QUATERNARY GOLAY SEQUENCE PAIRS

by

Richard G. Gibson
B.Sc., University of Victoria, 2006

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
in the Department
of
Mathematics

SIMON FRASER UNIVERSITY
Fall 2008

APPROVAL

Name: Richard G. Gibson

Degree: Master of Science

Title of Thesis: Quaternary Golay Sequence Pairs

Examining Committee: Dr. Jason Bell
Chair

Dr. Jonathan Jedwab
Associate Professor of Mathematics
Simon Fraser University
Senior Supervisor

Dr. Luis Goddyn
Professor of Mathematics
Simon Fraser University
Supervisor

Dr. Michael Monagan
Professor of Mathematics
Simon Fraser University
SFU Examiner

Date Approved: November 6, 2008

Abstract

This thesis classifies all ordered quaternary Golay sequence pairs of length less than 22. Previous results, both classical and recent, are applied to explain the existence pattern for all even lengths less than 22. In addition, a general construction is developed which derives quaternary Golay pairs of length congruent to 5 modulo 8 from binary Barker sequences of the same odd length. Applying this construction to lengths 5 and 13 explains all such known pairs.

Furthermore, this thesis explores the possibility of reversing the Barker-to-Golay derivation by attempting to construct an odd-length binary Barker sequence from a quaternary Golay sequence of the same length. This procedure is successful for all quaternary Golay sequences of length congruent to 5 modulo 8 satisfying certain conditions. Since there are no binary Barker sequences of odd length greater than 13, all quaternary Golay sequences fulfilling these conditions are known.

Acknowledgments

Firstly, I would like to extend my sincere gratitude to my supervisor, Jonathan Jedwab, for encouraging me to come to Simon Fraser University, introducing me to a very interesting topic, entertaining any ideas I came up with and encouraging me to excel in my work.

I would also like to thank both Simon Fraser University and NSERC for providing me with generous scholarships which allowed me to partake in graduate studies with very few worries.

Finally, I would like to thank my friends and family for supporting me throughout my studies, even if they still don't have any clue as to what math researchers actually do.

Contents

List of Tables

Chapter 1

Introduction

In 1953, R.H. Barker sought binary sequences with optimally small aperiodic autocorrelations for use in a group synchronization digital system [Bar53]. He was able to find such sequences for small lengths, but could not find ones for larger, more desirable lengths and speculated that none exist. Subsequently, a binary sequence for which the aperiodic autocorrelations are, independently, as small as possible in magnitude became known as a (binary) Barker sequence. Other authors soon recognized that Barker sequences of large lengths would also be beneficial in other applications, including radar [Wel60] and pulse compression [Boe67].

As evidence mounted against the existence of a binary Barker sequence of length larger than 13 (see [Jed08] for a review), alternatives have been proposed and studied. Examples of these studies include multi-dimensional Barker arrays ([AS89], [Dym92], [DJS07] and [JP07b]), the peak sidelobe level of binary sequences ([JY06] and [DJ07]), the merit factor of binary sequences (see [Jed05] for a survey), generalized Barker sequences ([GS65] and [Tur74a]) and, of interest to us, pairs of complementary Golay sequences and arrays (as introduced by Marcel J. E. Golay in [Gol51] who later revisited them in [Gol61]). The lattermost example has been used in areas such as infrared multislit spectrometry [Gol51], X-ray and gamma-ray coded aperture imaging [OHT78], optical time domain reflectometry [NNG$^+$89], power control for multicarrier wireless transmission [DJ99], and medical ultrasound [NSL$^+$03]. On the theoretical side, Golay sequences have a connection with Hadamard matrices [CHK02].

Binary Golay sequence pairs exist for lengths 2, 10 [Gol51] and 26 [Gol62]. In 1974, Turyn developed a product construction for such pairs, proving the existence of binary

Golay sequence pairs of length $2^a 10^b 26^c$ for all integers $a, b, c \geq 0$ [Tur74b]. Although not all known pairs are derivable from the construction, every known length of a binary Golay pair does have this form. Later, Budišin derived a construction method specific to Golay pairs of length 2^m which accounted for all such known binary pairs [Bud90]. In addition, Davis and Jedwab discovered that all known binary pairs of length 2^m occur as complete cosets of the first-order Reed-Muller code $\mathrm{RM}(1, m)$ within the second-order Reed-Muller code $\mathrm{RM}(2, m)$ [DJ99]. This occurrence is actually more general as it holds for all 2^h-phase Golay sequence pairs, rather than just binary, under a suitable generalization of the Reed-Muller code. Furthermore, in 2003, Borwein and Ferguson classified all binary pairs for lengths less than 100 and identified 5 "primitive" pairs that could be used to construct all other pairs of these lengths [BF03]. Some of these primitive pairs are derivable from simple ternary Golay pairs [EKS91] and binary Barker sequences [JP08].

Turning to Golay array pairs, Jedwab and Parker provided a projection method for obtaining a Golay array pair directly from one of larger dimension [JP07a]. Using this, together with computer search results in [BF03] and a generalization of Turyn's product construction, they explicitly gave all sizes of binary Golay arrays with fewer than 100 elements [JP07a]. A year later, Fiedler, Jedwab and Parker developed a three-stage array construction process for obtaining long Golay sequence pairs from a series of smaller-length pairs [FJP08]. This process explained all known (at the time) H-phase Golay sequences of length 2^m (and still does, after the recent discovery of a new source of 6-phase Golay sequence pairs [FJW08]); however, it was unclear as to how well it could explain other known results, in particular the construction of quaternary Golay sequence pairs of length not a power of 2. These objects had been searched for in [HK94] and [CHK02] up to length 23, but the pairs found were, for the most part, left unexplained.

Very few general nonexistence results for Golay sequence pairs have been found. In 1961, Golay showed that the length of a binary Golay sequence pair must be even [Gol61]. 30 years later, Eliahou, Kervaire and Saffari proved that the length of a binary pair has no prime factor congruent to 3 modulo 4 [EKS91]. To our knowledge, these imply all known nonexistence results and there are none for phases other than binary.

We summarize the major contributions of this thesis below:

1. A classification of all ordered quaternary Golay sequence pairs of length less than 22. We show that all of the even-length pairs can be explained by combining the three-stage construction process of [FJP08] with other construction methods.

2. The derivation of a quaternary Golay sequence pair whose length is congruent to 5 modulo 8 from a binary Barker sequence of the same odd length. This is the first known relationship between binary Barker and quaternary Golay sequences.

3. A partial converse to item 2 above. Since there are no Barker sequences of odd length greater than 13 (see Theorem 2.2), we rule out the existence of quaternary Golay sequence pairs satisfying certain conditions beyond length 13.

The remainder of this thesis is organized as follows. Chapter 2 contains notations, definitions and background results. Chapter 3 presents our classification of all ordered quaternary Golay sequence pairs of length less than 22 and explains the existence, with the exception of lengths 3 and 11, of all such pairs. In particular, we give a general derivation of quaternary Golay pairs from binary Barker sequences of length congruent to 5 modulo 8 and apply it to lengths 5 and 13. In Chapter 4, we prove a series of lemmas that provide a partial result for constructing binary Barker sequences from quaternary Golay pairs of length congruent to 5 modulo 8. Finally, Chapter 5 provides concluding remarks and comments on some open problems.

Chapter 2

Background and Notation

2.1 H-phase, $H^{(0)}$-phase and sequences over $\mathbb{Z}_H$

When working with Barker or Golay sequences, there are two different notations commonly used. Firstly, let $A = (A_0, ..., A_{n-1})$ be a complex-valued sequence of length n. For a finite set S, we say that A is a *sequence over* S if $A_j \in S$ for all j satisfying $0 \leq j < n$; here, S is called the sequence *alphabet*. If $S = \{1, \xi, \xi^2, ..., \xi^{H-1}\}$ or $S = \{0, 1, \xi, \xi^2, ..., \xi^{H-1}\}$ for some integer H, where ξ is a primitive H^{th} root of unity, then A is an H*-phase* or $H^{(0)}$*-phase* sequence respectively. In this thesis, we are only interested in *binary* (2-phase, $S = \{1, -1\}$), *ternary* ($2^{(0)}$-phase, $S = \{0, 1, -1\}$) and *quaternary* (4-phase, $S = \{1, i, -1, -i\}$ where $i = \sqrt{-1}$ throughout this thesis) sequences. For example,

$$\begin{pmatrix} 1 & 1 & 1 & -1 & 1 \end{pmatrix} \tag{2.1}$$

is a binary (and ternary, and quaternary) sequence of length 5,

$$\begin{pmatrix} 1 & 0 & -1 \end{pmatrix}$$

is a ternary sequence of length 3, and

$$\begin{pmatrix} 1 & i & -1 & 1 & -i \end{pmatrix} \tag{2.2}$$

is a quaternary sequence of length 5.

The second notation applies to an H-phase sequence $A = (A_0, ..., A_{n-1})$ only; define the sequence $A' = (a_0, ..., a_{n-1})$ over $\mathbb{Z}_H := \{0, 1, ..., H-1\}$ by the relationship

$$\xi^{a_j} := A_j \text{ for all } j \text{ satisfying } 0 \leq j < n.$$

Then we say that A' is the sequence over $\mathbb{Z}_H$ *corresponding to* A, and that A is the H-phase sequence *corresponding to* A'. For example, the sequences (0 0 0 2 0) and (0 1 2 0 3) over $\mathbb{Z}_4$ correspond to the sequences (2.1) and (2.2) respectively. Throughout this thesis, when we say a sequence is complex-valued, we are implying that the sequence is not represented over $\mathbb{Z}_H$ (even though technically speaking sequences over $\mathbb{Z}_H$ are complex-valued). In addition, we primarily work with sequences over $\mathbb{Z}_4$ and label the sequence elements with lower-case letters corresponding to the letter representing the sequence (for example, a_j is the j^{th} element of A); upper-case letters for sequence elements are reserved for complex-valued sequences. Furthermore, we often refer to both a 4-phase (2-phase) sequence and its corresponding sequence over $\mathbb{Z}_4$ (over $\mathbb{Z}_2$) as a quaternary (binary) sequence, as they both represent the same combinatorial object.

For sequences A and B of length n over some alphabet, we define the length n sequence $A+B$ to be the sequence obtained through element-wise addition of A and B. If A and B are sequences over $\mathbb{Z}_H$, we reduce each element of $A+B$ modulo H so that $A+B$ is also a sequence over $\mathbb{Z}_H$. We note here that the sum of two H-phase sequences is not, in general, the same combinatorial object as the sum of the two corresponding sequences over $\mathbb{Z}_H$. For example, if $A = (\ 1 \quad 1 \quad -1)$ and $B = (\ i \quad -i \ \ -1)$ are 4-phase sequences of length 3, then their corresponding sequences over $\mathbb{Z}_4$ are $A' = (0\ 0\ 2)$ and $B' = (1\ 3\ 2)$, and

$$\begin{aligned} A+B &= (\ 1+i \quad 1-i \quad -2\ ), \\ A'+B' &= (\quad 1 \qquad 3 \qquad 0\quad). \end{aligned}$$

Clearly $A+B$ and $A'+B'$ do not correspond, as $A+B$ is not even a 4-phase sequence. Thus adding H-phase sequences and adding corresponding sequences over $\mathbb{Z}_H$ are two different operations.

For sequences A and B of length n and m respectively, we define the sequence $(A;B)$, the *concatenation* of A and B, to be the length $n+m$ sequence defined by

$$(A;B) := (a_0, ..., a_{n-1}, b_0, ..., b_{m-1}).$$

In addition, when $m = n-1$ or n, we define the sequence $\text{int}(A,B)$, the *interleaving* of A and B, to be the length $2n-1$ or $2n$ sequence defined by

$$\text{int}(A,B) := (a_0, b_0, a_1, b_1, ..., b_{n-2}, a_{n-1})$$

or

$$\text{int}(A,B) := (a_0, b_0, a_1, b_1, ..., a_{n-1}, b_{n-1})$$

respectively. In contrast to the addition of two sequences, the combinatorial object obtained via concatenation or interleaving is independent of the sequences' representation.

2.2 Barker and Golay sequences

The *aperiodic autocorrelation function* of a complex-valued sequence A of length n is given by

$$C_A(u) := \sum_{j=0}^{n-u-1} A_j \overline{A_{j+u}} \text{ for integer } u \geq 0, \tag{2.3}$$

where bar represents complex conjugation, and

$$C_A(u) := \overline{C_A(-u)} \text{ for integer } u < 0.$$

The *aperiodic autocorrelation function* of a sequence over $\mathbb{Z}_H$ is that of the corresponding H-phase sequence; thus, for a sequence $(a_0, ..., a_{n-1})$ over $\mathbb{Z}_4$ and integer $u \geq 0$,

$$C_A(u) = \sum_{j=0}^{n-u-1} i^{a_j - a_{j+u}}.$$

A binary or quaternary sequence A is a *Barker sequence* if

$$|C_A(u)| \in \{0, 1\} \text{ for all } u \neq 0.$$

A simple argument establishes the exact value of an odd length binary Barker sequence's aperiodic autocorrelation function:

Lemma 2.1 (Turyn and Storer [TS61]). *Let A be a binary Barker sequence of odd length n. Then*

(i) $C_A(2u+1) = 0$ *for all u satisfying* $0 \leq u < \frac{n-1}{2}$, *and*

(ii) $C_A(2u) = (-1)^{\frac{n-1}{2}}$ *for all u satisfying* $0 < u \leq \frac{n-1}{2}$.

The following sequences, written over $\mathbb{Z}_4$, are examples of binary Barker sequences of length

$n > 1$:

$$\begin{aligned} n = 2: &\quad (0\ 0) \\ n = 3: &\quad (0\ 0\ 2) \\ n = 4: &\quad (0\ 0\ 0\ 2) \\ n = 5: &\quad (0\ 0\ 0\ 2\ 0) \\ n = 7: &\quad (0\ 0\ 0\ 2\ 2\ 0\ 2) \\ n = 11: &\quad (0\ 0\ 0\ 2\ 2\ 2\ 0\ 2\ 2\ 0\ 2) \\ n = 13: &\quad (0\ 0\ 0\ 0\ 0\ 2\ 2\ 0\ 0\ 2\ 0\ 2\ 0) \end{aligned}$$

No binary Barker sequences of length greater than 13 are known. In fact:

Theorem 2.2 (Turyn and Storer [TS61]). *There are no binary Barker sequences of odd length greater than 13.*

The even length case is still open, but with the smallest open case having length $> 10^{22}$ (see [Jed08] for historical details), it looks more than likely that no binary Barker sequence exists beyond length 13. This is commonly known as the "Barker Sequence Conjecture":

Conjecture 2.3 (Barker Sequence Conjecture). *There is no binary Barker sequence of length greater than 13.*

A sequence pair (A, B) is a *Golay sequence pair* of length n if A and B have length n and

$$C_A(u) + C_B(u) = 0 \text{ for all } u \neq 0.$$

For example, the pair

$$((0, 0, 0, 3, 1), (0, 1, 2, 0, 3))$$

over $\mathbb{Z}_4$ is a quaternary Golay sequence pair of length 5, and the pair

$$((0, 0, 2, 0, 2, 0, 2, 2, 0, 0), (0, 0, 2, 0, 0, 0, 0, 0, 2, 2))$$

over $\mathbb{Z}_4$ is a binary Golay sequence pair of length 10. A sequence A is called a *Golay sequence* if it forms a Golay pair with some sequence B. A Golay sequence can be viewed as a natural relaxation of the definition of a Barker sequence of even length: one can easily check that if $\mathrm{int}(A, B)$ is a Barker sequence of length $2n$, then (A, B) forms a Golay pair of length n.

For an ordered Golay sequence pair (A, B) of length n over $\mathbb{Z}_H$ (by ordered, we mean the pair (A, B) is considered to be distinct from the pair (B, A) when $A \neq B$), it is well known that any combination of the following transformations preserves the Golay property:

$$\begin{aligned}
\text{reverse both: } (a_j) &\mapsto (a_{n-j-1}) \quad \text{and} \quad (b_j) \mapsto (b_{n-j-1}) && (2.4)\\
\text{interchange: } (a_j) &\mapsto (b_j) \quad \text{and} \quad (b_j) \mapsto (a_j) && (2.5)\\
\text{negative reverse: } (a_j) &\mapsto (-a_{n-j-1} \bmod H) \text{ or } (b_j) \mapsto (-b_{n-j-1} \bmod H) && (2.6)\\
\text{constant offset: } (a_j) &\mapsto ((a_j+1) \bmod H) \text{ or } (b_j) \mapsto ((b_j+1) \bmod H) && (2.7)\\
\text{incremental offset: } (a_j) &\mapsto ((a_j+j) \bmod H) \text{ and } (b_j) \mapsto ((b_j+j) \bmod H) && (2.8)
\end{aligned}$$

The sequence resulting from applying transformation (2.6) to the sequence A over $\mathbb{Z}_H$ is often given the special notation A^*. Following [CHK02], any two ordered Golay pairs that can be obtained from one another via any combination of transformations (2.4) to (2.8) are called *equivalent*. In addition, note that for an ordered $H^{(0)}$-phase Golay sequence pair (A, B) of length n, and ξ a primitive H^{th} root of unity, the corresponding transformations

$$\begin{aligned}
\text{reverse both: } (A_j) &\mapsto (A_{n-j-1}) \text{ and } (B_j) \mapsto (B_{n-j-1}) && (2.9)\\
\text{interchange: } (A_j) &\mapsto (B_j) \quad \text{and} \quad (B_j) \mapsto (A_j) && (2.10)\\
\text{conjugate reverse: } (A_j) &\mapsto (\overline{A_{n-j-1}}) \quad \text{or} \quad (B_j) \mapsto (\overline{B_{n-j-1}}) && (2.11)\\
\text{constant offset: } (A_j) &\mapsto (\xi A_j) \quad \text{or} \quad (B_j) \mapsto (\xi B_j) && (2.12)\\
\text{incremental offset: } (A_j) &\mapsto (\xi^j A_j) \quad \text{and} \quad (B_j) \mapsto (\xi^j B_j) && (2.13)
\end{aligned}$$

also preserve the Golay property (and again, the sequence resulting from applying (2.11) to A is denoted A^*).

