PAPER Special Section on Signal Design and its Application in Communications

# Autocorrelation of Some Quaternary Cyclotomic Sequences of Length $2p$*

**Young-Joon KIM**†a), **Yun-Pyo HONG**†, *Members, and* **Hong-Yeop SONG**†, *Nonmember*

**SUMMARY** We define a new quaternary cyclotomic sequences of length $2p$, where $p$ is an odd prime. We compute the autocorrelation of these sequences. In terms of magnitude, these sequences have the autocorrelations with at most 4 values.

***key words:*** *autocorrelation, quaternary cyclotomic sequences*

## 1. Quaternary Cyclotomic Sequences of Length $2p$

Let $p$ be an odd prime and $g$ a primitive root of $p$. Since either $g$ or $g+p$ is odd modulo $2p$ and both of them are primitive roots of $p$, simply we will assume that $g$ is an odd integer. Then it is well known that $g$ is also a primitive root of $2p$ [3]. Define

$$D_0^{(p)} = (g^2), \qquad D_1^{(p)} = gD_0^{(p)},$$
$$D_0^{(2p)} = (g^2), \qquad D_1^{(2p)} = gD_0^{(2p)}$$

where $(g^2)$ denotes the subgroup of $Z_p$ and $Z_{2p}$ generated by $g^2$, respectively. Then

$$\mathbf{Z}_{2p} = \{0, p\} \cup 2 \cdot D_0^{(p)} \cup 2 \cdot D_1^{(p)} \cup D_0^{(2p)} \cup D_1^{(2p)}.$$

Define a quaternary sequence $\{s(n)\}$ of length $2p$ as follows:

$$s(n) = \begin{cases} 0, & \text{if } n = 0 \pmod{2p} \\ 2, & \text{if } n = p \pmod{2p} \\ 0, & \text{if } n \in D_0^{(2p)} \\ 1, & \text{if } n \in D_1^{(2p)} \\ 2, & \text{if } n \in 2 \cdot D_0^{(p)} \\ 3, & \text{if } n \in 2 \cdot D_1^{(p)}. \end{cases} \tag{1}$$

Hereafter, we will call this sequence as a *quaternary cyclotomic sequence of length* $2p$.

**Example 1:** An example of a quaternary cyclotomic sequence of length 10 (when $p=5$, $g=3$) is shown below:

$$2 \cdot D_0^{(5)} = 2 \cdot \{3^2, 3^4\} = 2 \cdot \{1, 4\} = \{2, 8\},$$
$$2 \cdot D_1^{(5)} = 2 \cdot \{3^1, 3^3\} = 2 \cdot \{2, 3\} = \{4, 6\},$$
$$D_0^{(10)} = \{3^2, 3^4\} = \{1, 9\},$$
$$D_1^{(10)} = \{3^1, 3^3\} = \{3, 7\}.$$

Therefore, a quaternary cyclotomic sequence $\{s(n)\}$ of length 10 are given as follows:

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $s(n)$ | 0 | 0 | 2 | 1 | 3 | 2 | 3 | 1 | 2 | 0 |

## 2. Autocorrelation of Quaternary Cyclotomic Sequences of Length $2p$

The periodic autocorrelation of a quaternary sequence $\{u(n)\}$ of period $N$ is defined by

$$C_u(\tau) = \sum_{n=0}^{N-1} w^{u(n+\tau)-u(n)}$$

where $w = \exp(j\frac{2\pi}{4})$ is a complex primitive quadratic root of unity. Since the quaternary cyclotomic sequence of length $2p$ is defined in the similar way with the binary cyclotomic sequence of length $p$, it's desirable to review how to construct the binary cyclotomic sequence of length $p$ and their properties.

**Definition 1:** Let $p$ be an odd prime, then the sequence $\{t(n)\}$ of length $p$ defined as

$$t(n) = \begin{cases} 0, & \text{if } n \in C_0^{(p)} \triangleq D_0^{(p)} \\ 1, & \text{if } n \in C_1^{(p)} \triangleq \{0\} \cup D_1^{(p)}. \end{cases} \tag{2}$$

is called the binary cyclotomic sequence of length $p$, which is well known as the binary quardratic residue sequence or Legendre sequence of length $p$.

Define

$$d_t(i, j; \tau) = |C_i^{(p)} \cap (C_j^{(p)} + \tau)|, \quad \tau \in Z_p, \ i, j = 0, 1.$$

For the notational simplicity, we introduce the cyclotomic numbers of order 2 with respect to $p$ defined by

$$(i, j)_p = |(D_i^{(p)} + 1) \cap D_j^{(p)}|.$$

**Lemma 1:** [4] If $p \equiv 1 \pmod 4$, then

$$(0,1)_p = (1,0)_p = (1,1)_p = \frac{p-1}{4}, (0,0)_p = \frac{p-5}{4}. \tag{3}$$

If $p \equiv 3 \pmod 4$, then

$$(1,0)_p = (0,0)_p = (1,1)_p = \frac{p-3}{4}, (0,1)_p = \frac{p+1}{4}. \tag{4}$$

Manuscript received January 8, 2008.
Manuscript revised June 2, 2008.

†The authors are with School of Electrical and Electronic Engineering, Yonsei University, Seoul, Korea.

