New Construction of Quaternary Sequences With Ideal Autocorrelation From Legendre Sequences

Young-Sik Kim
Samsung Electronics Co. Ltd.
Yongin, 446-711, Korea
mypurist@gmail.com

Ji-Woong Jang
Department of Electrical and Computer Engineering
UCSD
La Jolla, CA 92093, USA
stasera.jang@gmail.com

Sang-Hyo Kim
School of Information and Communication Engineering
Sungkyunkwan University
Suwon 440-746, Korea.
iamshkim@skku.edu

Jong-Seon No
Department of Electrical Engineering and Computer Science
Seoul National University
Seoul 151-742, Korea.
jsno@snu.ac.kr

***Abstract*—In this paper, for an odd prime p, new quaternary sequences of even period $2p$ with ideal autocorrelation property are constructed using the Legendre sequences of period p. The distribution of autocorrelation function of the proposed quaternary sequences is also derived.**

I. Introduction

In the applications of the various wireless communication systems, the periodic autocorrelation property is used to extract desired information from the received signals. Therefore, the employed sequences should have out-of-phase autocorrelation values as low as possible to reduce interference and noise. But it is conjectured and supported by simulation that there is no binary or quaternary sequence with perfect autocorrelation whose the out-of-phase autocorrelation values are always equal to zero, except for a few cases of the sequences with short period [1].

Binary and quaternary sequences are preferred in the application of wireless communication systems due to their constant envelope property. They are also useful in the digital communication systems with binary and quaternary modulations. There have been numerous researches on binary sequences with good autocorrelation property, which include m-sequence [2], GMW sequences [3], and sequences from the images of polynomials [4], etc. The quaternary sequences with good autocorrelation property have been also studied in [1], [5], [6], [7], [8], [9].

In this paper, for an odd prime p, new quaternary sequences of even period $2p$ with ideal autocorrelation are constructed using the Legendre sequences of period p. The distribution of autocorrelation function of the proposed quaternary sequences is also derived.

II. Preliminaries

Let $g(t)$ be a q-ary sequence of period N for positive integers q and N. Then a sequence $g(t)$ of period N is said to be *balanced* iff the difference among numbers of occurrences of each element in a period is less than or equal to one.

The autocorrelation function of $g(t)$ is defined as

$$R_g(\tau) = \sum_{t=0}^{N-1} \omega_q^{g(t)-g(t+\tau)}$$

where $0 \le \tau < N$ and ω_q is the complex primitive qth root of unity, e.g., $\omega_4 = \sqrt{-1}$. The cross-correlation function of $g_1(t)$ and $g_2(t)$ is defined as

$$R_{g_1 g_2}(\tau) = \sum_{t=0}^{N-1} \omega_q^{g_1(t)-g_2(t+\tau)}.$$

In many applications of the wireless communication systems, it is known that it is desirable for the sequences to have the following properties:

- The maximum sidelobe of their autocorrelation functions should be as low as possible;
- For the given maximum sidelobe, the number of occurrence of the maximum sidelobe should be minimized.

These properties of the sequences guarantee the minimum false alarm rate in the synchronization of the wireless communication systems. Since these properties are conflicted with each other, for the possible minimum value of the maximum sidelobe of the autocorrelation functions, the sequences with the minimum number of occurrences of the maximum sidelobe is desirable in many applications. These sequences are said to have *the ideal autocorrelation property*. It is well known that the binary sequence of odd period N with ideal autocorrelation property has the distribution of autocorrelation values as

$$R_g(\tau) = \begin{cases} N, & 1 \text{ times} \\ -1, & N-1 \text{ times.} \end{cases}$$

It is not difficult to prove the ideal autocorrelation property of the quaternary sequences of even period with balance property as in the following theorem.

Theorem 1: Let N be an even integer. Then the autocorrelation distribution of a quaternary sequence $g(t)$ of period N with ideal autocorrelation and balance property is given as

$$R_g(\tau) = \begin{cases} N, & 1 \text{ times} \\ 0, & \frac{N}{2}-1 \text{ times} \\ -2, & \frac{N}{2} \text{ times.} \end{cases} \quad (1)$$

In general, optimal correlation property is defined for the families of sequences whose correlation values meet some correlation bound.

