# 낮은 상관도 특성을 갖는 주기 $\frac{p^n-1}{2}$인 새로운 $p$진 수열군

이위직, 김지엽, 노종선
서울대학교
leewj422@ccl.snu.ac.kr, lakroforce@ccl.snu.ac.kr, jsno@snu.ac.kr

# New Families of $p$-ary Sequence of Period $\frac{p^n-1}{2}$ with Low Maximum Correlation Magnitude

Lee Wijik, Kim Ji-Youp, No Jong-Seon
Seoul Natioal Univ.

요 약

본 논문에서는 소수 $p \equiv 3 \bmod 4$ 이고, $n$이 홀수일 때, 주기가 $N=\frac{p^n-1}{2}$인 m-수열의 두 개의 decimate 된 수열 $m(2t)$와 $m(dt)$간의 상호 상관도를 분석한다. 본 논문에서는 두 가지 수열 군을 분석하는데, 첫 번째 수열군은 $d=4$로, 다른 한 수열군은 $d=\frac{p^n+1}{2}=N+1$로 주어져 있다. 이 때 두 수열군의 상호 상관도 크기의 상한 값은 둘 다 $\frac{3}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}$로 나타났고 수열군의 크기는 주기의 4배인 $4N$으로 나타났다.

## Ⅰ. 서 론

낮은 상호 상관 특성을 갖는 수열 군을 찾는 많은 연구가 진행되어 왔다. 그러한 한 방법으로 $p$진 수열 군에 대해서 m-수열 $m(t)$와 m-수열을 decimate 한 수열 $m(dt)$간의 상호 상관도를 구하는 연구가 이루어져왔다[1]-[5].

최근에는 $p$진 수열 군에 주기가 반주기로 $N=\frac{p^n-1}{2}$인 연구가 진행되어왔다. Kim, Choi, No, Jung [6]은 Kloosterman 합을 이용한 반주기 $p$진 수열 군을 생성하였다. 여기서 $p \equiv 3 \bmod 4$이고, 이 수열 군의 크기는 $4N$이고, 상호 상관도의 크기의 상한 값은 $2\sqrt{N+\frac{1}{2}}$ 로 나타났다. 이 결과는 Kim, Chae, Song [7] 에 의해 더 일반화 되었다. 모든 홀수인 소수 $p$에 대해서도 수열 군이 생성되었고 수열 군의 크기는 마찬가지로 $4N$, 상호상관도의 크기의 상한은 $\frac{1}{2}\left(p^e\sqrt{p^n+\frac{1}{p^{2e}}}\right)$로 증명되었다.

상호 상관도 크기의 상한 값을 구하는데 Weil 경계를 사용한 연구도 많이 진행되었다[8]. Weil 경계에는 세 가지 유형이 있다. 곱셈 character들의 합, 덧셈 character들의 합, 그리고 곱셈과 덧셈 character를 곱한 혼합 유형 이렇게 세 가지이다. Han, Yang [9]은 Weil 경계의 곱셈 character을 이용해서 상호 상관도 크기의 상한 값을 구하였다. Wang, Gong [10]은 다상의 수열 군을 생성하였고, 이 수열의 상호상관도의 크기의 상한을 구할 때 Weil 경계의 세 가지 유형을 모두 적용하였다.

본 논문에서는 낮은 상호상관도 값을 가지는 $p$진 수열 군을 생성하였다. $p \equiv 3 \bmod 4$ 이고, $n$이 홀수일 때, 주기가 $N=\frac{p^n-1}{2}$인 두 종류의 수열 군을 생성하였다. 두 수열 군 모두 $p$진 m-수열 $m(2t), m(dt)$를 shift해서 더해서 생성하였으며 첫 번째 경우 $d=4$이고 두 번째 경우는 $d=N+1$이다. 두 수열군의 상호 상관도 크기의 상한 값은 둘 다 $\frac{3}{\sqrt{2}}\sqrt{N+\frac{1}{2}}+\frac{1}{2}$로 나타났고 수열군의 크기는 $4N$이다.

