GMW 수열과 No 수열에 의해서 생성된 수열의 확장수열

조성진* · 임지미** · 김진경** · 김석태***

Extended sequences of sequences generated by GMW sequences and No sequences

Sung-Jin Cho* · Ji-Mi Yim** · Jin-Gyoung Kim** · Seok-Tae Kim***

요 약

본 논문에서는 GMW 수열과 No 수열에 의해 생성된 이진수열을 확장하여 새로운 형태의 수열을 소개한다. 그리고 확장된 수열의 상관계수를 분석하고 르장드르 수열로부터 생성되는 확장수열을 제시한다. 이는 암호 시스템 및 통신 시스템에 도움이 되며 특히 CDMA 시스템 신호 디자인에 유용한 연구이다.

ABSTRACT`

In this paper, we introduce the extended sequences of sequences generated by GMW sequences and No sequences. And we analyze cross-correlatons of the extended sequences. Also we give extended sequences which are constructed from Legendre sequences. This is helpful to a cryptosystem and a communication system. Particularly this study is useful to the CDMA system signal design.

키워드

GMW seuqnce, No sequence, correlation, trace, Legendre sequence
GMW 수열, No 수열, 상관계수, 트레이스, Legendre 수열

Ⅰ. 서 론

낮은 상관계수를 갖는 수열들은 많은 사용자들을 구별하고 상호 간섭을 적게 일으키는 채널을 얻기 위한 무선 통신에 적용이 되고 있다. 또한 구별되는 다량의 수열들 또한 많은 사용자와 채널에 이용된다. 낮은 상관계수를 갖는 다량의 수열들을 얻기 위해 Gold[1], Kasami[2], Bent[3] 등이 연구해 왔다. 이러한 노력들은 Welch[4]의 연구에서와 같이 이론적으로 낮은 하한선을 갖는 상관계수를 갖고 주어진 상관계수에서 패밀리 사이즈를 최대화하는 이진 수열을 구성하는데 집중되었다. 그리고 Cho[5-8] 등은 비선형 수열의 생성과 그것들의 상호상관계수에 대해 연구하였다. 이진수열은 확산대역방식(Spread Spectrum System), 광대역 위성통신(Broadband Satelite Communication), 이동 라디오 통신 시스템에서 다중 접속 방식을 위해 채택되고 있는 코드 분할 다중 접근(Code Division Multiple Access, CDMA) 시스템에 많은 적용이 되고 있다. CDMA 시스템을 위한 신호 디자인은 응용 분야에서 흥미로운 연구과제이

* 교신저자 : 부경대학교(sjcho@pknu.ac.kr)
** 부경대학교(jimiya15@hanmail.com, 5892587@hanmail.net)
*** 부경대학교(setakim@pknu.ac.kr)
접수일자 : 2012. 01. 06 심사(수정)일자 : 2012. 03. 15 게재확정일자 : 2012. 04. 07

다. CDMA 시스템 신호 디자인을 위한 가장 중요한 연구주제 중 하나는 적합한 상관계수 공리를 갖는 이진수열을 디자인하는 것이다. GMW 수열과 No 수열은 이러한 조건들을 만족하는 이진수열들이다. No 수열은 주기가 $N=2^n-1$ 이고 $n=2m$ 이다. 수열들의 집합에는 2^m개의 수열들이 있고 상관계수의 최댓값은 2^m+1 이다. 본 논문에서는 2절에서 GMW 수열과 No 수열의 특성을 포함한 배경지식들을 소개하고 3절에서는 GMW 수열과 No 수열에 의해 생성된 이진수열[9]을 소개한다. 4절에서는 3절에서의 수열을 확장한 형태의 수열을 구성하여 상관계수를 분석하고 5절에서는 르장드르(Legendre) 수열로부터 생성되는 확장수열을 제시한다.

II. 배경지식

[정의 1] 집합 $C:=\{c_i(t)\,|\,0\le t\le N-1\}$를 주기가 $N:=2^n-1$인 이진 수열들의 집합이라 하자.
$1\le i,j\le |C|$에 대하여 다음과 같이 정의된 $R_{i,j}(\tau)$을 C의 i번째 수열과 j번째 수열에 대한 상관함수(correlation function)라 한다.

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

[정의 2] $m|n$을 만족하는 $m,n\in\mathbb{N}$에 대하여 다음과 같이 정의된 함수 $Tr_m^n: GF(2^n)\to GF(2^m)$을 트레이스(trace) 함수라 한다:

$$Tr_m^n(x)=\sum_{j=0}^{n/m-1}x^{2^{m\cdot j}}$$

[정리 3] 트레이스 함수는 다음 성질을 만족한다.

