논문 03-28-9C-1 한국통신학회논문지 '03-9 Vol.28 No.9C

최적의 상관 특성과 큰 선형 복잡도를 갖는 새로운 p-진 수열군

학생회원 장 지 용*, 김 영 식* 정회원 노 종 선* and Tor Helleseth**

New Family of p-ary Sequences with Optimal Correlation Property and Large Linear Span

Ji-Woong Jang*, Young-Sik Kim*, Jong-Seon No* , Tor Helleseth** *Regular Members*

요 약

홀수 소수 p와 $n=(2m+1)\cdot k$를 만족시키는 정수 n, m, k에 대해, 이상적인 자기상관 특성을 갖는 Helleseth-Gong 수열을 이용하여 수열군의 크기가 p^n이고 주기가 p^n-1인 최적의 상관 특성을 갖는 p진 수열군을 생성한다. 즉, 수열군 내의 서로 다른 수열간의 최대 상관값 $R_{\max}$가 Welch의 하한 측면에서 최적의 상관값인 $p^{n/2}+1$을 넘지 않는다. 또한, 새로운 수열군의 선형 복잡도는 수열군 내의 m-수열을 제외하면 $(m+2)\cdot n$이 된다.

ABSTRACT

For an odd prime p and integer n, m and k such that $n=(2m+1)\cdot k$, a new family of p-ary sequences of period p^n-1 with optimal correlation property is constructed using the p-ary Helleseth-Gong sequences with ideal autocorrelation, where the size of the sequence family is p^n. That is, the maximum nontrivial correlation value $R_{\max}$ of all pairs of distinct sequences in the family does not exceed $p^{n/2}+1$, which means the optimal correlation property in terms of Welch's lower bound. It is also derived that the linear span of the sequences in the family is $(m+2)\cdot n$ except for the m-sequence in the family.

I. 서 론

코드분할 다중접속 방식(CDMA)의 통신 시스템에 있어 서명 수열은 각각의 사용자에게 할당되어 해당 사용자가 다른 사용자들과 구별 될 수 있게 하여준다. CDMA 시스템을 위한 수열의 작성시 가장 중요한 수열의 특성은 수열군의 크기가 커야 한다는 것과 수열군내의 다른 수열들과의 주기적 상관값이 작아야 한다는 것이다. 주어진 홀수 소수 p에 대해, 주기가 p^n-1인 p진 수열군이 최적의 상관 특성을 가진다는 것은 수열의 위상이 맞지 않을 때의 자기 상관값과 수열군 내의 다른 수열과의 상호 상관값이 $R_{\max}=p^{n/2}+1$을 넘지 않는다는 것이고, 이러한 특성을 갖는 수열들이 지금까지 연구되어 왔다. Sidelnikov는 최적의 상관 특성을 갖는 p진 수열군을 제시하였으며, Kumar와 Moreno[3] 역시 최적의 상관 특성을 갖는 소수위상(prime-phase) 수열을 제시하였다. Liu와

* 서울대학교 전기컴퓨터공학부 부호 및 암호 연구실(jsno@snu.ac.kr),
** Department of Informatics, University of Bergen (Tor.Helleseth@ii.uib.no)
논문번호: #030219-0526, 접수일자: 2003년 5월 26일
※본 연구는 ITRC연구과제, BK21 및 Norwegian Research Council 지원으로 수행되었습니다.

Komo[7]는 alphabet 크기를 확장하여 최적의 상관특성을 갖는 p진 Kasami수열을 제시하였다. p진 bent 수열 역시 최적의 상관 특성을 갖는다.

표 3. 최적의 상관 특성을 갖는 주기가 p^n-1인 p진 수열군

수열군	n	family size	선형 복잡도	balance
새로운 수열	$(2m+1)k$	p^n	n, $(m+2)n$	No
Sidelnikov	even or odd	p^n	n, $2n$	No
Kumar and Moreno	$(2m+1)k$	p^n	n, $2n$	No
Kasami	even, $2m$	p^m	$\frac{3}{2}n$	No
bent 수열	even, $2m$	p^m	*	Yes
Moriuchi 등	even, $2m$	p^m	*	Yes

* Moriuchi등이 제시한 수열과 bent 수열의 선형 복잡도는 다른 수열군에 비하여 매우 크다.

