LETTER Special Section on Signal Design and its Application in Communications

Autocorrelation of New Generalized Cyclotomic Sequences of Period p^n*

Seok-Yong JIN[†a)], ***Student Member***, **Young-Joon KIM**[††], ***Member***, ***and*** **Hong-Yeop SONG**[†], ***Nonmember***

SUMMARY In this paper, we calculate autocorrelation of new generalized cyclotomic sequences of period p^n for any $n > 0$, where p is an odd prime number.

key words: *generalized cyclotomic sequence, autocorrelation, linear complexity*

1. Introduction

Let $n \geq 2$ be a positive integer and $Z_n^\times$ be the multiplicative group of the integer ring Z_n. For a partition $\{D_i | i = 0, 1, \cdots, d-1\}$ of $Z_n^\times$, if there exist elements $g_1, \cdots, g_d$ of $Z_n^\times$ satisfying $D_i = g_i D_0$ for all i where D_0 is a multiplicative subgroup of $Z_n^\times$, the D_i are called *generalized cyclotomic classes* of order d. There have been lots of studies about cyclotomy with respect to p or p^2 or pq where p and q are distinct odd primes [1]–[3]. In 1998, Ding and Helleseth [4] introduced the new generalized cyclotomy with respect to $p_1^{e_1} \cdots p_t^{e_t}$ and defined a *balanced* binary sequence based on their own generalized cyclotomy, where $p_1, \cdots, p_t$ are distinct odd primes and $e_1, \cdots, e_t$ are positive integers.

The linear complexity (LC) of new generalized cyclotomic sequence of order 2 with respect to p^2 [2] and p^3 [6] is known. Finally, the LC of those sequences of period p^n is calculated by by Yan, Li and Xiao [7] and by Kim and Song [8] independently.

While the linear complexity is an important measure of pseudo-random sequences for cryptographic application, autocorrelation is another important measure for their application to communication systems for various purposes [5].

In this paper, we compute autocorrelation of new generalized cyclotomic sequences of order 2 with respect to p^n for arbitrary positive integer n. Legendre sequences ($n = 1$) [5], prime square sequences ($n = 2$) [2], and prime cube sequences ($n = 3$) [6]–[8] are some important subclasses of these sequences. For simplicity, we will call these sequences as new generalized cyclotomic sequences of period p^n. It turned out that their autocorrelation property is not as good as that of Legendre sequences when $n > 1$. In Sect. 2, we review new generalized cyclotomic sequences of period p^n and present their autocorrelation values. In Sect. 3, we prove our main result.

Manuscript received January 14, 2010.

Manuscript revised May 20, 2010.

[†]The authors are with the School of Electrical and Electronics Engineering, Yonsei University, Seoul, 120-749, Korea.

[††]The author is currently with Samsung Electronics, Co., Ltd., Suwon, Korea.

*This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2009-0083888).

a) E-mail: sy.jin@yonsei.ac.kr

DOI: 10.1587/transfun.E93.A.2345

2. Generalized Cyclotomic Sequences of Period p^n and Its Autocorrlation

Given a prime $p \geq 2$, let g be a primitive root of p^2. Then it follows that g is also a primitive root of p^k, $k \geq 1$. By definition, the order of g modulo p^k is $p^k - p^{k-1}$ for $1 \leq k \leq n$. Let $D_0^{(p^k)} = \langle g^2 \rangle \pmod{p^k}$ be the cyclic group generated by g^2 modulo p^k, and let $D_1^{(p^k)} = g D_0^{(p^k)} \pmod{p^k}$ be the coset of $D_0^{(p^k)}$ by g. It then follows that $D_0^{(p^k)} \cup D_1^{(p^k)}$ is the multiplicative group $Z_{p^k}^\times$. In fact, $Z_{p^k} = Z_{p^k}^\times \cup pZ_{p^{k-1}}$, where $pZ_{p^{k-1}} = \{0, p, 2p, \cdots, (p^{k-1}-1)p\}$. It can be identified that

$$Z_{p^n} = \left(\bigcup_{k=1}^{n} p^{n-k} D_0^{(p^k)} \right) \cup \left(\bigcup_{k=1}^{n} p^{n-k} D_1^{(p^k)} \right) \cup \{0\}.$$

