Contemporary Mathematics

The merit factor of binary sequence families constructed from m-sequences

Jonathan Jedwab and Kai-Uwe Schmidt

Abstract. We consider the asymptotic merit factor of two binary sequence families obtained from an initial binary sequence family using a "negaperiodic" and a "periodic" construction. When the initial sequences are m-sequences, both of the constructed families have the same asymptotic merit factor as the initial family, at all rotations of sequence elements. A similar property was previously shown to hold when the initial sequences are Legendre sequences. However we show by example that this property appears to fail for a general initial sequence family.

1. Introduction

We consider a *sequence* A of length n to be an n-tuple $(a_0, a_1, \ldots, a_{n-1})$ of real numbers. The *aperiodic autocorrelation* of A at shift u is

$$C_A(u) := \begin{cases} \displaystyle\sum_{j=0}^{n-u-1} a_j a_{j+u} & \text{for } 0 \le u < n \\ C_A(-u) & \text{for } -n < u < 0, \end{cases}$$

and its *energy* $E(A)$ is $C_A(0)$. Provided that $\sum_{0<|u|<n}[C_A(u)]^2 > 0$, the *merit factor* of A is defined to be

$$F(A) := \frac{[E(A)]^2}{\displaystyle\sum_{0<|u|<n} [C_A(u)]^2}.$$

The sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n is called *binary* if each a_j takes the value $+1$ or -1, in which case $E(A) = n$. Our objective is to understand the behaviour, as $n \longrightarrow \infty$, of the optimal value of the merit factor $F(A)$ as A ranges over the set of all 2^n binary sequences of length n.

2000 *Mathematics Subject Classification.* Primary 94A55, 68P30.

Key words and phrases. aperiodic autocorrelation, asymptotic, binary sequence, m-sequence, merit factor, negaperiodic, periodic.

J. Jedwab is supported by NSERC of Canada.

K.-U. Schmidt is supported by Deutsche Forschungsgemeinschaft (German Research Foundation) under Research Fellowship SCHM 2609/1-1.

Date. July 27, 2009 (revised November 4, 2009).

The merit factor is important both practically and theoretically. The larger the merit factor of a binary sequence that is used to transmit information by modulating a carrier signal, the more uniformly the signal energy is distributed over the frequency range; this is particularly important in spread-spectrum communication [**BCH85**]. The optimal value of the merit factor of a binary sequence is studied in complex analysis, in statistical mechanics, and in theoretical physics and theoretical chemistry (see [**Jed05**] for a survey of the merit factor problem, and [**Jed08**] for a survey of related problems).

The only non-trivial infinite families of binary sequences for which the asymptotic value of the merit factor is known are: Legendre sequences and some generalisations, including Jacobi and modified Jacobi sequences; m-sequences; and Rudin-Shapiro sequences and some generalisations. The largest proven asymptotic merit factor of a binary sequence family is 6, which is attained by rotated Legendre sequences (see Theorem 5). Furthermore, there is numerical evidence, although not yet a proof, that a merit factor value greater than 6.34 can be consistently attained for long binary sequences [**BCJ04**].

In this paper, we study two product constructions that were previously analysed in [**SJP09**]. A first, "negaperiodic", construction inputs a length n binary sequence and outputs a length $2n$ binary sequence. A second, "periodic", construction inputs a length n binary sequence and outputs a length $4n$ binary sequence. We find in both the negaperiodic and the periodic case that the asymptotic merit factor of the output sequence family is the same as that of the input sequence family, at all rotations of sequence elements, when the input sequences are m-sequences. The same property was previously shown to hold (up to rotation of both output sequences by the same amount) when the input sequences are Legendre sequences. However we show by example that this property appears to fail for general input binary sequences.

2. Definitions and Notation

In this section we introduce further definitions and notation for the paper.

Let $A = (a_0, a_1, \ldots, a_{n-1})$ and $B = (b_0, b_1, \ldots, b_{n-1})$ be sequences of equal length n. The *aperiodic crosscorrelation* between A and B at shift u is

$$C_{A,B}(u) := \begin{cases} \sum_{j=0}^{n-u-1} a_j b_{j+u} & \text{for } 0 \le u < n \\ C_{B,A}(-u) & \text{for } -n < u < 0. \end{cases}$$

The aperiodic autocorrelation $C_A(u)$ defined in Section 1 equals $C_{A,A}(u)$ for $|u| < n$. From the definition of $C_A(u)$ and $F(A)$ we have the relation

$$\frac{1}{F(A)} = -1 + \frac{1}{[E(A)]^2} \sum_{|u|<n} [C_A(u)]^2 \tag{2.1}$$

for the reciprocal merit factor $1/F(A)$.

Given a sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n, we regard any expression for the sequence subscript to be reduced modulo n, so that $a_{i+n} = a_i$ for all i; we write $[A]_j$ to denote the sequence element a_j. Let $A = (a_0, a_1, \ldots, a_{n-1})$ and $B = (b_0, b_1, \ldots, b_{m-1})$ be sequences of length n and m, respectively. The *concatenation*

$A;B$ of A and B is the length $n+m$ sequence given by

$$[A;B]_j := \begin{cases} a_j & \text{for } 0 \le j < n \\ b_{j-n} & \text{for } n \le j < n+m. \end{cases}$$

Provided $\gcd(m,n)=1$, the *product* sequence $A \otimes B$ of length mn is defined by

$$[A \otimes B]_j := a_j b_j \quad \text{for } 0 \le j < mn.$$

Provided $\gcd(d,n)=1$, the *d-decimation* of A is the length n sequence C defined by

$$[C]_j := a_{dj} \quad \text{for } 0 \le j < n.$$

The *periodic rotation* A_r of A by a fraction r of its length (for any real r) is the length n sequence given by

$$[A_r]_j := a_{j+\lfloor nr \rfloor} \quad \text{for } 0 \le j < n,$$

and the *negaperiodic rotation* $A_{\widetilde{r}}$ of A by the fraction r is the length n sequence given by

$$[A_{\widetilde{r}}]_j := \begin{cases} a_{j+\lfloor nr \rfloor} & \text{for } 0 \le j < n - \lfloor nr \rfloor \\ -a_{j+\lfloor nr \rfloor} & \text{for } n - \lfloor nr \rfloor \le j < n. \end{cases}$$

