JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 3 : 609~616 Mar. 2014

데시메이션이 $d = 2^{m-2}(2^m + 3)$인 비선형 이진수열의 선형스팬 분석

임지미[1] · 조성진[1*] · 김한두[2] · 김석태[3]

Analysis of Linear Span of Non-linear Binary Sequences with Decimation $d = 2^{m-2}(2^m + 3)$

Ji-Mi Yim[1] · Sung-Jin Cho[1*] · Han-Doo Kim[2] · Seok-Tae Kim[3]

[1*]Department of Applied Mathematics, Pukyong National University, Busan, 608-737, Korea
[2]Department of Applied Mathematics, Inje University, GimHae, 621-749, Korea
[3]Department of Information and Communication Engineering, Pukyong National University, Busan, 608-737, Korea

요 약

선형스팬이 클수록 예측을 어렵게 하기 때문에 선형스팬을 크게 하는 것은 보안 및 암호 시스템에서 중요한 문제이다. 낮은 상관함숫값을 가지면서 큰 선형스팬을 가지는 비선형 이진수열에 대한 연구는 계속 이루어져 왔다. 본 논문에서는 $n = 2m$이고 데시메이션이 $d = 2^{m-2}(2^m + 3)$인 비선형 이진수열 $S_a^r(t) = Tr_1^m\left\{\left[Tr_m^n(a\alpha^t + \alpha^{dt})\right]^r\right\}$ $(a \in GF(2^m), 0 \le t \le 2^m - 2)$에 대한 선형스팬을 분석한다.

ABSTRACT

Large linear span makes difficult to predict, so this study is important to the security and code system. It has been studied about the non-linear binary sequences having low correlation values and large linear span. In this paper we analyze the linear span of $S_a^r(t) = Tr_1^m\left\{\left[Tr_m^n(a\alpha^t + \alpha^{dt})\right]^r\right\}(a \in GF(2^m), 0 \le t \le 2^m - 2)$ where $n = 2m$ and $d = 2^{m-2}(2^m + 3)$.

키워드 : 선형스팬, 비선형 이진수열, 데시메이션, 유한체, 트레이스

Key word : linear span, non-linear binary sequence, decimation, finite fields, trace

접수일자 : 2013. 12. 05 심사완료일자 : 2013. 12. 27 게재확정일자 : 2014. 01. 10

*** 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.2014.18.3.609 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

최대 주기를 갖는 수열에 대한 연구는 Niho[1], Helleseth[2], Rosendahl[3] 등 여러 연구자에 의해서 이루어져 왔다[4-7]. 특히 Niho는 주기가 $2^{2m}-1$인 수열에서 $d \equiv 1 \pmod{2^m-1}$을 만족하는 데시메이션(decimation) d값을 다루는 방법을 연구했다. 낮은 자기상관함숫값 또는 상호상관함숫값을 가지면서 선형스팬이 큰 비선형 이진수열들은 통신 및 암호시스템에서 활용되고 있다[8,9]. 디지털 통신 시스템에서 다중접속간섭(Multiple Access Interference)을 최소화하기 위해서 낮은 상관함숫값을 갖는 이진 의사난수열의 설계는 중요한 문제이다[10]. 그리고 선형스팬이 클수록 현재의 값으로 다음 값을 알아내기는 어려워지므로 보안 및 암호시스템에서 활용되고 있다. 위성통신의 다원 접속 방식의 하나인 스팩트럼 확산 다원접속(spread-spectrum multiple-access)통신 시스템에서는 낮은 상관함숫값과 선형스팬이 큰 값을 갖는 코드수열을 사용한다[11,12]. Bent 수열[13,14], Gold 수열[15,16], Kasami 수열[17,18] 등은 낮은 상관함숫값을 가지는 동시에 낮은 수치의 선형스팬을 갖는다. No 수열은 낮은 수치의 선형스팬을 갖는 이진수열을 보완하여 GMW 수열의 선형스팬보다 큰 값을 갖는다[19]. 이진수열의 최소다항식의 차수를 선형스팬이라고 정의하는데 최소다항식을 구하기는 쉽지 않다. 그래서 Key[20]는 선형스팬을 구하는 좀 더 편리한 방법을 제시하였다. 본 논문은 2장에서 유한체를 기반으로 한 배경지식을 소개하고[21] 3장에서 데시메이션이 $d=2^{m-2}(2^m+3)$인 비선형수열 $S_a^r(t)$의 선형스팬을 분석한다. 그리고 4장에서는 결론을 맺는다.

Ⅱ. 배경 지식

$k|l$을 만족하는 $k, l \in \mathbb{N}$에 대하여 다음과 같이 정의되는 함수 $Tr_k^l : GF(2^l) \rightarrow GF(2^k)$를 트레이스(trace) 함수라고 한다.

$$Tr_k^l(x) = x + x^{2^k} + x^{2^{2k}} + \cdots + x^{2^{(\frac{l}{k}-1)k}} \quad (1)$$

트레이스 함수는 이진의사난수열을 생성하는 도구이고 많은 이진수열들이 트레이스 함수에 의해 정의되었다.

