A construction of binary Golay sequence pairs from odd-length Barker sequences

Jonathan Jedwab Matthew G. Parker

12 September 2008 (revised 20 January 2009)

Abstract

Binary Golay sequence pairs exist for lengths 2, 10 and 26 and, by Turyn's product construction, for all lengths of the form $2^a10^b26^c$ where a, b, c are non-negative integers. Computer search has shown that all inequivalent binary Golay sequence pairs of length less than 100 can be constructed from five "seed" pairs, of length 2, 10, 10, 20 and 26.

We give the first complete explanation of the origin of the length 26 binary Golay seed pair, involving a Barker sequence of length 13 and a related Barker sequence of length 11. This is the special case $m = 1$ of a general construction for a length $16m + 10$ binary Golay pair from a related pair of Barker sequences of length $8m + 5$ and $8m + 3$, for integer $m \geq 0$. In the case $m = 0$, we obtain an alternative explanation of the origin of one of the length 10 binary Golay seed pairs. The construction cannot produce binary Golay sequence pairs for $m > 1$, having length greater than 26, because there are no Barker sequences of odd length greater than 13.

Keywords Barker sequence, binary sequence, construction, existence, Golay sequence pair

1 Introduction

We consider a *length s sequence* to be an s-tuple $\mathcal{A} = (A_0, A_1, \ldots, A_{s-1})$ of real-valued entries. The sequence (A_i) is defined over an *alphabet* W if each sequence element A_i takes values in W. In the case $W = \{1, -1\}$ the sequence is *binary*, and in the case $W = \{0, 1, -1\}$ it is *ternary*. The *aperiodic autocorrelation function* of a length s sequence $\mathcal{A} = (A_i)$ is given by

$$C_{\mathcal{A}}(u) := \sum_{i=0}^{s-1-u} A_i A_{i+u} \quad \text{for integer } u \text{ satisfying } |u| < s,$$

and measures the extent to which the sequence resembles a shifted copy of itself. A classical problem of digital sequence design is to determine long binary sequences $\mathcal{A}$ for which $|C_{\mathcal{A}}(u)|$ is small for all nonzero u. The ideal sequence from this point of view is a *Barker sequence*, namely a binary sequence $\mathcal{A}$ for which

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

(and where $|C_{\mathcal{A}}(u)| = 1$ exactly when $s - u$ is odd).

The only lengths $s > 1$ for which a Barker sequence (A_i) is known to exist are 2, 3, 4, 5, 7, 11 and 13. Using the symbols + and − to represent the sequence elements 1 and −1 respectively,

J. Jedwab is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC, Canada V5A 1S6. He is supported by NSERC of Canada.

M.G. Parker is with Department of Informatics, High Technology Center in Bergen, University of Bergen, Bergen 5020, Norway.

examples for these lengths are

$$
\begin{aligned}
s = 2: &\ [+\ +] \\
s = 3: &\ [+\ +\ -] && (1)\\
s = 4: &\ [+\ +\ +\ -] \\
s = 5: &\ [+\ +\ +\ -\ +] && (2)\\
s = 7: &\ [+\ +\ +\ -\ -\ +\ -] \\
s = 11: &\ [+\ +\ +\ -\ -\ -\ +\ -\ -\ +\ -] && (3)\\
s = 13: &\ [+\ +\ +\ +\ +\ -\ -\ +\ +\ -\ +\ -\ +]. && (4)
\end{aligned}
$$

These examples are unique for their length, up to equivalence under one or more of the transformations

$$(A_i) \mapsto (-A_i), \tag{5}$$
$$(A_i) \mapsto (A_{s-1-i}), \tag{6}$$
$$(A_i) \mapsto ((-1)^i A_i). \tag{7}$$

No Barker sequence of length greater than 13 is known, and it has been conjectured since at least 1960 [18, p. II-2] that no such sequence exists. The conjecture is known to hold for even lengths $s < 10^{22}$ [15], and was proved for all odd lengths in 1961:

Theorem 1 (Turyn and Storer [19])**.** *There is no Barker sequence of odd length $s > 13$.*

See [12] for further details, and a survey of historical responses to the apparent nonexistence of long Barker sequences.

A length s *Golay sequence pair* is a pair of length s sequences $\mathcal{A}$ and $\mathcal{B}$ for which

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

A *Golay sequence* is a sequence that is a member of at least one Golay sequence pair. Golay sequences and Golay sequence pairs are of practical importance as an alternative to Barker sequences, and have been used in diverse digital information processing applications including infrared multislit spectrometry [8], optical time domain reflectometry [16], power control for multicarrier wireless transmission [3], and medical ultrasound [17]. Golay sequence pairs are also of theoretical importance for their mathematical structure. The two central theoretical questions are: for what lengths and over what alphabets does a Golay sequence pair exist, and how many distinct Golay sequences and Golay sequence pairs of a given length over a given alphabet are there? See [6] and [7] for recent progress on this second question, for length 2^m.

