New Binary Sequences of Length 4p with Optimal Autocorrelation Magnitude *

Yuan Sun † *Hao Shen*
Department of Mathematics
Shanghai Jiaotong University
Shanghai 200240 China

Abstract: In this paper, we construct a new infinite family of balanced binary sequences of length $N = 4p$, $p \equiv 5 \pmod 8$ with optimal autocorrelation magnitude $\{N, 0, \pm 4\}$.

Key words: periodic autocorrelation function,binary sequence, optimal autocorrelation magnitude, merit factor.

1 Introduction

Let N be a natural number. Given a binary (0 and 1) sequence $s = \{s(t)|0 \le t < N\}$, the periodic autocorrelation function (PACF) of s at shift ω is defined by

$$\varphi_s(\omega) = \sum_{t=0}^{N-1} (-1)^{s((t+\omega) \mod N) - s(t)} \qquad \omega = 0, 1, 2, \cdots, N-1. \qquad (1)$$

It is implies that $\varphi_s(\omega) = N$ occurs the only at $\omega = 0$. If its autocorrelation $\varphi_s(\omega) = 0$ for $\omega = 1, 2, \cdots, N-1$, then s is called a perfect binary sequence. For binary sequences, only known perfect sequence is $s = \{0, 0, 0, 1\}$ of length 4 [10]. s is called balanced if $|\{t|s(t) = 1, 0 \le t < N\}| = |\{t|s(t) = 0, 0 \le t < N\}|$.

Binary sequences with good autocorrelation play important roles in communication systems employing phase-reversal modulation techniques and cryptography. For binary sequences of even length N, Lempel,Cohn

*Project supported by National Natural Science Foundation of China under Grant No. 10471093.

†sunyuan@sjtu.edu.cn

and Eastman [6] showed that *i)* the autocorrelation must have at least two distinct out-of-phase values and *ii)* any two autocorrelation valued is divisible by 4. If $N \equiv 2 \pmod 4$, therefore, optimal autocorrelation is $\{N, 2, -2\}$ and if $N \equiv 0 \pmod 4$, it is $\{N, 0, 4\}$ or $\{N, 0, -4\}$.

Several classes of binary sequences of even length with optimal autocorrelation are known. First, Lempel, Cohn and Eastman [6] presented a class of the balanced binary sequences of length $N = p^a - 1$, where p is an odd prime. In [3], Ding, Helleseth and Martinsen presented several families of binary sequences of length $N = 2p$ for odd prime $p \equiv 5 \pmod 8$ which correspond to almost difference sets. Using known cyclic difference sets, Arasu, Ding, Helleseth, Kumer and Martinsen [1] construct four classes of almost difference sets which give inequivalent classes of binary sequences of length $N \equiv 0 \pmod 4$. These sequences generally contain the binary sequences of length $N \equiv 0 \pmod 4$ constructed from the product method in [7].

For $N \equiv 0 \pmod 4$, the PACF of $\{N, 0, 4\}$ or $\{N, 0, -4\}$ is optimal from the Lempel, Cohn and Eastman's assertion in sense that it has two out-of-phase values with the smallest magnitude. In [11], if $\varphi_s(\omega) \in \{N, 0, \pm 4\}$ for $N \equiv 0 \pmod 4$, N.Y. Yu and G Gong consider that it is also optimal in the sense that its autocorrelation magnitude is identical to that of $\{N, 0, 4\}$ or $\{N, 0, -4\}$. If the out-of-phase values with the smallest magnitudes are allowed, the optimal autocorrelation should be $\{N, 0, -4, 4\}$, where the autocorrelation is optimal with respect to its magnitude. In practical applications, it should be the same meaning as conventional optimal autocorrelation.

When $N \equiv 0 \pmod 4$, there are several classes of known optimal binary sequences with $\varphi_s(\omega) \in \{N, 0, \pm 4\}$ are : the first class is the generalized Sidelnikov sequences S_1 of length $q^a - 1 \equiv 0 \pmod 4$, where q is an odd prime and $a = 1, 2, \cdots$, constructed by H.D. Lüke, H.D. Schotten and H. Hadinejad-Mahram [8]. The other two classes of the sequences resulting from the periodic product of the L_1 of length p_3 and the m-sequences M of length $2^a - 1$ [5] with the perfect binary sequence $s' = (1, 1, 1, -1)$ are denoted by $\Pi(L_1, 4) = \{L_1, L_1, L_1, -L_1\}$ of length $4p_3$ and $\Pi(m, 4) = \{M, M, M, -M\}$ of length $4(2^a - 1)$, respectively, where L_1 is gotten from a Legendre sequence L of length p_3 by replacing the leading zero by 1, $p_3 \equiv 3 \pmod 4$ and $a = 1, 2, \cdots$.

