확장 Zeng 수열의 상호상관 함숫값에 대한 연구

김한두* · 조성진a)** · 권민정** · 안현주**

A study on the cross-correlation function of extended Zeng sequences

Han-Doo Kim* · Sung-Jin Choa)** · Min-Jeong Kwon** · Hyun-Ju An**

요 약

코드분할 다중접속(CDMA) 시스템에서 대역확산 기법으로 사용되는 확산수열은 다중접속 간섭을 줄이고 높은 보안성을 위하여 상호상관관계가 낮고 선형복잡도가 큰 것으로 채택하는 것이 바람직하다. 그러나 수열군의 개수를 늘리고 선형복잡도를 높이기 위해서는 상호상관관계를 어느 정도 높이는 것은 불가피하다. 본 논문에서는 수열군의 개수가 크고 선형복잡도가 높은 확장 Zeng 수열을 제안하고 그 상호상관관계를 분석한다.

ABSTRACT

Spreading sequence is used for spreading spectrum in CDMA. For the purpose of minimizing multiple access interference and expanding linear span of the sequences, it is desirable to use such sequences with low correlation and high linear span. To obtain large family size and high linear span, the values of the correlation function of the sequences is more complex. In this paper, we propose the extended Zeng sequences with large family size and high linear span and analyze the correlation of the sequences.

키워드

Zeng sequences, Spread spectrum, Spreading sequences, Trace functions, Correlation functions
Zeng 수열, 대역확산, 확산수열, 트레이스 함수, 상호상관관계 함수

Ⅰ. 서 론

디지털 이동통신 기술 중 하나인 CDMA(Code Division Multiple Access)는 대역확산(Spread Spectrum) 기술을 활용하여 각각의 정보를 특정 부호로 분할하여 보내고 동일한 부호로 확산된 정보만을 선택하여 원래 신호를 재생하는 방식의 통신망이다. 직접 시퀀스(DS : Direct Sequence)를 대역확산 기법으로 사용하려면 PN(Pseudo Noise) 수열처럼 상호상호 상관관계가 낮고 개체수가 많은 수열이 필요하다. 이러한 수열을 확산수열(Spreading sequence)로 사용한 통신망은 다중접속 능력을 가지면서도 서로 다른 사용자에 의해 발생되는 간섭을 줄일 수 있다. 사용된 수열들의 상호상관관계가 낮으면 서로 다른 사용자에 의해 발생되는 다중접속 간섭(MAI : Multiple Access Interference)을 최소화하며, 통신 및 정보 보안성을 향상시킬 수 있다. 이와 같이 대역확산 다중접속 통신 시스템에서 사용되는 수열은 상호상관관계가 낮고 선형복잡도가 큰 수열을 확산수열로 도입하는 것이 바람직하다[1, 2].

* 인제대학교 컴퓨터응용과학부(mathkhd@inje.ac.kr), 기초과학연구소
a)** 교신저자 : 부경대학교 응용수학과(sjcho@pknu.ac.kr)
** 부경대학교 응용수학과
접수일자 : 2011. 12. 20 심사(수정)일자 : 2012. 01. 05 게재확정일자 : 2012. 01. 25

Welch의 하한 관점에서 최적 상호상관관계를 갖는 수열들은 사용할 수 있는 수열군의 개수가 작고 선형 복잡도(linear span)가 낮기 때문에 이를 개선하기 위해서는 확산수열의 상호상관관계를 높이는 것이 어느 정도 불가피하다[3-7]. Zeng 등은 상호상관 함숫값이 5개인 이진수열군을 제안했다[8]. 본 논문에서는 수열군의 크기가 크고 선형복잡도가 높은 새로운 확장 Zeng 수열을 제안하고 그 상호상관관계를 분석한다. 이 수열은 m-수열, GMW 수열, No 수열, Zeng 수열을 모두 포함한다.

II. 사전 지식

이 절에서는 새로운 수열군을 정의하고 그러한 수열군에 포함되는 수열들의 상호상관관계를 계산하기 위해 필요한 트레이스 함수를 살펴보고 이상적인 상호상관관계를 갖는 수열에 대해 간단히 정리한다.

