두 개의 m-수열에 의해 생성된 새로운 비선형 이진수열군

최언숙* · 조성진** · 김한두*** · 권숙희** · 권민정** · 김진경**

*동명대학교 · **부경대학교 · ***인제대학교

A New Family of Nonlinear Binary Sequences Generated by Two m-Sequences

Un-sook Choi* · Sung-jin Cho**· Han-doo Kim***

Sook-hee Kwon** · Min-jeong Kwon** · Jin-gyoung

*Tongmyoung Univ. · **Pukyoung National Univ. · ***Inje Univ.

E-mail : choie@tu.ac.kr

요 약

$n=2k$이고, $2s$가 k의 약수이며 홀수인 i에 대하여 주기가 2^n-1인 m-수열과 새로운 decimation $d=2^{k-1}(2^{s+1}-2^k+2^{k(i+1)}-2^{ki}-1)/(2^s-1)$인에 의해 생성된 수열의 합으로 생성된 새로운 이진수열군에 대하여 그 상관관계를 분석한다. 제안된 수열은 Rosendahl의 수열과 Dobbertin의 수열을 포함하는 확장된 수열이다.

ABSTRACT

In this paper we propose a new family of nonlinear binary sequences generated by m-sequences for decimations $d=2^{k-1}(2^{s+1}-2^k+\ +2^{k(i+1)}-2^{ki}-1)/(2^s-1)$ where $n=2k$, i is odd and s is such that $2s$ divides k. And we analyze the cross-correlation function between two m-sequences for new decimations d. Proposed sequences is extension of Rosendahl's sequnces and Dobbertin's sequences.

키워드

상호상관관계, decimation, m수열, 비선형 이진수열, 유한체

Ⅰ. 서 론

고속 통신을 위하여 현대의 무선통신은 점차 고주파 대역을 이용하는 방향으로 나아가고 있으며 고주파 대역의 특성상 셀의 크기는 점점 작아져 마이크로셀룰러 환경이 되고 있다. 이러한 환경에 적합한 시스템으로 부호 분할 다원 접속(CDMA) 시스템에서 링크 상에서 지연 수를 칩 내로 제한한 준 동기 분호 분할 다원 접속(Quasi Synchronous CDMA: QS-CDMA) 시스템이 제안되었다. 이러한 준 동기 부호 분할 다원 접속 시스템이 효율적인 성능을 내기 위해서는 낮은 상관관계를 갖는 수열 군을 사용하는 것이 필수적이다[1,2].

적당한 정수 n에 대하여 자기 상관 관계(auto-correlation)값으로 -1또는 2^n-1을 갖는 주기가 2^n-1인 균형이 잡힌 이진 수열(balanced binary sequences)[3]은 대역확산 통신 시스템(spread-spectrum communication system)에서 많이 응용되고 있다[4]. 이러한 이진수열은 1970년대부터 많은 연구자들에 의해 연구되어왔다. 이러한 수열은 트레이스 함수를 사용하여 제안되었으며 잘 알려진 대표적인 수열군은 m-수열, GMW 수열, Kasami 수열, No 수열, Gold 계열의 수열이 있다. 이 밖에도 트레이스를 이용한 여러 수열들이 연구되었다[5-10]. 본 논문에서는 두 개의 m-수열에 의해 생성되는 Gold 계열의 새로운 이진 수열군을 제안하고 그 수열의 상호상관관계를 분석하여 제안된 수열의 4값-상호상관관계를 갖는 우수한 비선형 이진수열임을 보인다.

Ⅱ. 연구배경 및 기존 연구

트레이스(Trace)함수는 유한체로부터 부분체로의 선형매핑인데, 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 가진 유한체라 하고, $GF(2^n)^* = GF(2^n)/\{0\}$라 하자. 1보다 큰 정수 k에 대하여 $n=km$라 하고 차수가 n인 원시다항식 $f(x)$의 원시근을 $\alpha(\in GF(2^n))$라 하자. $f(x)$를 차수가 n인 원시다항식이라 하자. 본 논문에서 사용되는 트레이스 함수 $Tr_1^n : GF(2^n) \rightarrow GF(2)$는 다음과 같다[11].

$$Tr_1^n(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}$$

여기서 x는 $GF(2^n)$의 원소이다.

다음은 함수 $Tr_1^n : GF(2^n) \rightarrow GF(2)$의 성질이다.

$GF(2^n)$의 원소 x, y에 대하여

(a) $Tr_1^n(x+y) = Tr_1^n(x) + Tr_1^n(y)$.

(b) Tr_1^n는 전사함수이다.

(c) $Tr_1^n(x^{2^i}) = Tr_1^n(x)$.

