두 Decimate 된 수열 간의 상호 상관도의 상한

*조창민°, *이위직, *노종선, **김영식

*서울대학교 전기정보공학부

**조선대학교 정보통신공학과

Upper Bound on the Cross-Correlation Magnitude of Two Decimated Sequences

*Chang-Min Cho°, *Wijik Lee, *Jong-Seon No, and **Young-Sik Kim

*Department of ECE, Seoul National University

**Department of ICE, Chosun University

ccm8686@ccl.snu.ac.kr, leewj422@ccl.snu.ac.kr, jsno@snu.ac.kr, iamyskim@chosun.ac.kr

요 약

본 논문에서는 홀수인 소수 p, $n=2m$, $p^m \equiv 1 \pmod 4$일 때에 m-수열의 서로 다른 두 개의 decimate 된 수열, $s(2t+i)$와 $s(2(p^m+1)t+j)$ 간의 상호 상관도(cross-correlation)를 분석한다. 두 수열 간의 상호 상관도의 절대값의 상한 값이 $\frac{3}{2}p^m+\frac{1}{2}$로 주어진다는 것을 Weil 의 exponential sum 에 대한 bound 를 이용해서 증명한다.

1. 서론

유사잡음수열(PN sequence)은 CDMA, 대역확산, 암호, GPS 등의 다양한 통신 분야에서 활용되는 신호이다. 이러한 수열이 가져야 하는 특성으로 낮은 상관도(correlation) 값이 있으며, 이를 만족하는 수열군을 생성하기 위한 방법으로 m-수열과 이를 decimate 한 수열 간의 상호 상관도를 구하는 연구들이 이루어졌다. [1]-[5]

한편, 최근에는 m-수열을 2 로 decimate 한 수열과 또다른 decimate 된 수열 간의 상호 상관도를 구하고, 이 수열들을 이용하여 새로운 수열 군을 생성하는 연구가 진행되었다. [6]-[9]

본 논문에서는 홀수인 소수 p, $n=2m$, $p^m \equiv 1 \pmod 4$ 일 때에 대하여, 2 로 decimate 된 수열 $s(2t+i)$ 와 $2(p^m+1)$ 으로 decimate 된 수열 $s(2(p^m+1)t+j)$ 간의 상호 상관도에 대하여 분석한다. 상호 상관도 함수는 p와 n, i 및 j에 따라 다양한 값을 가지고, 이때의 상호 상관도의 절대값의 상한은 $\frac{3}{2}p^m+\frac{1}{2}$로 주어진다.

2. 배경 이론

소수 p와 양의 정수 n에 대하여, F_{p^n}은 p^n개의 원소를 가지는 유한체(finite field)이고, $F_{p^n}^* = F_{p^n} \setminus \{0\}$이다. 이때 F_{p^n}에서 F_{p^m} $(m|n)$으로의 trace 함수 $\mathrm{tr}_m^n(\cdot)$을 다음과 같이 정의한다.

$$\mathrm{tr}_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{p^{mi}}$$

다음으로, group G 상에서의 character 는 G에서 multiplicative group U로의 group homomorphism 으로 정의되며, 이때 U의 원소는 크기가 1 인 복소수이다. 유한체에서는 additive character 와 multiplicative character 의 두 가지 character 를 정의할 수 있으며, additive character 는 trace 함수를 이용해 다음과 같이 정의된다.

$$\chi(c) = e^{\frac{2\pi i \mathrm{tr}_1^n(c)}{p}} \quad \text{for all } c \in F_{p^n}$$

한편 multiplicative character 는 다음과 같이 정의할 수 있다. α가 유한체 F_{p^n}의 원시근(primitive element) 이고, $j = 0,1,\dots,p^n-2$에 대해서

$$\psi_j(\alpha^k) = e^{\frac{2\pi i j k}{p^n-1}} \quad \text{for } k = 0,1,\dots,p^n-2$$

으로 나타낼 수 있다. 이러한 multiplicative character 중 한 가지로, $j=\frac{p^n-1}{2}$ 로 설정했을 경우 이를 quadratic character $\eta(x)$으로 표기하며, 이 함수는 x 의 값이 quadratic residue 일 때는 1 이 되고, quadratic nonresidue 일 때에는 -1 이다.

다음은 character 의 합의 크기에 대한 Weil 의 bound 로, 본 논문의 결과의 증명에 사용된다.

사전정리 1 (Weil's bound): [10] χ와 ψ가 각각 F_q의 additive character 와 order m인 multiplicative character 라 하자. $f, g \in F_q[x]$이고, 어떠한 $h \in \bar{F}_q[x]$에 대하여 $f \neq h^p - h$ 또는 $g \neq h^m$이 성립할 경우, 다음 식이 성립한다.

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

여기서 e는 f의 차수이고, s는 g의 $\bar{F}_q[x]$에서의 서로 다른 근의 개수이다.

