부분체를 이용한 비선형 수열의 상호상관관계의 효율적인 계산방법

최언숙* · 조성진** · 김석태***

Computing Method of Cross-Correlation of Non-Linear Sequences Using Subfield

Un-Sook Choi* · Sung-Jin Cho** · Seok-Tae Kim***

요 약

확산수열(spreading sequence)은 다중 반송파 대역확산(multi-carrier spectrum) 통신시스템과 CDMA와 같은 무선통신에서 중요한 역할을 한다. 이러한 통신 시스템에서 낮은 상호상관관계를 갖는 확산수열은 다중접속 충돌을 최소화하고, 시스템의 보안수준을 가능한 높일 수 있다. 수열을 설계하는 데 있어 상호상관관계를 분석한는 것을 반드시 필요한 절차이다. 상호상관관계를 분석하기 위해서는 많은 계산 시간이 요구된다. 본 논문에서는 비선형 이진수열의 상호상관관계를 실제적으로 계산하는 과정에서 부분체를 이용하여 효과적으로 구하는 방법을 제안한다.

ABSTRACT

Spreading sequence play an important role in wireless communications, such as in a CDMA(code division multiple access) communication system and multi-carrier spectrum communication system. Spreading sequences with low cross-correlation, in a direct-sequence spread spectrum communication system, help to minimize multiple access interference and to increase security degree of system. Analysis of cross-correlations between the sequences is a necessary process to design sequences. However it require lots of computing time for analysis of cross-correlations between sequences. In this paper we propose a method which is possible to compute effectively cross-correlation using subfield in the process of practical computation of cross-correlation between nonlinear binary sequences.

키워드

확산수열, 비선형 이진수열, 상호상관관계, 트레이스, 부분체

Key word

spreading sequence, nonlinear binary sequence, cross-correlation, trace, subfield

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

접수일자 : 2012. 03. 12
심사완료일자 : 2012. 04. 30

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.8.1686

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, 현재 국내휴대폰 가입자는 지난 해 9월 국내 휴대폰 가입자의 수는 5000만 명을 넘어섰다. 또한 스마트폰 사용자의 수도 2000만 명을 넘어섰다. 새롭게 등장하는 다양한 형태의 무선통신 서비스를 수용하기 위해 고려되어야 하는 가장 중요한 문제 중의 하나가 한정된 전파자원을 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.

다중접속기술은 하나의 무선통신채널에 여러 사용자의 신호를 사용자 서로 간에 간섭을 일으키지 않고 전송할 수 있도록 하는 기술로서 여러 가지 디지털통신 시스템의 요소기술 중에서 가장 중요한 것이며 또한 무선통신시스템의 구조를 가장 크게 바꾸어 주는 것이다. 따라서 디지털이동통신시스템의 방식을 나눌 때 다중접속방식에 따라 주파수분할다중접속 (FDMA: frequency division multiple access), 시분할다중접속 (TDMA: time division multiple access), 부호분할다중접속 (CDMA: code division multiple access) 등으로 나뉘게 된다(그림 1).

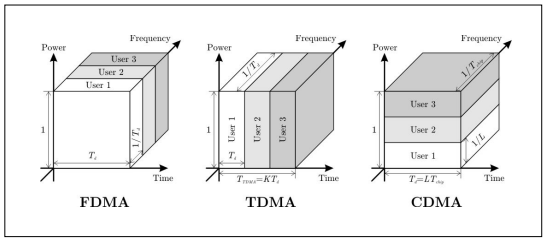

그림 1. 다중접속방식
Fig. 1 Multiple Access Schemes

CDMA 통신방식은 군통신시스템에서 주로 사용되어 왔던 확산대역(spread spectrum) 통신방식의 하나로 무선통신이론 중에서 가장 최신의 이론으로 매우 구현이 어려운 방식이라 할 수 있으며 우리나라에서 세계 최초로 대규모의 상용화 성공한 시스템이라 할 수 있다. 이러한 통신시스템 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, 낮은 상호상관관계(cross-correlation)를 갖는 확산수열은 다중 접속 충돌을 최소화 할 수 있다. 낮은 상호상관관계를 갖는 우수한 확산수열에 대한 연구가 많은 연구자들에 의해 진행되어왔다[1-7]. 생성된 수열의 상호상관관계의 기준은 Welch bound이다. 따라서 생성된 수열이 통신시스템에 응용되기 위해서는 Welch bound를 만족해야 한다[8].