Our principal interest in this paper is binary Golay sequence pairs. Examples of such pairs are known for lengths 2, length 10 (as classified by Golay [9] in 1961), and length 26 (as found by Golay [10] in 1962 by hand, and independently by Jauregui [11] by exhaustive computer search):

$$s = 2: \left.\begin{array}{l} \mathcal{A} = [+\ +] \\ \mathcal{B} = [+\ -] \end{array}\right\} \tag{8}$$

$$s = 10: \left.\begin{array}{l} \mathcal{A} = [+\ +\ -\ -\ +\ +\ +\ -\ +\ -] \\ \mathcal{B} = [+\ +\ +\ +\ +\ -\ +\ -\ -\ +] \end{array}\right\} \text{(first pair)} \tag{9}$$

$$s = 10: \left.\begin{array}{l} \mathcal{A} = [+\ +\ -\ +\ -\ +\ -\ -\ +\ +] \\ \mathcal{B} = [+\ +\ -\ +\ +\ +\ +\ +\ -\ -] \end{array}\right\} \text{(second pair)} \tag{10}$$

$$s = 26: \left.\begin{array}{l} \mathcal{A} = [+\ +\ +\ +\ -\ +\ +\ -\ -\ +\ -\ +\ -\ +\ -\ -\ +\ -\ +\ +\ +\ -\ -\ +\ +\ +] \\ \mathcal{B} = [+\ +\ +\ +\ -\ +\ +\ -\ -\ +\ -\ +\ +\ +\ +\ +\ -\ +\ -\ -\ -\ +\ +\ -\ -\ -] \end{array}\right\}. \tag{11}$$

An unordered binary Golay sequence pair $\mathcal{A}, \mathcal{B}$ is considered equivalent to another pair of the same length if it can be transformed into that pair by a sequence of operations taken from: applying (5) to $\mathcal{A}$ or $\mathcal{B}$; applying (6) to $\mathcal{A}$ or $\mathcal{B}$; applying (7) to both $\mathcal{A}$ and $\mathcal{B}$. Up to equivalence, the only binary Golay sequence pairs of length 2, 10 and 26 are (8)–(11).

In 1974, Turyn [20] gave a composition construction for binary Golay sequence pairs that produces a pair of length st from a pair of length s and a pair of length t. Repeated application of this construction to the pairs (8)–(11) shows that length $2^a 10^b 26^c$ binary Golay sequence pairs exist for all integers $a, b, c \geq 0$; and no binary Golay sequence pairs are known whose length does not have this form. Moreover, exhaustive computer search [1] shows that all inequivalent binary Golay sequence pairs of length less than 100 can be formed using a composition construction due to Budišin [2], starting from just five "seed" pairs: the pairs (8)–(11), together with the length 20 binary Golay sequence pair

$$\left.\begin{array}{l} \mathcal{A} = [+\ +\ +\ +\ -\ +\ -\ -\ -\ +\ +\ -\ -\ +\ +\ -\ +\ -\ -\ +] \\ \mathcal{B} = [+\ +\ +\ +\ -\ +\ +\ +\ +\ +\ -\ -\ -\ +\ -\ +\ -\ +\ +\ -] \end{array}\right\}. \tag{12}$$

It is then natural to ask how the binary seed pairs (9)–(12) arise. (The length 2 seed pair (8) hardly requires explanation but, if desired, it can be constructed from the trivial length 1 pair $[+], [+]$.) While it is known that the length 10 seed pairs (9) and (10) can be constructed from the simple length 3 ternary Golay pair $[+\ +\ -]$, $[+\ 0\ +]$ (see Section 4), no convincing explanation has yet been found for the origin of the length 26 seed pair (11).

In this paper we establish the (certainly to us) surprising result that the length 26 Golay seed pair (11) can be constructed from the length 13 Barker sequence (4) and the length 11 Barker sequence (3). In fact, we give a general construction for a binary Golay sequence pair of length $16m+10$ from a Barker sequence of length $8m+5$ and a related Barker sequence of length $8m+3$, for any integer $m \geq 0$. In the case $m = 0$, this gives an alternative method of construction of the second length 10 Golay pair (10), from the length 5 Barker sequence (2) and the length 3 Barker sequence (1). Although, by Theorem 1, the construction cannot produce any new binary Golay sequence pairs, it nonetheless provides insight into how the numbers 10 and 26 arise in the study of binary Golay sequence pairs.

2 Definitions and notation

This section contains definitions and notation that will be used in the rest of the paper.

Let $\mathcal{A} = (A_i)$ be a sequence of length s. The *polynomial corresponding to* $\mathcal{A}$ (also known as the *generating function of* $\mathcal{A}$) is the degree $s-1$ polynomial

$$A(x) := \sum_{i=0}^{s-1} A_i x^i.$$

If the elements of a sequence have been specified by a letter (in this case A), use of the same letter for a polynomial will indicate that the polynomial corresponds to the sequence. We will use polynomial notation as a convenient description for sequence operations such as shifting, padding with zeroes, interleaving, and concatenation. Define the *energy* of $\mathcal{A}$ to be

$$\epsilon(\mathcal{A}) := \sum_{i=0}^{s-1} A_i^2.$$

It is straightforward to show that (for $x \neq 0$)