978-1-4244-4313-0/09/$25.00 ©2009 IEEE

Let $\phi[a,b]$ be the Gray mapping defined by

$$\phi[a,b] = \begin{cases} 0, & \text{if } (a,b) = (0,0) \\ 1, & \text{if } (a,b) = (0,1) \\ 2, & \text{if } (a,b) = (1,1) \\ 3, & \text{if } (a,b) = (1,0). \end{cases} \quad (2)$$

Let $a(t)$ and $b(t)$ be binary sequences of period N. Then a quaternary sequence $q(t)$ is defined by $q(t) = \phi[a(t), b(t)]$, which can be also expressed as [9]

$$\omega_4^{q(t)} = \frac{1+\omega_4}{2}(-1)^{a(t)} + \frac{1-\omega_4}{2}(-1)^{b(t)}. \quad (3)$$

Krone and Sarwate derived the relation between the autocorrelation functions of the binary sequences and the corresponding quaternary sequences in (3) as follows.

Theorem 2 (Krone and Sarwate [9]): Let $a(t)$, $b(t)$, $c(t)$, and $d(t)$ be binary sequences of the same period. Let $p(t)$ and $q(t)$ be quaternary sequences defined by $p(t) = \phi[a(t), b(t)]$ and $q(t) = \phi[c(t), d(t)]$, respectively. Then cross-correlation function $R_{pq}(\tau)$ between $p(t)$ and $q(t)$ is given as

$$R_{pq}(\tau) = \frac{1}{2}\big\{R_{ac}(\tau) + R_{bd}(\tau) + \omega_4(R_{ad}(\tau) - R_{bc}(\tau))\big\}$$

where $R_{pq}(\tau)$ is the cross-correlation function between $p(t)$ and $q(t)$.

For an odd prime p, let $b_0(t)$ be the binary sequence defined by

$$b_0(t) = \begin{cases} 0, & \text{for } t = 0 \\ 0, & \text{for } t \in QR \\ 1, & \text{for } t \in QNR \end{cases} \quad (4)$$

where QR and QNR are the sets of quadratic residues and quadratic non-residues in the set of integers modulo p, Z_p, respectively. And let $b_1(t)$ be the binary sequence of period p defined by

$$b_1(t) = \begin{cases} 1, & \text{for } t = 0 \\ 0, & \text{for } t \in QR \\ 1, & \text{for } t \in QNR \end{cases} \quad (5)$$

which corresponds to a Legendre sequence. It is easy to check that $b_k(t)$ takes the symbol k one more time than the other symbol $1-k$, $k = 0, 1$, which corresponds to the balance property.

The following two definitions of the indicator function and the quadratic character are useful to express the sequences in (4) and (5).

Definition 3: The indicator function is defined as

$$I(x) = \begin{cases} 1, & \text{if } x = 0 \\ 0, & \text{if } x \neq 0. \end{cases}$$

Definition 4: The quadratic character of Z_p is defined as

$$\psi_2(t) = \begin{cases} 0, & \text{for } t = 0 \\ 1, & \text{for } t \in QR \\ -1, & \text{for } t \in QNR. \end{cases}$$

Then two binary sequences $b_0(t)$ and $b_1(t)$ in (4) and (5) can be represented by using the indicator function $I(x)$ and the quadratic character $\psi_2(t)$ of Z_p as

$$(-1)^{b_k(t)} = \psi_2(t) + (-1)^k I(t) \quad (6)$$

where $k = 0, 1$.

The autocorrelation property of Legendre sequences was already studied [6]. Here we will summarize the correlation distributions as in the following lemma.

Lemma 5: For an odd prime p, let $b_0(t)$ and $b_1(t)$ be binary sequences defined in (4) and (5), respectively. Then the correlation functions $R_{b_0}(\tau)$, $R_{b_1}(\tau)$, $R_{b_0 b_1}(\tau)$, and $R_{b_1 b_0}(\tau)$ are calculated as follows.

