5-값 상호상관관계를 갖는 비선형 이진수열군의 상호상관관계 빈도 분석

최언숙¹ · 조성진^{2*}

Analysis of Cross-correlation Frequency between Non-linear Binary Sequences Family with 5-Valued Cross-Correlation Functions

Un-sook Choi¹ · Sung-jin Cho^{2*}

¹Department of school of free major, Tongmyong University, Busan 608-711, Korea

²Department of Applied mathematics, Pukyong National University, Busan 608-737, Korea

요 약

여러 가지 디지털통신 시스템에서 많이 사용되고 있는 의사 난수열을 설계하는데 있어 가장 중요한 문제는 생성된 수열들 사이의 상호상관관계가 낮은 수열을 생성하는 것이다. 또한 설계된 이진수열의 상호상관관계의 빈도분석은 많은 연구자에 의해 연구되어왔다. 본 논문에서는 $n = 2m$, $d = 2^{m-1}(3 \cdot 2^m - 1)$ 일 때 5-값 상호상관관계를 갖는 비선형 이진수열군 $S^r = \{Tr_1^m\{[Tr_m^n(a\alpha^t + \alpha^{dt})^r]\} \mid a \in GF(2^m), 0 \leq t < 2^n - 1\}$ 에 대한 상호상관관계에 대한 빈도 분석과 여러 가지 상호상관관계 성질을 분석한다. 여기서 $\gcd(r, 2^m - 1) = 1$ 이다.

ABSTRACT

The design of PN(Pseudo Noise) sequences with good cross-correlation properties is important for many research areas in communication systems. Also analyses of cross-correlation frequency between designed sequences have been researched. In this paper we analyze of cross-correlation distribution and properties of non-linear binary sequences family $S^r = \{Tr_1^m\{[Tr_m^n(a\alpha^t + \alpha^{dt})^r]\} \mid a \in GF(2^m), 0 \leq t < 2^n - 1\}$, where $\gcd(r, 2^m - 1) = 1$ with 5-valued cross-correlation.

키워드 : 상호상관관계, 상호상관관계 빈도, 유한체, m -수열, 비선형 이진수열, 트레이스

Key word : cross-correlation, cross-correlation frequency, finite fields, m -sequence, non-linear binary sequence, trace

접수일자 : 2013. 08. 12 심사완료일자 : 2013. 09. 02 게재확정일자 : 2013. 09. 23

* **Corresponding Author** Sung-jin Cho(E-mail:sjcho@pknu.ac.kr, Tel:+82-51-629-5527)

Department of Applied mathematics, Pukyong National University, Busan 608-737, Korea

Open Access <http://dx.doi.org/10.6109/jkiice.2013.17.12.2875>

print ISSN: 2234-4772 online ISSN: 2288-4165

©This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright © The Korea Institute of Information and Communication Engineering.

I. 서 론

1970년대 부터 의사 난수열군에 대한 연구는 끊임없이 많은 연구자들에 의해 연구되고 있다[1~11]. 이는 의사 난 수열이 부호이론, 디지털 통신시스템을 비롯하여 최근 암호 시스템에 이르기 까지 다양한 분야에서 응용되고 있기 때문이다. 의사 난수열의 장점은 랜덤성을 가지면서도 수학적으로 모델링하여 생성할 수 있기 때문에 수학적 분석이 용이하다는 것이다[5].

디지털 통신 시스템에서 사용되는 디지털 변조방식은 다양하다. 현재 우리나라에서 사용되고 있는 방식인 코드분할 다중화 변조(이하 CDMA)가 가장 우월한 변조방식이라고 알려져 있다. CDMA는 여러 사용자가 시간과 주파수를 공유하면서 각 사용자에게 확산코드라고 하는 서로 다른 의사 난수열을 할당한다[12]. 각 사용자는 할당된 확산코드를 이용하여 송신할 신호를 변조한다. 신호를 변조하는데 사용하는 코드를 선택하는 것은 CDMA 시스템의 수행능력을 결정하는 데 있어 매우 중요하다[13]. 왜냐하면 품질이 좋은 수열은 사용자들 사이의 신호의 간섭을 줄이고 신호를 잘 복호할 수 있도록 하기 때문이다[14,15]. 이러한 의사 난수열이 가지는 바람직한 몇 가지 성질은 낮은 자기 상관 관계(auto-correlation)값, 낮은 상호상관관계(cross-correlation) 값, 큰 선형스팬(linear span), 많은 서로 다른 수열군의 존재성, 구현의 용이성 등이다[13]. 낮은 자기상관관계와 낮은 상호상관관계는 여러 가지 디지털통신 시스템에서 사용되기 위한 의사 난수열인 이진수열을 설계하는 데 있어 가장 중요한 문제이다[8,10]. 더 나아가 큰 선형스팬 성질은 암호 시스템 및 보안 통신에서 중요한 역할을 한다. 수열의 선형스팬은 현재의 값을 가지고 다음 값을 예측하는 것에 대한 척도로 사용되는데 선형스팬이 클수록 예측하는 것이 어렵기 때문이다. 따라서 암호시스템에 사용될 이진수열을 설계하는 데 있어서 큰 선형스팬을 갖는 이진수열에 대한 요구가 커지고 있다. 또한 많은 서로 다른 수열군의 존재성은 통신시스템에서 더 많은 사용자들이 동시에 사용하기 위해 필요하다[10,11].