$$\begin{aligned}\phi(A(x)) &:= A(x)A(x^{-1}) \\ &= \sum_{u=-(s-1)}^{s-1} C_{\mathcal{A}}(u)x^u \qquad (13) \\ &= \epsilon(\mathcal{A}) + \sum_{u=1}^{s-1} C_{\mathcal{A}}(u)(x^u + x^{-u}), \qquad (14)\end{aligned}$$

since $C_{\mathcal{A}}(u) = C_{\mathcal{A}}(-u)$ for all u. It follows that, for sequences $\mathcal{A} = (A_i)$ and $\mathcal{B} = (B_i)$ of equal length,

$$\mathcal{A} \text{ and } \mathcal{B} \text{ form a Golay sequence pair if and only if } \phi(A(x)) + \phi(B(x)) \text{ is constant,} \qquad (15)$$

and if (15) holds then the value of the constant is $\epsilon(\mathcal{A}) + \epsilon(\mathcal{B})$. It also follows from the definition of ϕ that

$$\phi(x^j A(x)) = \phi(A(x)) \text{ for any integer } j. \qquad (16)$$

Given a length s sequence $\mathcal{A} = (A_i)$, we write $\mathcal{A}^* = (A_i^*)$ for the length s sequence given by

$$A_i^* := A_{s-1-i} \text{ for } 0 \leq i < s,$$

which is the reverse of the sequence $\mathcal{A}$. The polynomial corresponding to $\mathcal{A}^*$ is then given by

$$A^*(x) = x^{s-1}A(x^{-1}).$$

We remark that extending the sequence $\mathcal{A}$ to length $s+1$ by setting $A_s = 0$ does not change $A(x)$, but does change $\mathcal{A}^*$ and $A^*(x)$: the sequence length s must be specified whenever $\mathcal{A}^*$ and $A^*(x)$ are used. It is readily verified that, for any sequence $\mathcal{A}$,

$$C_{\mathcal{A}}(u) = C_{\mathcal{A}^*}(u) \text{ for all } u. \qquad (17)$$

A length s sequence (A_i) is *symmetric* if

$$A_i = A_{s-1-i} \text{ for } 0 \leq i < s,$$

or equivalently $A^*(x) = A(x)$. It is *anti-symmetric* if

$$A_i = -A_{s-1-i} \text{ for } 0 \leq i < s,$$

or equivalently $A^*(x) = -A(x)$. For example, $\mathcal{A}_1 = [0\ +\ 0\ -\ +\ -\ 0\ +\ 0]$ is symmetric of length 9 and $\mathcal{A}_2 = [+\ 0\ 0\ -\ +\ 0\ 0\ -]$ is anti-symmetric of length 8, and the corresponding polynomials are $A_1(x) = x - x^3 + x^4 - x^5 + x^7$ and $A_2(x) = 1 - x^3 + x^4 - x^7$ respectively. Note that if the last element of $\mathcal{A}_1$, namely 0, is removed then the resulting sequence $\mathcal{A}_1' = [0\ +\ 0\ -\ +\ -\ 0\ +]$ is no longer symmetric, even though the polynomial corresponding to $\mathcal{A}_1'$ is identical to that for $\mathcal{A}_1$: the sequence length must be specified when describing symmetry or anti-symmetry of a sequence and its corresponding polynomial.

A binary length $2s+1$ sequence (A_i) is *skew-symmetric* if

$$A_{s+i} = (-1)^i A_{s-i} \text{ for } 0 < i \leq s.$$

We can write the polynomial corresponding to a skew-symmetric sequence (A_i) of length $2s+1$ in the form

$$A(x) = B(x^2) + xC(x^2), \qquad (18)$$

where $B(x^2)$ and $xC(x^2)$ each correspond to a ternary sequence of length $2s+1$. If s is even then the sequence corresponding to $B(x^2)$ is symmetric and the sequence corresponding to $xC(x^2)$ is anti-symmetric, while if s is odd then the sequence corresponding to $B(x^2)$ is anti-symmetric and the sequence corresponding to $xC(x^2)$ is symmetric.

Given sequences $\mathcal{A} = (A_i)$ and $\mathcal{B} = (B_i)$, we write $\mathcal{A}+\mathcal{B}$ for the sequence $(A_i + B_i)$ and $\mathcal{A}-\mathcal{B}$ for the sequence $(A_i - B_i)$. It is easily verified that

$$C_{\mathcal{A}+\mathcal{B}}(u) + C_{\mathcal{A}-\mathcal{B}}(u) = 2C_{\mathcal{A}}(u) + 2C_{\mathcal{B}}(u). \tag{19}$$

For a sequence $\mathcal{A} = (A_i)$ and a real constant K, we write $K\mathcal{A}$ for the sequence (KA_i).

3 Preliminary results

This section contains preliminary results that will be required in the proof of the construction.

