두 Decimate된 수열 간의 상호 상관도 분포

조창민, 노종선
서울대학교
ccm8686@ccl.snu.ac.kr, jsno@snu.ac.kr

Cross-Correlation Distribution between the Two Decimated Sequences

Chang-Min Cho, Jong-Seon No
Seoul National University

요 약

본 논문에서는 소수 $p=3 \bmod 4$이고 $n=0 \bmod 4$일 때, 또는 소수 $p=1 \bmod 4$이고 짝수 n일 때 m-수열의 두 개의 decimate된 수열 간의 상호 상관도를 분석한다. 이때 한 수열은 2로, 다른 한 수열은 $d'=\frac{1}{2}(p^{n/2}+1)^2$으로 decimate되었으며, 여기서 후자의 값은 Seo, Kim, No, Shin(2008)에서 사용된 $d=\left(\frac{p^{n/2}+1}{2}\right)^2$의 두 배이다. 이때의 상호 상관도는 shift 값에 따라 최대 세 개의 값을 가질 수 있음을 보이고, 상호 상관도의 분포를 구하였다.

Ⅰ. 서 론

낮은 상호 상관도를 가지는 수열 군을 찾기 위한 많은 연구가 진행되어 왔다. 그러한 한 방법으로, p-진 m-수열 $s(t)$와 그의 decimate된 수열 $s(dt)$ 간의 상호 상관도를 구하는 연구가 이루어져 왔다[1]-[4]. 한편, Kim, Choi, No와 Chung[5]은 $p=3 \bmod 4$이고 n이 홀수일 때 각각 2와 $2d=2\left(\frac{p^n-1}{2}-p^{n-1}\right)$으로 decimate된 m-수열을 이용하여 낮은 상호 상관도를 가지는 수열 군을 생성하였다. Xia와 Chen[6]은 위 연구의 영향을 받아, 홀수인 소수 p와 $n \geq 3$, $\frac{n}{\gcd(m,n)} \geq 3$을 만족하는 m에 대하여 각각 2와 p^m+1으로 decimate된 수열을 이용해 수열 군을 생성하고, 이때의 상관도 및 그 분포를 구하였다.

본 논문에서는 소수 $p=3 \bmod 4$이고 $n=0 \bmod 4$일 때, 또는 소수 $p=1 \bmod 4$이고 짝수 n일 때 2로 decimate된 수열 $s(2t+i)$, $i=0,1$과 $d'=2d=\frac{1}{2}(p^{n/2}+1)^2$으로 decimate된 수열 $s(d't+l)$, $0 \leq l < p^{n/2}+1$, $l \neq \frac{p^{n/2}+1}{2}$ 간의 상호 상관도를 분석한다. 이때 $d=\left(\frac{p^{n/2}+1}{2}\right)^2$는 Seo, Kim, No와 Shin[3]이 사용한 decimation 값이다. 상호 상관도는 i 및 l의 값에 따라 최대 세 가지 값을 가질 수 있으며, 이때의 최대값은 $\frac{-1+3p^{n/2}}{2}$이다. 또한 i 및 l의 값에 따른 수열들의 상호 상관도의 분포를 구하였다.

Ⅱ. 사전 지식

소수 p와 양의 정수 n에 대하여, F_{p^n}은 p^n개의 원소를 가지는 유한체이다. 유한체 F_{p^n}으로부터 $F_{p^m}(m|n)$으로의 trace 함수 $tr_m^n(x)$는 다음과 같이 정의된다.

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

α가 유한체 F_{p^n}의 원시근이라 할 때, trace 함수를 이용하여 주기가 p^n-1인 p-진 m-수열 $s(t)$를 다음과 같이 쓸 수 있다.

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

p-진 m-수열 $s(t)$와 이를 양의 정수 d로 decimate한 수열 $s(dt+l)$ 간의 상호 상관도는 다음과 같이 나타난다.

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

여기서 ω는 $e^{\frac{2\pi i}{p}}$ 이다.

$\gcd(p^n-1,d')=p^{n/2}+1$이므로 $s(d't+l)$의 주기는 $p^{n/2}-1$이고, $s(2t+i)$의 주기는 $L=\frac{p^n-1}{2}$이다. 한편 $l=\frac{p^{n/2}+1}{2}$일 경우에는 $s(d't+l)$의 모든 값이 0인 수열이 되므로, 이 경우는 cross-correlation 분석에서 제외하여야 한다.

