Even Length Binary Sequence Families with Low Negaperiodic Autocorrelation

Matthew G. Parker

Code Theory Group, Inst. for Informatikk, HIB,
University of Bergen, Norway
E-mail: matthew@ii.uib.no,
Web: http://www.ii.uib.no/∼matthew/MattWeb.html

Abstract. Cyclotomic constructions are given for several infinite families of even length binary sequences which have low negaperiodic autocorrelation. It appears that two of the constructions have asymptotic Merit Factor 6.0 which is very high. Mappings from periodic to negaperiodic autocorrelation are also discussed.

1 Introduction

The Periodic Autocorrelation Function (PACF) of a length N binary sequence, $s(t)$, is,

$$P_s(\omega) = \sum_{t=0}^{N-1} (-1)^{s(t+\omega)-s(t)}, \qquad 0 \leq \omega < N \tag{1}$$

where sequence indices, t, are taken mod N. $s(t)$ has optimal PACF when $|P_s(\omega)| = 1$ if N is odd. For N even, the PACF of $s(t) = 0001$ is $4, 0, 0, 0$, which is perfect as $P_s(\omega) = 0$, $\forall \omega \neq 0$. But, for N even, $N > 4$, it is conjectured (but not proven) that there is no binary $s(t)$ with perfect PACF. If this conjecture is true then, for N even, $N > 4$, binary $s(t)$ such that $\min_{s(t)}(\max_{1 \leq \omega < N} |P_s(\omega)|) = 2$ (4) has best possible PACF, for $4 \not| N$ ($4|N$), respectively. However, when $s(t)$ is balanced (an equal number of zeros and ones) or almost-balanced ($|\#\text{zeroes} - \#\text{ones}| = 1$) proof of optimality is possible. A recent paper [1] used cyclotomy to construct infinite [1] balanced (almost-balanced) binary sequence families of length $N = 2p$, for certain p prime, with optimal PACF. In this paper we consider the Negaperiodic Autocorrelation Function (NACF) of $s(t)$,

$$Q_s(\omega) = \sum_{t=0}^{N-1} (-1)^{s(t+\omega)-s(t)-\lfloor \frac{t+\omega}{N} \rfloor}, \qquad 0 \leq \omega < N \tag{2}$$

where sequence indices, t, are taken, mod N. For example, the NACF of $s(t) = 110101$ is $Q_s(\omega) = 6, -4, 2, 0, -2, 4$. Binary $s(t)$ has optimal NACF when $|Q_s(\omega)| =$

[1] 'infinite' means there is no upper limit on N for which the construction is valid.

1, $\forall\omega \neq 0$, if N is odd. For even N the NACF of $s(t) = 01$ is $2, 0$ which is perfect as $Q_s(\omega) = 0$, $\forall\omega \neq 0$. But for N even, $N > 2$, we conjecture (but cannot prove) that there is no binary $s(t)$ with perfect NACF. If this conjecture is true then, for N even, $N > 2$, binary $s(t)$ such that $\min_{s(t)}(\max_{1\leq\omega<N} |Q_s(\omega)|) = 2$, has best possible NACF. We provide constructions for such 'conjectured optimal' sequences, $s(t)$, in Theorems 1 and 2, where $s(t)$ is not necessarily balanced or almost-balanced. [2] We can always define an odd-length binary sequence, $e(t)$, such that $e(t) = s(t) + t \pmod 2$, where $Q_e(\omega) = (-1)^\omega P_s(\omega)$ (Lemma 2), so low odd-length N PACF constructions trivially map to low odd-length N NACF constructions. However most even-length sequences with low NACF cannot be trivially derived from even-length sequences with known PACF, although we do review some useful mappings in Section 5. In this paper cyclotomy is used to construct binary sequence families of even length $N = 2p$ ($N = 4p$) with low NACF for certain p prime. Unlike the sequences of [1], the sequences of this paper are not necessarily balanced or almost-balanced. Sequences with low NACF can be used in spread-spectrum systems in a similar way to sequences with low PACF, and for comparable complexity [9]. The Aperiodic Autocorrelation Function (AACF) of a length N binary sequence, $s(t)$, is,

$$A_s(\omega) = \sum_{t=0}^{N-1} (-1)^{s(t+\omega)-s(t)}, \qquad -N < \omega < N \tag{3}$$

where $s(t) = 0$ for $t < 0$ or $t \geq N$. AACF is the sum and difference of PACF and NACF:

