How Do More Golay Sequences Arise?

Frank Fiedler Jonathan Jedwab

May 13, 2005 (revised May 17, 2006)

Abstract

In 1999 Davis and Jedwab gave a direct construction of Golay complementary sequences over $\mathbb{Z}_{2^h}$ of length 2^m. Recently Li and Chu found 1024 more quaternary Golay complementary sequences of length 16, that cannot be obtained by the direct construction, using exhaustive computer enumeration. It is shown how these sequences arise from interleaving and concatenation of two classes of Golay complementary sequences given as an example by Davis and Jedwab. These examples spawn new Golay sequences over $\mathbb{Z}_{2^h}$ of length 2^m for all $h \geq 2$ and $m \geq 4$.

Keywords algebraic normal form, complementary, construction, Golay sequence, quaternary

1 Introduction

Let $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1})$ be a sequence of length n and characteristic H, that is, each entry $a_i \in \mathbb{Z}_H$. Let $\xi = \exp(2\pi\sqrt{-1}/H)$, and define the *aperiodic autocorrelation* of $\boldsymbol{a}$ at displacement u by

$$C_{\boldsymbol{a}}(u) = \sum_{i=0}^{n-1-u} \xi^{a_i - a_{i+u}}.$$

A *Golay pair*, or pair of complementary sequences, is a pair $(\boldsymbol{a}, \boldsymbol{b})$ of sequences with the property that their out-of-phase autocorrelations sum to zero, that is, $C_{\boldsymbol{a}}(u) + C_{\boldsymbol{b}}(u) = 0$, $0 < u < n$. Each sequence of a pair is called a *Golay complementary sequence*, or *Golay sequence*. We call a sequence binary, quaternary, or octary, respectively, if $H = 2, 4$, or 8. Sequences with $H > 2$ are also called *polyphase*. Note that it is also common to consider the sequence of complex modulated values $(\xi^{a_0}, \xi^{a_1}, \ldots, \xi^{a_{n-1}})$. In particular, a binary sequence can be regarded as a sequence of $+1$ and -1 entries, whereas we consider binary sequences of 0 and 1 entries. We will denote the all-1 sequence (whose length is to be understood from the context) by $\mathbf{1}$.

Complementary binary sequences were introduced by Marcel Golay [Gol 61] to study problems in infrared multislit spectrometry. Both binary and polyphase Golay sequences have since found many applications, such as in optical time-domain reflectometry or orthogonal frequency-division multiplexing (OFDM). They are known to guarantee a low peak-to-average power ratio in OFDM [Pop 91]. In [DJ 99] the then-known Golay sequences of length 2^m and characteristic $H = 2^h$, $m > 1$, $h \geq 1$, were shown to occur as cosets of the first-order Reed-Muller code within the second-order Reed-Muller code (appropriately defined for $h > 1$). Hence these Golay sequences also provide a good error correction capability. For a survey on Golay complementary sequences, see [PPT 03]. Recently Li and Chu [LC 05] found 1024 new quaternary Golay sequences of length 16 that do not occur as a single coset of the first-order Reed-Muller code in the second-order Reed-Muller code.

The authors are with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC, Canada V5A 1S6. J. Jedwab is grateful for support from NSERC of Canada via Discovery Grant # 31-611394.

2 Construction of Golay Pairs

Golay introduced several recursive constructions for binary Golay pairs, such as concatenation and interleaving. He also gave an explicit construction for length 2^m using generalized boolean sums [Gol 61]. Golay later noted [Gol 77] that this explicit construction gives $2^m m!$ distinct binary complementary sequences. Budišin [Bud 90] introduced an iterative construction for (polyphase) Golay pairs. This construction contains Golay's concatentation and interleaving of binary sequences as a particular case. Davis and Jedwab [DJ 99] gave an explicit construction of $(m!/2) \cdot 2^{h(m+1)}$ Golay sequences of characteristic $H = 2^h$ and length 2^m. Paterson [Pat 00] showed that the set of Golay sequences of length 2^m over $\mathbb{Z}_{2^h}$ obtainable by Golay's explicit construction for $h = 1$ and those obtainable by Budišin's iterative construction for $h \geq 1$ coincide with the sequences described in [DJ 99]. Furthermore, he generalized [DJ 99] to the case H even.

2.1 Concatenation and Interleaving

Let $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1})$ and $\boldsymbol{b} = (b_0, b_1, \ldots, b_{k-1})$ be sequences of length n and k, respectively. The *concatenation* of $\boldsymbol{a}$ and $\boldsymbol{b}$ is the sequence

$$\boldsymbol{a}\,;\boldsymbol{b} = (a_0, a_1, \ldots, a_{n-1}, b_0, b_1, \ldots, b_{k-1})$$

of length $n + k$. If $n = k$, then we construct the *interleaving* of $\boldsymbol{a}$ and $\boldsymbol{b}$ as the sequence

$$\mathrm{int}(\boldsymbol{a}, \boldsymbol{b}) = (a_0, b_0, a_1, b_1, \ldots, a_{n-1}, b_{n-1})$$

of length $2n$. Golay showed that if $\boldsymbol{a}$ and $\boldsymbol{b}$ form a binary Golay pair, then $\boldsymbol{a}\,;\boldsymbol{b}$ and $\boldsymbol{a}\,;(\boldsymbol{b} + \boldsymbol{1})$ also form a binary Golay pair [Gol 61, General Property 9]. Similarly, $\mathrm{int}(\boldsymbol{a}, \boldsymbol{b})$ and $\mathrm{int}(\boldsymbol{a}, \boldsymbol{b} + \boldsymbol{1})$ form a binary Golay pair [Gol 61, General Property 10].

Budišin [Bud 90] generalized concatenation and interleaving by allowing gaps in intermediate steps of an iterative construction. He noted that some Golay sequences generated by this method cannot be generated by Golay's recursive methods, meaning concatenation and interleaving. An example is the binary Golay sequence

$$\boldsymbol{a} = (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1).$$

The sequence $\boldsymbol{a}$ is neither the concatenation nor the interleaving of any binary Golay pair.

The recursive construction of concatenation and interleaving generalizes to other (even) characteristics. Suppose $\boldsymbol{a}$ and $\boldsymbol{b}$ are a Golay pair of characteristic H and length n. If H is even, it is straightforward to show that $\boldsymbol{a}\,;\boldsymbol{b}$ and $\boldsymbol{a}\,;(\boldsymbol{b} + \frac{H}{2} \cdot \boldsymbol{1})$, as well as $\mathrm{int}(\boldsymbol{a}, \boldsymbol{b})$ and $\mathrm{int}(\boldsymbol{a}, \boldsymbol{b} + \frac{H}{2} \cdot \boldsymbol{1})$, also form a Golay pair of characteristic H and length $2n$.

2.2 Cosets of Sequences

We would like to investigate under what circumstances adding a sequence $\boldsymbol{c}$ to each sequence of a Golay pair $(\boldsymbol{a}, \boldsymbol{b})$ creates another (possibly new) Golay pair $(\boldsymbol{a} + \boldsymbol{c}, \boldsymbol{b} + \boldsymbol{c})$. We begin with a small observation that does not seem to have appeared in print.

