확장된 비선형 이진수열의 상호상관관계 분석

최언숙* · 조성진** · 권숙희***

Analysis of Cross-Correlation of Extended Non-Linear Binary Sequences

Un-Sook Choi* · Sung-Jin Cho** · Sook-Hi Kwon***

요 약

CDMA는 여러 사용자가 시간과 주파수를 공유하면서 각 사용자에게 확산코드라고 하는 서로 다른 의사잡음 수열(pseudonoise 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. 본 논문에서는 확산 스펙트럼 통신에서 다중접속 충돌을 최소화하고, 시스템의 보안을 증가시키고 사용자의 수를 늘이는데 도움을 주는 비선형 수열을 생성하고 상호상관관계를 분석한다.

ABSTRACT

Code-Division Multiple-Access(CDMA) allows several users simultaneous access to a common channel by assigning a distinct pseudonoise sequence called spectrum code to each user. Each user in a CDMA system uses a assigned spectrum code to modulate their signal. Choosing the codes used to modulate the signal is very important in the performance of CDMA systems. The best performance will occur when there is good separation between the signal of a desired user and the signals of other users. The receiver synchronizes the code to recover the data. The use of an independent code allows multiple users to access the same frequency band at the same time. In this paper we propose a generalized model of non-linear binary sequence using trace function and analyze cross-correlation of these sequences. These sequences with low correlation, large linear span and large family size, in a direct-sequence spread spectrum communication system, help to minimize multiple access interference, increase security degree of system and enlarge user number.

키워드

CDMA, spread-spectrum communication systems, spreading sequence, nonlinear binary sequence, cross-correlation
부호분할 다중접속 시스템, 대역확산 통신 시스템, 확산수열, 비선형 이진수열, 상호상관관계

Ⅰ. 서 론

1990년대부터 정보통신 분야는 다른 어떠한 산업분야보다 급속한 성장을 보였고, 특히 80년대 초에 처음으로 사용서비스를 시작한 이동전화 서비스의 성장속도는 괄목할 만하다. 현대사회의 급격한 정보화의 추세에 따라, 지난 해 9월 국내 휴대폰 가입자의 수는 5000만 명을 넘어섰다. 또한 스마트폰 사용자의 수도 2000

* 동명대학교 자율전공학부(choies@tu.ac.kr)
** 교신저자 : 부경대학교 응용수학과(sjcho@pknu.ac.kr)
*** 부경대학교 응용수학과(habaqueen@naver.com)
접수일자 : 2011. 11. 27 심사(수정)일자 : 2012. 03. 15 게재확정일자 : 2012. 04. 07

만 명을 넘어섰다. 새롭게 등장하는 다양한 형태의 무선통신 서비스를 수용하기 위해 고려되어야 하는 가장 중요한 문제 중의 하나가 한정된 전파 자원을 어떻게 하면 효율적으로 이용할 수 있을까에 관한 것이다. 이동전화 시스템에서는 이렇게 부족한 주파수를 효율적으로 이용하기 위해 두 가지 기술을 채용하고 있다. 첫 번째가 주파수를 재사용하여 기지국의 수를 늘리는 셀룰러 기술이고 두 번째가 주파수를 동시에 여러 가입자가 사용하도록 하는 다중 접속방식이다.

확산수열(spreading sequence)은 다중 반송파 대역확산 통신시스템(multi-carrier spectrum communication system)과 직접수열(direct-sequence) CDMA와 같은 무선통신에서 중요한 역할을 한다. 이러한 통신 시스템 사이에서 확산수열의 중요한 기능은 다중접속 충돌을 최소화하고, 시스템의 보안수준을 가능한 높이는 것, 그리고 더 많은 사용자들이 사용할 수 있도록 사용자수를 확대하는 것 등이 있다. 다중접속 충돌은 여러 사용자가 동시에 접속할 때 생기는 충돌에 의해 발생 할 수 있는데, 확산수열의 낮은 상호상관관계(cross-correlation)는 다중 접속 충돌을 최소화 할 수 있다. 또한 이러한 통신시스템에서 어떤 사용자의 확산수열을 얻는 누군가는 그 사용자의 신호를 복호할 수 있다. 그 결과로 적법한 사용자의 비밀이 폭로되는 결과를 초래하게 된다. 이런 위험 정도를 평가하기 위해 선형스팬(linear span)이 그 척도로 사용된다. 선형스팬이 크면 수열의 복호가 더 어려워지므로 낮은 상호상관관계, 큰 선형스팬, 큰 패밀리 사이즈를 가지는 확산수열에 대한 연구가 진행되고 있다[1-7]. 확산수열을 분석하기 위해 많은 기준들이 제시되었고 그 결과는 [8]에 잘 나타나 있다. 생성된 수열의 상호상관관계의 기준은 Welch bound이다. 따라서 생성된 수열이 통신시스템에 응용되기 위해서는 Welch bound를 만족해야 한다[9].

