x}+x+\overline{x}+1$이고 $(x\overline{x})^d = x\overline{x}$이다. 그러므로 식 (8)은 식(9)와 같다.

$$x\overline{x}+x+\overline{x}+1 = x\overline{x}+x^d+(\overline{x})^d+1 \tag{9}$$

따라서 식 (10)을 만족한다.

$$x+\overline{x} = x^d+(\overline{x})^d \tag{10}$$

$d \equiv 1 \pmod{q-1}$이므로 식 (10)은 다음과 같다.

$0 = x^{2d-q-1} - x^{d-q} - x^{d-1} + 1 = (x^{d-1}-1)(x^{d-q}-1)$

따라서 $x^d = x$ 또는 $x^d = x^q = \overline{x}$이다.

i) $x^d = x$일 때, $(x+1)^d = x^d+1 = x+1$이므로 $(x+1)^{d-1} = 1$이다.

ii) $x^d = \overline{x}$일 때, $(x+1)^d = \overline{x}+1 = (x+1)^q$이므로 $(x+1)^{d-q} = 1$이다.

역에 대한 증명도 유사하므로 생략한다. □

앞에서 $GF(q^2)$의 부분체인 $GF(q)$의 모든 원소는 방정식 $(x+1)^d = x^d+1$의 원소임을 보였다. 그렇다면 $GF(q^2) \setminus GF(q)$인 원소에 대하여 $(x+1)^d = x^d+1$의 해가 있다고 가정해 보자.

$d = (q-1)s+1$이고, $u := x^{(d-1)/s}$, $v := (x+1)^{(d-1)/s}$라 하자. 정리 2에 의해서 $u^s = v^s = 1$ 또는 $u^{s-1} = v^{s-1} = 1$이다.

① $u, v \in S \setminus \{1\}$:

$u^{q+1} = \left(x^{\frac{d-1}{s}}\right)^{q+1} = x^{q^2-1} = 1$이고

유사한 방법으로 $v^{q+1} = (x+1)^{q^2-1} = 1$이다. 그러므로 $u, v \in S$이다. 그런데 만약 $u = 1$이라 하자. $u = x^{(d-1)/s} = x^{q-1} = 1$이므로 $x \in GF(q)$가 되고 $x \in GF(q^2) \setminus GF(q)$에 모순이다. 그러므로

$u \neq 1$ 이고, 유사한 방법으로 $v \neq 1$이다.

② $u \neq v$:

$u = v$라 가정하자. 그러면 $x^{q-1} = (x+1)^{q-1}$이다. 양변에 $x+1$을 곱하면 $(x+1)x^{q-1} = (x+1)^q$이다. 정리하면 $x^q + x^{q-1} = (x+1)^{q-1}$ 이다.
따라서 $x^{q-1} = 1$이다. 즉, $x \in GF(q)$이 되고 이것은 모순이다. 따라서 $u \neq v$이다.

③ $x = \dfrac{v-1}{u-v}$

$$\overline{x} = x^q = x^{(d-1)/s} \cdot x = ux \quad \cdots\cdots\cdots ㉠$$

$$\overline{x} + 1 = \overline{x+1} = (x+1)^q$$
$$= (x+1)^{\frac{d-1}{s}} \cdot (x+1) = v(x+1)$$

$$\overline{x} = v(x+1) - 1 \quad \cdots\cdots\cdots ㉡$$

㉠,㉡에 의해서 $ux = v(x+1) - 1$이다. 그러므로 방정식 $(x+1)^d = x^d + 1$을 만족하는 해 중 $GF(q^2) \setminus GF(q)$에 속하는 원소는 다음과 같이 표현할 수 있다.

$$x = \frac{v-1}{u-v} \tag{11}$$

그리고

$$x^d = x^{(q-1)s+1} = xu^s = x \quad (u^s = 1\text{인 경우})$$

또는

$$x^d = x^{(q-1)s+1} = x^{(q-1)(s-1)+q}$$
$$= x^q u^{s-1} = x^q \quad (u^{s-1} = 1\text{인 경우})$$

이다. 유사한 방법으로 $(x+1)^d = x+1$ $(v^s = 1$인 경우$)$ 또는 $(x+1)^d = (x+1)^q$ $(v^{s-1} = 1$인 경우$)$ 임을 알 수 있다. 따라서 정리 2에 의해 식 (11)의 x는 $(x+1)^d = x^d + 1$의 해이다. 이러한 x는 u와 v가 정해지면 유일하게 결정된다. 즉 u와 v가 다른 쌍에 대해 x는 서로 다르다.