The sequence $A_{\widetilde{r}}$ can be viewed as the first n elements of the length $2n$ sequence $(A;-A)_{\frac{r}{2}}$. For example, take $r = \frac{2}{7}$ and $A = (+,+,+,-,+,-,-)$, where $+$ and $-$ represent sequence elements $+1$ and -1, respectively. Then we have

$$\begin{aligned} A_r &= (+,-,+,-,-,+,+), \\ A_{\widetilde{r}} &= (+,-,+,-,-,-,-), \\ (A;-A)_{\frac{r}{2}} &= (+,-,+,-,-,-,-,-,+,-,+,+,+,+). \end{aligned}$$

Given a sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n, the *z-transform* of A is the function $Q_A : \mathbb{C} \to \mathbb{C}$ given by

$$Q_A(z) := \sum_{j=0}^{n-1} a_j z^j. \tag{2.2}$$

3. m-sequences

This section provides background and some required results on m-sequences.

Let $\mathrm{GF}(2^m)$ be the finite field containing 2^m elements, and let $\mathrm{tr} : \mathrm{GF}(2^m) \to \mathrm{GF}(2)$ be the absolute trace function on $\mathrm{GF}(2^m)$ given by $\mathrm{tr}(z) := \sum_{j=0}^{m-1} z^{2^j}$. An *m-sequence* $X = (x_0, x_1, \ldots, x_{n-1})$ of length $n = 2^m - 1$ is defined by

$$x_j := (-1)^{\mathrm{tr}(\beta\alpha^j)} \quad \text{for } 0 \le j < n \tag{3.1}$$

for some primitive element α of $\mathrm{GF}(2^m)$ and some nonzero element β of $\mathrm{GF}(2^m)$.

We shall require the following properties of m-sequences (see [**GG05**] for a detailed modern treatment; these properties were originally derived using an alternative definition of m-sequences involving a linear recurrence relation [**Gol67**]).

Lemma 1. *Let $X = (x_0, x_1, \ldots, x_{n-1})$ be an m-sequence of length $n = 2^m - 1$, as in* (3.1)*.*

(i) *The rotated sequence X_r is an m-sequence for every real r.*

(ii) ([**Gol67**, p. 78]) *Provided that* $\gcd(d,n)=1$*, the* d*-decimation of* X *is an* m*-sequence.*

(iii) ([**Gol67**, Thm. 4.3]) *There is a permutation* π *of* $\{1,2,\dots,n-1\}$*, determined by the primitive element* α *in* (3.1)*, for which*

$$x_j x_{j+u} = x_{j+\pi(u)} \quad \textit{for all } u\in\{1,2,\dots,n-1\} \textit{ and for all } j. \tag{3.2}$$

(iv) ([**Gol67**, p. 86]) *Let* $\epsilon_j := e^{2\pi\sqrt{-1}j/n}$ *for integer* j*. The* z*-transform of* X *satisfies*

$$|Q_X(\epsilon_j)|^2 = \begin{cases} 1 & \textit{for } j\equiv 0 \pmod n \\ n+1 & \textit{otherwise.}\end{cases}$$

The asymptotic merit factor of an m-sequence was calculated as 3 by Jensen and Høholdt in 1989, which by Lemma 1 (i) implies:

Theorem 2 ([**JH89**]). *Let* X *be an* m*-sequence of length* $n=2^m-1$ *and let* r *be a real number. Then*

$$\lim_{n\longrightarrow\infty} F(X_r) = 3.$$

4. The Negaperiodic and Periodic Construction

In this section we describe the negaperiodic and periodic constructions, outlining how they will be applied to m-sequences and summarising their previous application to Legendre sequences.

Let X be a sequence of odd length n. The negaperiodic construction applied to X outputs the length $2n$ sequence $N(X)$, where

$$N(X);-N(X) := X\otimes(+,+,-,-).$$

The periodic construction applied to X outputs the length $4n$ sequence

$$P(X) := X\otimes(+,+,+,-).$$

The following result gives an expression from which we can calculate the merit factor of $N(X)$ at negaperiodic rotations:

Lemma 3 ([**SJP09**, Lemma 4]). *Let* X *be a sequence of odd length* n*, each of whose elements is bounded in magnitude by a constant independent of* n*, and let* Z *be the* 2*-decimation of* X*. Let* r *be a real number, and write* $\rho := \lfloor nr\rfloor/n$ *and* $\delta := \frac{n+1}{2n}$*. Then, as* $n\longrightarrow\infty$*,*

$$\sum_{|u|<2n}[C_{(N(X))_{\bar\rho}}(u)]^2$$
$$= \sum_{|u|<n}\left([C_{Z_r}(u)+C_{Z_{r+\delta}}(u)]^2 + [C_{Z_r,Z_{r+\delta}}(u) - C_{Z_{r+\delta},Z_{r+2\delta}}(u)+O(1)]^2\right).$$

Similarly, the following result gives an expression from which we can calculate the merit factor of $P(X)$ at periodic rotations:

Lemma 4 ([**SJP09**, Lemma 7]). *Let* X *be a sequence of odd length* n*, each of whose elements is bounded in magnitude by a constant independent of* n*, and let* Z *be the* 4*-decimation of* X*. Let* r *be a real number, and write* $\rho := \lfloor nr\rfloor/n$ *and*

$$\delta := \begin{cases} \frac{3n+1}{4n} & \textit{for } n\equiv 1 \pmod 4 \\ \frac{n+1}{4n} & \textit{for } n\equiv 3 \pmod 4).\end{cases}$$

Then, as $n \longrightarrow \infty$,

$$\sum_{|u|<4n} \left[C_{(P(X))_\rho}(u)\right]^2 = \sum_{k=0}^{3} \sum_{|u|<n} \left(\sum_{i=0}^{3} (-1)^{\frac{ik(i+k+2)}{2}} C_{Z_{r+i\delta}, Z_{r+(i+k)\delta}}(u) + O(1) \right)^2 .$$

We will consider the sequences $N(X)$ and $P(X)$ in the case that X is an m-sequence. By Lemma 1 (ii), the asymptotic form of the expressions in Lemmas 3 and 4 involving the decimated sequence Z can then be determined, provided we can evaluate the asymptotic form of $\sum_{|u|<n} C_{X,X_s}(u)\, C_{X_t,X_{s+t}}(u)$ for suitable real s and t; this evaluation will be carried out in Section 5.