Moriuchi와 Imamura는 Kumar와 Moreno가 제시한 bent 함수를 이용하여 최적의 상관 특성과 균형(balance) 특성을 갖는 p진 수열을 제시하였다. 최적의 상관 특성을 갖는 p진 수열군들을 표 1에 정리하였다. 수열군의 크기는 Sidelnikov의 수열과 Kumar와 Moreno의 수열이 표 1의 다른 수열군에 비하여 크지만 선형 복잡도는 다른 수열군에 비하여 매우 작다.

본 논문에서는 홀수 소수 p와 $n=(2m+1)\cdot k$를 만족시키는 정수 n, m , k에 대하여, 이상적인 자기 상관 특성을 갖는 Helleseth-Gong 수열을 이용해서 주기가 p^n-1인 최적의 상관 특성을 갖는 p진 수열군을 제시하였다. 본 논문의 수열군은 군의 크기가 p^n이며, 상관 특성값의 크기가 $R_{\max}=p^{n/2}+1$을 넘지 않고 선형 복잡도는 같은 군 크기를 갖는 Sidelnikov의 수열군과 Kumar와 Moreno의 수열군 보다 큰 $(m+2)\cdot n$이다.

II. 사전지식

이제 주어진 홀수 소수 p에 대해 S가 다음과 같이 주어지는 주기가 $N=p^n-1$인 M개의 p진 수열들의 군이라 하자.

$$S=\{s_i(t)|0\le i\le M-1,\ 0\le t\le N-1\}.$$

이 때, 수열군 S의 두 수열 $s_i(t)$와 $s_j(t)$의 상관함수는 다음과 같이 주어진다.

$$R_{ij}(\tau)=\sum_{t=0}^{N-1} w^{s_i(\tau+t)-s_j(t)}$$

단, 위 식에서 w는 원시 p단위원이고, $0\le i,j\le M-1$, $0\le\tau\le N-1$이다. 또한, 상관값의 최대 값은 다음과 같이 정의된다.

$$R_{\max}=\max_{0\le i,j\le M-1,\ 0\le\tau\le N-1}|R_{i,j}(\tau)|$$

단, 위 식에서 $i=j$이면서 $\tau=0$인 경우는 제외된다. 이 때, 주기가 p^n-1인 p진 수열군의 $R_{\max}$가 $p^{n/2}+1$을 넘지 않을 경우, 이를 최적화된 수열군이라 한다.

이제 정수 z에 대해 V_z^n이 정수의 z에 대한 잉여 집합 J_z상의 n차 벡터공간이라 하자. 또한, $w_z=e^{j\frac{2\pi}{z}}$, $j=\sqrt{-1}$이고 $f(x)$가 V_z^n에서 J_z로의 함수라 하자. 그러면 함수 $f(x)$의 Fourier 변환은 다음과 같이 정의된다.

$$F(\lambda)=\frac{1}{\sqrt{z^n}}\sum_{x\in V_z^n} w_z^{f(x)-\lambda\cdot x^T},\quad \text{all } \lambda\in V_z^n$$

단, x^T는 x의 전치(transpose)이다. 이 때, 일반화된 bent함수는 아래와 같이 정의된다.

정의 1.[Olsen, Scholtz 및 Kumar[4]] : V_z^n에서 J_z로의 함수 $f(x)$가 임의의 $\lambda\in V_z^n$에 대해 Fourier 계수 $F(\lambda)$의 절대값이 항상 1인 경우 $f(x)$를 일반화된 bent함수라 한다.

본 논문에서는 z가 홀수 소수 p인 경우만을 다

룰 것이다. 따라서 V_p^n은, p개의 원소를 갖는 유한체 F_p상의 n차 벡터공간이고 $f(\underline{x})$는 V_p^n에서 F_p로의 함수이다.

Olsen, Scholtz 및 Welch는 F_{2^n}에서 F_2로의 trace 변환을 소개하였다. 이 때, F_{p^n}에서 F_p로의 trace 변환은 다음과 같이 일반화 될 수 있다.

