Shared Autocorrelation Property of Sequences

Corneliu Bodea, Calina Copos, Matt Der, David O'Neal, and James A. Davis

***Abstract*—Due to the low peak-to-mean envelope power ratio (PMEPR) of Golay sequences together with their connection to generalized Reed-Muller codes, many authors have proposed using Golay sequences as codewords in orthogonal frequency-division multiplexing (OFDM). Golay sequences that unexpectedly share the same aperiodic autocorrelation function can be used to construct longer Golay sequences. We study the shared autocorrelation property of general sequences with the ultimate goal of using those results to find other low power sequences. In this paper, we provide several new constructions of families of pairs of sequences with the shared autocorrelation property that enable us to explain nearly all of the binary shared autocorrelation property for sequences of lengths up to 24.**

***Index Terms*—Aperiodic autocorrelation function, Golay sequence, quaternary, shared autocorrelation property.**

I. Introduction

ORTHOGONAL frequency division multiplexing (OFDM) has many advantageous features due to the increased capabilities of digital signal processors, but it suffers from the difficulty of controlling the power of uncoded signals. Many publications ([1]–[3]) have proposed restricting the allowable transmitted sequences to Golay sequences and related objects as these sequences have predictably low peak-to-mean envelope power ratios (PMEPR). Understanding Golay sequences and their generalizations requires the introduction of the aperiodic autocorrelation function of a sequence. Whitehead [4] investigated the properties of the aperiodic autocorrelation function of binary sequences, and he observed that binary sequences of composite lengths occasionally shared aperiodic autocorrelation functions even though those sequences were not reversals, negations, or negative reversals of each other. He demonstrated that certain tensor products of shorter sequences could produce longer sequences with shared autocorrelation functions, and he was able to explain many of the shorter binary sequence shared autocorrelation pairs. More recently, Li and Chu [5] discovered 1024 additional nonstandard quaternary Golay sequences of length 16 that were not explained by Davis and Jedwab's [1] standard construction. Fiedler and Jedwab [6] later showed that all 1024 are either concatenations or interleavings of standard Golay sequences of length 8 whose aperiodic autocorrelation functions are unexpectedly equal. Motivated by these prior studies, Davis and Pohl [7] extended Whitehead's work to quaternary and produced several infinite families of quaternary sequences that had the shared autocorrelation property. These new families were not tensor products of smaller sequences, thus establishing that new techniques will be needed to understand when two sequences will have the same aperiodic autocorrelation. This paper provides further results that explain the shared autocorrelation property of sequences.

The paper is organized as follows. In Section II, we establish the notation that will be used in the rest of the paper and we provide details of the background material. Section III contains our first general result about the shared autocorrelation property, and Section IV contains our other main constructions. The results in Section III and IV enable us to explain almost all of the binary shared autocorrelation property up to length 24 and much of the quaternary up to length 14. Section V establishes some general results about the aperiodic cross correlation of sequences, results that are useful in building sequences with the shared autocorrelation property.

II. Background and Notation

An M-ary sequence $\mathbf{a}$ of length n is the vector $\mathbf{a} = \{a_0, a_1, \ldots, a_{n-1}\}$ where $a_j \in \{\xi^k | k \in \mathbb{Z}, \xi = e^{2\pi\sqrt{-1}/M}\}$ (for the remainder of the paper we will use the notation $\Xi_M = \{\xi^k | k \in \mathbb{Z}, \xi = e^{2\pi\sqrt{-1}/M}\}$ for the set of scalars being used in the sequences). In this context, binary sequences have terms consisting of ± 1 and quaternary sequences have terms consisting of ± 1, $\pm\sqrt{-1}$. The following two definitions provide tools for studying the relationship between two sequences (the cross correlation) and the self-similarity of a sequence (the autocorrelation).

Definition 2.1: Suppose $m \geq n$. The aperiodic cross correlation function of M-ary sequences $\mathbf{a}$ of length n and $\mathbf{b}$ of length m is $C(\mathbf{a}, \mathbf{b}) = \{C(\mathbf{a}, \mathbf{b})(-(m-1)), C(\mathbf{a}, \mathbf{b})(-(m-2)), \ldots, C(\mathbf{a}, \mathbf{b})(n-1)\}$, where $C(\mathbf{a}, \mathbf{b})(u) = \sum_{k=0}^{m+u-1} a_k \overline{b_{k-u}}$ if $-m < u < -(m-n)$; $C(\mathbf{a}, \mathbf{b})(u) = \sum_{k=0}^{n-1} a_k \overline{b_{k-u}}$ if $-(m-n) \leq u \leq 0$; and $C(\mathbf{a}, \mathbf{b})(u) = \sum_{k=0}^{n-u-1} a_{k+u} \overline{b_k}$ if $0 < u < n$ (the definition for $m < n$ is similar).

We have allowed for different length sequences in the definition of the aperiodic cross correlation function since our constructions will allow this possibility.

