5-값 상호상관관계를 갖는 새로운 비선형 이진수열군의 설계와 선형스팬 분석

최언숙* · 조성진** · 김한두***

Design and Analysis of Linear Span of A New Family of Non-linear Binary Sequences with 5-Valued Cross-Correlation Functions

Un-Sook Choi* · Sung-Jin Cho** · Han-Doo Kim***

요 약

여러 가지 디지털통신 시스템에서 많이 사용되고 있는 의사 난수열을 설계하는데 있어 가장 중요한 문제는 생성된 수열들 사이의 상호상관관계가 낮은 수열을 생성하는 것이다. 본 논문에서는 Gold 계열의 수열의 합성으로 이루어지는 새로운 이진수열군 $S^r=\left\{Tr_1^m\left\{\left[Tr_m^n(a\alpha^t+\alpha^{dt})\right]^r\right\}\middle| a\in GF(2^n), 0\le t<2^n-1\right\}$를 제안하고 $d=2^{n-1}(3\cdot 2^m-1)$일 때 상호상관관계 함숫값을 구한다. 여기서 $n=2m$이고 $\gcd(r,2^m-1)=1$이다. 또한 특별한 r에 대하여 이진수열군 S^r의 선형스팬을 분석한다. 제안된 수열은 Gold 계열 수열의 확장이기도 하고 GMW수열의 확장이기도 하다.

ABSTRACT

The design of PN(Pseudo Noise) sequences with good cross-correlation properties is important for many research areas in communication systems. In this paper we propose new family of binary sequences $S^r=\left\{Tr_1^m\left\{\left[Tr_m^n(a\alpha^t+\alpha^{dt})\right]^r\right\}\middle| a\in GF(2^n), 0\le t<2^n-1\right\}$ composed of Gold-like sequences and find the value of cross-correlation function when $d=2^{n-1}(3\cdot 2^m-1)$, where $n=2k$, $\gcd(r,2^m-1)=1$. Also we analyze the linear span of S^r for some special r. Proposed sequences are extension of Gold-like sequences and GMW-sequences.

키워드

상호상관관계, 데시메이션, m-수열, 비선형 이진수열, 트레이스, 선형스팬

Key word

cross-correlation, decimation, m-sequence, non-linear binary sequence, trace, linear span

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

접수일자 : 2012. 10. 22
심사완료일자 : 2012. 11. 13

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.3.619

Ⅰ. 서 론

의사 난수열군에 대한 바람직한 몇 가지 성질은 낮은 자기 상관 관계(auto-correlation) 값, 낮은 상호상관 관계(cross-correlation) 값, 큰 선형스팬(linear span), 많은 서로 다른 수열군의 존재성, 구현의 용이성 등이다. 낮은 자기상관관계와 낮은 상호상관관계는 여러 가지 디지털통신 시스템에서 사용되기 위한 의사 난수열을 설계하는 데 있어 가장 중요한 문제이다[1-4]. 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 설계하는데 있어서 큰 선형스팬을 갖는 이진수열에 대한 요구가 커지고 있다. 또한 많은 서로 다른 수열군의 존재성은 통신시스템에서 더 많은 사용자들이 동시에 사용하기 위해 필요하다.

이진수열은 1970년대부터 많은 연구자들에 의해 연구되어왔고 현재에도 활발히 연구되고 있다[5-14]. 수열 발생을 위한 여러 방법 중 가장 일반적인 것은 트레이스(trace) 함수를 사용하는 방법이다. 잘 알려진 대표적인 수열은 m-수열, GMW 수열, Kasami 수열, No 수열, Gold 계열의 수열이 있다. 그리고 트레이스를 이용한 여러 수열들이 연구되었다[5-9, 11]. 이러한 수열에 관한 연구의 주요 관심사는 제안된 수열의 상호상관 관계 함숫값이 몇 개이고 그 분포는 어떠한지 그리고 이러한 수열군의 크기는 어느 정도인지 등이다. 선형스팬에 관한 연구는 상호상관관계를 분석하는 것에 비해 어렵기 때문에 상대적으로 선형스팬에 대한 연구가 많지 않다.

