[29] J. K. Wolf, "Source coding for a noiseless broadcast channel," in *Proc. Conf. Information Science and Syst.ems*, Princeton, NJ, Mar. 2004.

[30] A. Kaspi, "Rate-distortion when side-information may be present at the decoder," *IEEE Trans. Inf. Theory*, vol. 40, no. 6, pp. 2031–2034, Nov. 1994.

[31] Y. Frank-Dayan and R. Zamir, "Dithered lattice-based quantizers for multiple descriptions," *IEEE Trans. Inf. Theory*, vol. 48, no. 1, pp. 192–204, Jan. 2002.

[32] C. Tian and S. S. Hemami, "Universal multiple description scalar quantizer: Analysis and design," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2089–2102, Sep. 2004.

[33] V. A. Vaishampayan, N. J. A. Sloane, and S. D. Servetto, "Multiple-description vector quantization with lattice codebooks: design and analysis," *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 1718–1734, Jul. 2001.

[34] R. Venkataramani, G. Kramer, and V. K. Goyal, "Multiple description coding with many channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 9, pp. 2106–2114, Sep. 2003.

Construction of Even Length Binary Sequences With Asymptotic Merit Factor 6

Tingyao Xiong and Jonathan I. Hall*, Member, IEEE*

***Abstract*—Starting with the family of Legendre sequences of length p, Parker constructed a new family of binary sequences of length $2p$ with good negacyclic correlation properties. Computer calculations indicated that the asymptotic merit factor of his family is 6. In this correspondence a simple version of Parker's construction is given and further applied to Jacobi and modified Jacobi sequences. It is then proven that each of the families constructed, including Parker's, has asymptotic merit factor 6.**

***Index Terms*—Aperiodic correlation, Jacobi sequence, Legendre sequence, merit factor.**

I. Introduction

A *binary sequence* x of *length* n is a sequence $x_j,\ 0 \leq j \leq N-1$, with values $+1$ or -1. The *aperiodic autocorrelation* function of x is defined to be

$$A_x(i) = \sum_{j=0}^{N-i-1} x_j x_{j+i}, \quad i = 1, \ldots, N-1 \tag{1}$$

and the *merit factor* of the sequence x, introduced by Golay [1], is defined as

$$F_x = \frac{N^2}{2\sum_{i=1}^{N-1} A_x^2(i)}. \tag{2}$$

Let X_n be the set of all binary sequences of length n. We define M_n to be the optimal value of the merit factor for binary sequences of length n

$$M_n := \max_{x \in X_n}(F_x).$$

One of the principal problems in the study of the merit factor is to determine the asymptotic behavior of M_n. Specifically [2] we are interested in

$$M = \limsup_{n \to \infty}(M_n).$$

Høholdt, J. M. Jensen, and H. E. Jensen [3], [4] proved that the asymptotic merit factors for Legendre sequences and twin-prime sequences under their optimal cyclic shifts are 6. Therefore $M \geq 6$. This is the best lower bound on M that has been proven, although computer calculations [5]–[7] strongly suggest that at least $M > 6.34$ (and in Section VI below we exhibit calculations supporting $M > 6.17$), so it seems unlikely that the value of M is 6. (Indeed it remains possible that $M = +\infty$ [2].)

Starting from Legendre sequences of length p, Parker [8] constructed a new family of binary sequences of length $2p$ and did computer calculations suggesting that the constructed sequences have merit factor 6. The present correspondence was motivated by an effort to understand Parker's sequences.

Section II gives a general doubling construction for binary sequences of length $2N$ based upon a given binary sequence of length N, and some fundamental properties of this construction are given. In Section III, Legendre sequences are used as base sequences, and the asymptotic merit factor of the resulting family is proven to be 6. Section IV explains Parker's construction and how it is included in the present doubling construction. In Section V the doubling construction is applied using certain Jacobi and modified Jacobi sequences as the base sequences. Again it is proven that the asymptotic merit factor of associated families is 6. In Section VI, sequences are constructed through the concatenation of a segment of its negative to any of Parker's (or the present related) sequences. Computer calculations suggest a family can be constructed in this way to have merit factor greater than 6.17. Jedwab [2] reports that Parker has made similar calculations.

II. Construction

Definition 2.1: Given two binary sequences $\alpha = \{\alpha_0, \alpha_1, \ldots, \alpha_{N-1}\}$ and $\epsilon = \{\epsilon_0, \epsilon_1, \ldots, \epsilon_{N-1}\}$, we define the product sequence $b = \alpha * \epsilon$ by $b_i = \alpha_i \epsilon_i$, for $i = 0, 1, \ldots, N-1$.

Definition 2.2: A binary sequence $\alpha = \{\alpha_0, \alpha_1, \ldots, \alpha_{N-1}\}$ of odd length is *symmetric* if $\alpha_i = \alpha_{N-i}$, for $1 \leq i \leq N-1$, and *antisymmetric* if $\alpha_i = -\alpha_{N-i}$, for $1 \leq i \leq N-1$.