Any Barker sequence of odd length $2s+1$ is skew-symmetric, and its aperiodic autocorrelation function is completely determined by the parity of s:

Lemma 2 (Turyn and Storer [19]). *Let $\mathcal{A}$ be a Barker sequence of odd length $2s+1$. Then $\mathcal{A}$ is skew-symmetric, and*

$$\begin{aligned} C_{\mathcal{A}}(2u) &= (-1)^s \quad \text{for } 0 < u \le s \\ C_{\mathcal{A}}(2u+1) &= 0 \qquad \text{for } 0 \le u < s. \end{aligned}$$

(It follows from Lemma 2 that a given Barker sequence of odd length $s > 1$ is equivalent to exactly three other binary sequences, all of which can be generated by the transformations (5) and (6) without needing to use (7).)

The following result is useful for transferring consideration from sequences $\mathcal{A}+\mathcal{B}$ and $\mathcal{A}-\mathcal{B}$ to (any shifted version of) sequences $\mathcal{A}$ and $\mathcal{B}$:

Lemma 3. *Let $A(x)$ and $B(x)$ be polynomials corresponding to sequences, and let j, k be integers. Then*

$$\phi(A(x) + B(x)) + \phi(A(x) - B(x)) = 2\phi(x^j A(x)) + 2\phi(x^k B(x)).$$

Proof. Multiply (19) by x^u and sum over all u. By (13), we obtain

$$\phi(A(x) + B(x)) + \phi(A(x) - B(x)) = 2\phi(A(x)) + 2\phi(B(x)).$$

The result follows from (16). □

It follows from (15) that we can transform one Golay sequence pair into another:

Corollary 4. *For any integers j, k, the sequences whose corresponding polynomials are $x^j A(x)$ and $x^k B(x)$ form a Golay pair if and only if the sequences whose corresponding polynomials are $A(x) + B(x)$ and $A(x) - B(x)$ form a Golay pair.*

The case $j = k = 0$ of the next result shows that the function ϕ operates linearly on the sum of a symmetric and anti-symmetric sequence. This result is stated and proved for even s in [14], but holds without modification for all s:

Lemma 5 (Koukouvinos *et al.* [14, Theorem 2]). *Let $\mathcal{A} = (A_i)$ and $\mathcal{B} = (B_i)$ be sequences of equal length s, where $\mathcal{A}$ is symmetric and $\mathcal{B}$ is anti-symmetric, and let j, k be integers. Then*

$$\phi(A(x) + B(x)) = \phi(x^j A(x)) + \phi(x^k B(x)).$$

Proof. Since $\mathcal{A}$ is symmetric and $\mathcal{B}$ is anti-symmetric,

$$\begin{aligned}\mathcal{A}+\mathcal{B} &= \mathcal{A}^* - \mathcal{B}^* \\ &= (\mathcal{A}-\mathcal{B})^*,\end{aligned}$$

because $\mathcal{A}$ and $\mathcal{B}$ have equal length s. Therefore, for all u,

$$\begin{aligned}C_{\mathcal{A}+\mathcal{B}}(u) &= C_{(\mathcal{A}-\mathcal{B})^*}(u) \\ &= C_{\mathcal{A}-\mathcal{B}}(u),\end{aligned}$$

by (17). Substitution for $C_{\mathcal{A}-\mathcal{B}}(u)$ in (19) gives

$$C_{\mathcal{A}+\mathcal{B}}(u) = C_{\mathcal{A}}(u) + C_{\mathcal{B}}(u) \quad \text{for all } u.$$

By (13), we obtain

$$\phi(A(x)+B(x)) = \phi(A(x)) + \phi(B(x)).$$

The result follows from (16). □

A classical result due to Golay shows that the elements of a non-trivial binary Golay sequence pair occur in "quads" whose product is -1:

Lemma 6 (Golay [9])**.** *Suppose that binary sequences (A_i) and (B_i) form a Golay pair of length $s > 1$. Then s is even and*

$$\{A_i,\, B_i,\, A_{s-1-i},\, B_{s-1-i}\} \in \{\{+,+,+,-\},\, \{+,-,-,-\}\} \quad \textit{for } 0 \le i < s.$$

4 A construction of binary Golay sequence pairs

This section describes the construction and its relation to previous studies.

We saw in Section 1 that the length 26 binary Golay seed pair (11), shown as $\mathcal{A}_3$, $\mathcal{B}_3$ in Figure 1, is unique up to equivalence. By Corollary 4 with $j = k = 0$, together with (17), the ternary sequences

$$\mathcal{A}_2 := (\mathcal{A}_3 + \mathcal{B}_3)/2 \text{ and } \mathcal{B}_2 := (\mathcal{A}_3 - \mathcal{B}_3)^*/2 \tag{20}$$

form a Golay sequence pair. By a further application of Corollary 4 with $j = k = 0$, the ternary sequences

$$\mathcal{A}_1 := (\mathcal{A}_2 + \mathcal{B}_2)/2 \text{ and } \mathcal{B}_1 := (\mathcal{A}_2 - \mathcal{B}_2)/2 \tag{21}$$