N.Y.Yu and G.Gong [11] gave new binary sequences of length $4(2^a - 1)$ for even $a \geq 4$ is optimal with respect to autocorrelation magnitude .

In this paper, we give a new family of the balanced binary sequences s of length $N = 4p$ with optimal autocorrelation magnitude $\varphi_s(\omega) \in \{0, \pm 4\}$ for $\omega = 1, 2, \cdots, N - 1$, where p is always a prime of form $4f + 1$, f is odd and has a quadratic partition of form $x^2 + 4$.

Let C be a subset of Z_N, we define the characteristic sequence s of C

as

$$s(t) = \begin{cases} 1 & \text{if } t \in C \\ 0 & \text{otherwise} \end{cases}$$

C is also called the support of s. The difference function of C at shift ω is defined as

$$d_C(\omega) = |(\omega + C) \cap C| \qquad \omega \in Z_N$$

The relationship between the PACF of s at shift ω and the difference function of C at shift ω is

Lemma 1 [2] *Let s be a binary sequence of length N, then*

$$\varphi_s(\omega) = N - 4(|C| - d_C(\omega)) \qquad \omega \in Z_N.$$

Let $GF(p)$ be the finite field of order p. The *cyclotomic classes* of order 4 in $GF(p)$ are $D_i^{(4,p)} = \{\alpha^{i+4j} | 0 \le j \le f-1\}$, $0 \le i \le 3$, where α is a primitive element of $GF(p)$. To simplify notation, we define $D_i = D_i^{(4,p)}$. The *cyclotomic numbers* of order 4 are defined as $(i,j) = |(D_i + 1) \cap D_j| \quad 0 \le i,j \le 3$.

When $p = 4f + 1 = x^2 + 4$ be a prime, where f is odd and $x \equiv 1 \pmod 4$. There are at most five distinct cyclotomic numbers of order 4 [2] which are

$(0,0) = (2,2) = (2,0) = \frac{p-7+2x}{16}$

$(0,1) = (1,3) = (3,2) = \frac{p+1+2x-8y}{16}$

$(0,2) = \frac{p+1-6x}{16}$

$(1,2) = (0,3) = (3,1) = \frac{p+1+2x+8y}{16}$

$(1,0) = (1,1) = (2,1) = (2,3) = (3,0) = (3,3) = \frac{p-3-2x}{16}$

Here $y = 1$ or -1, depending on the choice of the primitive element α employed to define the cyclotomic classes of order 4 [4].

2 New binary sequences with optimal autocorrelation magnitude

Our construction over Z_N is based on the Chinese Remainder Theorem (CRT) and the cyclotomic classes.

Since $(4,p) = 1$, by the CRT we have $Z_N \cong Z_4 \times Z_p \quad \omega \mapsto (\omega_1, \omega_2)$, where $\omega_1 \equiv \omega \bmod 4$, $\omega_2 \equiv \omega \bmod \text{p}$. The construction over Z_N is equivalent to the construction over $Z_4 \times Z_p$.

We are going to construct the balanced binary sequences of length $N = 4p$ with optimal autocorrelation magnitude now.

Let C_i be the union of two different cyclotomic classes of order 4, $0 \le i \le 3$. $G \subseteq Z_4$, $|G| = 2$. $C = (\{0\} \times C_0) \cup (\{1\} \times C_1) \cup (\{2\} \times C_2) \cup (\{3\} \times C_3) \cup (G \times \{0\})$.

When $\omega_2 = 0$, $\omega = (\omega_1, 0) \in Z_4 \times Z_p$, the difference function of C at shift ω is

$$d_C(\omega_1,0) = \begin{cases} |C_0|+|C_1|+|C_2|+|C_3|+2 \\ \qquad \omega_1 = 0 \\ |C_0\cap C_1|+|C_1\cap C_2|+|C_2\cap C_3|+|C_3\cap C_0| \\ \qquad \omega_1 = 1 \text{ or } 3 \quad G=\{0,2\} \text{ or } \{1,3\} \\ |C_0\cap C_1|+|C_1\cap C_2|+|C_2\cap C_3|+|C_3\cap C_0|+1 \\ \qquad \omega_1 = 1 \text{ or } 3 \quad G=\{1,2\} \text{ or } \{2,3\} \text{ or } \\ \qquad\qquad \{3,0\} \text{ or } \{0,1\} \\ 2|C_0\cap C_2|+2|C_1\cap C_3|+2 \\ \qquad \omega_1 = 2 \qquad G=\{0,2\} \text{ or } \{1,3\} \\ 2|C_0\cap C_2|+2|C_1\cap C_3| \\ \qquad \omega_1 = 2 \qquad G=\{1,2\} \text{ or } \{2,3\} \text{ or } \\ \qquad\qquad \{3,0\} \text{ or } \{0,1\} \end{cases}$$

where $|C| = d_C(0,0) = |C_0|+|C_1|+|C_2|+|C_3|+2$.