$$\begin{array}{ll} A_s(\omega) = \frac{1}{2}(P_s(\omega) + Q_s(\omega)), & 0 \leq \omega < N \\ A_s(\omega) = \frac{1}{2}(P_s(N-\omega) - Q_s(N-\omega)), & -N \leq \omega < 0 \end{array} \tag{4}$$

where $|A_s(\omega)| = |A_s(-\omega)|$. It is a well-known open problem to identify lowest possible values of $|A_s(\omega)|$ for a length N sequence, s. 'Golay Merit Factor' (MF) [8] is a common metric used to measure aperiodic optimality of a sequence and is given by,

$$M_s = \frac{N^2}{2\sum_{\omega=1}^{N-1} |A_s(\omega)|^2} \tag{5}$$

Lower values of $|A_s(\omega)|$ give higher MF. The highest MF for a given length N binary sequence is not known in general. The asymptote, $M_s = 6.0$, $N \to \infty$ is the highest known asymptote for a sequence, s, belonging to an infinite family of binary sequences, where the construction is a cyclic shift (cyclically shifted by approximately $N/4$) of a Legendre or Modified-Jacobi sequence [7, 8], although Golay has constructed skewsymmetric binary sequences with MFs generally between 8.00 and 9.00 [3–5] up to lengths $N = 100$ or so. [3]

[2] Computations show that binary $s(t)$ satisfying $\min_{s(t)}(\max_{1\leq\omega<N} |Q_s(\omega)|) = 2$ exist for all even N up to $N = 38$. This is in contrast to PACF when $4|N$, where computations suggest $\min_{s(t)}(\max_{1\leq\omega<N} |P_s(\omega)|) = 4$.

[3] The Rudin-Shapiro-based constructions [2, 6, 11, 10], achieve PACF and NACF upper bounds which appear to be asymptotically of the same order, leading to an asymptotic MF of 3.0.

This paper shows, experimentally, that the constructions of Theorems 1 and 2 also approach $M_s = 6.0$ as $N \to \infty$, and Section 5 argues that this is because these constructions are closely related to Legendre sequences.

2 Construction

Instead of constructing a length N sequence $s(t)$, we construct a length $2N$ sequence $s'(t)$, where $s'(t) = s(t)$, $0 \le t < N$, $s'(t) = s(t) + 1 \pmod 2$, $N \le t < 2N$. The NACF of $s(t)$ and the PACF of $s'(t)$ are related as follows,

$$Q_s(\omega) = \frac{1}{2} P_{s'}(\omega), \qquad 0 \le \omega < N$$

For example, if $s'(t) = 11010111110010100000$ then $s(t) = 1101011111$.
$P_{s'}(\omega) = 20, 0, 4, 0, -4, 0, 4, 0, -4, 0, -20, 0, -4, 0, 4, 0, -4, 0, 4, 0$, so
$Q_s(\omega) = 10, 0, 2, 0, -2, 0, 2, 0, -2, 0$. The constructing method uses cyclotomy, as in [1], to specify a subset C of Z_{2N} to define the characteristic sequence $s'(t)$ of C:

$$s'(t) = \begin{cases} 1, & \text{if } t \in C \\ 0, & \text{otherwise} \end{cases}$$

The PACF is determined by the difference function,

$$d_C(\omega) = |C \cap (C + \omega)|$$

where $C + \omega$ denotes the set $\{c + \omega : c \in C\}$ and '+' denotes addition, mod $2N$. The PACF of $s'(t)$ is then,

$$P_{s'}(\omega) = 2N - 4(|C| - d_C(\omega)) \tag{6}$$

This paper gives constructions for $N = 2p$ and $N = 4p$, p prime. We therefore specify C over Z_{4p} and Z_{8p}. By the Chinese Remainder Theorem (CRT), Z_{rp} is isomorphic to $Z_r \times Z_p$, $\gcd(r, p) = 1$. For $N = rp$, let $C' = \{\{n\} \times C_n \mid C_n \subseteq Z_p^*, 0 \le n < r\}$, $F = \{G \times 0 \mid G \subseteq Z_r\}$, and $C = C' \cup F$. Define $\omega = (\omega_1, \omega_2) \in Z_r \times Z_p$. Then,

$$\begin{aligned} d_C(\omega_1, \omega_2) = {} & |C \cap (C + (\omega_1, \omega_2))| \\ & = \textstyle\sum_{k=0}^{r-1} \sum_{n=0}^{r-1} |C_n \cap (C_{k-w_1} + w_2)| \\ & + |G \cap (G + (w_1, 0))| + \textstyle\sum_{k=0}^{r-1} |G \cap (k + w_1, C_k + w_2)| + \\ & + \textstyle\sum_{k=0}^{r-1} |(k, C_k) \cap (G + (w_1, w_2))| \end{aligned} \tag{7}$$