3. 상호 상관도 분석

두 수열 $s(2t+i)$와 $s(2(p^m+1)t+j)$ 간의 상호 상관도 함수는 다음과 같이 쓸 수 있다.

$$\begin{aligned} C_{i,j}(\tau) &= \sum_{t=0}^{\frac{p^n-1}{2}-1} \omega^{\mathrm{tr}_1^n\left(\alpha^{2(t+\tau)+i}-\alpha^{2(p^m+1)t+j}\right)} \\ &= \frac{1}{2}\sum_{t=0}^{p^n-2} \omega^{\mathrm{tr}_1^n\left(\alpha^{2(t+\tau)+i}-\alpha^{2(p^m+1)t+j}\right)} \\ &= \frac{1}{2}\sum_{x\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n\left(ax^2-bx^{2(p^m+1)}\right)} \end{aligned}$$

여기에서 $x=\alpha^t$, $a=\alpha^{2\tau+i}$, $b=\alpha^j$이다. $y=x^2$으로 놓으면 위 식을 다음과 같이 바꿀 수 있다.

$$C_b(a) = \frac{1}{2}\left[\sum_{y\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n\left(ay-by^{p^m+1}\right)} + \sum_{y\in F_{p^n}^*} \eta(y)\omega^{\mathrm{tr}_1^n\left(ay-by^{p^m+1}\right)}\right]$$

이제 상호 상관도 크기 $|C_b(a)|$의 상한을 구한다. 위 식에서 첫 번째 항은 p진 Kasami 수열[5]의 상호 상관도 특성으로부터

$$\left|\sum_{y\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n\left(ay-by^{p^m+1}\right)}\right| \le p^m+1$$

임을 알 수 있다. 다음으로,

$$\left|\sum_{y\in F_{p^n}^*} \eta(y)\omega^{\mathrm{tr}_1^n\left(ay-by^{p^m+1}\right)}\right| \le 2p^m$$

이 된다. 이는 함수 $\mathrm{tr}_1^n\left(ay-by^{p^m+1}\right)$와 $\mathrm{tr}_1^n(a'z-b'z^2)$이 변수 a,b,a',b'의 값을 잘 선택함으로써 동일한 값을 얻을 수 있음을 보이고, 여기에 Weil's bound를 적용하여

$$\left|\sum_{y\in F_{p^n}^*} \eta(y)\omega^{\mathrm{tr}_1^n\left(ay-by^{p^m+1}\right)}\right| = \left|\sum_{z\in F_{p^n}^*} \eta(g(z))\omega^{\mathrm{tr}_1^n(a'z-b'z^2)}\right| \le 2p^m$$

임을 보일 수 있다. 여기에서 $g(z)$은 z에서 y로의 하나의 서로 다른 근을 가지는 함수이다.

따라서, 상호 상관도 크기 $|C_b(a)|$의 상한은

$$\begin{aligned} |C_b(a)| &= \frac{1}{2}\left|\sum_{y\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n\left(ay-by^{p^m+1}\right)} + \sum_{y\in F_{p^n}^*} \eta(y)\omega^{\mathrm{tr}_1^n\left(ay-by^{p^m+1}\right)}\right| \\ &\le \frac{1}{2}\left(\left|\sum_{y\in F_{p^n}^*} \omega^{\mathrm{tr}_1^n\left(ay-by^{p^m+1}\right)}\right| + \left|\sum_{y\in F_{p^n}^*} \eta(y)\omega^{\mathrm{tr}_1^n\left(ay-by^{p^m+1}\right)}\right|\right) \\ &\le \frac{3}{2}p^m+\frac{1}{2} \end{aligned}$$

으로 주어진다.

4. 참고 문헌

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

[2] 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.

[3] J. Luo, "Cross correlation of nonbinary Niho-type sequences," *Proc. IEEE Int. Symp. Information Theory*, pp. 1297-1299, Austin, USA, Jun. 2010.

[4] Y. Xia and S. Chen, "Cross-correlation distribution between a *p*-ary m-sequence and its decimated sequence with decimation factor $\frac{(p^m+1)^2}{2(p^e+1)}$," *IEICE Trans. Fundamentals*, vol. E97-A, no. 5, pp. 1103-1112, May 2014.

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

[6] J. Y. Kim, S. T. Choi, J. S. No, and H. Chung, "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. 3825-3830, Jun. 2011.

[7] Y. Xia and S. Chen, "A new family of *p*-ary sequences with low correlation constructed from decimated sequences," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 6037-6046, Sep. 2012.

[8] W. Lee, J. Y. Kim, and J. S. No, "New families of *p*-ary sequences of period $\frac{p^n-1}{2}$ with low maximum correlation magnitude," *IEICE Trans. Commun.*, vol.E97-B, no.11, pp.2311-2315, Nov. 2014.

[9] C. M. Cho, J. Y. Kim, and J. S. No, "New *p*-ary sequence families of period $\frac{p^n-1}{2}$ with good correlation property using two decimated m-sequences," *IEICE Trans. Commun.*, vol.E98-B, no. 7, pp. 1268-1275, July 2015.

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