From Lemma 1 and $\varphi_s(\omega) \in \{0, \pm 4\}$, $\omega = 1, 2, \cdots, N-1$, we have

$$d_C(\omega_1, 0) \in \{p-1\ ,\ p\ ,\ p+1\} \tag{2}$$

Since the sequence s of length $4p$ is balanced, then $|C| = 2p$,

$$|C_0|+|C_1|+|C_2|+|C_3| = 2p-2 \tag{3}$$

From (2) and (3), there are four possible cases for (C_0, C_1, C_2, C_3) and G as below:

1: $(\{D_l, D_m\}, \{D_l, D_k\}, \{D_m, D_n\}, \{D_l, D_m\})$,
$G = \{0,2\}$ or $\{1,3\}$.

2: $(\{D_l, D_m\}, \{D_l, D_m\}, \{D_l, D_n\}, \{D_m, D_k\})$,
$G = \{0,2\}$ or $\{1,3\}$.

3: $(\{D_l, D_n\}, \{D_l, D_m\}, \{D_l, D_m\}, \{D_m, D_k\})$,
$G = \{0,2\}$ or $\{1,3\}$.

4: $(\{D_l, D_n\}, \{D_m, D_k\}, \{D_l, D_m\}, \{D_l, D_m\})$,
$G = \{0,2\}$ or $\{1,3\}$.

where (l,m,n,k) is an arrangement of 0,1,2,3. (l,m,n,k) is usually called the defining set of the binary sequence s.

We only consider Case 1 . The other cases are similar to it.

Let $C_0 = D_l \cup D_m \quad C_1 = D_l \cup D_k \quad C_2 = D_m \cup D_n \quad C_3 = D_l \cup D_m$.

When $\omega_2 = 0$, we have

$$d_C(\omega_1,0) = \begin{cases} 2p & \omega_1 = 0 & \text{and } G=\{0,2\} \text{ or } \{1,3\} \\ p-1 & \omega_1 = 1 \text{ or } 3 & \text{and } G=\{0,2\} \text{ or } \{1,3\} \\ p+1 & \omega_1 = 2 & \text{and } G=\{0,2\} \text{ or } \{1,3\} \end{cases} \tag{4}$$

When $\omega_2 \neq 0$, we have $|(C_i+\omega_2)\cap C_j| = |(\omega_2^{-1}C_i+1)\cap \omega_2^{-1}C_j|$.

Let $L_C(\omega_1, \omega_2) =$

$$\sum_{i=0}^{3}(|G\times\{0\}\cap(i+\omega_1, C_i+\omega_2)| + |(i, C_i)\cap(G\times\{0\}+(\omega_1,\omega_2))|)$$

$$M_C(\omega_1,\omega_2) = \sum_{i=0}^{3} |C_i \cap (C_{i-\omega_1} + \omega_2)|$$
$$= \sum_{i=0}^{3} |\omega_2^{-1} C_i \cap (\omega_2^{-1} C_{i-\omega_1} + 1)|$$

then $d_C(\omega_1,\omega_2) = L_C(\omega_1,\omega_2) + M_C(\omega_1,\omega_2)$.

If $\omega_2^{-1} \in D_h$, $0 \le h \le 3$, then $M_C(\omega_1,\omega_2)$ equals a sum of cyclotomic numbers of order 4 as below