본 논문에서는 GMW수열과 Gold 계열의 수열의 확장으로 큰 선형스팬을 갖는 비선형 이진수열을 제안하고 이 수열의 상호상관관계를 분석하여 제안한 수열군이 5-값 상호상관관계를 가짐을 보인다. 또한 Key[15]에 의해 제안된 방법으로 제안한 비선형 이진수열의 선형스팬을 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^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 하면 트레이스 함수 $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$는 다음과 같다[16].

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

여기서 x는 $GF(2^n)$의 원소이다.

다음은 함수 $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$의 성질이다[17]. $GF(2^n)$의 원소 x, y와 $GF(2^m)$의 원소 c에 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^n는 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) $Tr_m^n(x) = c$를 만족하는 x는 2^{n-m} 개이다.

이러한 트레이스 함수를 이용하여 생성하는 수열 중 부분체를 이용하여 생성하는 수열로는 GMW수열, Kasami 수열, No 수열 등이 있고 데시메이션(decimation)을 이용하여 서로 다른 두 개의 m-수열을 결합하여 생성하는 Gold 수열이 있다.

위에서 정의된 트레이스 함수를 이용하여 주기가 2^n-1인 여러 가지 수열을 정의할 수 있다. 양의 정수 n에 대하여 $m-$수열 $m(t)$는 (1)과 같다[5].

$$m(t) = Tr_1^n(\alpha^t) \tag{1}$$

여기서 α는 $GF(2^n)$의 원시원소이고 주기가 2^n-1이므로 t는 0에서 2^n-2의 값을 갖는다. 이러한 m-수열은 일반적으로 n개의 시프트 레지스터(shift register)

를 이용하여 생성되는데 그림 1은 시프트 레지스터의 구조를 보여준다.

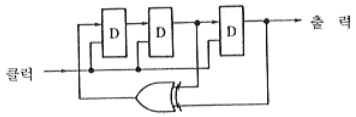

그림 1. 시프트레지스터의 구조
Fig. 1 Structure of shift register

GMW 수열은 m-수열과 상호상관관계가 같으면서 선형스팬이 높은 비선형 이진수열이다. GMW수열 $g(t)$는 식(2)와 같다[9].

$$g(t) = Tr_1^m\{[Tr_m^n(\alpha^t)]^r\} \tag{2}$$

여기서 α는 $GF(2^n)$의 원시원소이고, $m|n$, $0 \le t \le 2^n-2$, $\gcd(r, 2^n-1)=1$이다. 수열의 주기가 2^n-1이므로 t는 0에서 2^n-2의 값을 갖는다.

m-수열과 GMW 수열은 하나의 수열에 대해서 자기상관관계 성질을 고려하는 경우이고 Kasami 수열, No 수열, Gold 수열은 수열군에서 같은 군에 있는 수열들 사이의 상호상관관계와 각 수열의 자기상관관계를 고려하는 경우이다. Kasami 수열군은 식 (3)과 같이 정의된다[8]

$$S_{kasami} = \{K_i(t) | 0 \le t \le 2^n-2,\ 0 \le i \le 2^m-1\}$$
$$K_i(t) = Tr_1^n(\alpha^t) + Tr_1^m(\gamma_i \cdot \beta^t) \tag{3}$$

여기서 $n=2m$, α는 $GF(2^n)$의 원시원소이고, β는 $\beta=\alpha^{2^m+1}$이고 $GF(2^m)$의 원시원소가 된다. 또한 $\gamma_i \in GF(2^m)$ 이다. 따라서 Kasami 수열군의 크기는 2^m이다.