Lemma 1. *Let $\boldsymbol{a}$ and $\boldsymbol{c}$ be sequences of length n over $\mathbb{Z}_H$, where $\boldsymbol{c} = (c, c'+c, 2c'+c, \ldots, (n-1)c'+c)$, $c, c' \in \mathbb{Z}_H$. Let $\boldsymbol{a} + \boldsymbol{c}$ be the sequence obtained from $\boldsymbol{a}$ and $\boldsymbol{c}$ by elementwise addition* (mod H). *Then $C_{\boldsymbol{a}+\boldsymbol{c}}(u) = \xi^{-uc'} C_{\boldsymbol{a}}(u)$.*

Proof.

$$\begin{aligned} C_{\boldsymbol{a}+\boldsymbol{c}}(u) &= \sum_{i=0}^{n-1-u} \xi^{(a_i+ic'+c)-(a_{i+u}+(i+u)c'+c)} \\ &= \xi^{-uc'} \sum_{i=0}^{n-1-u} \xi^{a_i-a_{i+u}} \\ &= \xi^{-uc'} C_{\boldsymbol{a}}(u) \end{aligned}$$

□

So we may add a constant sequence $\boldsymbol{c} = c \cdot \mathbf{1}$, $c \in \mathbb{Z}_H$, to a sequence $\boldsymbol{a}$, and $\boldsymbol{a} + \boldsymbol{c}$ will have the same autocorrelation function as $\boldsymbol{a}$. This fact is well-known. We may also add a multiple of the sequence $(0, 1, 2, 3, 4, \ldots)$ to a sequence $\boldsymbol{a}$ and to another sequence $\boldsymbol{b}$. Generally, the new sequences will not have the same autocorrelation functions as $\boldsymbol{a}$ and $\boldsymbol{b}$, respectively. However, Lemma 1 can be used to construct new Golay pairs from a given one. If $\boldsymbol{a}$ and $\boldsymbol{b}$ form a Golay pair, we can add a sequence $\boldsymbol{c}$ to obtain new sequences $\boldsymbol{a} + \boldsymbol{c}$ and $\boldsymbol{b} + \boldsymbol{c}$, where $\boldsymbol{c}$ is as above with $c, c' \in \mathbb{Z}_H$. Then, by Lemma 1, we have $C_{\boldsymbol{a}+\boldsymbol{c}}(u) = \xi^{-uc'} C_{\boldsymbol{a}}(u)$ and $C_{\boldsymbol{b}+\boldsymbol{c}}(u) = \xi^{-uc'} C_{\boldsymbol{b}}(u) = -\xi^{-uc'} C_{\boldsymbol{a}}(u)$.

Corollary 2. *Let $\boldsymbol{a}$, $\boldsymbol{b}$, and $\boldsymbol{c}$ be sequences of length n over $\mathbb{Z}_H$, where $(\boldsymbol{a}, \boldsymbol{b})$ is a Golay pair and $\boldsymbol{c} = (c, c' + c, 2c' + c, \ldots, (n-1)c' + c)$, $c, c' \in \mathbb{Z}_H$. Then $(\boldsymbol{a} + \boldsymbol{c}, \boldsymbol{b} + \boldsymbol{c})$ is a Golay pair.*

For binary sequences, this amounts to General Property 5 of [Gol 61], which states that adding the alternating sequence $(0, 1, 0, 1, \ldots)$ to each sequence of a Golay pair creates another Golay pair. For quaternary sequences, it shows that adding a multiple of $(0, 1, 2, 3, 0, 1, 2, \ldots)$ to each sequence of a (quaternary) Golay pair creates another Golay pair.

In [LC 05] a two-step process of reducing sequences to "*d*"- and "*dd*"-sequences was introduced (without proof), which helped reduce the search space. It is essentially an application of Lemma 1.

There have been several recursive, iterative, and direct constructions of Golay pairs over even characteristic H [Gol 61], [Bud 90], [DJ 99], [Pat 00]. By design, all these constructions create Golay pairs $(\boldsymbol{a}, \boldsymbol{b})$ such that $\boldsymbol{b} - \boldsymbol{a}$ is a sequence that takes only two values, ℓ and $\frac{H}{2} + \ell \pmod H$, for a suitable $\ell \in \mathbb{Z}_H$. In such a case, $\boldsymbol{b} - \boldsymbol{a} - \ell \cdot \mathbf{1}$ is a $\{0, \frac{H}{2}\}$-sequence. Let $\boldsymbol{c} = \frac{2}{H}(\boldsymbol{b} - \boldsymbol{a} - \ell \cdot \mathbf{1})$. We will see that we can form more Golay pairs by adding a multiple of $\boldsymbol{c}$ to the Golay sequences $\boldsymbol{a}$ and $\boldsymbol{b}$.

Lemma 3. *Let $\boldsymbol{c}$ be a $\{0, 1\}$ (that is, binary) sequence, and suppose that $(\boldsymbol{a}, \boldsymbol{a} + \frac{H}{2}\boldsymbol{c} + \ell \cdot \mathbf{1})$ is a Golay pair over $\mathbb{Z}_H$, H even. Then $\boldsymbol{a} + k \cdot \boldsymbol{c}$ and $\boldsymbol{a} + (\frac{H}{2} + k)\boldsymbol{c} + \ell \cdot \mathbf{1}$ also form a pair of Golay complementary sequences for any $k \in \mathbb{Z}_H$.*

Proof. By Corollary 2 we may assume $\ell = 0$. Let u be fixed. Let $I_+(u)$ be the set of indices i such that $c_i = 1$ and $c_{i+u} = 0$. Thus, for $i \in I_+(u)$, $(\boldsymbol{a} + k\boldsymbol{c})_i = a_i + k$ and $(\boldsymbol{a} + k\boldsymbol{c})_{i+u} = a_{i+u}$. Similarly, let $I_-(u)$ denote the set of indices i such that $c_i = 0$ and $c_{i+u} = 1$. Hence, for any $i \in I_-(u)$, $(\boldsymbol{a} + k\boldsymbol{c})_i = a_i$ and $(\boldsymbol{a} + k\boldsymbol{c})_{i+u} = a_{i+u} + k$. If $c_i = c_{i+u}$ then $(\boldsymbol{a} + k\boldsymbol{c})_i - (\boldsymbol{a} + k\boldsymbol{c})_{i+u} = a_i - a_{i+u}$. Therefore

$$\begin{aligned} C_{\boldsymbol{a}+k\boldsymbol{c}}(u) = C_{\boldsymbol{a}}(u) & \\ - \sum_{i \in I_-(u)} \xi^{a_i - a_{i+u}} + \sum_{i \in I_-(u)} \xi^{a_i - (a_{i+u}+k)} & \\ - \sum_{i \in I_+(u)} \xi^{a_i - a_{i+u}} + \sum_{i \in I_+(u)} \xi^{(a_i+k) - a_{i+u}} & \\ = C_{\boldsymbol{a}}(u) + (\xi^{-k} - 1) \sum_{i \in I_-(u)} \xi^{a_i - a_{i+u}} + (\xi^k - 1) \sum_{i \in I_+(u)} \xi^{a_i - a_{i+u}}. & \end{aligned}$$

