GMW 수열과 No 수열에 의해서 생성된 이진 수열 분석

조성진* · 임지미**

Analysis of binary sequences generated by GMW sequences and No sequences

Sung-Jin Cho* · Ji-Mi Yim**

요 약

본 논문에서는 GMW 수열과 No 수열에 의해서 생성된 이진 수열들의 집합을 소개하고 분석한다. 집합안의 각 수열들은 주기 $N=2^n-1$이고 $n=2m$ 이며 2^m개의 수열들이 있다. 합성된 수열의 자기상관계수와 상호상관계수 그리고 선형스팬을 구한다.

ABSTRACT

In this paper, a family of binary sequences generated by GMW sequences and No sequences is introduced and analyzed. Each sequence within a family has period $N=2^n-1$, $n=2m$ and there are 2^m sequences within that family. We obtain auto and cross-correlation values and linear span of the synthesized sequence.

키워드

GMW 수열, No 수열, 상관계수, 선형스팬, 유한체

Key word

GMW sequences, No sequences, cross-correlation, linear spans, finite fields

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

접수일자 : 2011. 05. 09
심사완료일자 : 2011. 06. 10

Ⅰ. 서 론

Gordon-Mills-Welch(GMW) 수열은 2종류의 상관계수를 갖는 비선형수열 이다[1]. 2종류의 상관계수를 갖는 주기 $N=2^n-1$ 의 이진 의사난수열은 통신 및 암호 분야에 응용되고 있다. 위성통신의 다원 접속 방식의 하나인 스팩트럼 확산다원접속(spread-spectrum multiple-access)통신 시스템에서는 낮은 상관계수와 높은 선형스팬을 갖는 코드수열을 사용한다[2]-[4]. Bent 수열[5]-[7], Gordon 수열[8],[9], Kasami 수열[10],[11] 등은 이상적인 상관계수를 가지고 있지만 낮은 수치의 선형스팬을 갖는다. No 수열은 이러한 점을 보완하였다[12]. No 수열의 선형스팬은 GMW 수열 보다 크거나 같다[12].

본 논문에서는 두 이진 의사난수열 GMW 수열과 No 수열을 합성하여 얻어진 수열들의 집합을 소개하고 분석한다. 집합 안의 각 수열들은 주기 $N=2^n-1$ 이고 $n=2m$ 이며 2^m개의 수열들이 있다. 합성된 수열의 상관계수, 선형스팬의 크기, 생성할 수 있는 서로 다른 수열들의 개수에 관련하여 이진 합성 의사난수열을 분석한다.

2장에서는 이진 의사난수열에서 사용되는 트레이스 함수와 GMW 수열, No 수열에 대해 간단히 소개한다. 3장에서는 합성된 수열의 상관계수 값을 No 수열에 대한 상관계수 값을 구하는 방법 [12] 과는 다른 방법에 의하여 구하고 4장에서는 선형스팬 크기를 Key [13]의 선형스팬을 구하는 방법을 이용하여 구하고자 한다. 5장에서는 결론을 맺는다.

Ⅱ. 배경지식

[정리 1] $k|l$을 만족하는 $k,l\in\mathbb{N}$에 대하여 다음과 같이 정의된 함수 $Tr_k^l : GF(2^l) \rightarrow GF(2^k)$을 트레이스(trace)라 한다:

$$Tr_k^l(x)=\sum_{j=0}^{l/k-1} x^{2^{k\cdot j}}$$

$n:=2m(m>0, m\in\mathbb{N})$, $N:=2^n-1$, $Q:=2^m+1$ 라 하자. $S:=\{s_i(t)|0\le t\le N-1,\ 1\le i\le 2^m\}$을 다음을 만족하는 2^m개의 이진수열들로 이루어진 모임이라 하자:

$$s_i(t):=Tr_1^m\{[Tr_m^n(\alpha^{2t})+\gamma_i\alpha^{Q\cdot t}]^r\} \quad (1)$$

여기서 α는 $GF(2^n)$의 한 원시원소이며 r $(1\le r<2^m-1)$은 $\gcd(r,2^m-1)=1$을 만족한다. 또한 $i\neq j(1\le i,j\le 2^m)$이면 $\gamma_i\neq\gamma_j(\gamma_i,\gamma_j\in GF(2^m))$이며 $GF(2^m)=\{\gamma_i|1\le i\le 2^m\}$이다. (1)에서 $\gamma_i=0$ 일 때 GMW이고, $\gamma_i\neq 0$ 일 때, No 수열이다 [1],[12].

Ⅲ. 이진 의사난수열의 합성 및 상관계수

$n:=2m(m>0, m\in\mathbb{N})$, $N:=2^n-1$, $Q:=2^m+1$ 라 하자.