이진수열 발생을 위한 여러 방법 중 가장 일반적인 것은 트레이스(trace) 함수를 사용하는 방법이다. 트레이스 함수를 이용하여 모델링한 수열 중 대표적인 수열은 m -수열, GMW 수열, Kasami 수열, No 수열, Gold

계열의 수열이 있다. 그리고 트레이스를 이용한 여러 수열들이 연구되었다[1~3,5,6]. 이러한 수열에 관한 연구의 주요 관심사는 제안된 수열의 상호상관관계 함숫값이 몇 개이고 그 분포는 어떠한지 그리고 이러한 수열군의 크기는 어느 정도인지, 수열이 갖는 선형스팬은 어떠한지 등이다.

본 논문에서는 $n = 2m$, $d = 2^{n-1}(3 \cdot 2^m - 1)$ 이고 $\gcd(r, 2^m - 1) = 1$ 일 때 5-값 상호상관관계를 갖는 비선형 이진수열군

$$S^r = \{ Tr_1^m \{ [Tr_m^n (a\alpha^t + \alpha^{2t})]^r \} \mid a \in GF(2^m), 0 \leq t < 2^n - 1 \}$$

에 대한 상호상관관계 빈도 분석과 여러 가지 상호상관관계 성질을 분석한다.

II. 배경 지식 및 기존 연구

트레이스함수는 유한체로부터 부분체로의 선형매핑인데, 이 함수는 의사불규칙 수열의 설계와 분석을 위한 중요한 수학적 도구이다. 지금까지 제안된 많은 이진수열들이 트레이스함수에 의해 정의되었다.

$GF(2^n)$ 를 2^n 개의 원소를 가진 유한체라 하고, $GF(2^n)^* = GF(2^n) / \{0\}$ 라 하자. 1보다 큰 정수 k 에 대하여 $n = km$ 라 하고 차수가 n 인 원시다항식 $f(x)$ 의 원시근을 $\alpha (\in GF(2^n))$ 라 하면 트레이스 함수 $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$ 는 식(1)과 같다[16].

$$Tr_m^n(x) = x + x^{2^m} + x^{2^{2m}} + \dots + x^{2^{m(n/m-1)}} \quad (1)$$

여기서 x 는 $GF(2^n)$ 의 원소이다.

다음은 함수 $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$ 의 성질이다[16]. $GF(2^n)$ 의 원소 x, y 와 $GF(2^m)$ 의 원소 c 에 대하여

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

$$(b) Tr_m^n(cx) = c Tr_m^n(x).$$

$$(c) Tr_m^n \text{는 전사함수이다.}$$

$$(d) Tr_m^n(x^{2^{mi}}) = Tr_m^n(x).$$

$$(e) Tr_1^n(x) = Tr_1^m[Tr_m^n(x)].$$

$$(f) Tr_m^n(x) = c \text{를 만족하는 } x \text{는 } 2^{n-m} \text{ 개이다.}$$

표 1. 최적의 상호상관관계를 갖는 이진수열

Table. 1 Binary sequences with optimal cross-correlations

수열	수학적 모델링	상호상관관계
GMW 수열	$Tr_1^m \{ [Tr_m^n(\alpha^t)]^r \}$	$-2^m - 1, -1$
Kasami 수열	$Tr_1^n(\alpha^t) + Tr_1^m(\gamma_i \cdot \beta^t), \gamma_i \in GF(2^m)$	$-2^m - 1, -1, 2^m - 1$
No 수열	$Tr_1^m \{ [Tr_m^n(\alpha^{2t}) + \gamma_i \cdot \beta^t]^r \}, \gamma_i \in GF(2^m)$	$-2^m - 1, -1, 2^m - 1$

이러한 트레이스 함수를 이용하여 생성하는 수열 중 부분체를 이용하여 생성하는 수열로는 GMW 수열, Kasami 수열, No 수열 등이 있고 데시메이션(decimation)을 이용하여 서로 다른 두 개의 m -수열을 결합하여 생성하는 Gold 계열 수열이 있다[2,4,7,9].

다음은 논문에서 사용되는 기호로 논문 전개의 용이함을 위해 정의한다.

• Notations

- i) $\alpha : GF(2^n)$ 의 원시원소
- ii) $N = 2^n - 1$: 수열의 주기
- iii) $0 \leq t \leq N-1$
- iv) $0 \leq \tau \leq N-1$
- v) $m = n/2$
- vi) $\beta = \alpha^{2^{m+1}} : GF(2^m)$ 의 원시원소
- vii) $T = 2^m + 1$
- viii) $\gcd(r, 2^m - 1) = 1$
- ix) $H(t_2, \tau, r) = [Tr_m^n(a\alpha^{t_2+\tau} + \alpha^{dt_2+d\tau})]^r + [Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2})]^r$
- x) $h_{t_2} = |\{t_2 | H(t_2, \tau, r) = 0\}|$
- xi) $\bar{x} = x^{2^m}$
- xii) $S = \{x \in GF(2^n) | x \cdot x^{2^m} = 1\}$

식(1)에서 정의된 트레이스 함수를 이용하여 주기가 N 인 여러 가지 수열을 정의할 수 있다. 양의 정수 n 에 대하여 m -수열 $S_m(t)$ 는 식(2)와 같다[1].