<정의 1 [9]> 정수 n이 m의 배수일 때 트레이스 함수 $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$는 다음과 같이 정의한다.

$$Tr_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{m \cdot i}} = x + x^{2^m} + \cdots + x^{2^{m\left(\frac{n}{m}-1\right)}} \quad (1)$$

이때 $Tr_m^n(\cdot)$는 $GF(2^m)$상의 $GF(2^n)$의 트레이스 함수(trace function)라 한다.

<정리 2 [9]>

트레이스 함수 $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$는 다음과 같은 성질을 만족한다.

(a) x, y는 $GF(2^n)$의 원소, a, b는 $GF(2^m)$의 원소일 때, $Tr_m^n(ax+by) = aTr_m^n(x) + bTr_m^n(y)$이 성립한다.

(b) $GF(2^n)$의 임의의 원소 x와 음이 아닌 정수 i에 대하여 $Tr_m^n\left(x^{2^{mi}}\right) = \left\{Tr_m^n(x)\right\}^{2^{mi}}$, $Tr_m^n(x) = Tr_m^n\left(x^{2^{mi}}\right)$이 성립한다.

(c) $GF(2^m)$의 임의의 고정된 원소 β에 대하여, $Tr_m^n(x) = \beta$인 x는 2^{n-m}개 존재한다.

(d) $GF(2^n)$의 임의의 원소 x에 대하여, $Tr_1^n(x) = Tr_1^m\left[Tr_m^n(x)\right]$이 성립한다.

트레이스 함수의 성질 (a)로부터 트레이스 함수가 선형임을 알 수 있으며 성질 (d)는 m-수열의 확장된 형태인 GMW 수열을 생성하는데 중요한 역할을 한다. 이 트레이스 함수를 이용하여 다음과 같은 여러 가지 수열을 정의할 수 있다.

α가 $GF(2^n)$의 원시원소일 때, $GF(2)$상의 수열 $S = \{s(t) \mid t = 0, 1, 2, \cdots, 2^n - 2\}$에 대하여 주기 $2^n - 1$인 m-수열은 다음과 같이 정의한다[9].

$$s(t) := Tr_1^n(\alpha^t) \quad (2)$$

$n = km (m \geq 2)$인 양의 정수 m, n이 존재하고 정수 $r (2 \leq r \leq 2^m - 2)$이 $\gcd(r, 2^m - 1) = 1$을 만족할 때, $GF(2^n)$의 원시원소 α에 대하여 다음과 같이 정의된 $GF(2)$상의 수열 $S = \{s(t) \mid t = 0, 1, 2, \cdots, 2^n - 2\}$을 GMW 수열([10])이라 한다.

$$s(t) := Tr_1^m\left\{\left[Tr_m^n(\alpha^t)\right]^r\right\} \quad (3)$$

트레이스 함수의 성질 (d)를 이용하면 $r = 1$인 경우 GMW 수열은 m-수열이 된다는 것을 알 수 있다.

No 수열군([11])

$\mathbb{S} = \left\{\left\{s_i(t) \mid 0 \leq t \leq 2^n - 2\right\} \mid 0 \leq i \leq 2^m - 1\right\}$은 1보다 큰 양의 정수 m에 대해서 $n = 2m$일 때, $\gcd(r, 2^m - 1) = 1$인 정수 $r (2 \leq r \leq 2^m - 2)$에 대하여 다음과 같이 No 수열을 정의한다.

$$s_i(t) := Tr_1^m\left\{\left[Tr_m^n(\alpha^{2t}) + \gamma_i \alpha^{(2^m+1)t}\right]^r\right\} \quad (4)$$

단, α는 $GF(2^n)$의 원시원소이고 $\{\gamma_i \mid 0 \leq i \leq 2^m - 1\} = GF(2^m)$ 이다. No 수열에서 $\gamma_i = 0$을 대입하면 GMW 수열이 된다.