For an odd prime p such that $p \equiv 3 \bmod 4$, we have

$$R_{b_0}(\tau) = R_{b_1}(\tau) = \begin{cases} p, & \text{for } \tau = 0 \\ -1, & \text{otherwise} \end{cases}$$

$$R_{b_0 b_1}(\tau) = \begin{cases} p-2, & \text{for } \tau = 0 \\ -1 + 2\psi_2(\tau), & \text{otherwise} \end{cases}$$

$$R_{b_1 b_0}(\tau) = \begin{cases} p-2, & \text{for } \tau = 0 \\ -1 - 2\psi_2(\tau), & \text{otherwise.} \end{cases}$$

For an odd prime p such that $p \equiv 1 \bmod 4$, we have

$$R_{b_0}(\tau) = \begin{cases} p, & \text{for } \tau = 0 \\ -1 + 2\psi_2(\tau), & \text{otherwise} \end{cases}$$

$$R_{b_1}(\tau) = \begin{cases} p, & \text{for } \tau = 0 \\ -1 - 2\psi_2(\tau), & \text{otherwise} \end{cases}$$

$$R_{b_0 b_1}(\tau) = R_{b_1 b_0}(\tau) = \begin{cases} p-2, & \text{for } \tau = 0 \\ -1, & \text{otherwise.} \end{cases}$$

III. New Quaternary Sequences From Legendre Sequences

Applying the Gray mapping to two binary sequences in (4) and (5), we propose two construction methods of new quaternary sequences with ideal autocorrelation property.

For an odd prime p such that $p \equiv 1 \bmod 4$, let $b_0(t)$ and $b_1(t)$ be binary sequences of period p with $b_0(0) = 0$ and $b_1(0) = 1$ defined in (4) and (5), respectively. Then $b_0(t)$ has one more zero than one and $b_1(t)$ has one more one than zero. Let $s_0(t)$ and $s_1(t)$ be two binary sequences of period $2p$ defined by

$$s_0(t) = \begin{cases} b_0(t), & \text{for } t \equiv 0 \bmod 2 \\ b_1(t), & \text{for } t \equiv 1 \bmod 2 \end{cases} \quad (7)$$

$$s_1(t) = \begin{cases} b_0(t), & \text{for } t \equiv 0 \bmod 2 \\ b_1(t) \oplus 1, & \text{for } t \equiv 1 \bmod 2 \end{cases} \quad (8)$$

where $\oplus$ denotes modulo 2 addition and the subscript t is reduced modulo p. Then we have the following lemma.

Lemma 6: For an odd prime p such that $p \equiv 1 \bmod 4$, let $s_0(t)$ and $s_1(t)$ be binary sequences of period $2p$ defined in

(7) and (8). Then the autocorrelation function $R_{s_0}(\tau)$ of $s_0(t)$ and the autocorrelation function $R_{s_1}(\tau)$ of $s_1(t)$ are calculated as

$$R_{s_0}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \\ 2(p-2), & \text{for } \tau \equiv p \bmod 2p \\ -2, & \text{otherwise} \end{cases}$$

$$R_{s_1}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \\ -2(p-2), & \text{for } \tau \equiv p \bmod 2p \\ -2, & \text{for } \tau \not\equiv 0 \bmod 2p \\ & \quad \text{and } \tau \equiv 0 \bmod 2 \\ 2, & \text{for } \tau \not\equiv p \bmod 2p \\ & \quad \text{and } \tau \equiv 1 \bmod 2. \end{cases}$$

And their cross-correlation functions $R_{s_0 s_1}(\tau)$ and $R_{s_1 s_0}(\tau)$ are also computed as

$$\begin{aligned} R_{s_0 s_1}(\tau) &= R_{s_1 s_0}(\tau) \\ &= \begin{cases} 4\psi_2(\tau), & \text{for } \tau \not\equiv 0 \bmod 2p \\ & \quad \text{and } \tau \equiv 0 \bmod 2 \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Proof: From the definition of $s_0(t)$ and $s_1(t)$, we have