1) $Tr_m^n(\alpha)=Tr_m^n(\alpha^{2mi}),\ \alpha\in GF(2^n),\ i\in\mathbb{N}$
2) $Tr_m^n(a\alpha+b\beta)=aTr_m^n(\alpha)+bTr_m^n(\beta)$
   $a,b\in GF(2^m),\ \alpha,\beta\in GF(2^n)$
3) 방정식 $Tr_m^n(x)=a,\ a\in GF(2^m)$을 만족하는 해는 2^{n-m}개다. $x\in GF(2^n)$
4) 0이 아닌 모든 $\delta\in GF(2^n)$ 에 대하여
$$\sum_{\alpha\in GF(2^n)}(-1)^{Tr_1^n(\delta\alpha)}=0$$
5) $Tr_1^n(\alpha)=Tr_1^m(Tr_m^n(\alpha)),\ \alpha\in GF(2^n)$

$a_i=Tr_1^n(\alpha^i),\ 0\le i\le 2^n-2,\ i\in\mathbb{N}$라 두면 수열 $\{a_i\}$은 m-수열이 되고, 상관계수들의 집합은 $\{-1,2^n-1\}$이다.
$m|n$을 만족하는 $m,n\in\mathbb{N}$에 대하여 다음과 같이 정의된 수열 $\{b_i\}$을 GMW 수열이라 한다[10].
$b_i=Tr_1^m\{[Tr_m^n(\alpha^i)]^r\}$
여기서 α는 $GF(2^n)$의 한 원시원소이며 r $(1\le r<2^m-1)$은 $\gcd(r,2^m-1)=1$을 만족한다.
GMW 수열의 상관계수들의 집합은 $\{-1,2^n-1\}$이다.

$n:=2m(m>0,m\in\mathbb{N}),N:=2^n-1,Q=2^m+1$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.
$i\ne j(1\le i,j\le 2^m)$이면 $\gamma_i\ne\gamma_j(\gamma_i,\gamma_j\in GF(2^m))$이며 $GF(2^m)=\{\gamma_i\,|\,1\le i\le 2^m\}$이다.
(1)에서 $\gamma_i=0$ 일 때 GMW 수열이고, $\gamma_i\ne 0$ 일 때, No 수열이다 [10, 11]. No 수열의 상관계수들의 집합은 $\{-2^m-1,-1,2^m-1\}$ 이다.

III. GMW 수열과 No 수열에 의해 생성된 수열

GMW 수열과 No 수열의 합성수열 $c_i(t)$가 다음과 같다고 하자.

$$c_i(t) := Tr_1^m\{[Tr_m^n(\alpha^{2t})+\gamma_i\alpha^{Qt}]^r\}+Tr_1^m\{[Tr_m^n(\alpha^{2t})]^r\}$$
$$(\gamma_i \neq 0)$$

여기서 α는 $GF(2^n)$의 한 원시원소이며 r $(1 \le r < 2^m-1)$은 $\gcd(r,2^m-1)=1$을 만족한다. $i\neq j(1 \le i,j \le 2^m)$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.

[보조정리 4] 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.
(단, $\beta=\alpha^Q$)
(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. $t=t_1Q+t_2$ $(0 \le t_1 \le 2^m-2,\ 0 \le t_2 \le Q-1)$ 라 하자. 그러면 β는 $GF(2^m)$의 원시원소이며 $c_i(t)$는 다음과 같다.

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

$w(t_2)=\left[Tr_m^n\left(\alpha^{2t_2}\right)+\gamma_i\beta^{t_2}\right]^r+\left[Tr_m^n\left(\alpha^{2t_2}\right)\right]^r$ 라 하면 $c_i(t)=Tr_1^m\left\{\beta^{2rt_1}w(t_2)\right\}$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. □

[따름정리 5] 두 수열 $\{c_i\}$와 $\{c_j\}$와 합성 수열에 대한 $(2^m-1,Q)$ 삽입수열 $A(\{c_i\}+\{c_j\})$의 각 열은 0-수열이거나 β에 의해서 생성된 m-수열이다.
(단, $\beta=\alpha^Q$)

[정리 6] 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.

$$\begin{aligned} f_1(t) := &\left[Tr_m^n(\alpha^{2(t+\tau)})+\gamma_i\alpha^{Q(t+\tau)}\right]^r+\left[Tr_m^n(\alpha^{2(t+\tau)})\right]^r \\ &+\left[Tr_m^n(\alpha^{2t})+\gamma_j\alpha^{Qt}\right]^r+\left[Tr_m^n(\alpha^{2t})\right]^r \end{aligned}$$