정의 2.[Olsen, Scholtz, 및 Welch[10]] : $f(x)$가 F_{p^n}에서 F_p로의 함수라 하면 $f(x)$의 trace 변환과 그 역변환은 다음과 같이 정의된다.

$$F(\lambda) = \frac{1}{\sqrt{p^n}} \sum_{x \in F_{p^n}} w^{f(x) - \mathrm{tr}_1^n(\lambda x)}, \quad \text{all } \lambda \in F_{p^n}$$

$$w^{f(x)} = \frac{1}{\sqrt{p^n}} \sum_{\lambda \in F_{p^n}} F(\lambda) \cdot w^{\mathrm{tr}_1^n(\lambda x)}, \quad \text{all } x \in F_{p^n}.$$

□

이 때, F_{p^n}의 원소 x와 λ는 V_p^n의 원소 $\underline{x}$와 $\underline{\lambda}$에 대해 다음과 같은 관계를 갖는다.

$$x = \sum_{i=1}^{n} x_i \alpha_i \Rightarrow \underline{x} = (x_1, x_2, \cdots, x_n)$$

$$\lambda = \sum_{i=1}^{n} \lambda_i \alpha_i \Rightarrow \underline{\lambda} = (\lambda_1, \lambda_2, \cdots, \lambda_n)$$

단, 위 식에서 x_i와 λ_i는 F_p의 원소이고 $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$는 F_p상의 F_{p^n}의 basis이다. 이제 F_{p^n}의 원소 x를 V_p^n의 원소 $\underline{x}$로 치환하면 F_{p^n}에서 F_p로의 함수 $f(x)$는 V_p^n에서 F_p로의 함수 $f(\underline{x})$가 된다. 또한, $f(x)$의 trace 변환 값과 그에 대응하는 함수 $f(\underline{x})$의 Fourier 변환 값이 같기 때문에 F_{p^n}에서 F_p로의 함수 $f(x)$가 bent함수라는 것과 그에 대응되는 V_p^n에서 F_p로의 함수 $f(\underline{x})$가 bent함수라는 것은 동치이다.

이제, e, k가 $n = e \cdot k$를 만족시키는 정수라 하면 F_{p^k}상의 F_{p^n}의 basis $\{\alpha_1, \alpha_2, \cdots, \alpha_e\}$가 다음을 만족할 때 trace-orthogonal basis라 한다.

$$\mathrm{tr}_k^n(\alpha_i \alpha_j) = \begin{cases} a_i, & \text{if } i = j \\ 0, & \text{otherwise} \end{cases}$$

단, $a_i \in F_{p^k}^*$이다. 또한 임의의 양수 e와 홀수 소수 p에 대해 F_{p^k}상의 F_{p^n}의 trace-orthogonal basis가 항상 존재한다[13]. 그러므로 F_{p^n}의 원소인 x와 λ는 다음과 같은 관계에 의해 $V_{p^k}^e$의 원소인 $\underline{x}$와 $\underline{\lambda}$로 대응시킬 수 있다.

$$x = \sum_{i=1}^{e} x_i \alpha_i \Rightarrow \underline{x} = (x_1, x_2, \cdots, x_e) \quad (1)$$

$$\lambda = \sum_{i=1}^{e} \lambda_i \alpha_i \Rightarrow \underline{\lambda} = (\lambda_1, \lambda_2, \cdots, \lambda_e) \quad (2)$$

단, x_i와 λ_i는 F_{p^k}의 원소이다.

이 때 basis를 trace-orthogonal basis로 선택하면 다음의 관계를 얻는다.

$$\mathrm{tr}_k^n(\lambda x) = \sum_{i=1}^{e} a_i \lambda_i x_i. \quad (3)$$

이제 $1 \le i \le e$에 대해 $\lambda_i' = a_i \lambda_i$라 하고 $\underline{\lambda}' = (\lambda_1', \lambda_2', \cdots, \lambda_e')$이라하면 (3)식은 다음과 같이 다시 쓸 수 있다.

$$\mathrm{tr}_k^n(\lambda x) = \sum_{i=1}^{e} \lambda_i' x_i = \underline{\lambda}' \, \underline{x}^T.$$

이제 (1)과 (2)를 이용하여 F_{p^n}에서 F_p로의 함수 $f(x)$가 $V_{p^k}^e$에서 F_p로의 함수 $\mathrm{tr}_k^n(f(\underline{x}))$와 대응된다 가정하면 정의 2의 trace 변환은 다음과 같이 중간체에서의 trace 변환으로 수정할 수 있다.