Recall that $\xi^{\frac{H}{2}} = -1$. Now the same calculations with $C_{\boldsymbol{a}+(\frac{H}{2}+k)\boldsymbol{c}}(u)$ show

$$\begin{aligned} C_{\boldsymbol{a}+(\frac{H}{2}+k)\boldsymbol{c}}(u) &= C_{\boldsymbol{a}+\frac{H}{2}\boldsymbol{c}}(u) \\ &\quad + (\xi^{-k}-1)\sum_{i\in I_-(u)} \xi^{a_i-(a_{i+u}+\frac{H}{2})} \\ &\quad + (\xi^{k}-1)\sum_{i\in I_+(u)} \xi^{(a_i+\frac{H}{2})-a_{i+u}} \\ &= -C_{\boldsymbol{a}}(u) - (\xi^{-k}-1)\sum_{i\in I_-(u)} \xi^{a_i-a_{i+u}} - (\xi^{k}-1)\sum_{i\in I_+(u)} \xi^{a_i-a_{i+u}} \end{aligned}$$

by assumption. This completes the proof. □

Note that, even though by design the constructions [Gol 61], [Bud 90], [DJ 99], [Pat 00] create Golay pairs $(\boldsymbol{a}, \boldsymbol{b})$ such that $\boldsymbol{b} - \boldsymbol{a}$ is an $\{\ell, \ell + \frac{H}{2}\}$-sequence for some $\ell \in \mathbb{Z}_H$, it is not true that $\boldsymbol{b} - \boldsymbol{a}$ is a two-value sequence for every Golay pair $(\boldsymbol{a}, \boldsymbol{b})$ (cf. Section 3, (6)). As it turns out, it is actually Golay pairs $(\boldsymbol{a}, \boldsymbol{b})$ such that $\boldsymbol{b} - \boldsymbol{a}$ is a sequence with more than two values that will allow us to explain the newly discovered Golay sequences from [LC 05].

Corollary 2 and Lemma 3 naturally organize Golay pairs in sets. That is, we consider sets of Golay pairs where each member $(\boldsymbol{a}, \boldsymbol{b})$ of such a set can be obtained from any other member $(\boldsymbol{a}', \boldsymbol{b}')$ by adding a suitable combination of sequences in accordance with Corollary 2 and Lemma 3. Our main motivation for this approach is to obtain a starting point for the comparison of the properties of the known Golay sequences with the properties of the 1024 new sequences. We will discuss these questions in more detail in Sections 4 and 5.

The next result is well-known for binary sequences, but it has not often been applied to polyphase sequences. Strictly speaking, it does not involve adding a sequence $\boldsymbol{c}$ to the sequences of a Golay pair. However, it is a general way of constructing a Golay pair from a given Golay pair, and we would like to include it for completeness.

Lemma 4. *Let $(\boldsymbol{a}, \boldsymbol{b})$ be a Golay pair and let $\boldsymbol{a}^* = (-a_{n-1}, -a_{n-2}, \ldots, -a_0)$. Then $C_{\boldsymbol{a}}(u) = C_{\boldsymbol{a}^*}(u)$ for all $0 \le u < n$ and thus, $(\boldsymbol{a}^*, \boldsymbol{b})$ is a Golay pair.*

Proof.

$$\begin{aligned} C_{\boldsymbol{a}^*}(u) &= \sum_{i=0}^{n-1-u} \xi^{-a_{(n-1)-i}-(-a_{(n-1)-(i+u)})} \\ &= \sum_{i=0}^{n-1-u} \xi^{a_{(n-1)-(i+u)}-a_{(n-1)-i}} \\ &= \sum_{j=0}^{n-1-u} \xi^{a_j-a_{j+u}} \\ &= C_{\boldsymbol{a}}(u) \end{aligned}$$

where $j = (n-1) - (i+u)$. □

If $\boldsymbol{a}$ is a binary sequence, then $\boldsymbol{a}^* = (a_{n-1}, a_{n-2}, \ldots, a_0)$ since $-1 \equiv 1 \pmod 2$ and $-0 \equiv 0 \pmod 2$. Thus, if $(\boldsymbol{a}, \boldsymbol{b})$ is a binary Golay pair, then $((a_{n-1}, a_{n-2}, \ldots, a_0), \boldsymbol{b})$ is also a binary Golay pair [Gol 61, General Property 3]. In general, this is not true for polyphase Golay pairs. However, we will see in the next subsection how Golay pairs $(\boldsymbol{a}, \boldsymbol{b})$, $(\boldsymbol{a}^*, \boldsymbol{b})$, $(\boldsymbol{a}, \boldsymbol{b}^*)$, and $(\boldsymbol{a}^*, \boldsymbol{b}^*)$ occur naturally in the construction in [DJ 99].

Henceforth we will restrict our attention to the case $H = 2^h$, $h \geq 1$, and $n = 2^m$, $m \geq 1$. In this setting we can describe sequences algebraically.

2.3 Boolean Functions

When $H = 2^h$ and $n = 2^m$, sequences $\boldsymbol{a} \in \mathbb{Z}_{2^h}^{2^m}$ can be described using generalized boolean functions.

A *generalized boolean function* is a function $f : \mathbb{Z}_2^m \to \mathbb{Z}_{2^h}$, $h \geq 1$. Consider the test functions $f_i(x_1, x_2, \ldots, x_m) = x_i$. They give rise to 2^m monomials

$$\begin{aligned} &1, \\ &x_1, x_2, \ldots, x_m, \\ &x_1x_2, x_1x_3, \ldots, x_{m-1}x_m, \\ &\vdots \\ &x_1x_2 \cdots x_m \end{aligned} \tag{1}$$

Any (generalized) boolean function $f : \mathbb{Z}_2^m \to \mathbb{Z}_{2^h}$ can be expressed uniquely as a linear combination over $\mathbb{Z}_{2^h}$ of these monomials (1). The resulting polynomial is called the *algebraic normal form* of f. With f we associate a sequence $\boldsymbol{f}$ of length 2^m by listing the values $f(x_1, x_2, \ldots, x_m)$ as $(x_1, x_2, \ldots, x_m)$ ranges over $\mathbb{Z}_2^m$ lexicographically. For example, if $m = 3$ and $h = 2$ then

$$\begin{aligned} \boldsymbol{x}_3 &= (0,1,0,1,0,1,0,1) \\ 2\boldsymbol{x}_2 &= (0,0,2,2,0,0,2,2) \\ 2\boldsymbol{x}_2 + \boldsymbol{x}_3 &= (0,1,2,3,0,1,2,3). \end{aligned}$$

Here $\boldsymbol{x}_2$ and $\boldsymbol{x}_3$ denote the sequences corresponding to the functions x_2 and x_3, respectively. In particular, the sequence

$$\begin{aligned} \boldsymbol{c} &= c \cdot \mathbf{1} + c' \sum_{i=1}^{m} 2^{m-i} \boldsymbol{x}_i \\ &= c \cdot \mathbf{1} + c'(\boldsymbol{x}_m + 2\boldsymbol{x}_{m-1} + \cdots + 2^{h-1}\boldsymbol{x}_{m-h+1}) \end{aligned}$$

is the sequence used in Lemma 1.