From (7) we see that if we know $|C_n \cap (C_m + \omega_2)|$, $\forall n, m, \omega_2 \in Z_p$, and if we can also determine the last three terms involving G, then we can determine $d_C(\omega_1, \omega_2) = d_C(\omega)$, $\forall \omega$, and hence the PACF of $s'(t)$. If we construct C_n from the union of various cyclotomic classes over GF(p), $\forall n$, then $|C_n \cap (C_m + \omega_2)|$ is computable from the cyclotomic numbers over GF(p). Let D_i be the cyclotomic class of order d, given by,

$$D_i = \{\alpha^i, \alpha^{d+i}, \alpha^{2d+i}, \alpha^{3d+i}, \ldots, \alpha^{p-1-d+i}\}, \qquad 0 \le i < d$$

where α is a primitive generator over GF(p). Then the cyclotomic number $[i,j]$ of order d over GF(p) is,

$$[i,j] = |(D_i + 1) \cap D_j| \tag{8}$$

Note that $|C_n \cap (C_m + w_2)| = |w_2^{-1} C_n \cap (w_2^{-1} C_m + 1)|$, (mod p), for $w_2 \neq 0$. If $C_n = \bigcup_{k \in T_n} D_k$, $T_n \subseteq Z_r$, and $w_2^{-1} \in D_h$, then $w_2^{-1} C_n = \bigcup_{k \in T_n} D_{k+h}$. Therefore,

$$|w_2^{-1} C_n \cap (w_2^{-1} C_m + 1)| = |(\bigcup_{k \in T_n} D_{k+h}) \cap (\bigcup_{k \in T_m} D_{k+h} + 1)| = \sum_{k \in T_n} \sum_{j \in T_m} [k+h, j+h] \tag{9}$$

i.e. a sum of cyclotomic numbers. We later use cyclotomic numbers to prove the NACF of some of the sequences we construct.
Example 1: $s'(t)$ is described by C comprising F and the C_n which are, in turn, the union of various D_i of order d. Let $2N = rp = 4p$, $d = 2$, and $C_0 = D_0$, $C_1 = D_0$, $C_2 = D_1$, $C_3 = D_1$. Let $G = \{1, 2\}$. Then, for $p = 13$ we can choose $\alpha = 2$ to give $D_0 = \{1, 4, 3, 12, 9, 10\}$ and $D_1 = \{2, 8, 6, 11, 5, 7\}$. Thus, using the CRT, mod 52, we construct the sets, $F = \{13, 26\}$, and,

$$(0, C_0) = \{40\{1, 4, 3, 12, 9, 10\}\} \qquad (1, C_1) = \{13 + 40\{1, 4, 3, 12, 9, 10\}\}$$
$$(2, C_2) = \{26 + 40\{2, 8, 6, 11, 5, 7\}\} \quad (3, C_3) = \{39 + 40\{2, 8, 6, 11, 5, 7\}\}$$

Then $C = (0, C_0) \cup (1, C_1) \cup (2, C_2) \cup (3, C_3) \cup F =$
$\{1, 2, 4, 6, 7, 9, 11, 12, 13, 15, 16, 17, 18, 19, 25, 26, 29, 31, 34, 36, 40, 46, 47, 48, 49, 50\}$.
Therefore, $s'(t) = 0110101101011101111100000110010100101000100000111110$, and

$$P_{s'}(\omega) = 52, 0, 4, 0, -4, 0, 4, 0, -4, 0, 4, 0, -4, 0, 4, 0, -4, 0, 4, 0, -4, 0, 4, 0, -4, 0,$$
$$-52, 0, -4, 0, 4, 0, -4, 0, 4, 0, -4, 0, 4, 0, -4, 0, 4, 0, -4, 0, 4, 0, -4, 0, 4, 0$$

Finally, the first half of $s'(t)$ is $s(t) = 01101011010111011111000001$, and,

$$Q_s(\omega) = 26, 0, -2, 0, 2, 0, -2, 0, 2, 0, -2, 0, 2, 0, -2, 0, 2, 0, -2, 0, 2, 0, -2, 0, 2, 0$$

Example 1 highlights the following restriction.