정의 3 : $n = e \cdot k$라 하고 $f(\underline{x})$가 $V_{p^k}^e$에서 F_{p^k}로의 함수라 하자. 이 때, $\mathrm{tr}_1^k(f(\underline{x}))$의 trace 변환과 그 역변환은 다음과 같이 정의된다.

$$F_M(\lambda) = \frac{1}{\sqrt{p^n}} \sum_{x \in V_{p^k}^e} w^{\mathrm{tr}_1^k(f(x)) - \mathrm{tr}_1^k(\lambda \cdot x^T)},$$
all $\lambda \in V_{p^k}^e$

$$w^{f(x)} = \frac{1}{\sqrt{p^n}} \sum_{\lambda \in V_{p^k}^e} F_M(\lambda) \cdot w^{\mathrm{tr}_1^k(\lambda \cdot x^T)},$$
all $x \in V_{p^k}^e$.

□

이 때, $V_{p^k}^e$에서 F_p로의 함수 $\mathrm{tr}_1^k(f(x))$의 trace 변환이 그에 대응되는 F_{p^n}에서 F_p로의 함수 $\mathrm{tr}_1^k(f(x))$의 trace변환인 $F(\lambda)$와 아래와 같은 관계가 있다는 것은 자명하다.

$$F(\lambda) = F_M(\lambda').$$

즉, 함수 $\mathrm{tr}_1^k(f(x))$의 trace 변환값의 집합과 그에 대응되는 함수 $\mathrm{tr}_1^k(f(x))$의 trace 변환값의 집합은 같다. 따라서 함수 $\mathrm{tr}_1^k(f(x))$ 또는 $\mathrm{tr}_1^k(f(x))$의 trace변환 값의 절대값을 1만 갖게 된다면, 함수 $\mathrm{tr}_1^k(f(x))$와 $\mathrm{tr}_1^k(f(x))$는 일반화된 bent 함수가 된다.

이제 $Q(x)$가 F_{p^n}에서 F_{p^k}로의 quadratic 함수라 하자. 이 때, (1)을 이용하면 quadratic 함수 $Q(x)$를 다음과 같이 나타낼 수 있다.

$$Q(x) = \sum_{i=1}^{e} \sum_{j=1}^{e} b_{ij} x_i x_j. \quad (4)$$

단, $b_{ij} \in F_{p^k}$이다. Dickson[1]은 e가 홀수인 경우 임의의 quadratic form이 선형변환에 의해 다음과 같은 canonical form으로 바뀔 수 있음을 보였다.

$$Q(x) = \sum_{i=1}^{\rho} r x_i^2. \quad (5)$$

단, $\rho \le e$이고, $r=1$이거나 F_{p^k}상의 nonresidue 이다. 이 때, quadratic 함수 $Q(x)$의 rank는 ρ이다. 또한, $Q(x)$의 rank와 그에 대응되는 함수 $Q(x)$의 rank가 같다는 것은 자명하다. 이제 정의 3으로부터 다음의 lemma들을 쉽게 유도 해낼 수 있다.

보조정리 4 : $\mathrm{tr}_1^k(Q(x))$가 p진 quadratic bent 함수라는 것과 $V_{p^k}^e$에서 F_{p^k}로의 quadratic 함수 $Q(x)$가 full rank e를 갖는다는 것은 동치이다.

□

Helleseth와 Gong은 Helleseth-Gong(HG) 수열이라 불리는 이상적인 자기상관 특성을 갖는 새로운 p진 수열을 제시하였고 이는 다음 정리와 같다.

정리 5.[Helleseth and Gong[2]] : n, m, k가 $n=(2m+1)\cdot k$를 만족하는 양의 정수라 하고, s는 $\gcd(2m+1,2)=1$을 만족하는 $1 \le s \le 2m$인 정수라 하자. 또한, p는 홀수 소수, α는 F_{p^n}의 원시원, $q=p^k$이고 $l=0,1,\cdots,m$에 대해 $b_0=1$, $u_0=b_0/2$, $u_l=b_{2l}=b_{2m+1-2l}$ 의 관계가 성립한다 하자. 이 때 다음과 같이 주어지는 주기가 p^n-1인 Helleseth-Gong 수열은 이상적인 자기상관 특성을 갖는다.

$$s(t) = \mathrm{tr}_1^n\left(\sum_{l=0}^{m} u_l \cdot \alpha^{\frac{q^{2l}+1}{2} t}\right). \quad (6)$$

□

이제 $F_{p^n}^* = F_{p^n} \setminus \{0\}$이고 $x=\alpha^t$라 하면 (6)의 Helleseth-Gong 수열은 다음과 같이 다시 쓸 수 있다.