자연수 m, n이 $n = 2m$를 만족하고 $Q = \dfrac{2^n - 1}{2^m - 1} = 2^m + 1$일 때, $GF(2^n)$의 원시원소 α에 대하여, $GF(2)$ 상에서 다음과 같이 정의된 수열군

$$\mathbb{S} := \left\{\left\{s_i(t) \mid 0 \leq t \leq 2^n - 2\right\} \mid 0 \leq i \leq 2^m - 1\right\}$$

은 Kasami 수열군[3]이다.

$$s_i(t) := Tr_1^m\left\{Tr_m^n(\alpha^{2t})+\gamma_i\alpha^{Qt}\right\} \quad (5)$$

이 때 $\{\gamma_i \mid 0 \le i \le 2^m-1\} = GF(2^m)$이고 $(\alpha^Q)^{2^m-1}=1$이므로 α^Q은 $GF(2^m)$의 원시원소가 된다. 따라서 수열군 $\mathbb{S}$의 i번째 수열 $s_i(t)$는 주기가 2^n-1인 m-수열과 주기가 2^m-1인 더 짧은 m-수열을 더해서 만들어진다는 것을 알 수 있다. 식 (5)에서 $\gamma_i=0$인 경우는 m-수열이 되므로 Kasami 수열 또한 m-수열의 일반화된 형태임을 알 수 있다. $n=2m$을 만족하는 자연수 m, n과 $Q=2^m+1$에 대하여 $GF(2)$ 상에서 다음과 같이 정의된 수열군은 Zeng 수열군[8]이다.

$$\mathbb{S} = \{\{s_{i,j}(t) \mid 0 \le t \le N-1\} \mid 0 \le i \le 2^n-1, 0 \le j \le 2^m-1\}$$

$$s_{i,j}(t) := Tr_1^m\{\left[Tr_m^n\left(\alpha^{2t}+\gamma_i\alpha^{(3\cdot 2^{m-1})t}\right)+\eta_j\alpha^{(2^m+1)t}\right]^r\} \quad (6)$$

단, $N=2^n-1$, $r(1 \le r < 2^m-1)$은 $\gcd(r, 2^m-1)=1$을 만족하는 정수, $GF(2^n)=\{\gamma_i \mid 0 \le i \le 2^n-1\}$이고 $GF(2^m)=\{\eta_j \mid 0 \le j \le 2^m-1\}$이다. $\gamma_i=0$로 두면 식 (6)은 식 (4)의 형태가 되므로 Zeng 수열군은 No 수열군을 포함한다.

다음은 수열들의 상호상관관계를 계산할 때 유용한 정리이다.

<정리 3 [12]> 임의의 $\delta \in GF(2^n)$에 대하여 다음이 성립한다.

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

n이 m의 배수인 자연수 m, n에 대하여, 주기가 2^n-1인 수열로 구성된 수열군 $\mathbb{S}$가 다음과 같다고 하자.

$$\mathbb{S} := \{\{s_i(t) \mid 0 \le t \le 2^n-2\} \mid 0 \le i \le 2^m-1\} \quad (8)$$

이와 같은 수열군 $\mathbb{S}$의 상호상관관계 함수(correlation function)는 $R_{i,j}(\cdot)$는 다음과 같이 정의된다.

<정의 4 [9]> $0 \le i, j \le 2^m-1$에 대해 수열군 $\mathbb{S}$에서 i번째 수열과 j번째 수열의 상호상관관계 함수는 다음과 같다.

$$R_{i,j}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_i(t+\tau)-s_j(t)} \quad (0 \le \tau \le 2^n-2) \quad (9)$$

위에서 살펴본 수열들의 상호상관관계 함숫값을 구하면 GMW 수열은

$$R(\tau) = \begin{cases} 2^n-1, & \text{if } \tau \equiv 0 \pmod{2^n-1} \\ -1 & , otherwise \end{cases} \quad (10)$$

이고 No 수열의 상호상관관계 함숫값은

$$R(\tau) \in \{-2^m-1, -1, 2^m-1\} \quad (11)$$

이고 Kasami 수열의 상호상관관계 함숫값은

$$R(\tau) \in \{-2^m-1, -1, -1+2^m\} \quad (12)$$

이다. Zeng이 제안한 수열군은

$$R(\tau) \in \{-2^m-1, -1, 2^m-1, 2\cdot 2^m-1, 3\cdot 2^m-1\} \quad (13)$$

으로 상호상관관계 함숫값이 다소 커졌으나 수열군의 개수가 크고 선형복잡도가 높기 때문에 유용하게 활용될 수 있다[8].