적당한 정수 n에 대하여 2 가지 값을 갖는 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[5-9]. 이러한 수열이 제안될 때 꼭 분석해야하는 것이 바로 상호상관관계이다. 상호상관관계를 계산하기 위하여 유한체상에서 방정식을 푸는 문제, 이차형식을 고려하는 방법 등 여러 가지 방법들이 제안되었다[2,7,10,11]. 본 논문에서는 트레이스를 이용하여 발생되는 이진수열의 상호상관관계를 계산하는 방법으로 부분체를 이용하여 기존의 방법보다 효과적으로 빠르게 상호상관관계를 계산하는 방법을 제안한다.

Ⅱ. 본 론

디지털방식의 이동전화시스템은 근본적으로 송신되는 메시지가 디지털 데이터이어야 한다. 이러한 디지털 데이터를 전송하기 위하여 디지털통신방식이 사용되어야 하는데 이 방식에는 여러 가지 요소기술들이 있다. 예를 들면 아날로그 음성을 디지털 데이터로 바꾸어 압축하는 음성부호화, 채널에서 전송되는 데이터에 발생되는 비트오류를 정정하기 위한 오류정정부호, 신호의 전

송 및 수신을 위한 변조기 및 복조기, 그리고 가장 중요한 요소기술인 채널에서의 다중접속기술 등이 있다.

2.1. CDMA 방식

CDMA에서는 여러 사용자가 동일한 주파수를 동시에 사용한다[12]. 이를 위하여 송신자의 통화에 대해서 특별한 확산코드를 더하여 주파수 대역폭을 넓혀서 송신한다. 이 때 수신측은 송신측에서 부여한 것과 동일한 코드에 의해 자기에게 오는 통화를 구별해 낸다[12]. 그림 2는 CDMA방식을 이용한 통신시스템 블록도이다.

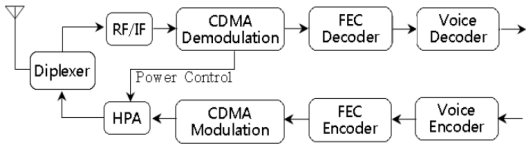

그림 2. CDMA 방식을 이용한 통신시스템
Fig. 2 Communication system using CDMA scheme

확산대역통신방식은 송신기에서 정보신호의 스펙트럼을 넓게 확산하여 전송하고 수신기에서는 수신된 신호의 주파수 스펙트럼을 역확산하여 복원하는 방식이다. 이동통신에서 사용하는 확산대역통신방식은 직접수열 방식의 부호분할다중접속(DS-CDMA) 방식이다. DS-CDMA 방식을 간단히 CDMA라고도 하는데 이 방식은 여러 사용자가 하나의 무선채널을 사용하는 경우 시간과 주파수를 공유하면서 사용자간의 간섭을 최소화하기 위하여 각 사용자에게 확산부호인 상호상관특성이 우수한 PN(pseudo-noise) 수열을 할당하고 각 사용자는 할당된 PN 수열을 이용하여 송신할 신호를 확산하여 전송하고 수신 측에서는 송신 측에서 사용한 것과 같은 PN 수열을 발생시켜서 동기를 맞추고 이를 이용하여 수신된 신호를 역확산하여 원하는 신호를 복원한다. 최근 들어서 PN 수열은 그 응용분야가 점점 넓어지면서 그 중요성이 증대되고 있다. PN 수열은 확산대역통신방식의 직접수열방식 및 CDMA 통신방식에 사용될 뿐 아니라 데이터나 영상신호 및 음성신호의 스크램블링을 위해서 사용되고 있다. 그리고 PN 수열은 컴퓨터에서 랜덤 데이터를 발생시키는데 사용되며 암호화과정에서 키스트림(key stream)으로 사용되고 있다. 이러한 PN 수열들이 가지고 있어야 할 바람직한 성질들은 낮은 상호상관관계, 큰 선형스팬, 많은 서로 다른 수열군의 존재 등이다.

