New Quaternary Sequences With Optimal Autocorrelation

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*—We propose a new construction of quaternary sequences using the reverse Gray mapping of a pair of binary Sidel'nikov sequences. The proposed construction provides sequences of even period N with the maximum nontrivial autocorrelation magnitude, $R_{\max} = 2$. For $N \equiv 0 \bmod 4$, the new quaternary sequences have the optimal $R_{\max} = 2$ and are almost-balanced in contrast to the only earlier optimal construction S_j [1].**

I. Introduction

Let $a(t)$ and $b(t)$ be M-ary sequences of period N, where M is a positive integer. We may express $\omega_M^{a(t)}$ as the sequence in the signal space or the root of unity sequence corresponding to M-ary sequence $a(t)$, where ω_M is the complex primitive Mth root of unity, e.g., $\omega_4 = j = \sqrt{-1}$ for $M = 4$. The periodic cross-correlation function $R_{a,b}(\tau)$ of the two sequences $a(t)$ and $b(t)$ is defined as

$$R_{a,b}(\tau) = \sum_{t=0}^{N-1} \omega_M^{a(t)-b(t+\tau)}.$$

If $a(t) = b(t)$, it becomes the autocorrelation function of the sequence $a(t)$ and the notation is simplified as $R_a(\tau)$. Clearly, $R_a(0) = N$, which is called the inphase or trivial autocorrelation. The out-of-phase autocorrelation is dependent on the realization of the sequence $a(t)$, so that it is called nontrivial.

Let $R_{\max}$ be the maximum magnitude of out-of-phase autocorrelation of a sequence $a(t)$ defined by

$$R_{\max} = \max_{1 \le \tau \le N-1} |R_a(\tau)|$$

i.e., the maximum out-of-phase autocorrelation. $R_{\max}$ of a sequence is one of critical merits in the signal design for various digital communication systems. A lot of effort have been devoted to find or construct sequences with the autocorrelation function with small $R_{\max}$ [2], [3], [4], [5], [6].

Since the quadrature modulations are preferred in the digital communication systems, binary and quaternary sequences have drawn more interests. Throughout the paper, our interest is confined to only periodic binary and quaternary sequences and their correlation properties. We only consider quaternary sequences whose elements are constant unity power in the signal space, such as $\omega_4^{a(t)}$.

TABLE I
Quaternary sequences with low autocorrelation

$N \bmod 4$	Type	N	$R_{\max}$
0	S_j [1]	$p^n - 1$	2
0	$\prod(C, (1,1,1,-1))$[7]	$2(p^n+1)$	4
0	New construction	$p^n - 1$	2
2	P_1 [7]	$p^n + 1$	2
2	$\prod(L_1, (1,j)), \prod(L_j, (1,j))$[7]	$2p_3, 2p_1$	2
2	$\prod(\boldsymbol{m}, (1,j))$ [7]	$2(2^n - 1)$	2
2	New construction	$p^n - 1$	2

• p_i denotes a prime which is $i \bmod 4$.

Lüke carried out an indepth survey on binary and quaternary sequences with good periodic and aperiodic autocorrelation [7]. According to the survey, quaternary sequences with unity power and even period having the lowest $R_{\max}$ are listed in Table I. S_j denotes the generalized Sidel'nikov sequence introduced in [7], which is an almost-binary sequence leaded by single imaginary symbol, $j = \omega_4$ in the signal space. S_j has been the only quaternary sequence with $R_{\max} = 2$ for the period $N \equiv 0 \bmod 4$. $\prod(C, (1,1,1,-1))$ [7] is the periodic product of the complementary-based sequence C [8] and the perfect binary sequence of length 4, $(1,1,1,-1)$. $R_{\max}$ of $\prod(C, (1,1,1,-1))$ is the same as that of binary Sidel'nikov sequences [3] for $N \equiv 0 \bmod 4$.