III. 확장 Zeng 수열

이 절에서는 Zeng이 제안한 수열보다 수열군의 크기가 크고 선형복잡도가 높은 확장 Zeng 수열군을 제안하고, 그 상호상관 함숫값을 분석한다.

m은 2이상의 자연수이고 $n=2m$, $Q=2^m+1$이라 하자. u와 v는 $u-v=2$인 음이 아닌 정수이고 $N=2^n-1$이라 하자. α는 $GF(2^n)$의 원시원소이고 $\beta=\alpha^Q$이라 하면 $\beta^{2^m-1}=(\alpha^Q)^{2^m-1}=\alpha^{2^{2m}-1}=1$이므로 β는 $GF(2^m)$의

원시원소이다. 주기 N인 $2^n \times 2^m$ 개로 구성된 수열군 $\mathbb{S}$를 다음과 같이 정의한다.

$$\mathbb{S} = \{\{s_{i,j}(t) \mid 0 \le t \le N-1\} \mid 0 \le i \le 2^n-1, 0 \le j \le 2^m-1\}$$

$$s_{i,j}(t) := Tr_1^m \left\{ \left[Tr_m^n\left(\alpha^{2t} + \gamma_i \alpha^{(2^m u - v)t}\right) + \eta_j \beta^t \right]^r \right\} \quad (14)$$

여기서 $r(1 \le r < 2^m-1)$은 $\gcd(r, 2^m-1) = 1$ 을 만족하는 정수이고 $GF(2^n) = \{\gamma_i \mid 0 \le i \le 2^n-1\}$, $GF(2^m) = \{\eta_j \mid 0 \le j \le 2^m-1\}$이다. 이 수열군을 확장 Zeng 수열군(extended Zeng sequences)이라 하자.

$\gamma_i = 0$이거나 $u = 2$이고 $v = 0$이면 수열군 $\mathbb{S}$는 No 수열군이다. 그리고 $u = 3, v = 1$이면 Zeng이 제안한 수열군이다. 또한 $\gamma_i = 0, \eta_j = 0$이고 $r = 1$이면 m-수열이며 $\gamma_i = 0, \eta_j = 0$이면 GMW 수열군이다. 따라서 확장 Zeng 수열군 $\mathbb{S}$는 m-수열, GMW 수열, No 수열, Zeng 수열을 모두 포함하는 수열군이다.

주기가 N인 두 이진수열 $s_{i,j}(t)$와 $s_{p,q}(t)$의 상호상관함수(cross-correlation function) $R_{ij,pq}(\tau)$는 다음과 같이 정의된다.

$$R_{ij,pq}(\tau) = \sum_{t=0}^{N-1} (-1)^{s_{ij}(t+\tau) - s_{pq}(t)} \quad (15)$$

(단, $0 \le \tau \le N-1$)

확장 Zeng 수열군 $\mathbb{S}$의 상호상관 함숫값을 계산하기 위해 $\alpha^{(2^m u - v)Q} = \left\{(\alpha^Q)^{2^m}\right\}^u \cdot (\alpha^Q)^{-v} = (\alpha^Q)^u \cdot (\alpha^Q)^{-v} = \alpha^{(u-v)Q}$를 이용하면 다음이 성립한다.

<보조정리 5> α가 $GF(2^n)$의 원시원소이고 $\beta = \alpha^Q$이면 $\alpha^{(2^m u - v)Q} = \alpha^{(u-v)Q}$ 이다.

수열 $s_{i,j}(t)$를 좀 더 쉽게 분석하기 위해 t를 Q진수로 표현하자. 즉, $t = t_1 \cdot Q + t_2$ $(0 \le t_1 \le 2^m-2, 0 \le t_2 \le Q-1)$라 하고 t_1의 값으로 행, t_2의 값으로 열의 위치를 정하자. 그러면 주기가 2^n-1인 수열 $s_{i,j}(t)$는 주기가 2^m-1인 수열 2^m+1개로 나타낼 수 있다. 보조정리 5에 의해 $\alpha^{(2^m u - v)Q} = \beta^2$이고 $\alpha^{Q^2} = \beta^Q = \beta^{2^m} \cdot \beta = \beta^2$ 임을 이용하면

$$\begin{aligned} &Tr_m^n\left(\alpha^{2t} + \gamma_i \alpha^{(2^m u - v)t}\right) + \eta_j \beta^t \\ &= Tr_m^n\left(\alpha^{2(t_1 Q + t_2)} + \gamma_i \alpha^{(2^m u - v)(t_1 Q + t_2)}\right) + \eta_j \beta^{t_1 Q + t_2} \\ &= \beta^{2t_1} \left\{ Tr_m^n\left(\alpha^{2t_2} + \gamma_i \alpha^{(2^m u - v)t_2}\right) + \eta_j \beta^{t_2} \right\} \end{aligned} \quad (16)$$