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

이러한 m -수열은 입력 비트가 이전 상태들의 선형 함수의 결과 값으로 되돌려지는 시프트 레지스터인 LFSR에 의해 생성되는데 그림 1은 LFSR의 구조를 보

여준다.

그림 1. LFSR의 구조

Fig. 1 Structure of LFSR

의사 난수열이 암호화되었을 때 상관공격에 대해 높은 안전성을 유지하기 위해 상호상관관계가 작은 값을 갖는 것이 바람직한데 주기가 N 인 두 개의 수열 $s_i(t)$ 와 $s_j(t)$ 의 상호상관관계 함수 $C_{ij}(\tau)$ 의 정의는 식(3)과 같다[1].

$$C_{ij}(\tau) = \sum_{t=0}^{N-1} (-1)^{s_i(t+\tau) + s_j(t)} \quad (3)$$

m -수열과 같이 낮은 상호상관관계를 가지면서 수열군의 크기가 큰 수열 또는 선형스팬이 큰 비선형 이진수열군에 대한 설계에 대한 연구가 매우 활발히 진행되었다. 표1은 트레이스 함수에 의해 설계된 대표적인 이진수열과 상호상관관계값을 나타낸다.

GMW 수열은 m -수열과 상호상관관계가 같으면서 선형스팬이 높은 비선형 이진수열이다. m -수열과 GMW 수열은 하나의 수열에 대해서 자기상관관계 성질을 고려하는 경우이고 Kasami 수열, No 수열, Gold 계열 수열은 수열군에서 같은 군에 있는 수열들 사이의 상호상관관계와 각 수열의 자기상관관계를 고려하는 경우이다. $\gamma_i \in GF(2^m)$ 이므로 Kasami 수열군과 No 수열군의 크기는 2^m 이다. No 수열군은 Kasami 수열군과 상호상관관계 값은 같으나 비선형 이진수열이므로 선

형스팬이 Kasami 수열군보다 높다.

Gold 계열 수열은 하나의 m -수열 $u(t)$ 와 $u(t)$ 에 데시메이션을 적용한 수열 $v(t)$ 를 생성하여 얻은 두 수열을 합하여 생성하는 수열로 식(4)와 같다[2].

$$u(t) = Tr_1^n(\alpha^t), v(t) = u(dt) = Tr_1^n(\alpha^{dt}) \quad (4)$$

여기서 데시메이션 $d(1 \leq d \leq 2^n - 2)$ 는 $\gcd(d, 2^n - 1) = 1$ 를 만족한다. 특히 $n = 2m$ 일 때 $d \equiv 1 \pmod{2^m - 1}$ 인 Gold 계열 수열을 **Niho 형태의 Gold 계열 수열**이라 한다[4,7,9].

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

Table. 2 Decimations of Gold-like binary sequences with 3-valued cross-correlations

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 계열 이진수열의 여러 가지 데시메이션

Table. 3 Decimations of Gold-like binary sequences with 4-valued cross-correlations

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

표 2는 Gold 계열의 이진수열에서 3값-상호상관관계를 갖는 경우이고, 표 3은 Gold 계열의 이진수열로 4값-상호상관관계를 갖는 경우의 데시메이션 값이다[9]. Gold 계열 수열의 확장으로 다음과 같은 비선형 이진수열이 제안되었다[11].

$$S^r = \{s_a^r(t) \mid a \in GF(2^m), 0 \leq t < N\} \quad (5)$$

여기서 $s_a^r(t) = Tr_1^m\{Tr_m^n(a\alpha^t + \alpha^{dt})^r\}$ 이다.

주어진 r 에 대하여 $a \in GF(2^m)$ 이므로 주어진 수열군 S^r 의 크기는 2^m 이다. 주어진 수열군 S^r 에 속한 두 수열의 상호상관관계는 식(6)과 같다.

$$C_{ab}(\tau) = \sum_{t=0}^{N-1} (-1)^{s_a^r(t+\tau) + s_b^r(t)} \quad (6)$$

상호상관관계를 분석의 용이함을 위해 주기가 N 인 수열을 $(T-2) \times T$ 의 배열로 생각한다. 다음은 본 논문에서 분석 하고자 하는 수열군에 대한 선행 연구결과이다[11].

<보조정리 1[11]> $n = 2m, d = 2^{n-1}(3 \cdot 2^m - 1)$ 일 때 다음이 성립한다.

- ① $d \equiv 1 \pmod{2^m - 1}$
- ② $d \equiv -2 \pmod{2^m + 1}$
- ③ $\gcd(d, 2^n - 1) = 1$

<정리 2[11]> $d = 2^{n-1}(3 \cdot 2^m - 1)$ 일 때 수열군 S^r 의 상호상관관계 $C_{ab}(\tau)$ 는 S^1 의 상호상관관계와 같고 다음을 만족한다.

$$C_{ab}(\tau) \in \{-1 + k \cdot 2^m \mid k = -1, 0, 1, 2, 3\}$$

III. τ 의 변화에 대한 상호상관관계 $C_{0,\beta^i}(\tau)$ 의 관계 분석

$s_a^r(t) = Tr_1^m\{Tr_m^n(a\alpha^t + \alpha^{dt})^r\}$ 에서 상호상관관계 값이 발생하는 발생빈도에 대한 (6)에서 $s_a^r(t+\tau) + s_b^r(t) = Tr_1^m\{H(t_2, \tau, r)\}$ 이다. 여기서 $t = t_1 T + t_2$ 라 두고 $GF(2^n)$ 의 부분체인 $GF(2^m)$ 의 원시원소 β 에 대하여 $u = \beta^{t_1 r}$ 라 하면 $C_{ab}(\tau)$ 는 (7)과 같다.