*This work was supported by the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MEST) (No. R01-2008-000-20578-0).

a) E-mail: yj.kim@yonsei.ac.kr

DOI: 10.1093/ietfec/e91–a.12.3679

**Lemma 2:** For $a \in Z_p^*$,

$$aD_0^{(p)}=\begin{cases} D_0^{(p)}, & \text{if } a \in D_0^{(p)} \\ D_1^{(p)}, & \text{if } a \in D_1^{(p)} \end{cases}, aD_1^{(p)}=\begin{cases} D_1^{(p)}, & \text{if } a \in D_0^{(p)} \\ D_0^{(p)}, & \text{if } a \in D_1^{(p)} \end{cases}.$$

For $b \in Z_{2p}^*$,

$$bD_0^{(2p)}=\begin{cases} D_0^{(2p)}, \text{if } b \in D_0^{(2p)} \\ D_1^{(2p)}, \text{if } b \in D_1^{(2p)} \end{cases}, bD_1^{(2p)} = \begin{cases} D_1^{(2p)}, \text{if } b \in D_0^{(2p)} \\ D_0^{(2p)}, \text{if } b \in D_1^{(2p)} \end{cases}.$$

**Proof:** First part of this lemma is pointed out in [5] and second part can be proved in the same way as [5]. ■

**Lemma 3:** [3] $2 \in D_0^{(p)}$ if $p \equiv \pm 1 \pmod 8$, and $2 \in D_1^{(p)}$ if $p \equiv \pm 3 \pmod 8$.

**Lemma 4:** [3] $-1 \pmod p \in D_0^{(p)}$ if $p \equiv 1 \pmod 4$, and $-1 \pmod p \in D_1^{(p)}$ if $p \equiv 3 \pmod 4$.

**Lemma 5:** $-1 \pmod p \in D_0^{(p)}$ if and only if $-1 \pmod{2p} \in D_0^{(2p)}$.

**Proof:** Obvious. ■

**Lemma 6:** When $p \equiv 1 \pmod 4$, then we have

$$d_t(1,0;\tau) = \begin{cases} \frac{p+3}{4}, & \text{if } \tau \in D_0^{(p)} \\ \frac{p-1}{4}, & \text{if } \tau \in D_1^{(p)}. \end{cases}$$

When $p \equiv 3 \pmod 4$, then we have

$$d_t(1,0;\tau) = \frac{p+1}{4}, \text{ if } \tau \in D_0^{(p)} \cup D_1^{(p)}.$$

**Proof:** It can be easily proved from Lemma 1. ■

For a given quaternary cyclotomic sequence of length $2p$, define $s^{(1)}(n) = s(2n)$, $0 \le n \le p-1$, and $s^{(2)}(n) = s(2n+1)$, $0 \le n \le p-1$. That is, they are defined as follows, respectively:

$$s^{(1)}(n) = \begin{cases} 0, & \text{if } n \equiv 0 \pmod p \\ 2, & \text{if } 2n \in 2D_0^{(p)} \iff n \in D_0^{(p)} \\ 3, & \text{if } 2n \in 2D_1^{(p)} \iff n \in D_1^{(p)}, \end{cases}$$

$$s^{(2)}(n) = \begin{cases} 2, & \text{if } 2n+1 \equiv p \pmod{2p} \\ 0, & \text{if } 2n+1 \in D_0^{(2p)} \\ 1, & \text{if } 2n+1 \in D_1^{(2p)}. \end{cases}$$

**Lemma 7:** Let $p$ be an odd prime. Then the autocorrelation of the quaternary cyclotomic sequence $\{s(n)\}$ of length $2p$ can be expressed as follows:

$$\begin{aligned} C_s(\tau) &= \sum_{i=0}^{2p-1} w^{s(i+\tau)-s(i)} \\ &= \begin{cases} C_{s^{(1)}}(k) + C_{s^{(2)}}(k), \\ \quad \text{if } \tau \equiv 2k \pmod{2p} \text{ and } 1 \le k \le p-1 \\ \\ C_{s^{(1)}s^{(2)}}(k) + C_{s^{(2)}s^{(1)}}(k-1), \\ \quad \text{if } \tau \equiv 2k-1 \pmod{2p} \text{ and } 1 \le k \le p \end{cases} \end{aligned}$$

where $w = \exp(j\frac{2\pi}{4}) = j$ is a complex primitive quadratic root of unity and $C_{s^{(i)}s^{(j)}}(t) = \sum_{z=0}^{p-1} w^{s^{(i)}(z+t)-s^{(j)}(z)}$ is a cross-correlation of $s^{(i)}$ and $s^{(j)}$ for $(i,j) \in \{(0,1),(1,0)\}$.

**Proof:** Obvious. ■

Without loss of generality, we can let $s^{(1)}(n) = t(n) + 2$, $1 \le n \le p-1$. Since $s^{(1)}(n)$ is a quaternary sequence, all the plus and minus operation should be done in modulo 4 throughout this paper even if $\{t(n)\}$ seems like a binary sequence.

**Lemma 8:** The autocorrelation of a quaternary sequence $\{s^{(1)}(n)\}$ of length $p$ is as follows:

1. When $p \equiv 1 \pmod 4$,

$$C_{s^{(1)}}(k) = \begin{cases} \frac{p-7}{2}, & \text{if } k \in D_0^{(p)} \\ \frac{p-3}{2}, & \text{if } k \in D_1^{(p)}. \end{cases} \tag{5}$$

2. When $p \equiv 3 \pmod 4$,

$$C_{s^{(1)}}(k) = \begin{cases} \frac{p-5}{2} + 2j, & \text{if } k \in D_0^{(p)} \\ \frac{p-5}{2} - 2j, & \text{if } k \in D_1^{(p)}. \end{cases} \tag{6}$$

**Proof:** The autocorrelation of $\{s^{(1)}(n)\}$ can be expressed as follows:

$$\begin{aligned} C_{s^{(1)}}(k) &= \sum_{i=0}^{p-1} j^{s^{(1)}(i+k)-s^{(1)}(i)} \\ &= j^{s^{(1)}(k)} + j^{-s^{(1)}(-k)} + \sum_{\substack{i \in Z_p \\ i \ne 0,-k}} j^{s^{(1)}(i+k)-s^{(1)}(i)} \end{aligned}$$