$C:=\{c_i(t)|0\le t\le N-1,\ 1\le i\le 2^m\}$을 다음을 만족하는 2^m개의 이진수열들로 이루어진 모임이라 하자:

합성수열 $c_i(t)$는 다음과 같다.

$$c_i(t):=Tr_1^m\{[Tr_m^n(\alpha^{2t})+\gamma_i\alpha^{Qt}]^r\}+Tr_1^m\{[Tr_m^n(\alpha^{2t})]^r\}$$

여기서 $\gamma_i\neq 0$이며 α는 $GF(2^n)$의 한 원시원소이며 $r(1\le r<2^m-1)$은 $\gcd(r,2^m-1)=1$을 만족한다. 또한 $i\neq j(1\le i,j\le 2^m)$이면 $\gamma_i\neq\gamma_j(\gamma_i,\gamma_j\in GF(2^m))$이며 $GF(2^m)=\{\gamma_i|1\le i\le 2^m\}$이다. 수열 $\{c_i\}$의 $(2^m-1)\times Q$ 배열을 $A(\{c_i\})$라 하자. 이 배열을 수열 $\{c_i\}$에 대한 $(2^m-1, Q)$ 삽입수열 (interleaved sequence)라 한다.

$1\le i,j\le 2^m$에 대하여 $R_{i,j}(\cdot)$을 C의 i번째 수열과 j번째 수열에 대한 상관함수(correlation function)라 하자:

$$R_{i,j}(\tau):=\sum_{t=0}^{N-1}(-1)^{c_i(t+\tau)+c_j(t)},\ 0\le\tau\le N-1$$

[보조정리 2] 위에서 생성된 수열 $\{c_i\}$에 대한 $(2^m-1, Q)$ 삽입수열 $A(\{c_i\})$의 각 열은 0-수열이거나 β에 의해서 생성된 m-수열이다.

(증명) 수열 $\{c_i\}$에 대하여

$c_i(t) := Tr_1^m\{[Tr_m^n(\alpha^{2t})+\gamma_i\alpha^{Qt}]^r\}+Tr_1^m\{[Tr_m^n(\alpha^{2t})]^r\}$
이다. $t=t_1Q+t_2 \quad (0\le t_1\le 2^m-2, \quad 0\le t_2\le Q-1)$, $\beta=\alpha^Q$ 라 하자. 그러면 β는 $GF(2^m)$의 원시원소이며 $c_i(t)$는 다음과 같다.

$$\begin{aligned} c_i(t) &= Tr_1^m\Big\{\Big[Tr_m^n\big(\beta^{2t_1}\alpha^{2t_2}\big)+\gamma_i\beta^{t_1Q}\beta^{t_2}\Big]^r\Big\}+ \\ &\qquad Tr_1^m\Big\{\beta^{2rt_1}\Big[Tr_m^n\big(\alpha^{2t_2}\big)\Big]^r\Big\} \\ &= Tr_1^m\Big\{\beta^{2rt_1}\Big(\Big[Tr_m^n\big(\alpha^{2t_2}\big)+\gamma_i\beta^{t_2}\Big]^r+\Big[Tr_m^n\big(\alpha^{2t_2}\big)\Big]^r\Big)\Big\} \end{aligned}$$

$w(t_2)=\Big[Tr_m^n\big(\alpha^{2t_2}\big)+\gamma_i\beta^{t_2}\Big]^r+\Big[Tr_m^n\big(\alpha^{2t_2}\big)\Big]^r$ 라 하면 $c_i(t)=Tr_1^m\{\beta^{2rt_1}w(t_2)\}$이다. 따라서 $w(t_2)=0$이면 $A(\{c_i\})$의 t_2-열은 0-수열이 되고 $w(t_2)\neq 0$이면 $A(\{c_i\})$의 t_2-열은 β^{2rt_1}에 의해서 생성된 m-수열이다. 그런데 $\gcd(r,2^m-1)=1$이므로 β^{2rt_1}에 의해서 생성된 m-수열과 β에 의해서 생성된 m-수열은 같다. □

[참고] [보조정리 2]에서 β에 의해서 생성된 수열을 기준수열(base sequence)이라 한다.