Given a binary sequence $\alpha = \{\alpha_0, \alpha_1, \ldots, \alpha_{N-1}\}$, we write $-\alpha$ for $\{-\alpha_0, -\alpha_1, \ldots, -\alpha_{N-1}\}$.

Definition 2.3: For $\delta = 0, 1$, let the four sequences $\pm\epsilon^{(\delta)}$ be given by

$$\epsilon_j^{(\delta)} = (-1)^{\binom{j+\delta}{2}} \tag{3}$$

For instance

$$-\epsilon^{(0)} = -1, -1, +1, +1, \ldots, -1, -1, +1, +1, \ldots$$

and

$$\epsilon^{(1)} = +1, -1, -1, +1, \ldots, +1, -1, -1, +1, \ldots$$

Manuscript received August 2, 2007; revised November 7, 2007. The work of T. Xiong was supported by the National Science Foundation. The work of J. Hall was supported by Institute for Quantum Sciences at Michigan State University and the National Science Foundation

The authors are with the Department of Mathematics, Michigan State University, East Lansing, MI, 48823 USA (xiongtin@msu.edu; jhall@math.msu.edu).

Communicated by G. Gong, Associate Editor for Sequences.

Color version of Figure 1 in this correspondence is available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2007.913421

Lemma 2.4: Let N be an odd number. If the binary sequence ϵ of length $2N$ is one of the four sequences $\pm\epsilon^{(\delta)}$ of Definition 2.3 then for $0 \leq a, b < 2N$ we have $\epsilon_a\epsilon_b = (-1)^{\frac{(b-a)(b+a+2\delta-1)}{2}}$.

Proof: When $0 \leq a, b < 2N$, by definition

$$\begin{aligned}\epsilon_a\epsilon_b &= (-1)^{\binom{a+\delta}{2}+\binom{b+\delta}{2}}\\ &= (-1)^{\frac{a^2+b^2-a-b}{2}+(a+b)\delta}\\ &= (-1)^{\frac{a^2+b^2-a-b}{2}-a^2+a+(a+b)\delta-2a\delta}\\ &= (-1)^{\frac{(b-a)(b+a+2\delta-1)}{2}}.\end{aligned}$$

□

The *periodic autocorrelation* function of a binary sequence x of length N is

$$P_x(i) = \sum_{j=0}^{N-1} x_{j+i}\,x_j, \quad 0 \leq i < N \tag{4}$$

where the sequence indices are taken mod N.

Lemma 2.5: Let α be an arbitrary binary sequence of length N, and let ϵ of length $2N$ be one of the four sequences $\pm\epsilon^{(\delta)}$ from Definition 2.3. Consider the new sequence $b = \{\alpha \mid \alpha\} * \epsilon$. For even i, we have

$$A_b(i) = \begin{cases} (-1)^{i/2}[A_\alpha(i) + P_\alpha(i)], & \text{if } 0 < i < N\\ (-1)^{i/2}A_\alpha(i-N), & \text{if } i \geq N\end{cases}$$

Proof: When $0 < i < N$

$$\begin{aligned}A_b(i) &= \sum_{j=0}^{N-i-1} b_jb_{j+i} + \sum_{j=N-i}^{N-1} b_jb_{j+i} + \sum_{j=N}^{2N-i-1} b_jb_{j+i}\\ &= I_l + I_m + I_r.\end{aligned} \tag{5}$$

Here I_l only contains the items from the first half of the sequence, I_r only contains the items from the second half, and I_m consists of the products of the terms from the first half and the terms from the second half. As i is even, the quantity $i + 2j + 2\delta - 1$ is always odd. Therefore by Lemma 2.4 we have

$$\begin{aligned}I_l &= \sum_{j=0}^{N-i-1} b_jb_{j+i} = \sum_{j=0}^{N-i-1} \epsilon_j\epsilon_{j+i}\alpha_j\alpha_{j+i}\\ &= \sum_{j=0}^{N-i-1} (-1)^{\frac{i(i+2j+2\delta-1)}{2}}\alpha_j\alpha_{j+i}\\ &= (-1)^{i/2}\sum_{j=0}^{N-i-1} \alpha_j\alpha_{j+i} = (-1)^{i/2}A_\alpha(i).\end{aligned} \tag{6}$$