가 되므로 식 (14)는

$$s_{i,j}(t) = Tr_1^m \left\{ \left[\beta^{2t_1} \left\{ Tr_m^n\left(\alpha^{2t_2} + \gamma_i \alpha^{(2^m u - v)t_2}\right) + \eta_j \beta^{t_2} \right\} \right]^r \right\} \quad (17)$$

가 된다. 그러면

$$\begin{aligned} &s_{i,j}(t+\tau) - s_{p,q}(t) \\ &= Tr_1^m \left[\beta^{2rt_1} \left\{ \left[Tr_m^n\left(\alpha^{2(t_2+\tau)} + \gamma_i \alpha^{(2^m u - v)(t_2+\tau)}\right) + \eta_j \beta^{(t_2+\tau)} \right]^r \right.\right. \\ &\quad \left.\left. - \left[Tr_m^n\left(\alpha^{2t_2} + \gamma_p \alpha^{(2^m u - v)t_2}\right) + \eta_q \beta^{t_2} \right]^r \right\} \Big] \end{aligned} \quad (18)$$

이고,

$$s_{i,j}(t+\tau) - s_{p,q}(t) = Tr_1^m \left\{ \beta^{2rt_1} f(t_2, \tau) \right\},$$

$$\begin{aligned} f(t_2, \tau) = &\left[Tr_m^n\left(\alpha^{2(t_2+\tau)} + \gamma_i \alpha^{(2^m u - v)(t_2+\tau)}\right) + \eta_j \beta^{t_2+\tau} \right]^r \\ &- \left[Tr_m^n\left(\alpha^{2t_2} + \gamma_p \alpha^{(2^m u - v)t_2}\right) + \eta_q \beta^{t_2} \right]^r \end{aligned} \quad (19)$$

로 나타낼 수 있다. 이제

$$N(\tau) = |\{t_2 \mid f(t_2, \tau) = 0, 0 \le t_2 \le Q-1\}| \quad (20)$$

라 정의하고 정리 3과 식 (19)를 이용하면 상호상관 함숫값 $R_{ij,pq}(\tau)$는

$$R_{ij,pq}(\tau)=\sum_{t=0}^{N-1}(-1)^{s_{i,j}(t+\tau)-s_{p,q}(t)} \quad (21)$$
$$=\sum_{t_2=0}^{Q-1}\sum_{t_1=0}^{2^m-2}(-1)^{Tr_1^m\{\beta^{2t_1}f(t_2,\tau)\}}$$
$$=\sum_{t_2=0}^{Q-1}\left(\sum_{x\in GF(2^m)}(-1)^{Tr_1^m\{\beta^{2t_1}f(t_2,\tau)\}}-1\right)$$
$$=2^mN(\tau)-Q$$

이 된다. $N(\tau)$는 $f(t_2,\tau)=0$이 되는 t_2의 개수이므로 $s_{i,j}(t+\tau)-s_{p,q}(t)$를 $(2^m-1)\times(2^m+1)$ 배열로 표현했을 때 모든 성분이 0인 열의 개수이다.

$N(\tau)$의 값을 구하기 위하여 $\alpha^{2\tau}-1=A$, $\gamma_i\alpha^{(u\cdot 2^m-v)\tau}-\gamma_p=B$, $\eta_j\alpha^{(2^m+1)\tau}-\eta_q=C$라 하고

$$F(t_2,\tau)=Tr_m^n\left(A\alpha^{2t_2}+B\alpha^{(u\cdot 2^m-v)t_2}\right)+C\alpha^{(2^m+1)t_2} \quad (22)$$

라 하면 $\gcd(r,2^m-1)=1$이므로 $f(t_2,\tau)=0$일 필요충분조건은 $F(t_2,\tau)=0$이다. 식 (22)에서 α^{t_2}를 x로 바꾼 식을 $g(x)$라 하면

$$x^{(u\cdot 2^m-v)2^m}=x^{u-v\cdot 2^m}$$

이므로 다음이 성립한다.