표 1. 트레이스 함수에 의해 정의된 수열들
Table. 1 Sequences defined by trace function

수열	함수
GMW 수열	$Tr_1^m\{[Tr_m^n(\alpha^t)]^r\}$ $n=2m,\ \gcd(r, 2^m-1)=1$
Kasami 수열	$Tr_1^n(\alpha^{2t}) + Tr_1^m(\eta_i \alpha^{Q \cdot t})$ $n=2m,\ Q=2^m+1,$ $\eta_i \in GF(2^m)$
No 수열	$Tr_1^m\{[Tr_m^n(\alpha^{2t}) + \gamma_i \alpha^{Q \cdot t}]^r\}$ $n=2m,\ \gcd(2^m-1, r)=1,$ $Q=2^m+1,\ \gamma_i \in GF(2^m)$

$f(x)$가 $GF(2)$위에서 n차 기약다항식이고 s가 양의 정수라 하자. 수열 $\boldsymbol{a}=\{a_i\}=\{Tr_k^l(\alpha^i)\}$ ($i \geq 0$인 정수, α는 $f(x)$의 원시근)와 $\boldsymbol{b}=\{a_{si}\}=\{Tr_k^l(\alpha^{si})\}$에 대하여 수열 $\boldsymbol{b}$는 수열 $\boldsymbol{a}$의 s-데시메이션이라고 한다.

<예제 1> 기약다항식 $f(x)=x^4+x+1$에 대한 수열은 $\boldsymbol{a}=(000100110101111)$이다. 수열 $\boldsymbol{a}$의 3-데시메이션은 $\boldsymbol{b}=(01111)$이고, 7-데시메이션은 $\boldsymbol{c}=(011110101100100)$이다.

LFSR 수열 $\boldsymbol{a}$에 대하여 $\boldsymbol{a}$의 최소다항식의 차수를 선형스팬(linear span)이라고 한다. 그러나 수열 $\boldsymbol{a}$의 최소다항식을 구하기는 쉽지 않다. Key[20]는 주기가 2^n-1인 $GF(2)$위에서의 수열 $\boldsymbol{a}=(a_i)$의 선형스팬을 구하는 방법을 정리 2와 같이 제시하였다.

[정리 2] $a_i = \sum_{j=0}^{2^n-2} c_j \alpha^{ji}$ ($c_j \in GF(2)$, α는 $GF(2^n)$의 원시원소)에 대하여 수열 $\boldsymbol{a}=(a_i)$의 선형스팬 L은 다음과 같다.

$$L = |\{c_j | c_j \neq 0,\ 0 \leq j < 2^n-1\}| \quad (2)$$

<예제 3> GMW 수열 $a_i = Tr_1^3\{[Tr_3^6(\alpha^t)]^3\}$에서 $\alpha^t = x$라 두면

$$Tr_1^3\{[Tr_3^6(x)]^3\}=x^3+x^{10}+x^{17}+x^{24}+x^6+x^{20}+x^{34}+x^{48}+x^{12}+x^{40}+x^5+x^{33}$$

이다. 따라서 수열 (a_t)의 선형스팬은 12이다.

[정리 4] GMW 수열의 선형스팬 LS는

$$LS=m\left(\frac{n}{m}\right)^{w(r)} \tag{3}$$

이다. $w(r)$은 r의 이진표현에서 1의 개수이다.

<예제 5> α가 $GF(2^6)$의 원시원소일 때, GMW 수열 $a_t=Tr_1^3\{[Tr_3^6(\alpha^t)]^3\}$의 선형스팬은 $3\cdot\left(\frac{6}{3}\right)^{w(3)}=12$ 이다.

Ⅲ. $S_a^r(t)$의 선형스팬 분석

$n=2m$, $d=2^{m-2}(2^m+3)$일 때 비선형수열 $s_a^r(t)$를 다음과 같이 정의한다.

$$s_a^r(t)=Tr_1^m\left\{\left[Tr_m^n(a\alpha^t+\alpha^{dt})\right]^r\right\} \tag{4}$$

선형스팬 분석을 위해 $s_a^r(t)$를 전개하여 항의 개수를 조사한다. $\alpha=\delta\gamma$ $(\delta^{2^m-1}=1,\gamma^{2^m+1}=1)$라 두면 (5)가 성립한다.

$$\begin{aligned}&Tr_m^n(a\alpha^t+\alpha^{dt})\\&=Tr_m^n(a\delta^t\gamma^t+\delta^{dt}\gamma^{dt})\\&=Tr_m^n[\delta^t(a\gamma^t+\gamma^{2^{m-1}t})]\\&=\delta^t(a\gamma^t+\gamma^{2^{m-1}t})+\delta^{2^mt}(a\gamma^{-t}+\gamma^{-2^{m-1}t})\\&=\delta^t\gamma^{-2^{m-1}t}(\gamma^{2^mt}+a\gamma^{(2^{m-1}+1)t}+a\gamma^{(2^{m-1}-1)t}+1)\end{aligned} \tag{5}$$

$\delta^t\gamma^{-2^{m-1}t}=x$, $\gamma^t=y$ 라 두면 (5)는 (6)과 같다.

$$Tr_m^n(a\alpha^t+\alpha^{dt})=x(y^{2^m}+ay^{2^{m-1}+1}+ay^{2^{m-1}-1}+1)=xg(y) \tag{6}$$

여기서 $g(y)=y^{2^m}+ay^{2^{m-1}+1}+ay^{2^{m-1}-1}+1$ 이다.