[따름정리 3] 두 수열 $\{c_i\}$와 $\{c_j\}$와 합 수열에 대한 $(2^m-1, Q)$ 삽입수열 $A(\{c_i\}+\{c_j\})$의 각 열은 0-수열이거나 β에 의해서 생성된 m-수열이다.
(증명) $A(\{c_i\})$와 $A(\{c_j\})$의 각 열은 0-수열이거나 β에 의해서 생성된 m-수열이다. 정리 4.3 [14] 에 의하여 주기가 2^m-1인 쉬프트 레지스터 수열들의 집합은 mod2 연산에 관하여 가환군(Abelian group)을 이룬다. 따라서 이 집합에 속하는 두 수열들의 합도 역시 주기가 2^m-1인 쉬프트 레지스터 수열이 된다. 그러므로 정리 1에 의하여 $A(\{c_i\}+\{c_j\})$의 각 열은 0-수열이거나 β에 의해서 생성된 수열이다. □

[정리 4] 임의의 $i, j, \tau(1\le i,j\le 2^m,\ 0\le\tau\le N-1)$에 대하여 $i\neq j$이거나 $\tau\neq 0$이면
$R_{i,j}(\tau)\in\{-2^m-1,\ -1,\ 2^m-1\}$ 이다.
(증명) $0\le t\le N-1$에 대하여
$t=t_1Q+t_2 \quad (0\le t_1\le 2^m-2,\ 0\le t_2\le Q-1)$라 하자.
$f_1(t) := \Big[Tr_m^n(\alpha^{2(t+\tau)})+\gamma_i\alpha^{Q(t+\tau)}\Big]^r+\Big[Tr_m^n(\alpha^{2(t+\tau)})\Big]^r$
$+\Big[Tr_m^n(\alpha^{2t})+\gamma_j\alpha^{Qt}\Big]^r+\Big[Tr_m^n(\alpha^{2t})\Big]^r$ 라 하면

$$c_i(t+\tau)+c_j(t)=Tr_1^m\{\alpha^{2rQt_1}\cdot f_1(t_2)\} \tag{2}$$

보조정리 2와 따름정리 3에 의하여 (2)의 각 열은 0-수열 이거나 m-수열이다.

$$z := |\{t_2\mid f_1(t_2)=0,\ 0\le t_2\le Q-1\}|$$

라 두면 0-수열인 열의 개수는 z, m-수열인 열의 개수는 $(2^m+1)-z$이다. 그러므로

$$\begin{aligned} R_{i,j}(\tau) &= \sum_{t=0}^{N-1}(-1)^{c_i(t+\tau)+c_j(t)} \\ &= z(2^m-1)-(2^m+1-z)=2^m(z-1)-1 \end{aligned}$$

이다. $\gamma_i=\gamma_j$, $\tau=0$인 경우를 제외하고 $\gamma_i,\ \gamma_j\in GF(2^m)$와 $\tau(0\le\tau\le N-1)$에 대하여 z은 0, 1, 2의 세 개의 값 중 하나를 가짐을 보이면 증명은 끝이 난다.
$0\le t\le N-1$에 대하여

$$f_2(t_2) := Tr_m^n\{\alpha^{2t_2}(1+\alpha^{2\tau})\}+\alpha^{Qt_2}(\gamma_i\alpha^{Q\tau}+\gamma_j)$$

라 정의하자. $\gcd(r,2^m-1)=1$이면

$$f_2(t_2)=0 \quad\Leftrightarrow\quad f_1(t_2)=0 \ \ (0\le t_2\le Q-1)$$

이다. 왜냐하면 $f_2(t_2)=0$이면 $\alpha^{2\tau}=1$이고 $\gamma_j=\gamma_i\alpha^{Q\tau}$이므로

$$\begin{aligned} f_1(t_2) &= \Big[Tr_m^n(\alpha^{2(t_2+\tau)})+\gamma_i\alpha^{Q(t_2+\tau)}\Big]^r+\Big[Tr_m^n(\alpha^{2(t_2+\tau)})\Big]^r \\ &\quad+\Big[Tr_m^n(\alpha^{2t_2})+\gamma_j\alpha^{Qt_2}\Big]^r+\Big[Tr_m^n(\alpha^{2t_2})\Big]^r \\ &= \Big[Tr_m^n(\alpha^{2t_2})+\gamma_j\alpha^{Qt_2}\Big]^r+\Big[Tr_m^n(\alpha^{2t_2})\Big]^r \\ &\quad+\Big[Tr_m^n(\alpha^{2t_2})+\gamma_j\alpha^{Qt_2}\Big]^r+\Big[Tr_m^n(\alpha^{2t_2})\Big]^r=0 \end{aligned}$$

이다. 역으로 $f_1(t_2)=0$이면 다음 세 가지 경우가 생긴다.

(ⅰ) $\Big[Tr_m^n(\alpha^{2(t_2+\tau)})+\gamma_i\alpha^{Q(t_2+\tau)}\Big]^r=\Big[Tr_m^n(\alpha^{2(t_2+\tau)})\Big]^r$ 이고 $\Big[Tr_m^n(\alpha^{2t_2})+\gamma_j\alpha^{Qt_2}\Big]^r=\Big[Tr_m^n(\alpha^{2t_2})\Big]^r$ 인 경우에 $\gamma_i=\gamma_j=0$ 이다.