$$g(x)=Tr_m^n\left(Ax^2+Bx^{(u\cdot 2^m-v)}\right)+Cx^Q \quad (23)$$
$$=Ax^2+Bx^{u\cdot 2^m-v}+x^QA^{2^m}x^{2^{m+1}}$$
$$+B^{2^m}x^{(u\cdot 2^m-v)2^m}+C$$
$$=Ax^2+Bx^{u\cdot 2^m-v}+A^{2^m}x^{2^{m+1}}$$
$$+B^{2^m}x^{u-v\cdot 2^m}+Cx^Q$$
$$=0$$

식 (23)에서 $x^{2^m-1}=y$라 하고 식 (23)의 양변을 x^2으로 나누어 정리하면

$$A+By^u+A^{2^m}y^2+B^{2^m}y^{-v}+Cy=0 \quad (24)$$

이 되고 식 (24)의 양변에 y^v를 곱하면

$$B^{2^m}+Ay^v+Cy^{v+1}+A^{2^m}y^{v+2}+By^{u+v}=0 \quad (25)$$

이 된다. 식 (25)는 기껏해야 $u+v$개의 근을 갖는다. 따라서 다음 정리를 얻는다.

<정리 6> 수열군 $\mathbb{S}$에 포함되는 임의의 두 이진 수열 $s_{i,j}(t)$, $s_{p,q}(t)$에 대하여

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

이 성립한다.

<예제 7> $\gamma_i=\gamma_p=0$인 경우 $u=3$, $v=1$, $\eta_j=1$, $\eta_q=\beta^2$, $p(x)=x^6+x^5+1$, $\beta=\alpha^9$이면 $\beta^3=\beta+1$을 만족한다. $r=5$인 수열군에서 상호상관 함숫값을 계산해보자. 이 경우 수열은 No 수열의 형태가 된다.

$$s_{i,j}(t)=Tr_1^3\left\{\left[Tr_3^6(\alpha^{2t})+\beta^{(2\cdot 2^3-1)t}\right]^5\right\}$$
$$s_{p,q}(t)=Tr_1^3\left\{\left[Tr_3^6(\alpha^{2t})+\beta^2\beta^{(2\cdot 2^3-1)t}\right]^5\right\}$$

$$s_{i,j}(t)\qquad s_{p,q}(t)$$
$$\begin{pmatrix}1&1&1&0&1&1&0&0&1\\1&1&1&0&1&0&0&1&1\\1&1&1&0&1&0&0&1&1\\0&0&0&0&0&1&0&1&0\\1&1&1&0&1&1&0&0&1\\0&0&0&0&0&1&0&1&0\\0&0&0&0&0&0&0&0&0\end{pmatrix}\quad\begin{pmatrix}1&0&0&1&1&1&0&1&0\\1&0&0&1&0&1&1&0&0\\0&0&1&0&0&0&1&0&0\\1&0&1&1&1&1&1&1&0\\0&0&1&0&1&0&0&1&0\\0&0&0&0&1&0&1&1&0\\1&0&1&1&0&1&0&0&0\end{pmatrix}$$

τ의 값을 0부터 2^n-2까지 차례대로 변화시키면서 이 수열의 상호상관 함숫값을 구해보면

$$R_{ij,pq}(\tau)=$$
$$\begin{pmatrix}-9&7&-1&-9&7&7&7&7&7\\-1&7&7&7&7&7&-9&-1&7\\-9&-9&7&-9&7&-1&-9&7&-9\\-9&-9&7&-1&7&7&7&7&-9\\7&-1&7&-9&7&7&-9&7&-1\\7&-9&7&7&7&7&-1&7&-9\\-9&-9&7&-9&-1&7&-9&7&-9\end{pmatrix}$$

이므로 이 수열의 상호상관 함숫값은 $\{-9,-1,7\}$의 원소임을 알 수 있다.

<예제 8> $n=6$, $m=3$, $p(x)=x^6+x+1$이라 하면 $Q=9$이다. $u=3$, $v=1$이고 $\beta=\alpha^9$이면 $\beta^3=\beta^2+1$을 만족한다.