also form a Golay sequence pair. Eliahou, Kervaire and Saffari [5] observed that transformations (20) and (21) can be applied to any binary Golay sequence pair $\mathcal{A}_3$, $\mathcal{B}_3$ to derive Golay pairs $\mathcal{A}_2$, $\mathcal{B}_2$ and $\mathcal{A}_1$, $\mathcal{B}_1$ (called, after suitable normalisation, the *penultimate pair* and *antepenultimate pair* respectively of the pair $\mathcal{A}_3$, $\mathcal{B}_3$ in [5]); and since the positions of the zero elements of $\mathcal{A}_2$ and $\mathcal{B}_2$ must match (by applying Lemma 6 to the pair $\mathcal{A}_3$, $\mathcal{B}_3$), both derived Golay pairs will be ternary. Transforming the binary Golay pair $\mathcal{A}_3$, $\mathcal{B}_3$ into the ternary Golay pair $\mathcal{A}_1$, $\mathcal{B}_1$ in this way is advantageous if it is easily seen that $\mathcal{A}_1$, $\mathcal{B}_1$ form a Golay pair; in that case, we can explain the existence of the Golay pair $\mathcal{A}_3$, $\mathcal{B}_3$ from $\mathcal{A}_1$, $\mathcal{B}_1$ by reversing the process under Corollary 4.

For example, let $\mathcal{F} = [+\ +\ -]$ and $\mathcal{G} = [+\ 0\ +]$ be the length 3 ternary Golay pair with corresponding polynomials $F(x) = 1+x-x^2$ and $G(x) = 1+x^2$ respectively. When transformations (20) and (21) are applied to the first length 10 binary Golay seed pair (9), the polynomials corresponding to the sequences $\mathcal{A}_1$ and $\mathcal{B}_1$ are $xF(x^3)$ and $G(x^3)$ respectively; for the second length 10 binary Golay seed pair (10), these polynomials are $F(x)$ and $x^3G(x)$. Therefore both length 10

$$
\begin{array}{ll}
\mathcal{A}_3 = [& + \; + \; + \; + \; - \; + \; + \; - \; - \; + \; - \; + \; - \; + \; - \; - \; + \; - \; + \; + \; + \; - \; - \; + \; + \; + \;] \\
\mathcal{B}_3 = [& + \; + \; + \; + \; - \; + \; + \; - \; - \; + \; - \; + \; + \; + \; + \; + \; - \; + \; - \; - \; - \; + \; + \; - \; - \; - \;] \\
 & \\
\mathcal{A}_2 = [& + \; + \; + \; + \; - \; + \; + \; - \; - \; + \; - \; + \; 0 \; + \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \;] \\
\mathcal{B}_2 = [& + \; + \; + \; - \; - \; + \; + \; + \; - \; + \; - \; - \; 0 \; - \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \;] \\
 & \\
\mathcal{A}_1 = [& + \; + \; + \; 0 \; - \; + \; + \; 0 \; - \; + \; - \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \;] \\
\mathcal{B}_1 = [& 0 \; 0 \; 0 \; + \; 0 \; 0 \; 0 \; - \; 0 \; 0 \; 0 \; + \; 0 \; + \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \; 0 \;]
\end{array}
$$

Figure 1: Decomposition of the length 26 binary Golay sequence pair under two applications of Corollary 4

seed pairs can be constructed using (16) from the simple ternary Golay pair $\mathcal{F}$, $\mathcal{G}$, as noted in [5], and no further explanation of their origin is required. (See [7] for a generalisation of this technique, that constructs new Golay pairs of length 2^m over non-binary alphabets.)

But when the transformations (20) and (21) are applied to the length 26 binary Golay seed pair, as shown in Figure 1, it is not clear how the resulting ternary pair $\mathcal{A}_1$, $\mathcal{B}_1$ arises. A partial explanation was provided by C.H. Yang, who gave the general construction of Theorem 7 for a binary Golay sequence pair of length $8k+2$ from binary sequences $\mathcal{G}$, $\mathcal{H}$ and $\mathcal{J}$. (Yang's construction is described without proof in [13], and attributed there to Ref. 15, a paper in preparation. However this reference does not seem to have appeared in print, and neither do unpublished articles by the same author with similar titles cited elsewhere as not yet published [5, Ref. Y3],

Theorem 7 (C.H. Yang)**.** *Let $k \geq 1$ be an integer. Let $\mathcal{G}$ be an anti-symmetric binary sequence of length $2k$, $\mathcal{H}$ be a binary sequence of length k, and $\mathcal{J}$ be a symmetric binary sequence of length k, with corresponding polynomials $G(x)$, $H(x)$ and $J(x)$. Suppose that*

$$\phi(G(x)) + \phi(H(x^2) + x^{2k-1}) + \phi(J(x^2)) \text{ is constant,} \tag{22}$$

and define

$$A_1(x) := G(x^2) + xJ(x^4) \text{ and } B_1(x) := x^3 H(x^4) + x^{4k+1}, \tag{23}$$

$$A_2(x) := A_1(x) + B_1(x) \text{ and } B_2(x) := A_1(x) - B_1(x), \tag{24}$$

$$A_3(x) := A_2(x) + x^{4k} B_2^*(x) \text{ and } B_3(x) := A_2(x) - x^{4k} B_2^*(x).$$

Then the sequences whose corresponding polynomials are $A_3(x)$ and $B_3(x)$ form a length $8k+2$ binary Golay pair.

