Quaternary Golay sequence pairs II: Odd length

Richard G. Gibson and Jonathan Jedwab

11 August 2009 (revised 9 July 2010)

Abstract

A 4-phase Golay sequence pair of length $s \equiv 5 \pmod 8$ is constructed from a Barker sequence of the same length whose even-indexed elements are prescribed. This explains the origin of the 4-phase Golay seed pairs of length 5 and 13. The construction cannot produce new 4-phase Golay sequence pairs, because there are no Barker sequences of odd length greater than 13. A partial converse to the construction is given, under the assumption of additional structure on the 4-phase Golay sequence pair of length $s \equiv 5 \pmod 8$.

1 Introduction

We use the definitions and notation of the companion paper [GJ]. In that paper, we accounted for all 4-phase Golay sequences and Golay sequence pairs of even length at most 26, assuming the existence of the following 4-phase Golay seed pairs $(\mathcal{A}_s, \mathcal{B}_s)$ of length s for each $s \in \{3, 5, 11, 13\}$:

$$\left.\begin{array}{lcl} \mathcal{A}_3 & = & [0,\ 0,\ 2] \\ \mathcal{B}_3 & = & [0,\ 1,\ 0] \end{array}\right\},$$

$$\left.\begin{array}{lcl} \mathcal{A}_5 & = & [0,\ 0,\ 0,\ 3,\ 1] \\ \mathcal{B}_5 & = & [0,\ 1,\ 2,\ 0,\ 3] \end{array}\right\},$$

$$\left.\begin{array}{lcl} \mathcal{A}_{11} & = & [0,\ 0,\ 0,\ 1,\ 2,\ 0,\ 1,\ 3,\ 1,\ 0,\ 2] \\ \mathcal{B}_{11} & = & [0,\ 1,\ 2,\ 2,\ 2,\ 1,\ 1,\ 0,\ 3,\ 1,\ 0] \end{array}\right\},$$

$$\left.\begin{array}{lcl} \mathcal{A}_{13} & = & [0,\ 0,\ 0,\ 1,\ 2,\ 0,\ 0,\ 3,\ 0,\ 2,\ 0,\ 3,\ 1] \\ \mathcal{B}_{13} & = & [0,\ 1,\ 2,\ 2,\ 2,\ 1,\ 2,\ 0,\ 0,\ 3,\ 2,\ 0,\ 3] \end{array}\right\}.$$

In this paper we examine the relationship between the 4-phase Golay seed pairs $(\mathcal{A}_5, \mathcal{B}_5)$ and $(\mathcal{A}_{13}, \mathcal{B}_{13})$, and Barker sequences of length 5 and 13, respectively.

A *Barker sequence* is a 2-phase sequence $\mathcal{A} = (A[j])$ satisfying

$$|C_{\mathcal{A}}(u)| = 0 \text{ or } 1 \quad \text{for all } u \neq 0.$$

An example $\mathcal{E}_s$ of a Barker sequence of length $s > 1$ is known for each $s \in \{2, 3, 4, 5, 7, 11, 13\}$:

$$\mathcal{E}_2 = \ [+, +],$$

R.G. Gibson is with Department of Computing Science, University of Alberta, 2-21 Athabasca Hall, Edmonton, Alberta, Canada T6G 2E8. He was supported during 2006–8 at Simon Fraser University by NSERC of Canada via a Postgraduate Scholarship. Email: rggibson@cs.ualberta.ca

J. Jedwab is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC, Canada V5A 1S6, and is supported by NSERC of Canada. Email: jed@sfu.ca

$$
\begin{aligned}
\mathcal{E}_3 &= [+,+,-], \\
\mathcal{E}_4 &= [+,+,+,-], \\
\mathcal{E}_5 &= [+,+,+,-,+], \\
\mathcal{E}_7 &= [+,+,+,-,-,+,-], \\
\mathcal{E}_{11} &= [+,+,+,-,-,-,+,-,-,+,-], \\
\mathcal{E}_{13} &= [+,+,+,+,+,-,-,+,+,-,+,-,+].
\end{aligned}
$$

No Barker sequence of length greater than 13 is known. Turyn [Tur60] conjectured in 1960 that no such sequence exists, and Turyn and Storer proved the conjecture in the case of odd length:

Theorem 1 ([TS61])**.** *There is no Barker sequence of odd length $s > 13$.*

Mossinghoff [Mos09], building on work by Turyn [Tur65], Eliahou, Kervaire, and Saffari [EKS90], Schmidt [Sch99], and Leung and Schmidt [LS05], recently showed that a counterexample to Turyn's conjecture would require a Barker sequence of even length greater than $1.89 \cdot 10^{29}$. (The paper [Jed08] gives background on Barker sequences, and argues that the study of sequences and arrays having small aperiodic autocorrelations, including Golay pairs, can be viewed as historical responses to the apparent scarcity of Barker sequences.)