(6)으로부터 (4)는 (7)과 같다.

$$s_a^r(t)=Tr_1^m\left\{\left[Tr_m^n(a\alpha^t+\alpha^{dt})\right]^r\right\}=\sum_{j=0}^{m-1}x^{r\cdot 2^j}[g(y)]^{r\cdot 2^j} \tag{7}$$

$\delta^t y^{-2^{m-1}}=x$ 는 $y^{-2^{m-1}(2^m-1)}=x^{2^m-1}$ 가 된다.

$$y^{-2^{m-1}(2^m-1)}=y^{-2^{m-1}(2^m+1-2)}=y^{-2^{m-1}(-2)}=y^{2^m} \tag{8}$$

이므로 $y=x^{\frac{2^m-1}{2^m}}$ 이다. 따라서

$$x^r[g(y)]^r=\sum_{l=0}^{2^m r}c_l x^{\frac{(2^m-1)l}{2^m}+r} \tag{9}$$

이다. 여기서 $c_l\in GF(2^m)$이다.

[보조정리 6] $x^{r\cdot 2^{j_1}}[g(y)]^{r\cdot 2^{j_1}}$과 $x^{r\cdot 2^{j_2}}[g(y)]^{r\cdot 2^{j_2}}$의 전개식에서 x의 지수는 다르다. 단, $0\le j_1<j_2\le m-1$이다.

〈증명〉 $x^{r\cdot 2^{j_1}}[g(y)]^{r\cdot 2^{j_1}}$과 $x^{r\cdot 2^{j_2}}[g(y)]^{r\cdot 2^{j_2}}$의 전개식에서 x의 지수가 같다고 하자. $j=j_2-j_1\,(0<j\le m-1)$라 두면 (10)이 성립한다.

$$\frac{2^m-1}{2^m}l_1+r\equiv\left(\frac{2^m-1}{2^m}l_2+r\right)2^j\pmod{2^n-1} \tag{10}$$

(10)의 양변에 $2^m(2^m+1)$을 곱하면

$$(2^n-1)(l_2-l_1)+2^m(2^m+1)(2^j-1)r\equiv 0\pmod{2^n-1} \tag{11}$$

이고 $(2^j-1)r\equiv 0\pmod{2^m-1}$이다. $\gcd(r,2^m-1)=1$이므로 $2^j-1\equiv 0\pmod{2^m-1}$이다. 이것은 모순이므로 $x^{r\cdot 2^{j_1}}[g(y)]^{r\cdot 2^{j_1}}$과 $x^{r\cdot 2^{j_2}}[g(y)]^{r\cdot 2^{j_2}}$의 전개식에서 x의 지수들은 서로 다르다. □

보조정리 6에 의해서 $s_a^r(t)$의 선형스팬은 $[g(y)]^r$의 전개식에서 항들의 개수의 m배이다. 분석의 편의를 위하여 $[g(y)]^r$ 대신 $[y^3+ay^2+ay+1]^r$의 항의 개수를 구하여 m배를 하면 $s_a^r(t)$의 선형스팬의 하한값을 구할 수

있다. 이제는 $G(y)=[y^3+ay^2+ay+1]^r$라 두고 r을 (12)와 같이 나타내고 (13)을 만족하는 경우로 제한하자.

$$r=\sum_{j=1}^{R}2^{e_j}\left(\sum_{k=0}^{L_j-1}2^k\right) \tag{12}$$

· R : r의 이진 전개에서 블록들의 수
· L_j : j번째 블록의 길이
· e_j : j번째 블록에서 가장 낮은 2의 지수

$$e_{j+1}\geq e_j+L_j+2\ (j=1,2,\cdots,R-1) \tag{13}$$

(12)에 의해서

$$\begin{aligned}G(y)&=\left[y^3+ay^2+ay+1\right]^r\\&=\left[y^3+ay^2+ay+1\right]^{\sum_{j=1}^{R}2^{e_j}r_j}\\&=\prod_{j=1}^{R}\left[y^{3\cdot 2^{e_j}}+a^{2^{e_j}}y^{2\cdot 2^{e_j}}+a^{2^{e_j}}y^{2^{e_j}}+1\right]^{r_j}\end{aligned} \tag{14}$$

이다. 여기서 $r_j=\sum_{k=0}^{L_j-1}2^k=2^{L_j}-1\ (1\leq j\leq R)$이다.