본 논문에서 상호 상관도 및 그 분포를 구하기 위해 다음과 같은 사전정리를 사용하였다.

사전정리 1: [1] 홀수인 소수 p와 짝수 n에 대해 다음이 성립한다.

$$\sum_{y \in F_{p^n}} \omega^{tr(ay^{p^{n/2}+1})}=\begin{cases} p^n, & \text{if } a+a^{p^{n/2}}=0 \\ -p^{n/2}, & \text{if } a+a^{p^{n/2}} \neq 0 \end{cases}$$

사전정리 2: [1] 홀수인 소수 p에 대해 다음이 성립한다.

$$\sum_{y \in F_{p^n}} \omega^{ay^2}=\begin{cases} p^n, & \text{if } a=0 \\ (-1)^{n+1}((-1)^{\frac{p-1}{2}}p)^{n/2}, & \text{if } a\text{: square} \\ (-1)^n((-1)^{\frac{p-1}{2}}p)^{n/2}, & \text{if } a\text{: nonsquare} \end{cases}$$

Ⅲ. 상호 상관도 계산

수열 $s(2t+i)$와 $s(d't+l)$ 간의 상호 상관도는 다음과 같이 주어진다.

$$C_{i,l}(\tau)=\sum_{t=0}^{L-1}\omega^{s(2(t+\tau)+i)-s(d't+l)}=\sum_{t=0}^{L-1}\omega^{tr_1^n(\alpha^{2(t+\tau)+i}-\alpha^{d't+l})}$$

$\gcd(p^n-1,d')$이 2의 배수이므로

$$\sum_{t=L}^{p^n-2}\omega^{tr_1^n(\alpha^{2(t+\tau)+i}-\alpha^{d't+l})}=\sum_{t=0}^{L-1}\omega^{tr_1^n(\alpha^{2(t+\tau)+i}-\alpha^{d't+l})}$$

이 성립하고, 상호 상관도 식을 다음과 같이 변형할 수 있다.

$$C_{i,l}(\tau)=\frac{1}{2}\sum_{t=0}^{p^n-2}\omega^{tr_1^n(\alpha^{2(t+\tau)+i}-\alpha^{d't+l})}=\frac{1}{2}\sum_{x\in F_{p^n}^*}\omega^{tr_1^n(ax^2-bx^{d'})}$$

여기서 $x=\alpha^t$, $a=\alpha^{2\tau+i}$, $b=\alpha^l$이다.

이제 [3]에서와 유사한 방식으로 상호 상관도의 개수를 구할 수 있다. $x=\alpha^j y^{\frac{p^{n/2}+1}{2}}$, $0\le j<\frac{p^{n/2}+1}{2}$으로 치환하면 $y^{\frac{p^{n/2}+1}{2}d'}=y^{p^{n/2}+1}$이고,

$$C_{i,l}(\tau)+\frac{1}{2}=\frac{1}{2}\sum_{x\in F_{p^n}}\omega^{tr_1^n(ax^2-bx^{d'})}$$
$$=\frac{1}{p^{n/2}+1}\sum_{j}\sum_{y\in F_{p^n}}\omega^{tr_1^n(y^{p^{n/2}+1}(a\alpha^{2j}-b\alpha^{d'j}))}$$

이다. $K(a,b)$를 $(a\alpha^{2j}-b\alpha^{d'j})^{p^{n/2}}+a\alpha^{2j}-b\alpha^{d'j}=0$의 해의 개수라 하면, 사전정리 1에 의해

$$C_{i,l}(\tau)+\frac{1}{2}=p^{n/2}(K(a,b)-\frac{1}{2})$$

이 된다. $2j=k$로 치환하면 $d'j=dk$가 되어 [3]에서의 계산 과정을 적용할 수 있다. $l\neq\frac{p^{n/2}+1}{2}$일 때, 가능한 해의 개수는 $i=0$일 때는 0, 1, 2가 되고 $i=1$일 때는 0, 1이 된다. 따라서 상호 상관도의 값의 종류는 다음과 같다.