(ⅱ) $\Big[Tr_m^n(\alpha^{2(t_2+\tau)})+\gamma_i\alpha^{Q(t_2+\tau)}\Big]^r=\Big[Tr_m^n(\alpha^{2t_2})+\gamma_j\alpha^{Qt_2}\Big]^r$ 이고 $\Big[Tr_m^n(\alpha^{2(t_2+\tau)})\Big]^r=\Big[Tr_m^n(\alpha^{2t_2})\Big]^r$ 인 경우에 $\alpha^{2\tau}=1$이고 $\gamma_j=\gamma_i\alpha^{Q\tau}$ 이다.

(ⅲ) $\Big[Tr_m^n(\alpha^{2(t_2+\tau)})+\gamma_i\alpha^{Q(t_2+\tau)}\Big]^r=\Big[Tr_m^n(\alpha^{2t_2})\Big]^r$ 이고 $\Big[Tr_m^n(\alpha^{2(t_2+\tau)})\Big]^r=\Big[Tr_m^n(\alpha^{2t_2})+\gamma_j\alpha^{Qt_2}\Big]^r$ 인 경우에 $\gamma_i=\gamma_j=0,\ \alpha^{2\tau}=1$ 이다.

$\gamma_i \neq 0,\ \gamma_j \neq 0$이므로 (i), (iii)을 제외한 (ii)에 의해서 $f_2(t_2)=0$이다.그러므로 $f_1(t_2)=0(0 \le t_2 \le Q-1)$을 만족하는 t_2의 개수를 구하는 것과 $f_2(t_2)=0$을 만족하는 t_2의 개수를 구하는 것은 같다.

$$x := \alpha^{t_2} \in GF(2^n)^* \ (GF(2^n)^* = GF(2^n) - \{0\})$$

라 하자. 그러면

$$\begin{aligned} f_2(t_2) &= Tr_m^n\{\alpha^{2t_2}(1+\alpha^{2\tau})\} + \alpha^{Qt_2}(\gamma_i\alpha^{Q\tau}+\gamma_j) \\ &= Tr_m^n\{x^2(1+\alpha^{2\tau})\} + x^{2^m+1}(\gamma_i\alpha^{Q\tau}+\gamma_j) \\ &= x^2(1+\alpha^{2\tau}) + x^{2^{(m+1)}}(1+\alpha^{2\tau})^{2^m} + x^{2^m+1}(\gamma_i\alpha^{Q\tau}+\gamma_j) \\ &= x^2\{y^2(1+\alpha^{2\tau})^{2^m} + y(\gamma_i\alpha^{Q\tau}+\gamma_j) + (1+\alpha^{2\tau})\} \end{aligned}$$

이다. 여기서 $y := x^{2^m-1}$이다.

$F_2(y) := y^2(1+\alpha^{2\tau})^{2^m} + y(\gamma_i\alpha^{Q\tau}+\gamma_j) + (1+\alpha^{2\tau})$라 하자. 그러면 $f_2(t_2)=0$를 만족하는 t_2의 개수는 $F_2(y)=0$를 만족하는 y의 개수와 같다. 따라서 $F_2(y)=0$를 만족하는 y의 개수가 0, 1 혹은 2임을 보이면 된다.

두 가지 경우로 나누어 생각하자.

(i) $\tau=0,\ \gamma_i \neq \gamma_j$ 인 경우:

$F_2(y) = y(\gamma_i+\gamma_j) \neq 0$ 이므로 $z=0$ 이다. 그러므로 $R_{i,j}(0) = -2^m - 1\ (i \neq j)$ 이다.

(ii) $\tau \neq 0$ 인 경우:

$$F_2(y)=0 \Leftrightarrow y^2(1+\alpha^{2\tau})^{2^m} + y(\gamma_i\alpha^{Q\tau}+\gamma_j) + (1+\alpha^{2\tau}) = 0 \quad (3)$$

이다. y에 관한 2차방정식의 계수들은 모두 $GF(2^n)$의 원소들이므로 이 2차방정식은 $GF(2^n)$ 위에서 해를 0개, 1개 혹은 2개를 가질 수 있다.

$$A := (1+\alpha^{2\tau})^{2^m},\ B := (\gamma_i\alpha^{Q\tau}+\gamma_j),\ C := 1+\alpha^{2\tau}$$

라 두면 (3)에서의 2차방정식은 $Ay^2+By+C=0$ 이다. $B=0$이면 해를 하나만 갖고 $B \neq 0$인 경우에 $Tr_1^n\left(\frac{AC}{B^2}\right)=1$ 이면 해가 존재하지 않으며 $Tr_1^n\left(\frac{AC}{B^2}\right)=0$ 이면 두 개의 해를 갖는다[15].