The following well-known symmetry lemma allows us to transform one Golay pair into another, in general non-equivalent, pair:

Lemma 2.4. *For sequences A, B of length n over a complex-valued alphabet, and integer u satisfying $0 \le u < n$,*

$$C_{A+B}(u) + C_{A-B}(u) = 2C_A(u) + 2C_B(u).$$

Proof. For u satisfying $0 \le u < n$,

$$\begin{aligned}
C_{A+B}(u) + C_{A-B}(u) &= \sum_{j=0}^{n-u-1} \Big((A_j + B_j)\overline{(A_{j+u} + B_{j+u})} + (A_j - B_j)\overline{(A_{j+u} - B_{j+u})} \Big)\\
&= \sum_{j=0}^{n-u-1} \big(2A_j\overline{A_{j+u}} + 2B_j\overline{B_{j+u}} \big)
\end{aligned}$$

$$= \quad 2C_A(u) + 2C_B(u). \quad \square$$

Corollary 2.5. *The sequence pair (A, B) forms a Golay pair of length n over some complex-valued alphabet if and only if the sequence pair $(A+B, A-B)$ forms a Golay pair of length n over some complex-valued alphabet.*

The next theorem presents the classic "quads property" of nontrivial (i.e. length greater than 1) binary Golay sequence pairs. There are several different proofs of the property and we present one of them here:

Theorem 2.6 (Golay [Gol61])**.** *For a Golay sequence pair (A, B) over $\mathbb{Z}_2$ of length $n \geq 2$,*

$$a_u + b_u + a_{n-u-1} + b_{n-u-1} \equiv 1 \pmod 2 \text{ for all } u \text{ satisfying } 0 \leq u < n.$$

Proof. We adopt a similar argument to that given in [TS61]. Let u satisfy $1 \leq u \leq n-1$ and consider

$$0 = C_A(u) + C_B(u) = \sum_{j=0}^{n-u-1} (-1)^{a_j + a_{j+u}} + \sum_{j=0}^{n-u-1} (-1)^{b_j + b_{j+u}}.$$

Since each term of the summations is either 1 or -1 and they all sum to zero, the number of 1 terms equals the number of -1 terms. Thus there are exactly $n-u$ terms equal to -1 and so multiplying the terms in the summations gives

$$\prod_{j=0}^{n-u-1} (-1)^{a_j + a_{j+u}} \prod_{j=0}^{n-u-1} (-1)^{b_j + b_{j+u}} = (-1)^{n-u}. \tag{2.14}$$

For $u = n-1$, this gives

$$(-1)^{a_0 + a_{n-1} + b_0 + b_{n-1}} = -1$$

and so the result holds for $u = n-1$ (and, by symmetry, for $u = 0$). For $u < n-1$, by considering $C_A(u+1) + C_B(u+1)$, we similarly get

$$\prod_{j=0}^{n-u-2} (-1)^{a_j + a_{j+u+1}} \prod_{j=0}^{n-u-2} (-1)^{b_j + b_{j+u+1}} = (-1)^{n-u-1}. \tag{2.15}$$

Then multiplying (2.14) and (2.15) gives

$$\begin{aligned} -1 &= \prod_{j=0}^{n-u-1} (-1)^{a_j + a_{j+u} + b_j + b_{j+u}} \prod_{j=0}^{n-u-2} (-1)^{a_j + a_{j+u+1} + b_j + b_{j+u+1}} \\ &= (-1)^{a_u + a_{n-u-1} + b_u + b_{n-u-1}}, \end{aligned}$$

completing the proof. $\square$

Corollary 2.7. *All nontrivial binary Golay sequence pairs have even length.*

Proof. Setting $j = \frac{n-1}{2}$ in Theorem 2.6 with $n > 1$ odd gives a contradiction. □

A classical method of constructing larger Golay sequences from smaller ones is the concatenation procedure (or *doubling* as it is referred to in [HK94] and [CHK02]):

Theorem 2.8 (Golay [Gol61])**.** *If (A, B) is a complex-valued Golay sequence pair of length n, then $((A; B), (A; -B))$ is a complex-valued Golay sequence pair of length $2n$.*

Occasionally, it is useful to study the *aperiodic cross-correlation function* of the complex-valued sequences A of length n and B of length m, given by

$$C_{AB}(u) := \sum_{j=0}^{\min\{n-1, m-u-1\}} A_i \overline{B_{i+u}} \text{ for integer } u \geq 0.$$

Again, the *aperiodic cross-correlation function* of two sequences over $\mathbb{Z}_H$ is that of the corresponding H-phase sequences. One can easily verify the following:

Lemma 2.9. *For sequences A, B and integer $u \geq 0$,*

(i) $C_{\mathrm{int}(A,B)}(2u) = C_A(u) + C_B(u)$, *and*

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

This gives rise to another classical method, the interleaving procedure, of obtaining a Golay pair from another Golay pair of half the length:

Theorem 2.10 (Golay [Gol61])**.** *If (A, B) is a complex-valued Golay sequence pair of length n, then $(\mathrm{int}(A, B), \mathrm{int}(A, -B))$ is a complex-valued Golay sequence pair of length $2n$.*

For a complex-valued sequence A of length n, the *generating function of* A is defined as

$$A(x) := \sum_{j=0}^{n-1} A_j x^j, \text{ for real } x.$$

We will always use the same letter (in this case A) to denote both the sequence and the generating function. We define the *energy* of A to be

$$\epsilon(A) := \sum_{j=0}^{n-1} |A_j|^2.$$

If we define $\phi(A(x)) := \overline{A(x)}A(x^{-1})$, one can easily show that for $x \neq 0$,

$$\begin{aligned}\phi(A(x)) &= \sum_{u\in\mathbb{Z}} C_A(u)x^u \\ &= \epsilon(A) + \sum_{u\neq 0} C_A(u)x^u.\end{aligned}$$

It follows that, for sequences A and B of equal length,

$$A \text{ and } B \text{ form a Golay sequence pair if and only if } \phi(A(x)) + \phi(B(x)) \text{ is constant.} \quad (2.16)$$

Also note that, for any integer j,

$$\phi(x^j A(x)) = \phi(A(x)) \quad (2.17)$$

and, since $\phi(A(x^j)) + \phi(B(x^j))$ is constant if and only if $\phi(A(x)) + \phi(B(x))$ is constant, by (2.16) and (2.17) we have:

Lemma 2.11. *Let j, k, ℓ be integers. The sequences with generating functions $x^k A(x^j)$ and $x^\ell B(x^j)$ form a Golay pair if and only if the sequences with generating functions $A(x)$ and $B(x)$ form a Golay pair.*

2.3 Golay arrays

The definitions of Barker and Golay sequences can easily be generalized to higher dimensions. In this thesis, we are concerned only with the Golay higher-dimensional objects, so we omit the discussion of Barker arrays here.

We define an *array* of size $n_1 \times \cdots \times n_r$ to be an r-dimensional array $\mathcal{A} = (A[j_1, ..., j_r])$, where $j_1, ..., j_r$ are integers, for which

$$A[j_1, ..., j_r] = 0 \text{ if } j_k < 0 \text{ or } j_k \geq n_k \text{ for at least one } k \in \{1, ..., r\}.$$

Call the set of array elements

$$\{A[j_1, ..., j_r] \mid 0 \leq j_k < n_k \text{ for all } k\}$$

the *in-range entries* of $\mathcal{A}$. Similar to the corresponding sequence definitions, $\mathcal{A}$ is an *array over the alphabet* S if all the in-range entries of $\mathcal{A}$ lie in S. When ξ is a primitive H^{th} root of unity and $S = \{1, \xi, \xi^2, ..., \xi^{H-1}\}$, $\mathcal{A}$ is an *H-phase array*. In this case, the *array over*

$\mathbb{Z}_H$ *corresponding to* $\mathcal{A}$ is the $n_1 \times \cdots \times n_r$ array $(a[j_1, ..., j_r])$ whose in-range entries are obtained via

$$\xi^{a[j_1,...,j_r]} := A[j_1, ..., j_r] \text{ for all } (j_1, ..., j_r).$$

The *aperiodic autocorrelation function* of an $n_1 \times \cdots \times n_r$ complex-valued array $\mathcal{A}$ is given by

$$C_{\mathcal{A}}(u_1, ..., u_r) := \sum_{j_1} ... \sum_{j_r} A[j_1, ..., j_r]\overline{A[j_1 + u_1, ..., j_r + u_r]} \text{ for integers } u_1, ..., u_r$$

and again, the *aperiodic autocorrelation function* of an array over $\mathbb{Z}_H$ is that of the corresponding H-phase array. Note that in the case $r = 1$, this definition is equivalent to the definition of the aperiodic autocorrelation function for sequences. Also note that with arrays, for example $r = 2$, in-range entries are a convenient way to define both $C_A(u_1, u_2)$ and $C_A(-u_1, u_2)$ for $u_1 \neq 0$ simultaneously. (We could have defined in-range entries for sequences similarly to how we have for arrays, but we considered this an unnecessary complication.) We say the array pair $(\mathcal{A}, \mathcal{B})$ is a *Golay array pair* of size $n_1 \times \cdots \times n_r$ if both $\mathcal{A}$ and $\mathcal{B}$ are of size $n_1 \times \cdots \times n_r$ and

$$C_{\mathcal{A}}(u_1, ..., u_r) + C_{\mathcal{B}}(u_1, ..., u_r) = 0 \text{ for all } (u_1, ..., u_r) \neq (0, ..., 0),$$

and $\mathcal{A}$ is a *Golay array* if it forms a Golay array pair with some array $\mathcal{B}$.

Similar to transformation (2.11), for $\mathcal{A} = (A[j_1, ..., j_r])$ a complex-valued array of size $n_1 \times \cdots \times n_r$, we define $\mathcal{A}^* = (A^*[j_1, ..., j_r])$ to be the $n_1 \times \cdots \times n_r$ array given by

$$A^*[j_1, ..., j_r] := \overline{A[n_1 - j_1 - 1, ..., n_r - j_r - 1]} \text{ for all } (j_1, ..., j_r).$$

If A^* (and thus A) is an H-phase array, the corresponding array $(a^*[j_1, ..., j_r])$ over $\mathbb{Z}_H$ is given by

$$a^*[j_1, ..., j_r] = -a[n_1 - j_1 - 1, ..., n_r - j_r - 1] \bmod H, \text{ for all } (j_1, ..., j_r).$$

In Chapter 3, we apply the three-stage array construction process introduced in [FJP08] to help classify all ordered quaternary Golay sequence pairs of length less than 22. Stage 1 of this process builds a Golay array pair from an arbitrary number of Golay sequence pairs. An auxiliary construction for Stage 1 is the following product construction using two H-phase Golay sequence pairs, one of which satisfies a particular condition:

Theorem 2.12 (Fiedler, Jedwab and Parker [FJP08, Theorem 4])**.** *Suppose that* (A, B) *is an* H*-phase Golay sequence pair of length* n*. Suppose that* (C, D) *is an* H*-phase Golay sequence pair of length* m *and that*

$$\text{for each } k = 0, 1, ..., m-1, \text{ either } C_k = D_k \text{ or } C_k = -D_k. \tag{2.18}$$

Then the H*-phase arrays* $(F[j, k])$ *and* $(G[j, k])$ *of size* $n \times m$ *given by*

$$\begin{aligned} F[j,k] &:= A_j \cdot \left(\frac{C_k + D_k}{2}\right) + B_j \cdot \left(\frac{C_k - D_k}{2}\right), \\ G[j,k] &:= A_j \cdot \left(\frac{C_k^* - D_k^*}{2}\right) - B_j \cdot \left(\frac{C_k^* + D_k^*}{2}\right) \end{aligned}$$

form a Golay array pair.

After overcoming condition (2.18) by adding a dimension of size 2 and then generalizing to more inputs, we obtain the construction of Stage 1. Note that the following theorem uses array notation for sequences to avoid double subscripts:

Theorem 2.13 (Fiedler, Jedwab and Parker [FJP08, Theorem 7])**.** *Let* $m \geq 1$ *be an integer. Suppose that* $A_k = (a_k[j_k])$ *and* $B_k = (b_k[j_k])$ *form a Golay sequence pair of length* n_k *over* $\mathbb{Z}_H$*, for* $k = 0, 1, ..., m$*. Then the arrays* $(f_m[j_0, ..., j_m, x_1, ..., x_m])$ *and* $(g_m[j_0, ..., j_m, x_1, ..., x_m])$ *of size* $n_0 \times \cdots \times n_m \times 2 \times \cdots \times 2$ *(where* m *copies of* 2 *appear) over* $\mathbb{Z}_H$ *given by*

$$\begin{aligned} f_m[j_0, ..., j_m, x_1, ..., x_m] &:= \sum_{k=1}^{m-1} \left(a_k[j_k] + a_k^*[j_k] - b_k[j_k] - b_k^*[j_k] + \frac{H}{2}\right) x_k x_{k+1} + \\ &\quad \sum_{k=1}^{m} \left(b_{k-1}^*[j_{k-1}] + b_k[j_k] - a_{k-1}[j_{k-1}] - a_k[j_k]\right) x_k + \sum_{k=0}^{m} a_k[j_k], \\ g_m[j_0, ..., j_m, x_1, ..., x_m] &:= f'_m[j_0, ..., j_m, x_1, ..., x_m] + \frac{H}{2} x_1, \end{aligned}$$

form a Golay array pair, where $f'_m[j_0, ..., j_m, x_1, ..., x_m]$ *is* $f_m[j_0, ..., j_m, x_1, ..., x_m]$ *with* $a_0[j_0]$*,* $b_0[j_0]$ *interchanged and with* $a_0^*[j_0], b_0^*[j_0]$ *interchanged.*

Stage 2 of the three-stage process sees a generalization of the constant offset (2.7) and incremental offset (2.8) transformations applied to Golay array pairs to create additional Golay array pairs from those constructed in Stage 1. The following lemma says that any "affine offset" of a Golay array pair over $\mathbb{Z}_H$ is also a Golay array pair:

Lemma 2.14 (Fiedler, Jedwab and Parker [FJP08, Lemma 8]). *Suppose that* $((a[j_1,...,j_r]),(b[j_1,...,j_r]))$ *is an* $n_1 \times \cdots \times n_r$ *Golay array pair over* $\mathbb{Z}_H$*. Then*

$$\left(\left(a[j_1,...,j_r]+\sum_{k=1}^{r}e_kj_k+e_0\right),\left(b[j_1,...,j_r]+\sum_{k=1}^{r}e_kj_k+e_0'\right)\right)$$

is also an $n_1 \times \cdots \times n_r$ *Golay array pair over* $\mathbb{Z}_H$*, for all* $e_0', e_0, e_1, ..., e_r \in \mathbb{Z}_H$*.*

Before finally presenting Stage 3, we first need a definition. Given an $n_1 \times \cdots \times n_r$ array $\mathcal{A} = (a[j_1,...,j_r])$, we define the "projection mapping" $\psi_{1,2}(\mathcal{A})$ to be the array $(b[j,j_3,...,j_r])$ of size $n_1n_2 \times n_3 \times \cdots \times n_r$ given by

$$b[j_1+n_1j_2,j_3,...,j_r] := a[j_1,...,j_r] \text{ for all } (j_1,...,j_r).$$

For example, if $\mathcal{A}$ is the array of size 3×2 over $\mathbb{Z}_4$ whose in-range entries are given by

$$\mathcal{A} = \begin{pmatrix} 0 & 3 \\ 1 & 4 \\ 2 & 5 \end{pmatrix},$$

then

$$\psi_{1,2}(\mathcal{A}) = (0\ 1\ 2\ 3\ 4\ 5)$$

can be obtained by reading off the columns of $\mathcal{A}$ in order. For distinct $k, \ell \in \{1,...,r\}$, we similarly define the array $\psi_{k,\ell}(\mathcal{A})$ by removing the array argument j_k and replacing the array argument j_ℓ by $j_k+n_kj_\ell$. Thus in the example above, we can calculate $\psi_{2,1}(\mathcal{A}) = (0\,3\,1\,4\,2\,5)$ by reading off the rows of $\mathcal{A}$ in turn.

Theorem 2.15 (Jedwab and Parker [JP07a, Theorem 11 and subsequent remarks]). *For integer* $r \geq 2$*, suppose that* $\mathcal{A}$ *and* $\mathcal{B}$ *form an* $n_1 \times \cdots \times n_r$ *Golay array pair over an alphabet* S*. Then, for distinct* $j,k \in \{1,...,r\}$*,* $\psi_{j,k}(\mathcal{A})$ *and* $\psi_{j,k}(\mathcal{B})$ *form a Golay array pair over* S*.*

The final stage of the three-stage process successively applies Theorem 2.15, each time reducing the dimension of the input Golay array pair by 1, until the resulting Golay array has dimension 1 (and thus can be interpreted as a sequence).

Chapter 3

A Classification of Quaternary Golay Sequences of Small Length

There have been several studies concerned with enumerating, classifying and explaining the origin of binary Golay sequences of small length; see, for example, [BF03], [JP07a] and [JP08]. While quaternary Golay sequences have not been completely ignored, they have certainly received less attention. Holzmann and Kharaghani computed by exhaustive search all ordered quaternary Golay sequence pairs up to length 13 [HK94] and then with Craigen furthered the search up to length 23 (though not exhaustively for lengths 20, 22 and 23) [CHK02]. For each length, they partitioned the pairs into equivalence classes arising from the transformations (2.4) to (2.8). See Table 3.1 for a summary of these results. Note that the exact number of ordered quaternary Golay sequence pairs of length 20 is now known to be 215040 [Fie].

Along with the search results, they comment that since there are no quaternary Golay sequences of length 9 or 15, there cannot be a product construction obtaining a length st quaternary Golay sequence pair from a length s pair and a length t pair [CHK02]. However, Theorem 2.12 and Theorem 2.15 state that we do have such a product construction when condition (2.18) holds for one of the pairs; it just so happens that no length 3 or length 5 quaternary Golay pair satisfies (2.18). Furthermore, other than referring to Theorem 2.8, no attempt is made in [CHK02] to explain the origin of the sequence pairs that do exist.

Table 3.1: Ordered quaternary Golay sequence pair counts via exhaustive search for small lengths n [CHK02].

n	# of ordered quaternary Golay sequence pairs	# of equivalence classes
1	16	1
2	64	1
3	128	1
4	512	2
5	512	1
6	2048	3
7	0	0
8	6656	17
9	0	0
10	12288	20
11	512	1
12	36864	52
13	512	1
14	0	0
15	0	0
16	106496	204
17	0	0
18	24576	24
19	0	0
20	many	many
21	0	0
22	many	many
23	possibly 0	possibly 0

Using small "seed pairs" and the three-stage array construction process [FJP08], as well as an original construction and previous results in [EKS91] and [JF06], we can classify and explain the existence of all quaternary Golay sequence pairs of length less than 22, except for lengths 3 and 11. We focus here on answering two questions:

- How many ordered quaternary Golay sequence pairs counted in Table 3.1 (and the recent length 20 count) arise from the three-stage array construction process and other constructions?
- How do the seed pairs arise?

3.1 Even lengths except 10 and 20

In this section, we show that many of the quaternary Golay sequence pairs of even length less than 22 can be explained using recent results. To start, consider length 6. Table 3.2 (below) shows the three class representatives given in [HK94] for Golay pairs of length $n = 6$ over $\mathbb{Z}_4$. While the existence of the second class is explained through Theorem 2.8 in [CHK02], the remaining two are left unexplained. In fact, the first class in Table 3.2 can be obtained through Theorem 2.10, whose use appears to have been overlooked in [CHK02]; however, this fact is not needed in our classification.

Table 3.2: Holzmann and Kharaghani's equivalence class representatives for length 6 Golay sequence pairs over $\mathbb{Z}_4$. The trailing D indicates that the class can be constructed via Theorem 2.8 from Golay sequence pairs of length 3 over $\mathbb{Z}_4$ [HK94].

(0 0 0 1 2 0)	(0 0 3 2 0 2)	
(0 0 2 0 1 0)	(0 0 2 2 3 2)	D
(0 0 2 1 2 0)	(0 0 3 0 0 2)	

We can construct quaternary Golay sequence pairs of length 6 following the three-stage construction process (see Section 2.3):

Stage 1. We wish to apply Theorem 2.13 to construct Golay array pairs over $\mathbb{Z}_4$. In anticipation of projecting these arrays down to sequences of length 6, we require that each array have exactly 6 entries. Thus if we take a length 3 Golay pair over $\mathbb{Z}_4$ and a trivial length 1 Golay pair over $\mathbb{Z}_4$ as inputs into Theorem 2.13 (with $m = 1$), we will obtain a Golay array pair of size $3 \times 1 \times 2$ up to reordering of dimensions, which has the desired number of entries.

So, take the two ordered Golay sequence pairs

$$((2\ 0\ 0), (0\ 1\ 0)) \tag{3.1}$$

and

$$((2\ 0\ 0), (0\ 3\ 0)) \tag{3.2}$$

of length 3 over $\mathbb{Z}_4$. Up to constant and incremental offsets (2.7) and (2.8), it is easy to check that these two are the only such pairs. Note that we do not need to worry about transformations (2.7) and (2.8) in Stage 1 as the more general transformations applied in Stage 2 (Lemma 2.14) account for these other potential inputs (see Appendix A). Then along with the trivial length 1 pair $((0),(0))$ and by reordering the inputs, we obtain 4 sets of input parameters for Theorem 2.13. These 4 sets of parameters, along with the output ordered Golay array pairs with their singleton dimensions removed, are displayed below:

$$a_0 = (2\ 0\ 0), b_0 = (0\ 1\ 0), a_1 = (0), b_1 = (0) \quad \mapsto \quad f_1 = \begin{pmatrix} 2 & 0 \\ 0 & 3 \\ 0 & 0 \end{pmatrix}, g_1 = \begin{pmatrix} 0 & 2 \\ 1 & 2 \\ 0 & 0 \end{pmatrix};$$

$$a_0 = (0), b_0 = (0), a_1 = (2\ 0\ 0), b_1 = (0\ 1\ 0) \quad \mapsto \quad f_1 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}, g_1 = \begin{pmatrix} 2 & 2 \\ 0 & 3 \\ 0 & 2 \end{pmatrix};$$

$$a_0 = (2\ 0\ 0), b_0 = (0\ 3\ 0), a_1 = (0), b_1 = (0) \quad \mapsto \quad f_1 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}, g_1 = \begin{pmatrix} 0 & 2 \\ 3 & 2 \\ 0 & 0 \end{pmatrix};$$

$$a_0 = (0), b_0 = (0), a_1 = (2\ 0\ 0), b_1 = (0\ 3\ 0) \quad \mapsto \quad f_1 = \begin{pmatrix} 2 & 0 \\ 0 & 3 \\ 0 & 0 \end{pmatrix}, g_1 = \begin{pmatrix} 2 & 2 \\ 0 & 1 \\ 0 & 2 \end{pmatrix}.$$

Stage 2. For each of the four Golay array pairs arising from Stage 1, we apply Lemma 2.14 to obtain a set of $4^4 = 256$ ordered Golay array pairs of size 3×2 over $\mathbb{Z}_4$. This gives us a total of $4 \cdot 256 = 1024$ ordered Golay array pairs, all of which are distinct.

Stage 3. For each ordered array pair $(\mathcal{A}, \mathcal{B})$ from Stage 2, we apply Theorem 2.15 to obtain the ordered Golay array (sequence) pairs $(\psi_{1,2}(\mathcal{A}), \psi_{1,2}(\mathcal{B}))$ and $(\psi_{2,1}(\mathcal{A}), \psi_{2,1}(\mathcal{B}))$ of size $3 \cdot 2 = 6$. This gives us a total of $2 \cdot 1024 = 2048$ ordered Golay array (sequence) pairs of size 6, all of which are distinct.

