$\frac{3^{4k+2}-3^{2k+1}+2}{4}+3^{2k+1}$로 Decimation 된 3 진 m-수열의 상호 상관도에 관하여

*김지엽°, *최성태, *임태형, *노종선, **정하봉

*서울대학교 전기컴퓨터공학부, 뉴미디어 통신 공동연구소

**홍익대학교 전기전자공학부

On the Cross-Correlation of Ternary m-Sequences Decimated by $\frac{3^{4k+2}-3^{2k+1}+2}{4}+3^{2k+1}$

*Ji-Youp Kim°, *Sung-Tai Choi, *Taehyung Lim, *Jong-Seon No, and **Habong Chung

*Department of Electronics Engineering and Computer Science, INMC, Seoul National University

**Department of Electronic and Electrical Engineering, Hongik University

lakroforce@ccl.snu.ac.kr, stchoi@ccl.snu.ac.kr, jayelish@gmail.com, habchung@hongik.ac.kr

요 약

본 논문에서는 자연수 k, $n=2m=4k+2$에 대해 주기 3^n-1의 m-수열과 $\frac{3^{4k+2}-3^{2k+1}+2}{4}+3^{2k+1}$로 decimated 된 m-수열 간의 상호 상관도를 분석한다. 상호 상관도의 상한은 $4.5\cdot 3^m+1$로 구해 졌으며 이차 형식에 관한 이론이 사용되었다. 일반적인 경우와 달리, 이 문제의 경우 2 개가 아닌 4 개의 이차 형식이 상호 상관도에 연관되어 나타났다. 각각의 이차 형식에 대응되는 선형다항식의 차수는 3^{n-1}임에 비해, 해의 개수는 n의 값과 상관없이 항상 1, 9, 81 의 값만을 갖는다. 또한 4 개의 선형다항식 중 오직 하나만이 81 개의 해를 가질 수 있음을 증명하였다. 이 과정에서 유한체 $GF(q)$ 에서 정의된 다항식 $x^{q+1}-cx+c$의 해의 개수 및 해의 특징에 대한 Bluher 의 결과를 이용하였다.

1. 서론

p진 m-수열과 decimation d에 의해 decimated 된 수열 간의 상호 상관도에 대한 연구는 많은 연구자들에 의해 이미 수행되었다. Trachtenburg [1] 는 홀수 p에 대해서 $d=\frac{p^k+2}{2}$와 $d=p^{2k}-p^k+1$에 관한 상호 상관도를 조사하였으며, Helleseth [2] 는 다양한 decimation 에 대한 상호 상관도를 정리하였고, 새로운 decimation 에 대한 결과를 추가하였다. Muller [3] 는 홀수 n에 대해서 3 진 m-수열과 $d=\frac{(3^n+1)}{3+1}+\frac{3^n-1}{2}$로 decimation 된 수열의 상호 상관도의 절대값이 $2\sqrt{p^n}$ 이하임을 증명하였다. Hu [4] 는 Muller 의 결과를 $p=3\ mod\ 4$인 경우로 확장하였고 Xia [5] 는 상호 상관도의 분포를 계산하였다. 최근에는 Ness [6] 가 $\gcd(n,k)=1$인 홀수 k에 대해서 $d=\frac{3^k+1}{2}$인 경우에 3 진 m-수열의 상호 상관도를 유도하였다. 또한 홀수인 소수 p, 짝수 n, $\gcd(n,k)=1$ 인 k, $d=p^k+1$에 대해서 Seo [7] 가 상호 상관도의 크기가 $1+p\sqrt{p^n}$ 이하임을 보였다. Choi [8] 는 홀수인 소수 p, 홀수 m, $d=\frac{(p^m+1)^2}{2(p+1)}$에 대해서 상호 상관도 값을 연구하였다.