라 하면

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

보조정리 4와 따름정리 5에 의하여 (2)의 각 열은 0-수열이거나 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 γ_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

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

라 정의하자. $\gcd(r,2^m-1)=1$이면

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

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

$$f_1(t_2)=\left[Tr_m^n(\alpha^{2(t_2+\tau)})+\gamma_i\alpha^{Q(t_2+\tau)}\right]^r+\left[Tr_m^n(\alpha^{2(t_2+\tau)})\right]^r$$
$$+\left[Tr_m^n(\alpha^{2t_2})+\gamma_j\alpha^{Qt_2}\right]^r+\left[Tr_m^n(\alpha^{2t_2})\right]^r$$
$$=\left[Tr_m^n(\alpha^{2t_2})+\gamma_j\alpha^{Qt_2}\right]^r+\left[Tr_m^n(\alpha^{2t_2})\right]^r$$
$$+\left[Tr_m^n(\alpha^{2t_2})+\gamma_j\alpha^{Qt_2}\right]^r+\left[Tr_m^n(\alpha^{2t_2})\right]^r=0$$

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

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

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

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

$\gamma_i\neq0,\ \gamma_j\neq0$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.

$x:=\alpha^{t_2}\in GF(2^n)-\{0\}$ 라 하자. 그러면

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

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:

$F_2(y)=y(\gamma_i+\gamma_j)\neq0$ 이므로 $z=0$ 이다. 그러므로 $R_{i,j}(0)=-2^m-1\ (i\neq j)$ 이다.

(ii) $\tau\neq0$ 인 경우:

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

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 $B\neq0$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[12].

따라서 $z=0,\ 1,\ 2$ 가 된다. □

Ⅳ. GMW 수열과 No 수열에 의해 생성된 수열의 확장수열과 상관계수

m은 양의 정수이고 $n=2m,\ q=2^m$이라 하자. α,β는 각각 $GF(q^2)$, $GF(q)$의 원시원소이고 $\alpha^Q=\beta,\ Q=2^m+1$이다. 인덱스 집합 I와 집합 $\{b(t_1)\,|\,t_1=0,1,\cdots,M-1\},\ M=q-1$ 에 대해서 $b(t_1)=\sum_{a\in I}Tr_1^m(\beta^{at_1})$ 이 이상적인 자기상관계수 공리를 만족하는 경우만을 생각한다[13]. r은 $\gcd(r,M)=1,\ 1\le r<M$을 만족하는 양의 정수일 때, 확장수열은 다음과 같다:

$$c_E^{(ij)}(t)=\sum_{a\in I}Tr_1^m([N(\alpha^t)]^{ar})$$
$$N_{(ij)}(\alpha^t)=Tr_m^n(\alpha^{2t})+\gamma_i\alpha^{Qt}+Tr_m^n(\eta_j\alpha^{2t})$$
$$(\gamma_i\in GF(2^m),\ \eta_j\in GF(2^n))$$

α는 $GF(2^n)$의 고정된 원시원소라 하면 다음의 정리가 성립한다.

[정리 7] 수열 $\{c_E^{(ij)}(t)\}$, $\{c_E^{(ks)}(t)\}$의 상관계수는

$$R_{(ij)(ks)}(\tau)=\frac{qz_\tau-(q^2-1)}{q-1}$$

이다.

$(z_\tau = |\{t \mid N_{ij}(\alpha^t) + N_{ks}(\alpha^{t+\tau}) = 0\}| \ ) \ (0 \le t < q^2 - 1)$

(증명) $t = t_1 Q + t_2 \ (0 \le t_1 \le 2^m - 2,$
$0 \le t_2 \le Q-1), \ \beta = \alpha^Q$ 라 하자.

$N_{ij}(\alpha^t) = \beta^{2t_1}\{N_{ij}(\alpha^{t_2})\}$ 이고
$c_E^{(ij)}(t) = \sum_{a \in I} Tr_1^m\{\beta^{2rat_1}[N_{ij}(\alpha^{t_2})]^{ar}\}$ 이다.
$f(t) = [N_{ij}(\alpha^t)]^{ar} + [N_{ks}(\alpha^{t+\tau})]^{ar}$ 라 두면
$c_E^{(ij)}(t) + c_E^{(ks)}(t+\tau) = \sum_{a \in I} Tr_1^m\{\beta^{2rat_1} f(t_2)\}$이다.