$$\begin{aligned} C_{ab}(\tau) &= -T + \sum_{t_2=0}^{2^m} \sum_{u \in GF(2^m)} (-1)^{Tr_1^m\{u^r H(t_2, \tau, r)\}} \\ &= -1 + (h_{t_2} - 1)2^m \end{aligned} \quad (7)$$

$\gcd(r, 2^m - 1) = 1$ 이므로 $H(t_2, \tau, r) = 0$ 은 $H(t_2, \tau,$

1)=0와 같다. $GF(2^n)$ 의 원시원소 α 에 대하여 $\alpha = \delta\gamma$ 라 표현할 수 있다. 이때 $\delta^{2^m-1} = 1$, $\gamma^{2^m+1} = 1$ 이 되고 δ 는 $GF(2^m)$ 의 원시원소이다. 따라서 $\delta^{2^m} = \delta$, $\gamma^{2^m} = \gamma^{-1}$ 이고 보조정리 1에 의해 $\delta^d = \delta$, $\gamma^d = \gamma^{-2}$ 이다. $x = \delta^{t_2} \gamma^{-2t_2}$, $y = \gamma^{t_2}$ 라 두면 $x^{2^m-1} = y^4$ 이고, $A(\tau) = a\alpha^\tau + b$, $B(\tau) = \alpha^{d\tau} + 1$ 라 하면 $H(t_2, \tau, 1) = 0$ 는 (8)과 같다.

$$x(\overline{B(\tau)} y^4 + A(\tau) y^3 + \overline{A(\tau)} y + B(\tau)) = 0 \quad (8)$$

$x \neq 0$ 이므로 (8)을 양변을 x 로 나누면 h_{t_2} 는 (9)와 같다.

$$h_{t_2} = \{t_2 \mid \overline{B(\tau)} y^4 + A(\tau) y^3 + \overline{A(\tau)} y + B(\tau) = 0\} \quad (9)$$

이다.

본 논문에서는 $a = 0$, $b = \beta^i \in GF(2^m)^*$ 인 경우에 대하여 상호상관관계 발생빈도를 분석하고자 한다. 따라서 (9)의 방정식은 (10)과 같다.

$$\overline{B(\tau)} y^4 + by^3 + by + B(\tau) = 0 \quad (10)$$

<정리 3> $\tau = \tau_1 T + \tau_2$ 라 할 때 $C_{0,b}(\tau)$ 를 τ_1 과 τ_2 를 이용하여 $C_{0,b}(\tau_1, \tau_2)$ 로 나타내면 $C_{0,b}(\tau_1, \tau_2) (\tau_2 \neq 0)$ 는 다음을 만족한다. 단, $0 \leq \tau_1 < T-2, 0 \leq \tau_2 < T$.

$$C_{0,b}(\tau_1, \tau_2) = C_{0,b}(\tau_1 + \tau_2 - 1, T - \tau_2) \quad (11)$$

$$\langle \text{증명} \rangle \alpha^T = \beta, \beta^d = \beta \text{이므로}$$

$$B(\tau) = B(\tau_1 T + \tau_2) = \alpha^{d(\tau_1 T + \tau_2)} + 1 = \beta^{\tau_1} \alpha^{d\tau_2} + 1 \text{ 이고,}$$

$$\overline{B(\tau)} = \overline{B(\tau)}^{2^m} = (\beta^{\tau_1} \alpha^{d\tau_2} + 1)^{2^m} = \beta^{\tau_1} \alpha^{2^m d\tau_2} + 1 \text{ 이다.}$$

$C_{0,b}(\tau_1, \tau_2) = C_{0,b}(\tau_1 + \tau_2 - 1, T - \tau_2)$ 임을 보이기 위해 $\tau = \tau_1 T + \tau_2$ 일 때 $\tau' = (\tau_1 + \tau_2 - 1)T + (T - \tau_2)$ 라 하자. 그러면 $B(\tau')$ 와 $\overline{B(\tau')}$ 은 다음과 같다.

$$\begin{aligned} B(\tau') &= \alpha^{d\tau'} + 1 = \alpha^{d((\tau_1 + \tau_2 - 1)T + (T - \tau_2))} + 1 \\ &= \beta^{\tau_1 + \tau_2 - 1} \beta \alpha^{-d\tau_2} + 1 = \beta^{\tau_1 + \tau_2} \alpha^{-d\tau_2} + 1. \end{aligned}$$

$$\overline{B(\tau')} = (\beta^{\tau_1 + \tau_2} \alpha^{-d\tau_2} + 1)^{2^m} = \beta^{\tau_1 + \tau_2} \alpha^{-2^m d\tau_2} + 1.$$

$B(\tau)$ 와 $\overline{B(\tau)}$ 결과를 (10)에 대입하면 (12)와 같다.

$$(\beta^{\tau_1} \alpha^{2^m d\tau_2} + 1)y^4 + by^3 + by + (\beta^{\tau_1} \alpha^{d\tau_2} + 1) = 0 \quad (12)$$