$g_j(y)=\left[y^{3\cdot 2^{e_j}}+a^{2^{e_j}}y^{2\cdot 2^{e_j}}+a^{2^{e_j}}y^{2^{e_j}}+1\right]^{r_j}$라 두면 $g_j(y)$에서 y의 지수는 2^{e_j}의 배수이며 0이상 $3\cdot 2^{e_j}\cdot r_j$ 이하이다. $G(y)=\prod_{j=1}^{R}g_j(y)$이므로 $G(y)$의 전개식에서 생길 수 있는 y의 지수들은 $\sum_{j=1}^{R}a_j$와 같은 형태이다. 여기서 a_j는 $g_j(y)$에서 선택된 항의 y의 지수이다. (13)에 의해서

$$2^{e_{j+1}}\geq 2^{e_j+2}\cdot 2^{L_j}>3\cdot 2^{e_j}\left(2^{L_j}-1\right)=3\cdot 2^{e_j}\cdot r_j \tag{15}$$

이므로 $0\leq a_j\leq 3\cdot 2^{e_j}\cdot r_j<2^{e_{j+1}}$ 이다. $2^{e_j}\mid a_j$ 이므로 $\sum_{j=1}^{R}a_j=\sum_{j=1}^{R}u_j2^{e_j}(0\leq u_j\leq 3r_j)$이다.
$\sum_{j=1}^{R}b_j=\sum_{j=1}^{R}v_j2^{e_j}(0\leq v_j\leq 3r_j)$라 두고 $\sum_{j=1}^{R}a_j=\sum_{j=1}^{R}b_j$이면 $a_j=b_j$임을 증명하자. 가정에 의해서

$$\begin{aligned}&\sum_{j=1}^{R}(a_j-b_j)=\sum_{j=1}^{R}(u_j-v_j)2^{e_j}\\&=(u_1-v_1)2^{e_1}+(u_2-v_2)2^{e_2}+\cdots+(u_R-v_R)2^{e_R}\\&=\left\{\frac{(u_1-v_1)}{2^{e_2-e_1}}+(u_2-v_2)+\cdots+(u_R-v_R)2^{e_R-e_2}\right\}2^{e_2}\end{aligned} \tag{16}$$

이다. $0\leq|u_i-v_i|\leq 3r_j<2^{L_j+2}\leq 2^{e_{j+1}-e_j}$이므로 (16)이 0이 되기 위해서는 먼저 $u_1=v_1$이다. 같은 방법에 의해서 $u_j=v_j\ (1\leq j\leq R)$이어야 한다. 따라서 $\sum_{j=1}^{R}a_j$와 $\sum_{j=1}^{R}b_j$가 같으려면 $a_j=b_j\ (1\leq j\leq R)$이어야 한다. 이 결과에 의해서 $G(y)$의 전개식에서의 y의 서로 다른 지수들의 개수를 M이라 하고 $g_j(y)$에서의 y의 서로 다른 지수들의 개수를 M_j라고 하면 $M=\prod_{j=1}^{R}M_j$ 이다.

세 가지 경우로 나누어 M에 대하여 알아보자.

(a) $a=0$인 경우:
$z=y^{2^{e_j}}$라 두면 $g_j(y)=\left[1+z^3\right]^{r_j}=\sum_{k=0}^{r_j}z^{3k}$ 이고 $M_j=r_j+1$ 이므로

$$M=\prod_{j=1}^{R}M_j=\prod_{j=1}^{R}(r_j+1)=\prod_{j=1}^{R}2^{L_j}=2^{\sum_{j=1}^{R}L_j}=2^{w(r)} \tag{17}$$

이다. 그러므로 $a=0$인 경우 $s_a^r(t)$의 선형스팬은 $m\cdot 2^{w(r)}$이고 GMW 수열의 선형스팬과 같다.
(b) $a=1$인 경우:
$z=y^{2^{e_j}}$라 두면

$$g_j(z)=\left[1+z+z^2+z^3\right]^{r_j}=(1+z)^{3r_j} \tag{18}$$

이다. (18)을 전개하여 정리하면 (19)와 같다.

$$\sum_{k=0}^{r_j}A_kz^k+\sum_{k=0}^{r_j}A_kz^{3r_j-k}+\sum_{k=1}^{\frac{r_j-1}{2}}B_kz^{r_j+k}+\sum_{k=1}^{\frac{r_j-1}{2}}B_kz^{2r_j-k} \tag{19}$$

여 기 서 $A_0=1, A_k=1+\sum_{i=1}^{k}C_i$, $B_k=\sum_{i=k}^{r_j-k-1}C_i$, $C_i=\begin{cases}0, & i\text{가 홀수}\\1, & i\text{가 짝수}\end{cases}$ 이다. (19)의 $\sum_{k=0}^{r_j}A_kz^k$에서 $A_k=1$인 개수는 $\frac{r_j+1}{2}$개이고 $\sum_{k=1}^{\frac{r_j-1}{2}}B_kz^{r_j+k}$ 에서는 모두 $B_k=0$이다. 따라서 (18)을 전개했을 때 항의 개수는 r_j+1개가 되어 $M_j=r_j+1$ 이다. 따라서

$$M=\prod_{j=1}^{R}M_j=\prod_{j=1}^{R}(r_j+1)=\prod_{j=1}^{R}2^{L_j}=2^{\sum_{j=1}^{R}L_j}=2^{w(r)} \quad (20)$$

이다. 그러므로 $a=1$인 경우 $s_a^r(t)$의 선형스팬은 $m\cdot 2^{w(r)}$이고 GMW 수열의 선형스팬과 같다.