No 수열군은 식 (4)와 같이 정의된다[11].

$$S_{No} = \{N_i(t) | 0 \le t \le 2^n-2,\ 0 \le i \le 2^m-1\}$$
$$N_i(t) = Tr_1^m\{[Tr_m^n(\alpha^{2t}) + \gamma_i \cdot \beta^t]^r\} \tag{4}$$

여기서 $n=2m$, α는 $GF(2^n)$의 원시원소이고, β는 $\beta=\alpha^{2^m+1}$이고 $GF(2^m)$의 원시원소가 된다. 또한 $\gamma_i \in GF(2^m)$, $1 \le r \le 2^m-1$, $\gcd(r, 2^m-1)=1$이다. 따라서 No 수열군의 크기는 2^m이다.

그림 2는 m-수열과 GMW수열, Kasami 수열, No 수열의 관계를 나타낸다[18].

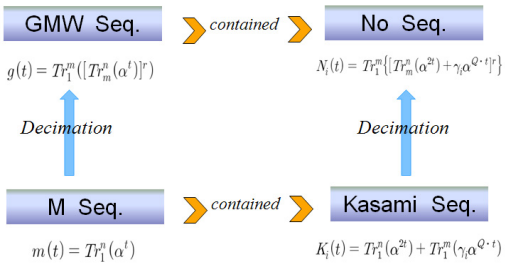

그림 2. 의사불규칙 수열 사이의 관계
Fig. 2 Relation between PN sequences

Gold 수열은 하나의 m-수열 $u(t)$와 $u(t)$에 데시메이션을 적용한 수열 $v(t)$를 생성하여 얻은 두 수열을 합하여 생성하는 수열이다. Gold 수열군은 식 (5)와 같다[7].

$$S_{Gold} = \{s_j(t) | 0 \le t \le 2^n-1, 0 \le j \le 2^n\}$$
$$s_j(t) = Tr_1^n(\alpha^t) + Tr_1^n(\gamma_j \cdot \alpha^{dt}) \tag{5}$$

여기서 α는 $GF(2^n)$의 한 원시원소이고, 데시메이션 $d(1 \le d \le 2^n-2)$는 $\gcd(d, 2^n-1)=1$를 만족한다. 특히 $n=2m$ 일 때 $d \equiv 1 \pmod{2^m-1}$인 Gold 수열을 Niho 형태의 Gold 수열이라 한다[6,13]. Gold 수열군의 크기는 2^n이다.

여러 개의 수열이 존재하는 의사 난수열군의 경우에는 수열군 내의 여러 수열 사이의 상관관계의 특성인 상호상관관계 함수를 고려해야 한다. 이 경우 의사 난수열이 암호화되었을 때 상관공격에 대해 높은 안전성을 유지하기 위해 작은 값을 갖는 것이 바람직한데 주기가 2^n-1인 두 개의 수열 $s_i(t)$와 $s_j(t)$의 상호상관관계 함수 $C_{ij}(\tau)$의 정의는 식 (6)과 같이 주어진다[5].

$$C_{ij}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_i(t+\tau)+s_j(t)} \tag{6}$$

표 1은 지금까지 알려진 우수한 상호상관관계를 갖는 이진수열군이다.

표 1. 최적의 상호상관관계를 갖는 이진수열
Table. 1 Binary sequences with optimal cross-correlations

수열	상호상관관계
m-수열	-1
GMW수열	$-2^m-1,\ -1,\ 2^m-1$
Kasami 수열	$-2^m-1,\ -1,\ 2^m-1$
No 수열	$-2^m-1,\ -1,\ 2^m-1$

표 2. 3값-상호상관관계를 갖는 Gold 계열 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 2는 Gold 계열의 이진수열에서 3값-상호상관관계를 갖는 경우이고, 표 3은 Gold 계열의 이진수열로 4값-상호상관관계를 갖는 경우의 데시메이션 값이다[13].