For $N \equiv 2 \bmod 4$, P_1 is the constant unity power sequence obtained by placing $\omega_4^0 = 1$ at the head of the perfect sequence introduced by Lee [4]. L_1 and L_j [7] are the Legendre sequences whose heads are determined to be 1 and j in signal space, respectively, so that L_j is a quaternary sequence. Their periodic product sequences with $(1, j)$ yield $R_{\max} = 2$. $\boldsymbol{m}$ denotes the binary m-sequences with the ideal autocorrelation. Actually, $\boldsymbol{m}$ in the product can be replaced by any binary sequences with the ideal autocorrelation, such as Gordon-Mills-Welch sequences [9]. For quaternary sequences with even period, $R_{\max}$ is lower-bounded by 2 although there are particular exceptions [10]. Therfore, let quaternary sequences having even period and $R_{\max} = 2$ be called optimal.

In this paper, we propose a new constructive result on

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

periodic unity power quaternary sequences with even period. New quaternary sequence can be constructed by the reverse Gray mapping of a pair of Sidel'nikov sequences with different tags.

Even though S_j is claimed to be a quaternary sequence, it has in fact only three elements, $\omega_4^0, \omega_4^1, \omega_4^2$ and is extremely imbalanced. It can be considered that the ordinary quaternary sequence having the lowest $R_{\max}$ has been $\prod(C, (1,1,1,-1))$ for $N \equiv 0 \bmod 4$ so far. The new construction of quaternary sequence has the same $R_{\max} = 2$ as that of S_j for $N \equiv 0 \bmod 4$ and is almost balanced. From that point of view, the new construction is the first nontrivial quaternary sequence achieving the optimal $R_{\max} = 2$. The new construction also provides quaternary sequences with $R_{\max} = 2$ for $N \equiv 2 \bmod 4$ which is also optimal.

II. Preliminaries

Sidel'nikov [3] introduced M-ary sequences as follows.

Definition 1 (Sidel'nikov [3]): Let p be an odd prime and α a primitive element in the finite field F_{p^n}. Let $M|p^n - 1$ and $\mathcal{S}_k$, $k = 0, 1, \ldots, M-1$, be the disjoint subsets of F_{p^n} defined by

$$\mathcal{S}_k = \{\alpha^{Mi+k} - 1 \mid 0 \le i < \frac{p^n - 1}{M}\}.$$

The M-ary Sidel'nikov sequence $s(t)$ of period $p^n - 1$ is defined as

$$s(t) = \begin{cases} k, & \text{if } \alpha^t \in \mathcal{S}_k, \quad 0 \le k \le M-1 \\ k_0, & \text{if } t = \frac{p^n-1}{2} \end{cases}$$

where k_0 is an integer in the set $\{0, 1, 2, \cdots, M-1\}$.

Note that $\alpha^{\frac{p^n-1}{2}} = -1$, $\bigcup_{k=0}^{M-1} \mathcal{S}_k = F_{p^n} \backslash \{-1\}$, and $0 \in \mathcal{S}_0$. Let N_k be the number of occurrences of k in one period of the Sidel'nikov sequence, i.e.,

$$N_k = |\{t \mid s(t) = k, \quad 0 \le t \le p^n - 2\}|.$$

If $k_0 \neq 0$, then we have

$$N_k = \begin{cases} \frac{p^n-1}{M}, & \text{if } k \neq 0, k_0 \\ \frac{p^n-1}{M} + 1, & \text{if } k = k_0 \\ \frac{p^n-1}{M} - 1, & \text{if } k = 0. \end{cases}$$

It is clear that $k_0 = 0$ yields perfectly balanced sequences.

The definition of M-ary Sidel'nikov sequences has close relation with the cyclotomic numbers of order M [12], which are defined as follows.

Definition 2: Let α be a primitive element in F_{p^n}. The cyclotomic classes C_u, $0 \le u \le M-1$, in F_{p^n} are defined as

$$C_u = \{\alpha^{Ml+u} \mid 0 \le l < \frac{p^n - 1}{M}\}.$$

For fixed positive integers u and v, not necessarily distinct, the cyclotomic number $(u, v)_M$ is defined as the number of elements $z_u \in C_u$ such that $1 + z_u \in C_v$.