By taking $k = 1$ and

$$\left.\begin{array}{rl} G(x) & = 1 - x \\ H(x) & = 1 \\ J(x) & = 1 \end{array}\right\} \tag{25}$$

in Theorem 7, we obtain the second length 10 binary Golay seed pair (10). Moreover, by taking $k = 3$ and

$$\left.\begin{array}{rl} G(x) & = 1 + x - x^2 + x^3 - x^4 - x^5 \\ H(x) & = 1 - x + x^2 \\ J(x) & = 1 + x + x^2 \end{array}\right\} \tag{26}$$

in Theorem 7, we obtain the length 26 binary Golay seed pair (11). However it is not clear why sequences $\mathcal{G}$, $\mathcal{H}$ and $\mathcal{J}$ having the required symmetry properties and whose corresponding polynomials satisfy the key equation (22) should exist, at least in the case $k = 3$, so Theorem 7 still does not satisfactorily explain how the pair (11) arises.

We now present what we believe is the first convincing explanation of the origin of the length 26 binary Golay seed pair, which also gives an alternative construction for the second length 10 binary Golay seed pair. Our construction can be viewed as the special case of $k = 2m + 1$ odd and $J(x) = \sum_{i=0}^{2m} x^i$ of Theorem 7; the novelty lies in how the polynomials $G(x)$ and $H(x)$ are derived. Our motivating observation was that when sequence elements $2i$ and $2i + 1$ of $\mathcal{A}_2$ in Figure 1 are interchanged for all i, we recover the length 13 Barker sequence (4) (followed by 13 zeroes); and when we apply the same operation to $\mathcal{B}_2$ in Figure 1, we recover the image of the length 11 Barker sequence (3) under the equivalence transformation (7) (preceded by a + symbol, and followed by a − symbol and 13 zeroes)! It is readily shown from (23) and (24) that this is equivalent to the observation that, for $G(x)$ and $H(x)$ as given in (26) and $m = 1$, we can decompose the polynomial corresponding to the length 13 Barker sequence (4) as

$$xG(x^2) + x^2H(x^4) + \sum_{i=0}^{2m+1} x^{4i}, \tag{27}$$

and the polynomial corresponding to the length 11 Barker sequence (3) in the related form

$$G(x^2) + xH(x^4) - \sum_{i=0}^{2m-1} x^{4i+3}. \tag{28}$$

Furthermore, for $G(x)$ and $H(x)$ as given in (25) and $m = 0$, we can decompose the polynomial corresponding to the length 5 Barker sequence (2) in the form (27) and the polynomial corresponding to the length 3 Barker sequence (1) in the form (28). These observations suggest a general construction for a binary Golay sequence pair of length $16m + 10$ from a Barker sequence of length $8m + 5$ having the form (27) and a Barker sequence of length $8m + 3$ having the related form (28), for any integer $m \geq 0$. We consider the related Barker sequences of this construction to be given initial objects, and make use of the structural properties of odd-length Barker sequences given by Lemma 2.

Theorem 8. *Let $m \geq 0$ be an integer. Suppose that there exist Barker sequences $\mathcal{S}_1$ and $\mathcal{S}_2$ of length $8m + 5$ and $8m + 3$ respectively, whose corresponding polynomials have the form*

$$S_1(x) := xG(x^2) + x^2H(x^4) + \sum_{i=0}^{2m+1} x^{4i},$$

$$S_2(x) := G(x^2) + xH(x^4) - \sum_{i=0}^{2m-1} x^{4i+3}$$

for some binary sequences $\mathcal{G} = (G_i)$ and $\mathcal{H} = (H_i)$ of length $4m + 2$ and $2m + 1$ respectively. Let $\mathcal{A}_1$, $\mathcal{B}_1$ be the length $8m + 6$ ternary sequences with corresponding polynomials

$$A_1(x) := G(x^2) + \sum_{i=0}^{2m} x^{4i+1} \text{ and } B_1(x) := x^3H(x^4) + x^{8m+5},$$

let $\mathcal{A}_2$, $\mathcal{B}_2$ be the length $8m + 6$ ternary sequences with corresponding polynomials

$$A_2(x) := A_1(x) + B_1(x) \text{ and } B_2(x) := A_1(x) - B_1(x),$$

and let $\mathcal{A}_3$, $\mathcal{B}_3$ be the length $16m+10$ binary sequences with corresponding polynomials

$$A_3(x) := A_2(x) + x^{8m+4}B_2^*(x) \text{ and } B_3(x) := A_2(x) - x^{8m+4}B_2^*(x).$$

Then $\mathcal{A}_3$ and $\mathcal{B}_3$ form a length $16m+10$ binary Golay pair.

Proof. We can verify from the definition of $\mathcal{A}_i$ and $\mathcal{B}_i$ for $i = 1, 2, 3$ that $\mathcal{A}_3$ and $\mathcal{B}_3$ are indeed length $16m+10$ binary sequences. We claim that $\mathcal{A}_1$ and $\mathcal{B}_1$ form a Golay pair. It then follows from Corollary 4 with $j = k = 0$ that $\mathcal{A}_2$ and $\mathcal{B}_2$ form a Golay pair. Then from (17), together with Corollary 4 with $j = 0$, $k = -(8m+4)$, it follows that $\mathcal{A}_3$ and $\mathcal{B}_3$ form a Golay pair, completing the proof. It remains only to establish the claim.