본 논문에서는 주기 $3^{4k+2}-1$ 의 3 진 m-수열과 $d=\frac{3^{4k+2}-3^{2k+1}+2}{4}+3^{2k+1}$로 decimation 된 수열 사이의 상호 상관도의 크기가 $4.5\,3^{2k+1}+1$이하임을 증명한다. 증명 과정에서 이차 형식(Quadratic form)에 대한 이론이 사용되며, 일반적인 경우와는 달리 4 개의 이차 형식이 관련된다. 이차 형식에 대응되는 선형 다항식(Linearized polynomial)의 해의 개수는 1, 9, 81 중 하나의 값만 가지며 특히 4 개의 선형 다항식 중 81 개의 근을 가지는 것은 단 하나 뿐이다. 이를 보이기 위해 Bluher [9] 의 결과를 이용하였다.

2. 상호 상관도의 크기

k 를 정수라 하고 $n = 2m = 4k + 2$, $d = \frac{3^{4k+2} - 3^{2k+1} + 2}{4} + 3^{2k+1}$ 라고 하자. $\mathbb{F}_{3^n}$ 을 3^n 개의 원소를 갖는 유한체라고 하고 α를 그 원시근이라고 하자. $N = 3^n - 1$을 $\mathbb{F}_{3^n}$에서 m-수열의 주기라고 하면 $(d, N) = \frac{3^m + 1}{4}$이고 $N/(d, N) = 4(3^m - 1)$ 이다. 이 장에서는 $0 \le l < N/(d, N)$ 에 대해 $tr_1^n(\alpha^t)$ 와 $tr_1^n(\alpha^{dt+l})$ 사이의 상호 상관도의 크기가 $4.5\, 3^{2k+1} + 1$ 이하임을 논할 것이다. 상호 상관도의 식은 다음과 같이 주어진다.

$$\begin{aligned} C(\tau) &= \sum_{t=0}^{N-1} \omega^{tr_1^n(\alpha^t) - tr_1^n(\alpha^{d(t+\tau)+l})} \\ &= \sum_{t=0}^{N-1} \omega^{tr_1^n(\alpha^t - \gamma\alpha^{dt})} \\ &= \sum_{x \in \mathbb{F}_{3^n}^*} \omega^{tr_1^n(x - \gamma x^d)} \end{aligned}$$

여기서 $\gamma = \alpha^{d\tau + l}$이고 ω는 원시 3 승근이다. 여기서 $x = y^{3^{n-1}-1}$로 치환한다. 이 때 $d(3^{n-1} - 1) = 3^m + 1 \mod N$이므로 다음과 같이 식이 주어진다.

$$tr_1^n(x - \gamma x^d) = tr_1^n(y^{3^{n-1}-1} - \gamma y^{3^m+1})$$

따라서 y 에 대한 이차 형식을 얻는다. 특히 $(3^{n-1} - 1, N) = 4$이므로 4 승 원분류(Cyclotomic class)의 원소 $a_i \in C_i$에 대해 다음이 성립한다.

$$4\big(1 + C(\tau)\big) = \sum_{i=0}^{3} \sum_{y \in \mathbb{F}_{3^n}} \omega^{tr_1^n\left(a_i y^{3^{n-1}-1} - \gamma a_i^d y^{3^m+1}\right)}$$

위 식의 상호 상관도를 구하기 위해서 사용하는 일반적인 기법은 이차 형식 $g_i(y) = tr_1^n\left(a_i y^{3^{n-1}-1} - \gamma a_i^d y^{3^m+1}\right)$의 계수(Rank)를 구하는 방법이다 [3]-[8]. 이는 임의의 y에 대해서 다음을 만족시키는 $z \in \mathbb{F}_{3^n}$ 의 개수와 관련이 있다.

$$g_i(y + z) - g_i(y) - g_i(z) = 0$$

위 식을 정리하면 다음과 같은 관계를 얻는다.

$$a_i^3 z^3 + a_i z^{3^{n-1}} - tr_m^n\left(\gamma a_i^d\right) z^{3^m} = 0$$

위 식은 선형 다항식이 됨을 알 수 있다. 따라서 근의 개수는 3 의 승수이며, $3^{n - rank(g_i)}$가 된다. 여기서 $rank(g_i)$는 이차 형식 g_i의 계수를 의미한다. 위 선형 다항식을 $f_i(z)$라고 하자. 이제 f_i의 근의 개수가 1, 9, 81 로 주어진다는 것을 증명할 것이다. 이를 위해서는 다음의 보조 정리가 필요하다.