## Ⅱ. 사전 지식

### A. 표기법과 정의

1) 소수 $p$는 $p \equiv 3 \bmod 4$ 이고, $n$은 홀수이고 $q=p^n$이다.
2) $F_q$는 $q$개의 원소를 갖는 유한체이고 $\alpha$는 $F_q$의 원시 근이다.
3) $F_q \rightarrow F_p$ 인 trace 함수는 다음과 같이 정의 된다.

$$tr_1^n(x)=\sum_{i=0}^{n-1}x^{p^i}$$

4) $\omega=e^{\frac{2\pi i}{p}}$ 이고 $i=\sqrt{-1}$ 이다.
5) trace 함수를 이용한 $p$진 m-수열은 다음과 같이 쓸 수 있다.

$$m(t)=tr_1^n(\alpha^t)$$

6) $p$진 m-수열 $m(t)$와 이를 양의 정수 $d$로 decimate 한 수열 $s(dt+l)$간의 상호 상관도는 다음과 같이 나타난다.

$$C_l(\tau)=\sum_{t=0}^{p^n-2}\omega^{s(t+\tau)-s(dt+l)}$$

그리고 $C_l(\tau)$의 최댓값은 $C_{\max}$이다.

### B. character와 Weil 경계

Character에는 덧셈 character와 곱셈 character 두 가지가 있다[11].

정의 1 (덧셈 character) : 임의의 $\beta \in F_q$에 대해, 덧셈 character는 다음

과 같이 정의된다.

$$\psi_\beta(x) = e^{\frac{2\pi i Tr_1^n(\beta x)}{p}},\ x \in F_q$$

정의 2 (곱셈 character) : $g$를 $F_q$의 원시 근이라고 할 때, 곱셈 character는 다음과 같다.

$$\chi_j(g^k) = e^{\frac{2\pi ijk}{q-1}},\ \chi_j(0) = 0$$

곱셈 character 중 하나인 2차 character $\eta$는 다음과 같다.

$$\eta(y) = \begin{cases} 1, y\text{는 } F_q\text{에서 제곱수인 경우} \\ -1, y\text{는} F_q\text{에서 제곱수가 아닌 경우} \\ 0, y = 0\text{인 경우} \end{cases}$$

보조정리 3 (가우스 합 [14]) : $\psi$를 $F_q$의 덧셈 character, $\chi$를 $F_q$의 곱셈 character라고 할 때, 가우스 합 $G(\psi,\chi)$는 다음과 같이 정의 된다.

$$G(\psi,\chi) = \begin{cases} p^n - 1, \psi = \psi_0, \chi = \chi_0\text{ 인 경우} \\ 0, \psi = \psi_0, \chi \neq \chi_0\text{ 인 경우} \\ -1, \psi \neq \psi_0, \chi = \chi_0\text{ 인 경우} \end{cases}$$

$\psi \neq \psi_0, \chi \neq \chi_0$일 때는 $|G(\psi,\chi)| = q^{\frac{1}{2}}$가 성립한다.

정리 4 (Weil 경계 [8]) : $\psi$를 $F_q$의 덧셈 character, $\chi$를 $F_q$의 곱셈 character라고 하고, $f(x) \in F_q[x]$의 차수를 $e$, $g(x) \in F_q[x]$의 $\overline{F_q}$내에서의 근의 개수를 $s$라고 하자. $g(x) \neq c \cdot h^M(x), h(x) \in F_q[x]$이 성립한다면, 다음 부등식이 성립한다.

$$\left| \sum_{x \in F_q} \chi(g(x))\psi(f(x)) \right| \leq (e+s-1)\sqrt{q}$$

## Ⅲ. 새로운 수열 군과 상호 상관도 크기의 상한

본 논문에서는 두 종류의 수열 군을 생성한다. 다음과 같이 집합 $S$를 정의하자.

$S = \{m(2t+i) + m(d(t+l)+j) | 0 \leq i,j \leq 1; 0 \leq l \leq N-1\}$

정리 5 : $d = 4, N+1$일 때, 두 경우 모두 집합 $S$내의 수열 간의 상호 상관도 $C(\tau)$ 크기의 최댓값인 $C_{\max}$는 다음 부등식이 성립한다.

$$C_{\max} \leq \frac{3}{\sqrt{2}}\sqrt{N+\frac{1}{2}} + \frac{1}{2}$$

정리 6 : $S$ 수열군의 크기는 $4N$ 이다.