Table 3.1 shows that the three-stage process explains all ordered Golay sequence pairs of length 6 over $\mathbb{Z}_4$. Note that the original length 3 pairs (3.1) and (3.2) can be obtained from one another by applying transformation (2.6) (negative reversal) to the second sequence. We can now classify all length 6 ordered Golay sequence pairs over $\mathbb{Z}_4$ by collapsing the 3 equivalence classes into a single class arising from the three-stage process, using the single length 3 ordered Golay pair (3.1) and a trivial length 1 pair over $\mathbb{Z}_4$.

For another example, we turn our attention to length 12 pairs. Table 3.3 displays the equivalence classes found in [HK94], where many of the classes are left unexplained. Again, we apply the three-stage process to construct length 12 ordered Golay sequence pairs over $\mathbb{Z}_4$. As before, we use each of the two ordered Golay sequence pairs (3.1) and (3.2) of length 3, but this time we combine each with two trivial length 1 pairs to form a triple of pairs for input into Theorem 2.13. By reordering the pairs as before, we obtain $2 \cdot \frac{3!}{2!} = 6$ sets of inputs and 6 ordered Golay array pairs of size $3 \times 2 \times 2$ over $\mathbb{Z}_4$ (after removing singleton dimensions) as outputs. To each of these array pairs, we then apply Lemma 2.14 to obtain 4^5 ordered array pairs. Finally, Theorem 2.15 is applied to each of these pairs to obtain 3! sets of length 12 ordered Golay sequence pairs over $\mathbb{Z}_4$, all of which are distinct. This gives us a total of $6 \cdot 4^5 \cdot 3! = 36864$ ordered Golay sequence pairs of length 12 and again, they are all distinct. Table 3.1 again shows that these are indeed all such pairs that exist. Thus, we can classify all length 12 ordered Golay sequence pairs over $\mathbb{Z}_4$ by collapsing all of the equivalence classes into a single class arising from the three-stage process, using the length 3 Golay pair (3.1) and two trivial length 1 pairs over $\mathbb{Z}_4$.

Using this process similarly explains the existence of all ordered quaternary Golay pairs of lengths 2, 4 and 18 from two trivial length 1 pairs, three trivial length 1 pairs and two copies of the length 3 ordered Golay pair (3.1) respectively. However, some ordered pairs of lengths 8, 10, 16 and 20 are not so straightforward to explain. To finish this section, we examine lengths 8 and 16 by summarizing the appropriate results of [JF06] and [FJP08]. Lengths 10 and 20 are reserved for the next section.

For length 8, only $4^5 \cdot 3! = 6144$ of the 6656 ordered pairs are produced via the three-stage process with four trivial length 1 pairs as inputs. The remaining 512 ordered pairs can be explained from an anomalous property known as the "shared autocorrelation property", whereby two sequences have identical aperiodic autocorrelation function, but one cannot be derived from the other using transformations (2.6) and (2.7). When (A_1, B_1) and (A_2, B_2) are Golay pairs and the pair (A_1, A_2) have the shared autocorrelation property, it follows that (A_2, B_1) and (A_1, B_2) are also Golay pairs. The Golay pair

$$((0\ 0\ 0\ 2\ 0\ 0\ 2\ 0), (0\ 1\ 1\ 2\ 0\ 3\ 3\ 2)) \tag{3.3}$$

Table 3.3: Holzmann and Kharaghani's equivalence class representatives for length 12 Golay sequence pairs over $\mathbb{Z}_4$. The trailing D indicates that the class can be constructed via Theorem 2.8 from Golay sequence pairs of length 6 over $\mathbb{Z}_4$ [HK94].

(000022201320)	(001100200202)		(000022310231)	(003300311313)	
(000022312031)	(001100311313)		(000010230220)	(002210010202)	
(000012030220)	(002212210202)		(000210120200)	(000223212022)	
(000212100200)	(000203012022)		(000211020020)	(000222312202)	
(000211200020)	(000200312202)		(000120202100)	(000120020322)	D
(000120221020)	(000120003202)	D	(000120313211)	(000120131033)	D
(000120332131)	(000120110313)	D	(002000132220)	(002011020002)	
(002002212030)	(002220212212)		(002002303121)	(002220303303)	
(002002323101)	(002220323323)		(002022132220)	(002011200002)	
(002010220010)	(002010002232)	D	(002010212200)	(002010030022)	D
(002010323311)	(002010101133)	D	(002010331121)	(002010113303)	D
(002201102020)	(000001322002)		(002220010010)	(002002010232)	
(002222201320)	(001100202002)		(002222310231)	(003300313113)	
(002222312031)	(001100313113)		(002221122020)	(000021302002)	
(002212002030)	(002212220212)	D	(002212113101)	(002212331323)	D
(002101232311)	(002101010133)	D	(002101121200)	(002101303022)	D
(002120200100)	(002120022322)	D	(002120221220)	(002120003002)	D
(002120311211)	(002120133033)	D	(002120332331)	(002120110113)	D
(001002002320)	(001002220102)	D	(001002113031)	(001002331213)	D
(001202000320)	(001202222102)	D	(001202111031)	(001202333213)	D
(001100020220)	(002222023102)		(001100022020)	(000022023102)	
(001110300231)	(003310120213)		(001112100231)	(003312320213)	
(001310230211)	(001323322033)		(001312210211)	(001303122033)	
(001311130031)	(001322022213)		(001311310031)	(001300022213)	
(001333130031)	(001322202213)		(001333310031)	(001300202213)	
(003301212031)	(001101032013)		(003321232031)	(001121012013)	

over $\mathbb{Z}_4$ arises in this manner. Applying transformations (2.4) to (2.8) to this pair yields the 512 remaining ordered pairs. To our knowledge, this is the only known example of additional Golay pairs arising from the shared autocorrelation property.

Finally for length 16, we can explain $4^6 \cdot 4! = 98304$ of the 106496 ordered pairs using five trivial length 1 pairs as inputs into the three-stage process. The missing 8192 ordered pairs can also be explained via the three-stage process. To do so, we can consider the pairs arising from (3.3) and transformations (2.4) to (2.8) as new seed pairs. Thus, we take each of the $\frac{512}{4^3} = 8$ such pairs of length 8, up to transformations (2.7) and (2.8), together with a trivial length 1 pair as input into the process. For more details, see [JF06] and [FJP08].

3.2 Lengths 10 and 20

Table 3.4: Holzmann and Kharaghani's equivalence class representatives for length 10 Golay sequence pairs over $\mathbb{Z}_4$. The trailing D indicates that the class can be constructed via Theorem 2.8 from Golay sequence pairs of length 5 over $\mathbb{Z}_4$ [HK94].

(0000020220)	(0022000202)		(0001031231)	(0032230313)	
(0001301321)	(0001323103)	D	(0001303201)	(0001321023)	D
(0001321231)	(0032300313)		(0001332130)	(0001310312)	D
(0003021031)	(0012332313)		(0003331031)	(0012202313)	
(0020202200)	(0020000022)		(0020303311)	(0020101133)	
(0022112020)	(0000132002)		(0021023231)	(0030330113)	
(0021212311)	(0021010133)		(0021111200)	(0021313022)	
(0021333231)	(0030200113)		(0023033031)	(0010232113)	
(0023323031)	(0010302113)		(0011030231)	(0033010213)	
(0013121001)	(0013103223)	D	(0033122031)	(0011102013)	

In an attempt to classify the length 10 ordered quaternary Golay sequence pairs (see Table 3.4), we shall again use the three-stage construction process. For length 10, we need to take a length 5 pair along with a trivial length 1 pair to obtain an array pair from Theorem 2.13 with exactly 10 entries. It turns out that there are 8 different ordered Golay sequence pairs of length 5 up to transformations (2.7) and (2.8), namely

$$\left.\begin{array}{ll} ((3\ 1\ 0\ 0\ 0), (1\ 2\ 3\ 1\ 0)), & ((3\ 1\ 0\ 0\ 0), (1\ 0\ 2\ 3\ 0)), \\ ((1\ 3\ 0\ 0\ 0), (3\ 0\ 2\ 1\ 0)), & ((1\ 3\ 0\ 0\ 0), (3\ 2\ 1\ 3\ 0)), \\ ((1\ 3\ 1\ 0\ 0), (3\ 0\ 1\ 1\ 0)), & ((1\ 3\ 1\ 0\ 0), (3\ 2\ 2\ 3\ 0)), \\ ((3\ 1\ 3\ 0\ 0), (1\ 2\ 2\ 1\ 0)), & ((3\ 1\ 3\ 0\ 0), (1\ 0\ 3\ 3\ 0)). \end{array}\right\} \tag{3.4}$$

Note that each sequence pair can be obtained from any of the other 8 by a series of transformations (2.4) to (2.6). By again reordering with the length 1 pair, we have 16 sets of inputs to Theorem 2.13 and hence 16 output array pairs of size 5×2 (after removing singleton dimensions). To each of these, we apply the 4^4 transformations from Lemma 2.14 followed by 2! projections from Theorem 2.15. This leaves us with a total of $16 \cdot 4^4 \cdot 2! = 8192$ ordered Golay sequence pairs of length 10 over $\mathbb{Z}_4$ and again, they are all distinct. However, Table 3.1 shows that there are actually a total of 12288 ordered quaternary Golay sequence pairs of length 10. With no more appropriate seed pairs available for inputs, the three-stage process can only classify exactly two-thirds of the length 10 pairs as originating from the length 5 Golay pair $((3\ 1\ 0\ 0\ 0), (1\ 2\ 3\ 1\ 0))$ and a trivial length 1 pair over $\mathbb{Z}_4$. We are left with 8 unexplained equivalence classes of pairs of length 10. A class representative of each is given below:

$$((0\ 0\ 2\ 0\ 2\ 0\ 2\ 2\ 0\ 0), (0\ 0\ 2\ 0\ 0\ 0\ 0\ 0\ 2\ 2)) \tag{3.5a}$$

$$((0\ 0\ 2\ 0\ 3\ 0\ 3\ 3\ 1\ 1), (0\ 0\ 2\ 0\ 1\ 0\ 1\ 1\ 3\ 3)) \tag{3.5b}$$

$$((0\ 0\ 2\ 1\ 1\ 1\ 1\ 2\ 0\ 0), (0\ 0\ 2\ 1\ 3\ 1\ 3\ 0\ 2\ 2)) \tag{3.5c}$$

$$((0\ 0\ 2\ 1\ 2\ 1\ 2\ 3\ 1\ 1), (0\ 0\ 2\ 1\ 0\ 1\ 0\ 1\ 3\ 3)) \tag{3.5d}$$

$$((0\ 0\ 2\ 2\ 0\ 0\ 0\ 2\ 0\ 2), (0\ 0\ 0\ 0\ 0\ 2\ 0\ 2\ 2\ 0)) \tag{3.5e}$$

$$((0\ 0\ 3\ 3\ 0\ 1\ 0\ 2\ 1\ 3), (0\ 0\ 1\ 1\ 0\ 3\ 0\ 2\ 3\ 1)) \tag{3.5f}$$

$$((1\ 0\ 2\ 1\ 0\ 0\ 1\ 2\ 0\ 1), (1\ 0\ 0\ 3\ 0\ 2\ 1\ 2\ 2\ 3)) \tag{3.5g}$$

$$((1\ 0\ 3\ 2\ 0\ 1\ 1\ 2\ 1\ 2), (1\ 0\ 1\ 0\ 0\ 3\ 1\ 2\ 3\ 0)) \tag{3.5h}$$

Each of these classes contains exactly 512 ordered Golay sequence pairs, for a total of 4096 unexplained pairs. (In particular, all of the binary Golay sequence pairs are represented by (3.5a) and (3.5e).)

So, to complete the classification of all length 10 ordered quaternary Golay pairs, it remains to explain the origin of each of the sequence pairs (3.5a) to (3.5h). With no shared autocorrelation property to be found, as was exhibited for length 8 pairs, we must consider a different approach. To this end, we refer to an observation made by Eliahou, Kervaire and Saffari [EKS91]. Given a 2-phase (binary) Golay pair (A_3, B_3), we call the ternary pair (A_2, B_2) the *penultimate pair* of (A_3, B_3), where

$$\begin{aligned} A_2 &:= \frac{A_3 + B_3}{2}, \text{ and} \\ B_2 &:= \frac{(A_3 - B_3)^*}{2}. \end{aligned}$$

By Corollary 2.5, transformation (2.11) (recall that $(A_3 - B_3)^*$ is obtained from $A_3 - B_3$ via transformation (2.11)), and the observation that multiplying all elements in both sequences of a complex-valued Golay pair by a scalar (in this case, $\frac{1}{2}$) preserves the Golay property, (A_2, B_2) forms a ternary Golay pair. We then define the *antepenultimate pair* of (A_3, B_3) to be the sequence pair (A_1, B_1) where

$$\begin{aligned} A_1 &:= \frac{A_2 + B_2}{2}, \text{ and} \\ B_1 &:= \frac{A_2 - B_2}{2} \end{aligned}$$

and again by Corollary 2.5 and multiplication by a scalar, (A_1, B_1) forms a Golay pair over some complex-valued alphabet. But, since the positions of the zero elements of A_2 and B_2 must match due to Theorem 2.6, A_1 and B_1 are also ternary sequences. Note that our definitions of the penultimate and antepenultimate pairs differ slightly from the corresponding definitions in [EKS91]; they perform an additional normalization of the pairs which is unnecessary for our discussion.

If it is easy to see that the antepenultimate pair of (A, B) is a Golay pair, then we can explain the existence of (A, B) by reversing this process under Corollary 2.5. For example, the binary Golay pairs corresponding to (3.5a) and (3.5e) can be explained from the single ternary Golay pair (F, G), where

$$\begin{aligned} F &:= (1 \quad 1 \quad -1) \quad \text{and} \\ G &:= (1 \quad 0 \quad 1), \end{aligned}$$

by comparing the generating functions of F and G with the generating functions of the binary Golay sequences [EKS91]. We now demonstrate this in detail.

Take (A_3, B_3) to be the 4-phase sequence corresponding to (3.5a), so that

$$\begin{aligned} A_3 &= (1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad -1 \quad 1 \quad 1) \quad \text{and} \\ B_3 &= (1 \quad 1 \quad -1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad -1 \quad -1). \end{aligned}$$

The penultimate pair of (A_3, B_3) is (A_2, B_2), where

$$\begin{array}{rcl} A_2 & = & (1\ \ 1\ \ -1\ \ \ 1\ \ \ 0\ \ \ 1\ \ \ 0\ \ 0\ \ 0\ \ 0) \quad \text{and} \\ B_2 & = & (1\ \ 1\ \ -1\ \ -1\ \ 0\ \ -1\ \ 0\ \ 0\ \ 0\ \ 0). \end{array} \tag{3.6}$$

The antepenultimate pair of (A_3, B_3) is then (A_1, B_1), where

$$\begin{array}{rcl} A_1 & = & (1\ \ 1\ \ -1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0) \quad \text{and} \\ B_1 & = & (0\ \ 0\ \ \ \ 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0). \end{array}$$

Now, the generating functions of A_1 and B_1 are

$$\begin{array}{rcccl} A_1(x) & = & 1 + x - x^2 & = & F(x), \text{ and} \\ B_1(x) & = & x^3 + x^5 & = & x^3 G(x). \end{array}$$

So, because (F, G) forms a Golay pair, by Lemma 2.11 so does the pair (A_1, B_1). Hence, $(A_2 = A_1 + B_1, B_2 = A_1 - B_1)$ and therefore $(A_3 = A_2 + B_2^*, B_3 = A_2 - B_2^*)$ are both Golay pairs under Corollary 2.5 and transformation (2.11). We have therefore explained the existence of the pair (3.5a) as being derived from the simple ternary Golay pair (F, G) under two applications of Corollary 2.5.

To explain the existence of (3.5e), we consider the corresponding 4-phase sequences

$$\begin{array}{rcl} A_3 & = & (1\ \ 1\ \ -1\ \ -1\ \ 1\ \ \ 1\ \ \ 1\ \ -1\ \ \ 1\ \ \ -1) \quad \text{and} \\ B_3 & = & (1\ \ 1\ \ \ 1\ \ \ \ 1\ \ \ 1\ \ -1\ \ 1\ \ -1\ \ -1\ \ \ 1). \end{array}$$

The penultimate pair is (A_2, B_2), where

$$\begin{array}{rcl} A_2 & = & (\ 1\ \ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ \ 1\ \ \ -1\ \ 0\ \ 0) \quad \text{and} \\ B_2 & = & (-1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ -1\ \ -1\ \ 0\ \ 0) \end{array}$$

and the antepenultimate pair is (A_1, B_1), where

$$\begin{array}{rcl} A_1 & = & (0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ -1\ \ 0\ \ 0) \quad \text{and} \\ B_1 & = & (1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ \ \ 0\ \ \ 0\ \ 0). \end{array} \tag{3.7}$$

Now, since $A_1(x) = xF(x^3)$ and $B_1(x) = G(x^3)$, by Lemma 2.11 (A_1, B_1) is also a ternary Golay pair. Thus, by two applications of Corollary 2.5 and transformation (2.11), so is (A_3, B_3).

We now explain how to obtain the pairs (3.5b), (3.5c), (3.5d), (3.5f), (3.5g) and (3.5h) similarly from the same ternary pair (F, G). Firstly, we look at the pair (3.5b). Take (A_3, B_3) to be the 4-phase sequence corresponding to (3.5b), so that

$$\begin{aligned} A_3 &= (1 \quad 1 \quad -1 \quad 1 \quad -i \quad 1 \quad -i \quad -i \quad i \quad i) \quad \text{and} \\ B_3 &= (1 \quad 1 \quad -1 \quad 1 \quad i \quad 1 \quad i \quad i \quad -i \quad -i). \end{aligned} \tag{3.8}$$

Next, define $A_2 := \frac{A_3+B_3}{2}$ and $B_2 := \frac{i(A_3-B_3)^*}{2}$ so that

$$\begin{aligned} A_2 &= (1 \quad 1 \quad -1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0) \quad \text{and} \\ B_2 &= (1 \quad 1 \quad -1 \quad -1 \quad 0 \quad -1 \quad 0 \quad 0 \quad 0 \quad 0). \end{aligned} \tag{3.9}$$

Now, (A_2, B_2) is the same as the penultimate pair (3.6) of the 4-phase sequence pair corresponding to (3.5a)! Since the derivation of (3.9) from (3.8) can be reversed (apply transformations (2.11) and (2.12) to B_2, then apply Corollary 2.5), there is no need to proceed further as it is clear that (3.5b) can also be derived from (F, G).

As another example, we examine the pair (3.5g). The corresponding 4-phase sequences are

$$\begin{aligned} A_3 &= (i \quad 1 \quad -1 \quad i \quad 1 \quad 1 \quad i \quad -1 \quad 1 \quad i) \quad \text{and} \\ B_3 &= (i \quad 1 \quad 1 \quad -i \quad 1 \quad -1 \quad i \quad -1 \quad -1 \quad -i). \end{aligned}$$

Take $A_2 := \frac{A_3+B_3}{2}$ and $B_2 := \frac{(A_3-B_3)^*}{2}$ so that

$$\begin{aligned} A_2 &= (i \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad i \quad -1 \quad 0 \quad 0) \quad \text{and} \\ B_2 &= (-i \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad -i \quad -1 \quad 0 \quad 0). \end{aligned}$$

Then take $A_1 := \frac{A_2+B_2}{2}$ and $B_1 = \frac{-i(A_2-B_2)}{2}$ so that

$$\begin{aligned} A_1 &= (0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad -1 \quad 0 \quad 0) \quad \text{and} \\ B_1 &= (1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0). \end{aligned}$$

This time, (A_1, B_1) is equal to the antepenultimate pair (3.7) of the 4-phase sequence pair corresponding to (3.5e), showing that the pair (3.5g) can also be derived from the simple ternary pair (F, G). Table 3.5 breaks down this procedure for each of the pairs (3.5a) to (3.5h).

Table 3.5: Explaining the existence of the Golay pairs (3.5a) to (3.5h) over $\mathbb{Z}_4$ as derived from the simple ternary Golay pair ($F = (1\ 1\ -1), G = (1\ 0\ 1)$) under Corollary 2.5.