이러한 좋은 특성을 갖는 수열 중에 m-수열라는 것이 있는데 이들은 IS-95 CDMA 방식의 이동전화시스템에서는 주기가 32768인 Pilot PN 수열라는 이름으로 사용되고 있고 또한 주기가 $2^{42}-1$인 수열이 긴부호(long code)라는 이름으로 매우 중요한 역할을 하며 사용되고 있다[13].

2.2. 트레이스 함수를 이용한 비선형 이진수열과 상호상관관계

주기가 $2^n-1(:=N)$이고 이상적인 자기상관 특성을 갖는 의사불규칙 수열은 확산스펙트럼 통신시스템, 레이다 시스템, 스트림암호시스템, CDMA 등에서 사용영역을 넓혀왔다. 수열 $\{s(t), t=0,1,\cdots,N-1\}$의 자기상관함수 $R_s(\tau)$가 식(1)과 같은 값을 가질 때 이상적인 자기상관특성을 갖는다고 말한다[3].

$$R_s(\tau)=\begin{cases} N & , \ \tau \equiv 0 \mod N \\ -1 & , \ \tau \not\equiv 0 \mod N \end{cases} \tag{1}$$

여기서 N은 수열의 주기이고 $R_s(\tau)$는 식(2)와 같이 정의한다.

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

이를 만족하는 대표적인 수열들은 m-수열, GMW 수열, Kasami 수열, No 수열, Gold 수열, Niho 유형의 수열, 확장된 비선형 이진수열 등이 있다[5-10]. 이러한 수열은 트레이스(trace) 함수를 이용하여 설계되었다. 트레이스 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 약수이

므로 $GF(2^m) \subset GF(2^n)$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(3)과 같이 정의된다.

$$Tr_m^n(x)=\sum_{i=0}^{k-1} x^{2^{m\cdot i}} \tag{3}$$

트레이스함수 $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$는 다음 성질을 만족한다[14].

(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 (4),(5)와 같다[5,6].

$$m(t)=Tr_1^n(\alpha^t) \tag{4}$$

$$g(t)=Tr_1^m([Tr_m^n(\alpha^t)]^r) \tag{5}$$

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 식 (6),(7)과 같다[7,9].

$$K_i(t)=Tr_1^n(\alpha^{2t})+Tr_1^m(\gamma_i\alpha^{Q\cdot t}) \tag{6}$$

$$N_i(t)=Tr_1^m\{[Tr_m^n(\alpha^{2t})+\gamma_i\alpha^{Q\cdot t}]^r\} \tag{7}$$

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.

α가 $GF(2^n)$의 한 원시원소라 할 때, $Tr_1^n(\alpha^t)$에 의해 생성된 수열을 $s_i(t)$라 하고 수열 $s_i(t)$를 r만큼 씩 건너뛰며 생성한 수열을 $s_j(t)$라 하면 $s_j(t)=Tr_1^n[(\alpha^t)^r]$이다. 이렇게 하나의 수열과 그 수열을 적당히 건너뛰어 얻은 수열에 대해 고려하는 수열을 Niho 형태의 수열이라 한다.