$r_0 = \gcd(s, q+1)$, $r_1 = \gcd(s-1, q+1)$이라 하자. $u^s = 1$(또는 $u^{s-1} = 1$), $u \in S \setminus \{1\}$ 이고 $u^{q+1} = 1$ 이면 $u^{\gcd(s, q+1)} = 1$ 또는 $u^{\gcd(s-1, q+1)} = 1$이므로 $u^{r_0} = 1$ 또는 $u^{r_1} = 1$이다. 방정식 $(x+1)^d = x^d + 1$의 해의 개수 N은 다음과 같다.

$$N = q + (r_0 - 1)(r_0 - 2) + (r_1 - 1)(r_1 - 2) \tag{12}$$

<예제> $n = 4$, $q = 3^2 = 9$ 이라 하자. $s = 2$라 두면, $d = 17$이고 $d \equiv 1 \pmod 8$로 Niho 형태의 데시메이션이다. 또한 $\gcd(d, p^n - 1) = \gcd(17, 80) = 1$을 만족한다. $r_0 = \gcd(s, q+1) = \gcd(2, 10) = 2$ 이고, $r_1 = \gcd(s-1, q+1) = \gcd(1, 10) = 1$이다. 그러므로 식 (12)에 의해 방정식 $(x+1)^{17} = x^{17} + 1$의 해의 개수는 $9 + (2-1)(2-2) + (1-1)(1-2) = 9$이다. 실제 해는 $x = 0, 1, \alpha^{10}, \alpha^{20}, \alpha^{30}, \alpha^{40}, \alpha^{50}, \alpha^{60}, \alpha^{70}$이다. 이는 $GF(q)$와 같다. $s = 5$이면 $d = 41$이다. 그러면 $r_0 = 5$이고, $r_1 = 1$이다. 따라서 식 (12)에 의한 방정식의 해의 개수는 $9 + 4 \cdot 3 = 21$이다. 실제로 $(x+1)^{41} = x^{41} + 1$의 해는 $x = 0, 1, \alpha^2, \alpha^6, \alpha^{10}, \alpha^{16}, \alpha^{18}, \alpha^{20}, \alpha^{26}, \alpha^{30}, \alpha^{32}, \alpha^{40}, \alpha^{48}, \alpha^{50}, \alpha^{54}, \alpha^{60}, \alpha^{62}, \alpha^{64}, \alpha^{70}, \alpha^{74}, \alpha^{78}$이다.

Ⅳ. 결 론

본 논문에서는 소수 p에 대하여 $q = p^k$이고 $d \equiv 1 \pmod{q-1}$인 Niho 형태의 데시메이션을 지수로 하는 유한체 방정식 $(x+1)^d = x^d + 1$의 해의 개수를 구함으로 주어진 p진 수열의 상호상관관계의 분포를 구하는 방법에 대하여 알아보았다. 이때 방정식이 해를 갖기 위한 필요충분조건을 제시하였다.

참고 문헌

[1] S.W. Golomb, "Shift Register Sequences," Holden Day, 1967.

[2] R.A. Scholtz and R. Welch, "GMW sequences," IEEE Trans. Inform. Theory, Vol. IT-30, pp. 548-553, 1984.

[3] 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.

[4] 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.
[5] T. Kasami, "Weight distribution of Bose-Chaudhuri-Hocquenghem codes," in Combinatorial Mathematics and Its Applications. Chapel Hill, NC: Univ. North Carolina Press, 1969.
[6] 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.
[7] S.J. Cho, Finite Fields with Their Applications, Kyowoosa Press, 2007. [
[8] 조성진, 최언숙, 김한두, 안현주, “수축생성기에 기반한 비선형 수열의 분석”, 한국전자통신학회논문지, 5권, 4호, pp. 412-417, 2010.
[9] 김진경, 조성진, 최언숙, 황윤희, “Kasami 수열들과 No 수열들의 상호상관관계”, 한국전자통신학회논문지, 6권, 1호, pp. 13-19, 2011.
[10] 최언숙, 조성진, “최적의 상호상관관계를 갖는 이진 수열의 설계”, 한국전자통신학회논문지, 6권, 4호, pp. 539-544, 2011.
[11] 최언숙, 조성진, 권숙희, “확장된 비선형 이진수열의 상호상관관계 분석”, 한국전자통신학회논문지, 7권, 2호, pp. 263-270, 2012.
[12] R. Gold, "Maximal recursive sequences with 3-valued cross-correlation functions," IEEE Trans. Inform. Theory, Vol. 14, pp. 154-156, 1967.
[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 Applications, Vol. 11, No. 4, pp. 674-683, 2005.
[15] Y. Niho, “Multi-valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences”, Ph.D. thesis, University of Southern California, 1972.
[16] S.W. Golomb and G. Gong, Signal Design for Good Correlation, Cambridge University Press, 2005.

저자 소개

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

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