$A_1(x)$	$B_1(x)$	A_2	B_2	A_3	B_3	Sequence pair over $\mathbb{Z}_4$ whose corresponding 4-phase sequence pair is (A_3, B_3)
$F(x)$	$x^3G(x)$	$A_1 + B_1$	$A_1 - B_1$	$A_2 + B_2^*$	$A_2 - B_2^*$	(3.5a)
$F(x)$	$x^3G(x)$	$A_1 + B_1$	$A_1 - B_1$	$A_2 + iB_2^*$	$A_2 - iB_2^*$	(3.5b)
$F(x)$	$x^3G(x)$	$A_1 + iB_1$	$A_1 - iB_1$	$A_2 + B_2^*$	$A_2 - B_2^*$	(3.5c)
$F(x)$	$x^3G(x)$	$A_1 + iB_1$	$A_1 - iB_1$	$A_2 + iB_2^*$	$A_2 - iB_2^*$	(3.5d)
$xF(x^3)$	$G(x^3)$	$A_1 + B_1$	$A_1 - B_1$	$A_2 + B_2^*$	$A_2 - B_2^*$	(3.5e)
$xF(x^3)$	$G(x^3)$	$A_1 + B_1$	$A_1 - B_1$	$A_2 + iB_2^*$	$A_2 - iB_2^*$	(3.5f)
$xF(x^3)$	$G(x^3)$	$A_1 + iB_1$	$A_1 - iB_1$	$A_2 + B_2^*$	$A_2 - B_2^*$	(3.5g)
$xF(x^3)$	$G(x^3)$	$A_1 + iB_1$	$A_1 - iB_1$	$A_2 + iB_2^*$	$A_2 - iB_2^*$	(3.5h)

To end this section, we classify all 215040 ordered Golay sequence pairs of length 20 over $\mathbb{Z}_4$ using similar approaches. Firstly, we obtain $8 \cdot \frac{3!}{2!} \cdot 4^5 \cdot 3! = 147456$ ordered pairs from the eight length 5 pairs (3.4) and two trivial length 1 Golay pairs, via the three-stage construction process. We then use the three-stage process again, this time with each of the $\frac{4096}{4^3} = 64$ length 10 pairs represented by the equivalence classes (3.5a) to (3.5h) (up to transformations (2.7) and (2.8)) together with a trivial length 1 pair as input, to construct an additional $64 \cdot 2! \cdot 4^4 \cdot 2! = 65536$ ordered pairs of length 20. This leaves us with 2048 ordered pairs, or 4 classes under transformations (2.4) to (2.8), to explain. These classes have the following representatives:

$$((0\ 0\ 0\ 0\ 2\ 0\ 2\ 2\ 2\ 0\ 0\ 2\ 2\ 0\ 0\ 2\ 0\ 2\ 2\ 0), (0\ 0\ 0\ 0\ 2\ 0\ 0\ 0\ 0\ 0\ 2\ 2\ 2\ 0\ 2\ 0\ 2\ 0\ 0\ 2)) \quad (3.10a)$$
$$((0\ 0\ 0\ 0\ 2\ 0\ 3\ 3\ 3\ 0\ 1\ 2\ 2\ 0\ 1\ 3\ 1\ 3\ 3\ 1), (0\ 0\ 0\ 0\ 2\ 0\ 1\ 1\ 1\ 0\ 3\ 2\ 2\ 0\ 3\ 1\ 3\ 1\ 1\ 3)) \quad (3.10b)$$
$$((0\ 1\ 1\ 0\ 2\ 0\ 1\ 2\ 2\ 0\ 0\ 2\ 2\ 1\ 0\ 2\ 0\ 1\ 1\ 0), (0\ 1\ 1\ 0\ 2\ 0\ 3\ 0\ 0\ 0\ 2\ 2\ 2\ 1\ 2\ 0\ 2\ 3\ 3\ 2)) \quad (3.10c)$$
$$((0\ 1\ 1\ 0\ 2\ 0\ 2\ 3\ 3\ 0\ 1\ 2\ 2\ 1\ 1\ 3\ 1\ 2\ 2\ 1), (0\ 1\ 1\ 0\ 2\ 0\ 0\ 1\ 1\ 0\ 3\ 2\ 2\ 1\ 3\ 1\ 3\ 0\ 0\ 3)) \quad (3.10d)$$

We again adapt Eliahou, Kervaire and Saffari's approach to show that all of these pairs arise from the antepenultimate pair of (3.10a). The antepenultimate pair of (3.10a) is the length 20 ternary pair (H, K), where

$$\begin{array}{lllllllllllllllllllllll} H & := & (1 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 1 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0) & \text{and} \\ K & := & (0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0). & \end{array}$$

The pairs (3.10a) to (3.10d) can then be derived from (H, K) as in Table 3.6. Note that (3.10a) is the length 20 binary seed pair identified in [BF03] and, after [JP08], is the only one of the five binary seed pairs in [BF03] still requiring explanation.

Table 3.6: Explaining the existence of the Golay pairs (3.10a) to (3.10d) over $\mathbb{Z}_4$ as derived from the antepenultimate pair (H, K) of (3.10a) under Corollary 2.5.

$A_1(x)$	$B_1(x)$	A_2	B_2	A_3	B_3	Sequence pair over $\mathbb{Z}_4$ whose corresponding 4-phase sequence pair is (A_3, B_3)
$H(x)$	$K(x)$	$A_1 + B_1$	$A_1 - B_1$	$A_2 + B_2^*$	$A_2 - B_2^*$	(3.10a)
$H(x)$	$K(x)$	$A_1 + B_1$	$A_1 - B_1$	$A_2 + iB_2^*$	$A_2 - iB_2^*$	(3.10b)
$H(x)$	$K(x)$	$A_1 + iB_1$	$A_1 - iB_1$	$A_2 + B_2^*$	$A_2 - B_2^*$	(3.10c)
$H(x)$	$K(x)$	$A_1 + iB_1$	$A_1 - iB_1$	$A_2 + iB_2^*$	$A_2 - iB_2^*$	(3.10d)

3.3 Odd lengths

We now turn our attention to explaining the existence of odd length quaternary Golay sequences. As evidenced in Table 3.1, there are only four equivalence classes of nontrivial odd length Golay sequence pairs over $\mathbb{Z}_4$ of length ≤ 21. A representative of each of these four classes of pairs is:

- $(A_{3,1}, A_{3,2}) = ((0\ 0\ 2), (0\ 1\ 0))$
- $(A_{5,1}, A_{5,2}) = ((0\ 0\ 0\ 3\ 1), (0\ 1\ 2\ 0\ 3))$
- $(A_{11,1}, A_{11,2}) = ((0\ 0\ 0\ 1\ 2\ 0\ 1\ 3\ 1\ 0\ 2), (0\ 1\ 2\ 2\ 2\ 1\ 1\ 0\ 3\ 1\ 0))$
- $(A_{13,1}, A_{13,2}) = ((0\ 0\ 0\ 1\ 2\ 0\ 0\ 3\ 0\ 2\ 0\ 3\ 1), (0\ 1\ 2\ 2\ 2\ 1\ 2\ 0\ 0\ 3\ 2\ 0\ 3))$

Note that because the three-stage construction process adds dimensions of size 2 during Stage 1, it is clear that this process only helps explain existence patterns for even length pairs. Also, we cannot use Theorem 2.12 because each of the lengths 3, 5, 11 and 13 is prime. So, what can be done for odd lengths?

Although published exhaustive search results do not exceed length 21, there is an interesting pattern in the existence results for small lengths. First of all, there is no known quaternary Golay sequence of odd length greater than 13, whereas Theorem 2.2 states that there are no binary Barker sequences of odd length greater than 13. Secondly, with the exception of length 7, lengths $3, 5, 11$ and 13 match the only nontrivial odd lengths for which binary Barker sequences exist. Furthermore, a recent result in [JP08] shows that a binary Golay seed pair of length 10 (as identified in [BF03]) can be derived from a pair of related binary Barker sequences of length 3 and 5, and that the binary Golay seed pair of length 26 can be derived from a pair of related binary Barker sequences of length 11 and 13. We find a pattern in the "offsets" from the binary Barker to the quaternary Golay sequences, which we now discuss.

Consider just the sequence pairs of lengths 5 and 13. Take the Barker sequences

$$\begin{aligned} B_5 &= (0\ 0\ 0\ 2\ 0), \\ B_{13} &= (0\ 0\ 0\ 0\ 0\ 2\ 2\ 0\ 0\ 2\ 0\ 2\ 0) \end{aligned}$$

over $\mathbb{Z}_4$ (which correspond to binary sequences) and calculate the sum with each of the Golay sequences over $\mathbb{Z}_4$ of the respective length:

$$\begin{aligned} B_5 + A_{5,1} &= (0\ 0\ 0\ 1\ 1) = \mathrm{int}((0\ 0\ 1), (0\ 1)), \\ B_5 + A_{5,2} &= (0\ 1\ 2\ 2\ 3) = \mathrm{int}((0\ 2\ 3), (1\ 2)), \\ B_{13} + A_{13,1} &= (0\ 0\ 0\ 1\ 2\ 2\ 2\ 3\ 0\ 0\ 0\ 1\ 1) = \mathrm{int}((0\ 0\ 2\ 2\ 0\ 0\ 1), (0\ 1\ 2\ 3\ 0\ 1)), \\ B_{13} + A_{13,2} &= (0\ 1\ 2\ 2\ 2\ 3\ 0\ 0\ 0\ 1\ 2\ 2\ 3) = \mathrm{int}((0\ 2\ 2\ 0\ 0\ 2\ 3), (1\ 2\ 3\ 0\ 1\ 2)). \end{aligned}$$

We can identify a pattern in the above interleaved representations. For a sequence A and nonnegative integer m, define A^m as the sequence A repeated m times. Now define

$$\begin{aligned} W_m &:= ((0\ 0\ 2\ 2)^m\ 0\ 0\ 1), \\ X_m &:= ((0\ 1\ 2\ 3)^m\ 0\ 1), \\ Y_m &:= ((0\ 2\ 2\ 0)^m 0\ 2\ 3),\ \text{and} \end{aligned}$$

$$Z_m \quad := \quad ((1\ 2\ 3\ 0)^m\ 1\ 2).$$

Then we have

$$\begin{aligned}
B_5 + A_{5,1} &= \operatorname{int}(W_0, X_0), \\
B_5 + A_{5,2} &= \operatorname{int}(Y_0, Z_0), \\
B_{13} + A_{13,1} &= \operatorname{int}(W_1, X_1), \\
B_{13} + A_{13,2} &= \operatorname{int}(Y_1, Z_1).
\end{aligned}$$

This is the catalyst for one of our main results:

Theorem 3.1. *Let $m \geq 0$ be an integer. Suppose $\operatorname{int}(A, B)$ is a binary Barker sequence (written over $\mathbb{Z}_4$) of length $8m + 5$ where $A = ((0\ 0\ 0\ 2)^m\ 0\ 0\ 0)$. Then the sequences*

$$\begin{aligned}
E &:= \operatorname{int}(A + W_m, B + X_m), \\
F &:= \operatorname{int}(A + Y_m, B + Z_m)
\end{aligned}$$

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

Proof. Write $W := W_m, X := X_m, Y := Y_m, Z := Z_m$. Define n by $2n-1 := 8m+5$, so that $A+W, A+Y$ are of length n and $B+X, B+Z$ are of length $n-1$. Note that $n = 4m+3$ is odd and that a_j, w_j, x_j, y_j and z_j satisfy

$$\begin{aligned}
a_{2j} &= 0 && \text{for } j \text{ satisfying } 0 \leq 2j \leq n-1, \\
a_{2j+1} &= 2j \bmod 4 && \text{for } j \text{ satisfying } 1 \leq 2j+1 \leq n-2, \\
w_{2j} &= 2j \bmod 4 && \text{for } j \text{ satisfying } 0 \leq 2j < n-1, \\
w_{2j+1} &= 2j \bmod 4 && \text{for } j \text{ satisfying } 1 \leq 2j+1 \leq n-2, \\
w_{n-1} &= 1, && \\
x_j &= j \bmod 4 && \text{for } j \text{ satisfying } 0 \leq j \leq n-2, \\
y_{2j} &= 2j \bmod 4 && \text{for } j \text{ satisfying } 0 \leq 2j < n-1, \\
y_{2j+1} &= (2j+2) \bmod 4 && \text{for } j \text{ satisfying } 1 \leq 2j+1 \leq n-2, \\
y_{n-1} &= 3, && \\
z_j &= (j+1) \bmod 4 && \text{for } j \text{ satisfying } 0 \leq j \leq n-2.
\end{aligned}$$

We will use these facts throughout the proof.

By Lemma 2.9, to prove that (E, F) forms a Golay pair, i.e. that

$$C_E(u) + C_F(u) = 0 \text{ for all } u \text{ satisfying } 0 < u \leq 2n-2,$$

it suffices to show that for u satisfying $0 < u \leq n-1$,

$$C_{A+W}(u) + C_{B+X}(u) + C_{A+Y}(u) + C_{B+Z}(u) = 0 \tag{3.11}$$

and that for u satisfying $0 \leq u < n-1$,

$$C_{(A+W)(B+X)}(u) + C_{(B+X)(A+W)}(u+1) + C_{(A+Y)(B+Z)}(u) + C_{(B+Z)(A+Y)}(u+1) = 0. \tag{3.12}$$

We first prove (3.11). Fix u in the range $0 < u \leq n-1$. Then

$$\begin{aligned} C_{B+X}(u) + C_{B+Z}(u) &= \sum_{j=0}^{n-u-2} \left(i^{b_j+x_j-b_{j+u}-x_{j+u}} + i^{b_j+z_j-b_{j+u}-z_{j+u}} \right) \\ &= \sum_{j=0}^{n-u-2} i^{b_j-b_{j+u}} \left(i^{j-(j+u)} + i^{j+1-(j+u+1)} \right) \\ &= 2i^{-u} C_B(u). \end{aligned} \tag{3.13}$$

We also have

$$\begin{aligned} C_{A+W}(u) + C_{A+Y}(u) &= \sum_{j=0}^{n-u-1} \left(i^{a_j+w_j-a_{j+u}-w_{j+u}} + i^{a_j+y_j-a_{j+u}-y_{j+u}} \right) \\ &= i^{a_{n-u-1}-a_{n-1}} \left(i^{w_{n-u-1}-w_{n-1}} + i^{y_{n-u-1}-y_{n-1}} \right) + \\ &\quad \sum_{j=0}^{\lfloor \frac{n-u-2}{2} \rfloor} i^{a_{2j}-a_{2j+u}} \left(i^{w_{2j}-w_{2j+u}} + i^{y_{2j}-y_{2j+u}} \right) + \\ &\quad \sum_{j=0}^{\lfloor \frac{n-u-3}{2} \rfloor} i^{a_{2j+1}-a_{2j+u+1}} \left(i^{w_{2j+1}-w_{2j+u+1}} + i^{y_{2j+1}-y_{2j+u+1}} \right). \end{aligned} \tag{3.14}$$

We now consider two cases depending on the parity of u:

Case 1 $u = 2v$. Then (3.14) gives

$$\begin{aligned} C_{A+W}(u) + C_{A+Y}(u) &= i^{a_{n-2v-1}-a_{n-1}} \left(i^{n-2v-1-1} + i^{n-2v-1-3} \right) + \\ &\quad \sum_{j=0}^{\frac{n-2v-3}{2}} i^{a_{2j}-a_{2j+2v}} \left(i^{2j-(2j+2v)} + i^{2j-(2j+2v)} \right) + \end{aligned}$$

$$\begin{aligned}
& \sum_{j=0}^{\frac{n-2v-3}{2}} i^{a_{2j+1}-a_{2j+2v+1}} \left(i^{2j-(2j+2v)} + i^{2j+2-(2j+2v+2)}\right) \\
= \;& 2i^{-2v} \sum_{j=0}^{n-2v-2} i^{a_j - a_{j+2v}} \\
= \;& 2i^{-u}\left(C_A(u) - i^{a_{n-2v-1}-a_{n-1}}\right) \\
= \;& 2i^{-u}\left(C_A(u) - 1\right)
\end{aligned}$$

and so with (3.13) we have

$$\begin{aligned}
& C_{A+W}(u) + C_{B+X}(u) + C_{A+Y}(u) + C_{B+Z}(u) \\
&\quad = 2i^{-u}\left(C_A(u) + C_B(u) - 1\right) \\
&\quad = 2i^{-u}\left(C_{\mathrm{int}(A,B)}(2u) - 1\right), \text{ by Lemma 2.9 (i)} \\
&\quad = 0 \qquad (3.15)
\end{aligned}$$

since $C_{\mathrm{int}(A,B)}(2u) = (-1)^{\frac{8m+4}{2}} = 1$ by Lemma 2.1 (ii).

Case 2 $u = 2v+1$. Then (3.14) gives

$$\begin{aligned}
C_{A+W}(u) + C_{A+Y}(u) &= i^{a_{n-2v-2}-a_{n-1}}\left(i^{n-2v-3-1} + i^{n-2v-1-3}\right) + \\
&\quad \sum_{j=0}^{\frac{n-2v-3}{2}} i^{a_{2j}-a_{2j+2v+1}} \left(i^{2j-(2j+2v)} + i^{2j-(2j+2v+2)}\right) + \\
&\quad \sum_{j=0}^{\frac{n-2v-5}{2}} i^{a_{2j+1}-a_{2j+2v+2}} \left(i^{2j-(2j+2v+2)} + i^{2j+2-(2j+2v+2)}\right) \\
&= 2i^{a_{4m-2v+1}-a_{4m+2}+4m+3-2v} \\
&= -2i
\end{aligned}$$

and combining with (3.13) we have

$$\begin{aligned}
& C_{A+W}(u) + C_{B+X}(u) + C_{A+Y}(u) + C_{B+Z}(u) \\
&\quad = -2i + 2i^{-u} C_B(u) \\
&\quad = -2i + 2i^{-2v-1} C_B(2v+1) + 2i^{-2v-1} C_A(2v+1) - 2i^{-2v-1} C_A(2v+1)
\end{aligned}$$

$$= \quad -2i\left(1+(-1)^v C_{\mathrm{int}(A,B)}(4v+2)-(-1)^v C_A(2v+1)\right) \tag{3.16}$$

by Lemma 2.9 (i). Now

$$\begin{aligned}
C_A(2v+1) &= \sum_{j=0}^{n-2v-2} i^{a_j-a_{j+2v+1}} \\
&= \sum_{j=0}^{2m-v} \left(i^{a_{2j}-a_{2j+2v+1}}+i^{a_{2j+1}-a_{2j+2v+2}}\right) \\
&= \sum_{j=0}^{2m-v} \left(i^{-2j-2v}+i^{2j}\right) \\
&= 1+(-1)^v,
\end{aligned}$$

and substitution into (3.16) gives

$$\begin{aligned}
&C_{A+W}(u)+C_{B+X}(u)+C_{A+Y}(u)+C_{B+Z}(u) \\
&\qquad = -2i\left(1+(-1)^v C_{\mathrm{int}(A,B)}(4v+2)-(-1)^v(1+(-1)^v)\right) \\
&\qquad = 0
\end{aligned} \tag{3.17}$$

since again $C_{\mathrm{int}(A,B)}(4v+2)=(-1)^{\frac{8m+4}{2}}=1$ by Lemma 2.1 (ii).

