5값 상호상관함숫값과 높은 선형스팬을 갖는 새로운 데시메이션들

김진경* · 조성진** · 김한두*** · 최언숙****

New decimations with 5-level cross-correlation and large linear span

Jin-Gyoung Kim* · Song-Jin Cho** · Han-Doo Kim*** · Un-Sook Choi****

요 약

본 논문에서는 $n=2m$, $m=4k\,(k\geq 2)$일 때 새로운 데시메이션 $d=3\cdot 2^m-2$에 대한 상호상관함숫값을 구하는 방법을 제시하고 특별한 경우의 제안된 수열군에 속한 수열들의 선형스팬을 계산한다.

ABSTRACT

In this paper we give a proof for finding the values of the cross-correlation function $C_d(\tau)$ when $d=3\cdot 2^m-2$, where $n=2m$, $m=4k\,(k\geq 2)$. And the linear span of the sequences in the proposed sequence family are derived in the some cases.

키워드

트레이스 함수, 상호상관관계, 선형스팬, 데시메이션, 수열

trace function, cross-correlation, linear span, decimations, sequences

Ⅰ. 서 론

의사난수열(pseudorandom sequence)은 디지털 통신 시스템에서 사용되고 있다. 의사난수열을 설계하는데 있어서 낮은 상호상관관계 값, 큰 선형스팬, 큰 수열군, 구현의 용이성 등이 바람직한 성질이다[1-3]. 낮은 상호상관관계 값을 갖는 수열군을 설계하는 것이 중요하지만 수열을 분석하는 것이 얼마나 어려운지를 알려주는 중요한 척도인 선형스팬을 높이는 것도 중요한 문제이다. 잘 알려진 수열군으로 m-수열, GMW 수열, Kasami 수열, No 수열 등이 있고, 트레이스를 이용한 여러 가지 수열들에 대한 연구가 이루어졌다[4-14]. 본 논문에서는 $n=2m$, $m=4k\,(k\geq 2)$일 때 낮은 상호상관함숫값을 갖는 새로운 데시메이션 $d=3\cdot 2^m-2$에 대한 상호상관함숫값을 구하는 방법을 제시하고 특별한 경우의 제안된 수열군에 속한 수열들의 선형스팬을 계산한다.

Ⅱ. 배경지식 및 기존연구

트레이스 함수(trace function)는 의사난수열인 m-

* 부경대학교 응용수학과(5892587@pknu.ac.kr)
** 교신저자 : 부경대학교 응용수학과(sjcho@pknu.ac.kr)
*** 인제대학교 컴퓨터응용과학부(mathkhd@inje.ac.kr)
**** 동명대학교 자율전공학부(choies@tu.ac.kr)
접수일자 : 2012. 11. 15 심사(수정)일자 : 2012. 12. 29 게재확정일자 : 2013. 02. 20

수열의 설계와 분석을 위한 중요한 수학적 도구이다. 이진수열들을 트레이스 함수로 표현하면 분석이 용이하다. $GF(2^n)$를 2^n개의 원소를 가진 유한체라 하고, $GF(2^n)^* = GF(2^n) \setminus \{0\}$ 라 하자. 1보다 큰 정수 k에 대하여 $n = km$라 하고, 차수가 n인 원시다항식(primitive polynomial) $f(x)$의 원시근을 $\alpha(\in GF(2^n))$라 하자. 그러면 트레이스 함수 $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$는 다음과 같다[15,16].

$$Tr_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^i}$$

함수 $Tr_m^n : GF(2^n) \rightarrow GF(2^m)$는 다음과 같은 성질을 갖는다. $GF(2^n)$의 임의의 원소 x, y와 $GF(2^m)$의 임의의 원소 a, b에 대하여 다음이 성립한다.

(a) $Tr_m^n(ax+by) = aTr_m^n(x) + bTr_m^n(y)$.

(b) $Tr_1^n(x) = Tr_1^m\left[Tr_m^n(x)\right]$.

(c) $Tr_m^n\left(x^{2^m}\right) = Tr_m^n(x)$

(d) Tr_m^n는 전사함수이다.

(e) $GF(2^m)$의 임의의 원소 c에 대하여 $Tr_m^n(x) = c$를 만족하는 x는 균등하게 2^{n-m}개이다.

수열군에 속한 수열들의 특성을 파악하려면 수열군에 속한 수열들 사이의 상관관계의 특성인 상호상관관계를 고려해야 한다. 두 이진수열 $u(t)$와 $v(t)$ $(t = 0, 1, 2, \cdots)$에 대하여 상호상관관계함숫값은 다음과 같이 정의된다.

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

여기서 $u(t)$와 $v(t)$의 주기는 $2^n - 1$이다.