Theorem ([DJ 99, Corollary 5])**.** *Let*

$$f = 2^{h-1} \sum_{k=1}^{m-1} x_{\pi(k)} x_{\pi(k+1)} + \sum_{k=1}^{m} c_k x_k,$$

where π is a permutation of the symbols $\{1, 2, \ldots, m\}$ and $c_k \in \mathbb{Z}_{2^h}$. Then any sequence in the set

$$A = \{\boldsymbol{f} + c \cdot \mathbf{1}, \boldsymbol{f} + 2^{h-1}(\boldsymbol{x}_{\pi(1)} + \boldsymbol{x}_{\pi(m)}) + c \cdot \mathbf{1} \mid c \in \mathbb{Z}_{2^h}\}$$

forms a Golay complementary pair over $\mathbb{Z}_{2^h}$ of length 2^m with any sequence in the set

$$B = \{\boldsymbol{f} + 2^{h-1}\boldsymbol{x}_{\pi(1)} + c' \cdot \mathbf{1}, \boldsymbol{f} + 2^{h-1}\boldsymbol{x}_{\pi(m)} + c' \cdot \mathbf{1} \mid c' \in \mathbb{Z}_{2^h}\}.$$

We remark that either of the two sequences $\boldsymbol{f} + c \cdot \mathbf{1}$ and $\boldsymbol{f} + 2^{h-1}(\boldsymbol{x}_{\pi(1)} + \boldsymbol{x}_{\pi(m)}) + c \cdot \mathbf{1}$ can be formally obtained from one another (up to a constant c') by mapping each $x_i \to -(1 - x_i)$, $1 \leq i \leq m$, in the definition of f. Thus, (up to a constant) they are negative reverses of each other

and have the same autocorrelation function (Lemma 4). The same is true for the two sequences $\boldsymbol{f} + 2^{h-1}\boldsymbol{x}_{\pi(1)} + c' \cdot \mathbf{1}$ and $\boldsymbol{f} + 2^{h-1}\boldsymbol{x}_{\pi(m)} + c' \cdot \mathbf{1}$.

For instance, for the three quaternary sequences $\boldsymbol{b} = 2(x_1x_2 + x_1x_3) + x_1$, $\boldsymbol{b}' = 2(x_1x_2 + x_1x_3) + x_1 + 2x_2 + 2x_3 + 3$, and $\boldsymbol{b}'' = 2(x_1x_2 + x_1x_3) + 3x_1 + 2x_2 + 2x_3 + 1$ of length 8 (where we have identified the functions with their associated sequences), we have

$$\begin{aligned}\boldsymbol{b} &= (0,0,0,0,1,3,3,1),\\ \boldsymbol{b}' &= (3,1,1,3,0,0,0,0),\\ \boldsymbol{b}'' &= (1,3,3,1,0,0,0,0).\end{aligned}$$

These sequences are of the form given in [DJ 99, Corollary 5] with $m = 3$, $h = 2$, and $\pi = (1, 2)$. We see that $\boldsymbol{b}''$ is the reverse of $\boldsymbol{b}$, $\boldsymbol{b}' = \boldsymbol{b} + 2(x_{\pi(1)} + x_{\pi(3)}) + 3$, and $\boldsymbol{b}' = \boldsymbol{b}^*$ (that is, $b'_i \equiv -b_{7-i} \pmod 4$). We calculate the autocorrelation function for each of these sequences.

$$\begin{aligned}(C_{\boldsymbol{b}}(u) \mid 0 \le u \le 7) &= (8, 2-\sqrt{-1}, 0, 2+\sqrt{-1}, 0, \sqrt{-1}, 0, -\sqrt{-1}),\\ (C_{\boldsymbol{b}'}(u) \mid 0 \le u \le 7) &= (8, 2-\sqrt{-1}, 0, 2+\sqrt{-1}, 0, \sqrt{-1}, 0, -\sqrt{-1}),\\ (C_{\boldsymbol{b}''}(u) \mid 0 \le u \le 7) &= (8, 2+\sqrt{-1}, 0, 2-\sqrt{-1}, 0, -\sqrt{-1}, 0, \sqrt{-1}).\end{aligned}$$

Clearly, the autocorrelation function of $\boldsymbol{b}''$ does not coincide with that of $\boldsymbol{b}$ (see also the remark following Lemma 4).

3 Explaining the New Examples

With $h = 2$ and $m = 3$, define the sets

$$\begin{aligned}A = \{&2(x_1x_2 + x_2x_3) + c,\\ &2(x_1x_2 + x_2x_3) + 2x_1 + 2x_3 + c \mid c \in \mathbb{Z}_4\}\\ B = \{&2(x_1x_2 + x_2x_3) + 2x_1 + c,\\ &2(x_1x_2 + x_2x_3) + 2x_3 + c \mid c \in \mathbb{Z}_4\}\\ A' = \{&2(x_1x_2 + x_1x_3) + 3x_2 + x_3 + c,\\ &2(x_1x_2 + x_1x_3) + x_2 + 3x_3 + c \mid c \in \mathbb{Z}_4\}\\ B' = \{&2(x_1x_2 + x_1x_3) + x_2 + x_3 + c,\\ &2(x_1x_2 + x_1x_3) + 3x_2 + 3x_3 + c \mid c \in \mathbb{Z}_4\},\end{aligned} \tag{2}$$

in which we again identify the functions with their associated sequences. Then the sequences in A, B, A', and B' are quaternary sequences of length eight. Since they are of the form given in [DJ 99, Corollary 5], any of the eight sequences in A forms a quaternary Golay complementary pair with any of the sequences in B. Also, any of the sequences in A' forms a Golay pair with any of the sequences in B'. In particular, all sequences in A share the same autocorrelation function. Similarly, all sequences in A' have the same autocorrelation function. Let $\boldsymbol{a} \in A$ and $\boldsymbol{a}' \in A'$. Direct calculations show that

$$(C_{\boldsymbol{a}}(u) \mid 0 \le u \le 7) = (8, -1, 0, 3, 0, 1, 0, 1)$$

and

$$(C_{\boldsymbol{a}'}(u) \mid 0 \le u \le 7) = (8, -1, 0, 3, 0, 1, 0, 1).$$

Hence $C_{\boldsymbol{a}}(u) = C_{\boldsymbol{a}'}(u)$ for any $\boldsymbol{a} \in A$ and $\boldsymbol{a}' \in A'$, $0 \le u \le 7$. Consequently, $C_{\boldsymbol{b}}(u) = C_{\boldsymbol{b}'}(u)$ for any $\boldsymbol{b} \in B$ and $\boldsymbol{b}' \in B'$, $0 \le u \le 7$. As noted in [DJ 99, p. 2401], this "cross-over" of the corresponding autocorrelation function leads to more Golay pairs than one would expect from the construction. For instance, take any sequence $\boldsymbol{a}$ from A, and pair it with any sequence $\boldsymbol{b}'$ from B'. This gives a Golay pair $(\boldsymbol{a}, \boldsymbol{b}')$. So instead of $2 \cdot 8^2 = 128$ Golay pairs formed by pairs of sequences from $A \times B$ and $A' \times B'$, we obtain $(8+8)^2 = 256$ Golay pairs formed by pairs of sequences from $(A \cup A') \times (B \cup B')$.