주기가 N인 이진수열의 상관관계 $R_{ij}(\tau)$는 이동량이 $\tau\,(0 \le \tau \le N-1)$일 때, 두 수열 $s_i(t+\tau)$와 $s_j(t)$에 대하여 식(8)과 같다.

$$R_{ij}(\tau)=\sum_{t=0}^{N-1}(-1)^{s_i(t+\tau)+s_j(t)} \tag{8}$$

임의의 $\delta \in GF(2^m)$에 대하여 식 (9)는 이미 잘 알려져 있다[5].

$$\sum_{x \in GF(2^m)^*}(-1)^{Tr_1^m(\delta x)}=\begin{cases}-1 & ,\delta \neq 0\\ 2^m-1 & ,\delta=0\end{cases} \tag{9}$$

Ⅲ. 부분체를 이용한 이진수열의 상호상관관계

본 논문에서는 트레이스함수를 이용하여 생성된 수열의 상호상관관계를 효과적으로 계산하기 위한 방법으로 부분체를 이용하는 방법을 제안하고자 한다. 이를 위하여 다음과 같은 수열을 살펴보자.

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 $\alpha^Q=\beta$라 둘 수 있다. 여기서 $Q=(2^n-1)/(2^m-1)=2^m+1$이다. 주기가 $N=2^n-1$인 비선형 수열 S가 식(10)과 같이 정의된다고 하자[15].

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

여기에서 $s_{ij}(t)$는 식(11)을 만족한다.

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

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

$\gcd(u+v, 2^n-1)=1$ 이다.

식(11)에서 정의된 비선형 이진수열은 2절에서 언급한 지금까지 제안되었던 많은 수열들을 모두 포함하고 있다. 식(11)에서 $u+v=1,\ r=1, \gamma_i=0, \eta_i=0$라 두면 식(4)의 $m-$수열이 된다. 또한 $u+v=1, \gamma_i=0, \eta_i=0$라 두면 식(11)은 식(5)의 GMW 수열을 만족한다. $u+v=1,\ r=1, \gamma_i=0, \eta_i\neq 0$이면 식(6)의 Kasami 수열이 된다. 그리고 $u+v=1, \gamma_i=0, \eta_i\neq 0$이면 식(7)의 No 수열이 된다. Niho 형태의 수열은 식(11)에서 $s_i(t)$는 $u+v=1,\ \gamma_i=0, \eta_j=0$이고 $s_j(t)$는 $u+v=0$이고 동식에 $\gamma_i\neq 0$또는 $\eta_i\neq 0$이면 된다.

식(11)에서 정의된 상호상관관계 $R_{ij,kl}(\tau)$는 $\{-2^m-1, -1, 2^m-1, \cdots, (2u+2v-1)2^m-1\}$의 원소 중 하나이다[15]. 주어진 i, j, k, l에 대하여 τ에 관한 실제 상호상관관계를 계산하기 위해서는 수열을 발생시켜서 $R_{ij}(\tau) = \sum_{t=0}^{N-1}(-1)^{s_{ij}(t+\tau)+s_{kl}(t)}$를 계산해야 한다.

<예제 1> $n=6,\ m=3,\ f(x)=x^6+x^5+x^4+x+1$이라 하면 $Q=9$이다. $u=1, v=3, r=5$이고 $\gamma_i=\alpha^7, \eta_j=\beta,\ \gamma_k=\alpha^5, \eta_l=\beta^3$라 하자. 여기서 $\beta=\alpha^9$이고, $\beta^3=\beta^2+1$을 만족하며, α는 $GF(2^6)$의 원시원소로 $\alpha^6=\alpha^5+\alpha^4+\alpha+1$을 만족한다. 식 (8)에서 정의된 이동량 τ가 $\tau=15$일 때, 식(8)에 의해 상호상관관계는 $R_{ij,kl}(15)=7$이다. 그림 3은 주어진 조건에 따라 $s_{ij}(t)$와 $s_{kl}(t)$를 구하고 주어진 이동량을 $\tau=15$라 두었을때 $s_{ij}(t+\tau)+s_{kl}(t)$수열을 구한 뒤 식(8)에 따라 상호상관관계를 구하는 과정이다. 식(8)의 상호상관관계 $R_{ij,kl}(\tau)$는 $s_{ij}(t+\tau)+s_{kl}(t)$ 수열의 성분이 0이면 +1, 1이면 -1이 되고 한 주기 내의 수열의 개수는 2^n-1이므로 $s_{ij}(t+\tau)+s_{kl}(t)$의 한 주기 내의 수열 성분 중 0의 개수를 $N(0)$라 하면 $R_{ij,kl}(\tau)$는 식(12)를 만족한다.