Definition 2.2: The aperiodic autocorrelation function of the M-ary length n sequence $\mathbf{a} = \{a_0, a_1, \ldots, a_{n-1}\}$ is $A(\mathbf{a}) = \{A(\mathbf{a})(1), A(\mathbf{a})(2), \ldots, A(\mathbf{a})(n-1)\}$, where $A(\mathbf{a})(u) = C(\mathbf{a}, \mathbf{a})(u) = \sum_{k=0}^{n-u-1} a_{k+u} \overline{a_k}$.

We note that the vector $A(\mathbf{a})$ only includes $C(\mathbf{a}, \mathbf{a})(u)$ for $0 < u < n$. We do this for simplicity since $C(\mathbf{a}, \mathbf{a})(0) = n$ and $C(\mathbf{a}, \mathbf{a})(-u) = \overline{C(\mathbf{a}, \mathbf{a})(u)}$.

Manuscript received May 04, 2009; revised June 14, 2010; accepted November 29, 2010. Date of current version May 25, 2011. This work was supported in part by NSF Grant EMSW21-MCTP 0636528.

The authors are with the University of Richmond, Department of Mathematics and Computer Science, VA 23173 USA (e-mail: cornel.bodea@richmond.edu; calinacopos@gmail.com; calina.copos@richmond.edu; matthew.der@gmail.com; matt.der@richmond.edu; david.j.oneal@gmail.com; david.oneal@richmond.edu; jdavis@richmond.edu).

Communicated by M. G. Parker, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2011.2136250

TABLE I

Length	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Binary SAP	0	0	0	0	0	0	0	0	1	0	0	6	0	0
Quaternary SAP	0	0	0	0	0	4	0	12	120	92	0	2034	0	792

Length	15	16	17	18	19	20	21	22	23	24
Binary SAP	14	12	1	42	0	44	67	0	1	422

The associated *generating polynomial* of $\mathbf{a}$ is $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$. If $\mathbf{a}$ is a length n sequence and $\mathbf{b}$ is a length m sequence, then $a(x)\overline{b(x^{-1})} = \sum_{k=-(m-1)}^{n-1} C(\mathbf{a},\mathbf{b})(k)x^k$. Similarly, for a given length n sequence $\mathbf{a}$ we have $a(x)\overline{a(x^{-1})} = n + \sum_{k=1}^{n-1}(A(\mathbf{a})(k)x^k + \overline{A(\mathbf{a})(k)}x^{-k})$. The polynomial viewpoint will be used in Sections III and IV to prove our main results.

Given an M-ary sequence $\mathbf{a}$ of length n and a scalar $c \in \Xi_M$, we define the scalar multiple of $\mathbf{a}$ *by* c as the M-ary sequence $c \cdot \mathbf{a} = \{c \cdot a_0, c \cdot a_1, \ldots, c \cdot a_{n-1}\}$. Similarly, we define the reversal conjugate of $\mathbf{a}$ as the M-ary sequence $\overline{R(\mathbf{a})} = \{\overline{a_{n-1}}, \overline{a_{n-2}}, \ldots, \overline{a_0}\}$. The following lemma shows that all sequences of the form $c \cdot \mathbf{a}$ and $c \cdot \overline{R(\mathbf{a})}$ have the same aperiodic autocorrelation.

Lemma 2.3: Let $\mathbf{a}$ and $\mathbf{b}$ be M-ary sequences of length n. If $\mathbf{b} \in \{c \cdot \mathbf{a} | c \in \Xi_M\} \cup \{d \cdot \overline{R(\mathbf{a})} | d \in \Xi_M\}$, then $A(\mathbf{a}) = A(\mathbf{b})$.

The proof is trivial and is left to the reader. The fact that the converse of Lemma 2.3 is *not* true is what requires a formal definition of what we call the shared autocorrelation property.

Definition 2.4: Let $\mathbf{a}$ and $\mathbf{b}$ be M-ary sequences of length n. The sequences $\mathbf{a}$ and $\mathbf{b}$ possess the shared autocorrelation property (SAP) if $A(\mathbf{a}) = A(\mathbf{b})$ but $\mathbf{b} \notin \{c \cdot \mathbf{a} | c \in \Xi_M\} \cup \{d \cdot \overline{R(\mathbf{a})} | d \in \Xi_M\}$.

This definition is due to Fiedler and Jedwab [6], but the idea goes back to Whitehead [4]. Whitehead ran computer searches for binary sequences up to length 15 and found examples of pairs of sequences (up to the equivalence described in Lemma 2.3) with the SAP at the composite lengths 9, 12, and 15. Table I extends the computer searches for the number of equivalence classes of pairs of binary sequences with the SAP up to length 24, and Table I also includes the results from computer searches for the number of equivalence classes of pairs of quaternary sequences with the SAP up to length 14. We observe that we found binary pairs of sequences with the SAP for lengths 17 and 23, both prime lengths, and these pairs cannot be explained by any known results (including results in this paper).