(c) $a\neq 0$, $a\neq 1$인 경우:

$z=y^{2^{e_j}}$, $\eta=a^{2^{e_j}}$라 두면

$$g_j(z)=\left[1+\eta z+\eta z^2+z^3\right]^{r_j} \quad (21)$$

이다. (21)을 인수분해하면

$$\begin{aligned} g_j(z) &= (z+1)^{r_j}[z^2+(\eta+1)z+1]^{r_j} \\ &= (z+1)^{r_j}(z+\delta)^{r_j}(z+\delta^{-1})^{r_j} \\ &= (z+1)^{r_j}\left(\sum_{k=0}^{r_j}\delta^{r_j-k}z^k\right)\left(\sum_{l=0}^{r_j}\delta^{l-r_j}z^l\right) \end{aligned} \quad (22)$$

단, $\delta+\delta^{-1}=\eta+1$이다. (22)를 전개하여 정리하면 (23)과 같다.

$$\sum_{k=0}^{r_j}A_kz^k+\sum_{k=0}^{r_j}A_kz^{3r_j-k}+\sum_{k=1}^{\frac{r_j-1}{2}}B_kz^{r_j+k}+\sum_{k=1}^{\frac{r_j-1}{2}}B_kz^{2r_j-k} \quad (23)$$

여기서 $A_0=1$, $A_k=1+\sum_{i=1}^{k}C_i$, $B_k=C_{r_j}+\sum_{i=k}^{r_j-k-1}C_i$, $C_i=\frac{(\delta^{-2})^{i+1}+1}{\delta^{-2}+1}\cdot\delta^i$ 이다. A_k를 계산하면 (24)와 같다.

$$A_k=\frac{\delta^{-2}+1+\delta^{-3}+\delta+\delta^{-4}+\delta^2+\cdots+\delta^{-k-2}+\delta^k}{\delta^{-2}+1} \quad (24)$$

(24)의 분자를 정리하면 $\frac{(\delta^{k+1}+1)(\delta^{k+2}+1)}{\delta^{k+2}(\delta+1)}$이다. $A_k=0$이기 위해서는 $\delta^{k+1}=1$ 또는 $\delta^{k+2}=1$이다. 따라서 $A_k=0$가 되는 개수는

$$\left|\{k\mid\delta^{k+1}=1(\ 1\le k\le r_j)\}\right|+\left|\{k\mid\delta^{k+2}=1(\ 1\le k\le r_j)\}\right| \quad (25)$$

이다. 이제는 $B_k=0$가 되는 k의 개수의 최댓값을 알아보자. $C_u=C_v$라고 하면 (26)과 같다.

$$\frac{(\delta^{-2})^{u+1}+1}{\delta^{-2}+1}\cdot\delta^u=\frac{(\delta^{-2})^{v+1}+1}{\delta^{-2}+1}\cdot\delta^v \quad (26)$$

(26)을 인수분해하면 $(\delta^u+\delta^v)(\delta^{-u-v-2}+1)=0$이다. $u+v=r_i-1$이면 $\delta^{u+v+2}\neq 1$이다. 따라서 $\delta^u=\delta^v$이고 $u=v$이다. $B_k=B_{k+1}+C_k+C_{r_j-1-k}$이고 $C_k\neq C_{r_j-1-k}$이므로 $B_k=0$이면 $B_{k+1}\neq 0$이다.

따라서 B_k $(1\le k\le\frac{r_j-1}{2})$는 연속해서 0이 될 수 없다. 그러므로 (23)의 $\sum_{k=1}^{\frac{r_j-1}{2}}B_kz^{r_j+k}$에서 $B_k=0$이 되는 개수를 최대로 계산하면 $\left\lfloor\frac{r_j-1}{4}\right\rfloor$ 개이다. (27)을 P_j라 두면

$$\begin{aligned} P_j=&\left|\{k\mid\delta^{k+1}=1(\ 1\le k\le r_j)\}\right|+\\ &\left|\{k\mid\delta^{k+2}=1(\ 1\le k\le r_j)\}\right|+\left\lfloor\frac{r_j-1}{4}\right\rfloor \end{aligned} \quad (27)$$

$g_j(z)$에서 없어지는 항들의 개수는 $2P_j$을 넘지 않는다. 따라서 다음이 성립한다.

$$\begin{aligned} M_j &\ge 3r_j+1-2P_j \\ &=3\cdot(2^{L_j}-1)+1-2P_j \\ &=3\cdot 2^{L_j}-2-2P_j \end{aligned} \quad (28)$$

[보조정리 7][22] 다음 두 집합은 일대일대응 이다.

$$\{y^3+(1+\gamma)y^2+(1+\gamma)y+1=0\mid\gamma\in GF(2^m)\} \quad (29)$$

$$\begin{aligned} K=\{&1,\alpha^{2^m+1},\alpha^{2(2^m+1)},\cdots,\alpha^{(2^{m-1}-1)(2^m+1)},\\ &\alpha^{2^m-1},\alpha^{2(2^m-1)},\cdots,\alpha^{2^{m-1}(2^m-1)}\} \end{aligned} \quad (30)$$

여기서 α는 $GF(2^n)$의 원시원소이다.