적당한 정수 n에 대하여 2-valued 자기상관관계(auto-correlation)를 갖는 주기가 2^n-1인 균형이 잡힌 이진수열(balanced binary sequences)[3]은 대역확산 통신 시스템에서 많이 응용되고 있다[4]. 이러한 수열로 잘 알려진 수열군은 m-수열, GMW 수열, Kasami 수열, No 수열 등이 있다. 이 밖에도 트레이스를 이용한 여러 수열들이 연구되었다[5-12]. 본 논문에서는 트레이스함수를 이용하여 생성하는 비선형 이진수열에 대하여 일반화된 모형을 제안하고 주어진 수열의 상관관계를 분석한다. 제안하는 수열군은 기존 연구 결과인 m-수열, GMW 수열, Kasami 수열, No 수열, Niho 형태의 수열 등을 모두 포함한다.

II. 배경지식 및 기존 연구 분석

2.1. CDMA 방식

주파수를 많은 사용자가 사용할 수 있는 다중접속 방식에는 크게 주파수 분할 다중접속(FDMA), 시분할 다중접속(TDMA), 코드분할 다중접속(CDMA) 등이 있다[13]. 그림 1은 다중접속 방식에 대한 그림이다.

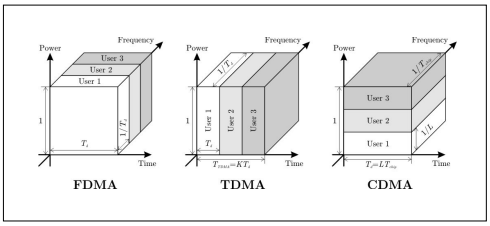

그림 1. 다중접속방식
Fig. 1 Multiple access schemes

FDMA방식은 주어진 주파수를 각 사용자가 서로 다른 신호간의 간섭을 방지할 수 있을 정도의 주파수 대역으로 나누어 동일한 주파수 대역의 주파수 신호는 통과시키고 그 외 주파수 신호는 제거하는 필터를 사용하는 방식으로 아날로그 방식이다[14].

디지털 신호란 신호의 크기가 연속적인 값을 가지지 않고 '0'과 '1'만 가지는 신호를 말한다. 이러한 디지털 신호는 '0'과 '1'만 구별하면 되므로 신호전송에 있어서 잡음에 강한 특성을 보인다. 이러한 디지털 신호 여러 개를 동시에 전송하는 방법으로 TDMA와 CDMA가 대표적인 방식이다.

그림 2는 TDMA 통신방식을 나타낸다. TDMA방식은 하나의 주파수 대역을 주기적인 일정한 시간 간격으로 나누어서 각 사용자가 차례차례로 자신에게 할당된 시간 간격에 자신의 신호를 실어 보내면 각 수신측에서 자기의 시간 간격에 있는 정보만을 골라 수집하는 방식이다[15].