의사난수열을 분석하는 것이 얼마나 어려운지를 알려주는 척도로 사용되는 개념이 수열의 선형스팬(linear span)이다. 선형스팬이 클수록 보안수준이 높다. 주어진 수열이 선형 이진수열이면 그 이진수열을 생성하는 최소다항식의 차수가 그 수열의 선형스팬이다. 그런데 트레이스 함수로 표현된 비선형 이진수열의 선형스팬은 주어진 함수를 전개했을 때 계수가 0이 아닌 항의 개수이다[17].

III. 상호상관함숫값에 대한 기본 성질

이 절에서는 $n = 2m$, $m = 4k(k \geq 2)$인 경우에 대하여 새로운 데시메이션 $d = 3 \cdot 2^m - 2$과 $\gcd(r, 2^m - 1) = 1$인 r을 이용하여 주기가 $2^n - 1$인 임의의 m-수열에 대하여, 그 m-수열을 적당히 이동한 수열과 d만큼 데시메이션한 수열을 이용해 선형스팬이 큰 다음과 같이 정의된 수열군의 상호상관함숫값을 계산한다.

$$S_r = \left\{ S_a^r(t) \mid a \in GF(2^n), 0 \leq t \leq 2^n - 2 \right\},$$
$$s_a^r(t) = Tr_1^m\left\{ \left[Tr_m^n\left(a\alpha^t + \alpha^{dt}\right) \right]^r \right\}.$$

주어진 r에 대하여 이 수열군의 크기는 2^n개다.

보조정리 1> $n = 2m, m = 4k$, $d = 3 \cdot 2^m - 2$일 때 다음이 성립한다.

(i) $d \equiv 1 \pmod{2^m - 1}$

(ii) $d \equiv -5 \pmod{2^m + 1}$

(iii) $\gcd(d, 2^n - 1) = 1$

(증명) (i) $d = 3(2^m - 1) + 1$이므로 성립한다.

(ii) $d = 3(2^m + 1) - 5$이므로 성립한다.

(iii) (i)에 의해 $\gcd(d, 2^m + 1) = 1$이 성립함을 보이면 된다. $d = 3(2^m + 1) - 5$이므로 $\gcd(d, 2^m + 1) = \gcd(5, 2^m + 1)$이고 $2^m + 1 = (2^4)^k + 1 \equiv 2 \pmod 5$이므로 $\gcd(d, 2^n - 1) = 1$이다.

보조정리 2> $n = 2m$일 때, $GF(2^n)$의 임의의 원시원소 α는 다음과 같이 나타낼 수 있다.

$$\alpha = \delta\gamma.$$

여기서 δ, γ는 $\delta^{2^m-1} = 1, \gamma^{2^m+1} = 1$을 만족한다. 그리고 δ는 $GF(2^m)$의 원시원소이다.

(증명) $\delta = \alpha^{(2^m+1)(1-2^{m-1})}, \gamma = \alpha^{(2^m-1)2^{m-1}}$로 두면 $\alpha = \delta\gamma$이고 $\delta^{2^m-1} = 1, \gamma^{2^m+1} = 1$이다. i가 $1 \leq i < 2^m - 1$인 정수일 때 $\delta^i = \alpha^{(2^m+1)(1-2^{m-1})i} = 1$이므로 $2^n - 1$는 $(2^m + 1)(1 - 2^{m-1})i$ 의 약수이다. 그러면 $2^m - 1 \mid (1 - 2^{m-1})i$이고, $2^m - 1 = 2(2^{m-1} - 1) + 1$이므로 $\gcd(2^m - 1, 2^{m-1} - 1) = 1$이다. 그러므로 $2^m - 1 \mid i$이다. 그런데 $1 \leq i < 2^m - 1$이므로 모순이다. 그러므로 δ는 $GF(2^m)$의 원시원소이다.

보조정리 2에 의해 $\delta^{2^m}=\delta,\ \gamma^{2^m}=\gamma^{-1}$이다. 그리고 보조정리 1에 의해 $\delta^d=\delta,\ \gamma^d=\gamma^{-5}$이다.

두 수열 $s_a^r(t)$와 $s_b^r(t)$의 상호상관함수 $C_{a,b}(\tau)$는 다음과 같이 정의된다.

$$C_{a,b}(\tau)=\sum_{t=0}^{2^n-2}(-1)^{s_a^r(t+\tau)+s_b^r(t)}.$$

여기서 $s_a^r(t+\tau)+s_b^r(t)$

$=Tr_1^m\left\{\left[Tr_m^n\left(a\alpha^{t+\tau}+\alpha^{d(t+\tau)}\right)\right]^r+\left[Tr_m^n\left(b\alpha^t+\alpha^{dt}\right)\right]^r\right\}$

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

$s_b^r(t)=Tr_1^m\left\{\left[Tr_m^n\left(b\alpha^t+\alpha^{dt}\right)\right]^r\right\}$의 상호상관함수는

