New Quaternary Sequences With Ideal Autocorrelation Constructed From Binary Sequences With Ideal Autocorrelation

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

Young-Sik Kim
Samsung Electronics Co. Ltd.
Yongin, 446-711, Korea
mypurist@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, a new generation method of quaternary sequences of period $2(2^n-1)$ with ideal autocorrelation and balance property is proposed using the binary sequences of period 2^n-1 with ideal autocorrelation and reverse Gray mapping. The autocorrelation distribution of the proposed quaternary sequences is also derived.**

I. Introduction

Pseudorandom sequences with good autocorrelation play important roles in many areas of communications, cryptography, and other digital systems. Such sequences are required to be easily distinguished from their shifted versions, that is, to have low nontrivial autocorrelation values. Due to their usefulness in the digital communication systems with binary and quaternary modulations, binary and quaternary sequences have been paid more attention in the sequence design. Up to now, most researches have been devoted to the binary sequences rather than the quaternary sequences. There have been found several quaternary sequences with good autocorrelation property.

Let $R_{\max}$ be the maximum magnitude of the nontrivial autocorrelation values of the sequences. If $R_{\max}=0$, then the sequences have the perfect autocorrelation property. But, it is conjectured and supported by extensive simulation that there is no binary or quaternary sequences with perfect autocorrelation except for a few cases of the sequences with short period [1]. In the case of $R_{\max}=1$, there have been numerous researches on binary sequences, such as m-sequence [2], GMW sequences [3], and sequences from the images of polynomials [4], etc.

There have also been various researches on the quaternary sequences with good autocorrelation [1], [5], [6], [7], [8]. Sidel'nikov introduced M-ary sequences with good autocorrelation property, which includes the quaternary sequences as a special case [5]. Schotten's complementary-based sequences [1], [6], [7] have good autocorrelation property for odd period. Luke, Schotten, and Hadinejad-Mahram constructed quaternary sequences with $R_{\max}=2$ [1] for even period. For period $N\equiv 2 \pmod 4$, quaternary sequences with $R_{\max}=2$ [1] can be also constructed by modifying Lee's perfect sequences [9] or by periodic multiplication method. These are the best known results on the autocorrelation of pure quaternary (or quadriphase) sequences.

In this paper, the ideal autocorrelation of the quaternary sequences is proposed. A new generation method of quaternary sequences of period $2(2^n-1)$ with ideal autocorrelation and balance property is proposed using the binary sequences of period 2^n-1 with ideal autocorrelation and reverse Gray mapping. The autocorrelation distribution of the proposed quaternary sequences is also derived.

II. Preliminaries

In this section, we introduce some definitions and notations. For positive integers q and N, let $g(t)$ be a q-ary sequence of period N. Let

$$A_k=\{t\mid g(t)=k, 0\le t<N\}, k=0,1,\cdots,q-1.$$

Then a quaternary sequence $g(t)$ of period N is said to be *balanced* iff $|A_i-A_j|\le 1$ for any pair of i,j.

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., $\omega_4=\sqrt{-1}$.

When the sequences are used in the communication systems, such as preambles for the synchronization, it is known that it is desirable for the sequences to have the following properties:

- The maximum sidelobes of their autocorrelation functions is as low as possible;
- For a given maximum sidelobe, the number of occurrences of the maximum sidelobe is minimal. .

Those properties of the sequences guarantee the minimum false alarm rate in the application of the synchronization for wireless communication systems. The sequences having the above two properties in the order are said to have the *ideal autocorrelation property*. It is well known that the binary

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

sequence of odd period N with ideal autocorrelation property has the distribution of autocorrelation values as

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

Jang, Kim, Kim, and No [10] proposed the ideal autocorrelation property of the quaternary sequences of even period with balance property as in the following theorem.