Similarly

$$\begin{aligned}I_r &= \sum_{j=N}^{2N-i-1} b_jb_{j+i} = \sum_{j=N}^{2N-i-1} \epsilon_j\epsilon_{j+i}\alpha_{j-N}\alpha_{j+i-N}\\ &= (-1)^{i/2}\sum_{j=0}^{N-i-1} \alpha_j\alpha_{j+i} = (-1)^{i/2}A_\alpha(i)\end{aligned} \tag{7}$$

and

$$\begin{aligned}I_m &= \sum_{j=N-i}^{N-1} b_jb_{j+i} = \sum_{j=N-i}^{N-1} \epsilon_j\epsilon_{j+i}\alpha_j\alpha_{j+i-N}\\ &= (-1)^{i/2}\sum_{j=0}^{N-1-(N-i)} \alpha_j\alpha_{j+N-i}\\ &= (-1)^{i/2}A_\alpha(N-i).\end{aligned} \tag{8}$$

Combining (6), (7), and (8), we find

$$I_l + I_m + I_r = (-1)^{i/2}[A_\alpha(i) + P_\alpha(i)].$$

For even $i \geq N$, Lemma 2.4 gives

$$\begin{aligned}A_b(i) &= \sum_{j=0}^{2N-i-1} b_jb_{j+i} = \sum_{j=0}^{2N-i-1} \epsilon_j\epsilon_{j+i}\alpha_j\alpha_{j+i-N}\\ &= \sum_{j=0}^{2N-i-1} (-1)^{\frac{i(i+2j+2\delta-1)}{2}}\alpha_j\alpha_{j+i-N}\\ &= \sum_{j=0}^{N-(i-N)-1} (-1)^{i/2}\alpha_j\alpha_{j+(i-N)}\\ &= (-1)^{i/2}A_\alpha(i-N).\end{aligned}$$

□

Lemma 2.6: Let $\alpha = \{\alpha_0, \alpha_1, \ldots \alpha_{N-1}\}$ be a symmetric or anti-symmetric binary sequence of odd length N, and let $b = \{\alpha \mid \alpha\} * \epsilon$ be the corresponding sequence defined in Lemma 2.5. For odd i, we have

$$A_b(i) = \begin{cases} (-1)^{\delta + \frac{i-1}{2}}\alpha_0\alpha_{N-i}, & \text{if } 0 < i < N;\\ (-1)^{\delta + \frac{i-1}{2}}\alpha_0\alpha_{i-N}, & \text{if } i \geq N.\end{cases}$$

Proof: When $0 < i < N$, following (5) we write

$$A_b(i) = \sum_{j=0}^{2N-i-1} b_jb_{j+i} = I_l + I_m + I_r.$$

First consider any term $b_jb_{j+i} = \epsilon_j\epsilon_{j+i}\alpha_j\alpha_{j+i}$ in I_l. By Lemma 2.4

$$\begin{aligned}b_{j+N}b_{j+i+N} &= \epsilon_{j+N}\epsilon_{j+i+N}\alpha_j\alpha_{j+i}\\ &= (-1)^{\frac{i(2j+2N+i+2\delta-1)}{2}}\alpha_j\alpha_{j+i}\\ &= -(-1)^{\frac{i(2j+i+2\delta-1)}{2}}\alpha_j\alpha_{j+i}\\ &= -\epsilon_j\epsilon_{j+i}\alpha_j\alpha_{j+i} = -b_jb_{j+i}.\end{aligned}$$

Thus b_jb_{j+i} is canceled by $b_{j+N}b_{j+i+N}$ from I_r. That is, $I_l + I_r = 0$.

For any item $b_jb_{j+i} = \epsilon_j\epsilon_{j+i}\alpha_j\alpha_{j+i-N}$ in I_m with $i + j \neq N$, we have $0 < j < N$ and $i + j > N$. From Lemma 2.4

$$\begin{aligned}b_{2N-j}b_{2N-j-i} &= \epsilon_{2N-j}\epsilon_{2N-j-i}\alpha_{N-j}\alpha_{2N-j-i}\\ &= (-1)^{\frac{i(2j+i-2\delta+1)}{2}}\alpha_j\alpha_{j+i-N}\\ &= -(-1)^{\frac{i(2j+i+2\delta-1)}{2}}\alpha_j\alpha_{j+i-N}\\ &= -\epsilon_j\epsilon_{j+i}\alpha_j\alpha_{j+i-N} = -b_jb_{j+i}.\end{aligned}$$

The second equality follows from the symmetry properties of the sequence. Therefore when $i + j \neq N$, the item b_jb_{j+i} is canceled by $b_{2N-j}b_{2N-j-i}$. When $i + j = N$, $b_{2N-j}b_{2N-j-i} \in I_r$, so only $b_{N-i}b_N$ remains in I_m. From Lemma 2.4

$$\begin{aligned}b_{N-i}b_N &= \epsilon_{N-i}\epsilon_N\alpha_{N-i}\alpha_0 = (-1)^{\frac{i(2N-i+2\delta-1)}{2}}\alpha_{N-i}\alpha_0\\ &= (-1)^{N+\delta+\frac{i+1}{2}}\alpha_0\alpha_{N-i} = (-1)^{\delta+\frac{i-1}{2}}\alpha_0\alpha_{N-i}.\end{aligned}$$