(Here, the computation in the power of $j$ is done in modulo 4)

$$\begin{aligned} &= j^{t(k)+2} + j^{-t(-k)-2} - j^{t(k)-t(0)} - j^{t(0)-t(-k)} \\ &\quad + \sum_{i \in Z_p} j^{t(i+k)-t(i)} \end{aligned} \tag{7}$$

If $t(i+k) = 1$ and $t(i) = 0$, then $i+k \in C_1^{(p)}$ and $i \in C_0^{(p)}$. It gives us $i \in C_1^{(p)} - k$ and $i \in C_0^{(p)}$. Hence, there are such $i$'s as many as $|\{i | i \in (C_1^{(p)} - k) \cap C_0^{(p)}\}| = |C_1^{(p)} \cap (C_0^{(p)} + k)| = d_t(1,0;k)$. Likewise, there are $d_t(0,0;k)$, $d_t(0,1;k)$ and $d_t(1,1;k)$ number of pairs $(t(i+k), t(i)) = (0,0), (0,1)$ and $(1,1)$, respectively. Therefore Eq. (7) becomes as follows:

$$\begin{aligned} C_{s^{(1)}}(k) &= j^{t(k)+2} + j^{-t(-k)-2} - j^{t(k)-1} - j^{1-t(-k)} \\ &\quad + d_t(0,0;k)j^0 + d_t(0,1;k)j^{-1} + d_t(1,0;k)j^1 + d_t(1,1;k)j^0. \end{aligned}$$

Since $d_t(0,0;k) + d_t(0,1;k) + d_t(1,0;k) + d_t(1,1;k) = p$ and $d_t(0,1;k) = d_t(1,0;k)$, it becomes

$$C_{s^{(1)}}(k) = j^{t(k)+2} + j^{-t(-k)-2} - j^{t(k)-1} - j^{1-t(-k)} + p - 2d_t(1,0;k).$$

When $p \equiv 1 \pmod 4$, $k \in D_i^{(p)}$ if and only if $-k \in D_i^{(p)}$, $i = 0, 1$. So $k \in D_i^{(p)}$ implies $t(-k) = t(k) = i$, for $i = 0, 1$. Similarly, when $p \equiv 3 \pmod 4$, $k \in D_i^{(p)}$ if and only if

$-k \in D^{(p)}_{i+1\ mod\ 2}$, $i = 0, 1$. So $k \in D^{(p)}_i$ implies $t(k) = i$ and $t(-k) = i + 1 \pmod 2$, for $i = 0, 1$. By Lemma 4 and 6, we complete the proof. ■

The autocorrelation of $\{s^{(2)}(n)\}$ can be calculated in the similar way. For simplicity, we introduce the following $\{0, 1\}$−sequence of length $p$.

$$v(n) = \begin{cases} 0, & \text{if } 2n + 1 \in C^{(2p)}_0 \triangleq D^{(2p)}_0 \\ 1, & \text{if } 2n + 1 \in C^{(2p)}_1 \triangleq \{p\} \cup D^{(2p)}_1. \end{cases} \tag{8}$$

Although $\{v(n)\}$ is $\{0, 1\}$−sequence, the symbol 0 or 1 is not over $Z_2$ but over $Z_4$. Define

$$d_v(i, j; \tau) = |C^{(2p)}_i \cap (C^{(2p)}_j + 2\tau)|, \quad \tau \in Z_p,\ i, j = 0, 1.$$

where all the operations are computed in the modulo $2p$.

**Lemma 9:** The autocorrelation of a quaternary sequence $\{s^{(2)}(n)\}$ of length $p$ is as follows:

1. When $p \equiv 1 \pmod 8$,
$$C_{s^{(2)}}(k) = \begin{cases} \frac{p-7}{2}, & \text{if } k \in D^{(p)}_0 \\ \frac{p-3}{2}, & \text{if } k \in D^{(p)}_1. \end{cases} \tag{9}$$
2. When $p \equiv 3 \pmod 8$,
$$C_{s^{(2)}}(k) = \begin{cases} \frac{p-5}{2} - 2j, & \text{if } k \in D^{(p)}_0 \\ \frac{p-5}{2} + 2j, & \text{if } k \in D^{(p)}_1. \end{cases} \tag{10}$$
3. When $p \equiv 5 \pmod 8$,
$$C_{s^{(2)}}(k) = \begin{cases} \frac{p-3}{2}, & \text{if } k \in D^{(p)}_0 \\ \frac{p-7}{2}, & \text{if } k \in D^{(p)}_1. \end{cases} \tag{11}$$
4. When $p \equiv 7 \pmod 8$,
$$C_{s^{(2)}}(k) = \begin{cases} \frac{p-5}{2} + 2j, & \text{if } k \in D^{(p)}_0 \\ \frac{p-5}{2} - 2j, & \text{if } k \in D^{(p)}_1. \end{cases} \tag{12}$$

**Proof:** Without loss of generality, we can let $s^{(2)}(n) = v(n)$, $0 \le n \le p - 1$, $n \ne \frac{p-1}{2}$. Then, by similar procedure with the case of $\{s^{(1)}(n)\}$, the autocorrelation of $\{s^{(2)}(n)\}$ can be expressed as follows:

$$\begin{aligned} C_{s^{(2)}}(k) = {} & j^{v(\frac{p-1}{2}+k)-2} + j^{2-v(\frac{p-1}{2}-k)} - j^{v(\frac{p-1}{2}+k)-1} \\ & - j^{1-v(\frac{p-1}{2}-k)} + p - 2d_v(1, 0; k). \end{aligned}$$

Note that

$$\begin{aligned} d_v(1, 0; k) &= |C^{(2p)}_1 \cap (C^{(2p)}_0 + 2k)| \\ &= |\{p\} \cap (D^{(2p)}_0 + 2k)| + |D^{(2p)}_1 \cap (D^{(2p)}_0 + 2k)| \end{aligned}$$