A *Legendre sequence* $X = (x_0, x_1, \ldots, x_{n-1})$ of prime length n is defined for $0 \le j < n$ by

$$x_j := \begin{cases} 1 & \text{for } j \text{ a square modulo } n \\ -1 & \text{otherwise.} \end{cases}$$

The asymptotic merit factor of a Legendre sequence was calculated for all periodic rotations by Høholdt and Jensen in 1988:

Theorem 5 ([**HJ88**]). *Let X be a Legendre sequence of prime length $n > 2$, and let r be a real number satisfying $|r| \le \frac{1}{2}$. Then*

$$\frac{1}{\lim\limits_{n \longrightarrow \infty} F(X_r)} = \tfrac{1}{6} + 8\left(|r| - \tfrac{1}{4}\right)^2 .$$

Lemmas 3 and 4 were previously used to obtain asymptotic merit factor results for $N(X)$ and $P(X)$ in the case that X is a Legendre sequence:

Theorem 6 ([**SJP09**, Theorems 5 and 8]). *Let X be a Legendre sequence of prime length $n > 2$, and let r be a real number satisfying $|r| \le \frac{1}{2}$. Then*

$$\frac{1}{\lim\limits_{n \longrightarrow \infty} F((N(X))_{\tilde{r}})} = \frac{1}{\lim\limits_{n \longrightarrow \infty} F((P(X))_r)} = \begin{cases} \frac{1}{6} + 8r^2 & \textit{for } |r| \le \frac{1}{4} \\ \frac{1}{6} + 8(|r| - \frac{1}{2})^2 & \textit{for } \frac{1}{4} \le |r| \le \frac{1}{2}. \end{cases}$$

The results of Theorems 5 and 6 are displayed in Figure 1, for r taking values in the range $[0, 1)$ (noting that any sequence A satisfies $A_{r+1} = A_r$ for all r). The left graph shows how the asymptotic merit factor of a Legendre sequence X varies with periodic rotation r. The right graph shows how the asymptotic merit factor of $N(X)$ varies with negaperiodic rotation r; the same graph also shows how the asymptotic merit factor of $P(X)$ varies with periodic rotation r. Each of the functions represented in the right graph is simply a translation of the function represented in the left graph.

5. Asymptotic Cross-Correlation Expression for m-Sequences

In this section we find the asymptotic value of $\sum_{|u|<n} C_{X,X_s}(u)\, C_{X_t,X_{s+t}}(u)$ for real s, t and an m-sequence X of length n, in readiness for the calculation in Section 6 of the asymptotic form of the expressions in Lemmas 3 and 4.

Write

$$\epsilon_j := e^{2\pi\sqrt{-1}j/n} \quad \text{for integer } j.$$

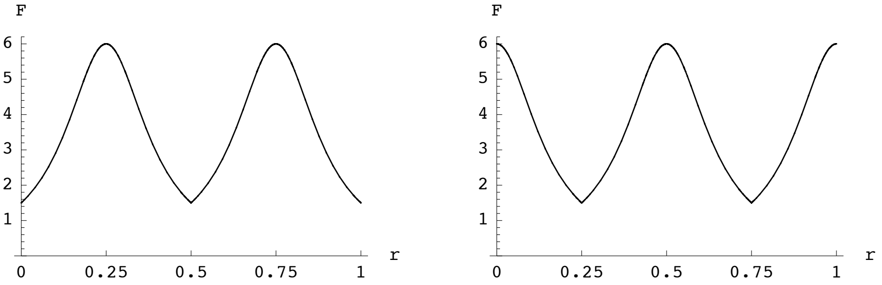

FIGURE 1. Variation of asymptotic merit factor of a Legendre sequence with rotation, before (left graph) and after (right graph) application of the negaperiodic/periodic construction.

Given a sequence $A = (a_0, a_1, \dots, a_{n-1})$ of length n, let

$$\Lambda_A(j,k,\ell) := \sum_{a=0}^{n-1} Q_A(\epsilon_a)\overline{Q_A(\epsilon_{a+j})}Q_A(\epsilon_{a+k})\overline{Q_A(\epsilon_{a+\ell})} \quad \text{for integer } j,\ k,\ \ell, \tag{5.1}$$

using the definition (2.2) of the function Q_A. The following result generalises the method of Høholdt and Jensen [**HJ88**] for calculating the reciprocal merit factor of an arbitrary sequence of odd length n as the sum of expressions involving complex nth roots of unity:

LEMMA 7 ([**SJP09**, Lemma 10]). *Let X be a sequence of odd length n. Let S and T be integers, and write $s := S/n$ and $t := T/n$. Then*

$$\frac{1}{n^2}\sum_{|u|<n} C_{X,X_s}(u)\, C_{X_t,X_{s+t}}(u) = \frac{2n^2+1}{3n^5}\,\Lambda_X(0,0,0)+B+C_1+C_2+D_1+D_2, \tag{5.2}$$

where

$$B = \frac{1}{n^5}\sum_{k=1}^{n-1}\Big[\big(\epsilon_k^T+\epsilon_k^S\big)\Lambda_X(0,0,k) + \big(\epsilon_k^{-(S+T-1)}+\epsilon_k\big)\overline{\Lambda_X(0,0,k)}\Big]\cdot\frac{1+\epsilon_k}{(1-\epsilon_k)^2},$$

$$C_1 = -\frac{2}{n^5}\sum_{\substack{1\le k,\ell<n\\ k\ne\ell}} \frac{\big(\epsilon_k^{-(S+T-1)}+\epsilon_k\big)\big(\epsilon_\ell^T+\epsilon_\ell^S\big)}{(1-\epsilon_k)(1-\epsilon_\ell)}\Lambda_X(0,k,\ell),$$

$$C_2 = -\frac{2}{n^5}\sum_{\substack{1\le k,\ell<n\\ k\ne\ell}} \frac{\epsilon_k^S\epsilon_\ell^T\Lambda_X(k,0,\ell)+\epsilon_k^{-(S+T-1)}\epsilon_\ell\,\overline{\Lambda_X(k,0,\ell)}}{(1-\epsilon_k)(1-\epsilon_\ell)},$$

$$D_1 = \frac{4}{n^5}\sum_{k=1}^{n-1}\frac{\epsilon_k^S+\epsilon_k^T}{|1-\epsilon_k|^2}\,\Lambda_X(0,k,k),$$

$$D_2 = \frac{4}{n^5}\sum_{k=1}^{n-1}\frac{\epsilon_k^{S+T-1}}{|1-\epsilon_k|^2}\,\Lambda_X(k,0,k).$$

We wish to apply Lemma 7 to an m-sequence X. The following lemma bounds the magnitude of some of the terms that will result.

Lemma 8. *Let X be an m-sequence of length $n = 2^m - 1$. Then*

$$|\Lambda_X(0,k,\ell)| \le n(n+1) \qquad \text{for } 0 \le k,\ell < n, \text{ where } k \ne \ell, \tag{5.3}$$

$$|\Lambda_X(k,0,\ell)| \le n(n+1)^{\frac{3}{2}} \qquad \text{for } 1 \le k,\ell < n. \tag{5.4}$$

Proof. Let α be the primitive element of $\mathrm{GF}(2^m)$ appearing in the definition (3.1) of the m-sequence $X = (x_0, x_1, \ldots, x_{n-1})$, and let π be the permutation determined by α satisfying (3.2). Then by the definition (2.2) we have, for $0 \le k < n$,

$$\begin{aligned} Q_X(\epsilon_a)\overline{Q_X(\epsilon_{a+k})} &= \sum_{m=0}^{n-1}\sum_{j=0}^{n-1} x_m x_j \epsilon_a^m \epsilon_{a+k}^{-j} \\ &= \sum_{u=0}^{n-1}\sum_{j=0}^{n-1} x_{j+u} x_j \epsilon_a^u \epsilon_k^{-j}, \end{aligned}$$

by writing $u := (m-j) \bmod n$. The $u = 0$ summand of this expression is zero, and then by (3.2) we get, for $0 \le k < n$,

$$\begin{aligned} Q_X(\epsilon_a)\overline{Q_X(\epsilon_{a+k})} &= \sum_{u=1}^{n-1}\sum_{j=0}^{n-1} x_{j+\pi(u)} \epsilon_k^{-(j+\pi(u))} \epsilon_k^{\pi(u)} \epsilon_a^u \\ &= \overline{Q_X(\epsilon_k)} \sum_{u=1}^{n-1} \epsilon_k^{\pi(u)} \epsilon_a^u. \end{aligned} \tag{5.5}$$

It follows from the definition (5.1) that, for $0 \le k,\ell < n$ and $k \ne \ell$,

$$\begin{aligned} \Lambda_X(0,k,\ell) &= \sum_{a=0}^{n-1} \Big(Q_X(\epsilon_a)\overline{Q_X(\epsilon_{a+\ell})}\Big) \overline{\Big(Q_X(\epsilon_a)\overline{Q_X(\epsilon_{a+k})}\Big)} \\ &= \overline{Q_X(\epsilon_\ell)} Q_X(\epsilon_k) \sum_{u=1}^{n-1}\sum_{v=1}^{n-1} \epsilon_\ell^{\pi(u)} \epsilon_k^{-\pi(v)} \sum_{a=0}^{n-1} \epsilon_a^{u-v} \\ &= n\,\overline{Q_X(\epsilon_\ell)} Q_X(\epsilon_k) \sum_{u=1}^{n-1} \epsilon_{\ell-k}^{\pi(u)} \\ &= -n\,\overline{Q_X(\epsilon_\ell)} Q_X(\epsilon_k) \epsilon_{\ell-k}^{\pi(0)}, \end{aligned}$$

which implies (5.3) using Lemma 1 (iv).

We can similarly use (5.5) to show that, for $1 \le k,\ell < n$,

$$\begin{aligned} \Lambda_X(k,0,\ell) &= \sum_{a=0}^{n-1} \Big(Q_X(\epsilon_a)\overline{Q_X(\epsilon_{a+k})}\Big) \Big(Q_X(\epsilon_a)\overline{Q_X(\epsilon_{a+\ell})}\Big) \\ &= \overline{Q_X(\epsilon_k) Q_X(\epsilon_\ell)} \sum_{u=1}^{n-1}\sum_{v=1}^{n-1} \epsilon_k^{\pi(u)} \epsilon_\ell^{\pi(v)} \sum_{a=0}^{n-1} \epsilon_a^{u+v} \\ &= n\,\overline{Q_X(\epsilon_k) Q_X(\epsilon_\ell)} \sum_{u=1}^{n-1} \epsilon_k^{\pi(u)} \epsilon_\ell^{\pi(n-u)}. \end{aligned}$$

This implies (5.4), by using Lemma 1 (iv) together with the inequality

$$\left|\sum_{u=1}^{n-1}\epsilon_k^{\pi(u)}\epsilon_\ell^{\pi(n-u)}\right| \le (n+1)^{\frac{1}{2}} \quad \text{for } 1 \le k, \ell < n$$

(see [**JJH91**, Lemma 3.5], for example). □

We now apply Lemma 7 to an m-sequence X in order to evaluate the desired asymptotic form.