This paper will explain many of the observed occurrences of SAP in Table I. Whitehead began the explanation with the concept of a tensor product construction, which we now define. The tensor product of two sequences $\mathbf{a} = \{a_0, a_1, \ldots, a_{n-1}\}$ and $\mathbf{b} = \{b_0, b_1, \ldots, b_{m-1}\}$ is $\mathbf{a} \otimes \mathbf{b} = \{a_0b_0, a_1b_0, \ldots, a_{n-1}b_0, a_0b_1, \ldots, a_{n-1}b_1, \ldots, a_0b_{m-1}, a_1b_{m-1}, \ldots, a_{n-1}b_{m-1}\}$. The generating polynomial of $\mathbf{a} \otimes \mathbf{b}$ is $a(x)b(x^n)$. The following theorem from Whitehead shows why tensor products are useful in explaining SAP.

Theorem 2.5: Let $\mathbf{a}$ and $\mathbf{b}$ be sequences of length m such that $A(\mathbf{a}) = A(\mathbf{b})$, and let $\mathbf{c}$ and $\mathbf{d}$ be sequences of length n such that $A(\mathbf{c}) = A(\mathbf{d})$. Then $A(\mathbf{a} \otimes \mathbf{c}) = A(\mathbf{b} \otimes \mathbf{d})$.

Proof:

$$\begin{aligned} a(x)c(x^n)\overline{a(x^{-1})c(x^{-n})} &= a(x)\overline{a(x^{-1})}c(x^n)\overline{c(x^{-n})} \\ &= b(x)\overline{b(x^{-1})}d(x^n)\overline{d(x^{-n})} \\ &= b(x)d(x^n)\overline{b(x^{-1})d(x^{-n})} \end{aligned}$$

□

Example 2.6: We demonstrate that the single occurrence of the shared autocorrelation property in binary sequences of length 9 can be explained by tensor products. The sequences $\mathbf{e} = \{1,1,-1,1,1,-1,-1,-1,1\}$ and $\mathbf{f} = \{1,1,-1,-1,-1,1,-1,-1,1\}$ exhibit the SAP since $A(\mathbf{e}) = A(\mathbf{f})$ but $\mathbf{f} \notin \{c \cdot \mathbf{e} | c \in \Xi_2\} \cup \{d \cdot \overline{R(\mathbf{e})} | d \in \Xi_2\}$. Theorem 2.5 explains this instance of SAP by letting $\mathbf{a} = \mathbf{b} = \mathbf{c} = \{1,1,-1\}$ and $\mathbf{d} = \{1,-1,-1\}$, leading to the construction of $\mathbf{e} = \mathbf{a} \otimes \mathbf{c}$ and $\mathbf{f} = \mathbf{b} \otimes \mathbf{d}$. Since $A(\mathbf{a}) = A(\mathbf{c})$ and $A(\mathbf{b}) = A(\mathbf{d})$, we have $A(\mathbf{e}) = A(\mathbf{f})$. In addition to the lone instance of binary length 9 SAP, Theorem 2.5 explain 36 of the 120 instances of the SAP for quaternary length 9 sequences in Table I.

III. Concatenation of Sequences

If $\mathbf{a} = \{a_0, a_1, \ldots, a_{\ell-1}\}$ and $\mathbf{b} = \{b_0, b_1, \ldots, b_{m-1}\}$, then the concatenation of $\mathbf{a}$ and $\mathbf{b}$ is defined as $\{\mathbf{a}|\mathbf{b}\} = \{a_0, a_1, \ldots, a_{\ell-1}, b_0, b_1, \ldots, b_{m-1}\}$. The following binary length 12 example uses concatenation to construct sequences with the SAP.

Example 3.1: Let $\mathbf{a} = \{1,1,1,1,-1,-1,1,-1,1,-1,-1,1\}$ and $\mathbf{b} = \{-1,-1,1,1,1,1,-1,1,1,-1,1,-1\}$. We notice that $\mathbf{a}$ and $\mathbf{b}$ have the SAP although $\mathbf{a}$ and $\mathbf{b}$ do not follow the construction described in Theorem 2.5. The key observation is that $\mathbf{a}$ is formed by concatenating the two sequences $\mathbf{a}_1 = \{1,1,1,1,-1,-1\}$ and $\mathbf{a}_2 = \{1,-1,1,-1,-1,1\}$, and $\mathbf{b}$ is formed by concatenating the two sequences $\mathbf{b}_1 = \{-1,-1,1,1,1,1\}$ and $\mathbf{b}_2 = \{-1,1,1,-1,1,-1\}$. We see that $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{b}_1$, and $\mathbf{b}_2$ have the following properties:

1) $A(\mathbf{a}_1) = \{3,0,-1,-2,-1\} = A(\mathbf{b}_1)$ (by Lemma 2.3 since $\mathbf{b}_1 = \overline{R(a_1)}$);
2) $A(\mathbf{a}_2) = \{-3,0,1,-2,1\} = A(\mathbf{b}_2)$ (by Lemma 2.3 since $\mathbf{b}_2 = -\overline{R(a_2)}$);
3) $C(\mathbf{a}_2,\mathbf{a}_1) = \{-1,0,1,0,3,0,-3,0,-1,0,1\} = C(\mathbf{b}_2,\mathbf{b}_1)$.

The following theorem generalizes Example 3.1.