Since $|\{p\} \cap (D^{(2p)}_0 + 2k)| = |\{0\} \cap (D^{(p)}_0 + 2k) \pmod p|$, by Lemmas 3 and 4,

1. When $p \equiv 1, 3 \pmod 8$, we have
$$|\{p\} \cap (D^{(2p)}_0 + 2k)| = \begin{cases} 1, & \text{if } k \in D^{(p)}_0 \\ 0, & \text{if } k \in D^{(p)}_1. \end{cases}$$
2. When $p \equiv 5, 7 \pmod 8$, we have
$$|\{p\} \cap (D^{(2p)}_0 + 2k)| = \begin{cases} 0, & \text{if } k \in D^{(p)}_0 \\ 1, & \text{if } k \in D^{(p)}_1. \end{cases}$$

Since $|D^{(2p)}_1 \cap (D^{(2p)}_0 + 2k)| = |D^{(p)}_1 \cap (D^{(p)}_0 + 2k) \pmod p| = |2^{-1}k^{-1}D^{(p)}_1 \cap (2^{-1}k^{-1}D^{(p)}_0 + 1)|$ and by Lemmas 2, 3 and 4,

1. When $p \equiv \pm 1 \pmod 8$, we have
$$|D^{(2p)}_1 \cap (D^{(2p)}_0 + 2k)| = \begin{cases} (0, 1)_p, & \text{if } k \in D^{(p)}_0 \\ (1, 0)_p, & \text{if } k \in D^{(p)}_1. \end{cases}$$
2. When $p \equiv \pm 3 \pmod 8$, we have
$$|D^{(2p)}_1 \cap (D^{(2p)}_0 + 2k)| = \begin{cases} (1, 0)_p, & \text{if } k \in D^{(p)}_0 \\ (0, 1)_p, & \text{if } k \in D^{(p)}_1. \end{cases}$$

Note that $2(\frac{p-1}{2} + k) + 1 = p + 2k \in D^{(2p)}_i$ means $2k \in D^{(p)}_i$ and $2(\frac{p-1}{2} - k) + 1 = p - 2k \in D^{(2p)}_i$ means $-2k \in D^{(p)}_i$ for $i = 0, 1$ and the converse is also true. Therefore, we have

1. When $p \equiv 1 \pmod 8$, $k \in D^{(p)}_i$ if and only if $2k \in D^{(p)}_i$ if and only if $-2k \in D^{(p)}_i$, $i = 0, 1$. So $k \in D^{(p)}_i$ implies $v(\frac{p-1}{2} + k) = v(\frac{p-1}{2} - k) = i$ for $i = 0, 1$.
2. When $p \equiv 3 \pmod 8$, $k \in D^{(p)}_i$ if and only if $2k \in D^{(p)}_{i+1}$ if and only if $-2k \in D^{(p)}_i$, $i = 0, 1$ So $k \in D^{(p)}_i$ implies $v(\frac{p-1}{2} + k) = i + 1 \pmod 2$ and $v(\frac{p-1}{2} - k) = i$ for $i = 0, 1$.
3. When $p \equiv 5 \pmod 8$, $k \in D^{(p)}_i$ if and only if $2k \in D^{(p)}_{i+1}$ if and only if $-2k \in D^{(p)}_{i+1}$, $i = 0, 1$ So $k \in D^{(p)}_i$ implies $v(\frac{p-1}{2} + k) = v(\frac{p-1}{2} - k) = i + 1 \pmod 2$ for $i = 0, 1$.
4. When $p \equiv 7 \pmod 8$, $k \in D^{(p)}_i$ if and only if $2k \in D^{(p)}_i$ if and only if $-2k \in D^{(p)}_{i+1}$, $i = 0, 1$ So $k \in D^{(p)}_i$ implies $v(\frac{p-1}{2} + k) = i$ and $v(\frac{p-1}{2} - k) = i + 1 \pmod 2$ for $i = 0, 1$.

Combining all of these computation, we can get to the (9),(10),(11) and (12). ■

Next, we are going to consider the autocorrelation of $\{s(n)\}$ when the time shift $\tau$ is odd. As is mentioned in Lemma 7, when $\tau = 2k - 1, 1 \le k \le p$, $C_s(\tau) = C_{s^{(1)}s^{(2)}}(k) + C_{s^{(2)}s^{(1)}}(k - 1)$. Define

$$d_{t,v}(i, j; k) = |2C^{(p)}_i \cap (C^{(2p)}_j + 2k - 1)|, \quad k \in Z^*_p,\ i, j = 0, 1,$$

and

$$d_{v,t}(i, j; k) = |C^{(2p)}_i \cap (2C^{(p)}_j + 2k - 1)|, \quad k \in Z^*_p,\ i, j = 0, 1,$$

where all the operations are computed in the modulo $2p$.

