낮은 상호 상관관계를 갖는 비선형 확장 이진 수열

최언숙* · 조성진** · 권숙희***

Non-linear Extended Binary Sequence with Low Cross-Correlation

Un-sook Choi* · Sung-jin Cho** · Sook-hee Kwon***

요 약

의사난수열은 코드 분할 다중접속과 같은 무선통신에서 중요한 역할을 한다. 여러 사용자가 동시에 시스템에 접속할 때 충돌이 발생 할 수 있는데, 의사난수열의 낮은 상관관계는 그런 통신시스템에서 다중 접속 간섭을 최소화 할 수 있다. 본 논문에서는 Welch bound의 관점에서 최적의 상호 상관관계 함숫값을 갖는 m-수열, GMW 수열, Kasami 수열, No 수열 등을 모두 포함하는 낮은 상호 상관관계를 갖는 비선형 확장 이진 수열군을 제안한다. 그리고 제안한 수열의 상호상관관계를 분석한다.

ABSTRACT

PN(Pseudo Noise) sequences play an important role in wireless communications, such as in a CDMA(code division multiple access) communication system. If there is a crash when multiple users simultaneously connected to a system, then PN sequences with low correlation help to minimize multiple access interference in such communication system. In this paper we propose a family of non-linear extended binary sequences with low cross-correlations and the family include m-sequence, GMW sequence, Kasami sequence and No sequence with optimal cross-correlation in terms of Welch bound. And we analyze cross-correlation of these sequences.

키워드

코드 분할 다중접속, 상관관계, m-수열, 비선형 이진 수열, 트레이스

Key word

CDMA, correlation, m-sequence, non-linear binary sequence, trace

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

접수일자 : 2011. 12. 27
심사완료일자 : 2012. 02. 16

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.4.730

Ⅰ. 서 론

정보화 사회로의 발전과 더불어 이동통신에 대한 수요와 관심이 급속이 증대되고 이에 따라 제한된 주파수 대역에서 아날로그 방식의 이동통신 시스템이 제공할 수 있는 수용 용량은 포화 상태에 이르렀다. 또한 이동통신망과의 접속에 따른 다양한 서비스 요구에 부응하기 위해 디지털 이동통신 시스템의 도입 및 그 방식으로의 전환이 불가피하게 된 것이다. 디지털 통신의 다중접속 방식은 크게 시간 분할 다중접속(TDMA, Time Division Multiple Access) 방식과 코드 분할 다중접속(CDMA) 방식으로 나눌 수 있다.

특히, 코드 분할 다중접속 방식은 여러 사용자가 주파수와 시간을 공유하면서 각 사용자에게 의사난수열을 할당하여 각 사용자는 송신 신호를 확산(spreading)하여 전송하고 수신부에서는 송신측에서 사용한 것과 동일한 의사난수열을 발생시켜 동기를 맞추고 수신된 신호를 역확산(despreading)하여 신호를 복원하는 방식으로 그 특성상 군사용으로 많이 이용되어 왔다. 하나의 위성과 여러 개의 지상 지구국으로 구성되어 있는 위성통신에 그 근원을 둔 다중접속은 일정의 주파수 대역을 가지는 공동의 통신 채널을 여러 사용자가 나누어 사용하는 것이다. 의사난수열은 이동통신 시스템의 다중접속방식의 표준으로 이용되는 코드 분할 다중 접속 방식과 같은 확산대역 통신시스템에서 많이 응용되고 있고 중요한 역할을 한다. 이러한 통신 시스템 사이에서 의사난수열의 중요한 기능은 다중 접속 충돌을 최소화하고, 가능한 시스템의 보안수준을 높이는 것, 그리고 더 많은 사용자들이 사용할 수 있도록 사용자수를 확대하는 것 등이 있다. 특히 다중 접속 충돌은 여러 사용자가 동시에 접속할 때 생기는 충돌에 의해 발생 할 수 있는데, 의사난수열의 낮은 상관관계는 다중 접속 충돌을 최소화 할 수 있다[1-5].