보조정리 7에서 $\gamma=0$인 경우는 $a=1$인 경우에 해당되고 $\gamma=1$인 경우는 $a=0$인 경우에 해당되므로 (20)과 (17)에 의해서 GMW 수열의 선형스팬과 같다. 따라서 $\gamma\neq 0$, $\gamma\neq 1$인 γ에 대하여 두 가지 경우로 나누어 선형스팬을 생각하자.

(a) $y^2+\gamma y+1=0$ $(\gamma\in GR(2^m)\setminus\{0,1\})$가 $GF(2^m)$에서 해를 가지는 경우 : 보조정리 7에 의해서 해는 $\delta=\alpha^{h(2^m+1)}$ $(1\le h\le 2^{m-1}-1)$의 형태이다. 먼저 (31)을 구해보자.

$$\left|\left\{k:\delta^{k+1}=1(\ 1\le k\le r_j)\right\}\right| \tag{31}$$

$\delta^{k+1}=\left(\alpha^{h(2^m+1)}\right)^{k+1}=\alpha^{h(k+1)(2^m+1)}=1$ 이므로 $h(k+1)\equiv 0 \pmod{2^m-1}$이다. $g=\gcd(h,\ 2^m-1)$라 두면 $k+1\equiv 0 \pmod{\frac{2^m-1}{g}}$ 이다. 그러면 자연수 l이 존재하여 (32)를 만족한다.

$$k+1=\frac{2^m-1}{g},\ \frac{2^m-1}{g}\times 2,\ \cdots,\ \frac{2^m-1}{g}\times l \tag{32}$$

그런데 $k+1\le r_j+1$이므로 $l\le\frac{r_j+1}{(2^m-1)/g}$이다. l은 자연수이므로

$$\left|\left\{k:\delta^{k+1}=1(\ 1\le k\le r_j)\right\}\right|=\left\lfloor\frac{r_j+1}{(2^m-1)/g}\right\rfloor \tag{33}$$

이다. 같은 방법으로 (34)도 구할 수 있다.

$$\left|\left\{k:\delta^{k+2}=1(\ 1\le k\le r_j)\right\}\right|=\left\lfloor\frac{r_j+2}{(2^m-1)/g}\right\rfloor \tag{34}$$

$r_j=2^{L_j}-1$이므로 (27), (28), (33), (34)에 의해서 $s_a^r(t)$의 선형스팬 l_{span}은 (35)를 만족한다.

$$l_{span}\ge m\cdot\prod_{j=1}^{R}\left(3\cdot 2^{L_j}-2-2\left\{\left\lfloor\frac{2^{L_j}}{(2^m-1)/g}\right\rfloor+\left\lfloor\frac{2^{L_j}+1}{(2^m-1)/g}\right\rfloor+\left\lfloor\frac{2^{L_j}-2}{4}\right\rfloor\right\}\right) \tag{35}$$

(b) $y^2+\gamma y+1=0(\gamma\in GF(2^m)\setminus\{0,1\})$가 $GF(2^m)$에서 해를 가지지 않는 경우 : 보조정리 7에 의해서 해는 $\delta=\alpha^{h(2^m-1)}(1\le h\le 2^{m-1})$의 형태이다. (a)와 같은 방법으로 선형스팬 l_{span}은 (36)을 만족한다.

$$l_{span}\ge m\cdot\prod_{j=1}^{R}\left(3\cdot 2^{L_j}-2-2\left\{\left\lfloor\frac{2^{L_j}}{(2^m+1)/g}\right\rfloor+\left\lfloor\frac{2^{L_j}+1}{(2^m+1)/g}\right\rfloor+\left\lfloor\frac{2^{L_j}-2}{4}\right\rfloor\right\}\right) \tag{36}$$

지금까지의 결과로 정리 8을 얻는다.