**Lemma 10:** The crosscorrelation of two quaternary sequences $\{s^{(1)}(n)\}$ and $\{s^{(2)}(n)\}$ of length $p$ is as follows:

1. When $p \equiv 1 \pmod 8$,

$$C_{s^{(1)}s^{(2)}}(k)=\begin{cases}-p, & \text{if } \tau=2k-1=p \pmod{2p}\\ \frac{-p+7}{2}, & \text{if } \tau = 2k-1 \in D_0^{(2p)}\\ \frac{-p+3}{2}, & \text{if } \tau = 2k-1 \in D_1^{(2p)}.\end{cases} \tag{13}$$

2. When $p \equiv 3 \pmod 8$,

$$C_{s^{(1)}s^{(2)}}(k)=\begin{cases}-1, & \text{if } \tau=2k-1=p \pmod{2p}\\ \frac{-p+1}{2}, & \text{if } \tau = 2k-1 \in D_0^{(2p)}\\ \frac{-p+5}{2}, & \text{if } \tau = 2k-1 \in D_1^{(2p)}.\end{cases} \tag{14}$$

3. When $p \equiv 5 \pmod 8$,

$$C_{s^{(1)}s^{(2)}}(k)=\begin{cases}-1, & \text{if } \tau=2k-1=p \pmod{2p}\\ \frac{-p+3}{2}+2j, & \text{if } \tau=2k-1\in D_0^{(2p)}\\ \frac{-p+3}{2}-2j, & \text{if } \tau=2k-1\in D_1^{(2p)}.\end{cases} \tag{15}$$

4. When $p \equiv 7 \pmod 8$,

$$C_{s^{(1)}s^{(2)}}(k)=\begin{cases}-p, & \text{if } \tau= 2k-1=p \pmod{2p}\\ \frac{-p+5}{2}-2j, & \text{if } \tau=2k-1\in D_0^{(2p)}\\ \frac{-p+5}{2}+2j, & \text{if } \tau=2k-1\in D_1^{(2p)}.\end{cases} \tag{16}$$

**Proof:** To begin with, we are going to consider $C_{s^{(1)}s^{(2)}}(k)$. When $2k-1 = p \pmod{2p}$,

$$\begin{aligned}C_{s^{(1)}s^{(2)}}\left(\frac{p+1}{2}\right) &= \sum_{i=0}^{p-1} j^{s^{(1)}(i+\frac{p+1}{2})-s^{(2)}(i)}\\ &= j^{s^{(1)}(0)-s^{(2)}(\frac{p-1}{2})} - j^{t(0)+2-v(\frac{p-1}{2})}\\ &\quad + \sum_{i\in Z_p} j^{t(i+k)+2-v(i)} = \sum_{i\in Z_p} j^{t(i+k)+2-v(i)}\end{aligned}$$

When $\tau = 2k-1 \in D_0^{(2p)} \cup D_1^{(2p)}$,

$$\begin{aligned}C_{s^{(1)}s^{(2)}}(k) &= \sum_{i=0}^{p-1} j^{s^{(1)}(i+k)-s^{(2)}(i)}\\ &= j^{-v(-k)}+j^{t(\frac{p-1}{2}+k)}-j^{3-v(-k)}-j^{t(\frac{p-1}{2}+k)+1}\\ &\quad+\sum_{i\in Z_p} j^{t(i+k)+2-v(i)}\end{aligned}$$

By similar procedure with the case of autocorrelation of $\{s^{(1)}(n)\}$ and $\{s^{(2)}(n)\}$, it becomes

$$\begin{aligned}C_{s^{(1)}s^{(2)}}(k) = j^{-v(-k)}+j^{t(\frac{p-1}{2}+k)}-j^{3-v(-k)}-j^{t(\frac{p-1}{2}+k)+1}\\ -p+2d_{t,v}(1,0;k).\end{aligned} \tag{17}$$

Note that

$$\begin{aligned}d_{t,v}(1,0;k)=&|2C_1^{(p)} \cap (C_0^{(2p)} + 2k-1)|\\ =&|\{0\}\cap(D_0^{(2p)}+2k-1)|+|2D_1^{(p)}\cap(D_0^{(2p)}+2k-1)|\end{aligned}$$

If $p \equiv 1 \pmod 4$, by Lemmas 4 and 5, $a \in D_i^{(2p)}$ if and only if $-a \in D_i^{(2p)}$. On the other hand, if $p \equiv 3 \pmod 4$, then $a \in D_i^{(2p)}$ if and only if $-a \in D_{i+1 \; mod\, 2}^{(2p)}$. Therefore,

1. When $p \equiv 1 \pmod 4$

$$|\{0\}\cap(D_0^{(2p)}+2k-1)|=\begin{cases}0, & \text{if } 2k-1 \equiv p \pmod{2p}\\ 1, & \text{if } 2k-1 \in D_0^{(2p)}\\ 0, & \text{if } 2k-1 \in D_1^{(2p)}.\end{cases}$$

2. When $p \equiv 3 \pmod 4$

$$|\{0\}\cap(D_0^{(2p)}+2k-1)|=\begin{cases}0, & \text{if } 2k-1 \equiv p \pmod{2p}\\ 0, & \text{if } 2k-1 \in D_0^{(2p)}\\ 1, & \text{if } 2k-1 \in D_1^{(2p)}.\end{cases}$$

Since $|2D_1^{(p)} \cap (D_0^{(2p)}+2k-1)| = |2D_1^{(p)} \cap (D_0^{(2p)}+\tau)(\text{mod } p)| = |2\tau^{-1}D_1^{(p)}\cap(\tau^{-1}D_0^{(p)}+1)|$ and by Lemmas 2, 3 and 4,

1. When $p \equiv \pm 1 \pmod 8$, we have

$$|2D_1^{(p)}\cap(D_0^{(2p)}+2k-1)|=\begin{cases}0, & \text{if } \tau=2k-1= p\\ (0,1)_p, & \text{if } \tau=2k-1\in D_0^{(2p)}\\ (1,0)_p, & \text{if } \tau=2k-1\in D_1^{(2p)}.\end{cases}$$

2. When $p \equiv \pm 3 \pmod 8$, we have

$$|2D_1^{(p)}\cap(D_0^{(2p)}+2k-1)|=\begin{cases}\frac{p-1}{2}, & \text{if } \tau=2k-1= p\\ (0,0)_p, & \text{if } \tau=2k-1 \in D_0^{(2p)}\\ (1,1)_p, & \text{if } \tau=2k-1 \in D_1^{(2p)}.\end{cases}$$

Now, we are ready to compute (17). When $p \equiv 1 \pmod 4$, $2(-k)+1 = -\tau \in D_i^{(2p)}$ if and only if $\tau \in D_i^{(2p)}$. So, in this case, $v(-k) = i$ if $\tau \in D_i^{(2p)}$ for $i = 0, 1$. On the other hand, when $p \equiv 3 \pmod 4$, $2(-k)+1 = -\tau \in D_i^{(2p)}$ if and only if $\tau \in D_{i+1 \; mod\, 2}^{(2p)}$. So, in this case, $v(-k) = i+1 \pmod 2$ if $\tau \in D_i^{(2p)}$ for $i = 0, 1$.