Theorem 1 (Jang, Kim, Kim, and No [10]): 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

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

Let Z_{2^n-1} be the set of integers modulo 2^n-1, i.e., $Z_{2^n-1} = \{0, 1, 2, \ldots, 2^n-2\}$. Let n be a positive integer and $s(t)$ a binary sequence of period 2^n-1 with ideal autocorrelation. Let D_u be the characteristic set of $s(t-u)$, i.e.,

$$D_u = \{t \mid s(t-u) = 1,\ 0 \le t \le 2^n-2\} = D_0 + u$$

where $u \in Z_{2^n-1}$, $D_0 + u = \{d+u \mid d \in D_0\}$, and + means addition modulo 2^n-1. Let $\overline{D}_u = Z_{2^n-1} \backslash D_u$. Since all binary sequences with ideal autocorrelation have balance property, it is clear that

$$|D_u| = 2^{n-1}, \quad |\overline{D}_u| = 2^{n-1}-1.$$

From the property of the binary sequence with ideal autocorrelation, it is easy to check that for $u \ne v$, we have

$$\begin{aligned} |D_u \cap D_v| &= 2^{n-2} && (2) \\ |D_u \cap \overline{D}_v| &= 2^{n-2} && (3) \\ |\overline{D}_u \cap D_v| &= 2^{n-2} && (4) \\ |\overline{D}_u \cap \overline{D}_v| &= 2^{n-2}-1 && (5) \end{aligned}$$

and for $u = v$,

$$\begin{aligned} |D_u \cap D_v| &= 2^{n-1} && (6) \\ |D_u \cap \overline{D}_v| &= 0 && (7) \\ |\overline{D}_u \cap D_v| &= 0 && (8) \\ |\overline{D}_u \cap \overline{D}_v| &= 2^{n-1}-1. && (9) \end{aligned}$$

By the Chinese remainder theorem, we can represent $Z_{2\times(2^n-1)} \cong Z_2 \otimes Z_{2^n-1}$ under the isomorphism $\phi : \zeta \longmapsto (\zeta \bmod 2, \zeta \bmod 2^n-1)$, where $\otimes$ means direct product. For convenience, we will use the notation $\zeta \in Z_{2\times(2^n-1)}$ interchangeably with $(\zeta \bmod 2, \zeta \bmod 2^n-1)$ throughout the paper.

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

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

Let $a(t)$ and $b(t)$ be binary sequences of period N. Then we have a quaternary sequence of period N defined by $q(t) = \phi[a(t), b(t)]$. It is easy to check [8] that

$$\omega_4^{q(t)} = \frac{1+\omega_4}{2}(-1)^{a(t)} + \frac{1-\omega_4}{2}(-1)^{b(t)}. \tag{10}$$

III. New Quaternary Sequence With Ideal Autocorrelation

In this section, a new construction method of quaternary sequence from binary sequence with ideal autocorrelation is proposed. The autocorrelation function of the proposed quaternary sequence takes the values 0 or -2 except for in-phase autocorrelation, which is the best for quaternary sequences of period $N \equiv 2 \bmod 4$. The autocorrelation distribution of the proposed quaternary sequences is also derived.

Krone and Sarwate introduced the relationship between correlation functions of binary sequences and the corresponding quaternary sequences in (10) as follows.

Lemma 2 (Krone and Sarwate [8]): 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 $R_{p,q}(\tau)$ of $p(t)$ and $q(t)$ is given as

$$R_{p,q}(\tau) = \frac{1}{2}\{R_{ac}(\tau) + R_{bd}(\tau)\} + \frac{\omega_4}{2}\{(R_{ad}(\tau) - R_{bc}(\tau))\}$$

where $R_{ac}(\tau)$ is the crosscorrelation of $a(t)$ and $c(t)$.

Using a binary sequence with ideal autocorrelation and reverse Gray mapping, we can construct a quaternary sequence with the autocorrelation distribution in (1) as in the following theorem.

Theorem 3: Let n be a positive integer and $s(t)$ a binary sequence of period 2^n-1 with ideal autocorrelation and D_0 a characteristic set of $s(t)$. Let $q(t)$ be the quaternary sequence defined by

$$q(t) = \phi[a(t), b(t)] \tag{11}$$

where $a(t)$ and $b(t)$ are the binary sequences of period $2^{n+1}-2$ defined as

$$a(t) = \begin{cases} 1, & \text{if } t \in \{0,1\} \otimes D_0 \\ 0, & \text{if } t \in \{0,1\} \otimes \overline{D}_0 \end{cases} \tag{12}$$

$$b(t) = \begin{cases} 1, & \text{if } t \in \{0\} \otimes D_0 \bigcup \{1\} \otimes \overline{D}_0 \\ 0, & \text{if } t \in \{0\} \otimes \overline{D}_0 \bigcup \{1\} \otimes D_0. \end{cases} \tag{13}$$