(g) $Tr_m^n(x) = 0$(또는 $Tr_m^n(x) = 1$)를 만족하는 x는 2^{n-1} 개 이다.

주기가 $2^n - 1$인 두 수열 $u(t)$와 $v(t)$사이의 상호상관관계(cross-correlation) 함수 $C_d(\tau)$는 $\tau = 0, 1, \cdots, 2^n - 2$에 대하여 다음과 같이 정의된다[9].

$$C_d(\tau) = \sum_{t=0}^{2^n-2} (-1)^{u(t+\tau)+v(t)} \quad (1)$$

예를 들어 $u(t)$와 $v(t)$가 $u(t) = 1001011$, $v(t) = 0010111$라 하자. $\tau = 2$일 때, $u(t+2) = 0101110$이므로, $C_d(2) = 1-1-1-1+1+1-1 = -1$이다.

표 1은 지금까지 알려진 우수한 상호상관관계를 갖는 이진수열군이다. 표 1의 수열은 유한체와 그 부분체를 이용하여 이진 수열을 발생시키는 함수를 구성하였다. 이때 $n = 2m$이므로 트레이스 함수 $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$는 다음과 같다.

$$Tr_m^n(x) = x + x^{2^m}$$

그리고 γ의 값에 따라 주어진 수열을 $s_i(t), s_j(t)$라고 할 때, 상호상관관계는 다음과 같다.

$$C_{ij}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_i(t+\tau)+s_j(t)}$$

표 1에서 m-수열을 제외한 모든 수열의 상호상관관계값은 3개의 값을 가지며 이와 같은 수열을 최적의 상호상관관계를 갖는다고 한다.

표 1. 최적의 상호상관관계를 갖는 이진수열

수열	함수	상호상관관계
m-수열	$Tr_1^n(\alpha^t)$	-1
GMW 수열	$Tr_1^m([Tr_m^n(\alpha^t)]^r)$ $n = 2m, \gcd(r, 2^m-1) = 1$	$-2^m-1, -1, 2^m-1$
Kasami 수열	$Tr_1^n(\alpha^{2t}) + Tr_1^m(\gamma_i \alpha^{Q \cdot t})$ $n = 2m, Q = 2^m+1,$ $\gamma_i \in GF(2^m),$	$-2^m-1, -1, 2^m-1$
No 수열	$Tr_1^m\{[Tr_m^n(\alpha^{2t}) + \gamma_i \alpha^{Q \cdot t}]^r\}$ $n = 2m, \gcd(2^m-1, r) = 1,$ $Q = 2^m+1$	$-2^m-1, -1, 2^m-1$
	$\sum_{a \in I} Tr_1^m\{[G_i(\alpha^t)]^{ar}\}$ $G_i(\alpha^t) : Tr_m^n(\alpha^{2t} + u_i \alpha^{2^{m+1}t}) + v_i \beta^t$ $\gcd(r, 2^m-1) = 1$ $u_i \in GF(2^n), v_i \in GF(2^m)$	$-2^m-1, -1, 2^m-1$

그림 1은 표 1의 수열중 m-수열과 GMW수열, Kasami수열, No수열과의 관계를 나타낸다.

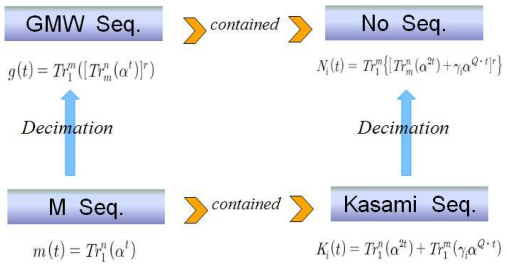

그림 1. 의사불규칙 수열 사이의 관계

표 1에 대한 이진수열의 확장으로 비선형 확장 이진수열은 Zeng등[12]에 의해 제안된 수열(식 (2))과 Choi등[13]에 의해 제안된 수열(식 (3))이 있으며 다음과 같다.

$$Z_i(t) = Tr_1^m\{[Tr_m^n(\alpha^{(u+v)t} + \gamma_i \alpha^{(u \cdot 2^m+v)t})]^r\} \quad (2)$$

$$s_{ij}(t) = Tr_1^m\{[Tr_m^n(\alpha^{(u+v)t} + \gamma_i \alpha^{(u2^m+v)t}) + \eta j^{2^{m-1}(u+v)t}]^r\} \quad (3)$$

확장된 비선형이진수열은 u와 v값에 따라 상호상관관계의 값이 여러 가지 값을 갖는데 u와 v 값에 따른 비선형 확장이진수열의 상호상관관계는 다음과 같다[13].