When $p \equiv \pm 1 (\text{mod } 8)$, if $\tau \in D_i^{(2p)}$, then $p + \tau(\text{mod } 2p)$ is an element of either $2D_i^{(p)}(\text{mod } 2p)$ or $2D_{i+1 \; mod\, 2}^{(p)}(\text{mod } 2p)$. Since it is valid when we apply modulo $p$ reduction, $\tau(\text{mod } p)$ is an element of either $2D_i^{(p)} = D_i^{(p)}(\text{mod } p)$ or $2D_{i+1 \; mod\, 2}^{(p)} = D_{i+1 \; mod\, 2}^{(p)}(\text{mod } p)$. Because $\tau \in D_i^{(2p)}$ implies $\tau \in D_i^{(p)}(\text{mod } p)$, $p+\tau(\text{mod } 2p) = 2(\frac{p-1}{2}+k) \in 2D_i^{(p)}(\text{mod } 2p)$. Therefore, $t(\frac{p-1}{2}+k) = i$. On the other hand, if $p \equiv \pm 3 (\text{mod } 8)$, $t(\frac{p-1}{2}+k) = i+1 (\text{mod } 2)$ when $\tau \in D_i^{(2p)}$.

Combining all of these computation, we can get to the (13),(14),(15) and (16). ■

**Lemma 11:** The crosscorrelation of two quaternary sequences $\{s^{(2)}(n)\}$ and $\{s^{(1)}(n)\}$ of length $p$ is as follows:

1. When $p \equiv 1 \pmod 8$,

$$C_{s^{(2)}s^{(1)}}(k-1)=\begin{cases}-p, & \text{if } \tau=2k-1=p \pmod{2p}\\ \frac{-p+7}{2}, & \text{if } \tau=2k-1\in D_0^{(2p)}\\ \frac{-p+3}{2}, & \text{if } \tau=2k-1\in D_1^{(2p)}.\end{cases} \tag{18}$$

2. When $p \equiv 3 \pmod 8$,

$$C_{s^{(2)}s^{(1)}}(k-1)=\begin{cases} -1, & \text{if } \tau = p \pmod{2p} \\ \frac{-p+5}{2}, & \text{if } \tau \in D_0^{(2p)} \\ \frac{-p+1}{2}, & \text{if } \tau \in D_1^{(2p)}. \end{cases} \tag{19}$$

3. When $p \equiv 5 \pmod 8$,

$$C_{s^{(2)}s^{(1)}}(k-1)=\begin{cases} -1, & \text{if } \tau = p \pmod{2p} \\ \frac{-p+3}{2} - 2j, & \text{if } \tau \in D_0^{(2p)} \\ \frac{-p+3}{2} + 2j, & \text{if } \tau \in D_1^{(2p)}. \end{cases} \tag{20}$$

4. When $p \equiv 7 \pmod 8$,

$$C_{s^{(2)}s^{(1)}}(k-1)=\begin{cases} -p, & \text{if } \tau = p \pmod{2p} \\ \frac{-p+5}{2} - 2j, & \text{if } \tau \in D_0^{(2p)} \\ \frac{-p+5}{2} + 2j, & \text{if } \tau \in D_1^{(2p)}. \end{cases} \tag{21}$$

**Proof:** When $2k-1 = p \pmod{2p}$,

$$\begin{aligned} C_{s^{(2)}s^{(1)}}\left(\frac{p+1}{2}-1\right) &= \sum_{i=0}^{p-1} j^{s^{(2)}(i+\frac{p-1}{2})-s^{(1)}(i)} \\ &= j^{s^{(2)}(\frac{p-1}{2})-s^{(1)}(0)} - j^{v(\frac{p-1}{2})-t(0)-2} \\ &\quad + \sum_{i\in Z_p} j^{v(i+k-1)-t(i)-2} = \sum_{i\in Z_p} j^{v(i+k-1)-t(i)-2}. \end{aligned}$$

When $\tau = 2k-1 \in D_0^{(2p)} \cup D_1^{(2p)}$, by similar procedure with $C_{s^{(1)}s^{(2)}}(k)$, the crosscorrelation $C_{s^{(2)}s^{(1)}}(k-1)$ becomes

$$\begin{aligned} C_{s^{(2)}s^{(1)}}(k-1) &= j^{v(k-1)} + j^{-t(\frac{p-1}{2}-k+1)} - j^{v(k-1)-3} \\ &\quad - j^{-1-t(\frac{p-1}{2}-k+1)} - p + 2d_{v,t}(1,0;k). \end{aligned} \tag{22}$$

Note that

$$\begin{aligned} d_{v,t}(1,0;k) &= |C_1^{(2p)} \cap (2C_0^{(p)} + 2k-1)| \\ &= |\{p\} \cap (2D_0^{(p)} + 2k-1)| + |D_1^{(2p)} \cap (2D_0^{(p)} + 2k-1)| \end{aligned}$$

If $p \equiv 1 \pmod 4$, by Lemmas 4 and 5, $a \in D_i^{(2p)}$ if and only if $-a \in D_i^{(2p)}$. On the other hand, if $p \equiv 3 \pmod 4$, then $a \in D_i^{(2p)}$ if and only if $-a \in D_{i+1\ mod\ 2}^{(2p)}$. Therefore, we have