Theorem 3.2: Let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$ and $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ be M-ary sequences. If:

1) $A(\mathbf{a}_k) = A(\mathbf{b}_k)$, $1 \le k \le n$;
2) $C(\mathbf{a}_k, \mathbf{a}_j) = C(\mathbf{b}_k, \mathbf{b}_j)$, $j \ne k$.

Then $A(\{\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_n\}) = A(\{\mathbf{b}_1|\mathbf{b}_2|\dots|\mathbf{b}_n\})$.

Proof: Let $\ell_1, \ell_2, \dots \ell_n$ be the lengths of the sequences $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n$ respectively (and, hence, also the lengths of $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n$, respectively). The two conditions imply $a_k(x)\overline{a_j(x^{-1})} = b_k(x)\overline{b_j(x^{-1})}$, $1 \le j, k \le n$. The polynomial for the sequence $\mathbf{a} = \{\mathbf{a}_1|\mathbf{a}_2|\cdots|\mathbf{a}_n\}$ is $a(x) = a_1(x) + x^{\ell_1}a_2(x) + x^{\ell_1+\ell_2}\, a_3(x) + \cdots + x^{\ell_1+\cdots+\ell_{n-1}}a_n(x)$, and similarly we get the polynomial $b(x) = b_1(x) + x^{\ell_1}b_2(x) + x^{\ell_1+\ell_2}b_3(x) + \cdots + x^{\ell_1+\cdots+\ell_{n-1}}b_n(x)$ for the sequence $\mathbf{b} = \{\mathbf{b}_1|\mathbf{b}_2|\cdots|\mathbf{b}_n\}$. A simple calculation yields the result. □

Theorem 3.2 provides a recipe for constructing sequences with the SAP if we can find shorter sequences with the aperiodic and cross-correlation properties. Section V will address the issue of determining how to create a collection of sequences that has all the cross correlation properties required.

IV. Reversal Concatenation

As in the previous section, we list an example to illustrate our next (and most general) construction technique.

Example 4.1: Let $\mathbf{a} = \{1,1,1,1,-1,-1,1,1\}$ and $\mathbf{b} = \{1,-1,1,-1,-1,1,1,-1\}$. We observe that $C(\mathbf{a},\mathbf{b}) = -C(\mathbf{b},\mathbf{a})$. Using $\mathbf{a}$ and $\mathbf{b}$ as subsequences, we build the sequences $\mathbf{S} = \{\mathbf{a}|\mathbf{b}|-\mathbf{b}\}$ and $\mathbf{S}' = \{\mathbf{b}|-\mathbf{b}|\mathbf{a}\}$. We can easily verify that $\mathbf{S}$ and $\mathbf{S}'$ have the SAP.

Theorem 8 of Whitehead [4] includes Example 4.1. The theorem below generalizes Whitehead's result by allowing (i) different length sequences $\mathbf{a}$ and $\mathbf{b}$; (ii) larger alphabets than binary; and (iii) different scalar multiples than -1 for the cross-correlation property. The sequences $\mathbf{S}$ and $\mathbf{S}'$ from Example 4.1 cannot be constructed via Theorem 2.5 or Theorem 3.2, so Theorem 4.2 is a new tool for constructing sequences with the SAP. Given M-ary sequences $\mathbf{a}$ of length ℓ and $\mathbf{b}$ of length m satisfying $C(\mathbf{a},\mathbf{b})(u) = c \cdot C(\mathbf{b},\mathbf{a})(m-\ell+u)$, $-(m-1) \le u \le (\ell-1)$, $c \in \Xi_M$, define two sequences $\mathbf{S}$ and $\mathbf{S}'$ as follows: $\mathbf{S} = \{\mathbf{S}_1|\mathbf{S}_2|\cdots|\mathbf{S}_n\}$ where each $\mathbf{S}_i$ is the sequence $d_i \cdot \mathbf{a}$ or $d_i \cdot \mathbf{b}$ for $d_i \in \Xi_M$. The partner sequence is $\mathbf{S}' = \{\mathbf{S}'_n|\mathbf{S}'_{n-1}|\cdots|\mathbf{S}'_1\}$, where $\mathbf{S}'_i = \overline{d_i} \cdot \mathbf{a}$ if $\mathbf{S}_i = d_i \cdot \mathbf{a}$ and $\mathbf{S}'_i = c \cdot \overline{d_i} \cdot \mathbf{b}$ if $\mathbf{S}_i = d_i \cdot \mathbf{b}$.

Theorem 4.2: Let $\mathbf{a}$ be a length ℓ M-ary sequence and $\mathbf{b}$ be a length m M-ary sequence, and suppose that $C(\mathbf{a},\mathbf{b})(u) = c \cdot C(\mathbf{b},\mathbf{a})(m-\ell+u)$, $-(m-1) \le u \le (\ell-1)$, $c \in \Xi_M$. Then the sequences $\mathbf{S}$ and $\mathbf{S}'$ defined above satisfy $A(\mathbf{S}) = A(\mathbf{S}')$.