선형스팬 LS는 현재의 비트를 생성하기 위해 미리 알아야 할 과거의 비트수로 정의된다. 주어진 수열이 선형 이진수열이면 이진수열을 생성하는 최소다항식의 차수가 된다. 그러나 트레이스 함수로 표현된 비선형 이진수열인 경우는 주어진 함수를 전개하였을 때 계수가 0이 아닌 항의 수가 선형스팬이다[18]. 수열의 선형스팬으로 알려진 것은 주기가 2^n-1 인 m-수열의 선형스팬은 n 이고, 같은 주기를 갖는 Gold 수열군 내의 각 수열의 선형스팬은 n 또는 $2n$ 이며, 주기가 $2^{2m}-1$ 인 Kasami 수열군의 최대 선형스팬은 $n+m$ 으로 주기에 비해 선형스팬이 작은 수열로 높은 보안수준을 요구하는 스트림 암호 시스템의 키스트림으로 사용되기는 어려운 수열이다[19].

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

이러한 선형스팬이 작은 단점을 보안하기 위하여 제안된 수열로 비선형 이진수열인 GMW수열이 있다. $n=km$이고, r을 이진으로 표현했을 때 Hamming weight를 $wt(r)$로 나타내면 GMW수열의 선형스팬 LS_{GMW}는 식 (7)과 같다[9].

$$LS_{GMW} = n \cdot \left(\frac{n}{m}\right)^{wt(r)-1} \tag{7}$$

식 (4)에서 정의된 No 수열군의 i번째 수열의 선형스팬 $LS_{No}(i)$는 식 (8)과 같다[11].

$$LS_{No}(i) = m \cdot \prod_{j=1}^{R}\left(2^{L_j+1}-1-2\left\lfloor \frac{2^{L_j}-1}{(2^m+\epsilon_i)/g_i} \right\rfloor\right) \tag{8}$$

ϵ_i는 1 또는 -1이고 L_j는 r을 이진으로 표현했을 때 j번째의 1-런의 길이를 나타낸다. No 수열군 내의 수열들은 서로 다른 선형스팬 값을 갖고 있으나 GMW 수열의 경우와 마찬가지로 큰 선형스팬을 가지고 있다. 선형스팬의 관점에서 볼 때 GMW 수열군과 No 수열군은 암호화 시스템에 적합한 키스트림이 될 수 있다.

Ⅲ. 상호상관관계 분석

다음 보조정리는 제안되는 데시메이션에 대한 성질이다.

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

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

(증명)
① $d \equiv 2^{n-1}(3-1) \equiv 2^n \equiv (2^m)^2 \equiv 1 \pmod{2^m-1}$
② $d \equiv 2^{n-1}(-3-1) \equiv (-2) \cdot 2^n \equiv -2 \pmod{2^m+1}$
③ $\gcd(2^{n-1}(3 \cdot 2^m-1), 2^n-1) = \gcd(3 \cdot 2^m-1, 2^n-1)$
$= \gcd(3 \cdot 2^m-1, 2^m+1)$
$= \gcd(4, 2^m+1)$
$= 1.$

$n=2m$일 때 주기가 2^n-1인 임의의 m-수열에 대하여 적당히 a만큼 평행이동한 수열과 m-수열을 적당히 d만큼 데시메이션한 수열을 이용해 생성한 수열군을 S라 하면 다음과 같다.

$$S = \left\{ s_a(t) \mid a \in GF(2^n), 0 \le t < 2^n-1 \right\}$$

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

선형스팬을 크게 하기 위해 S를 이용하여 다음과 같은 새로운 수열군을 제안한다.

$$S^r = \left\{ s_a^r(t) \mid a \in GF(2^n), 0 \le t < 2^n-1 \right\}$$

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

주어진 r에 대하여 $a \in GF(2^n)$이므로 주어진 수열군 S^r의 크기는 2^n이다. 주어진 수열군 S^r에 속한 두 수열 $s_a^r(t)$와 $s_b^r(t)$의 상호상관관계는 식(9)와 같다.

$$C_{ab}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_a^r(t+\tau) + s_b^r(t)} \tag{9}$$

상호상관관계를 분석하기 위하여 주기가 2^n-1인 수열을 $(2^m-1) \times (2^m+1)$배열로 생각한다. 이 때 $Q = \dfrac{2^n-1}{2^m-1} = 2^m+1$라 하자.