We may form further examples by adding multiples of $\boldsymbol{x}_3 + 2\boldsymbol{x}_2$ to each sequence in A, B, A', and B' (Corollary 2). This essentially creates *cosets* $A + c' \cdot (\boldsymbol{x}_3 + 2\boldsymbol{x}_2)$, $B + c' \cdot (\boldsymbol{x}_3 + 2\boldsymbol{x}_2)$, $A' + c' \cdot (\boldsymbol{x}_3 + 2\boldsymbol{x}_2)$, and $B' + c' \cdot (\boldsymbol{x}_3 + 2\boldsymbol{x}_2)$, $c' \in \mathbb{Z}_4$. However, note that $\{\boldsymbol{a} + 2(\boldsymbol{x}_3 + 2\boldsymbol{x}_2) \mid \boldsymbol{a} \in A\} = B$ and $\{\boldsymbol{b} + 2(\boldsymbol{x}_3 + 2\boldsymbol{x}_2) \mid \boldsymbol{b} \in B\} = A$. Hence by adding multiples of $\boldsymbol{x}_3 + 2\boldsymbol{x}_2$ we obtain only the original four sets (2), and the four sets $A + (\boldsymbol{x}_3 + 2\boldsymbol{x}_2)$, $B + (\boldsymbol{x}_3 + 2\boldsymbol{x}_2)$, $A' + (\boldsymbol{x}_3 + 2\boldsymbol{x}_2)$, and $B' + (\boldsymbol{x}_3 + 2\boldsymbol{x}_2)$. Exhaustive computer enumeration has confirmed that these two examples of four sets are the only ones exhibiting a "cross-over" of the autocorrelation function of Golay sequences of length 8 over $\mathbb{Z}_4$.

The sequences in (2) can be used to construct sequences which cannot be obtained with [DJ 99, Corollary 5]. For example, let $\boldsymbol{a} \in A$ and $\boldsymbol{b} \in B'$ where

$$\boldsymbol{a} = 2(x_1x_2 + x_2x_3) \tag{3}$$

$$\boldsymbol{b} = 2(x_1x_2 + x_1x_3) + x_2 + x_3. \tag{4}$$

Then

$$\begin{aligned} \boldsymbol{a}\,;\boldsymbol{b} &= 2x_1x_2x_4 + 2x_1x_3x_4 + x_1x_3 + x_1x_4 + 2x_2x_3 + 2x_3x_4 \\ &= (0,0,0,2,0,0,2,0,0,1,1,2,0,3,3,2). \end{aligned} \tag{5}$$

Note that x_i is a function from $\mathbb{Z}_2^4$ to $\mathbb{Z}_4$ in (5), $1 \le i \le 4$, whereas in (3) and (4) we have $x_i : \mathbb{Z}_2^3 \to \mathbb{Z}_4$, $1 \le i \le 3$.

The sequence $\boldsymbol{a}\,;\boldsymbol{b}$ forms a Golay pair with $\boldsymbol{a}\,;(\boldsymbol{b} + 2^{h-1} \cdot \mathbf{1}) = (\boldsymbol{a}\,;\boldsymbol{b}) + 2\boldsymbol{x}_1$, and both Golay sequences are not of the form given in [DJ 99, Corollary 5]. In fact, they correspond to entry #8 with $a_0 = 0$, $d_0 = 0$ and entry #5c with $a_0 = 0$, $d_0 = 0$ in [LC 05, Table 1].

We remark that

$$\begin{aligned} \boldsymbol{b} - \boldsymbol{a} &= 2(x_1x_3 + x_2x_3) + x_2 + x_3 \\ &= (0,1,1,0,0,3,1,2), \end{aligned} \tag{6}$$

so $\boldsymbol{b} - \boldsymbol{a}$ is not a sequence taking just two values ℓ and $\ell + \frac{H}{2} \pmod H$, $H = 4$. This distinguishes the Golay pair $(\boldsymbol{a}, \boldsymbol{b}) \in A \times B'$ from any Golay pair $(\boldsymbol{a}', \boldsymbol{b}')$ in $A \times B$ or $A' \times B'$. By design, the latter is such that $\boldsymbol{b}' - \boldsymbol{a}'$ is a sequence taking only two values.

We will now show how these sequences (2) give rise to the 1024 Golay sequences found in [LC 05]. Let $\boldsymbol{a} \in A$ and $\boldsymbol{b} \in B'$, or $\boldsymbol{a} \in A'$ and $\boldsymbol{b} \in B$. Then $\boldsymbol{a}\,;\boldsymbol{b}$ and $\boldsymbol{a}\,;(\boldsymbol{b} + 2^{h-1} \cdot \mathbf{1})$ form a Golay pair (Section 2.1). It can be easily verified that the algebraic normal form of each of these sequences is a cubic polynomial. Hence, both Golay sequences are not covered by the construction in [DJ 99]. By Corollary 2, for each pair $(\boldsymbol{a}, \boldsymbol{b})$ from $A \times B'$ or $A' \times B$ we can construct four quaternary Golay sequences $(\boldsymbol{a}\,;\boldsymbol{b}) + c(\boldsymbol{x}_4 + 2\boldsymbol{x}_3)$ of length 16, $c \in \mathbb{Z}_4$. Thus, we obtain $2 \cdot 64 \cdot 4 = 512$ quaternary Golay sequences of length 16 which are not of the form in [DJ 99, Corollary 5]. All these sequences are distinct, since equality of $(\boldsymbol{a}\,;\boldsymbol{b}) + c(\boldsymbol{x}_4 + 2\boldsymbol{x}_3)$ and $(\boldsymbol{a}'\,;\boldsymbol{b}') + c'(\boldsymbol{x}_4 + 2\boldsymbol{x}_3)$, $c, c' \in \mathbb{Z}_4$, occurs exactly when

$$\begin{aligned} \boldsymbol{a} + c(\boldsymbol{x}_3 + 2\boldsymbol{x}_2) &= \boldsymbol{a}' + c'(\boldsymbol{x}_3 + 2\boldsymbol{x}_2) \\ \boldsymbol{b} + c(\boldsymbol{x}_3 + 2\boldsymbol{x}_2) &= \boldsymbol{b}' + c'(\boldsymbol{x}_3 + 2\boldsymbol{x}_2) \end{aligned}$$

as $(\boldsymbol{x}_3 + 2\boldsymbol{x}_2)\,;(\boldsymbol{x}_3 + 2\boldsymbol{x}_2) = \boldsymbol{x}_4 + 2\boldsymbol{x}_3$. Now notice that the difference of any two distinct elements of $A \cup A'$ is not a non-zero multiple of $\boldsymbol{x}_3 + 2\boldsymbol{x}_2$. The same is true for $B \cup B'$.