따라서 $z=0, 1, 2$ 가 된다. □

Ⅳ. 선형스팬

이 절에서는 GMW 수열과 No 수열에 의하여 합성된 새로운 수열의 선형스팬을 구하고자 한다. 다음 정리 5에서는

$$c_i(t) := Tr_1^m\{[Tr_m^n(\alpha^{2t}) + \gamma_i\alpha^{Qt}]^r\} + Tr_1^m\{[Tr_m^n(\alpha^{2t})]^r\}$$

$(\gamma_i \neq 0)$의 선형스팬에 대해 분석한다.

[정리 5] $c_i(t)$의 선형스팬 $l_{span} > m \cdot 2^w$ 이다.
(ω는 r을 이진수로 나타냈을 때 1의 총 개수)

(증명) 먼저 수열 $s(t) \in S$에 대해서 $l_{span} \ge m \cdot 2^w$ 임을 보이자.

$$s(t) := Tr_1^m\{[Tr_m^n(\alpha^{2t}) + \gamma\alpha^{Qt}]^r\} \quad (4)$$

선형 스팬(linear span)은 α^t에 관한 다항식으로 표현하여 0이 아닌 계수들을 갖는 α^t의 멱승의 개수를 구함으로서 결정된다. (4)에서 $\alpha^t := x$라 하면 다음과 같다.

$$s(x) = Tr_1^m\{\ [Tr_m^n(x^2) + \gamma \cdot x^{2^m+1}]^r\} \quad (5)$$

(5)에서 $y := x^{2^m-1}$라 두면

$$\begin{aligned} s(x) &= Tr_1^m\{[Tr_m^n(x^2) + \gamma \cdot x^{2^m+1}]^r\} \\ &= Tr_1^m\{[x^2 + (x^2)^{2^m} + \gamma \cdot x^{2^m+1}]^r\} \\ &= Tr_1^m\{x^{2r}[1 + x^{2(2^m-1)} + \gamma \cdot x^{2^m-1}]^r\} \\ &= Tr_1^m\{x^{2r}[1 + \gamma \cdot y + y^2]^r\} \\ &= \sum_{j=0}^{m-1} x^{2r \cdot 2^j}[1 + \gamma \cdot y + y^2]^{r \cdot 2^j} \end{aligned} \quad (6)$$

이다. (6)에서의 임의의 두 항

$x^{2r \cdot 2^{j_1}}[1+\gamma \cdot y+y^2]^{r \cdot 2^{j_1}}$과 $x^{2r \cdot 2^{j_2}}[1+\gamma \cdot y+y^2]^{r \cdot 2^{j_2}}$

의 전개식에서 x의 지수들은 서로 다르다. 그러므로 수열 $s(t)$의 선형 스팬은

$$g(y) := [1+\gamma \cdot y+y^2]^r \quad (7)$$

의 전개식에서 서로 다른 x의 멱승들의 수의 m 배이다. r의 이진 전개에서 R을 런(run)들의 수라 하고 $L_j(1 \le j \le R)$를 j번째 런의 길이라고 하자. 따라서 r을 다음과 같은 형태로 나타낼 수 있다.

$$r=\sum_{j=1}^{R}2^{e_j}\left(\sum_{k=0}^{L_j-1}2^k\right) \tag{8}$$

여기서 e_j는 j번째 런에서 가장 낮은 2의 지수승을 나타낸다. 그러면

$$e_{j+1}\geq e_j+L_j+1\,(j=1,2,\cdots,R-1) \tag{9}$$

이다. (8), (9)를 이용하면 (7)은 다음과 같다.

$$\begin{aligned}g(y)&=\left[1+\gamma\cdot y+y^2\right]^r=\left[1+\gamma\cdot y+y^2\right]^{\sum_{j=1}^{R}2^{e_j}r_j}\\&=\prod_{j=1}^{R}\left[1+(\gamma\cdot y)^{2^{e_j}}+\left(y^2\right)^{2^{e_j}}\right]^{r_j}\end{aligned} \tag{10}$$

여기서 $r_j:=\sum_{k=0}^{L_j-1}2^k=2^{L_j}-1\,(1\leq j\leq R)$이다. (10)에서

$$g_j(y)=\left[1+(\gamma\cdot y)^{2^{e_j}}+\left(y^2\right)^{2^{e_j}}\right]^{r_j} \tag{11}$$

라 하자. (11)에서 y의 0이 아닌 지수는 2^{e_j}의 상수배이며 2^{e_j}와 $2^{e_j+1}\cdot r_j$ 사이에 있다. $g(y)=\prod_{j=1}^{R}g_j(y)$이므로 $g(y)$의 전개식에서 생길 수 있는 y의 지수들은 $a:=\sum_{j=1}^{R}a_j$와 같은 형태이다.