보조 정리 1. [9] p 를 소수라고 하자. 다항식 $h_c(x) = x^{p^s+1} - cx + c,\ c \in \mathbb{F}_{p^n}^*$의 0 이 아닌 근은 0, 1, 2, $p^{(s,n)} + 1$개이다.

다음의 치환식을 이용하여 다항식 f_i의 형태를 바꿀 수 있다.

$$c_i = \frac{\left(tr_m^n(\gamma a_i)\right)^{3^{m-1}+1}}{a_i^{3^m+1}},\ y = \frac{tr_m^n(\gamma a_i)}{a_i^3} z^{3^m-3}$$

선형 다항식 f_i는 다음과 같은 형태로 변환된다.

$$y^{3^{m-1}+1} - c_i y + c_{\mathrm{i}}$$

보조 정리 1 에 의해 $c_i \neq 0$이면 위 다항식은 0, 1, 2, 10 개의 해를 갖는다. $c_i = 0$이면 1 개의 0 이 아닌 해를 갖는다. 여기서 위 y, z에 관한 치환식이 8-1 mapping 이므로 원래의 선형 다항식은 0, 8, 16, 80 개의 0 이외의 해를 가지며 따라서 0 을 포함해서 모두 1, 9, 17, 81 개의 해를 갖는다. 선형 다항식은 3 의 승수의 해의 개수를 가지므로 해의 개수는 1, 9, 18 개이다.

지금까지의 논의에 의해 이차 형식의 계수는 $n, n-2, n-4$ 중 하나임을 알 수 있다. 다음 보조 정리를 이용하면 4 개의 선형 다항식 중에 81 개의 근을 가지는 것은 단 하나 뿐이라는 것을 증명할 수 있다.

보조 정리 2. [9] k를 정수, $n = 4k + 2$, p는 홀수인 소수라고 하자. 그러면 $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^{2k}} = \mathbb{F}_{p^2}$ 이다. $c \in \mathbb{F}_{p^n}^*$ 일 때, $f(x) = x^{p^{2k}+1} - cx + c$ 라고 하자. 이 때 다음은 동치이다.

1) f는 $\mathbb{F}_{3^n}$에서 $p^2 + 1$개의 해를 갖는다.
2) f는 $\mathbb{F}_{3^n}$에서 최소한 2 개의 해를 가지고 모든 $\mathbb{F}_{3^n}$에서의 근 r에 대해 다음을 만족한다.
$$(r-1)^{\frac{p^n-1}{p^2-1}} = 1$$

위 보조 정리를 이용해서 다음 정리를 증명할 수 있다. 정리의 증명은 생략한다.

정리 1. 선형 다항식 f_i 가 81 개의 근을 가지면 $i = 0$이다. 즉 81 개의 근을 가지는 선형 다항식은 4 개의 다항식 중 하나 뿐이다.

따라서 이차 형식 $g_i,\ i = 0, 1, 2, 3,$ 이 가질 수 있는 계수의 조합은 다음과 같다.

$$\begin{gathered} (n, n, n, n), (n, n, n, n-2), (n, n, n, n-4), \\ (n, n, n-2, n-2), (n, n, n-2, n-4), \\ (n, n-2, n-2, n-2), (n, n-2, n-2, n-4), \\ (n-2, n-2, n-2, n-2), (n-2, n-2, n-2, n-4) \end{gathered}$$

위 결과와 다음 보조 정리로부터 상호 상관도의 크기의 상한을 유도할 수 있다.

보조 정리 3. [6] η 를 유한체 $\mathbb{F}_3$ 의 이차 지표

(Quadratic character)라고 하자. f를 $\mathbb{F}_{3^n}$에서의 정상적(Nondegenerate) 이차 형식이라 하고 그 행렬식을 Δ라고 하자. ω를 원시 3 승근이라고 하면 다음 식

$$S = \sum_{x \in \mathbb{F}_{3^n}} \omega^{f(x)}$$

의 값은 다음과 같이 주어진다.

$$S = \begin{cases} \epsilon 3^{\frac{n}{2}}, & n\text{이 짝수} \\ i\epsilon 3^{\frac{n}{2}} & n\text{이 홀수} \end{cases}$$

여기서 n이 짝수이면 $\epsilon = \eta((-1)^{\frac{n}{2}}\Delta)$이고 홀수이면 $\epsilon = \eta((-1)^{\frac{n-1}{2}}\Delta)$이다.