The remaining 512 of the new 1024 Golay complementary sequences in [LC 05] can be constructed by interleaving (rather than concatenating) sequences from A with sequences from B', sequences from A' with sequences from B, sequences from $A + (\boldsymbol{x}_3 + 2\boldsymbol{x}_2)$ with sequences from $B' + (\boldsymbol{x}_3 + 2\boldsymbol{x}_2)$, or sequences from $A' + (\boldsymbol{x}_3 + 2\boldsymbol{x}_2)$ with sequences from $B + (\boldsymbol{x}_3 + 2\boldsymbol{x}_2)$. For instance, taking $\boldsymbol{a}$ and $\boldsymbol{b}$ as in (3) and (4), we see

$$\begin{aligned} \mathrm{int}(\boldsymbol{a}, \boldsymbol{b}) &= 2x_1x_3x_4 + 2x_2x_3x_4 + 2x_1x_2 + 2x_2x_3 + x_2x_4 + x_3x_4 \\ &= (0,0,0,1,0,1,2,2,0,0,0,3,2,3,0,2) \end{aligned} \tag{7}$$

which corresponds to entry #3 with $a_0 = 0$, $d_0 = 0$ in [LC 05, Table 1]. The sequence $\mathrm{int}(\boldsymbol{a}, \boldsymbol{b})$ forms a Golay pair with $\mathrm{int}(\boldsymbol{a}, (\boldsymbol{b} + 2^{h-1} \cdot \mathbf{1}))$ and also with $\mathrm{int}((\boldsymbol{b} + 2^{h-1} \cdot \mathbf{1})^*, \boldsymbol{a}^*)$ (Lemma 4) where

$$\begin{aligned} (\boldsymbol{b} + 2^{h-1} \cdot \mathbf{1})^* &= \boldsymbol{b}^* + 2^{h-1} \cdot \mathbf{1} \\ &= 2(x_1x_2 + x_1x_3) + 3x_2 + 3x_3 + 2, \\ \boldsymbol{a}^* &= 2(x_1x_2 + x_2x_3) + 2x_1 + 2x_3. \end{aligned}$$

Similarly to concatenation, we may choose a pair $(\boldsymbol{a}, \boldsymbol{b})$ from $A \times B'$ or $A' \times B$, and construct two Golay sequences $\mathrm{int}(\boldsymbol{a}, \boldsymbol{b}) + c(\boldsymbol{x}_4 + 2\boldsymbol{x}_3)$, $c \in \mathbb{Z}_2$. We can construct two more sequences by choosing $(\boldsymbol{a}, \boldsymbol{b})$ from $(A + \boldsymbol{x}_3 + 2\boldsymbol{x}_2) \times (B' + \boldsymbol{x}_3 + 2\boldsymbol{x}_2)$ or $(A' + \boldsymbol{x}_3 + 2\boldsymbol{x}_2) \times (B + \boldsymbol{x}_3 + 2\boldsymbol{x}_2)$. Again, we obtain $2 \cdot 64 \cdot 2 \cdot 2 = 512$ quaternary Golay sequences of length 16 which are different from the sequences described in [DJ 99, Corollary 5]. As before, all these sequences are distinct. Finally, we observe that the algebraic normal form of sequences obtained by interleaving has cubic terms that are distinct from those in the sequences obtained by concatenation (cf. (7) and (5)). Hence the 1024 sequences described above are all distinct.

The sequences in (2) can be naturally lifted to $\mathbb{Z}_{2^{2+k}}^8$, $k \geq 1$, such that the corresponding sequences of complex modulated values do not change. For instance, the quaternary sequence $\boldsymbol{b}$ in (4) has a representation

$$\boldsymbol{b} = (0,1,1,2,0,3,3,2)$$

which corresponds to $(\xi^0, \xi^1, \xi^1, \xi^2, \xi^0, \xi^3, \xi^3, \xi^2)$, where $\xi = \sqrt{-1}$. As an octary sequence, $\boldsymbol{b}$ can be written as $(0,2,2,4,0,6,6,4)$, which corresponds to

$$\begin{aligned} &(\sqrt{\xi}^0, \sqrt{\xi}^2, \sqrt{\xi}^2, \sqrt{\xi}^4, \sqrt{\xi}^0, \sqrt{\xi}^6, \sqrt{\xi}^6, \sqrt{\xi}^4) \\ &= (\xi^0, \xi^1, \xi^1, \xi^2, \xi^0, \xi^3, \xi^3, \xi^2) \end{aligned}$$

that is, we multiply each entry of the sequence $\boldsymbol{b}$ by 2. In other words, we can write the quaternary sequence $\boldsymbol{b} = 2(x_1x_2 + x_1x_3) + x_2 + x_3$ (4) as an octary sequence $2\boldsymbol{b}$, and generally as $2^k\boldsymbol{b}$ over $\mathbb{Z}_{2^{2+k}}$. Since the complex modulated values of the lifted sequences do not change, the quaternary sequence $\boldsymbol{b}$ has the same autocorrelation function as $2^k\boldsymbol{b}$ over $\mathbb{Z}_{2^{2+k}}$, which in turn has the same autocorrelation function as $2^k\boldsymbol{b} + c \cdot \mathbf{1}$, $c \in \mathbb{Z}_{2^{2+k}}$ (Lemma 1). Hence the lifting of $\boldsymbol{b}$ to $\mathbb{Z}_{2^{2+k}}^8$ belongs to a set $\{2^k\boldsymbol{b} + c \cdot \mathbf{1} \mid \boldsymbol{b} \in B', c \in \mathbb{Z}_{2^{2+k}}\}$ of size $8 \cdot 2^k$ of Golay sequences with the same autocorrelation function. We call this set the lifting of B'. Hence, by lifting the sets A, B, A', and B' to $\mathbb{Z}_{2^{2+k}}^8$, we can construct Golay complementary sequences of length 16 and any characteristic $H = 2^{2+k}$. We remark that the algebraic normal form of these Golay sequences is always a cubic polynomial. Hence, by applying concatenation or interleaving we will be able to produce (new) Golay sequences of any length 2^m, $m \geq 4$.

Corollary 5. *For every $m \geq 4$, $h \geq 2$, there are Golay sequences over $\mathbb{Z}_{2^h}$ of length 2^m which are not of the form in [DJ 99, Corollary 5].*

4 Number of Sequences Spawned By a Pair

One of the drawbacks of the application of Golay sequences to OFDM is the achievable code rate. Until the publication of [LC 05], the number of known Golay sequences of length 2^m over $\mathbb{Z}_{2^h}$ was $(m!/2) \cdot 2^{h(m+1)}$. This results in a code rate of $(w+h(m+1))/(2^m h)$ [DJ 99], where w is such that 2^w is the largest integer power of 2 no greater than $m!/2$. This rate drops quickly as m increases. More Golay sequences give a higher code rate.