$$\begin{aligned}
M_C(0,\omega_2) &= 3(l+h,l+h) + 2(l+h,m+h) \\
&\quad +(l+h,k+h) + 2(m+h,l+h) \\
&\quad +3(m+h,m+h) + (m+h,n+h) \\
&\quad +(n+h,m+h) + (n+h,n+h) \\
&\quad +(k+h,l+h) + (k+h,k+h) \\
M_C(1,\omega_2) &= 2(l+h,l+h) + 2(l+h,m+h) \\
&\quad +(l+h,n+h) + (l+h,k+h) \\
&\quad +3(m+h,l+h) + 2(m+h,m+h) \\
&\quad +(m+h,k+h) + (n+h,l+h) \\
&\quad +(n+h,m+h) + (k+h,m+h) \\
&\quad +(k+h,n+h) \\
M_C(2,\omega_2) &= 2(l+h,l+h) + 2(l+h,m+h) \\
&\quad +(l+h,n+h) + (l+h,k+h) \\
&\quad +2(m+h,l+h) + 2(m+h,m+h) \\
&\quad +(m+h,k+h) + (m+h,n+h) \\
&\quad +(n+h,l+h) + (n+h,m+h) \\
&\quad +(k+h,m+h) + (k+h,l+h) \\
M_C(3,\omega_2) &= 2(l+h,l+h) + 3(l+h,m+h) \\
&\quad +2(m+h,l+h) + (l+h,n+h) \\
&\quad +2(m+h,m+h) + (m+h,n+h) \\
&\quad +(m+h,k+h) + (n+h,l+h) \\
&\quad +(n+h,k+h) + (k+h,l+h) \\
&\quad +(k+h,m+h)
\end{aligned}$$

Therefore, we have

Lemma 2 *For $(l,m,n,k) = (0,1,2,3)$, $G = \{0,2\}$ or $\{1,3\}$ and $\omega_2^{-1} \in D_h$, we have*

$$L_C(\omega_1,\omega_2) = 2 \qquad 0 \le \omega_1 \le 3, h = 0,1,2,3$$

$$M_C(\omega_1,\omega_2) = \begin{cases} p-3 & \omega_1 = 0, h = 0,1,2,3 \\ p-2-y & \omega_1 = 1 \text{ or } 3\ ,\ h = 0 \text{ or } 2 \\ p-2 & \omega_1 = 2, h = 0,1,2,3 \\ p-2+y & \omega_1 = 1 \text{ or } 3\ ,\ h = 1 \text{ or } 3 \end{cases}$$

then

$d_C(\omega_1,\omega_2) = L_C(\omega_1,\omega_2) + M_C(\omega_1,\omega_2)$

$$= \begin{cases} p-1 & \omega_1 = 0, h = 0,1,2,3 \\ p-y & \omega_1 = 1 \text{ or } 3 \ , \ h = 0 \text{ or } 2 \\ p & \omega_1 = 2, h = 0,1,2,3 \\ p+y & \omega_1 = 1 \text{ or } 3 \ , \ h = 1 \text{ or } 3 \end{cases} \quad (5)$$

Since the evaluation of $d_C(\omega_1, \omega_2)$ is straightforward but tedious, we omit the results which are similar to Lemma 2.

Now we have the main result from (4) and (5)

Theorem 1 *Let $p = 4f + 1 = x^2 + 4y^2$ be a prime, where f is odd and $y = 1$ or -1. If $(l, m, n, k) \in A = \{(0,1,2,3),$ $(0,3,2,1), (2,3,0,1), (1,0,3,2), (1,2,3,0), (2,1,0,3), (3,0,1,2),$ $(3,2,1,0)\}$ and $G \in \{\{0,2\}, \{1,3\}\}$, then balanced binary sequence s of length $N = 4p$ has optimal autocorrelation magnitude $\max_{\omega \neq 0(\mathrm{modN})} |\varphi_s(\omega)| = 4$.*

Proof: For $(l, m, n, k) \in A$ and $G = \{0, 2\}$ or $\{1, 3\}$. From Lemma 2, when $y = 1$ or -1, if $\omega = (\omega_1, \omega_2) \neq (0, 0)$, then $d_C(\omega_1, \omega_2) \in \{p-1\ ,\ p\ ,\ p+1\}$.

From Lemma 1, we have

$$\begin{aligned} \varphi_s(\omega) &= N - 4(|C| - d_C(\omega)) \\ &= -4p + 4d_C(\omega) \\ &\in \{\ -4\ ,\ 0\ ,\ 4\ \} \end{aligned}$$

then $\max_{\omega \neq 0(\mathrm{modN})} |\varphi_s(\omega)| = 4.$ □

Example : Let $p = 5 = 1 + 4 \times 1^2$, and $N = 4p = 20$. We use the primitive element 2 in $GF(5)$ to define the cyclotomic classes,and y=1. Then $D_0 = \{1\}$, $D_1 = \{2\}$, $D_2 = \{4\}$, $D_3 = \{3\}$. Let (l, m, n, k)=(0,1,2,3) and $G = \{0, 2\}$. Then $C_0 = \{1, 2\}$, $C_1 = \{1, 3\}$, $C_2 = \{2, 4\}$, $C_3 = \{1, 2\}$. The corresponding balanced binary sequence is