위 보조 정리를 이용하여 위 9 가지 계수 조합에 대해서 상호 상관도의 상한을 유도할 수 있다. 위 9 가지의 경우 중 가장 큰 상한을 유도하는 것은 $(n-2, n-2, n-2, n-4)$이다. 이 경우 상호 상관도는 다음과 같이 표현된다.

$$4\big(1 + C(\tau)\big) = \sum_{i=0}^{3} \sum_{y \in \mathbb{F}_{3^n}} \omega^{g_i(y)}$$
$$= \epsilon_0 3^2 3^{\frac{n-2}{2}} + \epsilon_1 3^2 3^{\frac{n-2}{2}} + \epsilon_2 3^2 3^{\frac{n-2}{2}} + \epsilon_3 3^4 3^{\frac{n-4}{2}}$$
$$= 3(\epsilon_0 + \epsilon_1 + \epsilon_2)3^m + 3^2\epsilon_3 3^m$$
$$\leq 18 \cdot 3^m$$

여기서 $\epsilon_0, \ldots, \epsilon_3$은 ± 1이므로 위 식으로부터 $C(\tau)$의 절대값은 $4.5\ 3^m + 1$로 상한 된다는 것을 알 수 있다.

3. 결론

본 논문에서는 이차 형식 이론을 이용하여 3 진 m-수열과 decimation $d = \frac{3^{4k+2} - 3^{2k+1} + 2}{4} + 3^{2k+1}$ 로 decimation 된 수열 간의 상호 상관도의 절대값 크기가 $4.5\ 3^m + 1$이하임을 증명하였다.

4. 감사의 글

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

5. 기타

본 논문의 내용은 2012 년 7 월에 개최되는 IEEE Symposium on Information Theory 2012 에 제출되었음

6. 참고 문헌

[1] H. M. Trachtenberg, “On the cross-correlation functions of maximal recurring sequences,” Ph.D. dissertation, Univ. of Southern California, Los Angeles, CA, 1970.

[2] T. Helleseth, ”Some results about the cross-correlation function between two maximal linear sequences,” *Discr. Math.*, vol. 16, pp. 209-232, 1976.

[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] Z. Hu, X. Li, D. Mills, E. Mller, W. Sun, W. Willems, Y. Yang, and Z.Zhang, ”On the crosscorrelation of sequences with the decimation factor $d = \frac{(p^n+1)}{p+1} + \frac{p^n-1}{2}$,” *Appl. Algebra Eng. Commun. Comput.*, vol. 12, no. 3, pp. 255-263, 2001.

[5] Y. Xia, X. Zeng, and L. Hu, ”Further crosscorrelation properties of sequences with the decimation factor $d = \frac{(p^n+1)}{p+1} + \frac{p^n-1}{2}$,” *Appl. Algebra Eng. Commun. Comput.*, vol. 21, no. 5, pp. 329-342, 2010.

[6] G. J. Ness, T. Helleseth, and A. Kholosha, ”On the correlation distribution of the coulter-matthews decimation,” *IEEE Trans. Inf. Theory*, vol.52, no. 5, pp. 2241-2247, May. 2006.

[7] E.-Y. Seo, Y.-S. Kim, J.-S. No, and D.-J. Shin, ”Cross-correlation distribution of p-ary m-sequence and its p + 1 decimated sequences with shorter period,” *IEICE Trans. Fundamentals.*, vol. E90-A, no. 11, pp. 2568-2574, Nov. 2007.

[8] S.-T. Choi, T. Lim, J.-S. No, and H. Chung, ”On the crosscorrelation of a p-ary m-sequences of period $p^{2m} - 1$ and its decimated sequences by $d = \frac{(p^m+1)^2}{2(p+1)}$,” *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1873-1879, March 2012.

[9] A. W. Bluher, ”On $x^{q+1} + ax + b$,” *Finite Fields and Their Applications*, vol. 10, no. 3, pp. 285-305, Jul. 2004.