Define C_0 and C_1 as

$$C_0 = \bigcup_{k=1}^{n} p^{n-k} D_0^{(p^k)}, \tag{1}$$

$$C_1 = \bigcup_{k=1}^{n} p^{n-k} D_1^{(p^k)} \cup \{0\}. \tag{2}$$

In [4], Ding and Helleseth defined the new generalized cyclotomic sequences $\mathbf{s} = \{s(i)\}_{i=0}^{p^n-1}$ of period p^n as shown below:

$$s(i) = \begin{cases} 0, & i \in C_0 \\ 1, & i \in C_1. \end{cases}$$

The periodic autocorrelation function $C_s(\tau)$ of a binary sequence $\{s(n)\}$ of period N is defined by

$$C_s(\tau) = \sum_{n=0}^{N-1} (-1)^{s(n+\tau)+s(n)},$$

where $n + \tau$ takes modulo N.

Theorem. *Let p be an odd prime and n be a positive integer. Then the autocorrelation function $C_s(\tau)$ of new generalized cyclotomic sequence* **s** *of period p^n is given as follows:*

Copyright © 2010 The Institute of Electronics, Information and Communication Engineers

1. *If $p \equiv 1 \pmod 4$, then $C_s(\tau)$ is given as*

$$C_s(\tau) = \begin{cases} p^n, & \tau = 0 \pmod{p^n} \\ p^n - p^u - p^{u-1} - 2, & \tau \in p^{n-u}D_0^{(p^u)} \\ p^n - p^u - p^{u-1} + 2, & \tau \in p^{n-u}D_1^{(p^u)} \end{cases}$$

for $u = 1, \ldots, n$.

2. *If $p \equiv 3 \pmod 4$, then $C_s(\tau)$ is given as*

$$C_s(\tau) = \begin{cases} p^n, & \tau = 0 \pmod{p^n} \\ p^n - p^u - p^{u-1}, & \tau \in p^{n-u}D_0^{(p^u)} \cup p^{n-u}D_1^{(p^u)} \end{cases}$$

for $u = 1, \ldots, n$. ■

3. Proof of Theorem

To compute the autocorrelation of new generalized cyclotomic sequences of period p^n, we use the generalized cyclotomic numbers of order 2 with respect to p^k for $k \geq 1$, defined in [10],

$$(i, j)_{p^k} = \left|\left(D_i^{(p^k)} + 1\right) \cap D_j^{(p^k)}\right|,$$

where $i, j = 0, 1$ and $k = 1, \ldots, n$. It is known [4] that:

1. If $p = 1 \pmod 4$, then

$$(0,0)_{p^k} = \frac{p^{k-1}(p-5)}{4},$$
$$(0,1)_{p^k} = (1,0)_{p^k} = (1,1)_{p^k} = \frac{p^k(p-1)}{4}.$$

2. If $p = 3 \pmod 4$, then

$$(0,1)_{p^k} = \frac{p^{k-1}(p+1)}{4},$$
$$(0,0)_{p^k} = (1,0)_{p^k} = (1,1)_{p^k} = \frac{p^{k-1}(p-3)}{4}.$$

Now let us define $\Delta_{*,k}(\tau)$ and $\Delta_{l,k}(\tau)$ as

$$\Delta_{*,k}(\tau) := \left|\{0\} \cap \left(p^{n-k}D_0^{(p^k)} + \tau\right)\right| \quad \text{and}$$
$$\Delta_{l,k}(\tau) := \left|p^{n-l}D_1^{(p^l)} \cap \left(p^{n-k}D_0^{(p^k)} + \tau\right)\right|.$$

Then we have the following two lemmas, which play an important role to prove our main result.

Lemma 1 *$\Delta_{*,k}(\tau)$ is given as*:

$$p = 1 \pmod 4: \quad \Delta_{*,k}(\tau) = \begin{cases} 1, & \tau \in p^{n-k}D_0^{(p^k)}, \\ 0, & \text{otherwise.} \end{cases}$$

$$p = 3 \pmod 4: \quad \Delta_{*,k}(\tau) = \begin{cases} 1, & \tau \in p^{n-k}D_1^{(p^k)}, \\ 0, & \text{othewise.} \end{cases}$$

■

Lemma 2 *$\Delta_{l,k}(\tau)$ is as follows*:

- *If $l = k$,*

$$\Delta_{k,k}(\tau) = \begin{cases} (0,1)_{p^k}, & \tau \in p^{n-k}D_0^{(p^k)} \\ (1,0)_{p^k}, & \tau \in p^{n-k}D_1^{(p^k)} \\ 0, & \text{othewise.} \end{cases}$$