$$R_{ij,kl}(\tau) = 1\cdot N(0)+(-1)\cdot(2^n-1-N(0)) = 2N(0)-2^n+1 \quad (10)$$

상호상관관계를 효과적으로 구하기 위해 부분체를 생각해 보자. $n=2m$을 만족하므로 주어진 수열의 주기는 $(2^m-1)(2^m+1)$로 표현 할 수 있다. 따라서 $s_{ij}(t)$ 수열을 $(2^m-1)\times(2^m+1)$배열로 나타 낼 수 있다.

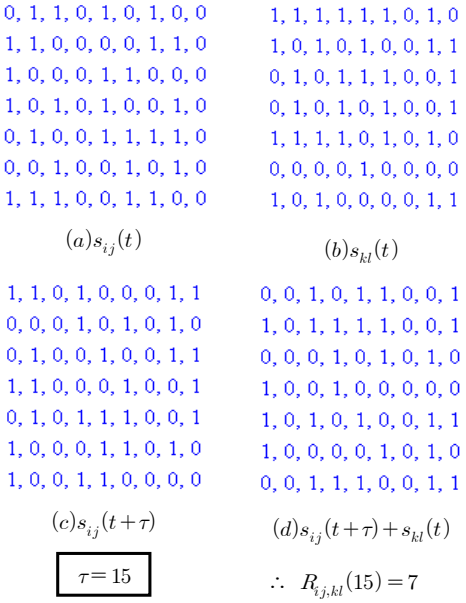

그림 3. 수열의 상호상관관계를 구하는 과정
Fig. 3 Computation procedure for cross-correlation of sequences

$s_{ij}(t)$ 수열은 비선형 이진수열이지만, 이 수열은 $(2^m-1)\times(2^m+1)$로 배열했을 때 각 열은 $GF(2^m)$에서 $m-$수열이 되거나 모든 성분이 0인 0-수열이 된다. $s_{kl}(t)$도 동일한 결과를 따른다. $s_{ij}(t)$와 $s_{kl}(t)$를 τ에 따라 이동한 $s_{ij}(t+\tau)+s_{kl}(t)$ 수열도 각 열은 $m-$수열이 되거나 모든 성분이 0인 0-수열이 된다. $R_{ij,kl}(\tau)$는 각 열의 상호상관관계 값의 합으로 구할 수 있으므로 $m-$수열인 열에 대한 경우의 상호상관관계는 -1이고 0-수열인 열의 상호상관관계는 2^m-1이다. 그러므로 $s_{ij}(t+\tau)+s_{kl}(t)$수열을 $(2^m-1)\times(2^m+1)$ 배열로 나타내었을 때 0-수열인 열의 개수를 $c(0)$라 하면 식 (12)는 식 (14)과 같다.

$$R_{ij,kl}(\tau) = (2^m-1)\cdot c(0)+(-1)\cdot(2^m+1-c(0)) = 2^m(c(0)-1)-1 \quad (11)$$

식 (11)을 $Tr_1^m(A_0(i,j)^r)$라 했을 때, $A_0(i,j)^r$는 $GF(2^n)$에서 $GF(2^m)$로 가는 함수이다. 그림 4는 그림 3의 (a) $s_{ij}(t)$와 (b) $s_{kl}(t)$ 에 대한 $A_0(i,j)^r$, $A_0(k,l)^r$ 값을 배열로 나타낸 것이다. 임의의 열에 대하여 0-수열을 제외

한 수열에 대하여 행 번호가 증가함에 따라 β의 지수가 5씩 커지고 있는 것은 예제 1에서 r값이 5이기 때문이다. 따라서 우리가 고려해야할 $c(0)$를 구하는데 있어서 r값은 고려할 필요가 없으므로 알고리즘의 간단화를 위해 r을 1로 두고 계산한다.