Proof: Let $a(x)$ be the generating polynomial for the sequence $\mathbf{a}$ and $b(x)$ for the sequence $\mathbf{b}$, and suppose $C(\mathbf{a},\mathbf{b})(u) = c \cdot C(\mathbf{b},\mathbf{a})(m-\ell+u)$, $c \in \Xi_M$, $-(m-1) \le u \le (\ell-1)$. The generating polynomial of $\mathbf{S}$ can be written as

$$s(x) = a(x)t(x) + b(x)u(x).$$

Similarly, if the total length of the sequence $\mathbf{S}$ is n then the partner sequence $\mathbf{S}'$ has polynomial

$$s'(x) = a(x)\overline{t(x^{-1})}x^{n-\ell} + c \cdot b(x)\overline{u(x^{-1})}x^{n-m}.$$

We know that $C(\mathbf{a},\mathbf{b})(u) = c \cdot C(\mathbf{b},\mathbf{a})(m-\ell+u)$ implies $a(x)\overline{b(x^{-1})} = c \cdot b(x)\overline{a(x^{-1})}x^{\ell-m}$. The polynomial computations for the aperiodic autocorrelation functions of $\mathbf{S}$ and $\mathbf{S}'$ go as follows:

$$\begin{aligned}
&s(x)\overline{s(x^{-1})}\\
&= (a(x)t(x) + b(x)u(x))(\overline{a(x^{-1})t(x^{-1})} + \overline{b(x^{-1})u(x^{-1})})\\
&= a(x)t(x)\overline{a(x^{-1})t(x^{-1})}\\
&\quad + a(x)t(x)\overline{b(x^{-1})u(x^{-1})}\\
&\quad + b(x)u(x)\overline{a(x^{-1})t(x^{-1})}\\
&\quad + b(x)u(x)\overline{b(x^{-1})u(x^{-1})}\\
&= a(x)t(x)\overline{a(x^{-1})t(x^{-1})}\\
&\quad + c \cdot b(x)t(x)\overline{a(x^{-1})u(x^{-1})}x^{\ell-m}\\
&\quad + \overline{c} \cdot a(x)u(x)\overline{b(x^{-1})t(x^{-1})}x^{m-\ell}\\
&\quad + b(x)u(x)\overline{b(x^{-1})u(x^{-1})}\\
&= (a(x)\overline{t(x^{-1})}x^{n-\ell} + c \cdot b(x)\overline{u(x^{-1})}x^{n-m})(\overline{a(x^{-1})}t(x)x^{\ell-n}\\
&\quad + \overline{c} \cdot \overline{b(x^{-1})}u(x)x^{m-n})\\
&= s'(x)\overline{s'(x^{-1})}
\end{aligned}$$

Thus, the sequences $\mathbf{S}$ and $\mathbf{S}'$ have the same aperiodic autocorrelation. □

A more general version of Theorem 4.2 is the following, which we only state. For $j = 1, 2, \dots, n$, suppose we have M-ary sequences $\mathbf{a}_j$ (not necessarily distinct) of length ℓ_j satisfying $C(\mathbf{a}_i,\mathbf{a}_j)(u) = c_{i,j} \cdot C(\mathbf{a}_j,\mathbf{a}_i)(\ell_j - \ell_i + u)$, $-(\ell_j - 1) \le u \le (\ell_i - 1)$, $c_{i,j} \in \Xi_M$. Define two sequences $\mathbf{S}$ and $\mathbf{S}'$ similar to the previous result: $\mathbf{S} = \{\mathbf{S}_1|\mathbf{S}_2|\cdots|\mathbf{S}_n\}$ where each $\mathbf{S}_i$ is the sequence $d_i \cdot \mathbf{a}_i$ for $d_i \in \Xi_M$, $1 \le i \le n$. The partner sequence is $\mathbf{S}' = \{\mathbf{S}'_n|\mathbf{S}'_{n-1}|\cdots|\mathbf{S}'_1\}$, where $\mathbf{S}'_i = c_{i,j} \cdot \overline{d_i} \cdot \mathbf{a}_j$ for some j.

Theorem 4.3: Suppose the M-ary sequences $\mathbf{a}_j$ satisfy $C(\mathbf{a}_i,\mathbf{a}_j)(u) = c_{i,j} \cdot C(\mathbf{a}_j,\mathbf{a}_i)(\ell_j - \ell_i + u)$, $1 \le j \le n$, $c_j \in \Xi_M$, $-(\ell_j - 1) \le u \le (\ell_i - 1)$. Then the sequences $\mathbf{S}$ and $\mathbf{S}'$ defined above satisfy $A(\mathbf{S}) = A(\mathbf{S}')$.

There still remain instances of SAP that Theorems 4.2 and 4.3 do not explain, but we can use these theorems in a new construction technique that ultimately relies upon Theorem 3.2. Recall that Theorem 3.2 concatenates subsequences with two key properties to form a pair of sequences $\{\mathbf{a}_1|\mathbf{a}_2|\dots|\mathbf{a}_n\}$ and $\{\mathbf{b}_1|\mathbf{b}_2|\dots|\mathbf{b}_n\}$ that have identical autocorrelations. Our next technique builds these sequences using Theorems 4.2 and 4.3 to satisfy $A(\mathbf{a}_k) = A(\mathbf{b}_k)$ and in such a way that guarantees $C(\mathbf{a}_k,\mathbf{a}_j) = C(\mathbf{b}_k,\mathbf{b}_j)$, $j \ne k$. As in the previous sections, we start with an example to illustrate the construction technique.