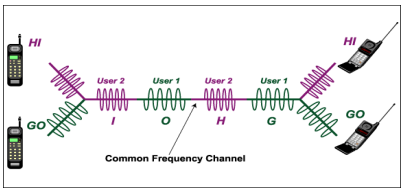

그림 2. TDMA 방식
Fig. 2 TDMA scheme

CDMA에서는 여러 사용자가 동일한 주파수를 동시에 사용한다[16]. CDMA는 송신자의 통화에 대해서 특별한 확산코드를 더하여 주파수 대역폭을 넓혀서 송신한다. 이 때 수신측은 송신측에서 부여한 것과 동일한 코드에 의해 자기에게 오는 통화를 구별해 낸다[14]. 그림 3은 CDMA방식을 나타낸다. 이러한 확산대역폭 통신시스템에서는 이론적인 주파수 대역폭보다 훨씬 더 넓은 대역폭을 사용하여 정보를 전송할 수 있다. 이때 사용하는 확산코드는 보내려는 정보와 독립적인 코드신호에 의해 이루어져야 하고 수신측에서는 송신측에서 정보를 확산시킨 코드신호와 동기가 맞추어진 신호의 상관관계에 의해 확산되어진 정보를 복원하게 된다.

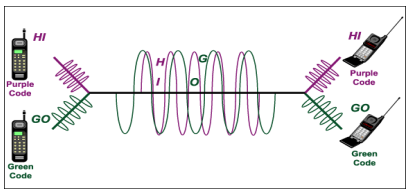

그림 3. CDMA 방식
Fig. 3 CDMA scheme

2.2. 비선형 이진수열에 대한 기존 연구

주어진 크기의 의사잡음수열 군에 대한 바람직한 몇 가지 성질은 낮은 상호상관관계, 큰 선형스팬, 균형성질(balanced property), 많은 서로 다른 수열군의 존재성, 구현의 용이성 등이다.

주기가 2^n-1이고 이상적인 자기상관 특성을 갖는 의사불규칙 수열들 중 대표적인 것이 m-수열, GMW 수열, Kasami 수열, No 수열, Gold 수열, Niho 유형의 수열 등이 있다. 수열의 바람직한 성질 중 낮은 상관관계는 코드 분할 다중 접속의 능력을 가지기 위해 중요하다. Welch[9]에 의해 유도된 최대 상관관계 값에 대한 하한은 의사불규칙 수열군의 상관관계 성질을 평가하는 데 자주 이용된다. m-수열, GMW 수열, 작은 집합의 Kasami 수열, No 수열 등은 이러한 하한의 관점에서 최적인 상관관계 값을 갖는 수열 군들이다.

트레이스(Trace)함수는 유한체로부터 부분체로의 선형 매핑인데, 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 가지는 유한체라 하고 $GF(2^n)^* = GF(2^n)/\{0\}$이라 하자. n은 $n=km$인 자연수라 하자. 여기서 m은 1 보다 큰 정수이다. 또한 $Q=(2^n-1)/(2^m-1)$ 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.

$$Tr_m^n(x) = \sum_{i=0}^{k-1} x^{2^{m \cdot i}} \tag{1}$$

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

(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 해가 2^{n-m}개 존재한다.

m-수열 $m(t)$와 GMW 수열 $g(t)$은 다음 식 (2), (3)과 같다[5,6].

$$m(t) = Tr_1^n(\alpha^t) \tag{2}$$

$$g(t) = Tr_1^n([Tr_m^n(\alpha^t)]^r) \tag{3}$$

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

$n = 2m$이라 하고 $Q = (2^n - 1)/(2^m - 1) = 2^m + 1$ 이라 하자. 그러면 Kasami 수열 $K_i(t)$와 No 수열 $N_i(t)$는 는 다음과 같다[7,10].

$$K_i(t) = Tr_1^n(\alpha^{2t}) + Tr_1^m(\gamma_i \alpha^{Q \cdot t}) \quad (4)$$

$$N_i(t) = Tr_1^m\{[Tr_m^n(\alpha^{2t}) + \gamma_i \alpha^{Q \cdot t}]^r\} \quad (5)$$

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.

주기가 N인 이진수열의 상관관계 $R_{ij}(\tau)$는 이동량이 τ일 때, 두 수열 $s_i(t+\tau)$와 $s_j(t)$에 대하여 식(6)과 같다.

$$R_{ij}(\tau) = \sum_{t=0}^{N-1} (-1)^{s_i(t+\tau) + s_j(t)} \quad (6)$$

임의의 $\delta \in GF(2^m)$에 대하여 식 (7)은 이미 잘 알려져 있다[5].

$$\sum_{x \in GF(2^m)^*} (-1)^{Tr_1^m(\delta x)} = \begin{cases} -1 & , \delta \neq 0 \\ 2^m - 1 & , \delta = 0 \end{cases} \quad (7)$$

III. 확장된 비선형 이진수열

본 논문에서는 트레이스함수를 이용하여 생성한 비선형 이진수열에 대하여 일반화된 모형을 제안하고 주어진 수열의 상관관계를 분석한다.