$$s = 11100001001111101000$$

The autocorrelation functions are
$\varphi_s(0) = 20$ $\varphi_s(1) = 4$ $\varphi_s(2) = 0$ $\varphi_s(3) = -4$ $\varphi_s(4) = -4$
$\varphi_s(5) = -4$ $\varphi_s(6) = 0$ $\varphi_s(7) = -4$ $\varphi_s(8) = -4$ $\varphi_s(9) = 4$
$\varphi_s(10) = 4$ $\varphi_s(11) = 4$ $\varphi_s(12) = -4$ $\varphi_s(13) = -4$ $\varphi_s(14) = 0$
$\varphi_s(15) = -4$ $\varphi_s(16) = -4$ $\varphi_s(17) = -4$ $\varphi_s(18) = 0$
$\varphi_s(19) = 4$.

Therefore, we have $\max_{\omega \neq 0(\mathrm{modN})} |\varphi_s(\omega)| = 4$.

At last, we consider the asymptotic merit factor MF_∞ which is defined in [9] as

$$\mathrm{MF}_\infty = \mathrm{N} \lim_{\mathrm{N} \to \infty} \frac{\mathrm{MF}}{\mathrm{N}}$$

It is easy to prove

Theorem 2 *The asymptotic merit factor of balanced binary sequences constructed in Theorem 1 is*

$$\mathrm{MF}_{\infty} = \frac{\mathrm{N}}{12}$$

3 The Concluding Remark

In this paper, we constructed a new family of balanced binary sequences of length $N = 4p$ with $\max_{\omega \neq 0(\mathrm{mod N})} |\varphi_s(\omega)| = 4$, where $p \equiv 5 (\mathrm{mod}\ 8)$ is a prime. It is important to note that the family of sequences constructed in Theorem 1 are different from those described in the introduction, as some integers $4p$ are not in form $q^a - 1$ or $4p_3$ or $4(2^a - 1)$, where q is an odd prime, $p_3 \equiv 3$ (mod 4) and $a \geq 1$ is an integer.

prime $p \equiv 5$ (mod8)	5	13	29	53	173	229
length $N = 4p$	20*	52	116*	212*	692*	916*

There are some length N marked with * above are not form $q^a - 1$.

References

[1] K.T. Arasu, C. Ding, T. Helleseth, P.V. Kumer, and H. Martinsen, Almost difference sets and their sequences with optimal autocorrelation ,*IEEE Trans. Inform. Theory* vol.47, pp.2934–2943, 2001.

[2] T. W. Cusick, C. Ding, and A. Renvall,*Stream Ciphers and Number Theory*(North-Holland Mathematical Library, vol. 55). Amsterdam, The Netherlands: North-Holland/Elsevier, 1998.

[3] C. Ding, T. Helleseth and H. Martinsen, New Families of Binary Sequences with Optimal Three-Level Autocorrelation. *IEEE Trans. Inform. Theory,* vol. 47, pp. 428-433, Jan. 2001.

[4] L. E. Dickson, Cyclotomy, higher congruences, and Warings problem, Amer. J. Math. 57, 391-424, and 463-474, 1935.

[5] S.W.Golomb, Ed, *Digital Communications With Space Applications.* Englewood Cliffs, NJ: Prentice-Hall, 1964.

[6] A. Lempel, M. Cohn, and W. L. Eastman, A class of binary sequences with optimal autocorrelation properties, *IEEE Trans. Inform. Theory,* vol. IT-23, pp.38-42, Jan. 1977.

[7] H.D. Lüke, Sequences and arrays with perfect periodic autocorrelation. *IEEE Trans. Aerosp. Electron. Syst.* vol. 24, no. 3, pp. 287-294, May 1988.

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

[9] H.D. Lüke, H.D. Schotten, and H. H. Mahram.Binary and quadriphase sequences with optimal autocorrelation properties: A survey . *IEEE Trans. Inform. Theory,* vol. 49, pp.3271-3282, 2003.

[10] B. Schmidt. Cyclotomic integers and finite geomerty, *J.Amer. Math. Soc.,* vol. 12, pp.929-952, 1999.

[11] N.Y. Yu and G Gong , Interleaved Construction of Binary Sequences with Optimal Autocorrelation Magnitude.*Proceedings of IEEE Information Theory Workshop* pp. 530-534, 2006.