Thus (3.15) and (3.17) establish (3.11). We now prove (3.12). Fix u in the range $0 \le u < n-1$. Then

$$\begin{aligned}
&C_{(A+W)(B+X)}(u)+C_{(A+Y)(B+Z)}(u) \\
&\qquad = \sum_{j=0}^{n-u-2} \left(i^{a_j+w_j-b_{j+u}-x_{j+u}}+i^{a_j+y_j-b_{j+u}-z_{j+u}}\right) \\
&\qquad = \sum_{j=0}^{\lfloor\frac{n-u-2}{2}\rfloor} i^{a_{2j}-b_{2j+u}}\left(i^{w_{2j}-x_{2j+u}}+i^{y_{2j}-z_{2j+u}}\right)+ \\
&\qquad\quad \sum_{j=0}^{\lfloor\frac{n-u-3}{2}\rfloor} i^{a_{2j+1}-b_{2j+u+1}}\left(i^{w_{2j+1}-x_{2j+u+1}}+i^{y_{2j+1}-z_{2j+u+1}}\right) \\
&\qquad = \sum_{j=0}^{\lfloor\frac{n-u-2}{2}\rfloor} i^{a_{2j}-b_{2j+u}}\left(i^{2j-(2j+u)}+i^{2j-(2j+u+1)}\right)+
\end{aligned}$$

$$
\begin{aligned}
& \sum_{j=0}^{\lfloor \frac{n-u-3}{2} \rfloor} i^{a_{2j+1}-b_{2j+u+1}} \left(i^{2j-(2j+u+1)} + i^{2j+2-(2j+u+2)} \right) \\
= \; & i^{-u}(1-i)C_{AB}(u) \qquad (3.18)
\end{aligned}
$$

and

$$
\begin{aligned}
& C_{(B+X)(A+W)}(u+1) + C_{(B+Z)(A+Y)}(u+1) \\
= \; & \sum_{j=0}^{n-u-2} \left(i^{b_j+x_j-a_{j+u+1}-w_{j+u+1}} + i^{b_j+z_j-a_{j+u+1}-y_{j+u+1}} \right) \\
= \; & i^{b_{n-u-2}-a_{n-1}} \left(i^{x_{n-u-2}-w_{n-1}} + i^{z_{n-u-2}-y_{n-1}} \right) + \qquad (3.19) \\
& \sum_{j=0}^{\lfloor \frac{n-u-3}{2} \rfloor} i^{b_{2j}-a_{2j+u+1}} \left(i^{x_{2j}-w_{2j+u+1}} + i^{z_{2j}-y_{2j+u+1}} \right) + \\
& \sum_{j=0}^{\lfloor \frac{n-u-4}{2} \rfloor} i^{b_{2j+1}-a_{2j+u+2}} \left(i^{x_{2j+1}-w_{2j+u+2}} + i^{z_{2j+1}-y_{2j+u+2}} \right).
\end{aligned}
$$

Again, we consider two cases:

Case 1 $u = 2v$. Then (3.19) gives

$$
\begin{aligned}
& C_{(B+X)(A+W)}(u+1) + C_{(B+Z)(A+Y)}(u+1) \\
= \; & i^{b_{n-u-2}-a_{n-1}} \left(i^{4m+3-2v-2-1} + i^{4m+3-2v-1-3} \right) + \\
& \sum_{j=0}^{2m-v} i^{b_{2j}-a_{2j+2v+1}} \left(i^{2j-(2j+2v)} + i^{2j+1-(2j+2v+2)} \right) + \\
& \sum_{j=0}^{2m-v-1} i^{b_{2j+1}-a_{2j+2v+2}} \left(i^{2j+1-(2j+2v+2)} + i^{2j+2-(2j+2v+2)} \right) \\
= \; & i^{-2v}(1-i)C_{BA}(2v+1) \\
= \; & i^{-u}(1-i)C_{BA}(u+1). \qquad (3.20)
\end{aligned}
$$

Case 2 $u = 2v + 1$. Then (3.19) gives

$$\begin{aligned}
&C_{(B+X)(A+W)}(u+1) + C_{(B+Z)(A+Y)}(u+1) \\
&\quad = i^{b_{n-2v-3}-a_{n-1}} \left(i^{4m+3-2v-3-1} + i^{4m+3-2v-2-3}\right) + \\
&\qquad \sum_{j=0}^{2m-v-1} i^{b_{2j}-a_{2j+2v+2}} \left(i^{2j-(2j+2v+2)} + i^{2j+1-(2j+2v+2)}\right) + \\
&\qquad \sum_{j=0}^{2m-v-1} i^{b_{2j+1}-a_{2j+2v+3}} \left(i^{2j+1-(2j+2v+2)} + i^{2j+2-(2j+2v+2+2)}\right) \\
&\quad = i^{-2v-1}(1-i)C_{BA}(2v+2) \\
&\quad = i^{-u}(1-i)C_{BA}(u+1). \qquad (3.21)
\end{aligned}$$

Thus in either case, (3.18), (3.20) and (3.21) give us

$$\begin{aligned}
&C_{(A+W)(B+X)}(u) + C_{(B+X)(A+W)}(u+1) + C_{(A+Y)(B+Z)}(u) + C_{(B+Z)(A+Y)}(u+1) \\
&\quad = i^{-u}(1-i)(C_{AB}(u) + C_{BA}(u+1)) \\
&\quad = 0
\end{aligned}$$

by Lemma 2.9 (ii) and Lemma 2.1 (i). Thus (3.12) holds, completing the proof. □

To our knowledge, Theorem 3.1 is only the second known result connecting Barker sequences of odd length and Golay pairs; however, the approaches of these two results differ. Jedwab and Parker found a general construction for a binary Golay pair of length $16m + 10$ from two related binary Barker sequences of lengths $8m + 3$ and $8m + 5$ [JP08]. On the other hand, Theorem 3.1 uses a binary Barker sequence of length $8m + 5$ with fixed even-indexed elements to construct a quaternary Golay pair of length $8m + 5$. The proof of [JP08] relies heavily on the generating functions of these objects and Corollary 2.5, while ours does not depend on either. We were unable to find an alternative construction of quaternary Golay sequences using the conditions and techniques of this other result.

Unfortunately, similar to the conclusion of [JP08], Theorem 3.1 does not give rise to any new quaternary Golay sequence pairs as the supply of Barker sequences of length $8m + 5$ runs out at $m = 1$ (by Theorem 2.2). Also, no similar result was found to hold for length $8m + 3$, and thus the origins of the pairs $(A_{3,1}, A_{3,2})$ and $(A_{11,1}, A_{11,2})$ are still unknown (although it is reasonable to regard $(A_{3,1}, A_{3,2})$ as a simple pair that needs no further explanation). However, the result does allow us to explain the existence of pairs $(A_{5,1}, A_{5,2})$ and $(A_{13,1}, A_{13,2})$ when we consider the Barker sequences of lengths 5 and 13 respectively as given objects. The other 511 ordered quaternary Golay pairs of length 5 and 511 pairs of length 13 are then explained by applying transformations (2.4) to (2.8) to $(A_{5,1}, A_{5,2})$ and $(A_{13,1}, A_{13,2})$ respectively. While Theorem 3.1 certainly does not prove that no odd length quaternary Golay sequences exist past length 13, this result along with the fact that none beyond length 13 have been found suggests that this may be the case, at least for lengths congruent to 5 modulo 8. We explore this possibility in the next chapter.

3.4 Summary

Table 3.7 summarizes results of this chapter by listing each of the classes in our classification of ordered quaternary Golay sequence pairs of small length.

Table 3.7: Classification of all ordered Golay sequence pairs over $\mathbb{Z}_4$ of length less than 22. Recall that $(A_{3,1}, A_{3,2})$ and $(A_{5,1}, A_{5,2})$ are Golay pairs over $\mathbb{Z}_4$ of length 3 and 5 respectively, (F, G) is a ternary Golay pair of length 3, (H, K) is the antepenultimate pair of a length 20 binary Golay seed pair, and B_5 and B_{13} are Barker sequences of length 5 and 13 respectively.

Length	# of ordered pairs contained in class	Sequences used to derive class	Explanation
1	16	-	trivial class
2	64	two trivial length 1 pairs	three-stage process
3	128	unknown (simple class)	transformations (2.4) to (2.8)
4	512	three trivial length 1 pairs	three-stage process
5	512	B_5	Theorem 3.1
6	2048	$(A_{3,1}, A_{3,2})$ and a trivial length 1 pair	three-stage process
8	6144	four trivial length 1 pairs	three-stage process
8	512	$((0\ 0\ 0\ 2\ 0\ 0\ 2\ 0), (0\ 1\ 1\ 2\ 0\ 3\ 3\ 2))$	shared autocorrelation property
10	8192	$(A_{5,1}, A_{5,2})$ and a trivial length 1 pair	three-stage process
10	4096	(F, G)	two applications of Corollary 2.5
11	512	unknown	transformations (2.4) to (2.8)
12	36864	$(A_{3,1}, A_{3,2})$ and two trivial length 1 pairs	three-stage process
13	512	B_{13}	Theorem 3.1
16	98304	five trivial length 1 pairs	three-stage process
16	8192	$((0\ 0\ 0\ 2\ 0\ 0\ 2\ 0), (0\ 1\ 1\ 2\ 0\ 3\ 3\ 2))$ and a trivial length 1 pair	three-stage process
18	24576	two copies of $(A_{3,1}, A_{3,2})$	three-stage process
20	147456	$(A_{5,1}, A_{5,2})$ and two trivial length 1 pairs	three-stage process
20	65536	length 10 pairs derived from (F, G) and a trivial length 1 pair	three-stage process
20	2048	(H, K)	two applications of Corollary 2.5

Chapter 4

Obtaining Binary Barker Sequences from Quaternary Golay Sequences

In the previous chapter, we saw that binary Barker sequences of length 5 and length 13 can be used to produce, up to transformations (2.4) to (2.8), all ordered quaternary Golay sequence pairs of length 5 and 13 respectively. Additionally, numerical evidence is beginning to suggest that quaternary Golay sequences of odd length greater than 13 may not exist, which is true for binary Barker sequences by Theorem 2.2.

In this chapter, we attempt to reverse the procedure in Theorem 3.1 to obtain an odd length binary Barker sequence from a quaternary Golay sequence of the same length, thus forcing the length of the Golay sequence to be at most 13. We will start by presenting our main result (Theorem 4.2), which rules out the existence of a class of quaternary Golay sequences of length greater than 13 and congruent to 5 modulo 8. This is motivated by an interesting property found in odd length quaternary Golay sequences. We then establish several lemmas before finally proving Theorem 4.2 at the end of the chapter.

4.1 The main result

Given a Golay sequence pair of length $8m+5$ over $\mathbb{Z}_4$, we would like to construct a binary Barker sequence of the same length. We start by observing an interesting pattern among the

Golay sequence pairs of length 5 and length 13. Consider again the Golay pairs $(A_{5,1}, A_{5,2})$ and $(A_{13,1}, A_{13,2})$ over $\mathbb{Z}_4$ (see Section 3.3). Notice that if we add the two sequences in each of the pairs, the results are

$$\begin{aligned} A_{5,1} + A_{5,2} &= (0\ 1\ 2\ 3\ 0) \text{ and} \\ A_{13,1} + A_{13,2} &= (0\ 1\ 2\ 3\ 0\ 1\ 2\ 3\ 0\ 1\ 2\ 3\ 0). \end{aligned}$$

In both cases, the j^{th} element is equal to j mod 4. We have the following simple lemma:

Lemma 4.1. *If A and B are sequences of length n over $\mathbb{Z}_4$ and $A+B = (0\ 1\ 2\ 3\ 0\ 1\ 2\ 3\ ...)$, then*

$$C_B(u) = i^{-u} \cdot \overline{C_A(u)}$$

for all integers u satisfying $0 \leq u < n$.

Proof. For u satisfying $0 \leq u < n$,

$$\begin{aligned} C_B(u) &= \sum_{j=0}^{n-u-1} i^{b_j - b_{j+u}} \\ &= \sum_{j=0}^{n-u-1} i^{j - a_j - (j+u-a_{j+u})} \\ &= i^{-u} \sum_{j=0}^{n-u-1} i^{-a_j + a_{j+u}} \\ &= i^{-u}\overline{C_A(u)}. \quad \square \end{aligned}$$

Since $(A_{5,1}, A_{5,2})$ and $(A_{13,1}, A_{13,2})$ are Golay pairs, Lemma 4.1 tells us that

$$C_{A_{5,1}}(u) + i^{-u}\overline{C_{A_{5,1}}(u)} = 0$$

and

$$C_{A_{13,1}}(u) + i^{-u}\overline{C_{A_{13,1}}(u)} = 0$$

for all integers $u \neq 0$. We will call a sequence A of length n over $\mathbb{Z}_4$ *good* if

$$C_A(u) = -i^{-u}\overline{C_A(u)} \text{ for all integers } u \text{ satisfying } 0 < u < n.$$

Thus a good sequence is necessarily a Golay sequence over $\mathbb{Z}_4$ (take the pair $(A, (0\ 1\ 2\ 3\ ...) - A))$, and any two sequences over $\mathbb{Z}_4$ that form a Golay pair and sum to

(0 1 2 3 ...) are both good. We find it very interesting that every known odd length Golay sequence over $\mathbb{Z}_4$ is, up to equivalence, a good sequence. In particular, this is true for the Golay sequences of length 3 and length 11, although a connection between these sequences and binary Barker sequences has yet to be found. In addition, the output Golay sequences E, F over $\mathbb{Z}_4$ of Theorem 3.1 are good, since

$$\begin{aligned}
E+F &= \operatorname{int}(A+W_m, B+X_m) + \operatorname{int}(A+Y_m, B+Z_m) \\
&= \operatorname{int}(2A+W_m+Y_m, 2B+X_m+Z_m) \\
&= \operatorname{int}(W_m+Y_m, X_m+Z_m), \text{ since } A \text{ and } B \text{ are binary} \\
&= ((0\ 1\ 2\ 3\ 0\ 1\ 2\ 3)^m\ 0\ 1\ 2\ 3\ 0).
\end{aligned}$$

Note that a good sequence cannot have even length $2m$ since

$$C_A(2m-1) + i^{-(2m-1)}\overline{C_A(2m-1)} = i^{a_0 - a_{2m-1}}\left(1 + i^{2a_0 + 2a_{2m-1} + 2m+1}\right) \neq 0.$$

We would like to show that no good sequence of length $8m+5$ exists for $m > 1$. We were able to establish this, subject to two extra conditions:

Theorem 4.2. *Let A be a good sequence of length $n = 8m+5$. Assume that*

(1) $a_{2u-1} + a_{2u+1} \equiv 1 \pmod 2$*, for all u satisfying $1 \leq 2u-1 \leq \frac{n-7}{2}$, and*

(2) $a_{4u} \equiv 0 \pmod 2$*, for all u satisfying $4 \leq 4u \leq \frac{n-5}{2}$.*

Then there exists a binary Barker sequence of length n.

Note that these extra conditions of Theorem 4.2 hold for all of $A_{5,1}$, $A_{5,2}$, $A_{13,1}$ and $A_{13,2}$ (all of which are good sequences).

4.2 Building up to Theorem 4.2

To prove Theorem 4.2, we will establish a series of lemmas in turn. Firstly, notice that the differences of opposite elements in $A_{5,1}$ and $A_{13,1}$ (as defined in Section 3.3), except for the outermost elements, follow a pattern themselves, namely

$$a_u - a_{n-u-1} \equiv 2 - u \pmod 4 \text{ for all } u \text{ satisfying } 1 \leq u \leq n-2. \tag{4.1}$$

The first objective of these lemmas will be to prove this property. This is achieved, subject to condition (1) of Theorem 4.2, in Proposition 4.6 for the more general case $n \equiv 1 \pmod 4$ and is summarized by (4.7).

Lemma 4.3. *Let A be a sequence of length n over $\mathbb{Z}_4$. Then A is a good sequence if and only if all of the following conditions hold:*

(i) $\text{Re } C_A(4v) = 0$ *for all v satisfying* $4 \leq 4v < n$,

(ii) $\text{Re } C_A(4v+1) = \text{Im } C_A(4v+1)$ *for all v satisfying* $1 \leq 4v+1 < n$,

(iii) $\text{Im } C_A(4v+2) = 0$ *for all v satisfying* $2 \leq 4v+2 < n$, *and*

(iv) $\text{Re } C_A(4v+3) = -\text{Im } C_A(4v+3)$ *for all v satisfying* $3 \leq 4v+3 < n$.

Proof. Let $j \in \{0, 1, 2, 3\}$ and let $4v$ satisfy $0 < 4v + j < n$. The results follow from

$$C_A(4v+j) = -i^{-j}\overline{C_A(4v+j)}$$

by taking $j = 0, 1, 2, 3$ in turn. □

Lemma 4.4. *Let A be a good sequence of length $n \equiv 1 \pmod 4$. Then*

(i) $a_0 - a_{n-1} \equiv 1 \pmod 2$, *and*

(ii) $a_u - a_{n-u-1} \equiv u \pmod 2$ *for all u satisfying* $1 \leq u \leq n-2$.

Proof. Firstly, we have $\text{Re } C_A(n-1) = 0$ by Lemma 4.3 (i), and so

$$i^{a_0 - a_{n-1}} \in \{i, -i\}$$

or equivalently, $a_0 - a_{n-1} \equiv 1 \pmod 2$, proving (i).

To prove (ii), we claim that

$$h(2u) := a_{2u-1} + a_{2u} - a_{n-2u-1} - a_{n-2u} \equiv 1 \pmod 2$$

for all u satisfying $2 \leq 2u \leq n-3$. After proving the claim by induction, we then use induction again to establish the result.

The proof of the claim is motivated by the proof of Theorem 2.6. Let u satisfy $2 \leq 2u \leq n-3$ and assume $h(2t) \equiv 1 \pmod 2$ for all t satisfying $2 \leq 2t < 2u$. Consider

$$P(u) := \prod_{j=0}^{2u} i^{a_j - a_{j+n-2u-1}}.$$

Then $P(u) \in \{1, -1\}$ if and only if the number of terms in

$$C_A(n-2u-1) = \sum_{j=0}^{2u} i^{a_j - a_{j+n-2u-1}}$$

equal to $\pm i$ is even; otherwise, $P(u) \in \{i, -i\}$. Now when $u = 2v+1$ is odd, the imaginary part of $C_A(n-4v-3)$ is zero by Lemma 4.3 (iii) and so the number of terms equal to i is the same as the number of terms equal to $-i$; thus, $P(2v+1) \in \{1, -1\}$. When $u = 2v$ is even, the real part of $C_A(n-4v-1)$ is zero by Lemma 4.3 (i) and so the number of terms equal to 1 is the same as the number of terms equal to -1. Since $C_A(n-4v-1)$ has exactly $4v+1$ terms, an odd number, there must be an odd number of terms equal to $\pm i$, and thus $P(2v) \in \{i, -i\}$. It follows that

$$i^{\sum_{j=0}^{2u}(a_j - a_{j+n-2u-1})} = P(u) \in \{i^{u+1}, i^{u+3}\}$$

and so

$$\begin{aligned} u+1 &\equiv \sum_{j=0}^{2u}(a_j - a_{j+n-2u-1}) \pmod 2 \\ &\equiv a_0 - a_{n-1} + \sum_{j=1}^{u} h(2j) \\ &\equiv u + h(2u) \pmod 2 \end{aligned}$$

by (i) and, for $u > 1$, the induction hypothesis. The claim then follows.

To complete the proof of (ii), first notice that

$$a_{\frac{n-1}{2}} - a_{n-\frac{n-1}{2}-1} = 0 \equiv \frac{n-1}{2} \pmod 2$$

and thus (ii) holds for $u = \frac{n-1}{2}$. Let u satisfy $1 \leq u < \frac{n-1}{2}$ and assume that $a_t - a_{n-t-1} \equiv t \pmod 2$ for all t satisfying $u < t \leq \frac{n-1}{2}$. When $u = 2v+1$ is odd, we have $2 \leq 2v + 2 \leq \frac{n-1}{2} \leq n - 3$ (we may assume $n > 1$, otherwise there's nothing to prove for (ii)) so by the claim we have

$$\begin{aligned} 1 &\equiv h(2v+2) \pmod 2 \\ &\equiv a_{2v+1} + a_{2v+2} - a_{n-2v-3} - a_{n-2v-2} \\ &\equiv a_{2v+1} - a_{n-2v-2} \pmod 2 \end{aligned}$$

by the induction hypothesis. When $u = 2v$ is even, we have $2 \leq \frac{n-1}{2} < n - 2v - 1 \leq n - 3$ so we have

$$\begin{aligned} 1 &\equiv h(n-2v-1) \pmod 2 \\ &\equiv a_{n-2v-2} + a_{n-2v-1} - a_{2v} - a_{2v+1} \\ &\equiv a_{2v} - a_{n-2v-1} + 1 \pmod 2 \end{aligned}$$

by the induction hypothesis. Thus (ii) holds for all u satisfying $1 \leq u \leq \frac{n-1}{2}$ and, by symmetry, the result follows for all u satisfying $1 \leq u \leq n-2$. $\square$

Given a good sequence A of length $n \equiv 1 \pmod 4$, from Lemma 4.4 we may define

$$\left.\begin{aligned} \alpha_0 &:= \tfrac{a_0 - a_{n-1}+1}{2} \bmod 2, \\ \alpha_{2u-1} &:= \tfrac{a_{2u-1} - a_{n-2u}+1}{2} \bmod 2, \quad \text{for } u \text{ satisfying } 1 \leq 2u-1 \leq n-2, \text{ and} \\ \alpha_{2u} &:= \tfrac{a_{2u} - a_{n-2u-1}}{2} \bmod 2, \quad \text{for } u \text{ satisfying } 2 \leq 2u \leq n-3. \end{aligned}\right\} \tag{4.2}$$

Then, to show that (4.1) holds for all u satisfying $1 \leq u \leq n-2$ and $n \equiv 5 \pmod 8$, it suffices to show that $\alpha_{2u-1} = u \bmod 2$, and that $\alpha_{2u} = (u+1) \bmod 2$. The next lemma will be used in the proof of Proposition 4.6 to do just that for the more general case $n \equiv 1 \pmod 4$. We note here that for a good sequence A, we may assume without loss of generality that $a_0 = 0$ (we establish this in the proof of Theorem 4.2) and we make this assumption in all of the upcoming lemmas.