Theorem 9. *Let X be an m-sequence of length $n = 2^m - 1$, and let s and t be real numbers satisfying $|s| < 1$ and $|t| < 1$. Let $\{s(n)\}$ and $\{t(n)\}$ be sets of real numbers such that $ns(n)$ and $nt(n)$ are integers for each n, and such that, as $n \longrightarrow \infty$, $s(n) = s + O(n^{-1})$ and $t(n) = t + O(n^{-1})$. Then, as $n \longrightarrow \infty$,*

$$\frac{1}{n^2}\sum_{|u|<n} C_{X,X_{s(n)}}(u)C_{X_{t(n)},X_{s(n)+t(n)}}(u)$$
$$= \tfrac{1}{3} + 2\left(|s| - \tfrac{1}{2}\right)^2 + 2\left(|t| - \tfrac{1}{2}\right)^2 + O\left(n^{-\frac{1}{2}}(\log n)^2\right).$$

Proof. Apply Lemma 7 to X, setting $S := ns(n)$ and $T := nt(n)$. Since S and T are integers for each n by assumption, the left hand side of (5.2) becomes

$$\frac{1}{n^2}\sum_{|u|<n} C_{X,\,X_{s(n)}}(u)\,C_{X_{t(n)},\,X_{s(n)+t(n)}}(u).$$

We now prove the result by finding the asymptotic form of the right hand side of (5.2) as $n \longrightarrow \infty$, evaluating the term involving $\Lambda_X(0,0,0)$ and the sum D_1, and bounding the sums B, C_1, C_2, and D_2.

The term involving $\Lambda_X(0,0,0)$. From (5.1) and Lemma 1 (iv) we have

$$\frac{2n^2+1}{3n^5}\Lambda_X(0,0,0) = \frac{2n^2+1}{3n^5}\left(1 + (n-1)(n+1)^2\right)$$
$$= \frac{2}{3} + O(n^{-1}) \quad \text{as } n \longrightarrow \infty. \tag{5.6}$$

The sum D_1. From (5.1) and Lemma 1 (iv), for $1 \le k < n$ we have

$$\Lambda_X(0,k,k) = 2(n+1) + (n-2)(n+1)^2$$
$$= n^3\left(1 + O(n^{-1})\right) \quad \text{as } n \longrightarrow \infty. \tag{5.7}$$

We wish to apply the identity

$$\sum_{k=1}^{n-1}\frac{\epsilon_k^j}{|1-\epsilon_k|^2} = \frac{n^2}{2}\left(\frac{|j|}{n} - \frac{1}{2}\right)^2 - \frac{n^2+2}{24} \quad \text{for integer } j \text{ satisfying } |j| \le n \tag{5.8}$$

(see, [**JJH91**, p. 621], for example). By the definition of S and T and the assumptions $s(n) = s + O(n^{-1})$ and $t(n) = t + O(n^{-1})$, as $n \longrightarrow \infty$ we have

$$S = ns + O(1) \text{ and } T = nt + O(1). \tag{5.9}$$

Then, since $|s| < 1$ and $|t| < 1$ by assumption, we know that $|S| \le n$ and $|T| \le n$ for all sufficiently large n. Therefore, by (5.7) and (5.8), as

$n \longrightarrow \infty$ we have

$$\begin{aligned} D_1 &= \frac{4}{n^2}\left(1+O(n^{-1})\right)\left[\frac{n^2}{2}\left(\frac{|S|}{n}-\frac{1}{2}\right)^2+\frac{n^2}{2}\left(\frac{|T|}{n}-\frac{1}{2}\right)^2-\frac{n^2+2}{12}\right] \\ &= 2\left(|s|-\tfrac{1}{2}\right)^2+2\left(|t|-\tfrac{1}{2}\right)^2-\tfrac{1}{3}+O(n^{-1}), \qquad (5.10) \end{aligned}$$

by (5.9).

The remaining sums. By Lemma 8, we can bound the remaining sums by

$$\begin{aligned} |B|+|C_1| &\le \frac{1}{n^5}\sum_{k=1}^{n-1}\frac{8\,|\Lambda_X(0,0,k)|}{|1-\epsilon_k|^2}+\frac{2}{n^5}\sum_{\substack{1\le k,\ell<n\\ k\ne\ell}}\frac{4\,|\Lambda_X(0,k,\ell)|}{|1-\epsilon_k|\cdot|1-\epsilon_\ell|} \\ &\le \frac{8(n+1)}{n^4}\left(\sum_{k=1}^{n-1}\frac{1}{|1-\epsilon_k|^2}+\sum_{\substack{1\le k,\ell<n\\ k\ne\ell}}\frac{1}{|1-\epsilon_k|\cdot|1-\epsilon_\ell|}\right) \\ &= \frac{8(n+1)}{n^4}\left(\sum_{k=1}^{n-1}\frac{1}{|1-\epsilon_k|}\right)^2, \end{aligned}$$

$$\begin{aligned} |C_2|+|D_2| &\le \frac{2}{n^5}\sum_{\substack{1\le k,\ell<n\\ k\ne\ell}}\frac{2\,|\Lambda_X(k,0,\ell)|}{|1-\epsilon_k|\cdot|1-\epsilon_\ell|}+\frac{4}{n^5}\sum_{k=1}^{n-1}\frac{|\Lambda_X(k,0,k)|}{|1-\epsilon_k|^2} \\ &\le \frac{4(n+1)^{\frac{3}{2}}}{n^4}\left(\sum_{k=1}^{n-1}\frac{1}{|1-\epsilon_k|}\right)^2. \end{aligned}$$

Therefore

$$\begin{aligned} |B+C_1+C_2+D_2| &\le (n+1)^{\frac{1}{2}}(|B|+|C_1|)+(|C_2|+|D_2|) \\ &\le \frac{12(n+1)^{\frac{3}{2}}}{n^4}\left(\sum_{k=1}^{n-1}\frac{1}{|1-\epsilon_k|}\right)^2 \\ &= O\left(n^{-\frac{1}{2}}(\log n)^2\right) \quad \text{as } n\longrightarrow\infty, \qquad (5.11) \end{aligned}$$

since $\sum_{k=1}^{n-1}\frac{1}{|1-\epsilon_k|}\le n\log n$ (see [**HJ88**, p. 162], for example).