표 1은 각 $p,n$에 대해서 시뮬레이션 한 결과이다. $C_{\max}$는 $\sqrt{N}$으로 normalize 했을 때 값이 2 정도로 작은 것을 확인 할 수 있다.

| $p$ | $n$ | $N$ | $C_{\max}/\sqrt{N}$ | 값의 수 |
|---|---|---|---|---|
| 3 | 3 | 13 | 2.1650 | 5 |
| | 5 | 121 | 2.1259 | 6 |
| | 7 | 1093 | 2.1219 | 6 |
| | 9 | 9841 | 2.1214 | 6 |
| 7 | 3 | 171 | 2.0304 | 94 |
| | 5 | 8403 | 2.0951 | 852 |
| 11 | 3 | 665 | 2.0003 | 450 |

표 1 $C_{\max}$와 상호상관도 값의 수를 시뮬레이션 한 결과

## Ⅳ. 결론

본 논문에서는 두 가지 수열 군 $S$를 생성하였고, 두 수열군의 상호 상관도 크기의 상한 값은 둘 다 $\frac{3}{\sqrt{2}}\sqrt{N+\frac{1}{2}} + \frac{1}{2}$이고 수열군의 크기는 주기의 4배인 $4N$임을 확인하였다.

## ACKNOWLEDGMENT

이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2012-0000186). 본 연구는 방송통신위원회의 차세대통신네트워크원천기술개발사업의 연구결과로 수행되었음. (KCA-2012-08-911-04-003)

## 참 고 문 헌

[1] S. C. Liu and J. F. Komo, "Nonbinary Kasami sequences over GF(p)," IEEE Trans. Inf. Theory, vol. 38, no. 4, pp. 1409 - 1412, 1992.

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

[3] E. N. Muller, "On the cross-correlation of sequences over GF($p$) with short periods," IEEE Trans. Inf. Theory, vol. 45, no. 1, pp. 289 - 295, Jan 1999.

[4] E. Y. Seo, Y. S. Kim, J. S. No, and D. J. Shin, "Cross-correlation distribution of $p$-ary m-sequence of period $p^{4k}-1$ and its decimated sequences by $\left(\frac{p^{2k}+1}{2}\right)^2$," IEEE Trans. Inf. Theory, vol. 54, no. 7, pp. 3140 - 3149, Jul. 2008.

[5] S. T. Choi, T. H. Lim, J. S. No, and H. B. Chung, "On the cross-correlation of a p-ary m-sequence of period $p^{2m}-1$ and its decimated sequences by $\frac{(p^m+1)^2}{2(p+1)}$," IEEE Trans. Inf. Theory, vol. 58, no. 3, pp. 1873 - 1879, Mar. 2012.

[6]J. Y. Kim, S. T. Choi, and J. S. No, "A new family of $p$-ary sequences of period $\frac{p^n-1}{2}$ with low correlation," IEEE Trans. Inf. Theory, vol. 57, no. 6, pp. 3825 - 3829, Jun. 2011.

[7]D. S. Kim, H. J. Chae, and H. Y. Song, "A generalization of the family of $p$-ary decimated sequences with low correlation," IEEE Trans. Inf. Theory, vol. 57, no. 11, pp. 7614 - 7617, Nov. 2011.

[8]A. Weil, "On some exponential sums," in Proc. Natl. Acad. Sci. USA, vol. 34, no. 5, pp. 204 - 207, 1948.

[9]Y. K. Han and K. Yang, "New M-ary sequence families with low correlation and large size," IEEE Trans. Inf. Theory, vol. 55, no. 4, Apr. 2009.

[10]Z. Wang, G. Gong, and N. Y. Yu, "New polyphase sequence families with low correlation derived from the Weil bound of exponential sums," IEEE Trans. Inf. Theory, vol. 59, no. 6, pp. 3990 - 3998. Jun. 2013.

[11]R. Lidl and H. Niederreliter, *Finite Fields, vol. 20, Encyclopedia of Mathematics and Its Applications.* Amsterdam, The Netherlands: Addison-Wesley, 1983.