We can represent the M-ary Sidel'nikov sequences using the indicator function and the multiplicative character of F_{p^n}.

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 multiplicative character of order M of F_{p^n} is defined as

$$\psi_M(\alpha^t) = e^{j\frac{2\pi t}{M}}, \quad \text{for } \alpha^t \in F_{p^n}^*$$

and

$$\psi_M(0) = 0$$

where α is a primitive element in F_{p^n}, $M|p^n - 1$, and $0 \le t \le p^n - 2$.

Then the M-ary Sidel'nikov sequence can be expressed as

$$\omega_M^{s(t)} = \omega_M^{k_0} I(\alpha^t + 1) + \psi_M(\alpha^t + 1). \tag{1}$$

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

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

Let N be a positive integer, and $a(t)$ and $b(t)$ binary sequences of period N. A quaternary sequence $q(t)$ is defined as $q(t) = \phi[a(t), b(t)]$. Then the sequence in the signal space corresponding to $q(t)$ can be represented by using the binary sequences, $a(t)$ and $b(t)$ [11] as

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

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

Lemma 5 (Krone and Sarwate [11]): 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 $R_{p,q}(\tau)$ between $p(t)$ and $q(t)$ is given as

$$R_{p,q}(\tau) = \frac{1}{2}\big\{R_{a,c}(\tau) + R_{b,d}(\tau) + \omega_4(R_{a,d}(\tau) - R_{b,c}(\tau))\big\}$$

where $R_{a,b}(\tau)$ is the cross-correlation function between $a(t)$ and $b(t)$.

III. Construction of New Quaternary Sequences

Using the reverse Gray mapping, we can construct a quaternary sequence with optimal autocorrelation from two binary Sidel'nikov sequences. Let $s_0(t)$ and $s_1(t)$ be the binary Sidel'nikov sequences with $k_0 = 0$ and $k_0 = 1$, respectively. Then $s_0(t)$ is a balanced sequence while there are two more ones than zeros in the sequence $s_1(t)$. The new quaternary sequence is defined as

$$q(t) = \phi[s_0(t), s_1(t + N/2)].$$

Then the autocorrelation distribution of $q(t)$ is determined as in the following theorem.

Theorem 6: The autocorrelation function of $q(t)$ is given as

$$R_q(\tau) = \begin{cases} p^n - 1, & \text{once} \\ -2, & \frac{p^n-1}{2} - 1 \text{ times} \\ -j2, & \frac{p^n-1}{4} \text{ times} \\ j2, & \frac{p^n-1}{4} \text{ times} \end{cases}$$

for $N = p^n - 1 \equiv 0 \bmod 4$ and

$$R_q(\tau) = \begin{cases} p^n - 1, & \text{once} \\ -2, & \frac{p^n-1}{2} \text{ times} \\ -j2, & \frac{p^n-3}{4} \text{ times} \\ j2, & \frac{p^n-3}{4} \text{ times} \end{cases}$$

for $N \equiv 2 \bmod 4$.

Proof: It is trivial that $R_q(0) = p^n - 1$. And thus, we have to prove the distribution of autocorrelation values for $\tau \neq 0$. From Lemma 5, the autocorrelation function of $q(t)$ can be rewritten as

$$\begin{aligned} R_q(\tau) &= \frac{1}{2}[R_{s_0}(\tau) + R_{s_1}(\tau)] + \frac{j}{2}[R_{s_0,s_1}(\tau + N/2) \\ &\quad - R_{s_1,s_0}(\tau - N/2)]. \end{aligned}$$