[정리 8] $\gamma_i\in GF(2^m)\setminus\{0\}$에 대하여 $y^2+\gamma_i y+1=0$가 $GF(2^m)$에서 해를 가지면 $\epsilon_i=-1$라 하고 해를 가지지 않으면 $\epsilon_i=+1$이라고 하자. 그리고 γ_i에 대하여 δ_i를 (30)의 집합 K에 있는 $y^2+\gamma_i y+1=0$의 근이라고 하자. 그러면 (37)이 성립하고

$$\delta_i=\begin{cases}\alpha^{h_i(2^m+1)}, & \epsilon_i=-1\\ \alpha^{h_i(2^m-1)}, & \epsilon_i=+1\end{cases} \tag{37}$$

$g_i=\gcd(h_i,\ 2^m+\epsilon_i)$라 두면 $S_a^r(t)$의 선형스팬 l_{span}은 (38)을 만족한다.

$$l_{span}\ge m\cdot\prod_{j=1}^{R}\left(3\cdot 2^{L_j}-2-2\left\{\left\lfloor\frac{2^{L_j}}{(2^m+\epsilon_i)/g_i}\right\rfloor+\left\lfloor\frac{2^{L_j}+1}{(2^m+\epsilon_i)/g_i}\right\rfloor+\left\lfloor\frac{2^{L_j}-2}{4}\right\rfloor\right\}\right) \tag{38}$$

지금부터는 $S_a^r(t)$의 선형스팬과 GMW 수열의 선형스팬을 비교해보자.

먼저 (35)의 경우를 생각해보자.

(a) m이 짝수인 경우:

$\frac{2^m-1}{g}\ne 2$이다. $\frac{2^m-1}{g}=3$이라고 하자.

이 때, $h\le 2^{m-1}-1<2^m-1$ 이므로 $h=\frac{2^m-1}{3}$이다. $y^2+\gamma y+1=0(\gamma\in GR(2^m)\setminus\{0,1\})$가 $GF(2^m)$에서 해를 가지므로 $\delta=\alpha^{h(2^m+1)}$이고 $\delta^3=1$이다. 그러면 $\gamma=1$이 된다. 따라서 $\frac{2^m-1}{g}\ne 3$이다. $\frac{2^m-1}{g}\ne 4$ 이므로 $\frac{2^m-1}{g}>4$ 이다. 따라서 (39),(40)이 성립한다.

$$\left\lfloor\frac{2^{L_j}}{(2^m-1)/g}\right\rfloor<\left\lfloor\frac{2^{L_j}}{4}\right\rfloor=2^{L_j-2} \tag{39}$$

$$\left\lfloor\frac{2^{L_j}+1}{(2^m-1)/g}\right\rfloor<\left\lfloor\frac{2^{L_j}+1}{4}\right\rfloor=2^{L_j-2} \tag{40}$$

$$\left\lfloor\frac{2^{L_j}-2}{4}\right\rfloor=2^{L_j-2}-1 \tag{41}$$

(39), (40), (41)에 의해서 (42)가 성립한다.

$$
\begin{aligned}
l_{span} &> m \cdot \prod_{j=1}^{R}\left(3 \cdot 2^{L_j}-2-2(3 \cdot 2^{L_j-2}-1)\right) \\
&= m \cdot \prod_{j=1}^{R} 3 \cdot 2^{L_j-1} \\
&> m \cdot \prod_{j=1}^{R} 2^{L_j} = m \cdot 2^{w(r)} \qquad (42)
\end{aligned}
$$

(b) m이 홀수인 경우:

$\frac{2^m-1}{g} \neq 3$이므로 (39), (40), (41)이 성립하고 따라서 (42)가 성립한다. 유사한 방법으로 (36)의 경우도 (42)가 성립한다.

이상으로 $S_a^r(t)$의 선형스팬은 $a \neq 0,\ a \neq 1$인 경우에 GMW 수열의 선형스팬보다 크다는 것을 보였다.

표 2는 $S_a^r(t)$의 선형스팬 및 발생빈도 실험결과이다. 실제 결과는 $a \neq 0$인 모든 경우에 GMW 수열의 선형스팬보다 크다는 것을 알 수 있다.

표 2. $S_a^r(t)$의 선형스팬 및 발생빈도

Table. 2 Linear Span and Frequency of $S_a^r(t)$

n	r	GMW 수열의 선형스팬	선형스팬(발생빈도)
6	3	12	18(4), 24(3)
8	7	32	40(1), 56(2), 64(12)
	14	32	40(1), 56(2), 64(12)
10	7	40	90(1), 140(30)
	9	20	60(1), 70(30)
	15	80	90(1), 150(5), 160(25)
	19	40	90(1), 140(30)
12	17	24	72(1), 84(62)
	19	48	168(1), 204(2), 216(3), 228(57)
	25	48	168(1), 216(5), 228(57)
	31	192	204(1), 300(3), 312(2), 336(3), 360(6), 372(24), 384(24)

Ⅳ. 결 론

본 논문에서는 데시메이션이 $d=2^{m-2}(2^m+3)$인 비선형수열 $S_a^r(t)=Tr_1^m\left\{\left[Tr_m^n(a\alpha^t+\alpha^{dt})\right]^r\right\}$의 선형스팬에 대하여 분석하였다. 분석을 용이하게 하기 위하여 $\left[y^{2^m}+ay^{2^{m-1}+1}+ay^{2^{m-1}-1}+1\right]^r$ 대신 $[y^3+ay^2+ay+1]^r$을 전개하였고 r은 $e_{j+1} \geq e_j+L_j+2$을 만족하도록 제한하였다. 그 결과 $a=0$ 또는 $a=1$인 경우를 제외한 a에 대하여 GMW 수열의 선형스팬보다 크다는 것을 증명하였다. 실제로 $S_a^r(t)$의 선형스팬을 구한 결과는 $a=0$을 제외한 모든 경우에 대하여 GMW 수열의 선형스팬보다 크다. 앞으로 선형스팬에 대한 연구가 활발히 이루어져야 하겠다.