Jedwab and Parker [JP09] recently gave a construction linking odd-length Barker sequences to 2-phase Golay sequence pairs (see [GJ, Section 1] for a summary of existence results for 2-phase Golay sequences). The construction of [JP09] uses related Barker sequences of length 11 and 13 to produce the 2-phase Golay seed pair of length 26, and uses related Barker sequences of length 3 and 5 to produce one of the two 2-phase Golay seed pairs of length 10. It is striking that:

(A) the lengths of the Barker sequence ingredients that are available for use in the construction of [JP09], namely 3, 5, 11, and 13, are exactly the same as those of the 4-phase odd-length Golay sequence pairs whose origin we wish to explain.

(B) there are no known 4-phase Golay sequence pairs of odd length s greater than 13, and exhaustive search has established nonexistence for odd s in the range $13 < s <= 25$ (see [GJ, Table 1]); while by Theorem 1 we know that there are no Barker sequences of odd length greater than 13.

These apparent numerical similarities motivated the authors to seek a connection between a Barker sequence of odd length s and a 4-phase Golay sequence pair of length s. We show in Theorem 4 that, given a Barker sequence of length $s \equiv 5 \pmod 8$ whose even-indexed elements are prescribed, we can construct a 4-phase Golay sequence pair of the same length. Although Theorem 4 is valid for all lengths $s \equiv 5 \pmod 8$, it cannot be used to produce 4-phase Golay sequence pairs of length $s > 13$ because, by Theorem 1, the supply of odd-length Barker sequences runs out at length 13. Theorem 4 does, however, explain the origin of the 4-phase Golay seed pair of length 5 and 13, by regarding a Barker sequence of the same length as a given object.

We can also use Theorem 4 to explain another numerical similarity in existence patterns that was observed nearly thirty years ago by Frank [Fra80, p. 644]: "It is a curious and probably relevant fact that two of the quadriphase kernels have one half the length of Golay pairs, but the author has found no transform from one to the other." In the language of this paper, Frank sought a connection between 4-phase Golay seed pairs of length 5 and 13, and 2-phase Golay pairs of length 10 and 26. Such a connection is provided by relating both sets of objects to Barker sequences of length 3, 5, 11, and 13, using Theorem 4 to construct the former set and the method of [JP09] to construct the latter set.

The connection established in Theorem 4, and the apparent similarity in nonexistence patterns noted in point (B) above, suggests the possibility of a converse construction. This is, given a 4-phase Golay sequence pair of length $s \equiv 5 \pmod 8$, is there a construction for a Barker sequence of the same length? If so, Theorem 1 would then imply the nonexistence of 4-phase Golay sequence pairs of length $s \equiv 5 \pmod 8$ greater than 13. We were able to establish such a converse, but only by imposing additional structure on the 4-phase Golay sequence pair as described in Theorem 7.

The origin of the 4-phase Golay seed pair of length 3 and 11 remains open (although the length 3 pair could be regarded as sufficiently simple that it does not require explanation). While we suspect a connection with Barker sequences in these cases too, we were unable to determine a suitable construction procedure.

2 Definitions, notation, and preliminary results

We use the definitions and notation of [GJ]. We shall study 4-phase sequences $\mathcal{A}$ exclusively via their corresponding representation over $\mathbb{Z}_4$. Let $\mathcal{A} = (a[j])$ and $\mathcal{B} = (b[j])$ be length s sequences over $\mathbb{Z}_4$. Then the aperiodic autocorrelation function of $\mathcal{A}$ satisfies

$$C_{\mathcal{A}}(u) = \sum_{j=0}^{s-u-1} i^{a[j]-a[j+u]} \quad \text{for integer } u \geq 0,$$

and, since $C_{\mathcal{A}}(-u) = \overline{C_{\mathcal{A}}(u)}$ for integer $u > 0$, the sequences $\mathcal{A}$ and $\mathcal{B}$ form a length s Golay pair if and only if

$$C_{\mathcal{A}}(u) + C_{\mathcal{B}}(u) = 0 \quad \text{for integer } u \text{ satisfying } 0 < u < s.$$

We write $\mathcal{A}+\mathcal{B} := ((a[j]+b[j]) \bmod 4)$ and $\mathcal{A}-\mathcal{B} := ((a[j]-b[j]) \bmod 4)$ for the elementwise sum and difference of the sequences $\mathcal{A}$ and $\mathcal{B}$; note that this sum and difference are not the same as the sum and difference of 4-phase sequences used in [GJ, Section 3.2].