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

이고, 여기서 $Q=2^m+1$일 때 t를 t_1Q+t_2 $(0\le t_1\le 2^m-2,\ 0\le t_2\le 2^m)$로 나타내면 위 식은다음과 같다.

$$C_{a,b}(\tau)=\sum_{t_1=0}^{2^n-2}\sum_{t_2=0}^{2^m}\left[(-1)^{Tr_1^m\left\{\left[Tr_m^n\left(a\alpha^{t_1Q+t_2+\tau}+\alpha^{d(t_1Q+t_2+\tau)}\right)\right]^r\right\}}\right.$$
$$\left.\times(-1)^{Tr_1^m\left\{\left[Tr_m^n\left(b\alpha^{t_1Q+t_2}+\alpha^{d(t_1Q+t_2)}\right)\right]^r\right\}}\right]. \quad (1)$$

$\beta=\alpha^Q$로 두면 $\alpha^{dQ}=\beta^d=\beta$이므로 (1)은 다음과 같다.

$$C_{a,b}(\tau)=\sum_{t_1=0}^{2^n-2}\sum_{t_2=0}^{2^m}(-1)^{Tr_1^m\left\{\beta^{t_1r}H(t_2,\tau,r)\right\}},$$

$$H(t_2,\tau,r)=\left[Tr_m^n\left(a\alpha^{t_2+\tau}+\alpha^{d(t_2+\tau)}\right)\right]^r+\left[Tr_m^n\left(b\alpha^{t_2}+\alpha^{dt_2}\right)\right]^r. \quad (2)$$

여기서 $z=\beta^{t_1}$로 두면 $z\in GF(2^m)^*$이므로 다음이 성립한다.

$$\begin{aligned}C_{a,b}(\tau)&=\sum_{t_2=0}^{2^n}\sum_{z\in GF(2^m)^*}(-1)^{Tr_1^m\left\{z^rH(t_2,\tau,r)\right\}} \quad (3)\\&=-Q+\sum_{t_2=0}^{2^m}\sum_{z\in GF(2^m)}(-1)^{Tr_1^m\left(z^rH(t_2,\tau,r)\right)}\\&=-Q+2^mN(t_2,\tau,r)\\&=-1+2^m(N(t_2,\tau,r)-1),\end{aligned}$$

여기서

$$N(t_2,\tau,r)=\left|\left\{t_2\mid 0\le t_2\le 2^m,\ H(t_2,\tau,r)=0\right\}\right|.$$

$\gcd(r,2^m-1)=1$이므로 $r^{-1}\pmod{2^m-1}$이 존재하여 다음이 성립한다.

$$H(t_2,\tau,r)=0$$

$$\Leftrightarrow\ \left[Tr_m^n\left(a\alpha^{t_2+\tau}+\alpha^{d(t_2+\tau)}\right)\right]^r=\left[Tr_m^n\left(balpha^{t_2}+\alpha^{dt_2}\right)\right]^r \quad (4)$$

$$\Leftrightarrow\ Tr_m^n\left(a\alpha^{t_2+\tau}+\alpha^{d(t_2+\tau)}\right)=Tr_m^n\left(b\alpha^{t_2}+\alpha^{dt_2}\right) \quad (5)$$

그러므로 (5)를 만족하는 $t_2(0\le t_2\le 2^m)$의 개수는 $H(t_2,\tau,1)=0$을 만족하는 $t_2(0\le t_2\le 2^m)$의 개수와 같다. 즉

$$\begin{aligned}N(t_2,\tau,r)&=N(t_2,\tau,1)\\&=\left|\left\{t_2\mid 0\le t_2\le 2^m,\ H(t_2,\tau,1)=0\right\}\right|.\end{aligned}$$

위 사실로부터 다음을 알 수 있다.

정리 3> $n=2m,\ d\equiv 1\pmod{2^m-1}$ 일 때 수열군 $S_r=\left\{S_a^r(t)\mid a\in GF(2^n),\ 0\le t\le 2^n-2\right\}$ 에 속한 수열들 $s_a^r(t)=Tr_1^m\left\{\left[Tr_m^n\left(a\alpha^t+\alpha^{dt}\right)\right]^r\right\}$의 상호상관함숫값은 수열들 $s_a^1(t)=Tr_1^n\left(a\alpha^t+\alpha^{dt}\right)$의 상호상관함숫값과 같다.

(증명) 수열들 $s_a^r(t)=Tr_1^m\left\{\left[Tr_m^n\left(a\alpha^t+\alpha^{dt}\right)\right]^r\right\}$의 상호상관함숫값은 $C_{a,b}(\tau)=-1+2^m(N(t_2,\tau,r)-1)$이고 위에서 보였듯이 $N(t_2,\tau,r)=N(t_2,\tau,1)$이므로 $C_{a,b}(\tau)=-1+2^m(N(t_2,\tau,1)-1)$이다.