Then the quaternary sequence $q(t)$ of period $2^{n+1}-2$ has the ideal autocorrelation property with the following distribution

$$R_q(\tau) = \begin{cases} 2^{n+1}-2, & \text{for } \tau = 0 \\ 0, & \text{for } \tau \equiv 1 \bmod 2 \\ -2, & \text{for } \tau \equiv 0 \bmod 2 \text{ and } \tau \ne 0. \end{cases}$$

Proof: It is clear that $R_q(\tau) = 2^{n+1}-2$ for $\tau = 0$. From Lemma 2, $R_q(\tau)$ can be rewritten as

$$R_q(\tau) = \frac{1}{2}\{R_a(\tau) + R_b(\tau)\} + \frac{\omega_4}{2}\{(R_{ab}(\tau) - R_{ba}(\tau))\}.$$

Therefore, what we have to do is to calculate $R_a(\tau)$, $R_b(\tau)$, $R_{ab}(\tau)$, and $R_{ba}(\tau)$.

From the definition of $a(t)$, $a(t)$ can be written as

$$a(t) = s(t \bmod 2^n - 1). \tag{14}$$

Therefore, it is clear that

$$R_a(\tau) = \begin{cases} 2^{n+1}-2, & \text{for } \tau = 0 \text{ or } \tau = 2^n - 1 \\ -2, & \text{otherwise.} \end{cases} \tag{15}$$

Let $t = (t_0, t_1)$ and $\tau = (\tau_0, \tau_1)$, where $t_0, \tau_0 \in Z_2$ and $t_1, \tau_1 \in Z_{2^n-1}$. From the definition of $a(t)$ and $b(t)$ in the theorem, $b(t)$ can be represented as

$$b(t) = \begin{cases} a(t), & \text{if } t_0 = 0 \\ a(t) + 1 \mod 2, & \text{if } t_0 = 1. \end{cases} \tag{16}$$

Then the autocorrelation function of $b(t)$ can be written as

$$\begin{aligned} R_b(\tau) &= \sum_{t=0}^{2^{n+1}-3} (-1)^{b(t)+b(t+\tau)} \\ &= \sum_{t_0=0}^{1} \sum_{t_1=0}^{2^n-2} (-1)^{b(t_0,t_1)+b(t_0+\tau_0,t_1+\tau_1)}. \end{aligned} \tag{17}$$

For $\tau_0 = 0$, from (16), $R_b(\tau)$ in (17) can be rewritten as

$$\begin{aligned} R_b(\tau) &= \sum_{t_0=0}^{1} \sum_{t_1=0}^{2^n-2} (-1)^{b(t_0,t_1)+b(t_0,t_1+\tau_1)} \\ &= \sum_{t_1=0}^{2^n-2} (-1)^{a(0,t_1)+a(0,t_1+\tau_1)} \\ &\quad + \sum_{t_1=0}^{2^n-2} (-1)^{a(1,t_1)+1+a(1,t_1+\tau_1)+1} \\ &= \sum_{t_0=0}^{1} \sum_{t_1=0}^{2^n-2} (-1)^{a(t_0,t_1)+a(t_0+\tau_0,t_1+\tau_1)} \\ &= \sum_{t=0}^{2^{n+1}-3} (-1)^{a(t)+a(t+\tau)} = R_a(\tau). \end{aligned} \tag{18}$$

And for $\tau_0 = 1$, $R_b(\tau)$ in (17) can be also rewritten as

$$\begin{aligned} R_b(\tau) &= \sum_{t_0=0}^{1} \sum_{t_1=0}^{2^n-2} (-1)^{b(t_0,t_1)+b(t_0+1,t_1+\tau_1)} \\ &= \sum_{t_1=0}^{2^n-2} (-1)^{a(0,t_1)+a(1,t_1+\tau_1)+1} \\ &\quad + \sum_{t_1=0}^{2^n-2} (-1)^{a(1,t_1)+1+a(0,t_1+\tau_1)} \\ &= -\sum_{t_0=0}^{1} \sum_{t_1=0}^{2^n-2} (-1)^{a(t_0,t_1)+a(t_0+\tau_0,t_1+\tau_1)} \\ &= -\sum_{t=0}^{2^{n+1}-3} (-1)^{a(t)+a(t+\tau)} = -R_a(\tau). \end{aligned} \tag{19}$$