1. When $p \equiv 1, 3 \pmod 8$,

$$|\{p\} \cap (2D_0^{(p)} + 2k-1)| = \begin{cases} 0, & \text{if } 2k-1 \equiv p \pmod{2p} \\ 1, & \text{if } 2k-1 \in D_0^{(2p)} \\ 0, & \text{if } 2k-1 \in D_1^{(2p)} \end{cases},$$

2. When $p \equiv 5, 7 \pmod 8$,

$$|\{p\} \cap (2D_0^{(p)} + 2k-1)| = \begin{cases} 0, & \text{if } 2k-1 \equiv p \pmod{2p} \\ 0, & \text{if } 2k-1 \in D_0^{(2p)} \\ 1, & \text{if } 2k-1 \in D_1^{(2p)} \end{cases}.$$

Since $|D_1^{(2p)} \cap (2D_0^{(p)} + 2k-1)| = |D_1^{(2p)} \cap (2D_0^{(p)} + \tau) \pmod p)| = |\tau^{-1}D_1^{(p)} \cap (2\tau^{-1}D_0^{(p)} + 1)|$ and by Lemmas 2 and 3, we have

1. When $p \equiv \pm 1 \pmod 8$,

$$\begin{aligned} &|D_1^{(2p)} \cap (2D_0^{(p)} + 2k-1)| \\ &= \begin{cases} 0, & \text{if } \tau = 2k-1 = p \pmod{2p} \\ (0,1)_p, & \text{if } \tau = 2k-1 \in D_0^{(2p)} \\ (1,0)_p, & \text{if } \tau = 2k-1 \in D_1^{(2p)} \end{cases}, \end{aligned}$$

2. When $p \equiv \pm 3 \pmod 8$,

$$\begin{aligned} &|D_1^{(2p)} \cap (2D_0^{(p)} + 2k-1)| \\ &= \begin{cases} \frac{p-1}{2}, & \text{if } \tau = 2k-1 = p \pmod{2p} \\ (1,1)_p, & \text{if } \tau = 2k-1 \in D_0^{(2p)} \\ (0,0)_p, & \text{if } \tau = 2k-1 \in D_1^{(2p)} \end{cases}. \end{aligned}$$

Now, we are ready to compute (22).

Since $2(k-1)+1 = \tau$, $\tau \in D_i^{(2p)}$ implies $v(k-1) = i$ for $i = 0, 1$. When $p \equiv \pm 1 \pmod 8$, if $-\tau \in D_i^{(2p)}$, then $p - \tau \pmod{2p}$ is an element of either $2D_i^{(p)} \pmod{2p}$ or $2D_{i+1\ mod\ 2}^{(p)} \pmod{2p}$. Since it is valid when we apply modulo $p$ reduction, $-\tau \pmod p$ is an element of either $2D_i^{(p)} = D_i^{(p)} \pmod p$ or $2D_{i+1\ mod\ 2}^{(p)} = D_{i+1\ mod\ 2}^{(p)} \pmod p$. Because $-\tau \in D_i^{(2p)}$ implies $-\tau \in D_i^{(p)} \pmod p$, $p - \tau \pmod{2p} = 2(\frac{p-1}{2} - k + 1) \in 2D_i^{(p)} \pmod{2p}$. Therefore, $t(\frac{p-1}{2} - k + 1) = i$. On the other hand, if $p \equiv \pm 3 \pmod 8$, $t(\frac{p-1}{2} - k + 1) = i + 1 \pmod 2$ when $-\tau \in D_i^{(2p)}$.

Combining all of these computation, we can get to the (18),(19),(20) and (21). ■

**Theorem 1:** *[Main Result]* Let $p$ be an odd prime. Then the autocorrelation of the quaternary sequence of length $2p$ defined at (1) is as follows:

1. If $p \equiv 1 \pmod 8$,

$$C_s(\tau) = \begin{cases} 2p, & \text{if } \tau = 0 \pmod{2p} \\ -2p, & \text{if } \tau = p \pmod{2p} \\ p-7, & \text{if } \tau \in 2D_0^{(p)} \\ p-3, & \text{if } \tau \in 2D_1^{(p)} \\ -p+7, & \text{if } \tau \in D_0^{(2p)} \\ -p+3, & \text{if } \tau \in D_1^{(2p)}. \end{cases}$$

2. If $p \equiv \pm 3 \pmod 8$,

$$C_s(\tau) = \begin{cases} 2p, & \text{if } \tau = 0 \pmod{2p} \\ -2, & \text{if } \tau = p \pmod{2p} \\ p-5, & \text{if } \tau \in 2D_0^{(p)} \cup 2D_1^{(p)} \\ -p+3, & \text{if } \tau \in D_0^{(2p)} \cup D_1^{(2p)}. \end{cases}$$

3. If $p \equiv 7 \pmod 8$,

$$C_s(\tau) = \begin{cases} 2p, & \text{if } \tau = 0 \pmod{2p} \\ -2p, & \text{if } \tau = p \pmod{2p} \\ p-5+4j, & \text{if } \tau \in 2D_0^{(p)} \\ p-5-4j, & \text{if } \tau \in 2D_1^{(p)} \\ -p+5-4j, & \text{if } \tau \in D_0^{(2p)} \\ -p+5+4j, & \text{if } \tau \in D_1^{(2p)}. \end{cases}$$

**Proof:** When $\tau \equiv 0 \pmod{2p}$, obviously $C_s(\tau) = 2p$. When $\tau \equiv 2k \pmod{2p}$ and $1 \leq k \leq p-1$, we obtain what we want by combining (5), (6), (9), (10), (11) and (12). Likewise, when $\tau \equiv 2k-1 \pmod{2p}$ and $1 \leq k \leq p$, we also obtain what we want to prove by combining (13), (14), (15), (16), (18), (19), (20) and (21). ■