For $i \geq N$, if $j > 0$ then by Lemma 2.4, the symmetry properties of α, and i being odd

$$\begin{aligned}b_jb_{j+i} &= \epsilon_j\epsilon_{j+i}\alpha_j\alpha_{j+i-N}\\ &= (-1)^{\frac{i(2j+i+2\delta-1)}{2}}\alpha_{N-j}\alpha_{2N-j-i}\\ &= -(-1)^{\frac{i(2j+i-2\delta+1)}{2}}\alpha_{N-j}\alpha_{2N-j-i}\\ &= -(-1)^{\frac{i(2j+i-2\delta+1-4N)}{2}}\alpha_{N-j}\alpha_{2N-j-i}\\ &= -\epsilon_{2N-j}\epsilon_{2N-j-i}\alpha_{N-j}\alpha_{2N-j-i}\\ &= -b_{2N-j}b_{2N-j-i}.\end{aligned}$$

Therefore every term $b_j b_{j+i}$ is canceled by $b_{2N-j} b_{2N-j-i}$ except for the term

$$\begin{aligned} b_0 b_i = \epsilon_0 \epsilon_i \alpha_0 \alpha_{i-N} &= (-1)^{\binom{i+\delta}{2}} \alpha_0 \alpha_{i-N} \\ &= (-1)^{i\delta + i\frac{i-1}{2}} \alpha_0 \alpha_{i-N} = (-1)^{\delta + \frac{i-1}{2}} \alpha_0 \alpha_{i-N} \end{aligned}$$

where the last equality holds because i is odd. □

Lemma 2.7: Let $b = \{\alpha \mid \alpha\} * \epsilon$ be one of the sequences of Lemma 2.6. Then

$$\sum_{k=1}^{2N-1} A_b^2(k) = N + \sum_{k=1}^{N-1} A_\alpha^2(k) + 2 \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k) A_\alpha(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k)^2.$$

Proof:

$$\begin{aligned} \sum_{k=1}^{2N-1} A_b^2(k) &= \sum_{\substack{k=1 \\ \text{odd } k}}^{2N-1} A_b^2(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{2N-1} A_b^2(k) \\ &= N + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} (P_\alpha(k) \\ &\quad + A_\alpha(k))^2 + \sum_{\substack{k=1 \\ \text{odd } k}}^{N-1} A_\alpha^2(k) \\ &= N + \sum_{k=1}^{N-1} A_\alpha^2(k) \\ &\quad + 2 \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k) A_\alpha(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k)^2. \end{aligned}$$

□

III. The Asymptotic Merit Factor of Some Doubled Legendre Sequences

Recall that the Legendre sequence α of prime length p is given by the Legendre symbols given by, for $j = 0, \dots, p-1$,

$$\alpha_j = \left(\frac{j}{p}\right) = \begin{cases} 1, & \text{if } j \text{ is a square modulo } p \\ -1, & \text{otherwise.} \end{cases} \qquad (9)$$

The following properties of Legendre sequences are well known.

Proposition 3.1:

a) For $0 < j < p, \alpha_j = \begin{cases} \alpha_{p-j}, & \text{if } p \equiv 1 (\bmod 4) \\ -\alpha_{p-j}, & \text{if } p \equiv 3 (\bmod 4). \end{cases}$

b) $P_\alpha(i) = -1$, if $p \equiv 3 (\bmod 4)$.

c) $P_\alpha(i) = 1$ or -3, if $p \equiv 1 (\bmod 4)$.

In [3] it was proven that if F is the asymptotic merit factor of cyclically shifted Legendre sequences corresponding to the offset fraction f (the number of positions shifted divided by the length), then

$$1/F = 2/3 - 4|f| + 8f^2, \quad |f| \le 1/2. \qquad (10)$$

In particular for the Legendre sequences α of length p with no shifting $(f = 0)$ we have the following lemma.

Lemma 3.2:

$$\lim_{p \to \infty} \frac{p^2}{2 \sum_{k=1}^{p-1} A_\alpha^2(k)} = \frac{3}{2}.$$

Now we are ready to prove the first theorem of this correspondence.

Theorem 3.3: For each odd prime number p, let $\alpha = \alpha^p$ be the Legendre sequence of length p given in (9), and let $\epsilon = \epsilon^p$ be one of the binary sequences of length $2p$ from Definition 2.3. For each p, we further let b be the length $2p$ sequence $\{\alpha \mid \alpha\} * \epsilon$. Then the asymptotic merit factor $\lim_{p \to \infty} (F_b)$ is 6.