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

부분체를 이용하여 제안된 수열과 다른 형태로 최적의 상호상관관계를 갖는 이진수열이 Gold를 비롯한 많은 연구자들에 의해 제안되었다[9, 10, 14]. $u(t)$와 $v(t)$를 주기 2^n-1인 두 m-수열이라 하고 $u(t)$를 다음과 같이 정의하자.

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

여기서 α는 $GF(2^n)$의 한 원시원소이다.

또 하나의 m-수열 $v(t)$는 주기가 같으므로 일반성을 잃지 않고 $u(t)$를 이용하여 다음과 같이 표현할 수 있다.

$$v(t)=u(dt) \tag{5}$$

이때, d를 데시메이션(decimation)이라고 하며 $1\le d\le 2^n-2$, $\gcd(d,2^n-1)=1$를 만족한다. 표 2는 Gold 계열의 이진수열에서 3값-상호상관계를 갖는 경우이고, 표 3은 Gold 계열의 이진수열로 4값-상호상관관계를 갖는 경우의 데시메이션값이다[14].

표 2. 3값-상호상관관계를 갖는 Gold 계열의 이진수열의 여러 가지 데시메이션

d(데시메이션)	관련 조건
2^k+1	$n/\gcd(n,k)$: 홀수
$2^{2k}-2^k+1$	$n/\gcd(n,k)$: 홀수
$2^{n/2}+2^{(n+2)/4}+1$	$n\equiv 2 \pmod 4$
$2^{n/2+1}+3$	$n\equiv 2 \pmod 4$
$2^{(n-1)/2}+3$	n: 홀수
$2^{(n-1)/2}+2^{(n-1)/4}-1$	$n\equiv 1 \pmod 4$
$2^{(n-1)/2}+2^{(3n-1)/4}-1$	$n\equiv 3 \pmod 4$

표 3. 4값-상호상관관계를 갖는 Gold 계열의 이진수열의 여러 가지 데시메이션

d(데시메이션)	관련 조건
$2^{n/2+1}-1$	$n\equiv 0 \pmod 4$
$(2^{n/2}+1)(2^{n/4}-1)+2$	$n\equiv 0 \pmod 4$
$\sum_{i=0}^{n/2}2^{im}$	$n\equiv 0 \pmod 4$ $0<m<n,\ \gcd(m,n)=1$
$\frac{2^{k-1}}{2^s-1}(2^{2k}+2^{s+1}-2^{k+1}-1)$	$n=2k,\ 2s\mid k$

Ⅲ. 수열의 4값-상호상관관계를 갖는 이진수열

정리 1. $n=2k$라 하고 $2s|k$이며 i가 홀수일 때 식 (5)에서의 d를 다음과 같이 정의하자.

$$d=\frac{2^{k-1}}{2^s-1}(2^{s+1}-2^k+2^{k(i+1)}-2^{ki}-1) \tag{6}$$

그러면 다음을 만족한다.

① $d\equiv 1 \pmod{2^k-1}$

② $d\equiv \frac{2^{ki}-2^s}{2^s-1} \pmod{2^k+1}$

③ $\gcd(d,2^n-1)=1$

정리 1의 결과로 식 (4)의 $u(t)$와 식 (5)의 $v(t)$에 식 (6)에서 정의된 d를 이용하여 얻은 수열의 상호상관관계를 구해보자. 두 m-수열 $u(t), v(t)$의 상호상관관계 $C_d(\tau)$는 식 (1)에 따라 다음과 같다.

$$\begin{aligned}C_d(\tau)&=\sum_{t=0}^{2^n-2}(-1)^{u(t+\tau)+v(t)}\\&=\sum_{t=0}^{2^n-2}(-1)^{Tr_1^n(w^{t+\tau}+w^{dt})}\\&=\sum_{x\in GF(2^n)^*}(-1)^{Tr_1^n(yx+x^d)}\\&=\sum_{i=0}^{2^k-2}\sum_{j=0}^{2^k}(-1)^{Tr_1^n(y\alpha^i\beta^j+\alpha^{di}\beta^{dj})}\\&=\sum_{i=0}^{2^k-2}\sum_{j=0}^{2^k}(-1)^{Tr_1^n(y\alpha^i\beta^j+\alpha^i\beta^{\frac{2^{ki}-2^s}{2^s-1}j})}\end{aligned}$$

여기서 $x:=w^t, y=w^\tau$이고 x는 $GF(2^n)$의 원소로 $x=\alpha^i\beta^j$로 유일하게 표현할 수 있다. 이때 $0\le i\le 2^k-2$, $0\le j\le 2^k$ 이고 α는 $GF(2^k)$의 원시원소이고 β는 $GF(2^n)$에서 1의 2^k+1제곱근의 원시근이다. 즉 $\beta^{2^k+1}=1$이다. 따라서 $C_d(\tau)$는 다음과 같다.