From (18) and (19), $R_b(\tau)$ can be written as

$$R_b(\tau) = \begin{cases} 2^{n+1}-2, & \text{for } \tau = 0 \\ -2^{n+1}+2, & \text{for } \tau = 2^n - 1 \\ -2, & \text{for } \tau \equiv 0 \bmod 2 \text{ and } \tau \neq 0 \\ 2, & \text{for } \tau \equiv 1 \bmod 2 \text{ and } \tau \neq 2^n - 1. \end{cases} \tag{20}$$

Similarly, the cross-correlation function of $a(t)$ and $b(t)$ can be written as

$$\begin{aligned} R_{ab}(\tau) &= \sum_{t=0}^{2^{n+1}-3} (-1)^{a(t)+b(t+\tau)} \\ &= \sum_{t_0=0}^{1} \sum_{t_1=0}^{2^n-2} (-1)^{a(t_0,t_1)+b(t_0+\tau_0,t_1+\tau_1)}. \end{aligned} \tag{21}$$

For $\tau_0 = 0$, from (16), $R_{ab}(\tau)$ in (21) can be rewritten as

$$\begin{aligned} R_{ab}(\tau) &= \sum_{t_0=0}^{1} \sum_{t_1=0}^{2^n-2} (-1)^{a(t_0,t_1)+b(t_0,t_1+\tau_1)} \\ &= \sum_{t_1=0}^{2^n-2} (-1)^{a(0,t_1)+a(0,t_1+\tau_1)} \\ &\quad + \sum_{t_1=0}^{2^n-2} (-1)^{a(1,t_1)+a(1,t_1+\tau_1)+1}. \end{aligned} \tag{22}$$

From (14), it is easy to derive that

$$\sum_{t_1=0}^{2^n-2} (-1)^{a(0,t_1)+a(\tau_0,t_1+\tau_1)} = \sum_{t_1=0}^{2^n-2} (-1)^{s(t)+s(t+\tau)} = R_s(\tau)$$

$$\sum_{t_1=0}^{2^n-2} (-1)^{a(1,t_1)+a(1+\tau_0,t_1+\tau_1)+1}$$

$$= -\sum_{t_1=0}^{2^n-2} (-1)^{s(t)+s(t+\tau)} = -R_s(\tau).$$

Thus we have $R_{ab}(\tau) = 0$. And for $\tau_0 = 1$, (22) can be computed as

$$\begin{aligned} R_{ab}(\tau) &= \sum_{t_0=0}^{1} \sum_{t_1=0}^{2^n-2} (-1)^{a(t_0,t_1)+b(t_0+1,t_1+\tau_1)} \\ &= \sum_{t_1=0}^{2^n-2} (-1)^{a(0,t_1)+a(1,t_1+\tau_1)+1} \\ &\quad + \sum_{t_1=0}^{2^n-2} (-1)^{a(1,t_1)+a(0,t_1+\tau_1)} = 0. \end{aligned} \tag{23}$$

Similar to $R_{ab}(\tau)$, we can derive $R_{ba}(\tau) = 0$.

Using (15), (20), and (23), $R_q(\tau)$ can be calculated as

$$\begin{aligned} R_q(\tau) &= \frac{1}{2}\{R_a(\tau) + R_b(\tau)\} + \frac{\omega_4}{2}\{(R_{ab}(\tau) - R_{ba}(\tau))\} \\ &= \begin{cases} 2^{n+1}-2, & \text{for } \tau = 0 \\ 0, & \text{for } \tau \equiv 1 \bmod 2 \\ -2, & \text{for } \tau \equiv 0 \bmod 2 \text{ and } \tau \neq 0. \end{cases} \end{aligned}$$

□

Using a binary m-sequence, an example of the above theorem is given as follows.