Proof: By Proposition 3.1 the Legendre sequence α is symmetric for $p \equiv 1 (\bmod 4)$ and antisymmetric for $p \equiv 3 (\bmod 4)$. Therefore, by Lemma 2.7, we have

$$\sum_{k=1}^{2p-1} A_b^2(k) = p + \sum_{k=1}^{p-1} A_\alpha^2(k) + 2 \sum_{\substack{k=1 \\ \text{even } k}}^{p-1} c_k A_\alpha(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{p-1} {c_k}^2$$

where $c_k = P_\alpha(k) = \pm 1$ or -3 from Proposition 3.1.

As $|c_k| \le 3$

$$\sum_{\substack{k=1 \\ \text{even } k}}^{p-1} {c_k}^2 = \mathrm{O}(p).$$

By Lemma 3.2, $\sum_{k=1}^{p-1} A_\alpha^2(k) = O(p^2)$; so by the Cauchy–Schwarz inequality

$$\begin{aligned} \left| \sum_{\substack{k=1 \\ \text{even } k}}^{p-1} c_k A_\alpha(k) \right| &\le \sqrt{\left[\sum_{\substack{k=1 \\ \text{even } k}}^{p-1} A_\alpha^2(k) \right] \mathrm{O}(p)} \\ &\le \sqrt{\mathrm{O}(p^3)} = \mathrm{O}\left(p^{\frac{3}{2}}\right). \end{aligned}$$

We combine these results with Lemma 3.2 to find

$$\begin{aligned} \lim_{p \to \infty} (F_b) &= \lim_{p \to \infty} \frac{(2p)^2}{2 \left(\sum_{k=1}^{2p-1} A_b^2(k) \right)} \\ &= \lim_{p \to \infty} \frac{4p^2}{2 \sum_{k=1}^{p-1} A_\alpha^2(k)} \\ &= 4 \times \frac{3}{2} = 6 \end{aligned}$$

That is, $\lim_{p \to \infty} F_b = 6$. □

IV. The Asymptotic Merit Factor of Parker's Sequences

In [8] Parker gave a construction for sequences of length $N = 2p$, with p prime, which motivated the present investigations. We restate his results here. Let D_0 be the set of squares in $\mathrm{GF}(p) \backslash \{0\}$, and let D_1 be the set of nonsquares. First, Parker constructed a sequence of length $4p$ by specifying a subset C of Z_{2N}, then defining the characteristic sequence $s'(i)$ of C:

$$s'(i) = \begin{cases} 1, & \text{if } i \in C \\ 0, & \text{if } i \notin C \end{cases}$$

Let $C' = \{\{n\} \times C_n \mid C_n \subseteq Z_p^*, 0 \le n < r\}$, $F = \{G \times 0 \mid G \subseteq Z_r\}$, and $C = C' \cup F$. Then Parker gave the concrete description of C as follows:
If prime $p = 4f + 1$,
then let $C_0 = D_0,\ C_1 = D_0,\ C_2 = D_1,\ C_3 = D_1,\ G = \{1, 2\}$.
If prime $p = 4f + 3$,
then let $C_0 = D_0,\ C_1 = D_0,\ C_2 = D_1,\ C_3 = D_1,\ G = \{0, 1\}$.

Under this construction, the characteristic sequence $s'(i)$ of $C = C' \cup F$ is of the form $s'(i) = s(i)$, for $0 \le i < N$, and $s'(i) = s(i - N) + 1$, for $N \le i < 2N$, where $s(i)$ is a $\{0, 1\}$-sequence of length N. We convert $s(i)$ into ±1 binary form by putting

$$b_i = (-1)^{s(i)}, \quad 0 \le i \le N - 1. \qquad (11)$$

Parker did computer calculations indicating that the aymptotic merit factor of the sequences b given by (11) is 6.0. We will show that

Parker's sequence (11) is almost identical to the length $2p$ sequence b of Theorem 3.3 coming from the choice $\epsilon = -\epsilon^{(0)}$.

By the Chinese Remainder Theorem there exist n and m so that

$$\begin{aligned} n &\equiv 1 (\bmod 4), & n &\equiv 0 (\bmod p); \\ m &\equiv 0 (\bmod 4), & m &\equiv 1 (\bmod p). \end{aligned}$$

Specifically, when $p = 4f+1, n = p, m = 3p+1$; when $p = 4f+3, n = 3p, m = p+1$. Thus the construction of $C = C' \cup F$ as above becomes

$$\begin{aligned} (0, C_0) &= \{mD_0\} \equiv 0 (\bmod 4) \\ (1, C_1) &= \{n + mD_0\} \equiv 1 (\bmod 4) \\ (2, C_2) &= \{2n + mD_1\} \equiv 2 (\bmod 4) \\ (3, C_3) &= \{3n + mD_1\} \equiv 3 (\bmod 4). \end{aligned}$$

Now let $j \in (0, 2p)$ with $j \neq p$.