$$\mathrm{tr}_1^n\left(\sum_{l=0}^{m} u_l \cdot x^{\frac{q^{2l}+1}{2}}\right), \quad x \in F_{p^n}^*.$$

이 때, $h(x)$를 Helleseth-Gong 방정식이라 하고 다음과 같이 정의한다.

$$h(x) = \sum_{l=0}^{m} u_l \cdot x^{\frac{q^{2l}+1}{2}}, \quad x \in F_{p^n}^*.$$

그러면 (6)의 Helleseth-Gong 수열은 다음과 같이 다시 쓸 수 있다.

$$s(t) = \mathrm{tr}_1^n(h(\alpha^t)), \quad 0 \le t \le p^n - 2.$$

Helleseth-Gong 수열은 다음과 같이 변형될 수 있다.

$$s_b(t) = \mathrm{tr}_1^n(\alpha^t) + \mathrm{tr}_1^n(h(b\cdot\alpha^{2t})) = \mathrm{tr}_1^n(\alpha^t + \sum_{l=0}^{m} u_l \cdot b^{\frac{\alpha^{2l}+1}{2}} \cdot \alpha^{(\alpha^{2l}+1)t}). \quad (7)$$

단, $b\in F_{p^n}$이다. 이 때, (7)식이 주기가 p^n-1인 수열임은 자명하다.

Ⅲ. p진 수열군의 새로운 생성법

(7)에서 정의한 새로운 p진 수열을 이용하면, 다음과 같은 수열군의 크기가 p^n이고 최적의 상관 특성을 갖는 새로운 p진 수열군을 만들 수 있다.

정리 6 : $s_b(t)$가 (7)에서 정의된 p진 수열이라 하면 다음과 같이 주어지는 p진 수열군은 $R_{\max}=p^{2/n}+1$인 최적의 상관 특성을 갖는다.

$$S=\{s_b(t)\mid b\in F_{p^n},\ 0\le t\le p^n-2\}.$$

증명: 수열군 S내의 두 수열 $s_{b_i}(t)$와 $s_{b_j}(t)$간의 상호상관 함수는 다음과 같이 다시 쓸 수 있다.

$$R_{ij}(\tau)+1 = \sum_{t=0}^{p^n-2} w^{s_{b_i}(t_\tau)-s_{b_j}(t)}+1 = \sum_{x\in F_{p^n}} w^{\mathrm{tr}_1^n(c\cdot x+h(b_i\cdot c^2\cdot x^2))} \cdot w^{-x-h(b_j\cdot x^2))} \quad (8)$$

단, $c=\alpha^\tau\in F_{p^n}^*$이다. 이 때, 증명은 다음과 같이 3가지 경우로 나누어 생각할 수 있다.

경우 (i) $c=1,\ b_i=b_j$:

이 경우 $R_{ij}(\tau)=p^n-1$이라는 것은 자명하다.

경우 (ii) $c\neq 1,\ b_ic^2=b_j$:

이 경우 역시 $R_{ij}(\tau)=-1$이라는 것이 자명하다.

경우 (iii) $b_ic^2\neq b_j$:

본 논문에서는 $b_i=b_j=0$는 생각하지 않는다. 또한, $b_i\neq 0$인 경우의 증명이 $b_j\neq 0$인 경우와 유사하므로 $b_j\neq 0$인 경우만 증명할 것이다.

$\frac{k}{n}$이 홀수 정수이므로 F_{p^k}에서도 nonresidue는 F_{p^n}에서도 nonresidue가 된다. 따라서 b_i와 b_j를 $b_i=\gamma_i a_i^2$과 $b_j=\gamma_j a_j^2$으로 쓸 수 있다. 단, $a_i, a_j\in F_{p^n}$이고 γ_i와 γ_j는 1 또는 F_{p^k}상의 nonresidue이다. 이제 $b_j\neq 0$, 즉 $a_j\neq 0$라 가정하고 $u=\frac{a_i}{a_j}c,\ y=a_jx$라 하면 (8)의 상호상관 함수는 다음과 같이 다시 쓸 수 있다.