(9)로부터 $2^{e_{j+1}}\geq 2^{e_j+1}\cdot 2^{L_j}>2^{e_j+1}\left(2^{L_j}-1\right)=2^{e_j+1}\cdot r_j$이므로 $2^{e_j}\leq a_j\leq 2^{e_j+1}\cdot r_j<2^{e_{j+1}}$이며 $2^{e_j}\,|\,a_j$이다.

따라서 $a=\sum_{j=1}^{R}a_j$와 $b:=\sum_{j=1}^{R}b_j$가 같을 필요충분조건은 모든 $j=1,2,\cdots,R$에 대하여 $a_j=b_j$이다. 그러므로 $g(y)$의 전개식에서의 y의 서로 다른 지수들의 개수를 M이라 하고 $g_j(y)$에서의 y의 서로 다른 지수들의 개수를 M_j라 하면 $M=\prod_{j=1}^{R}M_j$ 이다.

(ⅰ) $\gamma=0$인 경우: $z:=y^{2^{e_j}}$라 두면

$g_j(y)=\left[1+z^2\right]^{r_j}=\sum_{k=0}^{r_j}z^{2k}$, $M_j=r_j+1$ 이며

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

여기서 w는 r의 이진표현에서 나타나는 1의 총 개수이다. 그러므로 수열 $s(t)$의 선형 스팬은 $m\cdot 2^w$이다.

(ⅱ) $\gamma\neq 0$인 경우: $z:=y^{2^{e_j}}$, $\eta:=\gamma^{2^{e_j}}$라 하면

$$g_j(z)=\left[1+\eta z+z^2\right]^{r_j} \tag{12}$$

이다. (12)을 인수분해 하면

$$\begin{aligned}g_j(z)&=(z+\delta)^{r_j}(z+\delta^{-1})^{r_j}\\&=\left(\sum_{k=0}^{r_j}\delta^{r_j-k}z^k\right)\left(\sum_{l=0}^{r_j}\delta^{l-r_j}z^l\right)\end{aligned} \tag{13}$$

(13)을 전개하여 정리하면 다음과 같다:

$$\begin{aligned}&g_j(z)=\\&\sum_{k=0}^{r_j}\delta^k z^k\left[\frac{(\delta^{-2})^{k+1}+1}{\delta^{-2}+1}\right]+\sum_{k=1}^{r_j}\delta^{k-1}z^{2r_j-(k-1)}\left[\frac{(\delta^{-2})^k+1}{\delta^{-2}+1}\right]\end{aligned} \tag{14}$$

$P_j:=\left|\left\{k:\delta^k=1(\ 1\leq k\leq r_j)\right\}\right|$라 두면

$(\delta^{-1})^k=(\delta^k)^{-1}=1$이므로 $g_j(z)$에서 없어지는 계수들의 수는 $2P_j$이다. 따라서

$M_j=2r_j+1-2P_j=2\cdot(2^{L_j}-1)+1-2P_j=2^{L_j+1}-1-2P_j$

이다. P_j를 알기 위하여 이차방정식의 집합

$\left\{y^2+\gamma_i y+1=0\,|\,1\leq i\leq 2^m\right\}$ 과

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

는 일대일대응임을 보이자. 여기서 α는 $GF(2^n)$의 원시원소이다. 만일 β가 $GF(2^m)$의 원시원소이면 $\beta=\alpha^{2^m+1}$이다.

$$\text{방정식 } y^2+\gamma\cdot y+1=0,\gamma\in GF(2^m) \tag{15}$$

의 근들의 집합은 어떤 $\delta\in GF(2^n)$에 대하여 $\{\delta,\delta^{-1}\}$이다.

(i) 2차방정식 (15)가 $GF(2^m)$ 위에서 인수분해 될 때: 만일 $\gamma=0$이면 $y=1\in R$이다. $GF(2^m)$의 원시원소를 β ($\beta^{2^m-1}=1$)라 하자. (15)는 반드시 해를 가져야 하므로 $A=C:=1,\ B:=\gamma$ 라면

$Tr_1^m\left(\frac{AC}{B^2}\right)=Tr_1^m(\gamma^{-2})=0$ 이다. 따라서

$y=\beta^l=(\alpha^{2^m+1})^l=\alpha^{l\cdot(2^m+1)}$ $(1\leq l\leq 2^m-2)$ 이다.

(ii) 2차방정식 (15)가 $GF(2^m)$ 위에서 인수분해 되지 않을 때: $GF(2^n)$에서 해 δ를 가지면 $\delta+\delta^{-1}=\gamma$ 이다. 따라

서 $(\delta+\delta^{-1})^{2^m-1}=\gamma^{2^m-1}=1$이다. 그러므로

$$\delta+\delta^{-1}=(\delta+\delta^{-1})^{2^m}=\delta^{2^m}+\delta^{-2^m} \quad (16)$$

이고 $\delta\notin GF(2^m)$ 이므로 $\delta^{-1}=\delta^{2^m}$ 이다. 즉, $\delta^{2^m+1}=1$ 이다. 그러므로 $\delta=(\alpha^{2^m-1})^u=\alpha^{u(2^m-1)}\ (1\le u\le 2^m)$ 형태가 되어야 한다. 임의의 $\delta\in T$에 대하여

$(y-\delta)(y-\delta^{-1})=y^2+(\delta+\delta^{-1})y+1=0$ 이다.