$$\begin{aligned} R_{s_0}(\tau) &= \begin{cases} R_{b_0}(\tau) + R_{b_1}(\tau), & \text{for } \tau \equiv 0 \bmod 2 \\ 2R_{b_0 b_1}(\tau), & \text{for } \tau \equiv 1 \bmod 2 \end{cases} \\ R_{s_1}(\tau) &= \begin{cases} R_{b_0}(\tau) + R_{b_1}(\tau), & \text{for } \tau \equiv 0 \bmod 2 \\ -2R_{b_0 b_1}(\tau), & \text{for } \tau \equiv 1 \bmod 2 \end{cases} \\ R_{s_0 s_1}(\tau) &= R_{s_1 s_0}(\tau) \\ &= \begin{cases} R_{b_0}(\tau) - R_{b_1}(\tau), & \text{for } \tau \equiv 0 \bmod 2 \\ 0, & \text{for } \tau \equiv 1 \bmod 2. \end{cases} \end{aligned}$$

From Lemma 5, the claimed results are proved. □

Applying the Gray mapping to two binary sequences in (7) and (8), new quaternary sequences with ideal autocorrelation property can be constructed as in the following theorem.

Theorem 7: For an odd prime p such that $p \equiv 1 \bmod 4$, let $s_0(t)$ and $s_1(t)$ be two binary sequences defined in (7) and (8). And let $q_1(t)$ be the quaternary sequence of period $2p$ defined by

$$q_1(t) = \phi(s_0(t), s_1(t)).$$

Then the autocorrelation function of $q_1(t)$ is given as

$$R_{q_1}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \\ -2, & \text{for } \tau \not\equiv 0 \bmod 2p \text{ and } \tau \equiv 0 \bmod 2 \\ 0, & \text{for } \tau \equiv 1 \bmod 2p. \end{cases}$$

Proof: From Theorem 2, it is clear that $R_{q_1}(\tau)$ can be rewritten as

$$R_{q_1}(\tau) = \frac{1}{2}(R_{s_0}(\tau) + R_{s_1}(\tau)) + \frac{\omega_4}{2}(R_{s_0,s_1}(\tau) - R_{s_1,s_0}(\tau)).$$

From Lemma 6, $R_{q_1}(\tau)$ can be derived as claimed. □

For an odd prime p such that $p \equiv 3 \bmod 4$, let $b_0(t)$ and $b_1(t)$ be two binary sequences of period p in (4) and (5), respectively. And let $s_2(t)$ and $s_3(t)$ be two binary sequences of period $2p$ defined by

$$s_2(t) = \begin{cases} b_0(t), & \text{for } 0 \le t < p \\ b_0(t), & \text{for } p \le t < 2p \end{cases} \quad (9)$$

$$s_3(t) = \begin{cases} b_1(t), & \text{for } t \equiv 0 \bmod 2 \\ b_1(t) \oplus 1, & \text{for } t \equiv 1 \bmod 2. \end{cases} \quad (10)$$

Then we have the following lemma.

Lemma 8: For an odd prime p such that $p \equiv 3 \bmod 4$, let $s_2(t)$ and $s_3(t)$ be binary sequences of period $2p$ defined in (9) and (10). Then the autocorrelation function $R_{s_2}(\tau)$ of $s_2(t)$ and the autocorrelation $R_{s_3}(\tau)$ of $s_3(t)$ calculated as

$$R_{s_2}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \text{ or } \tau \equiv p \bmod 2p \\ -2, & \text{otherwise} \end{cases}$$

$$R_{s_3}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \\ -2p, & \text{for } \tau \equiv p \bmod 2p \\ -2, & \text{for } \tau \not\equiv 0 \bmod 2p \text{ and } \tau \equiv 0 \bmod 2 \\ 2, & \text{for } \tau \not\equiv p \bmod 2p \text{ and } \tau \equiv 1 \bmod 2. \end{cases}$$

And the cross-correlation functions $R_{s_2,s_3}(\tau)$ and $R_{s_3,s_2}(\tau)$ are also calculated as

$$R_{s_2 s_3}(\tau) = R_{s_3 s_2}(\tau) = 0.$$

The proof of the above lemma is similar to that of Lemma 6 and thus we omit the proof of the above lemma.

Applying the Gray mapping to two binary sequences in (9) and (10), new quaternary sequences can be constructed as in the following theorem.