1) Suppose $j \equiv 0 (\bmod 4)$. If $j = m\beta$ for some $\beta \in D_0$, then $j \in (0, C_0)$ and $b_j = (-1)^{s(j)} = -1$. At the same time, $\beta \in D_0$ implies that $\alpha_\beta = 1$. Therefore $b_j = (-1)^{s(j)} = -\alpha_\beta$ since $j \equiv \beta (\bmod p)$. If $j \neq m\beta$ for any $\beta \in D_0$, then $s(j) = 0$ and so $b_j = (-1)^{s(j)} = 1 = -\alpha_j$. That is, if $j \equiv 0 (\bmod 4)$ then $b_j = -\alpha_j$.

   Similarly, if $j \equiv 1 (\bmod 4)$ then $b_j = -\alpha_j$.

2) Suppose $j \equiv 2 (\bmod 4)$. If $j = 2n + m\beta$ for some $\beta \in D_1$, then $j \in (2, C_2)$ and $b_j = (-1)^{s(j)} = -1$. At the same time, $\beta \notin D_0$ implies that $\alpha_\beta = -1$. Therefore $b_j = \alpha_\beta$ since $j \equiv \beta$ $(\bmod p)$. If $j \neq 2n + m\beta$ for any $\beta \in D_1$, then $s(j) = 0$ and so $b_j = (-1)^{s(j)} = 1 = \alpha_j$. That is, if $j \equiv 2 (\bmod 4)$ then $b_j = \alpha_j$.

   Similarly, if $j \equiv 3 (\bmod 4)$ then $b_j = \alpha_j$.

Finally, when $p = 4f+1$, we have $F = \{p, 2p\}$ under Parker's construction, so $s(0) = 0$ and $b_0 = (-1)^{s(0)} = 1$. Then $s(p) = 1$ gives $b_p = (-1)^{s(p)} = -1$. When $p = 4f+3$, we have $F = \{0, 3p\}$ under Parker's construction, so $s(0) = 1$ and $b_0 = (-1)^{s(0)} = -1$. Now $s(p) = 0$ gives $b_p = (-1)^{s(p)} = 1$. Therefore under Parker's construction the sequence b has the following form:

$$b_i = \begin{cases} (-1)^{\frac{p-1}{2}} \alpha_0, & \text{if } i = 0 \\ -\alpha_i, & \text{if } i \equiv 0 \text{ or } 1 (\bmod 4),\ i \neq 0 \\ \alpha_i, & \text{if } i \equiv 2 \text{ or } 3 (\bmod 4). \end{cases} \tag{12}$$

Comparing (12) with the $-\epsilon^{(0)}$ form of b in Theorem 3.3, we realize that the two sequences are exactly the same when $p = 4f+3$. When $p = 4f+1$ they are identical in every position except the first; Parker's sequence begins with α_0, while the $-\epsilon^{(0)}$ sequence from Theorem 3.3 starts with $-\alpha_0$. However, a change in one position of each sequence will not influence the aymptotic merit factor of a family (for instance, see [5, Corollary 6.3]). Therefore Parker's sequences have asymptotic merit factor 6 by Theorem 3.3.

V. The Asymptotic Merit Factor of Some Doubled Jacobi and Modified Jacobi Sequences

Jacobi symbols are generalizations of Legendre symbols. If $N = pq$, for p and q different primes, the Jacobi symbol $\left[\frac{j}{N}\right]$ is given by

$$\left[\frac{j}{N}\right] = \left(\frac{j}{p}\right) \cdot \left(\frac{j}{q}\right) \tag{13}$$

where the factors on the righthand side are the Legendre symbols of (9). The *Jacobi sequence* z of length $N = pq$ is defined by

$$z_j = \left[\frac{j}{N}\right].$$

The corresponding *modified Jacobi sequence* $m = \{m_0, m_1, \ldots, m_{N-1}\}$ of length $N = pq$ is given by

$$m_j = \begin{cases} +1, & j = 0, q, 2q, \ldots, (p-1)q \\ -1, & j = p, 2p, 3p, \ldots, (q-1)p \\ \left[\frac{j}{N}\right], & gcd(j, N) = 1. \end{cases} \tag{14}$$

In [4] it was proven that the asymptotic merit factor F of Jacobi or modified Jacobi sequences of length $N = pq$ offset by the factor f is

$$1/F = 2/3 - 4|f| + 8f^2, \quad |f| \leq 1/2 \tag{15}$$

provided p and q satisfy

$$\frac{(p+q)^5 \log^4 N}{N^3} \to 0, \quad \text{for } N \to \infty. \tag{16}$$

In particular for the sequence α (equal to z or m) with no shifting $(f = 0)$:

Lemma 5.1: Under (16) we have

$$\lim_{N \to \infty} \frac{N^2}{2 \sum_{k=1}^{N-1} A_\alpha^2(k)} = \frac{3}{2}.$$

It is important to realize that under (16) both p and q go to infinity as N goes to infinity; see ([4, p. 625]).