In [12], for $\tau \neq 0$, the autocorrelation functions, $R_{s_0}(\tau)$ and $R_{s_1}(\tau)$ are given as

$$\begin{aligned} R_{s_0}(\tau) &= \psi_2(-\alpha^\tau + 1) + \psi_2(-\alpha^{-\tau} + 1) - \psi_2(\alpha^{-\tau}) - 1 \\ R_{s_1}(\tau) &= -\psi_2(-\alpha^\tau + 1) - \psi_2(-\alpha^{-\tau} + 1) - \psi_2(\alpha^{-\tau}) - 1 \end{aligned}$$

and clearly $R_{s_0}(0) = R_{s_1}(0) = N$. Using $R_{s_0}(\tau)$ and $R_{s_1}(\tau)$, we can derive the cross-correlation function of $s_0(t)$ and $s_1(t)$ as

$$\begin{aligned} R_{s_0,s_1}\Big(\tau + \frac{N}{2}\Big) &= \sum_{t=0}^{N-1} (-1)^{s_0(t) - s_1(t+\tau+N/2)} \\ &= \sum_{t=0}^{N-1} \Big\{(-1)^{s_1(t)} + 2I(\alpha^t + 1)\Big\} (-1)^{-s_1(t+\tau+N/2)} \\ &= R_{s_1}(\tau + N/2) + 2(-1)^{s_1(\tau)} \\ &= R_{s_1}(\tau + N/2) + 2\left\{-I(\alpha^\tau + 1) + \psi_2(\alpha^\tau + 1)\right\}. \end{aligned}$$

For $\tau = N/2$, $R_{s_0,s_1}(\tau + N/2) = N - 2$ and for $\tau \neq N/2$, we have

$$R_{s_0,s_1}(\tau + N/2) = \psi_2(\alpha^\tau + 1) - \psi(\alpha^{-\tau} + 1) - \psi_2(-\alpha^{-\tau}) - 1.$$

Similarly, we have $R_{s_1,s_0}(\tau - N/2) = N - 2$ for $\tau = N/2$ and for $\tau \neq N/2$,

$$R_{s_1,s_0}(\tau - N/2) = -\psi_2(\alpha^\tau + 1) + \psi(\alpha^{-\tau} + 1) - \psi_2(-\alpha^{-\tau}) - 1.$$

Case 1) $p^n - 1 \equiv 0 \bmod 4$;

If $p^n - 1 \equiv 0 \bmod 4$, $\psi_2(-1) = \psi_2(\alpha^{(p^n-1)/2}) = 1$. Then we have

$$R_q(\tau) = -(\psi_2(\alpha^{-\tau}) + 1) + j[\psi_2(\alpha^\tau + 1) - \psi_2(\alpha^{-\tau} + 1)].$$

Since $\psi_2(\alpha^{-\tau} + 1) = \psi_2(\alpha^\tau + 1)/\psi_2(\alpha^\tau)$, for even $\tau \neq N/2$, we have

$$R_q(\tau) = -(1 + 1) + j[\psi_2(\alpha^\tau + 1) - \psi_2(\alpha^\tau + 1)] = -2$$

and clearly $R_q(N/2) = -2$. For odd τ, we have

$$\begin{aligned} R_q(\tau) &= -(-1 + 1) + j[\psi_2(\alpha^\tau + 1) + \psi_2(\alpha^\tau + 1)] \\ &= j2\psi_2(\alpha^\tau + 1). \end{aligned}$$

If, for odd τ, $\alpha^\tau + 1$ is a square in F_{p^n} then $R_q(\tau) = j2$ and otherwise, $R_q(\tau) = -j2$. Since the cyclotomic number of order 2 is given as $(0,0)_2 = (p^n - 5)/4$ and $(0,1)_2 = (1,0)_2 = (1,1)_2 = (p^n - 1)/4$ for $p^n - 1 \equiv 0 \bmod 4$ [13], the autocorrelation distribution is determined by

$$R_q(\tau) = \begin{cases} p^n - 1, & \text{once} \\ -2, & \frac{p^n-1}{2} - 1 \text{ times} \\ -j2, & \frac{p^n-1}{4} \text{ times} \\ j2, & \frac{p^n-1}{4} \text{ times.} \end{cases}$$

Case 2) $p^n - 1 \equiv 2 \bmod 4$;