<정리 2> $n=2m$, $Q=2^m+1$, $\gcd(r, 2^m-1)=1$이고 $d=2^{n-1}(3 \cdot 2^m-1)$일 때 수열군 S^r의 상호상관관계 $C_{ab}(\tau)$는 S의 상호상관관계와 같고 다음을 만족한다.
$C_{ab}(\tau) \in \{-1-2^m, -1, -1+2^m, -1+2 \cdot 2^m, -1+3 \cdot 2^m\}$

<증명>
식 (9)로부터 다음과 같이 나타낼 수 있다.

$$C_{ab}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s_a^r(t+\tau) + s_b^r(t)} \tag{10}$$
$$= \sum_{t=0}^{2^n-2} (-1)^{Tr_1^m\left\{ \left[Tr_m^n(a\alpha^{t+\tau} + \alpha^{d(t+\tau)}) \right]^r \right\} + Tr_1^m\left\{ \left[Tr_m^n(b\alpha^t + \alpha^{dt}) \right]^r \right\}}$$

주어진 수열을 $(2^m-1) \times (2^m+1)$배열로 생각한다면 t는 $t = t_1 Q + t_2$로 나타낼 수 있고 여기서 $0 \le t_1 \le 2^m-2$, $0 \le t_2 \le 2^m$이다. $GF(2^n)$의 부분체인 $GF(2^m)$의 원시원소 β에 대하여 $\beta = \alpha^Q$라 두면 β는 곱셈군 $GF(2^m)^*$의 원소이다. 보조정리 1의 ① $d \equiv 1 \pmod{2^m-1}$에 의하여 $\alpha^{dQ} = \beta^d = \beta$이므로 식 (10)는 다음과 같다.

$$C_{ab}(\tau) = \sum_{t_1=0}^{2^m-2} \sum_{t_2=0}^{2^m} (-1)^{Tr_1^m\left\{ \beta^r \left(\left[Tr_m^n(a\alpha^{t_2+\tau} + \alpha^{dt_2+d\tau}) \right]^r + \left[Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2}) \right]^r \right) \right\}} \tag{11}$$

식 (11)에서 $u = \beta^{t_1 r}$,
$G(t_2, \tau, r) = \left[Tr_m^n(a\alpha^{t_2+\tau} + \alpha^{dt_2+d\tau}) \right]^r + \left[Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2}) \right]^r$
라 두면 다음과 같다.

$$C_{ab}(\tau) = -Q + \sum_{t_2=0}^{2^m} \sum_{u \in GF(2^m)} (-1)^{Tr_1^m\{u^r G(t_2, \tau, r)\}} \tag{12}$$
$$= -1 + (N-1)2^m \tag{13}$$

여기서 N은 $G(t_2, \tau, r) = 0$을 만족하는 t_2의 개수이다.

$\gcd(r, 2^m-1) = 1$이므로 다음을 만족한다.

$$G(t_2, \tau, r) = 0$$
$$\Leftrightarrow \left[Tr_m^n(a\alpha^{t_2+\tau} + \alpha^{dt_2+d\tau}) \right]^r + \left[Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2}) \right]^r = 0$$
$$\Leftrightarrow \left[Tr_m^n(a\alpha^{t_2+\tau} + \alpha^{dt_2+d\tau}) \right] + \left[Tr_m^n(b\alpha^{t_2} + \alpha^{dt_2}) \right] = 0 \tag{14}$$

따라서 $G(t_2, \tau, r) = 0$이 되는 t_2의 개수는 $G(t_2, \tau, 1) = 0$이 되는 t_2의 개수와 같으므로 수열군 S^r의 상호상관관계는 S의 상호상관관계와 같다.