이 값은 수열 $s_a^1(t)=Tr_1^n\left(a\alpha^t+\alpha^{dt}\right)$의 상호상관함숫값이므로 수열들 $S_a^r(t)$의 상호상관함숫값은 수열들 $S_a^1(t)$의 상호상관함숫값과 같다.

정리 4> $n=2m,\ m=4k,\ \gcd(r,2^m-1)=1,$
$d=3\cdot 2^m-2$에 대하여 정의된 수열군
$S_r=\left\{S_a^r(t)\mid a\in GF(2^n),\ 0\le t\le 2^n-2\right\}$,
$s_a^r(t)=Tr_1^m\left\{\left[Tr_m^n\left(a\alpha^t+\alpha^{dt}\right)\right]^r\right\}$
의 상호상관함숫값은
$C_{a,b}(\tau)\in\{-1-2^m,-1,-1+2^m,-1+2\cdot 2^m,$
$-1+4\cdot 2^m\}$
이다.

(증명) 두 수열 $s_a^r(t)$와 $s_b^r(t)$의 상호상관함숫값은 $s_a^1(t)$와 $s_b^1(t)$의 상호상관함숫값과 같다. $s_a^1(t)$를 간단히 $s_a(t)$로 나타내기로 한다. 그러면 두 수열 $s_a(t)$와 $s_b(t)$는 다음과 같이 나타낼 수 있다.

$$s_a(t) = Tr_1^n(a\alpha^t + \alpha^{dt}),\ \ s_b(t) = Tr_1^n(b\alpha^t + \alpha^{dt}).$$

그리고 두 수열 $s_a(t)$와 $s_b(t)$의 상호상관함수는

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

이다. 여기서

$$s_a(t+\tau)+s_b(t) = Tr_1^n(a\alpha^{t+\tau} + \alpha^{d(t+\tau)} + b\alpha^t + \alpha^{dt})$$

이고, $Q=2^m+1$일 때 t를 $t_1Q+t_2(0 \le t_1 \le 2^m-2, 0 \le t_2 \le 2^m)$로 나타내면 위 식은 다음과 같다.

$$\begin{aligned} &Tr_1^n(a\alpha^{t+\tau} + \alpha^{d(t+\tau)} + b\alpha^t + \alpha^{dt}) \\ &= Tr_1^n\{a\alpha^{t_1Q+t_2+\tau} + \alpha^{d(t_1Q+t_2+\tau)} + b\alpha^{t_1Q+t_2} + \alpha^{d(t_1Q+t_2)}\} \\ &= Tr_1^n\{(a\alpha^\tau + b)\alpha^{t_1Q+t_2} + (\alpha^{d\tau}+1)\alpha^{d(t_1Q+t_2)}\}. \end{aligned} \tag{6}$$

여기서 $A(\tau)=a\alpha^\tau+b$라 두고 $B(\tau)=\alpha^{d\tau}+1$라 두면 (6)은 다음과 같다.

$$\begin{aligned} &Tr_1^n\{(a\alpha^\tau+b)\alpha^{t_1Q+t_2} + (\alpha^{d\tau}+1)\alpha^{d(t_1Q+t_2)}\} \\ &= Tr_1^n\{A(\tau)\alpha^{t_1Q+t_2} + B(\tau)\alpha^{d(t_1Q+t_2)}\} \end{aligned} \tag{7}$$

여기서 $\beta=\alpha^Q$라 두면 $\beta^{2^m-1}=(\alpha^Q)^{2^m-1}=1$이므로 $\beta \in GF(2^m)$이고 β는 $GF(2^m)$의 원시원소이다. 그러면 (7)은 다음과 같다.

$$\begin{aligned} &Tr_1^n\{A(\tau)\alpha^{t_1Q+t_2} + B(\tau)\alpha^{d(t_1Q+t_2)}\} \\ &\quad = Tr_1^n\{A(\tau)\beta^{t_1}\alpha^{t_2} + B(\tau)\beta^{dt_1}\alpha^{dt_2}\} \\ &\quad = Tr_1^m\left[Tr_m^n\{A(\tau)\beta^{t_1}\alpha^{t_2} + B(\tau)\beta^{dt_1}\alpha^{dt_2}\}\right] \end{aligned} \tag{8}$$

이때 $\beta^d = \beta^{3\cdot 2^m-2} = \beta^{3(2^m-1)+1} = \beta$이므로 (8)은 다음과 같다.

$$\begin{aligned} &Tr_1^m\left[Tr_m^n\{A(\tau)\beta^{t_1}\alpha^{t_2} + B(\tau)\beta^{dt_1}\alpha^{dt_2}\}\right] \\ &\quad = Tr_1^m\left[\beta^{t_1}Tr_m^n\{A(\tau)\alpha^{t_2} + B(\tau)\alpha^{dt_2}\}\right] \end{aligned} \tag{9}$$