Lemma 4.5. *Let A be a good sequence of length $n \equiv 1 \pmod 4$. Suppose $a_0 = 0$. Then*

(i) $a_{2u+1} + \sum_{j=0}^{2u+1} \alpha_j \equiv u + 1 \pmod 2$ *for all u satisfying $1 \leq 2u+1 \leq n-2$, and*

(ii) $a_{2u+1} + \sum_{j=0}^{2u} \alpha_j \equiv \frac{n+3}{4} \pmod 2$ *for all u satisfying $1 \leq 2u+1 \leq \frac{n-3}{2}$.*

Proof. To prove (i), let u satisfy $1 \leq 2u+1 \leq n-2$. Note that for $x, y \in \mathbb{Z}_4$ and integer u, one can easily verify that

$$\text{Re } i^x + (-1)^u \text{Im } i^x \equiv x^2 + (2u+3)x + 1 \pmod 4 \tag{4.3}$$

and that

$$x^2 + y^2 \equiv \begin{cases} 2x^2 \pmod 4 & \text{if } x + y \equiv 0 \pmod 2, \\ 1 \pmod 4 & \text{if } x + y \equiv 1 \pmod 2. \end{cases} \tag{4.4}$$

Now,

$$0 = \text{Re } C_A(n-2u-2) + (-1)^u \text{Im } C_A(n-2u-2), \text{ by Lemma 4.3 (ii) and (iv)}$$

$$
\begin{aligned}
&= \sum_{j=0}^{2u+1} \left(\mathrm{Re}\ i^{a_j - a_{j+n-2u-2}} + (-1)^u \mathrm{Im}\ i^{a_j - a_{j+n-2u-2}}\right) \\
&\equiv \sum_{j=0}^{2u+1} \left[(a_j - a_{j+n-2u-2})^2 + (2u+3)(a_j - a_{j+n-2u-2}) + 1\right] \pmod 4, \text{ by (4.3)} \\
&\equiv \sum_{j=0}^{2u+1} \left[a_j^2 + 2a_j a_{j+n-2u-2} + a_{j+n-2u-2}^2 + (2u+3)(a_j - a_{j+n-2u-2})\right] + 2u + 2 \\
&\equiv 2\sum_{j=0}^{2u+1} a_j a_{j+n-2u-2} + a_0^2 + a_{n-1}^2 + (2u+3)(a_0 - a_{n-1}) + \\
&\quad \sum_{j=1}^{u+1} \left[a_{2j-1}^2 + a_{n-2j}^2 + (2u+3)(a_{2j-1} - a_{n-2j})\right] + \\
&\quad \sum_{j=1}^{u} \left[a_{2j}^2 + a_{n-2j-1}^2 + (2u+3)(a_{2j} - a_{n-2j-1})\right] + 2u + 2 \\
&\equiv 2\sum_{j=0}^{2u+1} a_j a_{j+n-2u-2} + 1 + (2u+3)(2\alpha_0 - 1) + \sum_{j=1}^{u+1} [1 + (2u+3)(2\alpha_{2j-1} - 1)] + \\
&\quad \sum_{j=1}^{u} \left[2a_{2j}^2 + (2u+3)(2\alpha_{2j})\right] + 2u + 2, \text{ by Lemma 4.4, (4.2) and (4.4)} \\
&\equiv 2\sum_{j=0}^{2u+1} a_j a_{j+n-2u-2} + 2\sum_{j=0}^{2u+1} \alpha_j + 2\sum_{j=1}^{u} a_{2j}^2 + 2(u+1)^2 \pmod 4,
\end{aligned}
$$

and so

$$
u + 1 \equiv \sum_{j=0}^{2u+1} a_j a_{j+n-2u-2} + \sum_{j=0}^{2u+1} \alpha_j + \sum_{j=1}^{u} a_{2j} \pmod 2. \tag{4.5}
$$

Now,

$$
\begin{aligned}
&\sum_{j=0}^{2u+1} a_j a_{j+n-2u-2} + \sum_{j=1}^{u} a_{2j} \\
&\equiv a_0 a_{n-2u-2} + a_{2u+1} a_{n-1} + \sum_{j=1}^{u} (a_j a_{j+n-2u-2} + a_{2u+1-j} a_{n-1-j}) + \sum_{j=1}^{u} a_{2j} \pmod 2 \\
&\equiv a_{2u+1} + \sum_{j=1}^{\lfloor \frac{u+1}{2} \rfloor} (a_{2j-1} a_{2j+n-2u-3} + a_{2u+2-2j} a_{n-2j}) + \\
&\quad \sum_{j=1}^{\lfloor \frac{u}{2} \rfloor} (a_{2j} a_{2j+n-2u-2} + a_{2u+1-2j} a_{n-1-2j}) + \sum_{j=1}^{u} a_{2j},
\end{aligned}
$$

$$
\begin{aligned}
& \text{since } a_0 = 0 \text{ and thus } a_{n-1} \equiv 1 \pmod 2 \text{ by Lemma 4.4 (i)} \\
\equiv\ & a_{2u+1} + \sum_{j=1}^{\lfloor \frac{u+1}{2} \rfloor} [a_{2j-1}a_{2u-2j+2} + a_{2u-2j+2}(1 + a_{2j-1})] + \\
& \sum_{j=1}^{\lfloor \frac{u}{2} \rfloor} [a_{2j}(1 + a_{2u-2j+1}) + a_{2u-2j+1}a_{2j}] + \sum_{j=1}^{u} a_{2j}, \text{ by Lemma 4.4 (ii)} \\
\equiv\ & a_{2u+1} \pmod 2
\end{aligned}
$$

and substituting this into (4.5) proves (i).

For (ii), let u satisfy $1 \leq 2u+1 \leq \frac{n-3}{2}$. Then substitute $\frac{n-2u-3}{2}$ for u in (i) to get

$$
\begin{aligned}
\frac{n-2u-1}{2} &\equiv a_{n-2u-2} + \sum_{j=0}^{n-2u-2} \alpha_j \pmod 2 \\
&\equiv 1 + a_{2u+1} + \sum_{j=0}^{2u} \alpha_j + \sum_{j=0}^{n-4u-3} \alpha_{2u+1+j} \pmod 2, \text{ by Lemma 4.4 (ii)} \\
&\equiv 1 + a_{2u+1} + \sum_{j=0}^{2u} \alpha_j + \sum_{j=0}^{\frac{n-4u-5}{2}} (\alpha_{2u+1+j} + \alpha_{n-2u-2-j}) + \alpha_{\frac{n-1}{2}} \\
&\equiv 1 + a_{2u+1} + \sum_{j=0}^{2u} \alpha_j + \frac{n-4u-1}{4}, \text{ by Lemma 4.4 (ii) and (4.2)} \\
&\equiv a_{2u+1} + \sum_{j=0}^{2u} \alpha_j + \frac{n+3}{4} + u \pmod 2
\end{aligned}
$$

and since $u \equiv \frac{n-2u-1}{2} \pmod 2$, this establishes (ii). □

Proposition 4.6. *Let A be a good sequence of length $n \equiv 1 \pmod 4$. Suppose that $a_0 = 0$. Then the following hold:*

(i) $a_{2u+1} - a_{n-2u-2} \equiv 2u + \frac{n-3}{2} \pmod 4$ *for all u satisfying* $1 \leq 2u+1 \leq n-2$

(ii) *If, in addition,* $a_{2u-1} + a_{2u+1} \equiv 1 \pmod 2$ *for all u satisfying* $1 \leq 2u-1 \leq \frac{n-7}{2}$, *then* $a_{2u} - a_{n-2u-1} \equiv 2u + \frac{n-1}{2} \pmod 4$ *for all u satisfying* $2 \leq 2u \leq n-3$.

Proof. By symmetry, it is sufficient to prove (i) for all u satisfying $1 \leq 2u+1 \leq \frac{n-3}{2}$. Given u in this range, subtracting Lemma 4.5 (ii) from Lemma 4.5 (i) yields

$$\alpha_{2u+1} \equiv u + \frac{n-1}{4} \pmod 2 \tag{4.6}$$

and thus by (4.2), it follows that

$$a_{2u+1} - a_{n-2u-2} \equiv 2u + \frac{n-3}{2} \pmod 4.$$

Thus (i) holds.

Again by symmetry, it is sufficient to prove (ii) for all u satisfying $2 \leq 2u \leq \frac{n-1}{2}$. One can easily verify directly that (ii) holds for $2u = \frac{n-1}{2}$. So let u satisfy $2 \leq 2u \leq \frac{n-5}{2}$. Then adding the equation of Lemma 4.5 (i) for $u-1$ and u gives

$$\begin{aligned} 1 &\equiv a_{2u-1} + \sum_{j=0}^{2u-1} \alpha_j + a_{2u+1} + \sum_{j=0}^{2u+1} \alpha_j \pmod 2 \\ &\equiv a_{2u-1} + a_{2u+1} + \alpha_{2u} + \alpha_{2u+1} \\ &\equiv a_{2u-1} + a_{2u+1} + \alpha_{2u} + u + \frac{n-1}{4}\ \text{, by (4.6)} \\ &\equiv \alpha_{2u} + u + \frac{n+3}{4} \pmod 2 \end{aligned}$$

by the additional assumption. Multiplying by 2 gives

$$\begin{aligned} 2u + \frac{n-1}{2} &\equiv 2\alpha_{2u} \pmod 4 \\ &\equiv a_{2u} - a_{n-2u-1} \pmod 4 \end{aligned}$$

by (4.2), completing the proof. □

Proposition 4.6 confirms that for a good sequence A of length $n \equiv 1 \pmod 4$ with condition (1) of Theorem 4.2, we have

$$a_u - a_{n-u-1} \equiv \frac{n-1}{2} - u \pmod 4 \text{ for all } u \text{ satisfying } 1 \leq u \leq n-2. \tag{4.7}$$

Note that when $n \equiv 5 \pmod 8$, (4.7) is equivalent to the pattern (4.1) mentioned earlier. We make use of (4.7) in the upcoming lemmas.

Recall that in Theorem 3.1, we construct a good sequence (see Section 4.1) of length $8m+5$ from a binary Barker sequence represented over $\mathbb{Z}_4$ by adding the sequence $\text{int}(W_m, X_m)$, where $W_m = ((0\ 0\ 2\ 2)^m\ 0\ 0\ 1)$ and $X_m = ((0\ 1\ 2\ 3)^m\ 0\ 1)$. Eventually, we would like to reverse this by showing that subtracting $\text{int}(W_m, X_m)$ from a good sequence A yields a binary Barker sequence B. Thus for B to be binary, all elements of B must be 0 or 2 and so it is necessary that the parities of the elements of the good sequence match those of the corresponding sequence elements of $\text{int}(W_m, X_m)$; therefore, we need

$$a_{2u} \equiv 0 \pmod 2 \text{ for all } u \text{ satisfying } 0 \leq 2u \leq n-3, \tag{4.8}$$

$$\begin{aligned} a_{2u+1} &\equiv u \pmod 2 \text{ for all } u \text{ satisfying } 1 \leq 2u+1 \leq n-2, \text{ and} &(4.9)\\ a_{n-1} &\equiv 1 \pmod 2. &(4.10)\end{aligned}$$

We now work towards showing just this. Lemma 4.7 (with $n \equiv 5 \pmod 8$) establishes (4.9), while Lemma 4.8 (ii) and condition (2) of Theorem 4.2 establish (4.8) for $2u \neq 0$. We now note that in addition to assuming $a_0 = 0$, we may also assume without loss of generality that $a_{n-1} = 1$. These two assumptions (or just the first and Lemma 4.4 (i)) establish (4.8) for $2u = 0$ and (4.10). Again, we postpone the verification of this additional assumption until the proof of Theorem 4.2.

Lemma 4.7. *Let A be a good sequence of length $n \equiv 1 \pmod 4$. Suppose that $a_0 = 0$, $a_{n-1} = 1$ and that (4.7) holds. Then $a_{2u+1} \equiv u + \frac{n+3}{4} \pmod 2$ for all u satisfying $1 \leq 2u+1 \leq n-2$.*

Proof. Let u satisfy $1 \leq 2u+1 \leq n-2$. Then

$$\begin{aligned} C_A(2u+1) &= \sum_{j=0}^{n-2u-2} i^{a_j - a_{j+2u+1}} \\ &= i^{a_0 - a_{2u+1}} + i^{a_{n-2u-2} - a_{n-1}} + \sum_{j=1}^{\frac{n-2u-3}{2}} \left(i^{a_j - a_{j+2u+1}} + i^{a_{n-2u-2-j} - a_{n-1-j}} \right) \\ &= i^{-a_{2u+1}} + i^{(a_{2u+1} + 2u+1 - \frac{n-1}{2}) - 1} + \\ &\quad \sum_{j=1}^{\frac{n-2u-3}{2}} \left(i^{a_j - a_{j+2u+1}} + i^{(a_{j+2u+1} + j + 2u + 1 - \frac{n-1}{2}) - (a_j + j - \frac{n-1}{2})} \right), \text{ by (4.7)} \\ &= i^{-a_{2u+1}} \left(1 + (-1)^{a_{2u+1} + u + \frac{n-1}{4}} \right) + &(4.11)\\ &\quad \sum_{j=1}^{\frac{n-2u-3}{2}} i^{a_j - a_{j+2u+1}} \left(1 + i(-1)^{a_j + a_{j+2u+1} + u} \right). \end{aligned}$$

Let $\sigma_j := i^{a_j - a_{j+2u+1}} (1 + i(-1)^{a_j + a_{j+2u+1} + u})$. Note that for all j satisfying $1 \leq j \leq \frac{n-2u-3}{2}$, when u is even, $\sigma_j \in \{1+i, -1-i\}$ and when u is odd, $\sigma_j \in \{1-i, -1+i\}$; hence, $\text{Re}\, \sigma_j = (-1)^u \text{Im}\, \sigma_j$. Now since A is good, we also have $\text{Re}\, C_A(2u+1) = (-1)^u \text{Im}\, C_A(2u+1)$ by Lemma 4.3 (ii) and (iv). Therefore,

$$0 = \text{Re}\, C_A(2u+1) + (-1)^{u+1} \text{Im}\, C_A(2u+1) - \sum_{j=1}^{\frac{n-2u-3}{2}} \left(\text{Re}\, \sigma_j + (-1)^{u+1} \text{Im}\, \sigma_j \right)$$

$$\begin{aligned} &= \mathrm{Re}\left[i^{-a_{2u+1}}\left(1+(-1)^{a_{2u+1}+u+\frac{n-1}{4}}\right)\right] + \\ &\quad (-1)^{u+1}\mathrm{Im}\left[i^{-a_{2u+1}}\left(1+(-1)^{a_{2u+1}+u+\frac{n-1}{4}}\right)\right] \end{aligned} \tag{4.12}$$

by (4.11).

Now, if $a_{2u+1} \equiv 0 \pmod 2$, only the first term of (4.12) is possibly non-zero, and then

$$i^{-a_{2u+1}}\left(1+(-1)^{u+\frac{n-1}{4}}\right) = 0.$$

This implies $u + \frac{n+3}{4} \equiv 0 \equiv a_{2u+1} \pmod 2$ as desired. Otherwise, $a_{2u+1} \equiv 1 \pmod 2$ and only the second term of (4.12) is possibly non-zero. Hence

$$(-1)^{u+1} i^{-a_{2u+1}-1}\left(1+(-1)^{u+\frac{n-1}{4}+1}\right) = 0$$

implying that $u + \frac{n+3}{4} \equiv 1 \equiv a_{2u+1} \pmod 2$, completing the proof. □

Lemma 4.7 establishes the parity of the odd-indexed elements. We now determine the parities of some of the even-indexed elements. Like the previous two assumptions $a_0 = 0$ and $a_{n-1} = 1$, we can, without loss of generality, make the third assumption that $a_2 \equiv 0 \pmod 2$. Again, we will verify this in the proof of Theorem 4.2.

Lemma 4.8. *Let A be a good sequence of length $n \equiv 1 \pmod 4$. Suppose that $a_0 = 0$, $a_{n-1} = 1$ and that (4.7) holds. In addition, assume that $a_2 \equiv 0 \pmod 2$. Then*

(i) $a_{\frac{n-1}{2}} \equiv \frac{n+3}{4} \pmod 2$,

(ii) $a_{4u+2} \equiv 0 \pmod 2$ *for all u satisfying $2 \le 4u+2 \le n-3$, and*

(iii) $2\sum_{j=1}^{u} a_{4j} \equiv a_{4u+2} + \frac{n+3}{2} \pmod 4$ *for all u satisfying $2 \le 4u+2 \le n-3$.*

Proof. Let t satisfy $2 \le 2t \le n-3$ and consider

$$\begin{aligned} C_A(2t) &= \sum_{j=0}^{n-2t-1} i^{a_j - a_{j+2t}} \\ &= i^{a_0 - a_{2t}} + i^{a_{n-2t-1} - a_{n-1}} + i^{a_{\frac{n-2t-1}{2}} - a_{\frac{n+2t-1}{2}}} + \\ &\quad \sum_{j=1}^{\frac{n-2t-3}{2}} \left(i^{a_j - a_{j+2t}} + i^{a_{n-2t-1-j} - a_{n-1-j}}\right) \\ &= i^{-a_{2t}} + i^{a_{2t} + 2t - \frac{n-1}{2} - 1} + i^{\frac{n-1}{2} - \frac{n-2t-1}{2}} + \end{aligned}$$

$$\sum_{j=1}^{\frac{n-2t-3}{2}} \left(i^{a_j-a_{j+2t}} + i^{a_{j+2t}+j+2t-\frac{n-1}{2}-(a_j+j-\frac{n-1}{2})}\right), \text{ by (4.7)}$$

$$= i^{-a_{2t}} + i^{a_{2t}+2t-\frac{n+1}{2}} + i^t + \sum_{j=1}^{\frac{n-2t-3}{2}} i^{a_j-a_{j+2t}}\left(1+(-1)^{a_j+a_{j+2t}+t}\right). \quad (4.13)$$

To prove (i) and (ii), we take $t = 2u+1$ to get

$$C_A(4u+2) = i^{-a_{4u+2}} + i^{a_{4u+2}-\frac{n-3}{2}} + i(-1)^u + \sum_{j=1}^{\frac{n-4u-5}{2}} i^{a_j-a_{j+4u+2}}\left(1+(-1)^{a_j+a_{j+4u+2}+1}\right).$$

Next, we reduce modulo 4 to get

$$\begin{aligned}
C_A(4u+2) &\equiv i^{-a_{4u+2}} + i^{a_{4u+2}-\frac{n-3}{2}} + i(2u+1) + \sum_{j=1}^{\frac{n-4u-5}{2}} 2i\left(a_j + a_{j+4u+2}\right) \pmod 4,\\
&\quad \text{since } i^{x-y}\left(1+(-1)^{x+y+1}\right) \equiv 2i(x+y) \pmod 4 \text{ for } x, y \in \mathbb{Z}_4\\
&\equiv i^{-a_{4u+2}} + i^{a_{4u+2}-\frac{n-3}{2}} + i(2u+1) + 2i\frac{n-4u-5}{4} +\\
&\quad 2i\sum_{j=1}^{\frac{n-4u-5}{4}} \left(a_{2j} + a_{2j+4u+2}\right),\\
&\quad \text{since } 2i(a_{2j-1} + a_{2j+4u+1}) \equiv 2i((j-1)+(j+2u)) \equiv 2i \pmod 4\\
&\quad \text{for all } j \text{ satisfying } 1 \le j \le \frac{n-4u-5}{4} \text{ by Lemma 4.7}\\
&\equiv i^{-a_{4u+2}} + i^{a_{4u+2}-\frac{n-3}{2}} + i\frac{n-3}{2} + 2i\sum_{j=1}^{\frac{n-4u-5}{4}} \left(a_{2j} + a_{n-2j-4u-3}\right), \text{ by (4.7)}\\
&\equiv i^{-a_{4u+2}} + i^{a_{4u+2}-\frac{n-3}{2}} + i\frac{n-3}{2} + 2i\sum_{j=1}^{\frac{n-4u-5}{2}} a_{2j} \pmod 4.
\end{aligned}$$

Then replacing $4u+2$ with $n-4u-3$ in the above gives, for u satisfying $2 \le 4u+2 \le n-3$,

$$\begin{aligned}
C_A(n-4u-3) &\equiv i^{-a_{n-4u-3}} + i^{a_{n-4u-3}-\frac{n-3}{2}} + i\frac{n-3}{2} + 2i\sum_{j=1}^{2u} a_{2j} \pmod 4\\
&\equiv i^{-(a_{4u+2}+2-\frac{n-1}{2})} + i^{a_{4u+2}+2-\frac{n-1}{2}-\frac{n-3}{2}} + i\frac{n-3}{2} + 2i\sum_{j=1}^{2u} a_{2j} \pmod 4
\end{aligned} \quad (4.14)$$

by using (4.7). Thus, for u satisfying $2 \le 4u+2 \le \frac{n-5}{2}$ (so that $2u \le \frac{n-4u-9}{2} < \frac{n-4u-5}{2}$), we have

$$\begin{aligned}
&C_A(4u+2) + C_A(n-4u-3) \\
&\equiv i^{-a_{4u+2}}\left(1 + i^{\frac{n-1}{2}-2}\right) + i^{a_{4u+2}-\frac{n-3}{2}}\left(1 + i^{2-\frac{n-1}{2}}\right) + 2i + 2i \sum_{j=2u+1}^{\frac{n-4u-5}{2}} a_{2j} \pmod 4 \\
&\equiv \left(i^{-a_{4u+2}} + i^{a_{4u+2}-\frac{n-3}{2}}\right)\left(1 + (-1)^{\frac{n+3}{4}}\right) + 2i + 2ia_{4u+2} + 2i \sum_{j=1}^{\frac{n-8u-7}{2}} a_{2j+4u+2} \\
&\equiv i^{-a_{4u+2}}\left(1 + i(-1)^{a_{4u+2}+\frac{n-1}{4}}\right)\left(1 + (-1)^{\frac{n+3}{4}}\right) + 2i + 2ia_{4u+2} + \\
&\quad i \sum_{j=1}^{\frac{n-8u-9}{4}} (2a_{2j+4u+2} + 2a_{n-2j-4u-3}) + 2ia_{\frac{n-1}{2}} \\
&\equiv i^{-a_{4u+2}}\left(1 + i(-1)^{a_{4u+2}+\frac{n-1}{4}}\right)\left(1 + (-1)^{\frac{n+3}{4}}\right) + 2i + 2ia_{4u+2} + 2ia_{\frac{n-1}{2}} \pmod 4
\end{aligned}$$

again using (4.7). Now, by Lemma 4.3 (iii), it follows that

$$\begin{aligned}
0 &= \frac{1}{2}\mathrm{Im}\left(C_A(4u+2) + C_A(n-4u-3)\right) \\
&\equiv \mathrm{Im}\left[i^{-a_{4u+2}}\left(1 + i(-1)^{a_{4u+2}+\frac{n-1}{4}}\right)\frac{\left(1 + (-1)^{\frac{n+3}{4}}\right)}{2}\right] + 1 + a_{4u+2} + a_{\frac{n-1}{2}} \pmod 2 \\
&\equiv \frac{\left(1 + (-1)^{\frac{n+3}{4}}\right)}{2} + 1 + a_{4u+2} + a_{\frac{n-1}{2}} \\
&\equiv \frac{n+3}{4} + a_{4u+2} + a_{\frac{n-1}{2}} \pmod 2, \qquad (4.15)
\end{aligned}$$

for all u satisfying $2 \le 4u+2 \le \frac{n-5}{2}$. When $n > 5$, taking $u = 0$ in (4.15) proves (i) by the assumption on a_2 (note that there's nothing to prove for (i) when $n = 5$ since then $a_2 = a_{\frac{n-1}{2}}$). (4.15) then becomes

$$0 \equiv a_{4u+2} \pmod 2$$

for all u satisfying $2 \le 4u+2 \le \frac{n-5}{2}$ which, when combined with Lemma 4.4 (ii) (and (i) if $n \equiv 5 \pmod 8$), proves (ii).