$GF(2^n)$의 원시원소 α에 대하여 $\alpha = \alpha^{(2^m+1)(1-2^{m-1})} \cdot \alpha^{(2^{m-1})2^{m-1}}$라 표현할 수 있고 $\delta = \alpha^{(2^m+1)(1-2^{m-1})}$, $\gamma = \alpha^{(2^m-1)2^{m-1}}$라 두면, $\alpha = \delta\gamma$로 표현할 수 있다. 이때 $\delta^{2^{m-1}} = 1$, $\gamma^{2^{m-1}+1} = 1$이 되고 δ는 $GF(2^m)$의 원시원소이다. 따라서 $\delta^{2^m} = \delta$, $\gamma^{2^m} = \gamma^{-1}$이

고 보조정리 1에 의해 $\delta^d=\delta$, $\gamma^d=\gamma^{-2}$이므로 $A(\tau)=a\alpha^\tau+b$, $B(\tau)=\alpha^{d\tau}+1$라 두고, $x=\delta^{t_2}\gamma^{-2t_2}$, $y=\gamma^{t_2}$라 두면 $x^{2^m-1}=y^4$을 만족하고 식 (14)은 다음과 같다.

$$x\left(B(\tau)^{2^m}y^4+A(\tau)y^3+A(\tau)^{2^m}y+B(\tau)\right)=0 \quad (15)$$

식 (15)에서 $x\neq 0$이므로 주어진 방정식은 y에 대한 4차 방정식이고 해의 개수는 4이하이다. 즉 식 (13)에서 N은 $N\leq 4$이다.

Ⅳ. 선형스팬 분석

비선형 이진수열군 S^r의 선형스팬은 수열 $s_a^r(t)=Tr_1^m\{[Tr_m^n(a\alpha^t+\alpha^{dt})]^r\}$를 전개하였을 때 $s_a^r(t)=\sum_{i=0}^{2^n-2}b_i\alpha^i$로 나타낼 수 있고 이때 0이 아닌 항의 개수가 주어진 수열의 선형스팬이다[15].

$d=2^{n-1}(3\cdot 2^m-1)$이고, $a\in GF(2^n)$일 때 주어진 수열 $s_a^r(t)=Tr_1^m\{[\,Tr_m^n(a\alpha^t+\alpha^{dt})\,]^r\}$에 대하여 $\alpha=\delta\gamma$라 두고 $\delta^d=\delta$, $\gamma^d=\gamma^{-2}$, $\delta^{2^m}=\delta$, $\gamma^{2^m}=\gamma^{-1}$를 이용하여 $Tr_m^n(a\alpha^t+\alpha^{dt})$를 전개하면 다음과 같다.

$$\begin{aligned}Tr_m^n(a\alpha^t+\alpha^{dt}) &= a\alpha^t+\alpha^{dt}+a^{2^m}\alpha^{2^mt}+\alpha^{2^mdt}\\ &= a\delta^t\gamma^t+\delta^t\gamma^{-2t}+a^{2^m}\delta^t\gamma^{-t}+\delta^t\gamma^{2t}\\ &= \delta^t\gamma^{-2t}(\gamma^{4t}+a\gamma^{3t}a^{2^m}\gamma^t+1)\\ &= x\,g(y)\end{aligned} \quad (16)$$

여기서 $x=\delta^t\gamma^{-2t}$, $y=\gamma^t$이고 $g(y)=y^4+ay^3+a^{2^m}y+1$이다.

$x^{2^m-1}=y^4$이므로 $x^r\,[g(y)]^r=\sum_{l=0}^{4r}c_lx^{\frac{(2^m-1)l}{4}+r}$이다.

그러므로 트레이스함수의 정의에 의해

$$\begin{aligned}Tr_1^m\{[\,xg(y)\,]^r\} &= \sum_{i=0}^{m-1}(x^r[g(y)]^r)^{2^i}\\ &= x^r[g(y)]^r+(x^r[g(y)]^r)^2+\\ &\quad \cdots+(x^r[g(y)]^r)^{2^{m-1}}\end{aligned} \quad (17)$$

이다. 먼저 $(x^r[g(y)]^r)^{2^{s_i}}$와 $(x^r[g(y)]^r)^{2^{s_j}}$항 사이에 소거되는 항이 있는지 살펴보자.