We note firstly that by Lemma 2, the Barker sequence $\mathcal{S}_1$ of length $8m+5$ is skew-symmetric. By writing $S_1(x)$ in the form (18), it follows that

$$\text{the polynomial } H(x^4) \text{ corresponds to a symmetric sequence of length } 8m+1, \tag{29}$$

and

$$\text{the polynomial } G(x^2) \text{ corresponds to an anti-symmetric sequence of length } 8m+3. \tag{30}$$

We next use (16) to write $\phi(B_1(x)) = \phi(B_1(x)/x)$, so that from the definition of $A_1(x)$ and $B_1(x)$ we have

$$\begin{aligned} 2\left[\phi(A_1(x)) + \phi(B_1(x))\right] &= 2\phi\left(G(x^2) + \sum_{i=0}^{2m} x^{4i+1}\right) + 2\phi\left(x^2H(x^4) + x^{8m+4}\right) \\ &= 2\phi\left(G(x^2)\right) + 2\phi\left(\sum_{i=0}^{2m} x^{4i}\right) + 2\phi\left(x^2H(x^4) + x^{8m+4}\right), \end{aligned}$$

by (30) and Lemma 5 with $s = 8m+3$, $A(x) = \sum_{i=0}^{2m} x^{4i+1}$, $B(x) = G(x^2)$, $j = -1$ and $k = 0$. By applying Lemma 3 with $A(x) = x^2H(x^4) + x^{8m+4}$, $B(x) = \sum_{i=0}^{2m} x^{4i}$ and $j = k = 0$, we then obtain

$$\begin{aligned} &2\left[\phi(A_1(x)) + \phi(B_1(x))\right] \\ &\qquad = 2\phi\left(G(x^2)\right) + \phi\left(x^2H(x^4) + \sum_{i=0}^{2m+1} x^{4i}\right) + \phi\left(x^2H(x^4) + x^{8m+4} - \sum_{i=0}^{2m} x^{4i}\right). \end{aligned} \tag{31}$$

Now by (29) and (30) we can apply Lemma 5 with $s = 8m+5$, $A(x) = x^2H(x^4) + \sum_{i=0}^{2m+1} x^{4i}$, $B(x) = xG(x^2)$, $j = 0$ and $k = -1$ to obtain from the definition of $S_1(x)$ that

$$\phi(S_1(x)) = \phi(G(x^2)) + \phi\left(x^2H(x^4) + \sum_{i=0}^{2m+1} x^{4i}\right). \tag{32}$$

We can similarly apply Lemma 5 with $s = 8m+3$, $A(x) = xH(x^4) - \sum_{i=0}^{2m-1} x^{4i+3}$, $B(x) = G(x^2)$, $j = 1$ and $k = 0$ to obtain from the definition of $S_2(x)$ that

$$\begin{aligned} \phi(S_2(x)) &= \phi(G(x^2)) + \phi\left(x^2H(x^4) - \sum_{i=1}^{2m} x^{4i}\right) \\ &= \phi(G(x^2)) + \phi\left(x^2H(x^4) + x^{8m+4} - \sum_{i=0}^{2m} x^{4i}\right) - \phi\left(x^{8m+4} - 1\right) \end{aligned} \tag{33}$$

by (29) and Lemma 5 with $s = 8m + 5$, $A(x) = x^2 H(x^4) - \sum_{i=1}^{2m} x^{4i}$, $B(x) = x^{8m+4} - 1$ and $j = k = 0$. Substitution of (32) and (33) in (31) then gives

$$\begin{aligned} 2\left[\phi(A_1(x)) + \phi(B_1(x))\right] &= \phi(S_1(x)) + \phi(S_2(x)) + \phi\left(x^{8m+4} - 1\right) \\ &= \phi(S_1(x)) + \phi(S_2(x)) + 2 - x^{8m+4} - x^{-(8m+4)} \end{aligned} \tag{34}$$

by the definition of ϕ. But $\mathcal{S}_1$ and $\mathcal{S}_2$ are respectively a Barker sequence of length $8m + 5$ and $8m + 3$, and so by Lemma 2 and (14) we have

$$\begin{aligned} \phi(S_1(x)) &= 8m + 5 + \sum_{u=1}^{4m+2} 1.(x^{2u} + x^{-2u}), \\ \phi(S_2(x)) &= 8m + 3 + \sum_{u=1}^{4m+1} (-1).(x^{2u} + x^{-2u}). \end{aligned}$$

Substitution in (34) then gives

$$2\left[\phi(A_1(x)) + \phi(B_1(x))\right] = 16m + 10,$$

so that $\mathcal{A}_1$ and $\mathcal{B}_1$ form a Golay pair by (15). This establishes the claim. □