Example 4.4: Let $\mathbf{b}_1 = \{1,1,1\}$ and $\mathbf{b}_2 = \{-1,1,1\}$, and let $\mathbf{a}_1 = \{1,1\}$ and $\mathbf{a}_2 = \{1,-1\}$. Observe that $C(\mathbf{a}_1,\mathbf{a}_2) = -C(\mathbf{a}_2,\mathbf{a}_1)$. Now, build the sequences

$$\mathbf{T}_1 = \{\mathbf{a}_1 \otimes \mathbf{b}_1|\mathbf{a}_2 \otimes \mathbf{b}_1\} \quad \mathbf{T}_2 = \{\mathbf{a}_1 \otimes \mathbf{b}_2|\mathbf{a}_2 \otimes \mathbf{b}_2\}$$
$$\mathbf{T}'_1 = \{-\mathbf{a}_2 \otimes \mathbf{b}_1|\mathbf{a}_1 \otimes \mathbf{b}_1\} \quad \mathbf{T}'_2 = \{-\mathbf{a}_2 \otimes \mathbf{b}_2|\mathbf{a}_1 \otimes \mathbf{b}_2\}.$$

We can verify that $A(\{\mathbf{T}_1|\mathbf{T}_2\}) = A(\{\mathbf{T}'_1|\mathbf{T}'_2\})$. This result is straightforward since:

1) $A(\mathbf{T}_i) = A(\mathbf{T}'_i)$, $1 \le i \le 2$ by Theorem 4.2;
2) $C(\mathbf{T}_2,\mathbf{T}_1) = C(\mathbf{T}'_2,\mathbf{T}'_1)$.

Hence, Theorem 3.2 guarantees the autocorrelation equality.

TABLE II

Pair no.	Sequence 1	Sequence 2
1	++−−++−+++++−−+−+−+−−++−	++−−++−−−−−+−+−+−−+−−++−
2	++++++−++−−+−+−+++−−−+++	++++−−−−++−+−+++−+++−+++
3	+−+++−+++−+++++−−+−++−+−	+−++−++−++++++−−+++−+−+−
4	+−+++−++−−+−−+++−+−++−+−	+−++−++−−++−−+−++++−+−+−
5	++++++++−+−++−−++++++−−−	++++++−+−−+++++++−+++−−−
6	++−−+++−−−−−+++−+−+−+−−+	++−−−−++++−+−+−+−−−++−−+
7	+−++−+++−+−+−++−−−−+−+−+	+−++−+−+−−++−−−−−+−+−+−+
8	++++−−+−++++−−−+−+−+−++−	++−−−−++++−+−+−+++−++−+−
9	++++++−+−−−−++−−++−−−+++	++++−−−−−+−−+++−−+++−+++
10	++++−−−+−−−−++−+−+−++−−+	++−−++−−−−−+−+−++++−−+−+
11	++−−+++++++−−+−+−−−++−−+	++−−+++−−−−−−−+−+−−++−−+
12	++++−−+−++++++−+−++−−++−	++−−+++++++−−+−+++−++−+−
13	++++−−−+−−−−−−−+−++−+−−+	++−−−−−−−−+−−+−++++−−+−+
14	++−−++−++++++++−+−−+−++−	++−−−−−−−−+−−+−+−−+−−++−

TABLE III

Pair no.	Sequence 1	Sequence 2
1	$+1,+i,-1,+1,-i,-i,+1,-1,+1$	$+1,+i,-1,+i,-1,+1,+1,-1,+1$
2	$+1,+1,+1,-1,-1,+i,-1,+i,+1$	$+1,+1,+1,-i,+i,-1,-1,+i,+1$
3	$+1,+1,+1,+i,+1,+1,-1,-1,+1$	$+1,+i,-1,+i,+i,-1,-1,+i,+1$
4	$+1,+1,-1,-1,+1,+i,+1,-1,+1$	$+1,-i,-1,-i,+i,+1,-1,-i,+1$
5	$+1,+1,-1,-1,+1,+i,+i,-i,+i$	$+1,+i,-1,+1,+1,+i,-i,-1,+i$
6	$+1,+1,+1,+i,-i,-1,-i,+i,-i$	$+1,+i,-1,+i,-i,+1,-i,+1,-i$
7	$+1,+1,+1,-1,+i,+i,-i,-i,+i$	$+1,-i,-1,-1,+1,-i,-i,,+1,+i$
8	$+1,+1,+1,+i,+1,+1,+i,-i,+i$	$+1,+i,-1,+i,+i,-1,+i,-1,+i$
9	$+1,+1,+1,-1,-i,-i,+1,-1,+1$	$+1,+i,-1,-1,+1,+i,+1,+i,+1$
10	$+1,+1,+1,+i,-i,+1,+1,-1,+1$	$+1,+i,-1,+1,+1,+i,+1,+i,+1$