$$\begin{aligned} R_{ij}(\tau)+1 &= \sum_{x\in F_{p^n}} w^{\mathrm{tr}_1^n(h(\gamma_i\cdot a_i^2c_i^2\cdot x^2)-h(\gamma_j\cdot a_j^2\cdot x^2))} \cdot w^{\mathrm{tr}_1^n((c-1)\cdot x)} \\ &= \sum_{y\in F_{p^n}} w^{\mathrm{tr}_1^n(h(\gamma_i\cdot u^2\cdot y^2)-h(\gamma_j\cdot y^2))} \cdot w^{\mathrm{tr}_1^n\left(\frac{c-1}{a_j}\cdot y\right)}. \end{aligned}$$

위 식에 모든 $r\in F_{p^k}$에 대해 $h(rx)=rh(x)$임을 이용하면 다음을 얻을 수 있다.

$$\begin{aligned} R_{ij}(\tau)+1 &= \sum_{y\in F_{p^n}} w^{\mathrm{tr}_1^n(h(\gamma_i\cdot u^2\cdot y^2)-h(\gamma_j\cdot y^2))} \cdot w^{\mathrm{tr}_1^n\left(\frac{c-1}{a_j}\cdot y\right)} \\ &= \sum_{y\in F_{p^n}} w^{\mathrm{tr}_1^k(\mathrm{tr}_k^n(\gamma_i\cdot h(u^2\cdot y^2)-\gamma_j\cdot h(y^2)))} \cdot w^{\mathrm{tr}_1^n\left(\frac{c-1}{a_j}\cdot y\right)}. \end{aligned} \quad (9)$$

이제 $Q(y)$가 아래와 같이 정의되는 quadratic 함수라 하자.

$$
\begin{aligned}
&Q(y)\\
&= \mathrm{tr}_k^n(\gamma_i \cdot h(u^2 \cdot y^2) - \gamma_j \cdot h(y^2))\\
&= \mathrm{tr}_k^n\left(\sum_{l=0}^{m} u_l \cdot [\gamma_i \cdot u^{q^{2l}+1} - \gamma_j] \cdot y^{q^{2l}+1}\right)\\
&= \gamma_j \cdot \mathrm{tr}_k^n\left(\sum_{l=0}^{m} u_l \cdot \left[\frac{\gamma_i}{\gamma_j} \cdot u^{q^{2l}+1} - 1\right] \cdot y^{q^{2l}+1}\right).
\end{aligned}
$$

그러면 (9)식은 정의 2에서 정의된 quadratic 함수 $\mathrm{tr}_1^k(Q(y))$의 F_{p^n}에서 F_p로의 trace변환이 된다. 이 때, quadratic 함수 $\mathrm{tr}_1^k(Q(y))$가 p진 bent함수이면 $|R_{ij}(\tau)+1| = p^{n/2}$가 된다. 정의 3과 사전정리 4로부터 $Q(y)$가 full rank를 갖는다면 $\mathrm{tr}_1^k(Q(y))$가 bent함수가 됨을 알 수 있다. 그러므로 $Q(y)$의 rank가 full rank인 $2m+1$이 됨을 증명하는 것으로 충분하다.

모든 $y \in F_{p^n}$에 대해 $Q(y+z) = Q(y)$를 만족시키는 해 $z \in F_{p^n}$의 개수가 $p^{2m+1-\rho}$일 때, quadratic 함수 $Q(y)$의 rank가 ρ가 된다는 것은 이미 알려진 사실이다. 이제 $a_l = u_l \cdot \left[\frac{\gamma_i}{\gamma_j} \cdot u^{q^{2l}+1} - 1\right]$이라 하면 다음을 얻을 수 있다.

$$
\mathrm{tr}_k^n\left(\sum_{l=0}^{m} a_l \cdot (y+z)^{q^{2l}+1}\right) = \mathrm{tr}_k^n\left(\sum_{l=0}^{m} a_l \cdot y^{q^{2l}+1}\right).
$$

또한, 위 식은 다음과 같이 변형할 수 있다.

$$
tr_k^n\left(\sum_{l=0}^{m} a_l \cdot (y^{q^{2l}} z + y z^{q^{2l}}) + \sum_{l=0}^{m} a_l \cdot z^{q^{2l}+1}\right) = 0.
$$

위 식의 첫 번째 항에 $q^{2m+1-2l}$승을 해주면 다음을 얻게 된다.