- *If $l < k$, then $\Delta_{l,k}(\tau)$ is equal to*
  1. $p = 1 \pmod 4$

$$\Delta_{l,k}(\tau) = \begin{cases} \frac{p^l - p^{l-1}}{2}, & \tau \in p^{n-k}D_0^{(p^k)}, \\ 0, & \text{othewise.} \end{cases}$$

  2. $p = 3 \pmod 4$

$$\Delta_{l,k}(\tau) = \begin{cases} \frac{p^l - p^{l-1}}{2}, & \tau \in p^{n-k}D_1^{(p^k)}, \\ 0, & \text{othewise.} \end{cases}$$

- *If $l > k$, we have*

$$\Delta_{l,k}(\tau) = \begin{cases} \frac{p^k - p^{k-1}}{2}, & \tau \in p^{n-l}D_1^{(p^l)} \\ 0, & \text{othewise.} \end{cases}$$

■

Now we are ready to prove our main result. First we define the difference function $d_s(i, j; \tau)$ as

$$d_s(i, j; \tau) = \left|C_i \cap (C_j + \tau)\right|$$

for $i, j = 0, 1$. Since $C_s(\tau) = p^n - 4d_s(1, 0; \tau)$, we need to calculate $d_s(1, 0; \tau)$:

$$\begin{aligned} d_s(1,0;\tau) &= |C_1 \cap (C_0 + \tau)| = \sum_{k=1}^{n} \left|C_1 \cap (p^{n-k}D_0^{(p^k)} + \tau)\right| \\ &= \sum_{k=1}^{n} \left|\{0\} \cap (p^{n-k}D_0^{(p^k)} + \tau)\right| \\ &+ \sum_{k=1}^{n} \left|p^{n-k}D_1^{(p^k)} \cap (p^{n-k}D_0^{(p^k)} + \tau)\right| \\ &+ \sum_{l=1}^{n-1} \sum_{k=l+1}^{n} |p^{n-l}D_1^{(p^l)} \cap (p^{n-k}D_0^{(p^k)} + \tau)| \\ &+ \sum_{l=2}^{n} \sum_{k=1}^{l-1} \left|p^{n-l}D_1^{(p^l)} \cap (p^{n-k}D_0^{(p^k)} + \tau)\right| \\ &= \sum_{k=1}^{n} \left|\{0\} \cap (p^{n-k}D_0^{(p^k)} + \tau)\right| + \sum_{k=1}^{n} \Delta_{k,k}(\tau) \\ &+ \sum_{l=1}^{n-1} \sum_{k=l+1}^{n} \Delta_{l,k}(\tau) + \sum_{l=2}^{n} \sum_{k=1}^{l-1} \Delta_{l,k}(\tau). \end{aligned}$$

We take the case of $p = 1 \pmod 4$, first. If $\tau \in p^{n-u}D_0^{(p^u)}$, then by Lemma 1 and Lemma 2, we have

$$d_s(1,0;\tau) = 1 + (0,1)_{p^u} + \sum_{l=1}^{u-1} \Delta_{l,u}(\tau) + 0 = \frac{2 + p^u + p^{u-1}}{4},$$

for $u=1,\dots,n$. If $\tau\in p^{n-u}D_1^{(p^u)}$, we have

$$d_s(1,0;\tau)=\frac{-2+p^u+p^{u-1}}{4},\quad \text{for } u=1,\dots,n.$$

Now for the case of $p=3 \pmod 4$, we have in a similar way that

$$d_s(1,0;\tau)=\frac{p^u+p^{u-1}}{4},$$

if $\tau\in p^{n-u}Z_{p^u}^{\times}$ for $u=1,\dots,n$. Since $C_s(\tau)=p^n-4d_s(1,0;\tau)$, it completes the proof. ■

Now it remains to prove Lemma 1 and 2. To do that, we need the following two propositions:

Proposition 1 *For arbitrary integer b, and for any* $k=1,\dots,n$, *we have* $bp+D_i^{(p^k)}=D_i^{(p^k)} \pmod{p^k}$, *where* $i=0,1$.