The result now follows by substituting the asymptotic forms (5.6), (5.10), and (5.11) in (5.2). □

There is no loss of generality in Theorem 9 arising from the constraints $|s|<1$ and $|t|<1$, since any sequence A satisfies $A_{r+1}=A_r$ for all r.

6. Asymptotic Merit Factor Calculation

In this section we apply Lemmas 3 and 4 to an m-sequence X, using Theorem 9 to evaluate the resulting asymptotic form. In this way we calculate the asymptotic merit factor of $N(X)$ and $P(X)$.

We firstly note the following result, under which $o(\sqrt{n})$ elements of a length n sequence can be changed by a bounded amount without altering the asymptotic reciprocal merit factor:

Proposition 10 ([**SJP09**, Proposition 1]). *Let $\{A(n)\}$ and $\{B(n)\}$ be sets of sequences, where each of $A(n)$ and $B(n)$ has length n. Suppose that, for each n, all elements of $A(n)$ and $B(n)$ are bounded in magnitude by a constant independent of n. Suppose further that, as $n \longrightarrow \infty$, the number of nonzero elements of $B(n)$ is $o(\sqrt{n})$ and that $F(A(n)) = O(1)$ and $E(A(n)) = \Omega(n)$.*[1] *Then, as $n \longrightarrow \infty$, the elementwise sequence sums $\{A(n) + B(n)\}$ satisfy*

$$\frac{1}{F(A(n)+B(n))} = \frac{1}{F(A(n))}(1+o(1)).$$

We now prove the main results of the paper as Theorems 11 and 12.

Theorem 11. *Let X be an m-sequence of length $n = 2^m - 1$, and let r be a real number. Then*

$$\lim_{n \longrightarrow \infty} F((N(X))_{\widetilde{r}}) = 3.$$

Proof. Let $N(X) = (y_0, y_1, \dots, y_{2n-1})$ and write $\rho := \lfloor rn \rfloor / n$. By the definition of negaperiodic rotation,

$$[(N(X))_{\widetilde{r}}]_j = \begin{cases} y_{(j+\lfloor 2nr \rfloor) \bmod 2n} & \text{for } 0 \le j < 2n - \lfloor 2nr \rfloor \\ -y_{(j+\lfloor 2nr \rfloor) \bmod 2n} & \text{for } 2n - \lfloor 2nr \rfloor \le j < 2n, \end{cases}$$

$$[(N(X))_{\widetilde{\rho}}]_j = \begin{cases} y_{(j+2\lfloor nr \rfloor) \bmod 2n} & \text{for } 0 \le j < 2n - 2\lfloor nr \rfloor \\ -y_{(j+2\lfloor nr \rfloor) \bmod 2n} & \text{for } 2n - 2\lfloor nr \rfloor \le j < 2n. \end{cases}$$

For each n, either $\lfloor 2nr \rfloor = 2\lfloor nr \rfloor$, in which case the length $2n$ sequences $(N(X))_{\widetilde{r}}$ and $(N(X))_{\widetilde{\rho}}$ are identical, or else $\lfloor 2nr \rfloor = 2\lfloor nr \rfloor + 1$, in which case $(N(X))_{\widetilde{r}}$ and $(N(X))_{\widetilde{\rho}}$ share a common subsequence of length $2n-1$. So by Proposition 10, it is sufficient to show that $\lim_{n \longrightarrow \infty} F((N(X))_{\widetilde{\rho}}) = 3$.

Let Z be the 2-decimation of X. By Lemma 3, as $n \longrightarrow \infty$ we have

$$\frac{1}{n^2} \sum_{|u|<2n} [C_{(N(X))_{\widetilde{\rho}}}(u)]^2$$

(6.1)

$$= \frac{1}{n^2} \sum_{|u|<n} \left([C_{Z_r}(u) + C_{Z_{r+\delta}}(u)]^2 + [C_{Z_r, Z_{r+\delta}}(u) - C_{Z_{r+\delta}, Z_{r+2\delta}}(u) + O(1)]^2 \right),$$

where $\delta = \delta(n) := \frac{n+1}{2n}$. Ignoring temporarily the term $O(1)$, the six terms in the expansion of the right hand side of (6.1) each take the form

$$\frac{1}{n^2} \sum_{|u|<n} C_{Z_{r+i\delta}, Z_{r+(i+k)\delta}}(u) C_{Z_{r+j\delta}, Z_{r+(j+k)\delta}}(u)$$

for some $i, j, k \in \{0, 1\}$. Furthermore, $Z_{r+i\delta}$ is also an m-sequence, by Lemma 1 (i) and (ii). We can therefore apply Theorem 9 with $X = Z_{r+i\delta}$ and $s(n) = k\delta(n)$ and $t(n) = (j-i)\delta(n)$ (noting that $n\delta(n)$ is integer for each n and that $\delta(n) =$

[1] We use the notation o, O, and Ω to compare the growth rates of functions $f(n)$ and $g(n)$ from $\mathbb{N}$ to $\mathbb{R}^+$ in the following standard way: $f(n) = o(g(n))$ means that $f(n)/g(n) \to 0$ as $n \to \infty$; $f(n) = O(g(n))$ means that there is a constant c, independent of n, for which $f(n) \le cg(n)$ for all sufficiently large n; and $f(n) = \Omega(g(n))$ means that $g(n) = O(f(n))$.