$$R_{(ij)(ks)}(\tau) = \sum_{t=0}^{Q-1} (-1)^{c_E^{(ij)}(t) + c_E^{(ks)}(t+\tau)}$$
$$= \sum_{t_2=0}^{Q-1} \sum_{t_1=0}^{M-1} (-1)^{\sum_{a \in I} Tr_1^m[\beta^{2rat_1} f(t_2)]}$$

(i) $f(t_2) = 0$이면 $\sum_{t_1=0}^{M-1} (-1)^{\sum_{a \in I} Tr_1^m[\beta^{2rat_1} f(t_2)]} = M$

(ii) $f(t_2) \ne 0$이면 $\sum_{t_1=0}^{M-1} (-1)^{\sum_{a \in I} Tr_1^m[\beta^{2rat_1} f(t_2)]}$ 에서
(-1)의 지수는 수열 $\{b(2rt_1)\}$의 쉬프트이다.
$\gcd(2r, M) = 1$ 이므로 수열 $\{b(2rt_1)\}$는 밸런스이고 이상적인 자기상관계수 공리를 만족한다.
따라서 $f(t_2) \ne 0$ 이면

$$\sum_{t_1=0}^{M-1} (-1)^{\sum_{a \in I} Tr_1^m[\beta^{2rat_1} f(t_2)]} = -1 \text{ 이다.}$$

$z := |\{t_2 | f(t_2) = 0, 0 \le t_2 < Q\}|$ 라 두면

$R_{(ij)(ks)}(\tau) = -(Q - z) + (q-1)z = qz - \frac{q^2-1}{q-1}$이다.

$f(t+Q) = \alpha^{2arQ} f(t)$ 이므로

$$z = \frac{|\{t \mid f(t) = 0, 0 \le t < Q\}|}{q-1} = \frac{z_\tau}{q-1}$$

따라서 $R_{(ij)(ks)}(\tau) = \frac{qz_\tau - (q^2-1)}{q-1}$ 이다. □

정리 6, 정리 7 및 $b(t_1) = \sum_{a \in I} Tr_1^m(\beta^{at_1})$이 이상적인 자기상관계수 공리를 만족한다는 사실에 의해서 다음 정리가 성립한다.

[정리 8] 확장수열

$$c_E^{(ij)}(t) = \sum_{a \in I} Tr_1^m\{[Tr_m^n(\alpha^{2t}) + \gamma_i \alpha^{Qt} + Tr_m^n(\eta_j \alpha^{2t})]^{ar}\}$$

에 대해서 $\{c_E^{(ij)}(t)\}$와 $\{c_E^{(ks)}(t)\}$의 상관계수 $R_{(ij)(ks)}(\tau)$는 세 가지의 값 $-2^m - 1, \ -1, \ 2^m - 1$을 갖는다.
(증명) 정리 6에서 z의 값이 0, 1, 2가 되는 것과 마찬가지로 정리 7에서도 z의 값이 0, 1, 2가 된다.
$z = \frac{z_\tau}{q-1}$에 의해서 z_τ는 0, $q-1$, $2(q-1)$이다. 정리 7의 결과에 대입을 하면

$R_{(ij)(ks)}(\tau) \in \{-2^m - 1, \ -1, \ 2^m - 1\}$ 이다. □

Ⅴ. 르장드르 수열로부터 생성되는 확장수열

p를 2가 아닌 소수라 하면 주기가 p인 르장드르 수열 $\{b(t)\}$는 다음과 같다.

$$b(t) = \begin{cases} 1 & (t \equiv 0 \bmod p) \\ 0 & (t\text{가 이차잉여 } \bmod p) \\ 1 & (t\text{가 비이차잉여 } \bmod p) \end{cases}$$

$p \equiv 3 \pmod 4$이면 $b(t)$는 이상적인 자기상관계수 공리를 갖는다. 주기가 $p = 2^m - 1$(메르센느 소수)인 르장드르 수열의 트레이스 표현은 아래와 같다.

[보조정리 9][14] 소수 $M = 2^m - 1 \ (m \ge 3)$과 Z_M의 원시원소 u에 대해서 (Z_M은 $\bmod M$의 정수들의 집합) $\sum_{i=0}^{\frac{M-1}{2^m}-1} Tr_1^m(\alpha^{u^{2i}}) = 0$를 만족하는 $GF(2^m)$의 원

시원소 α가 존재하고 $c(t)=\sum_{i=0}^{\frac{M-1}{2m}-1} Tr_1^m(\alpha^{u^{2i}t})$인 주기 M인 수열 $\{c(t)|t=0,1,\cdots,M-1\}$는 르장드르 수열이다.