만일 $\delta:=\alpha^{u(2^m+1)}(1\le u\le 2^{m-1}-1)$라면

$\delta+\delta^{-1}=\alpha^{u(2^m+1)}+\alpha^{-u(2^m+1)}=\beta^u+\beta^{-u}\in GF(2^m)$

이다. 또한 $\delta:=\alpha^{v(2^m-1)}(1\le v\le 2^{m-1})$라면

$\delta+\delta^{-1}=\alpha^{v(2^m-1)}+\alpha^{-v(2^m-1)}$ 이다. (16)에 의하여

$(\delta+\delta^{-1})^{2m}=\delta^{2^m}+\delta^{-2m}=\delta^{-1}+\delta=\delta+\delta^{-1}$

이므로 $\delta+\delta^{-1}\in GF(2^m)$이다.

수열 $s(t)$의 선형 스팬을 구하기 위하여 두 가지로 나누어 생각한다.

(i) $y^2+\gamma\cdot y+1=0(\gamma\in GR(2^m))$가 $GF(2^m)$에서 해를 가지는 경우: 그 해는 $\delta=\alpha^{a(2^m+1)}(1\le a\le 2^{m-1}-1)$의 형태이다. $\gamma\neq 0,\ \delta\neq 1$이라 하자.

그러면 $P_j=|\{k(1\le k\le r_j):\delta^k=1\}|$ 이다.

$\delta^k=(\alpha^{a(2^m+1)})^k=\alpha^{ak(2^m+1)}=1,\ \alpha^{2^n-1}=(\alpha^{2^m+1})^{2^m-1}=1$

이므로 $ak\equiv 0(\mathrm{mod}(2^m-1))$ 이다.

$g:=\gcd(a,2^m-1)$라 하면 $k\equiv 0\ (\mathrm{mod}\frac{2^m-1}{g})$ 이다. 따라서 $P_j=\left\lfloor \frac{r_j}{(2^m-1)/g} \right\rfloor$ 이다. 그러므로 $s(t)$의 선형스팬 l_{span}은 다음과 같다:

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

$a\le 2^m-1$이고 $g\le 2^{m-1}-1$이므로 $\frac{2^m-1}{g}>2$이다. 따라서 다음과 같은 결과가 나온다.

$$l_{span}>m\cdot\prod_{j=1}^{R}(2^{L_j+1}-1-(2^{L_j}-1))=m\cdot\prod_{j=1}^{R}2^{L_j}=m\cdot 2^w$$

(ii) $y^2+\gamma y+1=0(\gamma\in GF(2^m))$가 $GF(2^m)$ 에서 해를 가지지 않는 경우:

그 해는 $\delta=\alpha^{a(2^m-1)}(1\le a\le 2^{m-1})$의 형태이다. (i)과 같은 방법으로 l_{span}을 다음과 같이 얻을 수 있다:

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

$\frac{2^m+1}{g}>2$ 이다. 따라서

$$l_{span}>m\cdot\prod_{j=1}^{R}(2^{L_j+1}-1-(2^{L_j}-1))=m\cdot\prod_{j=1}^{R}2^{L_j}=m\cdot 2^w$$

지금까지 수열 $s(t)\in S$에 대해서 $l_{span}\ge m\cdot 2^w$ 임을 보였다.

$c(t):=Tr_1^m\{[Tr_m^n(\alpha^{2t})+\gamma\alpha^{Qt}]^r+[Tr_m^n(\alpha^{2t})]^r\}$

에 대해서 $\alpha^t:=x$라 하면 다음과 같다:

$c(x)=Tr_1^m\{[Tr_m^n(x^2)+\gamma\cdot x^{2^m+1}]^r+[Tr_m^n(x^2)]^r\}$

$y:=x^{2^m-1}$라 두면

$c(x)=Tr_1^m\{[Tr_m^n(x^2)+\gamma\cdot x^{2^m+1}]^r+[Tr_m^n(x^2)]^r\}$

$=Tr_1^m\{[x^2+(x^2)^{2^m}+\gamma\cdot x^{2^m+1}]^r+[x^2+(x^2)^{2^m}]^r\}$

$=Tr_1^m\{x^{2r}[1+x^{2(2^m-1)}+\gamma\cdot x^{2^m-1}]^r+x^{2r}[1+x^{2(2^m-1)}]^r\}$