수열의 바람직한 성질 중 낮은 상관관계는 코드 분할 다중 접속의 능력을 가지기 위해 중요하다. Welch bound에 의한 최대 상관관계 값에 대한 하한은 의사난수열군의 상관관계 성질을 평가하는 데 자주 이용된다. 주기가 2^n-1이고 이상적인 자기상관 특성을 갖는 의사불규칙 수열들 중 대표적인 것이 m-수열, GMW 수열이 있고 최적의 상호 상관관계 함숫값을 갖는 Kasami 수열, No 수열 등이 있다[6-9].

본 논문에서는 코드 분할 다중접속과 같은 무선통신에서 다중 접속 충돌을 최소화하는데 도움을 주는 낮은 상호 상관관계를 갖는 비선형 확장 이진 수열군을 제안하고 이 수열들의 상호상관관계를 분석한다. 그리고 제안한 비선형 확장 이진 수열군은 Welch bound의 관점에서 최적의 상호 상관관계 함숫값을 갖는 기존 이진 수열 즉 m-수열, GMW 수열, Kasami 수열, No 수열, Zeng 수열 등을 모두 포함한다.

Ⅱ. 배경 지식 및 기존 연구

2.1. 코드 분할 다중접속

주파수를 많은 사용자가 사용할 수 있는 다중접속방식의 한 방법으로서 코드 분할 다중접속은 디지털 신호의 크기가 연속적인 값을 가지지 않고 '0'과 '1'만 가지는 신호로서 이러한 디지털 신호는 '0'과 '1'만 구별하면 되므로 신호전송에 있어서 잡음에 강한 특성을 보인다. 이러한 디지털 신호 여러 개를 동시에 전송하는 대표적인 방법이 코드 분할 다중접속이다[10,11].

코드 분할 다중접속에서 적합한 코드는 수신기가 입력신호의 동기화를 용이하게 하고 잡음이 신호를 왜곡시킬지라도 수신자가 원래의 데이터를 정확하게 재구성할 수 있도록 좋은 상관관계를 가지는 것이다. 예를 들면 A가 데이터 1,0,1을 전송할 때 신호가 그림 1과 같다면 키가 양의 신호 값이 +1인 경우 키 수열 A(A_k)는 0이 된다. 기존 데이터 값과 XOR연산하면 신호 A가 생긴다.

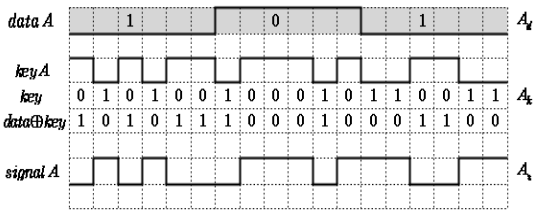


그림 1. 데이터 A의 신호화
Fig. 1 signaling of the data A

그리고 B가 데이터 1,0,0을 전송할 때는 그림 2와 같다. B 또한 A와 같은 과정을 거치고 A와 B의 신호가 겹치게 된다면 A+B가 된다.

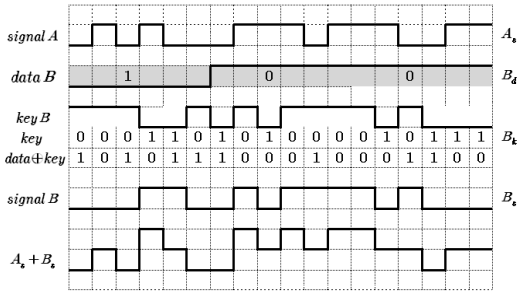


그림 2. 신호 A의 변조
Fig. 2 Modulation of the signal A

수신기는 A의 원래 데이터(A_d)를 재구성한다. 그림 3을 보면 (A+B)에 A_k를 곱하여 적분하게 되면 '-'값이 나올 경우 1을 의미하고 '+'값일 경우 0을 의미한다.