In Section 3 we have shown that the new 1024 Golay sequences [LC 05] are constructed by concatenation or interleaving of Golay pairs in $\mathbb{Z}_4^8$. If $(\boldsymbol{a}, \boldsymbol{b})$ is a Golay pair of the form in [DJ 99, Corollary 5], then both $\boldsymbol{a}\,;\boldsymbol{b}$ and $\mathrm{int}(\boldsymbol{a}, \boldsymbol{b})$ are of the form in [DJ 99, Corollary 5]. Hence, to obtain new Golay sequences by concatenation or interleaving of a Golay pair $(\boldsymbol{a}, \boldsymbol{b})$, we need a Golay pair which is not a Golay pair as constructed in [DJ 99, Corollary 5] (but each Golay *sequence* $\boldsymbol{a}$, $\boldsymbol{b}$ may be of that form). If we consider all Golay pairs $(\boldsymbol{a}, \boldsymbol{b})$ of the form in [DJ 99, Corollary 5], then the Golay sequences obtained by this construction are naturally organized in sets $A = \{\boldsymbol{a} + c \cdot \mathbf{1}, \boldsymbol{a}^* + c \cdot \mathbf{1} \mid c \in \mathbb{Z}_{2^h}\}$ and $B = \{\boldsymbol{b} + c \cdot \mathbf{1}, \boldsymbol{b}^* + c \cdot \mathbf{1} \mid c \in \mathbb{Z}_{2^h}\}$. Hence, as shown in Section 3, new Golay sequences may be found if there exist such (distinct) sets A, B, A', and B' for which every $(\boldsymbol{a}, \boldsymbol{b}) \in A \times B$ and every $(\boldsymbol{a}', \boldsymbol{b}') \in A' \times B'$ is a Golay pair as in [DJ 99, Corollary 5], and $C_{\boldsymbol{a}}(u) = C_{\boldsymbol{a}'}(u)$, $0 < u < n$, for some $\boldsymbol{a} \in A$ and $\boldsymbol{a}' \in A'$. Since the existence of such sequences $\boldsymbol{a}$ and $\boldsymbol{a}'$ is not implied by the construction, we speak of a "cross-over" effect of the autocorrelation function of Golay sequences. Understanding how wide-spread this phenomenon is helps find new Golay sequences.

We have checked by computer whether the cross-over effect occurs for Golay sequences that are constructed with the constructions in [Bud 90], [DJ 99]. For $h = 3, 4$ we verified that the only examples of length 8 and characteristic 2^h are those to be expected as liftings of the sets (2). We also considered binary, quaternary, and octary sequences of the form in [DJ 99] for each of the lengths 8, 16, 32, and 64. There are no new examples of this behavior. Also, we found that for every quaternary Golay sequence $\boldsymbol{a}$ of length 16 (including the sequences found in [LC 05]) there are exactly $2 \cdot 4$ quaternary Golay sequences with the same autocorrelation function (including $\boldsymbol{a}$). Hence, in this case the set of Golay sequences with the same autocorrelation function as $\boldsymbol{a}$ is just $A = \{\boldsymbol{a} + c \cdot \mathbf{1}, \boldsymbol{a}^* + c \cdot \mathbf{1} \mid c \in \mathbb{Z}_4\}$, which is of size 8. Thus, the cross-over of autocorrelation functions does not seem to propagate.

So currently (2) is the only starting point for the construction of new Golay sequences of length 2^m over $\mathbb{Z}_{2^h}$, $m \geq 4$, $h \geq 2$. Under the assumption that there is no further cross-over, it is interesting to know how many new quaternary Golay sequences arise from just concatenation and interleaving of the sequences in (2). For length 16 these are exactly the sequences found in [LC 05] (Section 3). Note that these sequences form $8 \cdot 1024$ Golay pairs, since each sequence $\boldsymbol{a}$ belongs to a set A of size 8 of Golay sequences with the same autocorrelation function. By applying concatenation and interleaving to these Golay pairs, we would expect to obtain $16 \cdot 1024$ quaternary Golay sequences of length 32. In fact, computer search shows that only $14 \cdot 1024$ of these sequences are distinct. They form $8 \cdot 14 \cdot 1024 = 112 \cdot 1024$ Golay pairs. By applying concatenation and interleaving to these $112 \cdot 1024$ distinct Golay pairs, we would then expect to obtain $224 \cdot 1024$ new Golay sequences of length 64. However, only $192 \cdot 1024$ of them were distinct. (We then checked by computer whether there is a cross-over of the autocorrelation function within the newly constructed quaternary sequences of length 16 and 32, and whether there is a cross-over between these sequences and sequences constructed as in [DJ 99]. In both cases, we found there is no new example of a cross-over.)

This illustrates one of the difficulties when counting the number of (new) sequences that can be obtained just from concatenation or interleaving. Some Golay sequences may be constructed in

more than one way. This fact is not new. For example, consider the binary Golay sequence

$$\begin{aligned}\boldsymbol{a} &= x_1x_2 + x_2x_3\\ &= (0,0,0,1,0,0,1,0)\end{aligned}$$

of length 8. It can be obtained as concatenation of a Golay pair

$$\begin{aligned}\boldsymbol{a} &= (x_1x_2)\,;(x_1x_2 + x_1)\\ &= (0,0,0,1)\,;(0,0,1,0)\end{aligned}$$

or as interleaving of a (different) Golay pair

$$\begin{aligned}\boldsymbol{a} &= \mathrm{int}((x_1x_2),(x_1x_2 + x_2))\\ &= \mathrm{int}((0,0,0,1),(0,1,0,0)).\end{aligned}$$

Moreover, as Budišin noted in [Bud 90], not all Golay sequences can be constructed using just concatenation and interleaving (cf. Section 2.1). In [Bud 90] and [DJ 99] it was possible to count the number of distinct Golay sequences by different means. If we assume that there is no more cross-over of the autocorrelation function for Golay sequences of length 8 and characteristic 2^h, $h \geq 2$, then we are able to get an accurate count of sequences (of length 16) that can be obtained from concatenation or interleaving of liftings to $\mathbb{Z}_{2^h}^8$ of the sets in (2) (and their cosets by $\boldsymbol{x}_3+2\boldsymbol{x}_2$). In that case we have exactly $2\cdot 2^h\cdot(2^{h+1})^2$ Golay pairs $(\boldsymbol{a},\boldsymbol{b})$ and $(\boldsymbol{b},\boldsymbol{a})$ from $(A+c(\boldsymbol{x}_3+2\boldsymbol{x}_2))\times(B'+c(\boldsymbol{x}_3+2\boldsymbol{x}_2))$, $c\in\mathbb{Z}_{2^h}$, which are not of the form in [DJ 99, Corollary 5]. Note that the set of these Golay pairs contains the Golay pairs $(\boldsymbol{a}',\boldsymbol{b}')$ and $(\boldsymbol{b}',\boldsymbol{a}')$ from $(A'+c(\boldsymbol{x}_3+2\boldsymbol{x}_2))\times(B+c(\boldsymbol{x}_3+2\boldsymbol{x}_2))$, $c\in\mathbb{Z}_{2^h}$, since $A+2^{h-1}(\boldsymbol{x}_3+2\boldsymbol{x}_2)=B$ and $B'+2^{h-1}(\boldsymbol{x}_3+2\boldsymbol{x}_2)=A'$. Therefore, by applying concatenation or interleaving we obtain $2\cdot 2\cdot 2^h\cdot(2^{h+1})^2 = 2^{3h+4}$ new Golay sequences. Similar to the argument in Section 3, they are distinct. However, in general we were not able to count the number of Golay sequences spawned by an arbitrary Golay pair, nor even the number of Golay sequences generated just by concatenation and interleaving of an arbitrary Golay pair.