Next, we are going to consider assigning another symbol to the each sets $D_0^{(2p)}, D_1^{(2p)}, 2 \cdot D_0^{(p)}$ and $2 \cdot D_1^{(p)}$. Let us introduce a vector $\mathbf{d} = (d_0, d_1, d_2, d_3)$, where $d_i \in \{0, 1, 2, 3\}$, $0 \leq i < 4$. Each $d_0, d_1, d_2$ and $d_3$ correspond to the symbol assigned to $D_0^{(2p)}, D_1^{(2p)}, 2 \cdot D_0^{(p)}$ and $2 \cdot D_1^{(p)}$ respectively. Since it is also possible to change the symbols at '0' and '$p$' position, we introduce another vector $\mathbf{e} = (e_0, e_1)$, where $e_i \in \{0, 1, 2, 3\}$, $i = 0, 1$. For the following pairs of vector $(\mathbf{d}, \mathbf{e})$, $((0, 1, 2, 3), (0, 2))$, $((0, 1, 2, 3), (2, 0))$, $((0, 1, 3, 2), (0, 2))$, $((0, 1, 3, 2), (2, 0))$, $((1, 0, 2, 3), (0, 2))$, $((1, 0, 2, 3), (2, 0))$, $((1, 0, 3, 2), (0, 2))$, and $((1, 0, 3, 2), (2, 0))$, we can verify that the number of distinct absolute values of autocorrelation is up to 4 and for any $\tau \notin \{0, p\}$, $|C_s(\tau)| \leq p + 1$. Furthermore, when $\mathbf{e} \in \{(0, 2), (2, 0)\}$ is fixed, it is easily checked that $\mathbf{d} = (0, 1, 2, 3)$ and $\mathbf{d}' = (1, 0, 3, 2)$ give us the same autocorrelation profile from the point of view of absolute value. Likewise $\mathbf{d}'' = (1, 0, 2, 3)$ and $\mathbf{d}''' = (0, 1, 3, 2)$ give us the same autocorrelation profile.

## 3. Conclusion

This paper proposes a simple method of constructing quaternary cyclotomic sequences of period $2p$ for any odd prime $p$, and calculates their autocorrelation functions. In general, it is preferred to have low out-of-phase correlation [1], [2], and the sequences proposed in this paper can be said to be not good in this sense. One contribution of this paper is the exact calculation of such correlation values, though it is not good.

One interesting observation is the case where $p \equiv \pm 3 \pmod 8$. Observe in this case that the correlation value $C_s(\tau = p)$ is $-2$ at the phase shift $p$ and $C_s(\tau \neq p)$ is of the order $p$ at all other phase shifts including the zero shift. Since the period is $2p$, it is almost the same as having ideal autocorrelation with the peak at the phase shift $p$ if we take the correlation measure as $1/C_s(\tau)$. This property of the proposed sequences can be equally useful when 4−ary modulation is used and the ideal peak correlation measure must be exploited.

One open problem is the calculation of Linear Complexity of the proposed sequences. So far, we have to leave this problem to the readership of this journal.

### References

[1] S. Boztas, R. Hammons, and P.V. Kumar, "4- phase sequences with near-optimum correlation properties," IEEE Trans. Inf. Theory, vol.38, no.3, pp.1101–1113, 1992.

[2] P.Z. Fan and M. Darnell, "Balanced quadriphase sequences with near-ideal autocorrelations," Proc. 1995 IEEE International Symposium on Information Theory, p.462, Sept. 1995.

[3] D.M. Burton, Elementary Number Theory, Fourth ed., McGraw-Hill International Editions, 1998.

[4] T. Cusick, C. Ding, and A. Renvall, Stream ciphers and number theory, North-Holland Mathematical Library 55, pp.198–212, 1998.

[5] C. Ding, "Linear complexity of some generalized cyclotomic sequences," International Journal on Algebra and Computation, vol.8, pp.431–442, 1998.

**Young-Joon Kim** received his B.S. and M.S. degrees in Electronic Engineering from Yonsei University in 2002 and 2004, respectively. He is currently a Ph.D. candidate in the Department of Electrical and Electronic Engineering, Yonsei University. His specific field of research interests includes application of pseudorandom sequences and error correcting codes used in mobile telecommunication systems.

**Yun-Pyo Hong** received his B.S. and M.S. degrees in Electronic Engineering from Yonsei University in 2000 and 2002, respectively. He is currently in a Ph.D. program in the Department of Electrical and Electronic Engineering, Yonsei University. His area of research interest includes application of pseudorandom sequences and error correcting codes to mobile telecommunication and crypto systems.

**Hong-Yeop Song** received his B.S. degree in Electronic Engineering from Yonsei University in 1984, MSEE and Ph.D. degrees from the University of Southern California, Los Angeles, CA in 1986 and 1991, respectively, specializing in the area of communication theory and coding. After spending 2 years as a research staff member in the Communication Sciences Institute at USC, and while working with Dr. S.W. Golomb, he joined Qualcomm Inc., San Diego, CA in 1994 as a senior engineer and worked on a team researching and developing North American CDMA Standards for PCS and cellular air-interface systems. Finally, he joined the Dept. of Electrical and Electronics Engineering at Yonsei University, Seoul, Korea in 1995, and is currently working as a professor. He visited Dr. G. Gong at University of Waterloo, Canada, in the year 2002. His area of research interest includes Spread Spectrum Communication and the application of discrete mathematics into various communication and coding problems. He is a member of IEEE, MAA(Mathematical Association of America), IEEK, KICS, and KIISC.