$B(\tau')$ 와 $\overline{B(\tau')}$ 결과를 (10)에 대입하면 (13)과 같다.

$$\begin{aligned} &(\beta^{\tau_1 + \tau_2} \alpha^{-2^m d\tau_2} + 1)y^4 + by^3 + by + (\beta^{\tau_1 + \tau_2} \alpha^{-d\tau_2} + 1) = 0 \\ \Leftrightarrow &(\beta^{\tau_1} \alpha^{2^m(T-d)\tau_2} + 1)y^4 + by^3 + by + (\beta^{\tau_1} \alpha^{(T-d)\tau_2} + 1) = 0 \end{aligned} \quad (13)$$

(11)을 만족하기 위해서는 모든 $\tau_2 (\neq 0)$ 에 대하여 (12)와 (13)이 같아야 한다. 따라서 $\alpha^{d\tau_2} = \alpha^{(T-d)\tau_2}$ 이어야 한다. 그런데 $d \equiv 1 \pmod{2^m-1}$, $T \equiv 2 \pmod{2^m-1}$ 이므로 $d \equiv T-d \pmod{2^m-1}$ 이다. 따라서 $\alpha^{d\tau_2} = \alpha^{(T-d)\tau_2}$ 이다. $\square$

-1	-17	-17	(15)	(1)	(3)	15	-17	15	-17	-17	-1	-17	-17	-1	47	-17
31	-1	-1	-17	-1	-1	47	-17	-1	15	-1	-1	-17	-1	15	-17	-1
31	15	-17	-1	-1	-1	15	-17	-1	-1	-1	15	-1	-17	(15)	-1	15
31	-1	-17	-17	-17	15	-1	-17	-1	-17	-1	15	15	(1)	-17	-17	-1
-1	-1	-17	-1	15	15	15	-1	-17	15	-17	15	(3)	-1	-1	-17	-1
31	-1	-1	-1	-17	15	15	15	-17	-17	15	(15)	-1	-1	-17	-17	-1
31	-17	-17	-1	15	-17	47	-17	15	-1	(-17)	47	-1	-17	-1	-1	-17
-1	-17	-1	15	-17	-17	-1	47	-17	(15)	-17	15	15	15	-1	-17	-17
-1	15	-1	-17	15	-17	15	-1	-17	-1	-17	-1	15	-17	-1	-1	15
31	15	-1	-17	-1	-1	-1	-17	15	-1	-17	15	15	15	-1	-1	15
-1	-17	15	-17	-17	-1	-1	-1	-1	-1	15	-17	-17	-17	-1	-17	-17
31	-17	-17	-17	15	-17	-1	-1	-17	-17	15	47	-17	15	-17	15	-17
-1	-1	-17	15	-17	-17	15	-1	15	-17	-17	-1	-17	-1	-17	-17	-1
-1	15	15	-1	-1	-1	15	-17	-17	15	47	15	-1	-17	-17	-17	15
-1	-17	47	15	-17	15	15	15	-1	-17	-1	-1	-17	15	15	15	-17

그림 2. $n=8$ 일 때 상호상관관계 $C_{0,\beta}(\tau_1, \tau_2)$

Fig. 2 Cross-correlation $C_{0,\beta}(\tau_1, \tau_2)$ when $n=8$

그림 2는 $n=8$, $d=151$ 이고 $a=0$, $b=\beta$ 라 할 때 $C_{0,\beta}(\tau)$ 를 $(T-2) \times T$ 배열로 나타낸 것이다. 그림에서 $C_{0,\beta}(0,3)$ 은 $C_{0,\beta}(2,14)$ 와 같다.

IV. 상호상관관계 $C_{0,\beta}(\tau)$ 의 빈도 분석

$d = 2^{n-1}(3 \cdot 2^m - 1)$ 일 때, $(x+1)^d = x^d + 1$ 의 해의 개수를 구해보자. 먼저 m 이 짝수일 때, $d+1 = (2^m+1)(3 \cdot 2^{n-1} - 2^{m+1} + 2) - 1$ 이므로 $\gcd(d+1, 2^m+1) = \gcd(1, 2^m+1) = 1$ 이다. 또한 $d-1 = (2^m+1)(3 \cdot 2^{n-1} - 5 \cdot 2^{m-1} + 2) - 3$ 이고, m 이 짝수이므로 $m = 2k (k=1, 2, \dots)$ 이라 두면 $2^m+1 = 2^{2k}+1 \equiv (-1)^{2k}+1 \equiv 2 \pmod{3}$ 이므로 $\gcd(d-1,$

$2^m + 1 = \gcd(3, 2^m + 1) = \gcd(3, 2) = 1$ 이다. 따라서 [17]의 정리 3.7에 의해 해의 개수는 2^m 개이다. m 이 홀수일 때, $d-1 = (2^m-1)s$ 라 두면 $d-1 = (2^m-1) \cdot (3 \cdot 2^{n-1} + 2^m + 1)$ 이므로 $s = 3 \cdot 2^{n-1} + 2^m + 1$ 이다. $\gcd(2^{m-1}, 2^m + 1) = 1$ 이므로

$$\begin{aligned}\gcd(s-1, 2^m+1) &= \gcd(3 \cdot 2^{n-1} + 2^m, 2^m+1) \\ &= \gcd(3 \cdot 2^{m-1} + 1, 2^m+1) \\ &= \gcd(2^{m-1}, 2^m+1) = 1\end{aligned}$$