[정리 10] 정수 m에 대하여 $M=2^m-1$이 소수이고, $q=2^m$이며 u는 Z_M의 원시원소라 두자.
α는 $GF(2^n)$의 원시원소이다. $1\le r<M$인 r에 대하여 수열 $\{c^{(ks)}(t)\}$와 수열의 집합 Γ를 다음과 같이 두자.

$$c^{(ks)}(t)=\sum_{i=0}^{\frac{M-1}{2m}-1} Tr_1^m\left\{[Tr_m^n(\alpha^{2t})+\gamma_k\alpha^{Qt}+Tr_m^n(\eta_s\alpha^{2t})]^{ru^{2i}}\right\}$$

$(\gamma_k\in GF(2^m),\ \eta_s\in GF(2^n))$

$$\Gamma=\{\{c^{(ks)}(t)\}|1\le k\le 2^m,\ 1\le s\le 2^n\}$$

Γ에 속하는 서로 다른 두 수열 사이의 상관계수는 $\{-2^m-1,\ -1,\ 2^m-1\}$의 세 가지 값 중 하나이다. (단 $\tau\not\equiv 0(\mathrm{mod}N)$)

(증명) 보조정리 9에서 $\{c(t)|t=0,1,\cdots,M-1\}$ $(c(t)=\sum_{i=0}^{\frac{M-1}{2m}-1} Tr_1^m(\alpha^{u^{2i}t}))$는 이상적인 자기상관계수 공리를 만족하므로 정리8에 의해서 Γ에 속하는 서로 다른 두 수열 사이의 상관계수는 -2^m-1, -1, 2^m-1중 하나이다. □

Ⅵ. 결 론

본 논문에서는 GMW 수열과 No 수열에 의해 생성된 이진수열을 확장한 수열을 소개하였다. 그리고 확장된 수열의 상관계수가 $\{-2^m-1,\ -1,\ 2^m-1\}$의 세 가지 값만 가짐을 보였다. 또한 르장드르 수열로부터 생성된 확장수열을 얻었다. 이는 암호 시스템 및 통신 시스템에 도움이 되며 특히 CDMA 시스템 신호 디자인에 유용한 연구라고 사료된다.

감사의 글

이 논문은 2010년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2010-371-B00008).

참고 문헌

[1] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," IEEE Trans. Inform. Theory, Vol. IT-14, No. 1, pp. 154-156, Jan. 1968.

[2] T. Kasami, "Weight enumerators for several classes of subcodes of the 2nd order Reed-Muller codes," Inform. and Control, Vol. 18, No. 4, pp. 369-394, May. 1971.

[3] 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.

[4] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," IEEE Trans. Inform. Theory, Vol. IT-20, No. 3, pp. 397-399, May. 1974.

[5] 조성진, 최은숙, 김한두, 안현주, "수축생성기에 기반한 비선형 수열의 분석", 한국전자통신학회논문지, 5권, 4호, pp. 412-417, 2010.

[6] 최은숙, 조성진, 김진경, "GF(2^p)위에서의 LFSR과 CA를 이용한 shrunken 수열의 분석", 한국전자통신학회논문지, 5권, 4호, pp. 418-424, 2010.

[7] 김진경, 조성진, 최은숙, 황윤희, "Kasami 수열들과 No 수열들의 상호상관관계", 한국전자통신학회논문지, 6권, 1호, pp. 13-19, 2011.

[8] 최은숙, 조성진, "최적의 상호상관관계를 갖는 이진 수열의 설계", 한국전자통신학회논문지, 6권, 4호, pp. 539-544, 2011.

[9] 조성진, 임지미, "GMW 수열과 No 수열에 의해서 생성된 이진 수열 분석", 한국해양정보통신학회, 15권, 10호, pp. 2181- 2187, 2011.

[10] R. A. Scholtz and L. R. Welch, "GMW Sequences," IEEE Trans. Inform. Theory, Vol. IT-30, No. 3, pp. 548-553, 1984.

[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. 35, No. 2, pp. 371-379, Mar. 1989.
[12] 조성진, 표용수, 김한두, “알기 쉬운 유한체론”, 경문사, 2005.
[13] C. Fu, H. Wen and Z. Shi, "Extended d- form Sequences and Extended QF Sequences" International Conference on ITS Telecommunications Proceedings, 2006.
[14] J. S. No and H. K. Lee, H. Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period" IEEE Trans. Inform. Theory, Vol. 42, No. 6, pp. 2254-2255, Nov. 1996.

저자 소개

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

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

김진경(Jin-Gyoung Kim)

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

김석태(Seok-Tae Kim)

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