(a) $\gamma_i=\alpha$, $\eta_j=\beta$, $\gamma_p=\alpha^2$, $\eta_q=\beta^2$이라 하자. 주어진 조건하에서 생성되는 주기 63인 두 수열 $s_{i,j}(t)$와 $s_{p,q}(t)$를 7×9배열로 나타내면 다음과 같다.

$$s_{i,j}(t)=Tr_1^3\left\{\left[Tr_3^6(\alpha^{2t}+\alpha^2\cdot\alpha^{23t})+\beta\cdot\beta^t\right]^3\right\}$$

$$s_{p,q}(t) = Tr_1^3\left\{\left[Tr_3^6(\alpha^{2t}+\alpha^2\cdot\alpha^{23t})+\beta^2\cdot\beta^t\right]^3\right\}$$

$$\underset{s_{i,j}(t)}{\begin{pmatrix}0&1&1&1&0&1&1&0&0\\1&0&0&0&0&1&0&1&0\\0&0&0&0&1&0&0&0&0\\1&1&1&1&0&0&1&1&0\\1&0&0&0&1&1&0&1&0\\1&1&1&1&0&1&1&0&0\\0&1&1&1&1&1&1&0&0\end{pmatrix}} \qquad \underset{s_{p,q}(t)}{\begin{pmatrix}0&0&1&1&1&1&1&0&0\\1&1&0&1&0&0&0&0&1\\1&1&0&0&0&1&0&0&0\\1&1&1&0&1&1&1&0&1\\0&0&0&1&0&1&0&0&1\\0&0&1&0&1&0&1&0&1\\1&1&1&1&0&1&0&0&1\end{pmatrix}}$$

τ의 값을 0부터 2^n-2까지 차례대로 변화시키면서 상호상관 함숫값을 구하면 다음과 같다.

$$R_{ij,pq}(\tau)=\begin{pmatrix}7&7&7&-9&7&-1&-9&-9&-1\\-9&7&7&7&-1&-9&-9&-1&7\\-1&-1&-9&-9&-9&-1&15&7&-9\\-9&7&-9&-1&-1&-9&-1&-9&-9\\7&15&7&7&-1&7&-1&-1&-9\\-9&15&-9&-1&-1&7&-9&7&-1\\7&7&-1&-1&-1&-1&7&-1&15\end{pmatrix}$$

이 수열의 상호상관 함숫값은 $\{-9,-1,7,15\}$의 원소이다.

(b) $\gamma_i=\alpha$, $\eta_j=\beta$, $\gamma_p=\alpha^2$, $\eta_q=\beta^3$이라 하자. 주어진 조건하에서 생성되는 주기 63인 두 수열 $s_{i,j}(t)$와 $s_{p,q}(t)$를 7×9 배열로 나타내면 다음과 같다.

$$s_{i,j}(t) = Tr_1^3\left\{\left[Tr_3^6(\alpha^{2t}+\alpha^2\cdot\alpha^{23t})+\beta\cdot\beta^t\right]^3\right\}$$
$$s_{p,q}(t) = Tr_1^3\left\{\left[Tr_3^6(\alpha^{2t}+\alpha^2\cdot\alpha^{23t})+\beta^3\cdot\beta^t\right]^3\right\}$$

$$\underset{s_{i,j}(t)}{\begin{pmatrix}0&1&1&1&0&1&1&0&0\\1&0&0&0&0&1&0&1&0\\0&0&0&0&1&0&0&0&0\\1&1&1&1&0&0&1&1&0\\1&0&0&0&1&1&0&1&0\\1&1&1&1&0&1&1&0&0\\0&1&1&1&1&1&1&0&0\end{pmatrix}} \qquad \underset{s_{p,q}(t)}{\begin{pmatrix}1&0&1&1&1&1&1&0&1&1\\1&0&1&0&0&1&1&0&1\\0&0&1&1&1&1&0&0&1\\0&0&0&1&1&0&1&1&0\\1&0&0&1&1&0&1&0&0\\0&0&1&0&0&1&1&1&1\\1&0&0&0&0&0&0&1&0\end{pmatrix}}$$

$$R_{ij,pq}(\tau)=\begin{pmatrix}-9&-1&-9&-9&-9&7&-1&15&-9\\-9&-9&-9&-1&7&-1&-1&-1&-9\\7&7&-9&-9&-1&-9&-1&23&23\\-1&-9&7&-1&-9&7&-9&-1&-1\\-1&-1&23&-1&-1&-1&-1&23&-1\\7&7&-9&-9&7&-9&7&-1&-9\\-1&-1&-1&23&-1&-1&-1&-1&-1\end{pmatrix}$$

이 수열의 상호상관 함숫값은 $\{-9,-1,7,15,23\}$의 원소이다.