Lemma 1. *For $s'(t)$ to satisfy $s'(t + N) = s'(t) + 1 \pmod 2$, $0 \leq t < N$, we require that, if $C_n = \bigcup_{i \in T_n} D_i$ $T_n \subseteq Z_d$, then $C_{n+\frac{r}{2}} = \bigcup_{i \notin T_n} D_i$. Moreover, if $j \in G$ ($\notin G$), then $j + \frac{r}{2} \pmod r \notin G$, ($\in G$).*

From Lemma 1 it is sufficient to describe $s(t)$ by defining C_n for $0 \leq n < \frac{r}{2}$, and by defining $G' \subset Z_{\frac{r}{2}}$, where $G' = \{g \mid g \in G, g < \frac{r}{2}\}$.
A Compact Description for $s(t)$: $s(t)$ is compactly described by $\mathbf{H} = (G', \{\bigcup_{i \in T_0} D_i\}, \{\bigcup_{i \in T_1} D_i\}, \ldots, \{\bigcup_{i \in T_{\frac{r}{2}-1}} D_i\})$.

So for Example 1 we define $s(t)$ by $\mathbf{H} = (\{1\}, \{D_0\}, \{D_0\})$. Example 1 is taken from Theorem 1 of Section 3 and is a construction for length $N = 2p$ sequences, $s(t)$, with low NACF.

3 Sequences with Low Negaperiodic Autocorrelation

3.1 Symmetries

Two length K sequences, $u(t)$ and $v(t)$ are called 'PACF-equivalent' ('NACF-equivalent') if they have the same distribution of PACF (NACF) magnitudes, and there exist well-defined operations that take $u(t)$ to and from $v(t)$. Such operations are called PACF-equivalent (NACF-equivalent) operations. Before presenting the constructions we first mention some PACF-equivalent operations on $s'(t)$. These translate into NACF-equivalent operations on $s(t)$.

PACF-equivalent operation on $s'(t)$	NACF-equivalent operation on $s(t)$
Cyclic Shift of $s'(t)$	Negacyclic Shift of $s(t)$
Reversal of $s'(t)$	Reversal of $s(t)$
Negation of $s'(t)$	Negation of $s(t)$

The following theorems and conjectures only present constructions for NACF-inequivalent sequences, $s(t)$, and proofs of Theorems 1 and 2 are given at the end of this section.

Theorem 1. *Let $p = 4f + 1$ be prime and $d = 2$. The length $N = 2p$ sequence $s(t)$ has conjectured optimal three-valued out-of-phase negaperiodic autocorrelation, $\{-2, 0, 2\}$, if $\mathbf{H} = (\{1\}, \{D_0\}, \{D_0\})$.*

Theorem 2. *Let $p = 4f + 3$ be prime and $d = 2$. The length $N = 2p$ sequence $s(t)$ has conjectured optimal three-valued out-of-phase negaperiodic autocorrelation, $\{-2, 0, 2\}$, if $\mathbf{H} = (\{0, 1\}, \{D_0\}, \{D_0\})$ or $\mathbf{H} = (\{-\}, \{D_0\}, \{D_0\})$.*

In the following three Conjectures let $\gamma = \{a, b\}\{c, d\}\{e, f\}\{g, h\}$ be short for $\{D_a \cup D_b\}, \{D_c \cup D_d\}, \{D_e \cup D_f\}, \{D_g \cup D_h\}$.

Conjecture 1. Let p be a prime of the form $(n^2 + 1)/2$, $8|(p-1)$, and $d = 4$. Let $s(t)$ be described by $\mathbf{H} = (G', \gamma)$. Then, for a given γ chosen from Conjecture 1 of Table 1, $\exists\alpha$ and α^{-1} such that the length $N = 4p$ sequence $s(t)$ has near-optimal five-valued out-of-phase negaperiodic autocorrelation $\{-4, -2, 0, 2, 4\}$ or $\{-18, -4, 0, 4, 18\}$, respectively, independent of choice of G'.

Table 1. G' and γ Values for Conjectures 1 and 2

Conjecture 1	
G'	γ
$\{2\}$	$\{0,3\}\{1,2\}\{0,1\}\{0,1\}$
$\{0,1,2\}$	$\{1,2\}\{0,3\}\{0,1\}\{0,1\}$
$\{3\}$	$\{2,3\}\{0,1\}\{1,2\}\{1,2\}$
$\{0,1,3\}$	$\{0,1\}\{2,3\}\{1,2\}\{1,2\}$

Conjecture 2	
G'	γ
$\{0\}$	$\{0,3\}\{1,2\}\{0,1\}\{0,1\}$
$\{1\}$	$\{1,2\}\{0,3\}\{0,1\}\{0,1\}$
$\{0,2,3\}$	$\{2,3\}\{0,1\}\{1,2\}\{1,2\}$
$\{1,2,3\}$	$\{0,1\}\{2,3\}\{1,2\}\{1,2\}$