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 $Q = (2^n - 1)/(2^m - 1) = 2^m + 1$이다. 주기가 $N = 2^n - 1$인 비선형 수열 S가 다음과 같이 정의된다고 하자.

$$S = \{s_i(t) | 0 \le t \le N-1, 1 \le i \le 2^m\} \quad (8)$$

여기에서 $s_i(t)$는 다음 식을 만족한다.

$$s_{ij}(t) = Tr_1^m\left\{\left[Tr_m^n\left(\alpha^{2(u+v)t} + \gamma_i \alpha^{2(u2^m+v)t}\right) + \eta_j \beta^{(u+v)t}\right]^r\right\} \quad (9)$$

여기서 $\gamma_i \in GF(2^n)$이고, $\eta_j \in GF(2^m)$이다. u와 v는 음이 아닌 서로 다른 정수이고 $u + v < 2^m$ 이다. $\gcd(r, 2^n - 1) = 1 (1 \le r < 2^m - 1)$ 이고, $\gcd(b, 2^n - 1) = 1$ 이다.

식을 간단히 하기위해 $b = u + v$이고 $d = u2^m + v$라 두자.

<보조정리 1> α를 $GF(2^n)$의 원시원소라 하고, β를 $GF(2^m)$의 원시원소라 할 때, $Q = 2^m + 1$에 대하여 $\beta = \alpha^Q$ 라 하면 $\alpha^{dQ} = \alpha^{bQ} = \beta^b$이다.

<증명> 주어진 보조정리의 증명은 $dQ = bQ$임을 보이면 된다.

$$\begin{aligned} dQ &= (u2^m + v)(2^m + 1) = u2^{2m} + u2^m + v2^m + v \\ &= (u+v)2^m + (u+v) \\ &= (u+v)(2^m + 1) \\ &= bQ \end{aligned}$$

이다. 따라서 $\alpha^{dQ} = \alpha^{bQ} = (\alpha^Q)^b = \beta^b$ 이다. □

주기가 $2^n - 1$인 수열 $s_{ij}(t)$의 상관관계를 분석하는데 있어서 주어진 수열을 주기가 $2^m - 1$인 수열 $2^m + 1$개로 나누어 생각해보자. $s_{ij}(t)$를 $(2^m - 1) \times (2^m + 1)$의 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 두고 보조정리 1을 이용하면 $s_{ij}(t)$는 다음과 같다.

$$\begin{aligned} s_{ij}(t) &= Tr_1^m\left\{\left[Tr_m^n\left(\alpha^{2bt} + \gamma_i \alpha^{2dt}\right) + \eta_j \beta^{bt}\right]^r\right\} \quad (10) \\ &= Tr_1^m\left\{\beta^{2brt_1}\left[Tr_m^n\left(\alpha^{2bt_2} + \gamma_i \alpha^{2dt_2}\right) + \eta_j \beta^{bt_2}\right]^r\right\} \end{aligned}$$

따라서 두 수열 $s_{ij}(t), s_{kl}(t)$와 이동량 τ에 대하여 식 (6)의 상관관계에서 $s_{ij}(t+\tau) + s_{kl}(t)$는 식(11)과 같다.

$$s_{ij}(t+\tau) + s_{kl}(t) = Tr_1^m[\beta^{2brt_1} \cdot G(t_2, \tau)] \quad (11)$$

여기서 $G(t_2, \tau)$는 식 (12)와 같다.

$$G(t_2,\tau) := [Tr_m^n(\alpha^{2b(t_2+\tau)} + \gamma_i \alpha^{2d(t_2+\tau)}) + \eta_j \beta^{b(t_2+\tau)}]^r + [Tr_m^n(\alpha^{2bt_2} + \gamma_k \alpha^{2dt_2}) + \eta_l \beta^{bt_2}]^r \quad (12)$$

그러므로 $R_{ij,kl}(\tau)$는 식 (13)과 같다.