$\alpha=\delta\gamma$, $\delta^d=\delta$, $\gamma^d=\gamma^{-5}$을 이용하면 (9)는 다음과 같다.

$$\begin{aligned} &Tr_1^m\left[\beta^{t_1}Tr_m^n\{A(\tau)\alpha^{t_2} + B(\tau)\alpha^{dt_2}\}\right] \\ &= Tr_1^m\left[\beta^{t_1}Tr_m^n\{A(\tau)\delta^{t_2}\gamma^{t_2} + B(\tau)\delta^{dt_2}\gamma^{dt_2}\}\right] \\ &= Tr_1^m\left[\beta^{t_1}\delta^{t_2}Tr_m^n\{A(\tau)\gamma^{t_2} + B(\tau)\gamma^{-5t_2}\}\right] \\ &= Tr_1^m\left[\beta^{t_1}\delta^{t_2}Tr_m^n\{\gamma^{-5t_2}(A(\tau)\gamma^{6t_2} + B(\tau))\}\right] \end{aligned} \tag{10}$$

그러므로 $C_{ab}(\tau)$는 다음과 같다.

$$\begin{aligned} C_{ab}(\tau) &= \sum_{t=0}^{2^n-2}(-1)^{s_a(t+\tau)+s_b(t)} \\ &= \sum_{t_1=0}^{2^m-2}\sum_{t_2=0}^{2^m}(-1)^{Tr_1^m[\beta^{t_1}\delta^{t_2}Tr_m^n\{\gamma^{-5t_2}(A(\tau)\gamma^{6t_2}+B(\tau))\}]} \\ &= -(2^m+1) \\ &\quad + \sum_{t_2=0}^{2^m}\sum_{z\in GF(2^m)}(-1)^{Tr_1^m[z\,\delta^{t_2}Tr_m^n\{\gamma^{-5t_2}(A(\tau)\gamma^{6t_2}+B(\tau))\}]} \\ &= 2^mN-(2^m+1) \\ &= -1+(N-1)2^m \end{aligned} \tag{11}$$

여기서 $z=\beta^{t_1}$이고 N은 다음과 같다.

$$N = |\{t_2 \in \{0,1,2,\cdots,2^m\} \mid Tr_m^n\{\gamma^{-5t_2}(A(\tau)\gamma^{6t_2} + B(\tau))\}=0\}|.$$

그러면

$$\begin{aligned} &Tr_m^n\{\gamma^{-5t_2}(A(\tau)\gamma^{6t_2}+B(\tau))\} \\ &\quad = \gamma^{-5t_2}(A(\tau)\gamma^{6t_2}+B(\tau)) \\ &\qquad + \gamma^{-5t_2 2^m}(A(\tau)^{2^m}\gamma^{6t_2 2^m} + B(\tau)^{2^m}) \\ &\quad = \gamma^{-5t_2}(A(\tau)\gamma^{6t_2}+B(\tau)) \\ &\qquad + \gamma^{5t_2}(A(\tau)^{2^m}\gamma^{-6t_2} + B(\tau)^{2^m}) \\ &\quad = B(\tau)^{2^m}\gamma^{5t_2} + A(\tau)\gamma^{t_2} \\ &\qquad + A(\tau)^{2^m}\gamma^{-t_2} + B(\tau)\gamma^{-5t_2} \\ &\quad = \gamma^{-5t_2}(B(\tau)^{2^m}\gamma^{10t_2} + A(\tau)\gamma^{6t_2} \\ &\qquad + A(\tau)^{2^m}\gamma^{4t_2} + B(\tau)). \end{aligned} \tag{12}$$

그러므로 다음을 만족하는 $t_2 \in \{0,1,2,\cdots,2^m\}$의 개수를 구한다.

$$B(\tau)^{2^m}\gamma^{10t_2} + A(\tau)\gamma^{6t_2} + A(\tau)^{2^m}\gamma^{4t_2} + B(\tau) = 0 \tag{13}$$

여기서 $x=\gamma^{2t_2}$라 두면 (13)은 다음과 같다.

$$B(\tau)^{2^m}x^5 + A(\tau)x^3 + A(\tau)^{2^m}x^2 + B(\tau) = 0 \tag{14}$$

(14)가 5차방정식이므로 $C_{ab}(\tau)$는 기껏해야 6값이다. $S=\{1,\gamma,\gamma^2,\cdots,\gamma^{2^m}\}$로 두면 S는 곱셈연산에 대하여 순환군을 이룬다. 그러므로 (14)의 해는 S의 원소이다. (14)가 S에서 4개의 해를 갖는 경우가 생기지 않는다는 것을 보이도록 한다. 만약 a,b,c,d가 S에 속한 (14)의 해라면 (14)의 4차항의 계수가 0이므로 다섯 번째 해를 e라 할 때 $a+b+c+d+e=0$이므로 e도 S의 원소이다. 그런데 (14)가 중근을 가진다면 다음 식을 만족한다.