그러므로 $\gcd(s-1, 2^m+1) = 1$ 이다. [17]의 정리 3.10에 의해 $GF(2^n)$ 에서 해집합은 $GF(2^m) \cup GF(2^2)$ 이고 해의 개수는 $2^m + 2^2 - 2 = 2^m + 2$ 이다. 그러므로 m 에 따라 $(x+1)^d = x^d + 1$ 의 해의 개수는 (14)와 같다.

$$\begin{cases} 2^m, & m : \text{even} \\ 2^m + 2, & m : \text{odd} \end{cases} \quad (14)$$

$\sum_{t=0}^{2^n-2} (-1)^{Tr_1^n(b\alpha^t + \alpha^{dt})}$ 를 계산하기 위해 $t = t_1 T + t_2$,

$(0 \leq t_1 \leq 2^m - 2, 0 \leq t_2 \leq T-1)$ 라 두고 식을 정리하면 $Tr_1^n(b\alpha^t + \alpha^{dt}) = Tr_1^m\{\beta^{t_1} Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2})\}$ 이다. 우변의 괄호 안의 $Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2})$ 를 $\alpha = \delta\gamma, \gamma^{t_2} = z$ 라 두고 정리하면 $Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2}) = \delta^{t_2}(bz + z^{-2} + bz^{-1} + z^2)$ 이다. 따라서

$$\begin{aligned}\sum_{t=0}^{2^n-2} (-1)^{Tr_1^n(b\alpha^t + \alpha^{dt})} &= \sum_{t_1=0}^{2^m-2} \sum_{t_2=0}^{2^m} (-1)^{Tr_1^m\{\beta^{t_1} \delta^{t_2} (bz + z^{-2} + bz^{-1} + z^2)\}} \\ &= \sum_{x \in GF(2^m)^*} \sum_{t_2=0}^{2^m} (-1)^{Tr_1^m\{x \delta^{t_2} (bz + z^{-2} + bz^{-1} + z^2)\}} \\ &= \sum_{t_2=0}^{2^m} \sum_{x \in GF(2^m)^*} (-1)^{Tr_1^m\{x \delta^{t_2} (bz + z^{-2} + bz^{-1} + z^2)\}} \\ &= N(2^m - 1) + (2^m + 1 - N) \cdot (-1) \\ &= (N-1)2^m - 1.\end{aligned} \quad (15)$$

단, $N = |\{z \in S | bz + z^{-2} + bz^{-1} + z^2 = 0\}|$ 이다.

N 의 값을 구하기 위해 $bz + z^{-2} + bz^{-1} + z^2 = 0$ 를

변형하면 $(z+1)^2(z^2 + bz + 1) = 0$ 이 된다. 만약, $Tr_1^m(1/b) = 0$ 이면 $GF(2^m)$ 에서 해가 존재하므로 S 에서는 더 이상 해가 없다.

따라서 $N=1$ 이다. 그리고 $Tr_1^m(1/b) = 1$ 이면 S 에서 해가 2개 존재하거나 $(GF(2^n) \setminus GF(2^m)) - S$ 에서 해가 2개 존재한다. 만약 $z^2 + bz + 1 = 0$ 를 만족하는 해 z_1, z_2 가 $(GF(2^n) \setminus GF(2^m)) - S$ 의 원소라 하자. $z_1 + z_2 \in GF(2^m)$, $z_1 z_2 = 1$ 이다. $z_1 + z_2$ 가 $GF(2^m)$ 의 원소이므로 $\overline{z_1 + z_2} = z_1 + z_2$ 이고, $\overline{z_1} + \overline{z_2} = z_1 + z_2$ 이다. $z_1 z_2 = 1$ 이므로 $z_2 = z_1^{-1}$ 을 대입하면, $\overline{z_1} + \overline{z_1^{-1}} = z_1 + z_1^{-1}$ 이다. 양변에 $z_1^{2^m}$ 을 곱하여 정리하면 $(z_1^{2^m+1} + 1)(z_1^{2^m-1} + 1) = 0$ 이다.

그런데 $z_1 \notin GF(2^m)$ 이고 $z_1 \in S$ 이므로 모순이다. 따라서 $Tr_1^m(1/b) = 1$ 이면 S 에서 해가 2개 존재한다. 그러므로 $N=3$ 이다. 따라서 (16)이 성립한다.

$$\sum_{t=0}^{2^n-2} (-1)^{Tr_1^n(b\alpha^t + \alpha^{dt})} = \begin{cases} -1, & Tr(1/b) = 0 \\ 2^{m+1} - 1, & Tr(1/b) = 1 \end{cases} \quad (16)$$

(14)와 (16)을 이용하여 Rosendahl의 방법으로 식을 정리하면 상호상관관계 빈도수를 계산하기 위한 중요한 정리를 얻을 수 있다.