$\frac{1}{2}+O(n^{-1})$) to show that, as $n \longrightarrow \infty$, the terms in the expansion of the right hand side of (6.1) are given by

$$\frac{1}{n^2}\sum_{|u|<n} C_{Z_{r+i\delta},Z_{r+(i+k)\delta}}(u)C_{Z_{r+j\delta},Z_{r+(j+k)\delta}}(u)$$

$$= \tfrac{1}{3}+2\left(\tfrac{|k|}{2}-\tfrac{1}{2}\right)^2+2\left(\tfrac{|j-i|}{2}-\tfrac{1}{2}\right)^2+O\left(n^{-\frac{1}{2}}(\log n)^2\right). \tag{6.2}$$

Since the right hand side of (6.2) is $O(1)$ as $n \longrightarrow \infty$, by the Cauchy-Schwarz inequality the additional contribution arising from the inclusion of the previously ignored term $O(1)$ in (6.1) is $O(n^{-\frac{1}{2}})$, which can be neglected. Using (6.2) to evaluate the expansion of the right hand side of (6.1), we then find that

$$\lim_{n\longrightarrow\infty}\frac{1}{(2n)^2}\sum_{|u|<2n}\left[C_{(N(X))_{\tilde{\rho}}}(u)\right]^2=\frac{4}{3},$$

and the required result follows from (2.1). □

Theorem 12. *Let X be an m-sequence of length $n=2^m-1$, and let r be a real number. Then*

$$\lim_{n\longrightarrow\infty}F((P(X))_r)=3.$$

Proof. The proof is similar to that of Theorem 11. Write $\rho := \lfloor rn\rfloor/n$. The length $4n$ sequences $(P(X))_r$ and $(P(X))_\rho$ share a common subsequence of length at least $4n-3$, and so by Proposition 10 it is sufficient to show that $\lim_{n\longrightarrow\infty}F((P(X))_\rho)=3$.

Let Z be the 4-decimation of X. By Lemma 4, as $n \longrightarrow \infty$ we have

$$\frac{1}{n^2}\sum_{|u|<4n}\left[C_{(P(X))_\rho}(u)\right]^2$$

$$=\frac{1}{n^2}\sum_{k=0}^{3}\sum_{|u|<n}\left(\sum_{i=0}^{3}(-1)^{\frac{ik(i+k+2)}{2}}C_{Z_{r+i\delta},Z_{r+(i+k)\delta}}(u)+O(1)\right)^2, \tag{6.3}$$

where $\delta=\delta(n):=\frac{n+1}{4n}$ (since $n\equiv 3 \pmod 4$ for all $n>1$). $Z_{r+i\delta}$ is an m-sequence, by Lemma 1 (i) and (ii). We can therefore apply Theorem 9 with $X=Z_{r+i\delta}$ and $s(n)=k\delta(n)$ and $t(n)=(j-i)\delta(n)$, where $i,j,k\in\{0,1,2,3\}$, to show that

$$\frac{1}{n^2}\sum_{|u|<n} C_{Z_{r+i\delta},Z_{r+(i+k)\delta}}(u)C_{Z_{r+j\delta},Z_{r+(j+k)\delta}}(u)$$

$$=\tfrac{1}{3}+2\left(\tfrac{|k|}{4}-\tfrac{1}{2}\right)^2+2\left(\tfrac{|j-i|}{4}-\tfrac{1}{2}\right)^2+O\left(n^{-\frac{1}{2}}(\log n)^2\right) \tag{6.4}$$

as $n \longrightarrow \infty$. Expand the right hand side of (6.3) and substitute from (6.4), neglecting the contribution of the term $O(1)$ in (6.3) as in the proof of Theorem 11, to give

$$\lim_{n\longrightarrow\infty}\frac{1}{n^2}\sum_{|u|<4n}\left[C_{(P(X))_\rho}(u)\right]^2$$

$$=\sum_{0\le k,i,j\le 3}(-1)^{\frac{ik(i+k+2)+jk(j+k+2)}{2}}\left(\tfrac{1}{3}+2\left(\tfrac{|k|}{4}-\tfrac{1}{2}\right)^2+2\left(\tfrac{|j-i|}{4}-\tfrac{1}{2}\right)^2\right).$$

Direct evaluation of the sum over k, i, and j reveals that

$$\lim_{n\longrightarrow\infty}\frac{1}{(4n)^2}\sum_{|u|<4n}\big[C_{(P(X))_\rho}(u)\big]^2=\frac{4}{3},$$

and the required result follows from (2.1). □

7. Conclusion

Comparison of Theorems 11 and 12 with Theorem 2 shows that the graphical property noted at the end of Section 4 for Legendre sequences also holds for m-sequences. These results suggest the possibility of three general properties of odd-length binary sequence families X:

(a) there is a constant $c = c(X)$ for which

$$\lim_{n\longrightarrow\infty}F((N(X))_{\widetilde{r+c}})=\lim_{n\longrightarrow\infty}F(X_r)\quad\text{for all } r, \tag{7.1}$$

provided both limits exist.

(b) there is a constant $d = d(X)$ for which

$$\lim_{n\longrightarrow\infty}F((P(X))_{r+d})=\lim_{n\longrightarrow\infty}F(X_r)\quad\text{for all } r, \tag{7.2}$$

provided both limits exist.

(c)

$$\lim_{n\longrightarrow\infty}F((N(X))_{\tilde{r}})=\lim_{n\longrightarrow\infty}F((P(X))_r),\quad\text{for all } r, \tag{7.3}$$

provided both limits exist.

However we now show numerically that at least one of these proposed properties, namely (7.3), appears not to hold in general.