$=Tr_1^m\{x^{2r}[1+\gamma\cdot y+y^2]^r+x^{2r}[1+y^2]^r\}$

$=\sum_{j=0}^{m-1}x^{2r\cdot 2^j}\{[1+\gamma\cdot y+y^2]^{r\cdot 2^j}+[1+y^2]^{r\cdot 2^j}\}$

이고, (10)과 같은 방법으로

$q(y)=[1+\gamma\cdot y+y^2]^r+[1+y^2]^r$

$=[1+\gamma\cdot y+y^2]^{\sum_{j=1}^{R}2^{e_j}r_j}+[1+y^2]^{\sum_{j=1}^{R}2^{e_j}r_j}$

$=\prod_{j=1}^{R}[1+(\gamma\cdot y)^{2^{e_j}}+(y^2)^{2^{e_j}}]^{r_j}+\prod_{j=1}^{R}[1+(y^2)^{2^{e_j}}]^{r_j}$

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

$q(y)=\prod_{j=1}^{R}[1+\eta z+z^2]^{r_j}+\prod_{j=1}^{R}[1+z^2]^{r_j}$ 이다.

$g_j(z)=[1+\eta z+z^2]^{r_j}$, $P_j:=|\{k:\delta^k=1(\ 1\le k\le r_j)\}|$ 라 두면 (14)에서 $\delta^k=1$ 또는 $\delta^{k+1}=1$ 이면 항이 없어지므로 없어지는 $2P_j$개의 z의 지수 중 절반이 짝수이다. $g_j(z)$에서 없어지는 항 중 지수가 짝수인 항은 $[1+z^2]^{r_j}$의 전개식에서 나타난다. $[1+z^2]^{r_j}$의 전개식에서 P_j개를 제외한 모든 항이 없어진다고 생각했을 때 $q(y)$ 선형스팬의 하한값은 아래와 같다:

$\prod_{j=1}^{R}(2r_j+1-2P_j)+\prod_{j=1}^{R}(r_j+1)-2\prod_{j=1}^{R}(r_j+1-P_j)$

$>\prod_{j=1}^{R}(r_j+1)=\prod_{j=1}^{R}2^{L_j}=2^w$

$(\because\ \prod_{j=1}^{R}(2r_j-2P_j+1)>2\prod_{j=1}^{R}(r_j-P_j+1))$

따라서 $l_{span}>m\cdot 2^w$ 이다. □

V. 결 론

지금까지 본 논문에서는 GMW 수열과 No 수열을 합성하여 얻은 수열들의 집합을 소개하고 분석하였다. 집합 안의 각 수열들은 주기 $N=2^n-1$ 이고 $n=2m$ 이며 2^m 개의 수열들이 있다. 합성된 수열의 상관계수 값이 -2^m-1, -1, 2^m-1이며 선형스팬의 크기가 $m2^w$ 이상임을 보였다.

참고문헌

[1] R. A. Scholtz and L. R. Welch, "GMW Sequences," IEEE Trans. Inform. Theory, vol. IT-30, no. 3, pp. 548-553, May 1984.

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

[3] M. P. Ristenbatt and J. L. Daws, Jr., "Performance criteria for spread spectrum communications," IEEE Trans. Commun., vol. COM-25, no. 8, pp. 756-763, Aug. 1977.

[4] 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.

[5] 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.

[6] 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.

[7] A. Lempel and M. Cohn, "Maximal families of bent sequences," IEEE Trans. Inform. Theory, vol. IT-28, pp. 865-868, Nov. 1982.

[8] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," IEEE Trans. Inform. Theory, vol. IT-13, no. 5, pp. 619-621, Oct. 1967.

[9] 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.

[10] T. Kasami, "Weight distribution formula for some class of cyclic codes," Coordinated Science Laboratory, University of Illinois, Urbana, Tech. Rep. R-285(AD632574), 1966.

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

[12] 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.

[13] E.L. Key, An analysis of the structure and complexity of nonlinear binary sequence generators, IEEE Trasn. Infor. Theor. vol. 22, no. 6, pp. 732-736, Nov. 1976.

[14] S.W. Golomb, Shift register sequences, Holden-Day, Inc, 1967.

[15] 조성진 외 2인, 알기 쉬운 유한체론, 경문사, 2005.

저자소개

조성진(Sung-Jin Cho)

1979년 2월: 강원대학교 수학교육과 학사
1981년 2월: 고려대학교 수학과 석사
1988년 2월: 고려대학교 수학과 박사
1988년 ~ 현재: 부경대학교 응용수학과 정교수
※관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론

임지미(Ji-Mi Yim)

1997년 2월: 부산대학교 수학교육과 학사
2008년 8월: 부경대학교 교육대학원 수학과 석사
2008년 ~ 현재: 부경대학교 응용수학과 박사과정
※관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론