Theorem 9: For an odd prime p such that $p \equiv 3 \bmod 4$, let $s_2(t)$ and $s_3(t)$ be binary sequences defined in (9) and (10). And let $q_2(t)$ be the quaternary sequence of period $2p$ defined by

$$q_2(t) = \phi(s_2(t), s_3(t)).$$

Then the autocorrelation function of $q_2(t)$ is computed as

$$R_{q_2}(\tau) = \begin{cases} 2p, & \text{for } \tau \equiv 0 \bmod 2p \\ -2, & \text{for } \tau \not\equiv 0 \bmod 2p \text{ and } \tau \equiv 0 \bmod 2 \\ 0, & \text{for } \tau \equiv 1 \bmod 2p. \end{cases}$$

Proof: From Theorem 2, it is clear that $R_{q_2}(\tau)$ can be rewritten as

$$R_{q_2}(\tau) = \frac{1}{2}(R_{s_2}(\tau) + R_{s_3}(\tau)) + \frac{\omega_4}{2}(R_{s_2 s_3}(\tau) - R_{s_3 s_2}(\tau)).$$

From Lemma 8, $R_{q_2}(\tau)$ can be calculated as claimed. □

Using the definitions of $s_0(t)$, $s_1(t)$, $s_2(t)$, and $s_3(t)$ in (7), (8), (9), and (10), it is not difficult to derive the balance property of two proposed quaternary sequences $q_1(t)$ and $q_2(t)$ as in the following theorem.

Theorem 10: Let $q_1(t)$ and $q_2(t)$ be two quaternary sequences defined in Theorems 7 and 9. Then $q_1(t)$ and $q_2(t)$

have the balanced property, i.e., for $p \equiv 1 \mod 4$, we have

$$q_1(t) = \begin{cases} 0, & \frac{p+1}{2} \text{ times} \\ 1, & \frac{p-1}{2} \text{ times} \\ 2, & \frac{p-1}{2} \text{ times} \\ 3, & \frac{p+1}{2} \text{ times} \end{cases}$$

and for $p \equiv 3 \mod 4$, we have

$$q_2(t) = \begin{cases} 0, & \frac{p+1}{2} \text{ times} \\ 1, & \frac{p+1}{2} \text{ times} \\ 2, & \frac{p-1}{2} \text{ times} \\ 3, & \frac{p-1}{2} \text{ times.} \end{cases}$$

REFERENCES

[1] H. Dieter Luke, H. D. Schotten, and H. Hadinejad-Mahram, "Binary and quadriphase sequences with optimal autocorrelation properties: A Survey," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3271–3282, Dec. 2003.

[2] J. F. Dillon and H. Dobbertin, "New cyclic difference sets with Singer parameters," *Finite Fields Appl.,* vol. 10, no. 3, pp. 342–389, July 2004.

[3] B. Gordon, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canadian J. Math.,* vol. 14, no. 4, pp. 614–625, 1962.

[4] J.-S. No, H. Chung, and M. S. Yun, "Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$," *IEEE Trans. Inf. Theory,* vol. 44, no. 3, pp. 1278–1282, May 1998.

[5] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "On the autocorrelation distributions of Sidel'nikov sequences," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3303–3307, Sep. 2005.

[6] V. M. Sidel'nikov, "Some k-valued pseudo-random sequences and nearly equidistant codes," *Probl. Inf. Transm.*, vol. 5, no. 1, pp. 12–16, 1969.

[7] H. D. Schotten, "New optimum ternary complementary sets and almost quadriphase, perfect sequences," in *Proc. Int. Conf. Neural Networks and Signal Process.'95*, Nanjing, China, Dec. 1995, pp. 1106–1109.

[8] H. D. Schotten, "Optimum complementary sets and quadriphase sequences derived from q-ary m-sequences," in *Proc. IEEE Int. Symp. Inf. Theory'97*, Ulm, Germany, 1997, p. 485.

[9] S. M. Krone and D. V. Sarwate,"Quadriphase sequences for spread spectrum multiple-access communication," *IEEE Trans. Inf. Theory,* vol. IT-30, no. 3, pp. 520–529, May 1984.

[10] T. Storer, *Cyclotomy and Difference Sets*, Lectures in Advanced Mathematics. Chicago, IL: Markham, 1967.