소거되는 항이 있다는 의미는 x의 어떤 두 지수에 대하여

$$\left(\frac{(2^m-1)l}{4}+r\right)2^{s_i}\equiv\left(\frac{(2^m-1)l'}{4}+r\right)2^{s_j}\ (\mathrm{mod}\ 2^n-1) \quad (18)$$

를 만족해야 한다는 것이다. 여기서 $0\leq s_i<s_j\leq m-1$이고 $s=s_j-s_i\ (0<s\leq m-1)$라 두면 식 (18)은 다음과 같다.

$\frac{(2^m-1)l}{4}+r\equiv\left(\frac{(2^m-1)l'}{4}+r\right)2^s\ (\mathrm{mod}\ 2^n-1)$ 이고

$(2^s-1)r\equiv\frac{2^m-1}{4}(l-2^sl')\quad(\mathrm{mod}\,2^n-1)$이다.

이는 $(2^s-1)r\equiv 0\left(\mathrm{mod}\ \frac{2^m-1}{4}\right)$를 의미한다. 그런데 $\gcd(r,2^m-1)=1$이고 2^m-1은 홀수 이므로 $\gcd(r,2^m-1)=\gcd\left(r,\ \frac{2^m-1}{4}\right)=1$이다. 따라서 소거되는 항이 있기 위해서는 $2^s-1\equiv 0\ \left(\mathrm{mod}\ \frac{2^m-1}{4}\right)$이어야 한다.

① $s\leq m-2$인 경우 : $s=m-2$일 때

$2^s-1=2^{m-2}-1=\frac{2^m-4}{4}<\frac{2^m-1}{4}$ 이므로 $2^{m-2}-1\neq 0\ \left(\mathrm{mod}\ \frac{2^m-1}{4}\right)$이다.

② $s=m-1$인 경우 :

$2^s-1=2^{m-1}-1=\frac{2(2^m-1)-2}{4}\equiv-\frac{1}{2}\neq 0\left(\mathrm{mod}\ \frac{2^m-1}{4}\right)$

이다. 따라서 지수가 같은 x항이 없으므로 소거되는 항은 존재하지 않는다. 그러므로 M이 $x^r[g(y)]^r$의 0이 아닌 항의 개수라 할 때 제안된 수열 S^r의 선형스팬 LS는 $LS=mM$이다.

$x^r[g(y)]^r$의 0이 아닌 항의 개수와 $[g(y)]^r$의 0이 아닌 항의 개수가 같으므로 $[g(y)]^r$를 전개하였을 때 0이 아닌 항의 개수에 대하여 살펴본다.

지수 r의 이진 전개표현을 $r=\sum_{i=1}^{w}2^{l_i}$와 같이 나타낼 수 있다. 여기서 w는 r을 이진수로 표현했을 때 Hamming weight이다. 따라서 $[g(y)]^r=\prod_{i=1}^{w}[g(y)]^{2^{l_i}}$이다.

아래 정리는 특별한 r에 대하여 선형스팬을 구한 것이다.

<정리 3> $n=2m$이고 $d=2^{n-1}(3\cdot 2^m-1)$이고 $\gcd(r,2^n-1)=1$이라 하자. r의 이진 전개표현을

$r=\sum_{i=1}^{w}2^{l_i}$라 할 때, $l_{i+1}>l_i+2$을 만족하는 수열 S^r의 선형스팬 LS는 다음과 같다.

$$LS=\begin{cases}2^w m & ,\ a=0\\ 4^w m & ,\ a\neq 0\end{cases} \tag{19}$$

<증명> S^r의 선형스팬 LS는 $LS=mM$이므로 $x^r[g(y)]^r$의 0이 아닌 항의 개수인 M을 구하면 된다. $[g(y)]^r=\prod_{i=1}^{w}[g(y)]^{2^{l_i}}$에서 $g_i(y)=[g(y)]^{2^{l_i}}$라 두면

$$g_i(y)=y^{4\cdot 2^{l_i}}+a^{2^{l_i}}y^{3\cdot 2^{l_i}}+a^{2^{m+l_i}}y^{2^{l_i}}+1 \tag{20}$$