For the case $m = 1$ of Theorem 8, take $\mathcal{S}_1$ to be the length 13 Barker sequence (4) and take $\mathcal{S}_2$ to be the length 11 Barker sequence (3). This fixes the sequences $\mathcal{G} = [+\ +\ -\ +\ -\ -]$ and $\mathcal{H} = [+\ -\ +]$. The pairs $\mathcal{A}_i$, $\mathcal{B}_i$ for $i = 1, 2, 3$ are then determined as in Figure 1 (but without 12 trailing zeroes for $i = 1, 2$), and $\mathcal{A}_3$, $\mathcal{B}_3$ is the length 26 binary Golay seed pair (11). For the case $m = 0$ of Theorem 8, take $\mathcal{S}_1$ to be the length 5 Barker sequence (2) and take $\mathcal{S}_2$ to be the length 3 Barker sequence (1). This fixes the sequences $\mathcal{G} = [+\ -]$ and $\mathcal{H} = [+]$, and the pairs $\mathcal{A}_i$, $\mathcal{B}_i$ for $i = 1, 2, 3$ are then determined as shown in Figure 2. We see that $\mathcal{A}_3$, $\mathcal{B}_3$ is the second length 10 binary Golay seed pair (10).

$$\begin{array}{ll} \mathcal{A}_1 = [& +\ +\ -\ 0\ 0\ 0\ ] \\ \mathcal{B}_1 = [& 0\ 0\ 0\ +\ 0\ +\ ] \end{array}$$

$$\begin{array}{ll} \mathcal{A}_2 = [& +\ +\ -\ +\ 0\ +\ ] \\ \mathcal{B}_2 = [& +\ +\ -\ -\ 0\ -\ ] \end{array}$$

$$\begin{array}{ll} \mathcal{A}_3 = [& +\ +\ -\ +\ -\ +\ -\ -\ +\ +\ ] \\ \mathcal{B}_3 = [& +\ +\ -\ +\ +\ +\ +\ +\ -\ -\ ] \end{array}$$

Figure 2: Construction of the second length 10 binary Golay seed pair under Theorem 8

5 Comments

We believe that Theorem 8 provides the first convincing explanation of the origin of the length 26 binary Golay seed pair (11), as well as an alternative explanation of the origin of the second length 10 binary Golay seed pair (10). The last of the five binary Golay seed pairs (8)–(12) described in Section 1 whose origin remains to be satisfactorily explained is the length 20 pair (12).

Although Theorem 8 is valid for all integers $m \geq 0$, it cannot be used to produce binary Golay pairs of length $16m + 10$ for $m > 1$ because the supply of odd-length Barker sequences runs out at length 13, by Theorem 1. This can also be explained by noting that the "gap number" of the binary Golay pair $\mathcal{A}_3$, $\mathcal{B}_3$ constructed in Theorem 8 (namely the number of internal zeroes in the pair $\mathcal{A}_2$, $\mathcal{B}_2$ resulting from (20)) is 1, and appealing to the result of Eliahou, Kervaire and Saffari [5, Thm. 4.8] that any binary Golay pair with a gap number of 1 must have length 10 or 26. (This observation was previously made in [5] in relation to C.H. Yang's Theorem 7, of which Theorem 8 can be viewed as a special case.)

To our knowledge, Theorem 8 is the first result linking binary Golay sequence pairs to odd-length Barker sequences. While we consider this connection to be unexpected, there is a well-known result linking binary Golay sequence pairs and even-length Barker sequences: if (A_i) is a Barker sequence of even length s, then (A_i) and $((-1)^i A_i)$ form a binary Golay sequence pair of length s. This result is used to deduce Corollary 10 from Theorem 9.

Theorem 9 (Eliahou, Kervaire and Saffari [4], [5])**.** *Suppose there exists a binary Golay sequence pair of even length s. Then s has no prime factor congruent to* 3 *modulo* 4*.*

Corollary 10. *Suppose there exists a Barker sequence of even length s. Then s has no prime factor congruent to* 3 *modulo* 4*.*

References

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

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

[3] 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**:2397–2417, 1999.

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

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

[6] 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**:753–776, 2008.

[7] 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.

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

[9] M.J.E. Golay. Complementary series. *IRE Trans. Inform. Theory*, **IT-7**:82–87, 1961.

[10] M.J.E. Golay. Note on 'Complementary series'. *Proc. IRE*, **50**:84, 1962.

[11] S. Jauregui, Jr. Complementary sequences of length 26. *IRE Trans. Inform. Theory*, **IT-8**:323, 1962.

[12] J. Jedwab. What can be used instead of a Barker sequence? *Contemporary Math.*, **461**:153–178, 2008.

[13] C. Koukouvinos, S. Kounias, J. Seberry, C.H. Yang, and J. Yang. Multiplication of sequences with zero autocorrelation. *Australasian J. Combin.*, **10**:5–15, 1994.

[14] C. Koukouvinos, S. Kounias, J. Seberry, C.H. Yang, and J. Yang. On sequences with zero autocorrelation. *Designs, Codes and Cryptography*, **4**:327–340, 1994.

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

[16] 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**:24–38, 1989.

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

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

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

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

[21] C.H. Yang. On composition of four-symbol δ-codes and Hadamard matrices. *Proc. Amer. Math. Soc.*, **107**:763–776, 1989.