Now let $\mathcal{A} = (a[j])$ and $\mathcal{B} = (b[j])$ be sequences over $\mathbb{Z}_4$ of length s and t, respectively. The *concatenation* $\mathcal{A};\mathcal{B}$ of $\mathcal{A}$ and $\mathcal{B}$ is the length $s+t$ sequence $(c[j])$ given by

$$c[j] := \begin{cases} a[j] & \text{for } 0 \leq j < s, \\ b[j-s] & \text{for } s \leq j < s+t. \end{cases}$$

For integer $m \geq 0$, we write $\mathcal{A}^m$ to represent the concatenation of m copies of $\mathcal{A}$, so for example $[0, 0, 2, 2]^2; [0, 0, 1]$ represents the sequence $[0, 0, 2, 2, 0, 0, 2, 2, 0, 0, 1]$. The *aperiodic cross-correlation function* of $\mathcal{A}$ and $\mathcal{B}$ is given by

$$C_{\mathcal{A},\mathcal{B}}(u) := \sum_{j=0}^{\min\{s-1,t-u-1\}} i^{a[j]-b[j+u]} \quad \text{for integer } u \geq 0$$

(which reduces to $C_{\mathcal{A}}(u)$ in the case $\mathcal{B} = \mathcal{A}$). In the case $t = s-1$, the *interleaving* $\mathrm{int}(\mathcal{A},\mathcal{B})$ of $\mathcal{A}$ and $\mathcal{B}$ is the length $2s-1$ sequence $(c[j])$ given by

$$c[2j] := a[j] \quad \text{for } 0 \leq j < s,$$
$$c[2j+1] := b[j] \quad \text{for } 0 \leq j < s-1.$$

The following result is easily verified:

Lemma 2. *Let $\mathcal{A}$ and $\mathcal{B}$ be sequences over $\mathbb{Z}_4$ of length s and $s-1$, respectively. Then, for integer $u \geq 0$,*

(i) $C_{\mathrm{int}(\mathcal{A},\mathcal{B})}(2u) = C_{\mathcal{A}}(u) + C_{\mathcal{B}}(u)$,

(ii) $C_{\mathrm{int}(\mathcal{A},\mathcal{B})}(2u+1) = C_{\mathcal{A},\mathcal{B}}(u) + C_{\mathcal{B},\mathcal{A}}(u+1)$.

Using elementary arguments, Turyn and Storer determined the exact value of the aperiodic autocorrelation function of a Barker sequence of odd length:

Lemma 3 ([TS61])**.** *Suppose that A is a Barker sequence of odd length s. Then*

$$C_{\mathcal{A}}(u) = \begin{cases} 0 & \text{for odd } u, \\ (-1)^{\frac{s-1}{2}} & \text{for even } u \text{ satisfying } 0 < u < s. \end{cases}$$

3 Construction of a quaternary Golay pair from a Barker sequence

In this section, we present a general construction for a Golay sequence pair over $\mathbb{Z}_4$ of length $s \equiv 5 \pmod 8$ from a Barker sequence of length s whose even-indexed elements are prescribed.

We firstly describe the motivating examples of length 5 and 13. All length 5 and length 13 Golay sequences and pairs over $\mathbb{Z}_4$ can be constructed from the seed pairs $(\mathcal{A}_5, \mathcal{B}_5)$ and $(\mathcal{A}_{13}, \mathcal{B}_{13})$ given in Section 1, as described in [GJ, Section 4.2]. Represent the Barker sequences $\mathcal{E}_5$ and $\mathcal{E}_{13}$ as interleaved sequences over $\mathbb{Z}_4$:

$$\begin{aligned} \mathcal{E}_5 &= \mathrm{int}([0,\ 0,\ 0],\ [0,\ 2]) \\ \mathcal{E}_{13} &= \mathrm{int}([0,\ 0,\ 0,\ 2,\ 0,\ 0,\ 0],\ [0,\ 0,\ 2,\ 0,\ 2,\ 2]). \end{aligned}$$

Then form the following differences:

$$\begin{aligned} \mathcal{A}_5 - \mathcal{E}_5 &= \mathrm{int}([0,\ 0,\ 1],\ [0,\ 1]), \\ \mathcal{B}_5 - \mathcal{E}_5 &= \mathrm{int}([0,\ 2,\ 3],\ [1,\ 2]), \\ \mathcal{A}_{13} - \mathcal{E}_{13} &= \mathrm{int}([0,\ 0,\ 2,\ 2,\ 0,\ 0,\ 1],\ [0,\ 1,\ 2,\ 3,\ 0,\ 1]), \\ \mathcal{B}_{13} - \mathcal{E}_{13} &= \mathrm{int}([0,\ 2,\ 2,\ 0,\ 0,\ 2,\ 3],\ [1,\ 2,\ 3,\ 0,\ 1,\ 2]). \end{aligned}$$

We identify a pattern in these differences, namely that for $m = 0, 1$ we can write

$$\begin{aligned} \mathcal{A}_{8m+5} - \mathcal{E}_{8m+5} &= \mathrm{int}(\mathcal{W}_m, \mathcal{X}_m), \\ \mathcal{B}_{8m+5} - \mathcal{E}_{8m+5} &= \mathrm{int}(\mathcal{Y}_m, \mathcal{Z}_m), \end{aligned}$$

where

$$\begin{aligned} \mathcal{W}_m &:= [0,\ 0,\ 2,\ 2]^m; [0,\ 0,\ 1], \\ \mathcal{X}_m &:= [0,\ 1,\ 2,\ 3]^m; [0,\ 1], \\ \mathcal{Y}_m &:= [0,\ 2,\ 2,\ 0]^m; [0,\ 2,\ 3], \\ \mathcal{Z}_m &:= [1,\ 2,\ 3,\ 0]^m; [1,\ 2]. \end{aligned}$$