If $p^n - 1 \equiv 2 \bmod 4$ and $\psi_2(-1) = \psi_2(\alpha^{(p^n-1)/2}) = -1$, then similarly for $\tau \neq N/2$ we have

$$R_q(\tau) = -(\psi_2(\alpha^{-\tau}) + 1) + j\Big[\psi_2(\alpha^\tau + 1) - \frac{\psi_2(\alpha^\tau + 1)}{\psi_2(\alpha^\tau)}\Big].$$

For even τ, we have

$$R_q(\tau) = -(1 + 1) + j[\psi_2(\alpha^\tau + 1) - \psi_2(\alpha^\tau + 1)] = -2,$$

and for odd $\tau \neq N/2$, we have

$$\begin{aligned} R_q(\tau) &= -(-1 + 1) + j[\psi_2(\alpha^\tau + 1) + \psi_2(\alpha^\tau + 1)] \\ &= j2\psi_2(\alpha^\tau + 1). \end{aligned}$$

It is easy to check that $R_q(N/2) = -2$. For odd $\tau \neq N/2$, if $\alpha^\tau + 1$ is a square then $R_q(\tau) = j2$ and if $\alpha^\tau + 1$ is a non-square, $R_q(\tau) = -j2$.

Since the cyclotomic number of order 2 is given as $(0,0)_2 = (1,0)_2 = (1,1)_2 = (p^n - 3)/4$ and $(0,1)_2 = (p^n + 1)/4$ for $p^n \equiv 3 \bmod 4$ [13], the autocorrelation distribution is given as

$$R_q(\tau) = \begin{cases} p^n - 1, & \text{once} \\ -2, & \frac{p^n-1}{2} \text{ times} \\ -j2, & \frac{p^n-3}{4} \text{ times} \\ j2, & \frac{p^n-3}{4} \text{ times.} \end{cases}$$

□

Example 7: For $p = 3$ and $n = 3$, we have $N = 26 \equiv 2 \bmod 4$. Then the binary Sidel'nikov sequences are given as

$$\begin{aligned} s_0(t) &= 11110110110000010011100010 \\ s_1(t) &= 11110110110001010011100010. \end{aligned}$$

Note that $h \equiv 1 \bmod 2$ because $s_{k_0}(0) = 1$. Then the quaternary sequence can be constructed as

$$s(t) = 23230221330101121022311030.$$

The number of occurrence of each symbol for the quaternary sequence $s(t)$ in a period is determined as

$$s(t) = \begin{cases} 0, & 6 \text{ times} \\ 1, & 7 \text{ times} \\ 2, & 7 \text{ times} \\ 3, & 6 \text{ times}. \end{cases}$$

The autocorrelation distribution of $s(t)$ is given as

$$R_s(\tau) = \begin{cases} 26, & \text{once at } \tau = 0 \\ 0, & \text{once at } \tau = 13 \\ -2, & 12 \text{ times} \\ -j2, & 6 \text{ times} \\ j2, & 6 \text{ times}. \end{cases}$$

REFERENCES

[1] H. D. Lüke, H. D. Schotten, and H. Hadinejad-Mahram, "Generalised Sidelnokov sequences with optimal autocorrelation properties," *Electron. Lett*, vol. 36, no. 6, pp. 525–527, Mar. 2000.

[2] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science, 1998.

[3] 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.

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

[5] 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.

[6] J.-S. No, H. Chung, H.-Y. Song, K. Yang, J.-D. Lee, and T. Helleseth, "New construction for binary sequences of period $p^m - 1$ with optimal autocorrelation using $(z+1)^d + az^d + b$," *IEEE Trans. inf. Theory,* vol. 47, no. 4, pp. 1638–1644, May 2001.

[7] H. D. Lüke, 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.

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

[10] Ji-Woong Jang, Young-Sik Kim, and Sang-Hyo Kim, "On the optimality of autocorrelation for quaternary sequences," in preparation.

[11] 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.

[12] 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.

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

[14] W. H. Mow, "A unified construction of perfect polyphase sequences," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'95)*, Whistler, Canada, 1995, p. 459.