Conjecture 2. Let p be a prime of the form $(n^2+1)/2$, $8 \not| (p-1)$, and $d=4$. Let $s(t)$ be described by $\mathbf{H} = (G', \gamma)$. Then, for a given γ chosen from conjecture 2 of Table 1, $\exists\alpha$ and α^{-1} such that the length $N = 4p$ sequence $s(t)$ has near-optimal five-valued out-of-phase negaperiodic autocorrelation $\{-4,-2,0,2,4\}$ or $\{-22,-4,0,4,22\}$, respectively, independent of choice of G'.

Conjecture 3. Let p be a prime of the form n^2+4, and $d=4$. Let $s(t)$ be described by $\mathbf{H} = (G', \gamma)$. Then, for a given γ chosen from the left-hand (right-hand) side of Table 2, $\exists\alpha$ and α^{-1} such that the length $N = 4p$ sequence $s(t)$ of H has near-optimal five and seven-valued out-of-phase negaperiodic autocorrelation $\{-4,-2,0,2,4\}$ or $\{-12,-4,-2,0,2,4,12\}$, respectively, for the single choice of G' from the left-hand (right-hand) side of Table 2.

Table 2. G' and γ Values for Conjecture 3

G'	γ	G'	γ
$\{0\}$	$\{1,3\}\{0,2\}\{0,1\}\{0,1\}$	$\{0,3\}$	$\{0,1\}\{0,2\}\{0,2\}\{0,1\}$
	$\{0,2\}\{1,3\}\{0,1\}\{0,1\}$		$\{0,1\}\{1,3\}\{1,3\}\{0,1\}$
	$\{1,3\}\{0,2\}\{1,2\}\{1,2\}$		$\{1,2\}\{0,2\}\{0,2\}\{1,2\}$
	$\{0,2\}\{1,3\}\{1,2\}\{1,2\}$		$\{1,2\}\{1,3\}\{1,3\}\{1,2\}$

Example 2: A representative sequence of Conjecture 3 is
$H = (\{0,3\}, \{D_0, D_1\}, \{D_0, D_2\}, \{D_0, D_2\}, \{D_0, D_1\})$. Then
$C = \{(0,0) \cup (3,0) \cup (5,0) \cup (6,0) \cup (0, C_0) \cup (1, C_1) \cup (2, C_2) \cup (3, C_3) \cup (4, C_4) \cup (5, C_5) \cup (6, C_6) \cup (7, C_7)\}$, where

$$\begin{array}{llll} C_0 = \{D_0 \cup D_1\}, & C_1 = \{D_0 \cup D_2\}, & C_2 = \{D_0 \cup D_2\}, & C_3 = \{D_0 \cup D_1\} \\ C_4 = \{D_2 \cup D_3\}, & C_5 = \{D_1 \cup D_3\}, & C_6 = \{D_1 \cup D_3\}, & C_7 = \{D_2 \cup D_3\} \end{array}$$

Let $p = 29$ and $d = 4$. Using $\alpha = 2$ as a primitive generator, mod 29, $D_0 = \{1,16,24,7,25,23,20\}$, $D_1 = \{2,3,19,14,21,17,11\}$, $D_2 = \{4,6,9,28,13,5,22\}$, $D_3 = \{8,12,18,27,26,10,15\}$. Using the CRT,

$$(0, C_0) = 88\{1,16,24,7,25,23,20,2,3,19,14,21,17,11\} (\text{mod } 232)$$
$$(1, C_1) = 145 + 88\{1,16,24,7,25,23,20,4,6,9,28,13,5,22\} (\text{mod } 232)$$
$\ldots$ etc

Similarly, $F = \{0, 203, 29, 174\}$
Therefore,
$s(t) =$ 11011000010110111001010011001100111001011011101111100000101
01010101001111101111000111110010001001000011101001000001000
and the NACF of $s(t)$ is,
$116, 2, 0, 2, -4, -2, 0, 2, 4, 2, 0, 2, -4, -2, 0, -2, 4, -2, 0, 2, -4, 2, 0, 2, 4, 2, \ldots$ etc