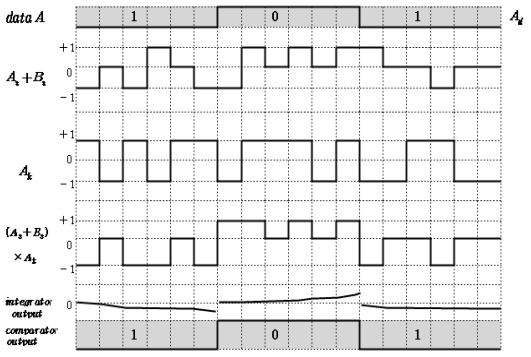


그림 3. 신호 A의 복조
Fig. 3 Demodulation of the signal A

여기서 만약 다른 키 수열을 가지고 있거나 송신기의 동기가 맞지 않는 경우는 적분 시에 0 또는 1로 값을 결정하기가 어렵다. 즉 잡음에 가까운 0에 가까운 값이 나타난다. 이는 도청에 대한 CDMA 고유의 방어능력을 보여준다. 이런 이유에서 보안을 위한 용도로도 사용될 수 있다.

2.2 트레이스 함수

트레이스 함수(trace function)는 유한체로부터 부분체로의 선형 매핑인데, 이 함수는 의사불규칙 수열의 설계와 분석을 위한 중요한 수학적 도구이다. 트레이스함수에 대한 정의와 그것들의 성질을 보면 대부분의 이진 의사난수열들은 트레이스 함수의 형태로 표현될 수 있다. 본 논문에서 수열의 생성을 위해 사용되는 트레이스 함수는 x는 $GF(2^n)$의 원소일 때, $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$는 식(1)과 같이 정의된다.

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

그리고 트레이스함수 $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$는 다음 성질을 만족한다[12].

(1) $Tr_m^n(x+y) = Tr_m^n(x) + Tr_m^n(y)\ \forall x, y \in GF(2^n)$.
(2) $Tr_m^n(ax) = a\,Tr_m^n(x),\ \forall a \in GF(2^m),\ x \in GF(2^n)$.
(3) Tr_m^n는 전사함수이다.
(4) $Tr_m^n(a) = ka,\ \forall a \in GF(2^m)$.
(5) $Tr_m^n(x^{2^{mi}}) = Tr_m^n(x),\ \forall x \in GF(2^n)$.
(6) $Tr_1^n(x) = Tr_1^m(Tr_m^n(x)),\ \forall x \in GF(2^n)$.
(7) 임의의 고정된 $\omega \in GF(2^m)$에 대하여 방정식 $Tr_m^n(x) = \omega$를 만족하는 해 $x(\in GF(2^n))$가 2^{n-m}개 존재한다.

2.3. 상관관계 함수

상관관계 함수(correlation function)란 두 수열사이의 유사성, 즉 관련성에 대한 측도이다. 자기 상관관계 함수(auto-correlation function)는 주기가 $2^n - 1$이며, t가 0에서 $2^n - 2$까지 변할 때 0 또는 1의 값을 가지는 이진 수열 $s(t)$의 자기 상관관계 함수 $R_a(\tau)$를 $\tau = 0, 1, 2, \cdots, 2^n - 2$에 대하여 다음과 같이 정의 한다.

$$R_a(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s(t+\tau)+s(t)} \tag{2}$$

이상적인 상관관계 함수를 갖는 의사난수열의 자기 상관관계 함수 $R_a(\tau)$는 다음 식과 같다.

$$R_a(\tau)=\begin{cases}2^n-1 & ,\ \tau=0 \bmod(2^n-1)\\ -1 & ,\ otherwise\end{cases} \quad (3)$$

그리고 상호 상관관계 함수(cross-correlation function)는 주기가 각각 2^n-1인 이진 수열의 $s_a(t)$와 $s_b(t)$의 상호 상관관계 함수 $R_{ab}(\tau)$를 $\tau=0,1,2,\cdots,2^n-2$에 대해 다음과 같이 정의할 수 있다.

$$R_{ab}(\tau)=\sum_{t=0}^{2^n-2}(-1)^{s_b(t+\tau)+s_a(t)} \quad (4)$$

Welch에 의해서 유도된 최대 상관관계 함숫값에 대한 하한은 의사난수열의 상관관계 성질을 평가하는데 이용되며, 주기가 2^n-1이고 $n=2m$인 경우, Welch Bound는 다음 식과 같다.