Theorem 5.2: For each pair p and q of distinct primes with $p \equiv q \equiv 1 (\bmod 4)$, let $\alpha = \alpha^N$ be a Jacobi sequence or a modified Jacobi sequence of length $N = pq$; and let $\epsilon = \epsilon^N$ be one of the binary sequences of length $2N$ from Definition 2.3. For each such N, we further let b be the length $2N$ sequence $\{\alpha \mid \alpha\} * \epsilon$. Then the asymptotic merit factor $\lim_{N \to \infty}(F_b)$ is 6 for $N = pq$ subject to (16).

Proof: It was shown in [4] that a Jacobi or modified Jacobi sequence of length $N = pq$ is symmetric when $p \equiv q \equiv 1 (\bmod 4)$. By Lemma 2.7, we thus have

$$\sum_{k=1}^{2N-1} A_b^2(k) = N + \sum_{k=1}^{N-1} A_\alpha^2(k) + 2 \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k) A_\alpha(k) + \sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k)^2.$$

We may assume throughout that $q > p$.

For α a Jacobi sequence, the periodic correlation function $P_\alpha(k)$ has the following distribution ([4, Th. 4.2]):

$$\begin{aligned} P_\alpha(k) = {} & p \text{ occurs } (q-1)/2 \text{ times} \\ & 3p \text{ occurs } (q-1)/2 \text{ times} \\ & q \text{ occurs } (p-1)/2 \text{ times} \\ & 3q \text{ occurs } (p-1)/2 \text{ times} \\ & 1 \text{ occurs } (p-1)(q-1)/4 \text{ times} \\ & 3 \text{ occurs } (p-1)(q-1)/2 \text{ times} \\ & 9 \text{ occurs } (p-1)(q-1)/4 \text{ times.} \end{aligned}$$

Therefore

$$\sum_{\substack{k=1 \\ \text{even } k}}^{N-1} P_\alpha(k)^2 = \mathrm{O}(pq^2).$$

By Lemma 5.1, when p and q satisfy (16) we have $\sum_{k=1}^{N-1} A_\alpha^2(k) = \mathrm{O}(N^2)$. Therefore by the Cauchy–Schwarz inequality

$$\left|\sum_{\substack{k=1\\ \text{even } k}}^{N-1} P_\alpha(k)A_\alpha(k)\right| \le \sqrt{\left[\sum_{\substack{k=1\\ \text{even } k}}^{N-1} A_\alpha^2(k)\right]\mathrm{O}(pq^2)}$$
$$\le \sqrt{\mathrm{O}(p^3q^4)} = \mathrm{O}\left(p^{\frac{3}{2}}q^2\right).$$

Combining these results with Lemma 5.1, we calculate (as in Theorem 3.3) that, for p and q subject to (16), the asymptotic merit factor is

$$\begin{aligned}\lim_{N\to\infty}(F_b) &= \lim_{N\to\infty}\frac{(2N)^2}{2(\sum_{k=1}^{2N-1}A_b^2(k))}\\ &= \lim_{N\to\infty}\frac{4N^2}{2\sum_{k=1}^{N-1}A_\alpha^2(k)}\\ &= 4\times\frac{3}{2} = 6.\end{aligned}$$

Similarly for α a modified Jacobi sequence, the periodic correlation function $P_\alpha(k)$ has the following distribution ([9, p. 246]):

$$\begin{aligned} P_\alpha(k) = q-p-3 &\quad \text{occurs } (q-1) \text{ times}\\ p-q+1 &\quad \text{occurs } (p-1) \text{ times}\\ 1 &\quad \text{occurs } (p-1)(q-1)/2 \text{ times}\\ -3 &\quad \text{occurs } (p-1)(q-1)/2 \text{ times.}\end{aligned}$$

Therefore

$$\sum_{\substack{k=1\\ \text{even } k}}^{N-1} P_\alpha(k)^2 = \mathrm{O}(pq) = \mathrm{O}(N).$$

By Lemma 5.1 when p and q satisfy (16) we have $\sum_{k=1}^{N-1} A_\alpha^2(k) = \mathrm{O}(N^2)$. Hence by the Cauchy–Schwarz inequality

$$\left|\sum_{\substack{k=1\\ \text{even } k}}^{N-1} P_\alpha(k)A_\alpha(k)\right| \le \sqrt{\left[\sum_{\substack{k=1\\ \text{even } k}}^{N-1} A_\alpha^2(k)\right]\mathrm{O}(N)}$$
$$\le \sqrt{\mathrm{O}(N^3)} = \mathrm{O}\left(N^{\frac{3}{2}}\right).$$