This leads to our main result:

Theorem 4. *Let $m \geq 0$ be an integer. Suppose that $\mathrm{int}(\mathcal{C}, \mathcal{D})$ is a Barker sequence of length $8m+5$, where $\mathcal{C} = [0,\ 0,\ 0,\ 2]^m; [0,\ 0,\ 0]$. Then the sequences*

$$\begin{aligned} \mathcal{A} &:= \mathrm{int}(\mathcal{C} + \mathcal{W}_m,\ \mathcal{D} + \mathcal{X}_m), \\ \mathcal{B} &:= \mathrm{int}(\mathcal{C} + \mathcal{Y}_m,\ \mathcal{D} + \mathcal{Z}_m) \end{aligned}$$

form a length $8m+5$ Golay pair over $\mathbb{Z}_4$.

Proof. For ease of presentation, we drop the subscript m on the sequences $\mathcal{W}_m$, $\mathcal{X}_m$, $\mathcal{Y}_m$, and $\mathcal{Z}_m$. Define $s := 4m+3$, so that $\mathcal{C}$, $\mathcal{W}$, $\mathcal{Y}$ have length s, and $\mathcal{D}$, $\mathcal{X}$, $\mathcal{Z}$ have length $s-1$. Throughout the proof, we shall make use of the prescribed values of the sequences $\mathcal{C} = (c[j])$, $\mathcal{W} = (w[j])$, $\mathcal{X} = (x[j])$, $\mathcal{Y} = (y[j])$, and $\mathcal{Z} = (z[j])$, as summarised in Table 1, without specific reference.

Sequence element	Sequence value	Range of integer j
$c[2j]$	0	$0 \le 2j \le s-1$
$c[2j+1]$	$2j \bmod 4$	$1 \le 2j+1 \le s-2$
$w[2j]$	$2j \bmod 4$	$0 \le 2j \le s-3$
$w[2j+1]$	$2j \bmod 4$	$1 \le 2j+1 \le s-2$
$w[s-1]$	1	
$x[j]$	$j \bmod 4$	$0 \le j \le s-2$
$y[2j]$	$2j \bmod 4$	$0 \le 2j \le s-3$
$y[2j+1]$	$(2j+2) \bmod 4$	$1 \le 2j+1 \le s-2$
$y[s-1]$	3	
$z[j]$	$(j+1) \bmod 4$	$0 \le j \le s-2$

Table 1: Prescribed sequence values in Theorem 4

To establish that $\mathcal{A}$ and $\mathcal{B}$ are a Golay pair, we need to show that

$$C_{\mathcal{A}}(u) + C_{\mathcal{B}}(u) = 0 \quad \text{for } 0 < u \le 2s-2.$$

By Lemma 2, this is equivalent to

$$C_{\mathcal{C}+\mathcal{W}}(u) + C_{\mathcal{D}+\mathcal{X}}(u) + C_{\mathcal{C}+\mathcal{Y}}(u) + C_{\mathcal{D}+\mathcal{Z}}(u) = 0 \quad \text{for } 0 < u \le s-1 \tag{1}$$

and

$$\begin{aligned} C_{\mathcal{C}+\mathcal{W},\mathcal{D}+\mathcal{X}}(u) + C_{\mathcal{D}+\mathcal{X},\mathcal{C}+\mathcal{W}}(u+1) + C_{\mathcal{C}+\mathcal{Y},\mathcal{D}+\mathcal{Z}}(u) + C_{\mathcal{D}+\mathcal{Z},\mathcal{C}+\mathcal{Y}}(u+1) \\ = 0 \quad \text{for } 0 \le u \le s-2. \end{aligned} \tag{2}$$

Proof of (1). Fix u in the range $0 < u \le s-1$. Then

$$\begin{aligned} C_{\mathcal{D}+\mathcal{X}}(u) + C_{\mathcal{D}+\mathcal{Z}}(u) &= \sum_{j=0}^{s-u-2} \left(i^{d[j]+x[j]-d[j+u]-x[j+u]} + i^{d[j]+z[j]-d[j+u]-z[j+u]} \right) \\ &= \sum_{j=0}^{s-u-2} i^{d[j]-d[j+u]} \left(i^{j-(j+u)} + i^{j+1-(j+u+1)} \right) \\ &= 2i^{-u} C_{\mathcal{D}}(u). \end{aligned} \tag{3}$$