5 A Question

Since the constructions in [Bud 90] and [DJ 99] give the same set of Golay sequences of length 2^m over $\mathbb{Z}_{2^h}$, we will use the latter to illustrate an interesting property of these sequences. Let $\boldsymbol{a}$ be a Golay sequence of length 2^m over $\mathbb{Z}_{2^h}$ constructed as in [DJ 99]. Let $\boldsymbol{c}$ be a sequence of the same length over $\mathbb{Z}_{2^h}$ associated with the function $c_0+\sum_{k=1}^m c_kx_k$, $c_k\in\mathbb{Z}_{2^h}$. By [DJ 99, Corollary 5], the sequence $\boldsymbol{a}+\boldsymbol{c}$ also is a Golay sequence. So to any Golay sequence $\boldsymbol{a}$ obtainable by [DJ 99] we may add any sequence $\boldsymbol{c}$ constructed from a linear polynomial, and get a Golay sequence $\boldsymbol{a}+\boldsymbol{c}$. This is much more than one would expect using just Corollary 2 and Lemma 3. Recall that Corollary 2 only guarantees Golay sequences if we add $c_1\cdot\boldsymbol{1}$ or $c_2(\boldsymbol{x}_m+2\boldsymbol{x}_{m-1}+\cdots+2^{h-1}\boldsymbol{x}_{m-h+1})$, $c_i\in\mathbb{Z}_{2^h}$. Lemma 3 gives Golay sequences if we add $c_3\boldsymbol{x}_{\pi(1)}$ or $c_4\boldsymbol{x}_{\pi(m)}$, $c_3,c_4\in\mathbb{Z}_{2^h}$, to a Golay sequence of the form in [DJ 99, Corollary 5].

In this sense, the Golay sequences in [LC 05] serve not only as an example of new sequences, but they also give some hint on how much structure to expect from Golay sequences in general. We verified by computer that the sequences given in Corollary 2 are the only sequences that can be added to *any* quaternary Golay sequence of length 16 and still give a Golay sequence. Of course, Lemma 3 and Lemma 4 hold, but they depend on the actual Golay pair $(\boldsymbol{a},\boldsymbol{b})$. This raises the following question: If in general we should not expect the $2^{h(m+1)}$ choices for $\boldsymbol{c}$ arising from linear polynomials, then what makes the Golay sequences in [DJ 99, Corollary 5], which arise as cosets

of certain codewords in the second order Reed-Muller code by the first-order Reed-Muller code, fundamentally different? While one could simply observe that the recursive approach of [Bud 90] to constructing the sequences in [DJ 99, Corollary 5] leads to the introduction of arbitrary linear terms, we would like to know if there is a deeper structural explanation.

6 Conclusion

We have shown that the new Golay complementary sequences found in [LC 05] can be constructed by concatenation or interleaving of appropriate quaternary Golay pairs. These Golay pairs have been noticed before in [DJ 99]. However, it was only on reading [LC 05] that we realized how these examples can be used to construct new Golay sequences.

With the benefit of hindsight we can find other clues as to the existence of these new Golay sequences in prior work. In 1994 Holzmann and Kharaghani [HK 94] used computer search to determine the number of ordered quaternary Golay pairs $(\boldsymbol{a}, \boldsymbol{b})$ of length 8 as $13 \cdot 512 = 6656$, rather than the $12 \cdot 512$ later given by [DJ 99, Corollary 5]. Then in 2002 Craigen, Holzmann and Kharaghani [CHK 02] found by computer search that the corresponding pair count for length 16 is $13 \cdot 8192 = 106,496$ rather than $12 \cdot 8192$, and pointed out the excess of the computer search pair counts for lengths 8 and 16 over those in [DJ 99]. However the papers [HK 94] and [CHK 02] do not analyze the structure of the identified Golay pairs beyond a classification into equivalence classes (in [HK 94]), and crucially they do not count the number of quaternary Golay *sequences*. As a result, [CHK 02] does not distinguish length 8 (for which there are additional quaternary Golay pairs but no additional Golay sequences) from length 16 (for which there are both). Such a distinction could have been a starting point for an earlier construction of the sequences reported in [LC 05] and an explanation for their existence via the cross-over phenomenon.

Li and Chu [LC 05] noted that the sequences they found can be used to construct longer (quaternary) sequences, and that new sequences for larger lengths and alphabets may exist. We have shown how to construct a large class of previously unknown sequences for all lengths 2^m, $m \geq 4$ and all characteristics $H = 2^h$, $h > 2$.

We have shown that these new sequences exist because of a cross-over of the autocorrelation function of certain Golay sequences. We believe this to be an interesting area of study in its own right.

7 Note Added in Proof

Li and Kao [LK 05] have shown independently that the 1024 new Golay sequences of [LC 05] can be constructed by concatenation or interleaving of certain length 8 quaternary Golay pairs, classifying the resulting sequences into sets of 64 in each of 16 third-order cosets of the generalised first-order Reed-Muller code of length 16. However [LK 05] does not explain the existence of these new sequences as depending explicitly on a cross-over property of autocorrelation functions, nor does it construct or count new Golay sequences at lengths other than 16 or over alphabets other than $\mathbb{Z}_4$.

References

[Bud 90] S. Z. Budišin. New Complementary Pairs of Sequences. *Electron. Lett.*, 26 (1990), 881–883.

[CHK 02] R. Craigen, W. Holzmann and H. Kharaghani. Complex Golay sequences: structure and applications. *Discrete Math.*, 252 (2002), 73–89.

[DJ 99] J. A. Davis and J. Jedwab. Peak-to Mean Power Control in OFDM, Golay Complementary Sequences, and Reed-Muller Codes. *IEEE Trans. Inform. Theory*, vol. 45 (1999), 2397–2417.

[Gol 61] M. J. E. Golay. Complementary series, *IRE Trans. Inform. Theory*, vol. IT-7 (1961), 82–87.

[Gol 77] M. J. E. Golay. Sieves for Low Autocorrelation Binary Sequences. *IEEE Trans. Inform. Theory*, vol. IT-23 (1977), 43–51.

[HK 94] W. H. Holzmann and H. Kharaghani. A computer search for complex Golay sequences. *Australasian J. Combinatorics*, 10 (1994), 251–258.

[LC 05] Y. Li and W. B. Chu. More Golay Sequences. *IEEE Trans. Inf. Theory*, vol. 51 (2005), 1141–1145.

[LK 05] Y. Li and Y.-C. Kao. Structures of non-GDJ Golay Sequences. Proc. *IEEE Int. Symp. on Inform. Theory* 2005*, Adelaide*, (2005), 378–381.

[PPT 03] M. G. Parker, K. G. Paterson, and C. Tellambura. Golay Complementary Sequences. In: *Wiley Encyclopedia of Telecommunications*, J. G. Proakis (ed.), John Wiley & Sons, (2003).

[Pat 00] K. G. Paterson. Generalized Reed-Muller Codes and Power Control in OFDM Modulation. *IEEE Trans. Inform. Theory*, vol. 46 (2000), 104–120.

[Pop 91] B. M. Popović. Synthesis of Power Efficient Multitone Signals with Flat Amplitude Spectrum. *IEEE Trans. Comm.*, vol. 39 (1991), 1031–1033.