이다. 그러므로 $a=0$이면 $g_i(y)$의 항의 개수는 2이고 $a\neq 0$일 때 $g_i(y)$의 항의 개수는 4이다. $l_{i+1}>l_i+2$일 때 $g_i(y)$와 $g_{i+1}(y)$의 항에 대하여 지수가 같은 경우는 존재하지 않으므로 r의 Hamming weight가 w일 때 $[g(y)]^r=\prod_{i=1}^{w}[g(y)]^{2^{l_i}}$의 0이 아닌 항의 개수는 $a=0$일 때 2^w이고, $a\neq 0$일 때 4^w이다. 따라서 주어진 수열군 S^r의 선형스팬은 $a=0$일 때 $2^w m$이고 $a\neq 0$일 때 $4^w m$이다.

<예제> $n=10, m=5, a=\alpha^{31}, b=\alpha^3$, $d=48640\equiv 559\ (\mathrm{mod}\ 1023)$, $r=9(=1001)$일 때 $s_a^r(t)$와 $s_b^r(t)$에 대한 $C_{ab}(\tau)$의 분포는 다음과 같다.

$C_{ab}(\tau)$:	-33	-1	31	63	95
발생횟수:	338	408	234	22	20

또한 선형스팬은 $LS=4^2\times 5=80$이다.

V. 결 론

본 논문에서는 GMW수열과 Gold 계열 수열의 확장으로 큰 선형스팬을 갖는 비선형 이진수열을 제안하였다. 또한 제안한 비선형 이진수열의 상호상관관계를 분석하여 제안한 수열군이 5값 상호상관관계를 가짐을 보였다. 이러한 수열은 낮은 상호상관관계값을 가지면서 수열군의 크기도 크고 선형스팬도 기존의 Gold 계열의 수열보다 더 크므로 통신 및 보안 시스템의 응용에 적합할 것으로 사료된다.

참고문헌

[1] R.A. Scholtz, "The origins of spread-spectrum communications," IEEE Trans. Commun., vol. COM-30, pp. 822-854, 1982.

[2] 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.

[3] D.V. Sarwarte and M.B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," Proc. IEEE., vol. 68, no. 5, pp. 593-620, 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] Y. Niho, Multi-valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences, Ph.D. thesis, University of Southern California, 1972.

[7] R. Gold, "Maximal recursive sequences with 3-valued cross-correlation functions," IEEE Trans. Inf. Theory, vol 14, pp. 154-156, 1967.

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

[10] 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.

[11] 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.
[12] 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.
[13] P. Rosendahl, Niho type cross-correlation functions and related equations, Ph.D. thesis, Turku center for computer science, 2004.
[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.
[15] E.L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," IEEE Trans. Inform. Theory, vol. IT-22, no. 6, pp. 732-736, 1976.
[16] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press 1997.
[17] 조성진, 유한체 및 그 응용, 교우사, 2007.
[18] 최언숙, 조성진, "최적의 상호상관관계를 갖는 이진 수열의 설계," 한국전자통신학회, 제6권, 제4호, pp.539-544, 2011.
[19] 노종선, "PN 시퀀스의 암호학적인 비도 특성," 통신정보보호학회지, 제3권, 제4호, pp. 7-14, 1993.

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 응용수학과 교수
※주 관심분야 : 셀룰라 오토마타론, 정보보호

김한두(Han-Doo Kim)

1982년 고려대학교 수학과 이학사
1984년 고려대학교 수학과 이학석사
1988년 고려대학교 수학과 이학박사
1989년 ~ 현재 인제대학교 응용수학과 교수
※ 관심분야 : 셀룰라 오토마타론, 전산수학