$$W_{MAX}\geq 2^m+1 \quad (5)$$

2.4. 기존 이진 수열

이상적인 상관관계를 갖는 m-수열 $m(t)$와 GMW 수열 $g(t)$은 다음 식 (6),(7)과 같다[6,7].

$$m(t)=Tr_1^n(\alpha^t) \quad (6)$$

$$g(t)=Tr_1^m([Tr_m^n(\alpha^t)]^r) \quad (7)$$

여기서 α는 $GF(2^n)$의 한 원시원소이고, $1\leq r<2^m-1$, $\gcd(r,2^m-1)=1$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 다음과 같다[8,9].

$$K_i(t)=Tr_1^n(\alpha^{2t})+Tr_1^m(\gamma_i\alpha^{Q\cdot t}) \quad (8)$$

$$N_i(t)=Tr_1^m\{[Tr_m^n(\alpha^{2t})+\gamma_i\alpha^{Q\cdot t}]^r\} \quad (9)$$

여기서 α는 $GF(2^n)$의 한 원시원소이고, $\gamma_i\in GF(2^m)$이다. 그리고 정수 r에 대하여 $1\leq r<2^m-1$이고 $\gcd(2^m-1,r)=1$이다.

Ⅲ. 비선형 이진수열

이 절에서는 트레이스함수를 이용하여 생성하는 확장된 비선형 이진 수열 모형을 제안하고 주어진 수열의 상호상관관계를 분석한다.

n과 m이 양의 정수이고 $n=2m$이라 하자. α가 $GF(2^n)$의 원시원소이고, β는 $GF(2^m)$의 원시원소라 하자. $\alpha^Q=\beta\left(Q=\frac{2^n-1}{2^m-1}=2^m+1\right)$이고 주기가 $N=2^n-1$인 비선형 수열 S가 다음과 같이 정의된다고 하자.

$$S=\{s_{ij}(t)|0\leq t\leq N-1,\ 1\leq i\leq 2^n,1\leq j\leq 2^m\} \quad (10)$$

$$s_{ij}(t)=Tr_1^m\{[Tr_m^n(\alpha^{(u+v)t}+\gamma_i\alpha^{(u2^m+v)t})+\eta_j\beta^{2^{m-1}(u+v)t}]^r\} \quad (11)$$

여기서 $u+v$는 짝수이고, $1\leq r<2^m-1$, $\gcd(r,2^m-1)=1$ $\gamma_i\in GF(2^n)$, $\gamma_i=\alpha^{i-2}$ $(\gamma_1=0,\gamma_2=1,\gamma_3=\alpha,\cdots)$이고, $\eta_j\in GF(2^m)$, $\eta_j=\beta^{j-2}$ $(\eta_1=0,\eta_2=1,\eta_3=\beta,\cdots)$이다.

다음은 수열의 상호 상관관계를 분석하는데 이미 잘 알려진 보조정리이다.

<보조정리 1> 임의의 $\delta\in GF(2^m)$에 대하여

$$\sum_{x\in GF(2^m)^*}(-1)^{Tr_1^m(\delta x)}=\begin{cases}-1 & ,\delta\neq 0\\ 2^m-1 & ,\delta=0\end{cases} \quad (12)$$

<보조정리 2> 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 다음을 만족한다.

$$\alpha^{(u2^m+v)Q}=\alpha^{(u+v)Q}=\beta^{(u+v)} \quad (13)$$

(증명) $\beta\in GF(2^m)$이면 $\beta^{2^m}=\beta$이므로

$$\begin{aligned}\alpha^{(u2^m+v)Q}&=\beta^{(u2^m+v)}\\ &=(\beta^{2^m})^u\cdot\beta^v\\ &=\beta^{u+v}\end{aligned} \quad (14)$$

주기가 2^n-1인 수열 $s_{ij}(t)$의 상호 상관관계를 분석을 위해 주기가 2^m-1인 수열 2^m+1개로 나누어서 $s_{ij}(t)$를 $(2^m-1)\times(2^m+1)$의 배열로 나타내어, 매개변수 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 2를 이용하면 $s_{ij}(t)$는 다음과 같다.