Proof. (of Theorem 1). We wish to compute $d_C(w_1, w_2)$ by evaluating (7) using (8) and (9). For $p = 4f + 1$, $w_2^{-1} \in D_h$ implies $\pm w_2 \in D_{h+1(\bmod 2)}$, and we need this for the last three terms of (7). The cyclotomic numbers of order $d = 2$ for $p = 4f + 1$ are $[0, 0] = \frac{p-5}{4}$, $[0, 1] = [1, 0] = [1, 1] = \frac{p-1}{4}$. We have $C_0 = C_1 = D_0$, $C_2 = C_3 = D_1$, $G = \{(1, 0), (2, 0)\}$. Therefore,

$$
\begin{aligned}
d_C(0,0) &= |C| = 2(p-1) + 2 = 2p \\
d_C(1,0) &= |C_0 \cap C_3| + |C_1 \cap C_0| + |C_2 \cap C_1| + |C_3 \cap C_2| + |G \cap (G + (1,0))| \\
&= |D_0| + |D_1| + 1 = p \\
d_C(2,0) &= 2(|C_0 \cap C_2| + |C_1 \cap C_3|) + |G \cap (G + (2,0))| = 0 + 0 = 0 \\
d_C(3,0) &= d_C(1,0) = p \qquad (\text{using } d_C(-w_1, -w_2) = d_C(w_1, w_2)) \\
d_C(0,w_2) &= \textstyle\sum_{n=0}^{r-1} |C_n \cap (C_n + w_2)| + \sum_{k=0}^{r-1} |G \cap (k, C_k + w_2)| \\
&\quad + \textstyle\sum_{k=0}^{r-1} |(k, C_k) \cap (G + (0, w_2))| \\
&= [0,0] + [0,0] + [1,1] + [1,1] \\
&\quad + |\{(1,0),(2,0)\} \cap \{(1, C_1 + w_2) \cup (2, C_2 + w_2)\}| \\
&\quad + |\{(1, C_1) \cup (2, C_2)\} \cap \{(1, w_2), (2, w_2)\}| = p - 3 + 1 + 1 = p - 1, \\
&\qquad \text{for } w_2^{-1} \in D_0, \text{ or } w_2^{-1} \in D_1 \\
d_C(1,w_2) &= \textstyle\sum_{n=0}^{r-1} |C_n \cap (C_{n-1} + w_2)| + \sum_{k=0}^{r-1} |G \cap (k+1, C_k + w_2)| \\
&\quad + \textstyle\sum_{k=0}^{r-1} |(k, C_k) \cap (G + (1, w_2))| \\
&= [0,1] + [0,0] + [1,0] + [1,1] \\
&\quad + |\{(1,0),(2,0)\} \cap \{(1, C_0 + w_2) \cup (2, C_1 + w_2)\}| \\
&\quad + |\{(2, C_2) \cup (3, C_3)\} \cap \{(2, w_2), (3, w_2)\}| = p - 2 + 2 = p, \\
&\qquad \text{for } w_2^{-1} \in D_0, \text{ or } w_2^{-1} \in D_1 \\
\text{similarly } d_C(2,w_2) &= p - 1 + 1 + 1 = p + 1, \qquad d_C(3, w_2) = p - 2 + 2 = p \\
&\qquad \text{for } w_2^{-1} \in D_0, \text{ or } w_2^{-1} \in D_1
\end{aligned}
$$

Substituting $d_C(w_1, w_2)$ back into (6) gives the PACF distribution $\{0, 4, -4, N\}$ for $s'(t)$, implying an NACF distribution $\{0, 2, -2\}$ for $s(t)$. □

Proof. (of Theorem 2) The proof is identical to that of Theorem 1, except that, for $p = 4f+3$, $w_2^{-1} \in D_h$ implies $w_2 \in D_{h+1(\bmod 2)}$, and $-w_2 \in D_h$. Moreover, the cyclotomic numbers of order $d = 2$ for $p = 4f + 3$ are $[0, 1] = \frac{p+1}{4}$, $[0, 0] = [1, 0] = [1, 1] = \frac{p-3}{4}$. □

Conjectures 1 - 3 will hopefully be proved in a similar way to the above, but now cyclotomic numbers of order 4 are required.