$$
\begin{aligned}
&\mathrm{tr}_k^n\Big(y \cdot \Big[\sum_{l=0}^{m} a_l^{q^{2m+1-2l}} \cdot z^{q^{2m+1-2l}} + \sum_{l=0}^{m} a_l \cdot z^{q^{2l}}\Big]\\
&\quad + \sum_{l=0}^{m} a_l \cdot z^{q^{2l}+1}\Big) = 0
\end{aligned}
$$

위 식은 다음과 동치이다.

$$
\begin{aligned}
&\sum_{l=0}^{m} a_l^{q^{2m+1-2l}} \cdot z^{q^{2m+1-2l}} + \sum_{l=0}^{m} a_l \cdot z^{q^{2l}} = 0 \quad (10)\\
&\mathrm{tr}_k^n\left(a_l \cdot z^{q^{2l}+1}\right) = 0.
\end{aligned}
$$

이 때, (10)식은 다음과 같이 다시 쓸 수 있다.

$$
\begin{aligned}
\sum_{l=0}^{m} u_l \cdot \Big\{&\left(\frac{\gamma_i}{\gamma_j} \cdot u^{(q^{2l}+1)\cdot q^{2m+1-2l}-1} - 1\right) \cdot z^{q^{2m+1-2l}}\\
&+ \left(\frac{\gamma_i}{\gamma_j} \cdot u^{(q^{2l}+1)} - 1\right) \cdot z^{q^{2l}}\Big\} = 0.
\end{aligned}
$$

따라서 다음을 얻을 수 있다.

$$
\sum_{l=0}^{2m} b_l \cdot \left(\frac{\gamma_i}{\gamma_j} \cdot u^{q^{2l}+1} - 1\right) \cdot z^{q^{2l}} = 0
$$

단, $u_0 = \frac{b_0}{2}$이고 $u_l = b_{2l} = b_{2m+1-2l}$이다. 따라서 $Q(y)$의 rank ρ가 $2m+1$임을 보이기 위해 다음의 방정식이 $\frac{\gamma_i}{\gamma_j} \cdot \left(\frac{a_i}{a_j} \cdot c\right)^2 \neq 1$인 경우 $z=0$을 유일한 해로 가짐을 보여야 하는데 이는 [2]에서 이미 증명이 되었다.

$$
\sum_{l=0}^{2m} b_l \cdot \left(\frac{\gamma_i}{\gamma_j} \cdot \left(\frac{a_i}{a_j} \cdot c\right)^{q^{2l}+1} - 1\right) \cdot z^{q^{2l}} = 0.
$$

또한 기본 조건들로부터 $\frac{\gamma_i}{\gamma_j} \cdot \left(\frac{a_i}{a_j} \cdot c\right)^2 \neq 1$임은 자명하다. 따라서 정리6이 증명이 되었다.

□

Kumar와 Moreno[3]는 full rank를 갖는 quadritic form의 Fourier 계수를 이용하여 그에 대응되는 수열군 내의 두 개의 수열간의 상관 값을 구함으로써 수열군 내의 수열들 간의 상관값의 분포를 구하였다. 본 논문의 정리 6에서 정의한 수열군의 상관값 분포와 그 증명 방식이 Kumar와 Moreno의 수열군의 그것과 같다는 것은 매우 흥미로운 사실이다.

Sidelnikov의 p진 수열과 Kumar와 Moreno의 p진 수열은 수열군 내의 m-s수열을 제외한 나머지 수열들의 선형복잡도가 $2n$이었다. 그러나 본 논문

의 정리 6에서 제안한 p진 수열 $s_b(t)$의 선형복잡도는 다음 정리와 같이 구해진다.

정리 7 : $b \in F_{p^n}^*$에 대해 정리 6에서 정의된 수열 $s_b(t)$의 선형복잡도는 $(m+2) \cdot n$이다.

증명 :

$0 \le i \le m$과 (7)의 $d_i = q^{2i}+1$에 대해 $\gcd(d_i, p^n-1)=2$임은 자명하다. 그러므로 α^{d_i}이 F_{p^n}의 어떠한 하위체에도 속하지 않음 역시 자명하다. 따라서 F_{p^n}상에서 α^2이 속한 coset의 크기는 n이 되고 이는 α^{d_i}에 대해서도 같다. 그러므로 $s_b(x)$의 선형복잡도는 $(m+2) \cdot n$이다.

