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

Young-Joon Kim, Yun-Pyo Hong and Hong-Yeop Song

{yj.kim, yphong, hysong}@yonsei.ac.kr
Coding and Information Theory Lab
Yonsei University, Seoul, KOREA

Construction of New Quaternary Sequences of Length $2p$

- p : a prime
- g : an odd primitive root (mod p)

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

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

Example of Quaternary Sequences of Length $2p$

$$p = 5, g = 3$$

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

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

Some Theory

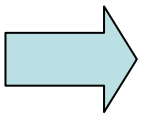
- Periodic autocorrelation

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

where $w = exp(j\frac{2\pi}{4})$

$$s^{(1)}(n) = s(2n), \quad 0 \le n \le p-1,$$

$$s^{(2)}(n) = s(2n+1), \quad 0 \le n \le p-1.$$



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

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

$$C_s(\tau) = \sum_{i=0}^{2p-1} w^{s(i+\tau)-s(i)}$$

$$= \begin{cases} C_{s^{(1)}}(k) + C_{s^{(2)}}(k), \\ \qquad \text{if } \tau \equiv 2k \pmod{2p} \text{ and } 1 \le k \le p-1 \\ \\ C_{s^{(1)}\,s^{(2)}}(k) + C_{s^{(2)}\,s^{(1)}}(k-1), \\ \qquad \text{if } \tau \equiv 2k-1 \pmod{2p} \text{ and } 1 \le k \le p \end{cases}$$

Autocorrelation $C_{s^{(1)}}(k)$ of $\{s^{(1)}(n)\}$ of length p

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

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

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

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

Autocorrelation $C_{s^{(2)}}(k)$ of $\{s^{(2)}(n)\}$ of length p

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

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

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

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

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

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

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

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

Crosscorrelation $C_{s^{(1)}s^{(2)}}(k)$ of $\{s^{(1)}(n)\}$ and $\{s^{(2)}(n)\}$

When $p \equiv 1 \pmod 8$

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

When $p \equiv 3 \pmod 8$,

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

When $p \equiv 5 \pmod 8$,

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

When $p \equiv 7 \pmod 8$,

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

Crosscorrelation $C_{s^{(2)}s^{(1)}}(k-1)$ of $\{s^{(2)}(n)\}$ and $\{s^{(1)}(n)\}$

When $p \equiv 1 \pmod 8$,
$$C_{s^{(2)}s^{(1)}}(k-1) = \begin{cases} -p, & \text{if } \tau = 2k-1 = p \pmod{2p} \\ \frac{-p+7}{2}, & \text{if } \tau = 2k-1 \in D_0^{(2p)} \\ \frac{-p+3}{2}, & \text{if } \tau = 2k-1 \in D_1^{(2p)}, \end{cases}$$

When $p \equiv 3 \pmod 8$,
$$C_{s^{(2)}s^{(1)}}(k-1) = \begin{cases} -1, & \text{if } \tau = p \pmod{2p} \\ \frac{-p+5}{2}, & \text{if } \tau \in D_0^{(2p)} \\ \frac{-p+1}{2}, & \text{if } \tau \in D_1^{(2p)}, \end{cases}$$

When $p \equiv 5 \pmod 8$,
$$C_{s^{(2)}s^{(1)}}(k-1) = \begin{cases} -1, & \text{if } \tau = p \pmod{2p} \\ \frac{-p+3}{2} - 2j, & \text{if } \tau \in D_0^{(2p)} \\ \frac{-p+3}{2} + 2j, & \text{if } \tau \in D_1^{(2p)}, \end{cases}$$

When $p \equiv 7 \pmod 8$,
$$C_{s^{(2)}s^{(1)}}(k-1) = \begin{cases} -p, & \text{if } \tau = p \pmod{2p} \\ \frac{-p+5}{2} - 2j, & \text{if } \tau \in D_0^{(2p)} \\ \frac{-p+5}{2} + 2j, & \text{if } \tau \in D_1^{(2p)}. \end{cases}$$

Let p be an odd prime. Then the autocorrelation of the quaternary sequence of length $2p$ is as follows:

- If $p \equiv 1(8)$,

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

Result

- If $p \equiv \pm 3(8)$,

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

- If $p \equiv 7(8)$,

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