Similarly

$$\begin{aligned} C_{\mathcal{C}+\mathcal{W}}(u) + C_{\mathcal{C}+\mathcal{Y}}(u) &= \sum_{j=0}^{s-u-1} i^{c[j]-c[j+u]} \left(i^{w[j]-w[j+u]} + i^{y[j]-y[j+u]} \right) \\ &= i^{c[s-u-1]-c[s-1]} \left(i^{w[s-u-1]-w[s-1]} + i^{y[s-u-1]-y[s-1]} \right) \end{aligned}$$

$$+\sum_{j=0}^{\lfloor\frac{s-u-2}{2}\rfloor} i^{c[2j]-c[2j+u]}\left(i^{w[2j]-w[2j+u]}+i^{y[2j]-y[2j+u]}\right)$$
$$+\sum_{j=0}^{\lfloor\frac{s-u-3}{2}\rfloor} i^{c[2j+1]-c[2j+u+1]}\left(i^{w[2j+1]-w[2j+u+1]}+i^{y[2j+1]-y[2j+u+1]}\right). \tag{4}$$

We now consider two cases according to the parity of u, and show that (1) holds in both cases.

Case 1*:* $u=2v$. In this case (4) gives

$$\begin{aligned}
C_{\mathcal{C}+\mathcal{W}}(u)+C_{\mathcal{C}+\mathcal{Y}}(u) &= i^{c[s-2v-1]-c[s-1]}\left(i^{(s-2v-1)-1}+i^{(s-2v-1)-3}\right)\\
&\quad+\sum_{j=0}^{\frac{s-2v-3}{2}} i^{c[2j]-c[2j+2v]}\left(i^{2j-(2j+2v)}+i^{2j-(2j+2v)}\right)\\
&\quad+\sum_{j=0}^{\frac{s-2v-3}{2}} i^{c[2j+1]-c[2j+2v+1]}\left(i^{2j-(2j+2v)}+i^{2j+2-(2j+2v+2)}\right)\\
&= 2i^{-2v}\sum_{j=0}^{s-2v-2} i^{c[j]-c[j+2v]}\\
&= 2i^{-2v}\left(C_{\mathcal{C}}(2v)-i^{c[s-2v-1]-c[s-1]}\right)\\
&= 2i^{-2v}\left(C_{\mathcal{C}}(2v)-1\right),
\end{aligned}$$

and so with (3) we have

$$\begin{aligned}
C_{\mathcal{C}+\mathcal{W}}(u)+C_{\mathcal{D}+\mathcal{X}}(u)+C_{\mathcal{C}+\mathcal{Y}}(u)+C_{\mathcal{D}+\mathcal{Z}}(u) &= 2i^{-2v}\left(C_{\mathcal{C}}(2v)+C_{\mathcal{D}}(2v)-1\right)\\
&= 2i^{-2v}\left(C_{\mathrm{int}(\mathcal{C},\mathcal{D})}(4v)-1\right)
\end{aligned}$$

by Lemma 2 (i). This gives (1) as required, because $C_{\mathrm{int}(\mathcal{C},\mathcal{D})}(4v)=(-1)^{\frac{8m+4}{2}}=1$ by Lemma 3.

Case 2*:* $u=2v+1$. In this case (4) gives

$$\begin{aligned}
C_{\mathcal{C}+\mathcal{W}}(u)+C_{\mathcal{C}+\mathcal{Y}}(u) &= i^{c[s-2v-2]-c[s-1]}\left(i^{(s-2v-3)-1}+i^{(s-2v-1)-3}\right)\\
&\quad+\sum_{j=0}^{\frac{s-2v-3}{2}} i^{c[2j]-c[2j+2v+1]}\left(i^{2j-(2j+2v)}+i^{2j-(2j+2v+2)}\right)\\
&\quad+\sum_{j=0}^{\frac{s-2v-5}{2}} i^{c[2j+1]-c[2j+2v+2]}\left(i^{2j-(2j+2v+2)}+i^{2j+2-(2j+2v+2)}\right)\\
&= i^{(s-2v-3)-0}(2i^{s-2v})\\
&= -2i
\end{aligned}$$

since $s\equiv 3 \pmod 4$, and so with (3) we have

$$C_{\mathcal{C}+\mathcal{W}}(u)+C_{\mathcal{D}+\mathcal{X}}(u)+C_{\mathcal{C}+\mathcal{Y}}(u)+C_{\mathcal{D}+\mathcal{Z}}(u)$$

$$
\begin{aligned}
&= -2i + 2i^{-2v-1}C_{\mathcal{D}}(2v+1) + \left(2i^{-2v-1}C_{\mathcal{C}}(2v+1) - 2i^{-2v-1}C_{\mathcal{C}}(2v+1)\right) \\
&= -2i\left(1 + (-1)^v C_{\mathrm{int}(\mathcal{C},\mathcal{D})}(4v+2) - (-1)^v C_{\mathcal{C}}(2v+1)\right) \qquad (5)
\end{aligned}
$$

by Lemma 2 (i). Now

$$
\begin{aligned}
C_{\mathcal{C}}(2v+1) &= \sum_{j=0}^{s-2v-2} i^{c[j]-c[j+2v+1]} \\
&= \sum_{j=0}^{2m-v} \left(i^{c[2j]-c[2j+2v+1]} + i^{c[2j+1]-c[2j+2v+2]}\right) \\
&= \sum_{j=0}^{2m-v} \left(i^{0-(2j+2v)} + i^{2j-0}\right) \\
&= 1 + (-1)^v, \qquad (6)
\end{aligned}
$$

and

$$
C_{\mathrm{int}(\mathcal{C},\mathcal{D})}(4v+2) = 1 \qquad (7)
$$

by Lemma 3. Substitution of (6) and (7) into (5) then gives (1), as required.