To get the generalization of this example, suppose we have the sequences $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ of equal length k and the sequences $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m$ of equal length ℓ with $C(\mathbf{a}_1, \mathbf{a}_j)(u) = c_j \cdot C(\mathbf{a}_j, \mathbf{a}_1)(u)$, $2 \leq j \leq m$, $c_j \in \Xi_M$. For $1 \leq i \leq n$, define $\mathbf{T}_i = \{d_1 \cdot \mathbf{x}_1 \otimes \mathbf{b}_i | d_2 \cdot \mathbf{x}_2 \otimes \mathbf{b}_i | \cdots | d_p \cdot \mathbf{x}_p \otimes \mathbf{b}_i\}$, where $\mathbf{x}_j \in \{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m\}$, $1 \leq j \leq p$ and $d_j \in \Xi_M$, $1 \leq j \leq p$. Similarly, define $\mathbf{T}'_i = \{\overline{d_p} \cdot \mathbf{y}_p \otimes \mathbf{b}_i | \overline{d_{p-1}} \cdot \mathbf{y}_{p-1} \otimes \mathbf{b}_i | \cdots | \overline{d_1} \cdot \mathbf{y}_1 \otimes \mathbf{b}_i\}$ for $\mathbf{y}_j = c_j \cdot \mathbf{x}_j$. The following corollary shows that $\mathbf{T} = \{\mathbf{T}_1 | \mathbf{T}_2 | \cdots | \mathbf{T}_n\}$ and $\mathbf{T}' = \{\mathbf{T}'_1 | \mathbf{T}'_2 | \cdots | \mathbf{T}'_n\}$ have the same aperiodic autocorrelation function.

Corollary 4.5: For the M-ary sequences $\mathbf{a}_i$, $1 \leq i \leq m$ of length ℓ and $\mathbf{b}_j$, $1 \leq j \leq n$ of length k, if $C(\mathbf{a}_1, \mathbf{a}_j)(u) = c_j \cdot C(\mathbf{a}_j, \mathbf{a}_1)(u)$ for $1 \leq j \leq m, c_j \in \Xi_M$, $-(\ell-1) \leq u \leq (\ell-1)$, then $A(\mathbf{T}) = A(\mathbf{T}')$ for $\mathbf{T}$ and $\mathbf{T}'$ defined above.

The proof uses Theorems 3.2 and 4.2, and is a polynomial argument similar to the proofs of those theorems and, hence, is left to the reader.

To illustrate the power of the theorems presented in this paper, we refer the reader back to Table I. According to the table, there are 422 instances of SAP for binary sequences of length 24. Theorems 2.5, 3.2, 4.2, 4.3, and Corollary 4.5 enable us to explain 408 of these instances. Table II contains representatives for the 14 binary pairs of length 24 that are SAP pairs but can't be explained by results in this paper (note that we use the notation $++-+$ to represent the sequence $\{1, 1, -1, 1\}$). Similarly, 64 more of the instances of the SAP for quaternary sequences of length 9 are explained by Theorems 4.2 and 4.3. When combined with the 36 instances of the SAP for quaternary sequences of length 9 already explained in Section II, this leaves 20 instances of the length 9 quaternary SAP unexplained by results in this paper. Using the observation that $A(\overline{\mathbf{a}}) = A(\overline{\mathbf{b}})$ whenever $A(\mathbf{a}) = A(\mathbf{b})$, Table III contains representatives for 10 of the SAP pairs that remain unexplained (the other 10 are simply conjugates of the pairs in the table).

V. Sequences With the Cross-Correlation Property

Theorems 3.2 and 4.2 and Corollary 4.5 require that we find sequences $\mathbf{a}_1$ and $\mathbf{a}_2$ satisfying $C(\mathbf{a}_1, \mathbf{a}_2)(u) = c \cdot C(\mathbf{a}_2, \mathbf{a}_1)(u)$ for some $c \in \Xi_M$. The following example illustrates sequences that have this cross correlation property, and we use it to set up our final theoretical result.

Example 5.1: Let $\mathbf{b}_1 = \{1, i, -1, 1, i, 1\}$ and $\mathbf{b}_2 = \{i, i, 1, 1, -1, -1\}$ be quaternary sequences of length 6. We use those to construct $\mathbf{a}_1 = \{\mathbf{b}_1 | i \cdot \overline{R(\mathbf{b}_1)}\} = \{1, i, -1, 1, i, 1, i, 1, i, -i, 1, i\}$ and $\mathbf{a}_2 = \{\mathbf{b}_2 | -\overline{R(\mathbf{b}_2)}\} = \{i, i, 1, 1, -1, -1, 1, 1, -1, -1, i, i\}$. It is easy to verify that $C(\mathbf{a}_1, \mathbf{a}_2)(u) = -i \cdot C(\mathbf{a}_2, \mathbf{a}_1)(u)$, $-11 \leq u \leq 11$. Similarly, if we define $\mathbf{a}_3 = \{\mathbf{b}_1 | i | (i)^2 \cdot \overline{R(\mathbf{b}_1)}\} = \{1, i, -1, 1, i, 1, i, -1, i, -1, 1, i, -1\}$ and $\mathbf{a}_4 = \{\mathbf{b}_2 | -1 | (-1)^2 \cdot \overline{R(\mathbf{b}_2)}\} = \{i, i, 1, 1, -1, -1, -1, -1, -1, 1, 1, -i, -i\}$, we can verify that $C(\mathbf{a}_3, \mathbf{a}_4)(u) = (i)^2 (-1)^2 C(\mathbf{a}_4, \mathbf{a}_3)(u)$, $-12 \leq u \leq 12$.