$$\begin{aligned} R_{ij,kl}(\tau) &= \sum_{t=0}^{2^n-2} (-1)^{Tr_1^m(\beta^{2brt_1} G(t_2,\tau))} \\ &= \sum_{t_2=0}^{Q-1} \sum_{t_1=0}^{2^m-2} (-1)^{Tr(\beta^{2brt_2} G(t_2,\tau))} \\ &= 2^m M_z - Q = 2^m(M_z-1) - 1 \end{aligned} \quad (13)$$

여기서 $M_z = |\{t_2 | G(t_2,\tau)=0\}|$로 수열 $s_{ij}(t+\tau) + s_{kl}(t)$를 $(2^m-1)\times(2^m+1)$의 배열로 나열했을 때, 모든 성분이 0인 열의 개수를 의미한다. $(r, 2^m-1)=1$이므로 $G(t_2,\tau)=0$은 식 (14)과 동치이다.

$$\begin{aligned} &Tr_m^n(\alpha^{2b(t_2+\tau)} + \gamma_i \alpha^{2d(t_2+\tau)}) + \eta_j \beta^{b(t_2+\tau)} \\ &+ Tr_m^n(\alpha^{2bt_2} + \gamma_k \alpha^{2dt_2}) + \eta_l \beta^{bt_2} = 0 \end{aligned} \quad (14)$$

$A := \alpha^\tau + 1$, $B := \gamma_i \alpha^{2dtau} - \gamma_k$, $C := \eta_j \beta^{btau} + \eta_l$라 두면 식 (14)은 식 (15)와 같다.

$$Tr_m^n(A\alpha^{2bt_2} + B\alpha^{2dt_2}) + C\beta^{bt_2} = 0 \quad (15)$$

식 (15)를 식(1)의 트레이스 정의에 의해 풀고 $\alpha^{(2^m-1)t_2}$를 y라 두면 식 (16)와 같다.

$$A + By^{2u} + A^{2^m} y^{2(u+v)} + B^{2^m} y^{2v} + Cy^{u+v} = 0 \quad (16)$$

식 (16)는 y에 대한 $2(u+v)$차 방정식이므로 해의 개수는 최대한 $2(u+v)$개 존재한다. 즉 $0 \le M_z \le 2(u+v)$ 이다. 따라서 제안된 비선형 이진수열의 일반화 모형에 대한 상관관계는 정리 2를 만족한다.

〈정리 2〉 S에 속하는 두 수열 $s_{ij}(t+\tau)$, $s_{kl}(t)$에 대한 상관관계 $R_{ij,kl}(\tau)$는 다음을 만족한다.

$$R_{ij,kj}(\tau) \in \{-2^m-1, -1, 2^m-1, \cdots, (2u+2v-1)2^m-1\}$$

〈예제〉 $n=6$, $m=3$, $f(x)=x^6+x^5+x^2+x+1$이라 하면 $Q=9$이다. $u=1, v=3$이고 $\gamma_i=\alpha^3, \eta_j=\beta$, $\gamma_k=\alpha^5, \eta_l=\beta^2$라 하자. 여기서 $\beta=\alpha^9$이고, $\beta^3=\beta+1$ 을 만족한다. 주어진 조건하에서 생성된 두 수열 $s_{ij}(t)$와 $s_{kl}(t)$를 $GF(2^3)$의 원소로 7×9배열로 표현하면 다음과 같다.

$$s_{ij}(t) = \begin{bmatrix} 1 & \beta^3 & \beta^6 & \beta^6 & \beta^3 & \beta^6 & \beta^5 & \beta^5 & \beta^2 \\ \beta^5 & \beta & \beta^4 & \beta^4 & \beta & \beta^4 & \beta^3 & \beta^3 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta^2 & \beta^5 & \beta & \beta & \beta^5 & \beta & 1 & 1 & \beta^4 \end{bmatrix}$$

$$s_{kl}(t) = \begin{bmatrix} \beta^6 & \beta^5 & \beta^3 & \beta^2 & 0 & \beta^4 & \beta & \beta^6 & \beta^6 \\ \beta^4 & \beta^3 & \beta & 1 & 0 & \beta^2 & \beta^6 & \beta^4 & \beta^4 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta & 1 & \beta^5 & \beta^4 & 0 & \beta^6 & \beta^3 & \beta & \beta \end{bmatrix}$$