<정리 4> $n = 2m, b \in GF(2^m)^*$ 이고

$d = 2^{n-1}(3 \cdot 2^m - 1)$ 라 할 때 $k = 1, 2, \dots, 2^k$ 에 대하여 다음이 성립한다.

$$\begin{aligned}\textcircled{1} \sum_{\tau=0}^{N-1} \{C_{0,b}(\tau) + 1\} &= \begin{cases} 2^n, & Tr(1/b) = 0 \\ 2^m(2^m - 2), & Tr(1/b) = 1 \end{cases} \\ \textcircled{2} \sum_{\tau=0}^{N-1} \{C_{0,b}(\tau) + 1\}^2 &= \begin{cases} 2^{2n}, & Tr(1/b) = 0 \\ 2^{2m}(2^{2m} - 2^2), & Tr(1/b) = 1 \end{cases} \\ \textcircled{3} \text{ i: } m : \text{even} & \\ \sum_{\tau=0}^{N-1} \{C_{0,b}(\tau) + 1\}^3 &= \begin{cases} 2^{2n+m}, & Tr(1/b) = 0 \\ 2^{3m}(2^m - 2^3), & Tr(1/b) = 1 \end{cases} \\ \textcircled{3} \text{ ii: } m : \text{odd} & \\ \sum_{\tau=0}^{N-1} \{C_{0,b}(\tau) + 1\}^3 &= \begin{cases} 2^{2n}(2^m + 2), & Tr(1/b) = 0 \\ 2^{3n}(2^n + 2^{m+1} - 2^3), & Tr(1/b) = 1 \end{cases}\end{aligned}$$

$|\{y \in S | \overline{B(\tau)}y^4 + by^3 + by + B(\tau) = 0\}| = i$ 를 만족하는 y 의 개수를 N_i 를 라 정의하면 정리4에 의하여

$Tr(1/b)=0$ 이고 m 이 짝수 일 때 다음과 같은 선형연립방정식을 얻을 수 있다.

$$\begin{cases} N_0 + N_1 + N_2 + N_3 + N_4 = 2^n - 1 \\ -2^m N_0 + 2^m N_2 + 2 \cdot 2^m N_3 + 3 \cdot 2^m N_4 = 2^n \\ 2^n N_0 + 2^n N_2 + 2^2 \cdot 2^n N_3 + 3^2 \cdot 2^m N_4 = 2^{2n} \\ -2^{3m} N_0 + 2^{3m} N_2 + 2^3 \cdot 2^{3m} N_3 + 3^3 \cdot 2^{3m} N_4 = 2^{2n+m} \end{cases} \quad (17)$$

연립방정식 (17)을 풀기위해 먼저 N_3 를 구한다. N_3 는 (10)의 해의 개수가 3인 경우로 반드시 중근을 갖는다. 따라서 (10)을 미분하여 0이 되는 조건을 찾으면 $by^2 + b = 0$ 이고 $b \neq 0$ 이므로 $y = 1$ 인 경우이다. $y = 1$ 을 (10)에 대입하면 $\overline{B(\tau)} = B(\tau)$ 이어야 하고 이는 $\tau_2 = 0$ 인 경우로 상호상관관계 배열에서 첫 번째 열에 해당된다. 또한 $y = 1$ 을 (10)에 대입하여 정리하면 식 (18)과 같다.

$$(y+1)^2(B(\tau)y^2 + by + B(\tau)) = 0 \quad (18)$$

$\tau_2 = 0$ 일 때 중근 $y = 1$ 을 가지므로 서로 다른 해의 개수는 3개 이하이다. (18)이 서로 다른 3개의 해를 갖기 위해서는 $(B(\tau)y^2 + by + B(\tau)) = 0$ 이 서로 다른 2개의 해를 S 에서 가져야 하는데, $S \setminus \{1\} \in GF(2^n) \setminus GF(2^m)$ 이므로 $Tr_1^m(B(\tau)/b) = 1$ 일 때 S 에서 서로 다른 두 근을 갖는다. 따라서 $\tau_2 = 0$ 일 때 $2^m - 1$ 개의 수열 중 $Tr_1^m(B(\tau)/b) = 1$ 를 만족하는 τ_1 의 개수는 2^{m-1} 또는 $2^{m-1} - 1$ 이다. 왜냐하면 $\tau_1 = 0$ 일 때 $B(\tau) = 0$ 이 되므로 $B(\tau)/b(\tau_1 = 1, 2, \dots, 2^m - 2)$ 는 $GF(2^m)^*$ 의 원소 중 하나 씩 빠지게 되므로 빠지는 원소의 트레이스 값에 따라 두 가지 양상을 보이게 된다.

$Tr_1^m(B(\tau)/b) = 0$ 인 경우 $B(\tau)y^2 + by + B(\tau) = 0$ 는 $GF(2^m)$ 에서 해를 2개 가지므로 해의 개수는 1이다.

따라서 $N_3 = 2^{m-1}$ 이라고 두고 방정식 (15)를 풀고 $N_3 = 2^{m-1} - 1$ 이라고 방정식 (15)를 풀면 된다. 나머지 경우에 대해서도 같은 방법으로 풀면 된다. 표 4는 $n = 2m$, $b \in GF(2^m)^*$ 이고 $d = 2^{n-1}(3 \cdot 2^m - 1)$ 일 때 $C_{0,b}(\tau)$ 의 발생빈도수이다. 표 5는 n 이 6, 8, 10, 12 일 때 상호상관관계 발생빈도를 나타낸 것이다.