The *Rudin-Shapiro sequence pair* $A^{(m)}$, $B^{(m)}$ of length 2^m is defined recursively by

$$\begin{cases}A^{(m)}:=A^{(m-1)};B^{(m-1)},\\ B^{(m)}:=A^{(m-1)};-B^{(m-1)},\end{cases}$$

where $A^{(0)}=B^{(0)}=(+)$. Littlewood calculated the asymptotic merit factor of each sequence $A^{(m)}$ and $B^{(m)}$ of a Rudin-Shapiro pair to be 3 in 1968:

Theorem 13 ([**Lit68**]). *Let $A^{(m)}$, $B^{(m)}$ be a Rudin-Shapiro pair of length $n = 2^m$. Then*

$$F(A^{(m)})=F(B^{(m)})=\frac{3}{1-\left(-\frac{1}{2}\right)^m}.$$

Remove the initial element of the sequence $A^{(m)}$ to produce a sequence ${A_1}^{(m)}$ of odd length 2^m-1 (whose asymptotic merit factor remains 3, by Proposition 10). It appears from the data shown in Figure 2 that

$$F(N({A_1}^{(m)}))\simeq 3\quad\text{and}\quad F(P({A_1}^{(m)}))\simeq 1.5\quad\text{for large } m, \tag{7.4}$$

which in turn implies that (7.3) is false for $X=A_1^{(m)}$ and $r=0$.

We propose the following open problems:

(1) Can the apparent property (7.4) be proved?

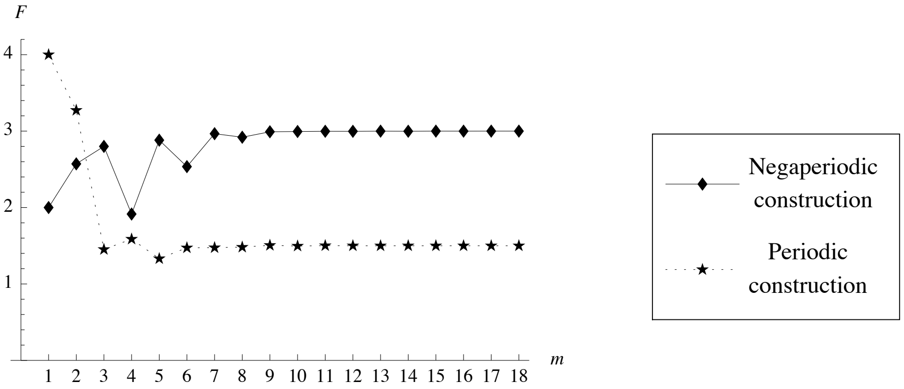

FIGURE 2. Variation of merit factor of $N(A_1^{(m)})$ and $P(A_1^{(m)})$ with m, where $A_1^{(m)}$ is the Rudin-Shapiro sequence $A^{(m)}$ of length 2^m with the initial element removed.

(2) For $r \neq 0$, how does the asymptotic value of $F((A_1^{(m)})_r)$, $F((N(A_1^{(m)}))_{\widetilde{r}})$, and $F((P(A_1^{(m)}))_r)$ behave?
(3) For which odd-length binary sequence families X do properties (7.1), (7.2), and (7.3) hold?

In closing, we remark that the asymptotic value of $F((N(X))_{\widetilde{r}})$ and $F((P(X))_r)$ can be calculated in the case that X is a Jacobi sequence or modified Jacobi sequence of length pq, by following the method of [**JJH91**] and deriving the corresponding version of Theorem 9 for such a sequence. Under the same conditions on the relative growth rate of the primes p and q as in [**JJH91**, Eq. 5.11], the resulting asymptotic merit factor graphs are identical to the right graph of Figure 1. The special cases $r = 0$ and $r = \frac{1}{2}$ of this result were proved for $p \equiv q \equiv 1 \pmod 4$ by Xiong and Hall [**XH08**, Thm. 5.2].

References

[BCH85] G.F.M. Beenker, T.A.C.M. Claasen, and P.W.C. Hermens, *Binary sequences with a maximally flat amplitude spectrum*, Philips J. Res. **40** (1985), 289–304.

[BCJ04] P. Borwein, K.-K.S. Choi, and J. Jedwab, *Binary sequences with merit factor greater than 6.34*, IEEE Trans. Inf. Theory **50** (2004), 3234–3249.

[GG05] S.W. Golomb and G. Gong, *Signal design for good correlation: for wireless communication, cryptography, and radar*, Cambridge University Press, New York, NY, 2005.

[Gol67] S.W. Golomb, *Shift register sequences*, Holden-Day, Inc., San Francisco, CA, 1967.

[HJ88] T. Høholdt and H.E. Jensen, *Determination of the merit factor of Legendre sequences*, IEEE Trans. Inf. Theory **34** (1988), 161–164.

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

[Jed08] ———, *What can be used instead of a Barker sequence?*, Contemp. Math. **461** (2008), 153–178.

[JH89] H.E. Jensen and T. Høholdt, *Binary sequences with good correlation properties*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-5 Proceedings (L. Huguet and A. Poli, eds.), Lecture Notes in Computer Science, vol. 356, Springer-Verlag, Berlin, 1989, pp. 306–320.

[JJH91] J.M. Jensen, H.E. Jensen, and T. Høholdt, *The merit factor of binary sequences related to difference sets*, IEEE Trans. Inf. Theory **37** (1991), 617–626.

[Lit68] J.E. Littlewood, *Some problems in real and complex analysis*, Heath Mathematical Monographs, D.C. Heath and Company, Lexington, MA, 1968.

[SJP09] K.-U. Schmidt, J. Jedwab, and M.G. Parker, *Two binary sequence families with large merit factor*, Adv. Math. Commun. **3** (2009), 135–156.

[XH08] T. Xiong and J.I. Hall, *Construction of even length binary sequences with asymptotic merit factor 6*, IEEE Trans. Inf. Theory **54** (2008), 931–935.

Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC, Canada V5A 1S6
E-mail address: jed@sfu.ca

Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC, Canada V5A 1S6
E-mail address: kuschmidt@sfu.ca