그림 4에서 (a) $A_0(i,j)$의 1행은 $[\beta^4, \beta^6, \beta^0, 0, \beta^3, \beta, \beta^6, \beta^2, 0]$이므로 그림 3의 (c)의 $s_{ij}(t+15)$에 대한 $A_{15}(i,j)$의 1행은$[\beta^0, \beta^3, 0, \beta^6, \beta, \beta^2, 0, \beta^5, \beta^3]$이 된다. 또한 그림 4의 (b)의 $A_0(k,l)$의 1행은 $[\beta^6, \beta^3, \beta^6, \beta^3, \beta^5, \beta^3, 0, \beta^6, \beta^4]$이 된다. 따라서 (d)의 $s_{ij}(t+\tau)+s_{kl}(t)$에 대한 $A_{15}(i,j)+A_0(k,l)$의 1행은 $[\beta^0, \beta^3, 0, \beta^6, \beta, \beta^2, 0, \beta^5, \beta^3]$ + $[\beta^6, \beta^3, \beta^6, \beta^3, \beta^5, \beta^3, 0, \beta^6, \beta^4]$ = $[\beta^4, 0, \beta^6, \beta^5, \beta^0, \beta^0, 0, \beta^3, \beta]$이 되고 따라서 $c(0)=2$이므로 식 (13)에 의하여 $R_{ij,kl}(\tau)=7$이다.

$$\begin{matrix}
\beta^6 & \beta^2 & \beta^0 & 0 & \beta & \beta^5 & \beta^2 & \beta^3 & 0 \\
\beta^4 & \beta^0 & \beta^3 & 0 & \beta^6 & \beta^3 & \beta^0 & \beta & 0 \\
\beta^2 & \beta^5 & \beta^3 & 0 & \beta^4 & \beta & \beta^5 & \beta^6 & 0 \\
\beta^0 & \beta^3 & \beta & 0 & \beta^2 & \beta^6 & \beta^3 & \beta^4 & 0 \\
\beta^5 & \beta & \beta^6 & 0 & \beta^0 & \beta^4 & \beta & \beta^2 & 0 \\
\beta^3 & \beta^6 & \beta^4 & 0 & \beta^5 & \beta^2 & \beta^6 & \beta^0 & 0 \\
\beta & \beta^4 & \beta^2 & 0 & \beta^3 & \beta^0 & \beta^4 & \beta^5 & 0
\end{matrix}$$

$(a) A_0(i,j)^r$

$$\begin{matrix}
\beta^2 & \beta & \beta^3 & \beta^2 & \beta & \beta^4 & \beta & 0 & \beta^2 & \beta^6 \\
\beta^0 & \beta^6 & \beta^0 & \beta^6 & \beta^3 & \beta^2 & \beta^6 & 0 & \beta^0 & \beta^4 \\
\beta^6 & \beta^4 & \beta^5 & \beta^4 & \beta^0 & \beta^4 & 0 & \beta^6 & \beta^3 \\
\beta^0 & \beta^2 & \beta^3 & \beta^2 & \beta^5 & \beta^3 & 0 & \beta^3 & \beta^0 \\
\beta^5 & \beta^0 & \beta & \beta^0 & \beta^3 & \beta^0 & 0 & \beta & \beta^5 \\
\beta^3 & \beta^5 & \beta^6 & \beta^5 & \beta & \beta^5 & 0 & \beta^6 & \beta^3 \\
\beta & \beta^3 & \beta^4 & \beta^3 & \beta^6 & \beta^4 & 0 & \beta^4 & \beta
\end{matrix}$$

$(b) A_0(k,l)^r$

그림 4. $s_{ij}(t)$와 $s_{kl}(t)$에 대한 $A_0(i,j)^r$와 $A_0(k,l)^r$
Fig. 4 $A_0(i,j)^r$ and $A_0(k,l)^r$ of $s_{ij}(t)$ and $s_{kl}(t)$