REFERENCES

[1] Y. Niho, “Multi-valued cross-correlation functions between two maximal linear recursive sequences”, Ph.D thesis, University of Southern California,1972.

[2] T. Helleseth, “Some results about the cross-correlation function between two maximal linear sequences”, *Discrete Mathematics*, vol. 16, No. 3, pp. 209-232, 1976.

[3] P. Rosendahl, “Niho type cross-correlation functions and related equations”, Ph.D thesis, Turku centre for computer science, 2004.

[4] X.H. Tang, T. Helleseth, L. Hu, and W. Jiang, “Two new families of optimal binary sequences obtained from quaternary sequences”, *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 433-436, 2009.

[5] 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.

[6] K.-U. Schmidt, “Z_4-valued quadratic forms and quaternary sequence families”, *IEEE. Trans. Inf. Theory*, vol. 55, no. 12, pp. 5803-5810, 2009.

[7] P. Udaya, X.H. Tang, “On the Construction of Binary Sequence Families With Low Correlation and Large Sizes”, *IEEE. Trans. Inf. Theory*, vol. 59, no. 2, pp. 1082-1089, 2013.

[8] T. Helleseth and P.V. Kumar, “Sequences with low correlation”, in *Handbook of Coding Theory*, ed. V. Pless and C. Huffman, Elsevier, Amsterdam, The Netherlands, 1998.

[9] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, “Spread spectrum communication”, vol. I, Computer Science Press, Rockville, MD, 1985.

[10] K. Fazel and S. Kaiser, “Multi-carrier and spread spectrum system”, John Wiley and Sons Ltd., 2003.

[11] D.V. Sarwarte and M.B. Pursley, “Crosscorrelation properties of pseudorandom and related sequences”, *Proc. IEEE*, vol. 68, no. 5, pp. 593-620, May. 1980.

[12] R.A. Scholtz, “The origins of spread-spectrum communications”, *IEEE Trans. Commun.*, vol. COM-30, pp.822-854, May. 1982.
[13] P.V. Kumar and R.A. Scholtz, “Bounds on the linear span of bent sequences”, *IEEE Trans. Inform. Theory*, vol. IT-29, no. 6, pp. 854-862, Nov. 1983.
[14] J.D. Olsen, R.A. Scholtz, and L. R. Welch, “Bent-function sequences”, *IEEE Trans. Inform. Theory*, vol. IT-28. no. 6, pp.858-864, Nov. 1982.
[15] R. Gold, “Maximal recursive sequences with 3-valued recursive crosscorrelation functions”, *IEEE Trans. Inform. Theory*, vol. IT-14, no. 1, pp. 154-156, Jan. 1968.
[16] R. Gold, “Optimal binary sequences for spread spectrum multiplexing”, *IEEE Trans. Inform. Theory*, vol. IT-13, no. 5, pp.619-621, Oct. 1967.
[17] T. Kasami, “Weight distribution formula for some class of cyclic codes”, Coordinated Science Laboratory, University of Illinois, Urbana, Tech. Rep. R-285(AD632574), 1966.
[18] T. Kasami, “Weight distribution of Bose-Chaudhuri-Hocquenghem codes in Combinatorial Mathematics and its Applications”, Chapel Hill, NC: University of North Carolina Press, 1969.
[19] 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. 35, no. 2, pp. 371-379, Mar. 1989.
[20] E.L. Key, “An analysis of the structure and complexity of non-linear binary sequence generators”, *IEEE Trans. Inform. Theory*, IT-22, pp. 732-736, 1976.
[21] R. Lidl and H. Niederreiter, “Finite fields”, Cambridge University Press, 1997.
[22] S.J. Cho, J.M. Yim, “Analysis of binary sequences generated by GMW sequences and No sequences”, *J. Korea Inst. Inf. Commun. Eng.*, vol. 15, no. 10, pp. 2183-2187, 2011.

임지미(Ji-Mi Yim)

1997년: 부산대학교 수학교육과 (이학사)
2008년: 부경대학교 교육대학원 수학과 석사
2008년~현재: 부경대학교 응용수학과 박사과정
※ 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
※ 관심분야 : 셀룰라 오토마타론, 정보보호

김한두(Han-Doo Kim)

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

김석태(Seok-Tae Kim)

1983년: 광운대학교 전자공학과 (공학사)
1988년: Kyoto Institute of Technology 전자공학과(공학석사)
1991년: Osaka대학 통신공학사(공학박사)
1991년~현재: 부경대학교 정보통신공학과 교수
※ 관심분야 : 영상처리, 패턴인식, 워터마킹, 셀룰라 오토마타론