Proposition 2 $-1 \pmod{p^k}\in D_0^{(p^k)}$ *if and only if* $p=1 \pmod 4$, *for* $k=1,\dots,n$.

proof: It is well known that $-1 \pmod p\in D_0^{(p)}$ if and only if $p=1 \pmod 4$. Using Proposition 1, we can show that $-1 \pmod p\in D_0^{(p)}$ implies $-1 \pmod{p^2}\in D_0^{(p^2)}$ and $-1 \pmod{p^3}\in D_g^{(p^3)}$, and so on. The converse is obvious. ■

Proof of Lemma 1 If $p=1 \pmod 4$, $\tau\in p^{n-k}D_i^{(p^k)}$ if and only if $-\tau\in p^{n-k}D_i^{(p^k)}$, by Proposition 2. Likewise, if $p=3 \pmod 4$, then $\tau\in p^{n-k}D_i^{(p^k)}$ if and only if $-\tau\in p^{n-k}D_{i+1 \pmod 2}^{(p^k)}$. It completes the proof. ■

Proof of Lemma 2
A. Let $l=k$.

1. If $\tau\in p^{n-k}D_0^{(p^k)}\cup p^{n-k}D_1^{(p^k)}$, we can put $\tau=p^{n-k}a$ for some $a\in Z_{p^k}^{\times}$. Then,

$$\begin{aligned}&\Delta_{k,k}(\tau)\\&=\left|p^{n-k}D_1^{(p^k)}\cap\left(p^{n-k}D_0^{(p^k)}+p^{n-k}a\right)\pmod{p^n}\right|\\&=\left|D_1^{(p^k)}\cap\left(D_0^{(p^k)}+a\right)\pmod{p^k}\right|\\&=\begin{cases}(0,1)_{p^k}, & \text{if }\tau\in p^{n-k}D_0^{(p^k)}\\(1,0)_{p^k}, & \text{if }\tau\in p^{n-k}D_1^{(p^k)}.\end{cases}\end{aligned}$$

2. For $\tau\in p^{n-u}D_0^{(p^u)}\cup p^{n-u}D_1^{(p^u)}$ such that $u\neq k$, put $\tau=p^{n-u}b$ for some $b\in Z_{p^u}^{\times}$. Then,
(1) If $u>k$, it implies $p^{n-u}<p^{n-k}$, so

$$\begin{aligned}&\Delta_{k,k}(\tau)\\&=\left|p^{n-k}D_1^{(p^k)}\cap\left(p^{n-k}D_0^{(p^k)}+p^{n-u}b\right)\pmod{p^n}\right|\\&=\left|p^{n-k}D_1^{(p^k)}\cap p^{n-u}\cdot\Lambda\pmod{p^n}\right|\\&=\left|p^{n-k}D_1^{(p^k)}\cap p^{n-u}\Lambda\right|=|\emptyset|=0,\end{aligned}$$

where $\Lambda:=p^{u-k}D_0^{(p^k)}+b \pmod{p^u}$ is a subset of $Z_{p^u}^{\times}$.
(2) If $u<k$, it implies $p^{n-u}>p^{n-k}$, so

$$\begin{aligned}&\Delta_{k,k}(\tau)\\&=\left|p^{n-k}D_1^{(p^k)}\cap\left(p^{n-k}D_0^{(p^k)}+p^{n-u}b\right)\pmod{p^n}\right|\\&=\left|p^{n-k}D_1^{(p^k)}\cap p^{n-k}\cdot\left(D_0^{(p^k)}+p^{k-u}b\right)\pmod{p^n}\right|\\&=\left|p^{n-k}D_1^{(p^k)}\cap p^{n-k}\cdot D_0^{(p^k)}\right|=|\emptyset|=0.\end{aligned}$$

B. Let $l<k$.

1. For $\tau\in p^{n-k}D_0^{(p^k)}\cup p^{n-k}D_1^{(p^k)}$, we put $\tau=p^{n-k}a$ for some $a\in Z_{p^k}^{\times}$. Then,

$$\begin{aligned}&\Delta_{l,k}(\tau)\\&=\left|p^{n-l}D_1^{(p^l)}\cap\left(p^{n-k}D_0^{(p^k)}+p^{n-k}a\right)\pmod{p^n}\right|\\&=\left|\left(p^{n-l}D_1^{(p^l)}-p^{n-k}a\right)\cap p^{n-k}D_0^{(p^k)}\pmod{p^n}\right|\\&=\left|\left(p^{k-l}D_1^{(p^l)}-a\right)\cap D_0^{(p^k)}\pmod{p^k}\right|.\end{aligned}$$