제안된 상호상관관계를 구하는 방법은 부분체를 이용하여 $A_\tau(i,j)$와 $A_0(k,l)$의 $Q(=2^m+1)$개의 성분만을 비교하여 $c(0)$의 값을 찾아 상호상관관계를 구할 수 있다. 기존의 상호상관관계를 구하는 방법은 설계된 $s_{ij}(t)$와 $s_{kl}(t)$, τ에 대하여 한 주기인 2^n-1개의 $s_{ij}(t+\tau)+s_{kl}(t)$ 수열을 발생시켜 수열 중 0의 개수를 세는 방법으로 제안된 방법보다 계산량과 수열을 발생시키는데 결리는 시간이 훨씬 오래 걸린다. 다시말해 제안된 방법은 $s_{ij}(t+\tau)=Tr_1^m(A_\tau(i,j)^r)$라 할 때 거듭제곱 계산을 줄이고, $A_\tau(i,j)+A_0(k,l)$만 계산하며 한 주기의 수열을 다 발생시킬 필요 없이 2^m+1개의 수열만으로 상호상관관계를 계산할 수 있는 방법으로 기존의 방법보다 빠르게 상호상관관계를 계산할 수 있다.

Ⅳ. 결 론

CDMA 통신시스템에서 확산수열로 매우 중요하게 사용되는 이진수열의 설계에서 수열의 상호상관관계와 선형스팬은 매우 중요한 요소이다. 특히 상호상관관계를 분석하는 방법은 수학적으로 매우 어렵다. 본 논문은 설계된 트레이스 함수를 이용하여 설계된 비선형 이진수열에 대하여 상호상관관계를 계산하는 과정에 있어 부분체를 이용하여 한 주기인 2^n-1개의 수열을 모두 발생시키지 않고 $2^m+1(=(2^n-1)/(2^m-1))$개의 수열만 발생시켜 상호상관관계를 계산하는 방법을 제안하여 기존의 상호상관관계를 계산하는 방법을 개선하였다.

참고문헌

[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 Netherlands: North-Holland, Vol. II, pp. 1765-1853, 1998.

[2] 최언숙, 조성진, 권숙희, "낮은 상호 상관관계를 갖는 비선형 확장 이진 수열", 한국정보통신학회논문지, Vol.16(4), pp.730-736, 2012.

[3] S.W. Golomb, "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] L.R. Welch, "Lower bounds on the maximum cross-correlation of signals", IEEE Trans. Inform. Theory, Vol. IT-20, pp. 397-399 1974.
[9] T. Kasami, "Weight distribution formula for some class of cyclic codes", Coordinated Science Laboratory, University of Illionos, Urbana, Tech. Rep. R-285 (AD632574), 1966.
[10] T. Helleseth, J. Lahtonen and P. Rosendahl, "On Niho type cross-correlation functions of m-sequences", Finite Fields and Their Applications, Vol. 13, pp. 305-317, 2007.
[11] A.M. Klapper, "d-form sequences: families of sequences with low correlation values and large linear spans", IEEE Trans. Inform. Theory, Vol. 41, pp. 423-431, 1995.
[12] R. Prasad, CDMA for Wireless Personal Communications, Artech House Publishers, 1996.
[13] D. Guo, L.K. Rasmussen and T.J. Lim, " Linear Parallel Interference Cancellation in Long-code CDMA Multiuser Detection", IEEE J. Selected Areas in Communications, Vol. 17, pp. 2074 - 2081, 1999.
[14] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 1997.
[15] U.S. Choi, S.J. Cho and S.H. Kwon, "Analysis of cross-correlation of extended non-linear binary sequences" (To appear).

저자소개

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

김석태(Seok-Tae Kim)

1983년: 광운대학교 전자공학과, 공학사
1988년: Kyoto Institute of Technology 전자공학과, 공학석사
1991년 : Osaka대학 통신공학과, 공학박사
1991년-현재 부경대학교 정보통신공학과 재직, 교수
※관심분야 : 영상처리, 패턴인식, 워터마킹, 셀룰라 오토마타론