The first construction in Example 5.1 can be generalized to generate even-length pairs of sequences with the cross correlation property as follows.

Theorem 5.2: Suppose $\mathbf{b}_1$ and $\mathbf{b}_2$ are length n M-ary sequences. Then the sequences $\mathbf{a}_1 = (\mathbf{b}_1 | c_1 \cdot \overline{R(\mathbf{b}_1)})$ and $\mathbf{a}_2 = (\mathbf{b}_2 | c_2 \cdot \overline{R(\mathbf{b}_2)})$ satisfy $C(\mathbf{a}_1, \mathbf{a}_2)(u) = c_1 \cdot \overline{c_2} \cdot C(\mathbf{a}_2, \mathbf{a}_1)(u)$, $-(2n-1) \leq u \leq (2n-1)$, where $c_1, c_2 \in \Xi_M$.

Proof: The polynomial for $\mathbf{a}_1$ is $a_1(x) = b_1(x) + x^n c_1 \cdot \overline{b_1(x^{-1})}$, and the polynomial for $\mathbf{a}_2$ is $a_2(x) = b_2(x) + x^n c_2 \cdot$

$\overline{b_2(x^{-1})}$. Using these to check the cross correlation yields the following polynomial equation:

$$\begin{aligned} a_1(x)\overline{a_2(x^{-1})} &= \left[b_1(x) + x^n c_1 \cdot \overline{b_1(x^{-1})}\right] \\ &\quad \times \left[b_2(x^{-1}) + x^{-n}\overline{c_2} \cdot b_2(x)\right] \\ &= b_1(x)\overline{b_2(x^{-1})} + \overline{c_2} \cdot x^{-n} b_1(x) b_2(x^{-1}) \\ &\quad + c_1 \cdot x^n \overline{b_1(x^{-1}) b_2(x^{-1})} \\ &\quad + c_1 \cdot \overline{c_2} \cdot b_2(x)\overline{b_1(x^{-1})} \\ &= c_1 \cdot \overline{c_2} \cdot a_2(x)\overline{a_1(x^{-1})}. \end{aligned}$$

□

The following theorem, based on the second construction in Example 5.1, provides a construction for a pair of odd-length sequences satisfying $C(\mathbf{a}_1, \mathbf{a}_2)(u) = (c_1)^2(c_2)^2 C(\mathbf{a}_2, \mathbf{a}_1)(u)$, $-2n \leq u \leq 2n$.

Theorem 5.3: Suppose $\mathbf{b}_1$ and $\mathbf{b}_2$ are length n M-ary sequences. Then the sequences $\mathbf{a}_1 = (\mathbf{b}_1 | c_1 | (c_1)^2 \cdot \overline{R(\mathbf{b}_1)})$ and $\mathbf{a}_2 = (\mathbf{b}_2 | c_2 | (c_2)^2 \cdot \overline{R(\mathbf{b}_2)})$ satisfy $C(\mathbf{a}_1, \mathbf{a}_2)(u) = (c_1)^2(c_2)^2 C(\mathbf{a}_2, \mathbf{a}_1)(u)$, $-2n \leq u \leq 2n$, where $c_1, c_2 \in \Xi_M$.

The proof is similar to Theorem 5.2 and is left to the reader. These two theorems can be used to identify pairs of sequences satisfying a cross-correlation property that enables them to be used in Theorems 3.2 and 4.2 as well as Corollary 4.5.

REFERENCES

[1] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2397–2417, Jul. 1999.

[2] K. G. Paterson, "Generalized Reed–Muller codes and power control in OFDM modulation," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 104–120, Jan. 2000.

[3] K. Schmidt, "On cosets of the generalized first-order Reed-Muller code with low PMEPR," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3220–3232, Jul. 2006.

[4] E. G. Whitehead, "Autocorrelation of $(+1, -1)$ sequences," in *Proc. Int. Conf. Combinatorial Mathematics*, 1978, vol. 686, Lecture Notes in Mathematics, pp. 329–336.

[5] Y. Li and W. B. Chu, "More Golay sequences," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 1141–1145, Mar. 2006.

[6] F. Fiedler and J. Jedwab, "How do more Golay sequences arise?," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 4261–4266, Sep. 2006.

[7] J. A. Davis and M. Pohl, "Crossover of aperiodic autocorrelation function quaternary sequences," *J. Combin. Inf. Syst. Sci.*, vol. 34, no. 1–4, pp. 127–134, 2009.

Corneliu Bodea, biography not available at the time of publication.

Calina Copos, biography not available at the time of publication.

Matt Der, biography not available at the time of publication.

David O'Neal, biography not available at the time of publication.

James A. Davis, biography not available at the time of publication.