$$B(\tau)^{2^m}x^4+A(\tau)x^2=0 \quad 즉 \quad B(\tau)^{2^m}x^2+A(\tau)=0.$$

즉 중근을 가진다면 $x^2=\dfrac{A(\tau)}{B(\tau)^{2^m}}$이 성립해야 하므로 (14)는 다음과 같다.

$$A(\tau)^{2^{m+1}}+B(\tau)^{2^{m+1}}=0$$

따라서 $A(\tau)=B(\tau)$이 되고 이를 본 식에 대입하면 다음과 같다.

$$A(\tau)^{2^m}x^5+A(\tau)x^3+A(\tau)^{2^m}x^2+A(\tau)=0$$

즉 $\left(A(\tau)^{2^m}x^2+A(\tau)\right)(x^3+1)=0$

$x^3+1=(x+a)(x+b)(x+c)$와 같이 된다면 $a,b,c\in S$이므로 $a=\gamma^i, b=\gamma^j, c=\gamma^l (0\le i<j<l\le 2^m)$로 놓을 수 있다. $b=\gamma^{j-i}a$, $c=\gamma^{l-i}a$이므로 $u=\gamma^{j-i}, v=\gamma^{l-i}$라 두면 $b=ua, c=va$이고 $u+v=1, uv=u+v=1$이다. 그러면 u,v는 $w^2+w+1=0$의 두 근이므로 $u^3=v^3=1$이고 $u^2=v, v^2=u$이다. 그런데 $u^{2^{m+1}}=v^{2^{m+1}}=1$이므로 $3\mid 2^m+1$이어야 한다. $3\mid 2^m+1$을 만족하기 위해서는 m이 홀수여야 하지만 m은 짝수이므로 성립하지 않는다. 따라서 중근을 갖지 않는다. 즉 $N=4$일 수 없으므로 $-1+3\cdot 2^m$가 발생하지 않는다. 그러므로 0,1,2,3 또는 5개의 근을 가지므로 $C_{ab}(\tau)=-1+(N-1)2^m$에 의하여 상호상관관계 함숫값이 다음과 같은 5값이다.

$$-1-2^m, -1, -1+2^m, -1+2\cdot 2^m, -1+4\cdot 2^m$$

Ⅳ. 주어진 수열의 선형스팬

비선형 이진수열군 S_r에 속한 수열들의 선형스팬은 수열 $s_a^r(t)=Tr_1^m\left\{\left[Tr_m^n(a\alpha^t)+Tr_m^n(\alpha^{dt})\right]^r\right\}$을 전개하여 $s_a^r(t)=\sum_{i=0}^{2^n-2}b_i\alpha^{it}\,(b_i\in GF(2))$로 나타냈을 때 0이 아닌 항의 개수이다[17]. $n=2m$, $m=4k$, $k\ge 2$이고 $d=3\cdot 2^m-2$일 때, $\gcd(r,2^m-1)=1$이고 $\gcd(d,2^n-1)=1$이다. 각 $a\in GF(2^n)$에 대하여 보조정리 2를 이용하여 주어진 수열 $s_a^r(t)=Tr_1^m\left\{\left[Tr_m^n(a\alpha^t)+Tr_m^n(\alpha^{dt})\right]^r\right\}$의 안쪽 트레이스를 계산하면 다음과 같다.

$$\begin{aligned} Tr_m^n(a\alpha^t+\alpha^{dt}) &= a\alpha^t+\alpha^{dt}+a^{2^m}\alpha^{t\cdot 2^m}+\alpha^{dt\cdot 2^m} \\ &= a\delta^t\gamma^t+\delta^{dt}\gamma^{dt}+a^{2^m}\delta^{t\cdot 2^m}\gamma^{t\cdot 2^m} \\ &\quad +\delta^{dt\cdot 2^m}\gamma^{dt\cdot 2^m} \\ &= a\delta^t\gamma^t+\delta^t\gamma^{-5t}+a^{2^m}\delta^t\gamma^{-t}+\delta^t\gamma^{5t} \\ &= \delta^t\gamma^{-5t}\left(\gamma^{10t}+a\gamma^{6t}+a^{2^m}\gamma^{4t}+1\right) \\ &= xg(y) \end{aligned} \tag{15}$$

여기서 $x=\delta^t\gamma^{-5t}$, $y=\gamma^{2t}$, $g(y)=y^5+ay^3+a^{2^m}y^2+1$이다. $x^{2^m-1}=y^5$이므로 $y=x^{\frac{2^m-1}{5}}$이다. $m=4k$일 때 $\dfrac{2^m-1}{5}$은 정수이다.