(1) $p=1 \pmod 4$: $a\in D_i^{(p^k)}$ if and only if $-a\in D_i^{(p^k)}$, by Proposition 2. If $a\in D_i^{(p^k)}$, for any element x of $p^{k-l}D_1^{p^l}-a \pmod{p^k}$, x becomes an element of $D_i^{(p^k)}$, by Proposition 1. Hence, $p^{k-l}D_1^{p^l}-a\subset D_i^{(p^k)}$. It follows that

$$\Delta_{l,k}(\tau)=\begin{cases}\left|p^{k-l}D_1^{(p^l)}-a\right|=\frac{p^l-p^{l-1}}{2}, & a\in D_0^{(p^k)}\\0, & a\in D_1^{(p^k)}.\end{cases}$$

(2) $p=3 \pmod 4$: if $a\in D_i^{(p^k)}$, any element x of $p^{k-l}D_1^{p^l}-a \pmod{p^k}$ becomes an element of $D_{i+1 \pmod 2}^{(p^k)}$. Hence, $p^{k-l}D_1^{p^l}-a\subset D_{i+1 \pmod 2}^{(p^k)}$. It follows that

$$\Delta_{l,k}(\tau)=\begin{cases}0, & a\in D_0^{(p^k)}\\\frac{p^l-p^{l-1}}{2}, & a\in D_1^{(p^k)}.\end{cases}$$

2. For $\tau\in p^{n-u}D_0^{(p^u)}\cup p^{n-u}D_1^{(p^u)}$ such that $u\neq k$, put $\tau=p^{n-u}b$ for some $b\in Z_{p^u}^{\times}$. Then,
(1) If $u>k$, note that $p^{n-k}D_0^{(p^k)}+\tau=p^{n-u}\left(p^{u-k}D_0^{(p^k)}+b\right)\subset p^{n-u}Z_{p^u}^{\times}$. Hence,

$$\Delta_{l,k}(\tau)=|\emptyset|=0.$$

(2) If $u<k$, note that $p^{n-k}D_0^{(p^k)}+\tau=p^{n-k}\left(D_0^{(p^k)}+p^{k-u}b\right)=p^{n-k}D_0^{(p^k)}$. Hence,

$$\Delta_{l,k}(\tau)=\left|p^{n-l}D_1^{(p^l)}\cap p^{n-k}D_0^{(p^k)}\right|=|\emptyset|=0.$$

C. Let $l > k$. The case of $l > k$ can be done in a similar way to the case of $l < k$. ■

References

[1] J.-H. Kim and H.-Y. Song, "Trace representation of Legendre sequences," Designs, Codes and Cryptography, vol.24, no.3, pp.343–348, 2001.
[2] T. Yan, R. Sun, and G. Xiao, "Autocorrelation and linear complexity of the new generalized cyclotomic sequences," IEICE Trans. Fundamentals, vol.E90-A, no.4, pp.857–864, April 2007.
[3] E. Bai, X. Liu, and G. Xiao, "Linear complexity of new generalized cyclotomic sequences of order two of length pq," IEEE Trans. Inf. Theory, vol.51, no.5, pp.1849–1853, 2005.
[4] C. Ding and T. Helleseth, "New generalized cyclotomy and its applications," Finit Fields and Their Applications, vol.4, pp.140–166, 1998.
[5] S.W. Golomb and G. Gong, Sequence Design for Good Correlation, Cambridge University Press, 2005.
[6] Y.-J. Kim, S.-Y. Jin, and H.-Y. Song, "Linear complexity and autocorrelation of prime cube sequences," Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, ed. S. Boztas and H.F.F. Lu, LNCS 4851, pp.188–197, Springer, 2007.
[7] T. Yan, S. Li, and G. Xiao, "On the linear complexity of generalized cyclotomic sequences with the period p^m," Applied Mathematics Letters, vol.21, pp.187–193, 2008.
[8] Y.-J. Kim and H.-Y. Song, "Linear complexity of prime n-square sequences," Proc. ISIT 2008, pp.2405–2408, Toronto, July 2008.
[9] Y.-J. Kim, Linear Complexity and Correlation of Some Cyclotomic Sequences, PhD Thesis, Yonsei University, 2009.
[10] T. Cusick, C. Ding, and A. Renvall, Stream Ciphers and Number Theory, North-Holland, 1998.