Proof of (2). Fix u in the range $0 \le u \le s-2$. Then

$$
\begin{aligned}
&C_{\mathcal{C}+\mathcal{W},\mathcal{D}+\mathcal{X}}(u) + C_{\mathcal{C}+\mathcal{Y},\mathcal{D}+\mathcal{Z}}(u) \\
&\quad = \sum_{j=0}^{s-u-2} i^{c[j]-d[j+u]}\left(i^{w[j]-x[j+u]} + i^{y[j]-z[j+u]}\right) \\
&\quad = \sum_{j=0}^{\lfloor\frac{s-u-2}{2}\rfloor} i^{c[2j]-d[2j+u]}\left(i^{w[2j]-x[2j+u]} + i^{y[2j]-z[2j+u]}\right) \\
&\qquad + \sum_{j=0}^{\lfloor\frac{s-u-3}{2}\rfloor} i^{c[2j+1]-d[2j+u+1]}\left(i^{w[2j+1]-x[2j+u+1]} + i^{y[2j+1]-z[2j+u+1]}\right) \\
&\quad = \sum_{j=0}^{\lfloor\frac{s-u-2}{2}\rfloor} i^{c[2j]-d[2j+u]}\left(i^{2j-(2j+u)} + i^{2j-(2j+u+1)}\right) \\
&\qquad + \sum_{j=0}^{\lfloor\frac{s-u-3}{2}\rfloor} i^{c[2j+1]-d[2j+u+1]}\left(i^{2j-(2j+u+1)} + i^{2j+2-(2j+u+2)}\right) \\
&\quad = i^{-u}(1-i)C_{\mathcal{C},\mathcal{D}}(u) \qquad (8)
\end{aligned}
$$

and

$$
\begin{aligned}
&C_{\mathcal{D}+\mathcal{X},\mathcal{C}+\mathcal{W}}(u+1) + C_{\mathcal{D}+\mathcal{Z},\mathcal{C}+\mathcal{Y}}(u+1) \\
&\quad = \sum_{j=0}^{s-u-2} i^{d[j]-c[j+u+1]}\left(i^{x[j]-w[j+u+1]} + i^{z[j]-y[j+u+1]}\right) \\
&\quad = i^{d[s-u-2]-c[s-1]}\left(i^{x[s-u-2]-w[s-1]} + i^{z[s-u-2]-y[s-1]}\right)
\end{aligned}
$$

$$+ \sum_{j=0}^{\lfloor \frac{s-u-3}{2} \rfloor} i^{d[2j]-c[2j+u+1]} \left(i^{x[2j]-w[2j+u+1]} + i^{z[2j]-y[2j+u+1]} \right)$$
$$+ \sum_{j=0}^{\lfloor \frac{s-u-4}{2} \rfloor} i^{d[2j+1]-c[2j+u+2]} \left(i^{x[2j+1]-w[2j+u+2]} + i^{z[2j+1]-y[2j+u+2]} \right). \quad (9)$$

We again consider two cases, according to the parity of u.

Case 1*:* $u = 2v$. In this case (9) gives

$$\begin{aligned} C_{\mathcal{D}+\mathcal{X},\mathcal{C}+\mathcal{W}}(u+1) &+ C_{\mathcal{D}+\mathcal{Z},\mathcal{C}+\mathcal{Y}}(u+1) \\ &= i^{d[s-2v-2]-c[s-1]} \left(i^{(s-2v-2)-1} + i^{(s-2v-1)-3} \right) \\ &\quad + \sum_{j=0}^{\frac{s-2v-3}{2}} i^{d[2j]-c[2j+2v+1]} \left(i^{2j-(2j+2v)} + i^{2j+1-(2j+2v+2)} \right) \\ &\quad + \sum_{j=0}^{\frac{s-2v-5}{2}} i^{d[2j+1]-c[2j+2v+2]} \left(i^{2j+1-(2j+2v+2)} + i^{2j+2-(2j+2v+2)} \right) \\ &= i^{-2v}(1-i)C_{\mathcal{D},\mathcal{C}}(2v+1), \end{aligned} \quad (10)$$

since $s \equiv 3 \pmod 4$.