$$\begin{aligned} & Tr_m^n\left(\alpha^{(u+v)t}+\gamma_i\alpha^{(u2^m+v)t}\right)+\eta_j\beta^{2^{m-1}(u+v)t} \\ &= Tr_m^n\left(\alpha^{(u+v)(t_1Q+t_2)}+\gamma_i\alpha^{(u2^m+v)(t_1Q+t_2)}\right)+\eta_j\beta^{2^{m-1}(u+v)(t_1Q+t_2)} \\ &= \beta^{(u+v)t_1}\left\{Tr_m^n\left(\alpha^{(u+v)t_2}+\gamma_i\alpha^{(u2^m+v)t_2}\right)+\eta_j\beta^{2^{m-1}(u+v)t_2}\right\} \end{aligned} \quad (15)$$

따라서 두 수열 $s_{ij}(t), s_{kl}(t)$와 이동 량 τ에 대하여 상호 상관관계에서 $s_{ij}(t+\tau)+s_{kl}(t)$는 식 (16)과 같다.

$$s_{ij}(t+\tau)+s_{kl}(t)=Tr_1^m[\beta^{(u+v)rt_1}\cdot f(t_2,\tau)] \quad (16)$$

여기서 $f(t_2,\tau)$는 식 (17)과 같다.

$$\begin{aligned} & f(t_2,\tau): \\ &= [Tr_m^n(\alpha^{(u+v)(t_2+\tau)}+\gamma_i\alpha^{(u2^m+v)(t_2+\tau)})+\eta_j\beta^{2^{m-1}(u+v)(t_2+\tau)}]^r \\ &\quad +[Tr_m^n(\alpha^{(u+v)t_2}+\gamma_k\alpha^{(u2^m+v)t_2})+\eta_l\beta^{2^{m-1}(u+v)t_2}]^r \end{aligned} \quad (17)$$

그러므로 $R_{ij,kl}(\tau)$는 다음과 같다.

$$\begin{aligned} R_{ij,kl}(\tau) &\equiv \sum_{t=0}^{2^n-2}(-1)^{s_{ij}(t+\tau)+s_{kl}(t)} \\ &= \sum_{t_2=0}^{Q-1}\sum_{t_1=0}^{2^m-2}(-1)^{Tr_1^m(\beta^{(u+v)rt_1}f(t_2,\tau))} \\ &= \sum_{t_2=0}^{Q-1}\left(\sum_{x\in GF(2^m)}(-1)^{Tr_1^m(\beta^{(u+v)rt_1}f(t_2,\tau))}-1\right) \\ &= 2^mM-Q=(M-1)2^m-1 \end{aligned} \quad (18)$$

여기서 $M=|\{t_2|f(t_2,\tau)=0\}|$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.

$\gcd(r,2^m-1)=1$이므로 $f(t_2,\tau)=0$은 식 (19)과 동치이다.

$$\begin{aligned} & Tr_m^n(\alpha^{(u+v)(t_2+\tau)}+\gamma_i\alpha^{(u2^m+v)(t_2+\tau)})+\eta_j\beta^{2^{m-1}(u+v)(t_2+\tau)} \\ &\quad +Tr_m^n(\alpha^{(u+v)t_2}+\gamma_k\alpha^{(u2^m+v)t_2})+\eta_l\beta^{2^{m-1}(u+v)t_2}=0 \end{aligned} \quad (19)$$

$A:=\alpha^{(u+v)\tau}+1, B:=\gamma_i\alpha^{(u2^m+v)\tau}+\gamma_k, C:=\eta_j\beta^{2^{m-1}(u+v)\tau}+\eta_l$라 두면 식 (19)는 다음과 같다.

$$\begin{aligned} & F(t_2,\tau) \\ &= Tr_m^n(A\alpha^{(u+v)t_2}+B\alpha^{(u2^m+v)t_2})+C\beta^{2^{m-1}(u+v)t_2}=0 \end{aligned} \quad (20)$$

그러면 $f(t_2,\tau)=0$이 $F(t_2,\tau)=0$일 필요충분조건은 $\gcd(r,2^m-1)=1$이다. 식 (20)을 식(1)의 트레이스 정의에 의해 풀고 α^{t_2}를 x라 두면 식을 $g(x)$라 하면 $\alpha^{(u2^m+v)2^m}=\alpha^{u+2^mv}$이므로 다음과 같다.