Ⅳ. 결 론

CDMA와 같은 무선 통신 시스템에서 대역확산 기술로 사용되는 확산수열은 수열군의 개수가 많고 선형복잡도가 높은 것이 바람직하다. 그러나 Welch의 하한 관점에서 위와 같이 바람직한 수열을 얻기 위해서는 상호상관 함숫값이 어느 정도 높아지는 것은 불가피하다. 본 논문에서는 수열군의 개수가 크고 선형복잡도가 높은 확장 Zeng 수열군을 제안하였고 그 상호상관 함숫값을 분석하였다. 이러한 수열군은 m-수열, GMW 수열, No 수열, Zeng 수열을 모두 포함한다.

참고 문헌

[1] L.D. Baumert, “Cyclic Difference Sets (Lecture Notes in Mathematics)”, New York : Springer-Verlag, Vol. 182, 1971.

[2] S.W. Golomb, “Shift-Register Sequences”, Revised Edition, Aegean Park Press, May, 1982.

[3] T. Kasami, “Weight distribution formula for some class of cyclic codes”, Coordinated Science Laboratory, University of Illinois, Urbana, Tech. Rep. R-285 (AD632574), 1966.

[4] L.R. Welch, “Lower bounds on the maximum cross correlation of signals”, IEEE Trans. Inf. Theory, Vol. IT-20, No. 3, pp. 397-399, 1974.

[5] 이규안, “과학적 조사기법에 적합한 컴퓨터 속기의 역할에 관한 연구”, 한국전자통신학회논문지, 6권, 4호, pp. 533-537, 2011.

[6] 서우석, 전문석, “스마트그리드 전력망과정보통신망 융합 보안 방향”, 한국전자통신학회논문지, 5권, 5호, pp. 477-486, 2010.

[7] 임세정, 김광준, 강태근 ”클라이언트 가상화를 이용한 중요정보 보호“, 한국전자통신학회논문지, 6권, 1호, pp. 111-117, 2011.

[8] F. Zeng and Z. Zhang, “Binary sequences with large family size and high linear complexity for spread spectrum communication systems”, 2010 2nd Inter. Conf. on Signal Processing Systems (ICSPS), pp. 48-51, 2010.

[9] S.W. Golomb and G. Gong, “Signal design for good correlation for wireless communication, Cryptography, and Radar”, Cambridge University Press, 2005.
[10] R.A. Scholtz and L. Welch, “GMW sequences”, IEEE Trans. Inform. Theory, Vol. IT-30, No. 3, pp. 548-553, 1984.
[11] J.S. No, “A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span”, Ph.D. dissertation, Univ. Southern California, Los Angeles, CA, May, 1988.
[12] R.J. McEliece, Finite fields for computer scientists and engineers, Kluwer Academic Publishers, 1987.

저자 소개

김한두(Han-Doo Kim)

1982년 2월 고려대학교 수학과 졸업 (이학사)
1984년 2월 고려대학교 대학원 수학과 졸업(이학석사)
1988년 2월 고려대학교 대학원 수학과 졸업(이학박사)
1989년~현재 인제대학교 컴퓨터응용과학부 교수
※ 관심분야 : 전산수학, 셀룰라 오토마타론

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 응용수학과 정교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호

권민정(Min-Jeong Kwon)

1997년 2월 부산대학교 수학교육과 졸업 (이학사)
2002년 8월 부산대학교 교육대학원 수학과 졸업(교육학석사)
2007년~현재 부경대학교 응용수학과 박사과정
※ 관심분야 : 셀룰라 오토마타론, 정보보호

안현주(Hyun-Ju An)

2010년~현재 부경대학교 응용수학과 석사과정
※ 관심분야 : 셀룰라 오토마타론, 정보보호