V. 결 론

본 논문에서는 [11]에서 제안되었던 5값 상호상관관계를 갖는 비선형 이진수열군 S^n 에 대하여 $a = 0$ 이고 $b \in GF(2^m)^*$ 일 때 상호상관관계 $C_{0,b}(\tau)$ 의 각 값에 대한 발생빈도수를 분석하였다. $C_{0,b}(\tau)$ 는 b^{-1} 의 트레이스 값에 따라 상호상관관계값이 -1 일 때와 $2^{m+1} - 1$ 일 때 발생빈도의 차이가 1씩 남을 보였고 m 이 홀수일 때와 짝수일 때에 따라 상호상관관계 각 값에 대한 발생빈도의 양상이 달라짐을 보였다. 실제 각 τ 의 변화에 따른 상호상관관계 값에 대한 계산복잡도는 $O(2^n)$ 로 매우 높다. 본 논문에서는 τ 를 $\tau = \tau_1 T + \tau_2$ 로 두고 분석하여 상호상관관계 배열로 분석하여 $\tau_2 (\neq 0)$ 와 $T - \tau_2$ 사이의 관계를 분석함으로 τ 의 변화에 따른 상호상관관계 계산에 대한 효율성을 높였다. 향후 $C_{a,b}(\tau)$ 에 대한 상호상관관계 및 빈도에 대해 분석하고자 한다.

표 4. $d = 2^{n-1}(3 \cdot 2^m - 1)$ 일 때 $C_{0,b}(\tau)$ 의 발생빈도
Table. 4 Cross-correlation Frequency of $C_{0,b}(\tau)$ when $d = 2^{n-1}(3 \cdot 2^m - 1)$

$C_{0,b}(\tau)$	발생빈도 ($\epsilon = Tr(1/b)$)
$-2^m - 1$	$2^{n-1} - 2^{m-3}(2^m + (-1)^{m+1} + 1) - 2^{m-1}$
-1	$(2^n + (-1)^{m+1}2^m)/3 + 2^{m-1} - 1 + \epsilon$
$2^m - 1$	$2^{n-1} - 2^{m-2}(2^m + (-1)^{m+1} + 1)$
$2^{m+1} - 1$	$2^{m-1} - \epsilon$
$3 \cdot 2^m - 1$	$(2^{m-3}(2^m + (-1)^{m+1} + 1) - 2^{m-1})/3$

표 5. $C_{0,b}(\tau)$ 의 발생빈도($n = 6, 8, 10, \dots, 20$)
Table. 5 Frequency of $C_{0,b}(\tau)$ ($n = 6, 8, 10, \dots, 20$)

n	$-2^m - 1$	-1	$2^m - 1$	$2^{m+1} - 1$	$3 \cdot 2^m - 1$	$Tr(1/b)$
6	18	27	12	4	2	0
	18	28	12	3	2	1
8	88	87	64	8	8	0
	88	88	64	7	8	1
10	360	367	240	16	40	0
	360	368	240	15	40	1
12	1504	1375	1024	32	160	0
	1504	1376	1024	31	160	1
14	6048	5567	4032	64	672	0
	6048	5568	4032	63	672	1
16	24448	21887	16384	128	2688	0
	24448	21888	16384	127	2688	1
18	97920	87807	65280	256	10880	0
	97920	87808	65280	255	10880	1
20	392704	349695	262144	512	43520	0
	392704	349696	262144	511	43520	1

REFERENCES

- [1] S.W. Golomb, *Shift Register Sequences*, Holden Day, 1967.
- [2] R. Gold, "Maximal recursive sequences with 3-valued cross-correlation functions," *IEEE Trans. Inf. Theory*, vol 14, pp. 154-156, 1967.
- [3] T. Kasami, "Weight distribution of Bose- Chaudhuri-Hocquenghem codes", in *Combinatorial Mathematics and Its Applications*, Chapel Hill, NC: Univ. North Carolina Press, 1969.
- [4] Y. Niho, Multi-valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences, Ph.D. thesis, University of Southern California, 1972.
- [5] R.A. Scholtz and R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 548-553, 1984.
- [6] 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.
- [7] T. Helleseth and P.V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman(Eds.), Amsterdam, vol. II, pp.1765-1853, 1998.
- [8] 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.
- [9] P. Rosendahl, Niho type cross-correlation functions and related equations, Ph.D. thesis, Turku center for computer science, 2004.
- [10] 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.
- [11] U.S. Choi, S.J. Cho, H.D. Kim, "Design and Analysis of Linear Span of A New Family of Non-linear Binary Sequences with 5-Valued Cross-Correlation Functions," *The Journal of the Korean Institute of Information and Communication Engineering*, vol.17, no. 3, pp. 619-626, 2013.
- [12] R.A. Scholtz, "The origins of spread-spectrum communications," *IEEE Trans. Commun.*, vol. COM-30, pp. 822-854, 1982.
- [13] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, *Spread Spectrum Communications*, vol. 1, Rockville, MD: Computer Science Press, 1985.
- [14] M.P. Ristenbatt and J.L. Daw, Jr., "Performance criteria for spread spectrum communications," *IEEE Trans. Commun.*, vol. COM-25, no. 8, pp. 756-763, 1977.
- [15] D.V. Sarwate and M.B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, no. 5, pp. 593-620, 1980.
- [16] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press 1997.
- [17] J.M. Yim et. al., "The number of solutions to the equation $(x+1)^d = x^d + 1$," *J. Appl. Math. & Informatics*, vol. 31, pp. 179~188, 2013.

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 조교수
 ※ 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 응용수학과 교수
 ※ 주 관심분야: 셀룰라 오토마타론, 정보보호