Case 2*:* $u = 2v+1$. In this case (9) similarly gives

$$\begin{aligned} C_{\mathcal{D}+\mathcal{X},\mathcal{C}+\mathcal{W}}(u+1) &+ C_{\mathcal{D}+\mathcal{Z},\mathcal{C}+\mathcal{Y}}(u+1) \\ &= i^{d[s-2v-3]-c[s-1]} \left(i^{(s-2v-3)-1} + i^{(s-2v-2)-3} \right) \\ &\quad + \sum_{j=0}^{\frac{s-2v-5}{2}} i^{d[2j]-c[2j+2v+2]} \left(i^{2j-(2j+2v+2)} + i^{2j+1-(2j+2v+2)} \right) \\ &\quad + \sum_{j=0}^{\frac{s-2v-5}{2}} i^{d[2j+1]-c[2j+2v+3]} \left(i^{2j+1-(2j+2v+2)} + i^{2j+2-(2j+2v+4)} \right) \\ &= i^{-2v-1}(1-i)C_{\mathcal{D},\mathcal{C}}(2v+2). \end{aligned} \quad (11)$$

The conclusions (10) and (11) of Cases 1 and 2 can both be represented in the form

$$C_{\mathcal{D}+\mathcal{X},\mathcal{C}+\mathcal{W}}(u+1) + C_{\mathcal{D}+\mathcal{Z},\mathcal{C}+\mathcal{Y}}(u+1) = i^{-u}(1-i)C_{\mathcal{D},\mathcal{C}}(u+1).$$

Combine this with (8) and use Lemma 2 (ii) to give

$$\begin{aligned} C_{\mathcal{C}+\mathcal{W},\mathcal{D}+\mathcal{X}}(u) + C_{\mathcal{D}+\mathcal{X},\mathcal{C}+\mathcal{W}}(u+1) + C_{\mathcal{C}+\mathcal{Y},\mathcal{D}+\mathcal{Z}}(u) + C_{\mathcal{D}+\mathcal{Z},\mathcal{C}+\mathcal{Y}}(u+1) \\ = i^{-u}(1-i)C_{\mathrm{int}(\mathcal{C},\mathcal{D})}(2u+1) \\ = 0 \end{aligned}$$

by Lemma 3, proving (2) as required.

□

4 A partial converse to Theorem 4

In this section, we present a partial converse to the construction of Theorem 4. That is, given a Golay sequence pair over $\mathbb{Z}_4$ of length $s \equiv 5 \pmod 8$ with a certain structure, we construct a Barker sequence of the same length; by Theorem 1, this implies $s = 5$ or 13.

The motivating examples are the Golay seed pairs of length 3, 5, 11 and 13 given in Section 1, from which all known Golay sequence pairs of odd length over $\mathbb{Z}_4$ can be derived via equivalence transformations [GJ, Section 4.2]. We find that the sequences $\mathcal{A}$ and $\mathcal{B}$ of each of these pairs have the property that

$$\mathcal{A} + \mathcal{B} = (j \bmod 4), \tag{12}$$

in other words they sum to $[0, 1, 2, 3, 0, 1, 2, 3, \ldots]$. Property (12) also holds for the output sequences $\mathcal{A}$ and $\mathcal{B}$ of Theorem 4 (under which we have $\mathcal{A}+\mathcal{B} = \text{int}(2\mathcal{C}+\mathcal{W}_m+\mathcal{Y}_m, 2\mathcal{D}+\mathcal{X}_m+\mathcal{Z}_m) = \text{int}(\mathcal{W}_m+\mathcal{Y}_m, \mathcal{X}_m+\mathcal{Z}_m)$, because $\mathcal{C}$ and $\mathcal{D}$ take values in $\{0, 2\}$). Property (12) implies the following easily-verified relationship between the aperiodic autocorrelation function of $\mathcal{A}$ and $\mathcal{B}$:

Lemma 5. *Let $\mathcal{A}$ and $\mathcal{B}$ be length s sequences over $\mathbb{Z}_4$ having property* (12)*. Then*

$$C_{\mathcal{B}}(u) = i^{-u}\overline{C_{\mathcal{A}}(u)} \quad \textit{for } 0 \le u < s.$$

We therefore define a length s sequence $\mathcal{A}$ over $\mathbb{Z}_4$ to be *good* if

$$C_{\mathcal{A}}(u) + i^{-u}\overline{C_{\mathcal{A}}(u)} = 0 \quad \text{for } 0 < u < s,$$

which by Lemma 5 implies:

Lemma 6.

(i) *Suppose $\mathcal{A}$ is a good sequence. Then $\mathcal{A}$ forms a Golay pair over $\mathbb{Z}_4$ with the sequence $(j \bmod 4) - \mathcal{A}$.*

(ii) *Suppose that $\mathcal{A}$ and $\mathcal{B}$ form a Golay sequence pair having property* (12)*. Then $\mathcal{A}$ and $\mathcal{B}$ are each good sequences.*

We can therefore rephrase our observations above as:

(A) A good sequence is a Golay sequence.