Example 4: Let $s(t)$ be the binary m-sequence of period 15 given by

$$s(t) = 0,0,0,1,0,0,1,1,0,1,0,1,1,1,1.$$

Then $a(t)$ and $b(t)$ in Theorem 3 are expressed as

$$\begin{aligned} a(t) &= 0,0,0,1,0,0,1,1,0,1,0,1,1,1,1, \\ &\quad\; 0,0,0,1,0,0,1,1,0,1,0,1,1,1,1 \\ b(t) &= 0,1,0,0,0,1,1,0,0,0,0,0,1,0,1, \\ &\quad\; 1,0,1,1,1,0,0,1,1,1,1,1,0,1,0. \end{aligned}$$

From the definition of $q(t)$ in Theorem 3, $q(t)$ can be generated as

$$\begin{aligned} q(t) &= 0,1,0,3,0,1,2,3,0,3,0,3,2,3,2, \\ &\quad\; 1,0,1,2,1,0,3,2,1,2,1,2,3,2,3. \end{aligned}$$

The autocorrelation $R_q(\tau)$ of $q(t)$ is calculated as

$$\begin{aligned} R_q(\tau) &= 30,0,-2,0,-2,0,-2,0,-2,0,-2,0,-2,0,-2, \\ &\quad\; 0,-2,0,-2,0,-2,0,-2,0,-2,0,-2,0,-2,0. \end{aligned}$$

Using (12) and (13), it is easy to derive the balance property of the proposed quaternary sequence $q(t)$, which is given in the following theorem.

Theorem 5: Let $q(t)$ be the quaternary sequence defined in Theorem 3. Then $q(t)$ has the balanced property, i.e.,

$$q(t) = \begin{cases} 0, & 2^{n-1} - 1 \text{ times} \\ 1, & 2^{n-1} - 1 \text{ times} \\ 2, & 2^{n-1} \text{ times} \\ 3, & 2^{n-1} \text{ times.} \end{cases}$$

Proof: From the definition of $q(t)$, we have

$$q(t) = \begin{cases} 0, & \text{for } t \in \{0\} \otimes (\overline{D}_0 \cap \overline{D}_0) \\ & \quad \text{or } t \in \{1\} \otimes (\overline{D}_0 \cap D_0) \\ 1, & \text{for } t \in \{0\} \otimes (\overline{D}_0 \cap D_0) \\ & \quad \text{or } t \in \{1\} \otimes (\overline{D}_0 \cap \overline{D}_0) \\ 2, & \text{for } t \in \{0\} \otimes (D_0 \cap D_0) \\ & \quad \text{or } t \in \{1\} \otimes (D_0 \cap \overline{D}_0) \\ 3, & \text{for } t \in \{0\} \otimes (D_0 \cap \overline{D}_0) \\ & \quad \text{or } t \in \{1\} \otimes (D_0 \cap D_0). \end{cases}$$

Since $D \cap \overline{D} = \emptyset$ and $D \cap D = D$, $q(t)$ can be rewritten as

$$q(t) = \begin{cases} 0, & \text{for } t \in \{0\} \otimes \overline{D}_0 \\ 1, & \text{for } t \in \{1\} \otimes \overline{D}_0 \\ 2, & \text{for } t \in \{0\} \otimes D_0 \\ 3, & \text{for } t \in \{1\} \otimes D_0. \end{cases}$$

From (6)–(9), it is clear that $q(t)$ has the following distribution

$$q(t) = \begin{cases} 0, & 2^{n-1} - 1 \text{ times} \\ 1, & 2^{n-1} - 1 \text{ times} \\ 2, & 2^{n-1} \text{ times} \\ 3, & 2^{n-1} \text{ times.} \end{cases}$$

From the above distribution, it is easy to see that $q(t)$ is balanced. □

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] 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.

[6] 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.

[7] 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.

[8] 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.

[9] C. E. Lee, “ Perfect q-ary sequences from multiplicative characters over $GF(p)$,” *Electron. Lett.*, vol. 28, pp. 833–835, 1992.

[10] J.-W. Jang, Y.-S. Kim, S.-H. Kim, and J.-S. No, “New construction of quaternary sequences with ideal autocorrelation using binary sequences with ideal autocorrelation,” submitted to IEEE Tran. Inform. Theory, Feb. 2009.