4 Asymptotic Merit Factors

By computation, using (5), the constructions of Theorems 1 and 2 give sequences, $s(t)$, with Merit Factor (MF) $M_s \to 6.0$ as $N \to \infty$. Figs 1 and 2 plot MF for increasing prime values, p, for the constructions of Theorems 1 and 2. Very good MFs occur for no negacyclic shift, but Fig 3 presents the best MF over all negacyclic shifts. The highest MF sometimes occurs for a non-zero negacyclic shift. The asymptote of $M_s = 6.0$ is the best known for an infinite construction class of binary sequences [7, 8], where cyclically-shifted Legendre and Modified-Jacobi sequences also attain this maximum. [4]. Unlike Legendre and Modified-Jacobi sequences, no final shift of the constructed sequences is required to obtain

[4] The constructions of [1] appear to asymptote to $M_s = 1.5$ or $M_s = 3.0$

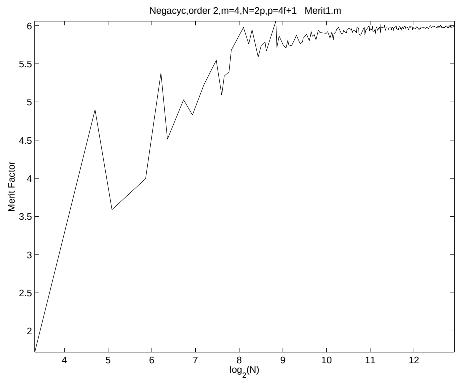

Fig. 1. NegaPeriodic Construction, Theorem 1, $p = 4f + 1$

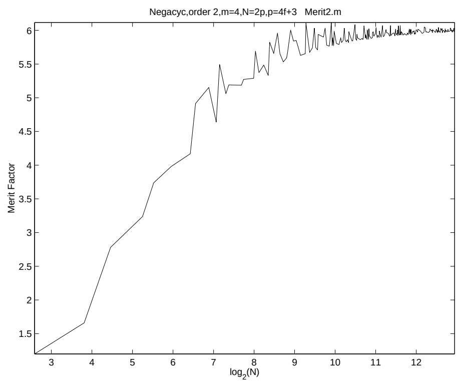

Fig. 2. NegaPeriodic Construction, Theorem 2, $p = 4f + 3$

the asymptote of 6.0. Lemma 3 of the next section shows that the constructions of Theorems 1 and 2 are closely related to Legendre sequences.

5 Mappings Between Periodic and Negaperiodic Autocorrelation

Although the sequence constructions of this paper are new, we also highlight further symmetries that trivially relate PACF and/or NACF coefficient distributions of binary sequences $s(t)$ and $e(t)$, where s and e are not necessarily the same length.

Lemma 2. *Let* $e(t) = s(t) + t \pmod 2$, *where* $s(t)$ *and* $e(t)$ *are binary sequences of length* K. *Then,*

$$Q_e(\omega) = (-1)^\omega P_s(\omega)$$

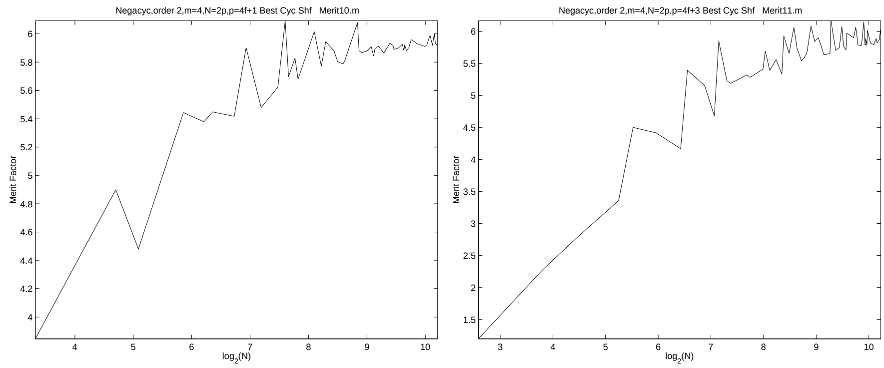

Fig. 3. NegaPeriodic Constructions, $p = 4f + 1$, Theorem 1 (lh), $p = 4f + 3$ Theorem 2 (rh), Best Negacyclic Shift

Proof. Direct inspection, or by examination of the $2K$-point Discrete Fourier Transform (DFT) of $s(t)$ and $e(t)$. □

Lemma 3. *Let* $e(t) = s(t \pmod K)$, $t = 0, 3 \pmod 4$, $e(t) = s(t \pmod K) + 1 \pmod 2$, $t = 1, 2 \pmod 4$, *where* $s(t)$ *and* $e(t)$ *are binary sequences of length* K *and* $2K$, *respectively,* K *odd, and* $0 \le t < 2K$. *Then,*

$$\begin{array}{ll} Q_e(\omega) = 0 & \omega \text{ odd} \\ Q_e(\omega) = (-1)^{\frac{\omega}{2}} 2P_s(\omega \pmod K) & \omega \text{ even}, \qquad 0 \le \omega < 2K \end{array}$$