(B) All known odd-length Golay sequence pairs over $\mathbb{Z}_4$ can be derived via equivalence transformations from a pair of good sequences.

(C) The output Golay sequences of Theorem 4 are both good sequences.

Given these close connections between good sequences and Golay sequences over $\mathbb{Z}_4$, a first step towards proving the nonexistence of Golay sequence pairs over $\mathbb{Z}_4$ of odd length $s > 13$ would be to prove the nonexistence of good sequences of odd length $s > 13$. We were able to establish this in the case $s \equiv 5 \pmod 8$, but only by placing parity constraints on the elements of the good sequence:

Theorem 7. *Suppose that $\mathcal{A} = (a[j])$ is a good sequence of length $s \equiv 5 \pmod 8$ whose elements satisfy the parity constraints*

$$\begin{aligned} a[2u-1] + a[2u+1] \equiv 1 \pmod 2 \quad &\textit{for } 1 \le u \le \tfrac{s-5}{4}, \\ a[4u] \equiv 0 \pmod 2 \quad &\textit{for } 1 \le u \le \tfrac{s-5}{8}. \end{aligned}$$

Then there exists a Barker sequence of length s.

Theorem 7 is proved at some length and with considerable effort in [Gib08, Chapter 4], by showing that the sequence $\mathcal{A} - \mathrm{int}(\mathcal{W}_m, \mathcal{X}_m)$ (where $s = 8m + 5$) must be a Barker sequence; the proof is omitted here. We remark that the parity constraints of Theorem 7 hold for each of the sequences $\mathcal{A}_5$, $\mathcal{B}_5$, $\mathcal{A}_{13}$, and $\mathcal{B}_{13}$ (as well as for the sequences $\mathcal{A}_3$, $\mathcal{B}_3$, $\mathcal{A}_{11}$, and $\mathcal{B}_{11}$). Theorems 1 and 7 together imply:

Corollary 8. *Suppose that $\mathcal{A} = (a[j])$ is a good sequence of length $s \equiv 5 \pmod 8$ whose elements satisfy the parity constraints*

$$\begin{aligned} a[2u-1] + a[2u+1] &\equiv 1 \pmod 2 \quad \textit{for } 1 \le u \le \tfrac{s-5}{4}, \\ a[4u] &\equiv 0 \pmod 2 \quad \textit{for } 1 \le u \le \tfrac{s-5}{8}. \end{aligned}$$

Then $s = 5$ or 13.

5 Open questions

We conclude with some open questions:

(i) Can every odd-length Golay sequence over $\mathbb{Z}_4$ be derived via equivalence transformations from a good sequence?

(ii) Can the parity constraints of Theorem 7 be removed?

(iii) Can Corollary 8 (preferably without the parity constraints) be proved directly, without reference to an odd-length Barker sequence?

(iv) Is there a connection between the Golay seed pairs $(\mathcal{A}_3, \mathcal{B}_3)$ and $(\mathcal{A}_{11}, \mathcal{B}_{11})$, and a Barker sequence of length 3 and 11?

(v) Does there exist a Golay sequence over $\mathbb{Z}_4$ of odd length greater than 13?

References

[EKS90] S. Eliahou, M. Kervaire, and B. Saffari, *A new restriction on the lengths of Golay complementary sequences*, J. Combin. Theory (A) **55** (1990), 49–59.

[Fra80] R.L. Frank, *Polyphase complementary codes*, IEEE Trans. Inform. Theory **IT-26** (1980), 641–647.

[Gib08] R.G. Gibson, *Quaternary Golay sequence pairs*, Master's thesis, Simon Fraser University, 2008, available online: `<http://sites.google.com/site/richardggibson>`.

[GJ] R.G. Gibson and J. Jedwab, *Quaternary Golay sequence pairs I: Even number of elements*, Designs, Codes and Cryptography, accepted 2010.

[Jed08] J. Jedwab, *What can be used instead of a Barker sequence?*, Contemp. Math. **461** (2008), 153–178.

[JP09] J. Jedwab and M.G. Parker, *A construction of binary Golay sequence pairs from odd-length Barker sequences*, J. Combin. Designs **17** (2009), 478–491.

[LS05] K.H. Leung and B. Schmidt, *The field descent method*, Designs, Codes and Cryptography **36** (2005), 171–188.

[Mos09] M.J. Mossinghoff, *Wieferich pairs and Barker sequences*, Designs, Codes and Cryptography **53** (2009), 149–163.

[Sch99] B. Schmidt, *Cyclotomic integers and finite geometry*, J. Am. Math. Soc. **12** (1999), 929–952.

[TS61] R. Turyn and J. Storer, *On binary sequences*, Proc. Amer. Math. Soc. **12** (1961), 394–399.

[Tur60] R. Turyn, *Optimum codes study*, Final Report. Contract AF19(604)-5473, Sylvania Electronic Systems, 29 January 1960.

[Tur65] R.J. Turyn, *Character sums and difference sets*, Pacific J. Math. **15** (1965), 319–346.