Finally, to prove (iii),we use (ii) in (4.14) to get, for u satisfying $2 \le 4u+2 \le n-3$,

$$C_A(n-4u-3) \equiv i^{-a_{4u+2}+2+\frac{n-1}{2}}\left(1 + i^{-\frac{n-3}{2}}\right) + i\frac{n-3}{2} + i\sum_{j=1}^{u}(2a_{4j-2} + 2a_{4j}) \pmod 4$$

$$\equiv \quad (-1)^{\frac{a_{4u+2}}{2}+\frac{n+3}{4}}\left(1+i(-1)^{\frac{n-1}{4}}\right)+i\frac{n-3}{2}+2i\sum_{j=1}^{u}a_{4j} \pmod 4$$

by (ii). Now applying Lemma 4.3 (iii) gives us

$$\begin{aligned}
0 &= \operatorname{Im} C_A(n-4u-3) \\
&\equiv (-1)^{\frac{a_{4u+2}}{2}+\frac{n+3}{4}+\frac{n-1}{4}}+\frac{n-3}{2}+2\sum_{j=1}^{u}a_{4j} \pmod 4 \\
&\equiv a_{4u+2}+\frac{n+3}{2}+\frac{n-1}{2}+1+\frac{n-3}{2}+2\sum_{j=1}^{u}a_{4j} \\
&\equiv 2\sum_{j=1}^{u}a_{4j}+a_{4u+2}+\frac{n+3}{2} \pmod 4,
\end{aligned}$$

establishing (iii). □

One might expect that, in a similar manner to the proof of Lemma 4.8, we could reduce $C_A(4u)$ modulo 4 to show that a_{4u} is even for all u satisfying $4 \leq 4u \leq n-5$. Unfortunately, this is not the case. A computer search for "good sequences mod 4" (i.e. the results of Lemma 4.3 are relaxed from equalities to congruences modulo 4) finds sequences where Proposition 4.6 and Lemmas 4.4, 4.7 and 4.8 are all satisfied but, for example, $a_4 \equiv 1 \pmod 2$. Such a sequence of length 13 is (0 0 0 1 1 2 2 1 3 2 0 3 1), and existence for larger lengths appears to be common. Establishing the parity of a_{4u} seems to be a difficult problem.

However, after imposing that a_{4u} is even for all u satisfying $4 \leq 4u \leq n-5$ (and thus imposing condition (2) of Theorem 4.2), we can actually solve for all of the even-indexed elements. In addition, we immediately see from Lemma 4.8 (i) that we also then have $n \equiv 5 \pmod 8$. Thus from here on, we disregard the $n \equiv 1 \pmod 8$ case when convenient.

Lemma 4.9. *Under the same conditions as Lemma 4.8, if we additionally assume that* $a_{4u} \equiv 0 \pmod 2$ *for all* u *satisfying* $4 \leq 4u \leq n-5$*, then*

(i) $a_{4u} = 2u \bmod 4$*, for all* u *satisfying* $0 \leq 4u \leq n-5$*, and*

(ii) $a_{4u+2} = \frac{n+3}{2} \bmod 4$*, for all* u *satisfying* $2 \leq 4u+2 \leq n-3$.

Proof. Firstly, note that (ii) follows immediately from Lemma 4.8 (ii) and (iii), the additional assumption and $\frac{n+3}{2} \equiv -\frac{n+3}{2} \pmod 4$. To prove (i), note that we assume $a_0 = 0$, so let t

satisfy $4 \leq 2t \leq n-5$. Take (4.13) with $t = 2u$ to get

$$C_A(4u) = i^{-a_{4u}} + i^{a_{4u}-\frac{n+1}{2}} + (-1)^u + \sum_{j=1}^{\frac{n-4u-3}{2}} i^{a_j - a_{j+4u}} \left(1 + (-1)^{a_j + a_{j+4u}}\right).$$

Then reducing modulo 4 gives

$$\begin{aligned} C_A(4u) &\equiv i^{-a_{4u}} + i^{a_{4u}-\frac{n+1}{2}} + \sum_{j=1}^{\frac{n-4u-3}{2}} 2(a_j + a_{j+4u} + 1) + 2u + 1 \pmod 4, \\ &\quad \text{since } i^{x-y}\left(1 + (-1)^{x+y}\right) \equiv 2(x+y+1) \pmod 4 \text{ for } x, y \in \mathbb{Z}_4 \\ &\equiv i^{-a_{4u}} + i^{a_{4u}-\frac{n+1}{2}} + n - 4u - 3 + 2u + 1, \\ &\quad \text{since } 2a_j \equiv 2a_{j+4u} \pmod 4 \text{ for all } j \text{ satisfying } 1 \leq j \leq \frac{n-4u-3}{2} \text{ by} \\ &\quad \text{Lemmas 4.7 and 4.8 (ii) and the additional assumption} \\ &\equiv i^{-a_{4u}} + i^{a_{4u}-\frac{n+1}{2}} + 2u - 1 \pmod 4) \end{aligned}$$

and so by Lemma 4.3 (i), we have

$$\begin{aligned} 0 &= \operatorname{Re} C_A(4u) \\ &\equiv \operatorname{Re}\left(i^{-a_{4u}} + i^{a_{4u}-\frac{n+1}{2}}\right) + 2u - 1 \pmod 4 \\ &\equiv a_{4u} + 2u \pmod 4 \end{aligned}$$

by the additional assumption. This proves (i). □

4.3 Constructing a binary Barker sequence

The previous section has put us in a position to construct a binary Barker sequence of odd length from a good sequence of the same length under the extra conditions of Theorem 4.2. Recall that in Section 3.3, we have that $\operatorname{int}(W_m, X_m) = ((0\ 0\ 0\ 1\ 2\ 2\ 2\ 3)^m\ 0\ 0\ 0\ 1\ 1)$ and we now reverse the approach of Theorem 3.1 by subtracting $\operatorname{int}(W_m, X_m)$ from a good sequence:

Lemma 4.10. *Let A be a good sequence of length $n = 8m + 5$, and let B be the length n sequence given by*

$$B := A - ((0\ 0\ 0\ 1\ 2\ 2\ 2\ 3)^m\ 0\ 0\ 0\ 1\ 1).$$

Suppose that $a_0 = 0$, $a_{n-1} = 1$ and that (4.7) holds. Then we have the following:

(i) Re $C_B(2u+1) = 0$ *for all* u *satisfying* $1 \le 2u+1 \le n-2$

(ii) $|C_B(4u)| = 1$ *for all* u *satisfying* $4 \le 4u \le n-1$

(iii) *If, in addition,* $a_2 \equiv 0 \pmod 2$ *and* $a_{4u} \equiv 0 \pmod 2$ *for all* u *satisfying* $4 \le 4u \le n-5$, *then* $C_B(4u+2) = 1$ *for all* u *satisfying* $2 \le 4u+2 \le n-3$.

Proof. We denote the j^{th} element of $((0\ 0\ 0\ 1\ 2\ 2\ 2\ 3)^m\ 0\ 0\ 0\ 1\ 1)$ as d_j. Note then that

$$\begin{aligned}
d_{2u+1} &\equiv u \pmod 4 \text{ for all } u \text{ satisfying } 1 \le 2u+1 \le n-2, \\
d_{4u} &\equiv 2u \pmod 4 \text{ for all } u \text{ satisfying } 0 \le 4u \le n-5, \\
d_{4u+2} &\equiv 2u \pmod 4 \text{ for all } u \text{ satisfying } 2 \le 4u+2 \le n-3, \\
d_{n-1} &= 1, \text{ and} \\
d_u - d_{n-u-1} &\equiv u+2 \pmod 4 \text{ for all } u \text{ satisfying } 1 \le u \le n-2,
\end{aligned} \tag{4.16}$$

and we shall use these relations freely.

We start by proving (i). Let u satisfy $1 \le 2u+1 \le n-2$. Then

$$\begin{aligned}
C_B(2u+1) &= \sum_{j=0}^{n-2u-2} i^{a_j - d_j - a_{j+2u+1} + d_{j+2u+1}} \\
&= \sum_{j=0}^{\frac{n-2u-3}{2}} \left(i^{a_j - d_j - a_{j+2u+1} + d_{j+2u+1}} + i^{a_{n-2u-2-j} - d_{n-2u-2-j} - a_{n-1-j} + d_{n-1-j}} \right) \\
&= i^{a_0 - d_0 - a_{2u+1} + d_{2u+1}} + i^{a_{n-2u-2} - d_{n-2u-2} - a_{n-1} + d_{n-1}} + \\
&\quad \sum_{j=1}^{\frac{n-2u-3}{2}} \left(i^{a_j - d_j - a_{j+2u+1} + d_{j+2u+1}} + \right. \\
&\qquad \left. i^{\left(a_{j+2u+1} + j + 2u + 1 - \frac{n-1}{2}\right) - (d_{j+2u+1} - j - 2u - 3) - \left(a_j + j - \frac{n-1}{2}\right) + (d_j - j - 2)} \right), \\
&\quad \text{by (4.7) and (4.16)} \\
&= i^{-a_{2u+1} + d_{2u+1}} \left(1 + (-1)^{a_{2u+1} + d_{2u+1} + 1} \right) + \\
&\quad \sum_{j=1}^{\frac{n-2u-3}{2}} i^{a_j - d_j - a_{j+2u+1} + d_{j+2u+1}} \left(1 + (-1)^{a_j + d_j + a_{j+2u+1} + d_{j+2u+1} + 1} \right)
\end{aligned}$$

by (4.7), (4.16) and $n \equiv 5 \pmod 8$. Since every outermost term is either $0, 2i$ or $-2i$, (i) is established.

We now prove (ii). Note that $C_B(n-1) = i^{a_0-d_0-a_{n-1}+d_{n-1}} = 1$ and so (ii) holds for $4u = n-1$. It remains to establish (ii) for u satisfying $4 \leq 4u \leq n-5$, and so let t satisfy $4 \leq 2t \leq n-5$ and take (4.13) with $t = 2u$ (note that establishing (4.13) did not use $a_2 \equiv 0 \pmod 2$) to get

$$C_A(4u) = i^{-a_{4u}} + i^{a_{4u}+1} + (-1)^u + \sum_{j=1}^{\frac{n-4u-3}{2}} i^{a_j-a_{j+4u}} \left(1 + (-1)^{a_j+a_{j+4u}}\right).$$

Then by Lemma 4.3 (i), we have

$$\begin{aligned} C_A(4u) &= i \cdot \operatorname{Im} C_A(4u) \\ &= i \cdot \operatorname{Im}\left(i^{-a_{4u}} + i^{a_{4u}+1} + \sum_{j=1}^{\frac{n-4u-3}{2}} i^{a_j-a_{j+4u}} \left(1 + (-1)^{a_j+a_{j+4u}}\right) + (-1)^u \right) \\ &= i \cdot \operatorname{Im}\left(i^{-a_{4u}} + i^{a_{4u}+1}\right). \end{aligned} \tag{4.17}$$

Now,

$$\begin{aligned} C_B(4u) &= \sum_{j=0}^{n-4u-1} i^{a_j-d_j-a_{j+4u}+d_{j+4u}} \\ &= i^{a_{n-4u-1}-\frac{n-4u-1}{2}} + \sum_{j=0}^{n-4u-2} i^{a_j-a_{j+4u}+2u}, \\ &\quad \text{since } d_{j+4u} - d_j \equiv 2u \pmod 4 \text{ for all } j \text{ satisfying } 0 \leq j \leq n-4u-2, \\ &\quad \text{and } a_{n-1} = 1 \\ &= i^{a_{n-4u-1}+2u+2} + (-1)^u \left(C_A(4u) - i^{a_{n-4u-1}-a_{n-1}}\right) \\ &= (-1)^u i^{a_{4u}} + (-1)^u \left(C_A(4u) - i^{a_{4u}+1}\right), \text{ by (4.7) and } a_{n-1} = 1 \\ &= (-1)^u \left(C_A(4u) + i^{a_{4u}}(1-i)\right) \\ &= (-1)^u \left(i \cdot \operatorname{Im}\left(i^{-a_{4u}} + i^{a_{4u}+1}\right) + i^{a_{4u}}(1-i)\right), \text{ by (4.17)} \\ &= \begin{cases} (-1)^u \left(i^{a_{4u}+1} + i^{a_{4u}}(1-i)\right) & \text{if } a_{4u} \equiv 0 \pmod 2 \\ (-1)^u \left(i^{-a_{4u}} + i^{a_{4u}}(1-i)\right) & \text{if } a_{4u} \equiv 1 \pmod 2 \end{cases} \\ &= \begin{cases} (-1)^u i^{a_{4u}} & \text{if } a_{4u} \equiv 0 \pmod 2 \\ (-1)^u i^{a_{4u}-1} & \text{if } a_{4u} \equiv 1 \pmod 2 \end{cases} \\ &\in \{1, -1\}, \end{aligned}$$

completing the proof of (ii).

We now assume that $a_2 \equiv 0 \pmod 2$ and that $a_{4u} \equiv 0 \pmod 2$ for all u satisfying $4 \leq 4u \leq n-5$. Let u satisfy $2 \leq 4u+2 \leq n-3$. Then to prove (iii), we first show that

$$i \cdot \operatorname{Im} C_A(4u+2) = i^{a_{n-4u-3}-a_{n-1}} + \sum_{j=0}^{\frac{n-4u-5}{2}} i^{a_{2j+1}-a_{2j+4u+3}} \tag{4.18}$$

and we will use (4.18) to show that $C_B(4u+2) = 1$.

So to prove (4.18), consider

$$\begin{aligned} C_A(4u+2) &= \sum_{j=0}^{n-4u-3} i^{a_j - a_{j+4u+2}} \\ &= i^{a_{n-4u-3}-a_{n-1}} + \sum_{j=0}^{\frac{n-4u-5}{2}} i^{a_{2j}-a_{2j+4u+2}} + \sum_{j=0}^{\frac{n-4u-5}{2}} i^{a_{2j+1}-a_{2j+4u+3}} \\ &= -i(-1)^{\frac{a_{n-4u-3}}{2}} + \sum_{j=0}^{\frac{n-4u-5}{2}} (-1)^{\frac{a_{2j}-a_{2j+4u+2}}{2}} + i \sum_{j=0}^{\frac{n-4u-5}{2}} (-1)^{\frac{a_{2j+1}-a_{2j+4u+3}-1}{2}} \end{aligned}$$

since a_{2k} is even for all k satisfying $0 \leq 2k \leq n-3$ by Lemma 4.9, and $a_{2k+1} \equiv k \pmod 2$ for all k satisfying $1 \leq 2k+1 \leq n-2$ by Lemma 4.7. Thus

$$\begin{aligned} i \cdot \operatorname{Im} C_A(4u+2) &= -i(-1)^{\frac{a_{n-4u-3}}{2}} + i \sum_{j=0}^{\frac{n-4u-5}{2}} (-1)^{\frac{a_{2j+1}-a_{2j+4u+3}-1}{2}} \\ &= i^{a_{n-4u-3}-a_{n-1}} + \sum_{j=0}^{\frac{n-4u-5}{2}} i^{a_{2j+1}-a_{2j+4u+3}}, \end{aligned}$$

establishing (4.18).

Next, consider

$$\begin{aligned} C_B(4u+2) &= \sum_{j=0}^{n-4u-3} i^{a_j - d_j - a_{j+4u+2} + d_{j+4u+2}} \\ &= i^{a_{n-4u-3}-d_{n-4u-3}-a_{n-1}+d_{n-1}} + \sum_{j=0}^{\frac{n-4u-5}{2}} i^{a_{2j}-d_{2j}-a_{2j+4u+2}+d_{2j+4u+2}} + \\ &\quad \sum_{j=0}^{\frac{n-4u-5}{2}} i^{a_{2j+1}-d_{2j+1}-a_{2j+4u+3}+d_{2j+4u+3}}. \end{aligned} \tag{4.19}$$

Now

$$
\begin{aligned}
& i^{a_{n-4u-3}-d_{n-4u-3}-a_{n-1}+d_{n-1}} + \sum_{j=0}^{\frac{n-4u-5}{2}} i^{a_{2j+1}-d_{2j+1}-a_{2j+4u+3}+d_{2j+4u+3}} \\
= \;& i^{a_{n-4u-3}-\frac{n-4u-5}{2}-a_{n-1}+1} + \sum_{j=0}^{\frac{n-4u-5}{2}} i^{a_{2j+1}-j-a_{2j+4u+3}+j+2u+1} \\
= \;& i(-1)^u \left(i^{a_{n-4u-3}-a_{n-1}} + \sum_{j=0}^{\frac{n-4u-5}{2}} i^{a_{2j+1}-a_{2j+4u+3}} \right) \\
= \;& (-1)^{u+1} \mathrm{Im}\, C_A(4u+2), \text{ by (4.18)} \\
= \;& 0
\end{aligned}
$$

by Lemma 4.3 (iii). Finally, substitution into (4.19) gives

$$
\begin{aligned}
& C_B(4u+2) \\
= \;& \sum_{j=0}^{\frac{n-4u-5}{2}} i^{a_{2j}-d_{2j}-a_{2j+4u+2}+d_{2j+4u+2}} \\
= \;& i^{a_0-d_0-a_{4u+2}+d_{4u+2}} + \sum_{j=1}^{\frac{n-4u-5}{4}} \left(i^{a_{4j-2}-d_{4j-2}-a_{4j+4u}+d_{4j+4u}} + i^{a_{4j}-d_{4j}-a_{4j+4u+2}+d_{4j+4u+2}} \right) \\
= \;& i^{-a_{4u+2}+2u} + \sum_{j=1}^{\frac{n-4u-5}{4}} \left(i^{a_{4j-2}-(2j-2)-a_{4j+4u}+2j+2u} + i^{a_{4j}-2j-a_{4j+4u+2}+2j+2u} \right) \\
= \;& (-1)^u + \sum_{j=1}^{\frac{n-4u-5}{4}} \left((-1)^{j+1} + (-1)^{j+u} \right), \text{ by Lemma 4.9} \\
= \;& (-1)^u + \left(1 + (-1)^{u+1}\right) \sum_{j=1}^{\frac{n-4u-5}{4}} (-1)^{j+1} \\
= \;& (-1)^u + \left(1 + (-1)^{u+1}\right) \frac{1 + (-1)^{\frac{n-4u-5}{4}+1}}{2} \\
= \;& (-1)^u + \frac{\left(1 + (-1)^{u+1}\right)^2}{2} \\
= \;& 1
\end{aligned}
$$

as desired. $\square$

Lemma 4.10 finally allows us to prove Theorem 4.2.