$$\begin{aligned} & g(x)=Tr_m^n(Ax^{(u+v)}+Bx^{(u2^m+v)})+Cx^{2^{m-1}(u+v)Q} \\ &= Ax^{(u+v)}+A^{2^m}x^{(u+v)2^m}+Bx^{(u2^m+v)}+B^{2^m}x^{(u2^m+v)2^m}+Cx^{2^{m-1}(u+v)Q} \\ &= Ax^{(u+v)}+A^{2^m}x^{(u+v)2^m}+Bx^{(u2^m+v)}+B^{2^m}x^{(u2^m+v)}+Cx^{2^{m-1}(u+v)Q}=0 \end{aligned} \quad (21)$$

$$x^{2^{m-1}(u+v)Q-(u+v)}=\left(x^Q\right)^{2^m\frac{u+v}{2}-2\frac{u+v}{2}}=\left(x^{2^m-1}\right)^{\frac{u+v}{2}}$$

이므로 양변을 $x^{(u+v)}$로 나누어 정리하고 $y:=x^{2^m-1}$로 나누어 정리하면

$$A+By^u+B^{2^m}y^v+Cy^{\frac{u+v}{2}}+A^{2^m}y^{u+v}=0 \quad (22)$$

식 (22)는 y에 대한 $u+v$차 방정식이므로 해의 개수 최대한 $u+v$개 존재한다. 즉 $0\le M\le u+v$이다. 따라서 제안된 비선형 확장 이진 수열의 상호 상관관계는 다음 정리를 만족한다.

<정리 3> S에 속하는 두 수열 $s_{ij}(t)$, $s_{kl}(t)$에 대한 상호상관관계 $R_{ij,kl}(\tau)$는 다음을 만족한다.

$$R_{ij,kl}(\tau)\in\{-2^m-1,-1,2^m-1,\cdots,(u+v-1)2^m-1\} \quad (23)$$

<예제 4> $n:=6,\ m:=3, f(x)=x^6+x+1, r:=3,$ $u=1,\ v=3$이고 $\gamma_i=\alpha,\ \eta_j=\beta,\ \gamma_k=\alpha^2, \eta_l=\beta^2$라 하자. 여기서 $\beta=\alpha^9$이고, $\beta^3=\beta^2+1$을 만족한다. 주어

진 조건하에서 생성된 두 수열 $s_{ij}(t)$와 $s_{kl}(t)$를 $GF(2^3)$의 원소로 7×9배열로 표현하면 다음과 표현하면 다음과 같다.

$$s_{ij}(t) = Tr_1^3\Big\{\big[\, Tr_3^6\big(\alpha^{4t}+\alpha\cdot\alpha^{11t}\big)+\beta\cdot\beta^{2t}\big]^3\Big\}$$

$$s_{kl}(t) = Tr_1^3\Big\{\big[\, Tr_3^6\big(\alpha^{4t}+\alpha^2\cdot\alpha^{11t}\big)+\beta^2\cdot\beta^{2t}\big]^3\Big\}$$

$$\begin{matrix} s_{ij}(t) \\ \begin{pmatrix} 001101011 \\ 000111001 \\ 101000110 \\ 001010010 \\ 101111111 \\ 100010100 \\ 100101101 \end{pmatrix} \end{matrix} \quad \begin{matrix} s_{kl}(t) \\ \begin{pmatrix} 010001010 \\ 001111011 \\ 100111100 \\ 011110001 \\ 101000111 \\ 111001101 \\ 110110110 \end{pmatrix} \end{matrix}$$

7	-1	-1	-1	-9	-9	-1	7	7
7	-9	1	-1	-1	-1	-1	-1	-1
-1	1	1	-1	1	-1	-1	-1	-9
-9	7	-9	-9	7	-1	15	-9	-1
7	-1	-1	7	-9	-9	15	-9	-1
-1	7	7	-1	-9	-1	-9	15	7
-9	-9	-1	7	15	7	-9	7	-9

이 수열의 상호 상관함수 $R_{ij,kl}\in\{-9,-1,7,15\}$이다. 표 1은 제안한 비선형 확장 이진 수열과 최적의 상호 상관관계 함숫값을 갖는 기존 이진 수열과 관계를 살펴본 것이다.