$$\begin{aligned}C_d(\tau)&=\sum_{i=0}^{2^k-2}\sum_{j=0}^{2^k}(-1)^{Tr_1^k(\alpha^i(y\beta^j+\beta^{\frac{2^k-2^s}{2^s-1}j}+y^{2^k}\beta^{-j}+\beta^{-\frac{2^k-2^s}{2^s-1}j}))}\\&=-1-2^k+\sum_{j=0}\sum_{z\in GF(2^k)}(-1)^{Tr_1^k(z(y\beta^j+\beta^{\frac{2^k-2^s}{2^s-1}j}+y^{2^k}\beta^{-j}+\beta^{-\frac{2^k-2^s}{2^s-1}j}))}\\&=-1+2^k(N(y)-1)\end{aligned} \tag{7}$$

여기서 $N(y)$는 $x:=\beta^j$라 두었을 때 다음 연립방정식 (8)과 (9)를 만족하는 해의 개수이다.

$$yx+x^{\frac{2^{ki}-2^s}{2^s-1}}+y^{2^k}x^{-1}+x^{-\frac{2^{ki}-2^s}{2^s-1}}=0 \tag{8}$$

$$x^{2^k+1}=1 \tag{9}$$

$\gcd(2^s-1,2^k+1)=1$이므로 x를 x^{2^s-1}로 바꾸어도 $N(y)$는 변화가 없다. 식 (9)를 이용하면 식 (8)은 다음과 같다.

$$yx^{-2}+x^{-2(2^s+1)}+y^{2^k}x^{-2\cdot 2^s}+1=0 \qquad (10)$$

식 (10)의 양변에 $x^{2(2^s+1)}$을 곱하고 x를 $\sqrt{x}$로 바꾸어도 $N(y)$는 변화없다. 따라서 $N(y)$는 다음 방정식의 해의 개수이다.

$$\begin{cases} x^{2^s+1}+yx^{2^s}+y^{2^k}x+1=0 \\ x^{2^k+1}=1 \end{cases} \qquad (11)$$

$y\in GF(2^n)\setminus\{0\}$일 때, 방정식 (11)은 y값에 따라 $GF(2^n)$에서 $0, 1, 2, 2^{\gcd(s,k)}+1$개의 해를 갖는다[].

식 (6) 의 d에서 $\gcd(k,s)=1$므로 $N(y)=0,1,2,3$의 값을 갖는다. 따라서 식 (7)에 의하여 주어진 수열의 $C_d(\tau)$는 다음과 같다.

$$C_d(\tau)\in\{-1-2^k,-1,-1+2^k,-1+2^{k+1}\} \qquad (12)$$

따라서 $n=2k$이고 $2s|k$이며 i가 홀수이며 $d=\frac{2^{k-1}}{2^s-1}(2^{s+1}-2^k+2^{k(i+1)}-2^{ki}-1)$이면, m-수열 $u(t)=Tr_1^n(w^t)$에 대하여 이진수열 $u(t)+u(dt)$ 은 4-값 상호상관관계를 갖는 이진수열이다.

Ⅳ. 결 론 및 향후 연구방향

본 논문에서는 4-값 상호상관관계를 갖는 새로운 이진수열군을 생성하였다. 제안된 수열은 Niho 형태의 수열이며 $i=1$일 때 Rosendahl이 제안한 이진수열군이 된다. 향후 연구방향은 제안된 이진수열의 τ값에 따라 결정되는 상호상관관계의 분포를 분석하고자 한다.

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] 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.

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

[5] A. Canteaut, P. Charpin, and H. Dobbertin, "Binary m-sequences with three-valued cross-correlation: a proof of Welch's conjecture," IEEE Trans. Inform. Theory Vol. 46, pp. 4-8, 2000.

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

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

[8] 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.

[9] R. Gold, "Maximal recursive sequences with 3-values cross-correlation functions," IEEE Trans. Inform. Theory, Vol 14, pp. 154-156, 1967.

[10] T. Helleseth, J. Lahtonen and P. Rosendahl, "On Nihotypecross-correlation functions of m-sequences," Finite Fields and Their Applications, Vol. 13(2), pp. 305-317, 2007.

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

[12] 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.

[13] U.S. Choi, S.J. Cho and S.H. Kwon, "Non-linear Extended Binary Sequence with Low Cross-Correlation," 한국정보통신학회 논문지 (To appear).

[14] T. Helleseth and P. Rosendah, "New pairs of m-sequences with 4-level cross-correlation," Finite Fields and Their Applications, Vol. 11(4),pp. 674-683, 2005.