$x^r g(y)^r=\sum_{l=0}^{5r}c_l x^{\frac{(2^m-1)l}{5}+r}$이므로

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

이다. 여기서 $0\le s_i<s_j\le m-1$인 임의의 두 항 $\left(x^r g(y)^r\right)^{2^{s_i}}$와 $\left(x^r g(y)^r\right)^{2^{s_j}}$을 전개했을 때 소거되는 항이 있는지를 조사해보자.

$$\left(x^r g(y)^r\right)^{2^{s_i}}=\sum_{l=0}^{5r}c_l^{2^{s_i}}x^{\left(\frac{(2^m-1)l}{5}+r\right)2^{s_i}},$$

$$\left(x^r g(y)^r\right)^{2^{s_j}}=\sum_{l=0}^{5r}c_l^{2^{s_j}}x^{\left(\frac{(2^m-1)l}{5}+r\right)2^{s_j}}$$

이므로 소거되는 항이 있다면 다음이 성립해야 한다.

$$\left(\frac{(2^m-1)l}{5}+r\right)2^{s_i}\equiv\left(\frac{(2^m-1)l'}{5}+r\right)2^{s_j}\pmod{2^n-1} \tag{16}$$

$s=s_j-s_i$라 두면 $0<s\le m-1$이고

$$(2^s-1)r\equiv\frac{2^m-1}{5}(l-2^s l')\pmod{2^n-1}$$

이다. 그런데 $\frac{2^m-1}{5}\mid 2^n-1$이므로 $(2^s-1)r\equiv 0\left(\mathrm{mod}\ \frac{2^m-1}{5}\right)$이고 $\gcd(r,2^m-1)=1$이므로 $\gcd(r,=\frac{2^m-1}{5})=1$이다. 그러므로 $2^s-1\equiv 0\left(\mathrm{mod}\ \frac{2^m-1}{5}\right)$이다.

$s\le m-3$인 경우

$$0<2^s-1\le 2^{m-3}-1=\frac{5(2^{m-3}-1)}{5}$$
$$=\frac{2^m-3\cdot 2^{m-3}-5}{5}<\frac{2^m-1}{5}$$

이므로 모순이다. $s=m-2$인 경우

$$2^{m-2}-1=\frac{5(2^{m-2}-1)}{5}=\frac{(2^m-1)+2^{m-2}-4}{5}$$

이고 $\frac{2^{m-2}-4}{5}\not\equiv 0\ \left(\mathrm{mod}\ \frac{2^m-1}{5}\right)$이므로 모순이다.

$s=m-1$인 경우

$$2^{m-1}-1=\frac{5(2^{m-1}-1)}{5}=\frac{2(2^m-1)}{5}+\frac{2^{m-1}-3}{5}$$

이고 $\frac{2^{m-3}-3}{5}\not\equiv 0\ \left(\mathrm{mod}\ \frac{2^m-1}{5}\right)$이므로 모순이다.

x의 지수가 같은 항이 나타나지 않으므로 소거되는 항은 없으므로 선형스팬은 $x^r g(y)^r$의 0이 아닌 항의 개수의 m배이다. $x^r g(y)^r$의 0이 아닌 항의 개수와 $x^r g(y)^r$의 0이 아닌 항의 개수가 같으므로 $[g(y)]^r$의 0이 아닌 항의 개수를 구하면 된다. 지수 r을 이진 전개로 다음과 같이 나타냈다고 하자. $r=\sum_{i=1}^{w}2^{l_i}$. (여기서 w는 r을 이진 전개로 나타냈을 때 Hamming weight이다.) 그러면

$$[g(y)]^r=\prod_{i=1}^{w}[g(y)]^{2^{l_i}}.$$

정리 5> $n=2m$, $d=3\cdot 2^m-2(m=8k)$, $\gcd(r,2^n-1)=1$이라 하고, r의 이진표현을 $r=\sum_{i=1}^{w}2^{l_i}$ (단, $0=l_1<l_2<\cdots<l_w\le m-1$)라 하자. $l_{i+1}>l_i+1$ 인 경우 S_r의 이진수열의 선형복잡도 L은 다음과 같다.

$$L=\begin{cases}m2^w\ \mathrm{if}\ a'=0\\ m4^w\ \mathrm{if}\ a'\neq 0\end{cases}\quad \text{단, } a'=a^{2^{l_i}}.$$

(증명) $a=a^{2^{l_i}}, z=y^{2^{l_i}}$라 하면 $g_i(y)=z^5+a'z^3$ $+(a')^{2^m}z^2+1$이고 편의상 이를 $G_i(z)$로 나타낸다. 그러면

$$G_i(z)=\begin{cases}z^5+1, & a'=0\\ z^5+a'z^3+(a')^{2^m}z^2+1, & a'\neq 0\end{cases}$$