We again combine all the results above with Lemma 5.1 and find that, when p and q satisfy (16), the asymptotic merit factor is

$$\begin{aligned}\lim_{N\to\infty}(F_b) &= \lim_{N\to\infty}\frac{(2N)^2}{2(\sum_{k=1}^{2N-1}A_b^2(k))}\\ &= \lim_{N\to\infty}\frac{4N^2}{2\sum_{k=1}^{N-1}A_\alpha^2(k)}\\ &= 4\times\frac{3}{2} = 6. \qquad \square\end{aligned}$$

VI. Some Merit Factors Larger Than 6.17

In this final section we present some numerical experimentation inspired by similar results in [5]–[7]. For the sequence b of Theorem 3.3, we write $(-b)_f$ for the sequence $(-b_0, -b_1, \ldots, -b_{\lfloor fp\rfloor -1})$ obtained by truncating $-b$ to the fraction f of its length. Computer calculation then indicated that

$$\limsup_{p\to\infty} F_{\{b:(-b)_f\}} > 6.17$$

for $0.06 \le f \le 0.07$. Fig. 1 shows the merit factor aymptote of $\{b : (-b)_f\}$ for Parker's sequences and the corresponding sequences of Theorem 3.3 when $f = 0.065$. Jedwab [2] reports that Parker has done similar calculations.

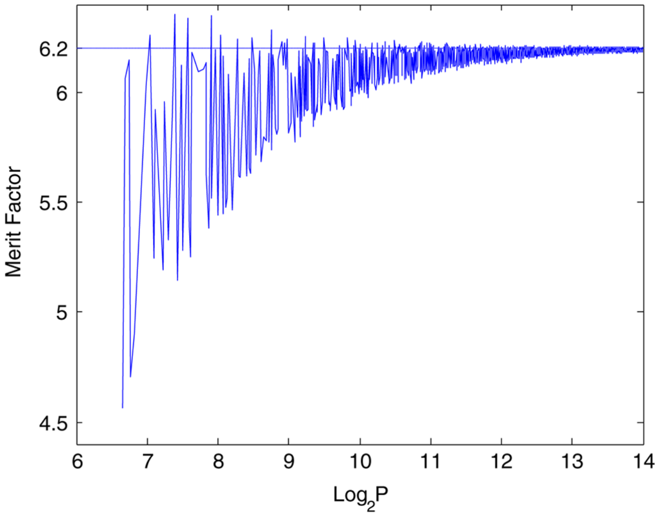

Fig. 1. Merit factor for Parker's sequences with appending ratio 0.065.

Calculations done with Jacobi and modified Jacobi sequences were not fruitful.

VII. Conclusion

It has been known for a while that families of sequences with asymptotic merit factor 6 can be obtained by cyclically shifting Legendre sequences, Jacobi sequences, or modified Jacobi sequences. In this correspondence, which is inspired by Parker's work [8] with Legendre sequences, a doubling method is introduced for constructing even length binary sequences. The doubling construction is free of cyclic shifting; but, when applied to Legendre sequences or to certain Jacobi or modified Jacobi sequences, it gives families of sequences that are proven to have asymptotic merit factor 6.

References

[1] M. J. E. Golay, "Sieves for low autocoreation binary sequences," *IEEE Trans. Inf. Theory*, vol. 23, no. 1, pp. 43–51, Jan. 1977.

[2] J. Jedwab, "A survey of the merit factor problem for binary sequences," in *Proc. SETA 2004*, T. Helleseth, Ed. *et al.*, 2005, vol. 3486, Lecture Notes in Computer Science, Sequences and Their Applications, pp. 30–55, Berlin, Germany: Springer-Verlag.

[3] T. Hø holdt and H. E. Jensen, "Determination of the merit factor of Legendre sequences," *IEEE Trans. Inf. Theory*, vol. 34, no. 1, pp. 161–164, Jan. 1988.

[4] J. M. Jensen, H. E. Jensen, and T. Hø holdt, "The merit factor of binary sequences related to difference sets," *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 617–625, May 1991.

[5] P. Borwein, K.-K. S. Choi, and J. Jedwab, "Binary sequences with merit factor greater than 6.34," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3234–3249, Dec. 2004.

[6] A. Kirilusha and G. Narayanaswamy, "Construction of new asymptotic classes of binary sequences based on existing asymptotic classes," Dept. Math. Comput. Sci., Univ. Richmond, Summer Science Program Tech. Rep., 1999.

[7] R. A. Kristiansen and M. G. Parker, "Binary sequences with merit factor >6.3," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3385–3389, Dec. 2004.

[8] M. G. Parker, "Even length binary sequence families with low negaperiodic autocorrelation," in *Proceedings of AAECC-14 2001*, 2001, vol. 2227, Lecture Notes in Computer Science, pp. 200–209, Berlin, Germany: Springer-Verlag.

[9] D. H. Green and P. R. Green, "Modified Jacobi sequences," *IEE Proc.-Comput. Digit. Tech.*, vol. 147, no. 4, pp. 241–251, Jul. 2000.