Case 1) $i=0$

$$\left\{\frac{-1-p^{n/2}}{2},\frac{-1+p^{n/2}}{2},\frac{-1+3p^{n/2}}{2}\right\}$$

Case 2) $i=1$

$$\left\{\frac{-1-p^{n/2}}{2},\frac{-1+p^{n/2}}{2}\right\}$$

다음으로 상호 상관도의 값의 분포를 구한다. 이를 위해서는 $\sum_{\tau=0}^{L-1}C_{i,l}(\tau)$ 및 $\sum_{\tau=0}^{L-1}C_{i,l}^2(\tau)$를 구한 뒤 각 값의 발생 회수에 대한 연립방정식을 풀면 된다.

$$\sum_{\tau=0}^{L-1}C_{i,l}(\tau)=\frac{1}{2}\sum_{\tau=0}^{L-1}\sum_{x\in F_{p^n}^*}\omega^{tr_1^n(ax^2-bx^{d'})}=\frac{1}{2}\sum_{x\in F_{p^n}^*}\omega^{-tr_1^n(bx^{d'})}\sum_{\tau=0}^{L-1}\omega^{tr_1^n(ax^2)}$$

$$\sum_{\tau=0}^{L-1}C_{i,l}^2(\tau)=\frac{1}{4}\sum_{\tau=0}^{L-1}\sum_{x_1\in F_{p^n}^*}\omega^{tr_1^n(ax_1^2-bx_1^{d'})}\sum_{x_2\in F_{p^n}^*}\omega^{tr_1^n(ax_2^2-bx_2^{d'})}$$
$$=\frac{1}{4}\sum_{x_1\in F_{p^n}^*}\sum_{x_2\in F_{p^n}^*}\omega^{-tr_1^n(b(x_1^{d'}+x_2^{d'}))}\sum_{\tau=0}^{L-1}\omega^{tr_1^n(a(x_1^2+x_2^2))}$$

$y=\alpha^\tau$로 치환하면 $a=y^2\alpha^i$이고, 이를 위 수식들에 적용하면 τ에 대한 합은 다음과 같이 표현할 수 있다.

$$\sum_{\tau=0}^{L-1}\omega^{tr_1^n(ax^2)}=\frac{1}{2}\sum_{y\in F_{p^n}^*}\omega^{tr_1^n(y^2\alpha^i x^2)}$$

$$\sum_{\tau=0}^{L-1}\omega^{tr_1^n(a(x_1^2+x_2^2))}=\frac{1}{2}\sum_{y\in F_{p^n}^*}\omega^{tr_1^n(y^2(x_1^2+x_2^2))}$$

이제 사전정리 1과 2를 이용하면 $\sum_{\tau=0}^{L-1}C_{i,l}(\tau)$과 $\sum_{\tau=0}^{L-1}C_{i,l}^2(\tau)$를 구할 수 있다. 상호 상관도의 분포를 정리하면 다음과 같다.

Case 1) $i=0$

$$C_{i,l}(\tau)=\begin{cases}\frac{-1-p^{n/2}}{2}, & \frac{1}{8}(3p^n-4p^{n/2}-7)\ \text{times}\\ \frac{-1+p^{n/2}}{2}, & \frac{p^{n/2}+1}{2}\ \text{times}\\ \frac{-1+3p^{n/2}}{2}, & \frac{1}{8}(p^n-1)\ \text{times}\end{cases}$$

Case 2) $i=1$

$$C_{i,l}(\tau)=\begin{cases}\frac{-1-p^{n/2}}{2}, & \frac{1}{4}(p^n-1)\ \text{times}\\ \frac{-1+p^{n/2}}{2}, & \frac{1}{4}(p^n-1)\ \text{times}\end{cases}$$

ACKNOWLEDGMENT

이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2012-0000186).

참 고 문 헌

[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] 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. 12, pp. 5345-5353, Dec. 2008.

[4] 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 $\frac{(p^m+1)^2}{2(p+1)}$,"IEEE Transactions on Information Theory, vol. 58, no. 3, pp. 1873-1879, March 2012.

[5] J. Y. Kim, S. T. Choi, J. S. No, and H. Chung, "A new family of p-ary decimated sequences with period $\frac{p^n-1}{2}$ with low correlation," IEEE Trans. Inf. Theory, vol. 57, no. 6, pp. 3825-3830, Jun. 2011.

[6] 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, September 2012