Proof. Direct inspection or by examination of K and $2K$-point DFTs of s and e, respectively. □

Example 3: Consider the negated Legendre sequence of length $K = 13$, $s(t) = 1101100001101$. This sequence has PACF
$P_s(\omega) = 13, 1, -3, 1, 1, -3, -3, -3, -3, 1, 1, -3, 1$. $e(t)$ is of length $2K = 26$ and is given by,

$$\begin{aligned} e(t) &= 11011000011011101100001101 + 01100110011001100110011001 \pmod 2 \\ &= 10111110000010001010010100 \end{aligned}$$

and $e(t)$ has NACF,

$$Q_e(\omega) = 26, 0, -6, 0, -2, 0, -6, 0, 6, 0, 2, 0, -2, 0, 2, 0, -2, 0, -6, 0, 6, 0, 2, 0, 6, 0$$

$e(t)$ is identical to $s'(t)$ of Example 1 apart from the first bit. In general, an equivalent construction to that of Theorems 1 and 2 for $K = p$ is to make $s(t)$ a negated Legendre sequence, apply Lemma 3, then flip bit 0 or bit K.

Lemma 4. *Let* $e(t) = s(t \pmod K)$, $4 \not| t$, $e(t) = s(t \pmod K) + 1 \pmod 2$, $4|t$, *where* $s(t)$ *and* $e(t)$ *are binary sequences of length* K *and* $4K$, *respectively,* K *odd. Then,*

$$\begin{array}{ll} Q_e(\omega) = 0 & 4 \not| \omega \\ Q_e(\omega) = 4P_s(\omega \pmod K) & 4|\omega, \qquad 0 \le \omega < 4K \end{array}$$

Proof. Direct inspection or by examination of K and $4K$-point DFTs of s and e, respectively. □

6 Conclusion

This paper has presented new cyclotomic constructions for infinite families of length $N = 2p$ and $N = 4p$ binary sequences with very low negaperiodic autocorrelation. The technique builds length $2N$ sequences with low periodic autocorrelation with the second half the negation of the first half. The desired length N sequence is then simply the first half. Two of the constructions exhibit a Merit Factor approaching 6.0 as N approaches infinity. This is the highest asymptote currently known. A final section highlights further mappings which relate periodic autocorrelation of a binary sequence to the periodic or negaperiodic autocorrelation of another binary sequence.

References

1. Ding, C.,Helleseth, T.,Martinsen, H.M.: New Classes of Binary Sequences with Three-Level Autocorrelation. IEEE Trans. Inform. Theory **47** 1. Jan. (2001) 428–433
2. Golay, M.J.E.: Complementary Series. IRE Trans. Inform. Theory **IT-7** Apr. (1961) 82–87
3. M.J.E.Golay, M.J.E.: Sieves for Low Autocorrelation Binary Sequences. IEEE Trans. Inform. Theory **23** 1. Jan. (1977) 43–51
4. Golay, M.J.E.: The Merit Factor of Long Low Autocorrelation Binary Sequences. IEEE Trans. Inform. Theory **28** 3. May (1982) 543–549
5. Golay, M.J.E.: A New Search for Skewsymmetric Binary Sequences with Optimal Merit Factors. IEEE Trans. Inform. Theory **36** 5. Sept. (1990) 1163–1166
6. Høholdt, T., Jensen, H.E., Justesen, J.: Aperiodic Correlations and the Merit Factor of a Class of Binary Sequences. IEEE Trans. Inform. Theory **31** 4. July (1985) 549–552
7. Jensen, J.M.,Elbrønd Jensen, H.,Høholdt T.: The Merit Factor of Binary Sequences Related to Difference Sets. IEEE Trans. Inform. Theory **37** 3. May (1991) 617–626
8. Høholdt, T.: The Merit Factor of Binary Sequences. Difference Sets, Sequences and their Correlation Properties, A.Pott et a. (eds.), Series C: Mathematical and Physical Sciences, Kluwer Academic Publishers **542** (1999) 227–237
9. Luke, H.D.: Binary Odd-Periodic Complementary Sequences. IEEE Trans. Inform. Theory **43** 1. Jan. (1997) 365–367
10. Parker, M.G., Tellambura, C.: Generalised Rudin-Shapiro Constructions. WCC2001, Workshop on Coding and Cryptography, Paris(France) Jan. 8-12 (2001)
11. Paterson, K.G., Tarokh, V.: On the Existence and Construction of Good Codes with Low Peak-to-Average Power Ratios. IEEE Trans. Inform. Theory **46** 6. Sept. (2000) 1974–1987