그러므로 $G_i(z)$의 항의 개수는 $a'=0$이면 2개이고 $a'\neq 0$이면 4개이다. 따라서 S_r의 이진수열 $s_a^r(t)$의 선형복잡도 L은 다음과 같다.

$$L=\begin{cases}m2^w\ \mathrm{if}\ a'=0\\ m4^w\ \mathrm{if}\ a'\neq 0\end{cases}\quad \text{단, } a'=a^{2^{l_i}}.$$

V. 결 론

본 논문에서는 $n=2m$, $m=4k$ $(k\ge 2)$일 때 새로운 데시메이션 $d=3\cdot 2^m-2$으로 생성된 주기 2^n-1인 새로운 m-수열들의 상호상관함숫값이 5개임을 보이고 선형스팬이 $4^w\cdot m$까지 높아짐을 보였다.

참고 문헌

[1] M. K. Simon, J. K. Omura, R.A. Sholtz and B. K. Levitt, “Spread Spectrum Communications”, Rockville, MD : Computer Sci., Vol. Ⅰ, 1985.

[2] S. W. Golomb, “Shift-Register Sequences”, Laguna Hills, CA : Aegean Park, 1982.

[3] R. Gold, “Maximal recursive sequences with 3-valued recursive cross-correlation functions”, IEEE Trans. Inform. Theory, IT-14, pp. 154-156, 1968.

[4] 최언숙, 조성진, “최적의 상호상관관계를 갖는 이진 수열의 설계”, 한국전자통신학회논문지, 6권, 4호, pp. 539-544, 2011.

[5] 김한두, 조성진, 권민정, 안현주, “확장 Zeng 수열의 상호상관 함숫값에 대한 연구”, 한국전자

통신학회논문지, 7권, 1호, pp. 69-80, 2012.
[6] 권민정, 조성진, 권숙희, 김진경, 김한두, 최언숙, “상호상관관계 함숫값이 4개인 새로운 데시메이션”, 한국전자통신학회논문지, 7권, 4호, pp. 827-832, 2012.
[7] 최언숙, 조성진, “유한체상의 방정식과 m-수열의 상호상관관분 분석”, 한국전자통신학회논문지, 7권, 4호, pp. 821-826, 2012.
[8] 조성진, 김석태, 김진경, 임지미, “GMW 수열과 No 수열에 의해서 생성된 수열의 확장수열”, 한국전자통신학회논문지, 7권, 2호, pp. 271-277, 2012.
[9] H.D. Kim and S.J. Cho, “A new proof about the decimations with Niho type five-valued cross-correlation functions”, Journal of Applied Mathematics and Informatics, Vol. 30, No. 5-6, pp. 903-911, 2012.
[10] T. Helleseth, J. Lahtonen and P. Rosendahl, “On Niho type cross-correlation functions of m-sequences”, Finite Fields and Their Applications, Vol. 13, No. 2, pp. 305-317, 2007.
[11] T. Helleseth and P. Rosendahl, “New pairs of m-sequences with 4-level cross-correlation”, Finite Fields and Their Applications, Vol. II, No. 4, pp. 674-683, 2005.
[12] Y. Niho, “Multi-valued Cross-Correlation functions between two maximal linear recursive sequences”, Ph. D. thesis, University of Southern California, 1972.
[13] P. Rosendahl, “Niho Type Cross-Correlation Functions and Related Equations”, Ph.D. thesis, University of Turku, 2004.
[14] Y. S. Kim, J. S. Chung and J. S. No, “New Construction of p-ary Sequence Family With Large Linear Span”, Proc. 2008 International Symposium on Information Theory and its Applications(Auckland, New Zealand), December 7-10, pp. 1563-1565, 2008.
[15] R. Lidl and H. Niederreiter, “Finite fields”, Cambridge University Press, 1997.
[16] R. McEliece, “Finite fields for computer scientists and engineers”, Kluwer Academic Publisher, Boston, 1987.
[17] E.L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators", IEEE Trans. Inform. Theory IT-22, pp. 732-736, 1976.

저자 소개

김진경(Jin-Gyoung Kim)

2006년 부경대학교 응용수학과 이학석사
2008년~현재 부경대학교 응용수학과 박사과정
※ 관심분야 : 셀룰라 오토마타론, 유한체론

조성진(Sung-Jin Cho)

1979년 강원대학교 수학교육학과 이학사
1981년 고려대학교 수학과 이학석사
1988년 고려대학교 수학과 이학박사
1988년~현재 부경대학교 응용수학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호

김한두(Han-Doo Kim)

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

최언숙(Un-Sook Choi)

1992년 성균관대학교 산업공학과 공학사
2000년 부경대학교 응용수학과 이학석사
2004년 부경대학교 응용수학과 이학박사
2009년 부경대학교 정보보호학과 공학박사
2006년~현재 동명대학교 자율전공학부 조교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호, 암호이론