□

V. 결 론

본 논문에서는 홀수 소수인 p와 m, k가 양의 정수 일 때, $n=(2m+1) \cdot k$인 n에 대해서 최적의 상관 특성을 갖는 새로운 p진 수열군을 제안하였다. 새로운 수열군은 최적의 상관 특성과 같은 크기를 갖는 기존의 p진 수열군들에 비해 선형 복잡도가 최소 50%이상 증가하였다.

참 고 문 헌

[1] L.E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory,* Dover, New York 1958.

[2] T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autocorrelation function," *IEEE Trans. Inform. Theory,* vol. , pp. 71-79, May 2002.

[3] P.V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," *IEEE Trans. Inform. Theory,* vol. 37, pp. 603-616, May 1991.

[4] P.V. Kumar, R.A. Scholtz and L.R. Welch, "Generalized bent functions and their properties," *Journal of Combinatorial Theory,* Series A. vol. 40, pp. 90-117, 1985.

[5] A. Lempel and M. Cohn, "Maximal families of bent sequences," *IEEE Trans. Inform. Theory,* vol. 38, pp. 865-868, Nov. 1982.

[6] R. Lidl and H. Niederreiter, *Finite Fields,* vol 20 of Encyclopedia of Mathematics and Its Applications, Addison-Wesley, Reading, MA, 1983.

[7] S. -C. Liu and J. F. Komo, "Nonbinary Kasami sequences over *GF(p),*" *IEEE Trans. Inform. Theory,* vol. 38, pp. 1409-1412, Jul. 1992.

[8] F. J. McWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes,* New York: North-Holland, 1977.

[9] T. Moriuchi and K. Imamura, "Balanced nonbinary sequences with good periodic correlation properties obtained from modified Kumar-Moreno sequences," *IEEE Trans. Inform. Theory,* vol. 41, pp. 572-576, Mar. 1995.

[10] J.D. Olsen, R.A. Scholtz and L.R. Welch, "Bent-function sequences," *IEEE Trans. Inform. Theory,* vol. 28, pp. 858-864, Nov. 1982.

[11] O,S. Rothaus, "On bent functions," *Journal of Combinatorial Theory,* Serues A. vol. 20, pp. 300-305, 1976.

[12] G. Seroussi and A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields," *SIAM J. Comput.,* vol. 9, no. 4, pp. 758-767, Nov. 1980.

[13] M.K. Simon, J.K. Omura, R.A. Scholtz and B.K. Levitt, *Spread Spectrum Communications,* vol. 1, Computer Science Press, Rockville, MD, 1985.

[14] L.R. Welch, "Lower bounds on the maximal cross correlation of signals," *IEEE Trans. Inform. Theory,* vol. 20, pp. 396-399, May 1976.

장 지 웅(Ji-Woong Jang) 학생회원

2000년 2월 : 서울대학교 전기공학부 공학사
2002년 2월 : 서울대학교 전기컴퓨터공학부 공학석사
2002년 3월~현재 : 서울대학교 전기컴퓨터공학부 박사과정

<주관심분야> 시퀀스, 오류정정부호, 디지털 통신

김 영 식(Young-Sik Kim) 학생회원

2001년 2월 : 서울대학교 전기공학부 공학사
2003년 2월 : 서울대학교 전기컴퓨터공학부 공학석사
2003년 3월~현재 : 서울대학교 전기컴퓨터공학부 박사과정

<주관심분야> 시퀀스, 오류정정부호, 디지털통신

노 종 선(Jong-Seon No) 정회원

1981년 2월 : 서울대학교 전자공학과 공학사
1984년 2월 : 서울대학교 대학원 전자공학과 석사
1988년 5월 : University of Southern California, 전기공학과 공학박사
1988년 2월 ~ 1990년 7월 : Hughes Network Systems, Senior MTS
1990년 9월 ~ 1999년 7월 : 건국대학교 전자공학과 부교수
1999년 8월 ~ 현재 : 서울대학교 전기컴퓨터공학부 부교수

<주관심분야> 시퀀스, 오류정정부호, 시공간부호, 암호학, 이동통신

Tor Helleseth
1971년 : University of Bergen, Cand. Real degrees in mathematics
1979년 : University of Bergen, Dr. Philos. in mathematics
1973년 ~ 1980년 : Department of Mathmatics in University of Bergen, Research Assistant
1981년 ~ 1984년 : Defense in Norway, Chief Headquarters
1984 ~ 현재 : Department of Informatics in University Bergen, Professor

<주관심분야> 시퀀스, 오류정정부호, 암호학,