$\tau=1$이면 $R_{ij}(1)=-9$이다. 또한 주어진 수열 $s_{ij}(t)$는 모든 성분이 0인 열이 없으므로 $s_{ij}(t+\tau)+s_{kl}(t)$에는 모든 성분이 0인 열이 없다. 따라서 식(13)에 의하여 모든 τ에 대하여 $R_{ij}(\tau)=-9$이다. □

제안된 비선형 수열 모형은 지금까지 제안되었던 많은 수열들을 모두 포함하고 있다. 식(9)에서 $u+v:=1, r:=1, \gamma_i:=0, \eta_i:=0$라 두면 m-수열이 된다. 또한 $u+v:=1, \gamma_i:=0, \eta_i:=0$라 두면 제안된 수열은 GMW 수열을 만족한다. $u+v:=1, r:=1, \gamma_i:=0, \eta_i:\neq 0$이면 Kasami 수열이 된다. $u+v:=1, \gamma_i:=0, \eta_i:\neq 0$이면 No 수열이 된다. $u+v:=1$이고 $\gamma_i:\neq 0$ 또는 $\eta_i:\neq 0$이면 Niho 형태의 수열이 된다.

Ⅳ. 결 론

본 논문에서는 트레이스함수를 이용하여 생성한 비선형 이진수열에 대하여 일반화된 모형을 제안하고 주어진 수열의 상관관계를 분석하였다. 제안하는 수열군은 Welch의 관점에서 최적의 상관관계를 갖는 기존 연구 결과인 m-수열, GMW 수열, Kasami 수열, No 수열, Niho 형태의 수열 등을 모두 포함한다. 따라서 훨씬 다양한 수열을 포함하고 있고 수열군의 크기도 크다. 따라서 다중접속 충돌을 최소화하는데 도움을 줄 것으로 사료된다. 향후 제안한 수열의 선형스

팬 분석이 필요하다.

감사의 글

이 논문은 2010년도 정부재원(교육과학기술부 인문사회연구역량강화사업비)으로 한국연구재단의 지원을 받아 연구되었습니다. (NRF-2010- 371-B00008).

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. Golombl, "On the classification of balanced binary sequences of period 2^n-1," IEEE Trans. Inform. Theory, Vol. IT-26(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 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(2), pp. 371-379, 1989.

[8] P. Z. Fan and M. Darnell, "Sequence design for communications applications," John Wiley and Sons Ltd., 1996.

[9] L.R. Welch, "Lower bounds on the maximum cross-correlation of signals," IEEE Trans. Inform. Theory, Vol. IT-20, pp. 397-399, 1974.

[10] T. Kasami, "Weight distribution of Bose-Chaudhuri-Hocquenghem codes," in Combinatorial Mathematics and Its Applications. Chapel Hill, NC: Univ. North Carolina Press, 1969.

[11] 최은숙, 조성진, 김진경, "GF(2^p)위에서의 LFSR과 CA를 이용한 shrunken 수열의 분석," 한국전자통신학회논문지, 5권, 4호, pp. 418-424, 2010.

[12] 최은숙, 조성진, "최적의 상호상관관계를 갖는 이진 수열의 설계," 한국전자통신학회논문지, 6권, 4호, pp. 539-544, 2011.

[13] K. Fazel and S. Kaiser, "Multi-carrier and Spread Spectrum Systems," John Wiley and Sons Ltd., 2003.

[14] D.J. Goodman and H.G. Myung, "Single Carrier FDMA; A New Air Interface for Long Term Evolution," John Wiley and Sons Ltd,. 2008.

[15] 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.

[16] R. Prasad, CDMA for Wireless Personal Communications, Artech House Publishers, 1996.

[17] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 1997.

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

권숙희(Sook-Hee Kwon)

1989년 2월 경북대학교 조경학과 졸업(농학사)
2011년 2월 부경대학교 응용수학과 졸업(이학석사)
2011년 3월~현재 : 부경대학교 응용수학과 박사과정
※ 관심분야 : 정보보호, 부호이론