Proof of Theorem 4.2. Firstly, we may assume that $a_0 = 0$; otherwise, we can transform A via $(a_j) \mapsto ((a_j - a_0) \bmod 4)$ which leaves the aperiodic autocorrelation function of A the same and thus A is still good. Then by Lemma 4.4 (i), $a_{n-1} \equiv 1 \pmod 2$ and by Proposition 4.6 and condition (1), we have that (4.7) holds. Next, we may assume that $a_{n-1} = 1$; otherwise, $a_{n-1} = 3$ and we can transform A via $(a_j) \mapsto ((j - a_j) \bmod 4)$ (i.e. A maps to $(0\ 1\ 2\ 3\ ...) - A$) which, by Lemma 4.1, maps $C_A(u)$ to $i^{-u}\overline{C_A(u)}$ for all u satisfying $1 \leq u \leq n-1$. Then it follows that A is still good, $a_0 = 0$ and

$$a_{n-1} \mapsto (n - 1 - a_{n-1}) \bmod 4 \ = 1.$$

Furthermore, we may assume that $a_2 \equiv 0 \pmod 2$; otherwise, $a_2 \equiv 1 \pmod 2$ and we transform A via (2.6) followed by (2.7) which one can easily check again leaves the aperiodic autocorrelation function unchanged. Thus A is still good, and

$$\begin{aligned} a_0 &\mapsto (-a_{n-1} + 1) \bmod 4 \ = 0, \\ a_{n-1} &\mapsto (-a_0 + 1) \bmod 4 \ = 1, \text{ and} \\ a_2 &\mapsto (-a_{n-3} + 1) \bmod 4 \ = (-a_2 + 1) \bmod 4 \ \equiv 0 \pmod 2 \end{aligned}$$

by (4.7).

Now define $B := A - ((0\ 0\ 0\ 1\ 2\ 2\ 2\ 3)^m\ 0\ 0\ 0\ 1\ 1)$. Then by condition (2) and (4.7), we have that

$$a_{4u} \equiv 0 \pmod 2 \text{ for all } u \text{ satisfying } 4 \leq 4u \leq n-5$$

and so by Lemma 4.10 (ii) and (iii), $|C_B(2u)| = 1$ for all u satisfying $2 \leq 2u \leq n-1$. Also, note that since

$$\begin{aligned} a_{2u} &\equiv 0 \pmod 2 \text{ for all } u \text{ satisfying } 0 \leq 2u \leq n-3 \text{ by Lemma 4.9,} \\ a_{2u+1} &\equiv u \pmod 2 \text{ for all } u \text{ satisfying } 1 \leq 2u+1 \leq n-2 \text{ by Lemma 4.7, and} \\ a_{n-1} &= 1, \end{aligned}$$

it follows that every element of B is either 0 or 2. Thus, B corresponds to a binary sequence of length n and so

$$C_B(2u+1) = \text{Re } C_B(2u+1) = 0 \text{ for all } u \text{ satisfying } 1 \leq 2u+1 \leq n-2$$

by Lemma 4.10 (i). Therefore B is a binary Barker sequence of length n as desired. □

4.4 Summary

This chapter has displayed our best attempt at establishing a converse to Theorem 3.1. We focused on constructing a binary Barker sequence from a quaternary Golay sequence, subject to the Golay sequence being "good". Even with the simplification from the two extra conditions of Theorem 4.2, the effort to achieve this partial result was considerable; however, the additional evidence connecting binary Barker and quaternary Golay sequences is perhaps what is most valuable. We hope that future work can find a more elegant relationship between binary Barker and quaternary Golay sequences of odd lengths.

To conclude this chapter, we state the non-existence result stemming from Theorem 2.2 and Theorem 4.2.

Corollary 4.11. *Let A be a good sequence of length $n = 8m + 5$. Assume that*

(1) $a_{2u-1} + a_{2u+1} \equiv 1 \pmod 2$, *for all u satisfying* $1 \leq 2u - 1 \leq \frac{n-7}{2}$, *and*

(2) $a_{4u} \equiv 0 \pmod 2$, *for all u satisfying* $4 \leq 4u \leq \frac{n-5}{2}$.

Then $m \in \{0, 1\}$.

Chapter 5

Conclusion and Open Problems

Chapter 3 classifies all ordered quaternary Golay sequence pairs of length less than 22 and explains almost all of the classes using either the three-stage construction process, the shared autocorrelation property, Corollary 2.5 or Theorem 3.1. The only classes left unexplained are the classes of length 3 and 11. Since the other nontrivial odd lengths less than 22 are derivable from binary Barker sequences via Theorem 3.1, we expect that these unexplained classes are also somehow related to binary Barker sequences. Thus, an interesting open problem is to find a more general construction of quaternary Golay sequence pairs of odd length from binary Barker sequences.

In Chapter 4, we introduced a "good" sequence and showed that a good sequence whose length is congruent to 5 modulo 8, and which satisfies two conditions, gives rise to a binary Barker sequence; this forces the length of the good sequence to be no greater than 13. This result required several lemmas which, for simplicity, we restricted to apply only to good sequences whose length is congruent to 1 modulo 4. We suspect that similar lemmas hold for lengths congruent to 3 modulo 4. If some general construction from binary Barker sequences to quaternary Golay sequence pairs could be established for such lengths, then perhaps Theorem 4.2 would apply to good sequences of more general odd lengths.

Corollary 4.11 proves the nonexistence of certain good sequences by directly constructing a Barker sequence and applying Theorem 2.2. An alternative approach would be to show directly, say by elementary techniques similar to those used by Turyn and Storer in the proof of Theorem 2.2, that a good sequence cannot exist past length 13. Given the high level of structure of known good sequences, for example as described in Lemma 4.3 and (4.7), this plan appears to have some merit. Ultimately, due to their apparent connection with binary Barker sequences, we suspect that there are no quaternary Golay sequences of odd length greater than 13. One big step towards establishing this would be to show that all quaternary Golay sequences of odd length are, up to equivalence, good sequences. However, this appears to be a difficult problem.

Appendix A

Affine Offsets and the Three-stage Construction Process

Here, we would like to show that taking affine offsets (i.e. applying constant offsets (2.7) and incremental offsets (2.8)) of the input sequence pairs at Stage 1 of the three-stage construction process only duplicates array pairs obtained during Stage 2. In other words, for integer $m \geq 1$ and even integer $H \geq 2$, we want to show that for all $e_0, ...e_k, \epsilon_0, ..., \epsilon_m, \epsilon'_0, ..., \epsilon'_m \in \mathbb{Z}_H$, if the Golay sequence pairs $((a_k[j_k]), (b_k[j_k]))$ of length n_k, $k = 0, 1, ..., m$, produce the Golay array pair (F, G) via Theorem 2.13 and the Golay sequence pairs $((a_k[j_k]+e_kj_k+\epsilon_k), (b_k[j_k]+e_kj_k+\epsilon'_k))$, $k = 0, ..., m$, produce the Golay array pair $(\hat{F}, \hat{G})$ via Theorem 2.13, then $(\hat{F}, \hat{G})$ can be obtained from (F, G) via Lemma 2.14.

Write $F = (f[j_0, ..., j_m, x_1, ..., x_m])$, $G = (g[j_0, ..., j_m, x_1, ..., x_m])$, $\hat{F} = (\hat{f}[j_0, ..., j_m, x_1, ..., x_m])$ and $\hat{G} = (\hat{g}[j_0, ..., j_m, x_1, ..., x_m])$. Then we want to show that

$$\hat{f}[j_0, ..., j_m, x_1, ..., x_m] = f[j_0, ..., j_m, x_1, ..., x_m] + \sum_{k=0}^{m} \delta_k j_k + \sum_{k=1}^{m} \lambda_k x_k + \gamma, \text{ and} \tag{A.1}$$

$$\hat{g}[j_0, ..., j_m, x_1, ..., x_m] = g[j_0, ..., j_m, x_1, ..., x_m] + \sum_{k=0}^{m} \delta_k j_k + \sum_{k=1}^{m} \lambda_k x_k + \gamma' \tag{A.2}$$

for some constants $\delta_0, ..., \delta_m, \lambda_1, ..., \lambda_m, \gamma, \gamma' \in \mathbb{Z}_H$. As defined in Theorem 2.13, we have

$$\begin{aligned} f[j_0, ..., j_m, x_1, ..., x_m] = & \sum_{k=1}^{m-1} \left(a_k[j_k] + a^*_k[j_k] - b_k[j_k] - b^*_k[j_k] + \frac{H}{2} \right) x_k x_{k+1} + \\ & \sum_{k=1}^{m} \left(b^*_{k-1}[j_{k-1}] + b_k[j_k] - a_{k-1}[j_{k-1}] - a_k[j_k] \right) x_k + \sum_{k=0}^{m} a_k[j_k], \end{aligned}$$

$$g[j_0,...,j_m,x_1,...,x_m] \quad = \quad f'_m[j_0,...,j_m,x_0,...,x_m] + \frac{H}{2}x_1$$

where $f'_m[j_0,...,j_m,x_1,...,x_m]$ is $f_m[j_0,...,j_m,x_1,...x_m]$ with $a_0[j_0], b_0[j_0]$ interchanged and with $a_0^*[j_0], b_0^*[j_0]$ interchanged. Now, similarly we have

$$\begin{aligned}
&\hat{f}[j_0,...,j_m,x_1,...,x_m] \\
&= \sum_{k=1}^{m-1}\Big[a_k[j_k] + e_kj_k + \epsilon_k + (a_k[j_k] + e_kj_k + \epsilon_k)^* - \\
&\qquad b_k[j_k] - e_kj_k - \epsilon'_k - \big(b_k[j_k] + e_kj_k + \epsilon'_k\big)^* + \frac{H}{2}\Big]\, x_kx_{k+1} + \\
&\quad \sum_{k=1}^{m}\Big[\big(b_{k-1}[j_{k-1}] + e_{k-1}j_{k-1} + \epsilon'_{k-1}\big)^* + b_k[j_k] + e_kj_k + \epsilon'_k - \\
&\qquad a_{k-1}[j_{k-1}] - e_{k-1}j_{k-1} - \epsilon_{k-1} - a_k[j_k] - e_kj_k - \epsilon_k\Big] x_k + \sum_{k=0}^{m}(a_k[j_k] + e_kj_k + \epsilon_k) \\
&= \sum_{k=1}^{m-1}\Big[a_k[j_k] + e_kj_k + \epsilon_k + a_k^*[j_k] - e_k(n_k - j_k - 1) - \epsilon_k - \\
&\qquad b_k[j_k] - e_kj_k - \epsilon'_k - b_k^*[j_k] + e_k(n_k - j_k - 1) + \epsilon'_k + \frac{H}{2}\Big]\, x_kx_{k+1} + \\
&\quad \sum_{k=1}^{m}\Big[b_{k-1}^*[j_{k-1}] - e_{k-1}(n_{k-1} - j_{k-1} - 1) - \epsilon'_{k-1} + b_k[j_k] + e_kj_k + \epsilon'_k - \\
&\qquad a_{k-1}[j_{k-1}] - e_{k-1}j_{k-1} - \epsilon_{k-1} - a_k[j_k] - e_kj_k - \epsilon_k\Big] x_k + \sum_{k=0}^{m}(a_k[j_k] + e_kj_k + \epsilon_k) \\
&= f[j_0,...,j_m,x_1,...,x_m] + \sum_{k=1}^{m}\big(-e_{k-1}n_{k-1} + e_{k-1} - \epsilon'_{k-1} + \epsilon'_k - \epsilon_{k-1} - \epsilon_k\big)\, x_k + \\
&\quad \sum_{k=0}^{m}(e_kj_k + \epsilon_k)
\end{aligned}$$

and

$$\begin{aligned}
&\hat{g}[j_0,...,j_m,x_1,...,x_m] \\
&= \sum_{k=1}^{m-1}\Big[a_k[j_k] + e_kj_k + \epsilon_k + (a_k[j_k] + e_kj_k + \epsilon_k)^* - \\
&\qquad b_k[j_k] - e_kj_k - \epsilon'_k - \big(b_k[j_k] + e_kj_k + \epsilon'_k\big)^* + \frac{H}{2}\Big] x_kx_{k+1} + \\
&\quad \big[(a_0[j_0] + e_0j_0 + \epsilon_0)^* + b_1[j_1] + e_1j_1 + \epsilon'_1 - b_0[j_0] - e_0j_0 - \epsilon'_0 - a_1[j_1] - e_1j_1 - \epsilon_1\big]\, x_1
\end{aligned}$$

$$
\begin{aligned}
& + \sum_{k=2}^{m} \Big[\big(b_{k-1}[j_{k-1}] + e_{k-1}j_{k-1} + \epsilon'_{k-1}\big)^* + b_k[j_k] + e_k j_k + \epsilon'_k - \\
& \qquad a_{k-1}[j_{k-1}] - e_{k-1}j_{k-1} - \epsilon_{k-1} - a_k[j_k] - e_k j_k - \epsilon_k \Big] x_k + \\
& b_0[j_0] + e_0 j_0 + \epsilon'_0 + \sum_{k=1}^{m} (a_k[j_k] + e_k j_k + \epsilon_k) + \frac{H}{2} x_1 \\
= & \sum_{k=1}^{m-1} \Big[a_k[j_k] + e_k j_k + \epsilon_k + a_k^*[j_k] - e_k(n_k - j_k - 1) - \epsilon_k - \\
& \qquad b_k[j_k] - e_k j_k - \epsilon'_k - b_k^*[j_k] + e_k(n_k - j_k - 1) + \epsilon'_k + \frac{H}{2} \Big] x_k x_{k+1} + \\
& \big[a_0^*[j_0] - e_0(n_0 - j_0 - 1) - \epsilon_0 + b_1[j_1] + \epsilon'_1 - b_0[j_0] - e_0 j_0 - \epsilon'_0 - a_1[j_1] - \epsilon_1\big] x_1 + \\
& \sum_{k=2}^{m} \Big[b_{k-1}^*[j_{k-1}] - e_{k-1}(n_{k-1} - j_{k-1} - 1) - \epsilon'_{k-1} + b_k[j_k] + \epsilon'_k - \\
& \qquad a_{k-1}[j_{k-1}] - e_{k-1}j_{k-1} - \epsilon_{k-1} - a_j[j_k] - \epsilon_k \Big] x_k + \\
& b_0[j_0] + e_0 j_0 + \epsilon'_0 + \sum_{k=1}^{m} (a_k[j_k] + e_k j_k + \epsilon_k) + \frac{H}{2} x_1 \\
= & g_m[j_0, ..., j_m, x_1, ..., x_m] + \sum_{k=1}^{m} \big(-e_{k-1}n_{k-1} + e_{k-1} - \epsilon'_{k-1} + \epsilon'_k - \epsilon_{k-1} - \epsilon_k \big) x_k + \\
& e_0 j_0 + \epsilon'_0 + \sum_{k=1}^{m} (e_k j_k + \epsilon_k) \, .
\end{aligned}
$$

Thus, (A.1) and (A.2) are satisfied with

$$
\begin{aligned}
\delta_k &= e_k && \text{for all } k \text{ satisfying } 0 \le k \le m, \\
\lambda_k &= -e_{k-1}n_{k-1} + e_{k-1} - \epsilon'_{k-1} + \epsilon'_k - \epsilon_{k-1} - \epsilon_k && \text{for all } k \text{ satisfying } 1 \le k \le m, \\
\gamma &= \textstyle\sum_{k=0}^{m} \epsilon_k, \text{ and} \\
\gamma' &= \epsilon'_0 + \textstyle\sum_{k=1}^{m} \epsilon_k.
\end{aligned}
$$

Therefore we only need to consider Golay pairs up to affine offsets during Stage 1 of the three-stage construction process.

Bibliography

[AS89] S. Alquaddoomi and R.A. Scholtz, *On the nonexistence of Barker arrays and related matters*, IEEE Trans. Inform. Theory **35** (1989), 1048–1057.

[Bar53] R.H. Barker, *Group synchronizing of binary digital systems*, Communication Theory (W. Jackson, ed.), Academic Press, New York, 1953, pp. 273–287.

[BF03] P.B. Borwein and R.A. Ferguson, *A complete description of Golay pairs for lengths up to 100*, Mathematics of Computation **73** (2003), 967–985.

[Boe67] A.M. Boehmer, *Binary pulse compression codes*, IEEE Trans. Inform. Theory **IT-13** (1967), 156–167.

[Bud90] S.Z. Budišin, *New complementary pairs of sequences*, Electron. Lett. **26** (1990), 881–883.

[CHK02] R. Craigen, W. Holzmann, and H. Kharaghani, *Complex Golay sequences: structure and applications*, Discrete Math. **252** (2002), 73–89.

[DJ99] J.A. Davis and J. Jedwab, *Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes*, IEEE Trans. Inform. Theory **45** (1999), 2397–2417.

[DJ07] D. Dmitriev and J. Jedwab, *Bounds on the growth rate of the peak sidelobe level of binary sequences*, Advances in Mathematics and Communications **1** (2007), 461–475.

[DJS07] J.A. Davis, J. Jedwab, and K.W. Smith, *Proof of the Barker array conjecture*, Proc. Amer. Math. Soc. **135** (2007), 2011–2018.

[Dym92] M. Dymond, *Barker arrays: existence, generalization and alternatives*, Ph.D. thesis, University of London, 1992.

[EKS91] S. Eliahou, M. Kervaire, and B. Saffari, *On Golay polynomial pairs*, Advances App. Math. **12** (1991), 235–292.

[Fie] F. Fiedler, *Small Golay sequences*, in preparation.

[FJP08] F. Fiedler, J. Jedwab, and M.G. Parker, *A multi-dimensional approach to the construction and enumeration of Golay complementary sequences*, J. Combin. Theory (A) **115** (2008), 753–776.

[FJW08] F. Fiedler, J. Jedwab, and A. Wiebe, *A new source of seed pairs for Golay sequences of length* 2^m, J. Combin. Theory (A), submitted 2008.

[Gol51] M.J.E. Golay, *Static multislit spectrometry and its application to the panoramic display of infrared spectra*, J. Opt. Soc. Amer. **41** (1951), 468–472.

[Gol61] ______, *Complementary series*, IRE Trans. Inform. Theory **IT-7** (1961), 82–87.

[Gol62] ______, *Note on "Complementary series"*, Proc. IRE **50** (1962), 84.

[GS65] S.W. Golomb and R.A. Scholtz, *Generalized Barker sequences*, IEEE Trans. Inform. Theory **IT-11** (1965), 533–537.

[HK94] W.H. Holzmann and H. Kharaghani, *A computer search for complex Golay sequences*, Austral. J. Combin. **10** (1994), 251–258.

[Jed05] J. Jedwab, *A survey of the merit factor problem for binary sequences*, Sequences and Their Applications – Proceedings of SETA 2004 (T. Helleseth et al., eds.), Lecture Notes in Computer Science, vol. 3486, Springer-Verlag, 2005, pp. 30–55.

[Jed08] ______, *What can be used instead of a Barker sequence?*, Contemporary Mathematics **461** (2008), 153–178.

[JF06] J. Jedwab and F. Fiedler, *How do more Golay sequences arise?*, IEEE Trans. Inform. Theory **52** (2006), 4261–4266.

[JP07a] J. Jedwab and M.G. Parker, *Golay complementary array pairs*, Designs, Codes and Cryptography **44** (2007), 209–216.

[JP07b] ______, *There are no Barker arrays having more than two dimensions*, Designs, Codes and Cryptography **43** (2007), 79–84.

[JP08] ______, *A construction of binary Golay sequence pairs from odd-length Barker sequences*, J. Combinatorial Designs, submitted 2008.

[JY06] J. Jedwab and K. Yoshida, *The peak sidelobe level of families of binary sequences*, IEEE Trans. Inform. Theory **52** (2006), 2247–2254.

[NNG$^+$89] M. Nazarathy, S.A. Newton, R.P. Giffard, D.S. Moberly, F. Sischka, W.R. Trutna, Jr., and S. Foster, *Real-time long range complementary correlation optical time domain reflectometer*, IEEE J. Lightwave Technology **7** (1989), 24–38.

[NSL+03] A. Nowicki, W. Secomski, J. Litniewski, I. Trots, and P.A. Lewin, *On the application of signal compression using Golay's codes sequences in ultrasound diagnostic*, Arch. Acoustics **28** (2003), 313–324.

[OHT78] N. Ohyama, T. Honda, and J. Tsujiuchi, *An advanced coded imaging without side lobes*, Optics Comm. **27** (1978), 339–344.

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

[Tur74a] R.J. Turyn, *Four-phase Barker codes*, IEEE Trans. Inform Theory **IT-20** (1974), 366–371.

[Tur74b] ———, *Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings*, J. Combin. Theory (A) **16** (1974), 313–333.

[Wel60] G.R. Welti, *Quaternary codes for pulsed radar*, IRE Trans. Inf. Theory **IT-6** (1960), 400–408.