Ⅳ. 결론

본 논문에서는 CDMA와 같은 무선통신에서 다중 접속 충돌을 최소화하는데 도움을 주는 낮은 상호 상관관계를 갖는 비선형 확장 이진 수열을 제안하고 이 수열의 상호 상관관계를 분석하였다. 제안한 비선형 확장 이진 수열은 Welch bound의 관점에서 최적의 상호 상관관계 함숫값을 갖는 기존 이진 수열 즉 m-수열, GMW 수열, Kasami 수열, No 수열, Zeng 수열 등을 모두 포함한다.

표 1. 비선형 확장 이진 수열과 기존 이진 수열의 관계
Table. 1 correlation between non-linear extended binary sequence and existing binary sequence

$s_{ij}(t) = Tr_1^m\Big\{\big[\, Tr_m^n\big(\alpha^{(u+v)t}+\gamma_i\alpha^{(2^m u+v)t}\big)+\eta_j\beta^{2^{m-1}(u+v)t}\big]^r\Big\}$	
m-수열	$u:=1, v:=1,\ r:=1\ ,\ \gamma_i:=0\ ,\ \eta_j:=0$ $m(t) = Tr_1^n(\alpha^{2t})$
GMW 수열	$u:=1, v:=1,\ \gamma_i:=0\ ,\ \eta_j:=0$ $g(t) = Tr_1^m\Big\{\big[\, Tr_m^n(\alpha^{2t})\big]^r\Big\}$
Kasami 수열	$u:=1, v:=1,\ r:=1\ ,\ \gamma_i:=0\ ,\ \eta_j:\neq 0$ $K_i(t) = Tr_1^m\Big\{\big[\, Tr_m^n(\alpha^{2t})+\eta_j\beta^t\big]\Big\}$
No 수열	$u:=1, v:=1,\ \gamma_i:=0\ ,\ \eta_j:\neq 0$ $N_i(t) = Tr_1^m\Big\{\big[\, Tr_m^n(\alpha^{2t})+\eta_j\beta^t\big]^r\Big\}$
Zeng 수열[14]	$\eta_j:=0$ $Z_i(t) = Tr_1^m\Big\{\big[\, Tr_m^n\big(\alpha^{(u+v)t}+\gamma_i\alpha^{(u\cdot 2^m+v)t}\big)\big]^r\Big\}$

참고문헌

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

[2] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, "Spread Spectrum Communications, Vol. 1, Rockville, MD: Computer Science Press," 1985.

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

[4] 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.

[5] 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.

[6] R.A. Games, "Cross correlation of m-sequences and GMW sequences with the same primitive polynomial", Discrete Appl. Math. Vol. 12, pp. 139-146, 1985.

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

[8] T. Kasami, "Weight distribution of Bose-Chaudhuri-Hocquenghem codes," in Combi- natorial Mathematics and Its Applications. Chapel Hill, NC: Univ. North Carolina Press, 1969.
[9] 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.
[10] N. Yee, J-P. Linnartz and G. Fettweis, "Multi-carrier CDMA in indoor wireless Radio Networks," Proc. of IEEE PIMRC '93, Yokohama, Japan, Sept. 1993, pp. 109-13.
[11] R. Prasad, "CDMA for Wireless Personal Communications," Artech House Publishers, 1996.
[12] R. Lidl and H. Niederreiter, "Finite Fields," Cambridge University Press 1997.
[13] L.R. Welch, "Lower bounds on the maximum cross-correlation of signals," IEEE Trans. Inform. Theory, vol. IT-20, pp. 397-399, 1974.
[14] F.X. Zeng and Z.Y. Zhang, "Several Families of Sequences with Low Correlation and Large Linear Span", IEEE Trans. Fundamentals. vol. E91-A, pp. 2263-2268, 2008.

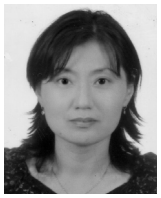
저자소개

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



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