Appended m-sequences with merit factor greater than 3.34

Jonathan Jedwab   Kai-Uwe Schmidt

12 April 2010 (revised 31 May 2010)

Abstract

We consider the merit factor of binary sequences obtained by appending an initial fraction of an m-sequence to itself. We show that, for all sufficiently large n, there is some rotation of each m-sequence of length n that has merit factor greater than 3.34 under suitable appending. This is the first proof that the asymptotic merit factor of a binary sequence family can be increased under appending. We also conjecture, based on numerical evidence, that *each* rotation of an m-sequence has asymptotic merit factor greater than 3.34 under suitable appending. Our results indicate that the effect of appending on the merit factor is strikingly similar for m-sequences as for rotated Legendre sequences.

1 Introduction

A *binary sequence* A of length n is an n-tuple $(a_0, a_1, \ldots, a_{n-1})$, where each a_j takes the value -1 or 1. The *aperiodic autocorrelation* of the binary sequence A at shift u is defined to be

$$C_A(u) := \sum_{j=0}^{n-u-1} a_j a_{j+u} \quad \text{for } u = 0, 1, \ldots, n-1,$$

and, provided that $n \geq 2$, its *merit factor* is

$$F(A) := \frac{n^2}{2\sum_{u=1}^{n-1} [C_A(u)]^2}.$$

The merit factor is important both practically and theoretically. For example, 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 merit factor of binary sequences is also 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

J. Jedwab and K.-U. Schmidt and are with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada.

J. Jedwab is supported by NSERC of Canada.

K.-U. Schmidt is supported by Deutsche Forschungsgemeinschaft (German Research Foundation).

Email: jed@sfu.ca, kuschmidt@sfu.ca.

problems). The general objective is to understand the behaviour, as $n \longrightarrow \infty$, of the optimal merit factor $F(A)$ as A ranges over the set of all 2^n binary sequences of length n.

The only non-trivial infinite families of binary sequences for which the asymptotic merit factor is known are: Legendre sequences, m-sequences, Rudin-Shapiro sequences, and some generalisations of these three families. The largest proven asymptotic merit factor of a binary sequence family is 6, which is attained by rotated Legendre sequences (see Theorem 13).

There is considerable numerical evidence that an asymptotic merit factor greater than 6 can be achieved [KN99], [KP04], [BCJ04]. The idea of [BCJ04], based on earlier work [KN99], is to start with a near-optimal rotation of a Legendre sequence (which has asymptotic merit factor close to 6) and append an initial fraction of the sequence to itself. Based on partial explanations and extensive numerical computations, [BCJ04] exhibits a binary sequence family that apparently has asymptotic merit factor greater than 6.34, although a proof for this has not yet been found.

In this paper we apply the idea of sequence appending to m-sequences and prove, for the first time, that the asymptotic merit factor of a binary sequence family can be increased under appending. The asymptotic merit factor of all m-sequences is known to equal 3 (see Theorem 3). We show that, for all sufficiently large n, there is some rotation of an m-sequence of length n that has merit factor greater than 3.34 under suitable appending. Our analysis makes critical use of the "shift-and-add" property of m-sequences (see Lemma 1 (ii)). We also conjecture, based on numerical evidence, that *each* rotation of an m-sequence has asymptotic merit factor greater than 3.34 under suitable appending. Our results reveal that the effect of appending is strikingly similar for m-sequences as for rotated Legendre sequences; this is discussed in the final section of the paper.

2 Notation

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

Given a binary sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n, we denote by $[A]_j$ 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 binary sequences of length n and m, respectively. The *concatenation* $A; B$ of A and B is the length $n+m$ binary sequence given by

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

Let r and t be real numbers, where $t \in [0,1]$. Following [BCJ04], the *rotation* A_r of A by a fraction r of its length is the binary sequence of length n given by

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

and the *truncation* A^t of A by a fraction t of its length is the binary sequence of length $\lfloor tn \rfloor$ given by

$$[A^t]_j := a_j \quad \text{for } 0 \le j < \lfloor tn \rfloor.$$

We also use the standard definition of the *periodic autocorrelation* of the binary sequence $A = (a_0, a_1, \ldots, a_{n-1})$ at an integer shift u, namely

$$R_A(u) := \sum_{j=0}^{n-1} a_j a_{(j+u) \bmod n}. \tag{1}$$

3 Properties of 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* $Y = (y_0, y_1, \ldots, y_{n-1})$ of length $n = 2^m - 1$ (for $m \geq 2$) is defined by

$$y_j := (-1)^{\mathrm{Tr}(\beta\alpha^j)} \quad \text{for } 0 \leq j < n \tag{2}$$

for some primitive element α of $\mathrm{GF}(2^m)$ and some nonzero element β of $\mathrm{GF}(2^m)$. By writing β as a power of α, it is seen that different choices for β correspond to different rotations of the sequence defined by a particular β. This implies that each rotation of an m-sequence is an m-sequence, as noted in Lemma 1 (i) below. For each $n = 2^m - 1$, there are exactly $n\phi(n)/m$ distinct m-sequences [GG05, Cor. 4.7], where ϕ is Euler's totient function (there are n choices for β, and $\phi(n)/m$ choices for α that arise by taking one representative of each conjugacy class of the $\phi(n)$ primitive elements 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 $Y = (y_0, y_1, \ldots, y_{n-1})$ be an m-sequence of length $n = 2^m - 1$, as in* (2)*.*

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

(ii) ([Gol67, p. 44, Thm. 4.3]) *There is a permutation σ of $\{1, 2, \ldots, n-1\}$, determined by the primitive element α in* (2)*, for which*

$$y_j y_{(j+u) \bmod n} = y_{(j+\sigma(u)) \bmod n} \quad \textit{for } 1 \leq u < n \textit{ and } 0 \leq j < n. \tag{3}$$

(iii) ([Gol67, p. 45]) *The periodic autocorrelation of Y satisfies*

$$R_Y(u) = \begin{cases} n & \textit{for } u \equiv 0 \pmod{n} \\ -1 & \textit{otherwise.} \end{cases}$$

Given an m-sequence Y of length n, Sarwate [Sar84a] computed $\mathbb{E}_k[1/F(Y_{k/n})]$ (throughout this paper, $\mathbb{E}_k$ denotes expectation over $k \in \{0, 1, \ldots, n-1\}$, where all such k occur with equal probability).

Theorem 2 (Sarwate [Sar84a])**.** *Let Y be an m-sequence of length $n = 2^m - 1$. Then*

$$\mathbb{E}_k\left[\frac{1}{F(Y_{k/n})}\right] = \frac{(n-1)(n+4)}{3n^2}.$$

As a consequence, there is some rotation of an m-sequence Y of length n having merit factor at least $3n^2/((n-1)(n+4))$, which asymptotically equals 3. This suggests the possibility that a particular rotation of an m-sequence has asymptotic merit factor greater than 3, but Jensen and Høholdt [JH89] showed that this is impossible.

Theorem 3 (Jensen and Høholdt [JH89]). *Let Y be an m-sequence of length $n = 2^m - 1$. Then*

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

(The limit in Theorem 3 is taken over all n of the form $n = 2^m - 1$ (for $m \geq 2$) and, for each such n, one of the $n\phi(n)/m$ different m-sequences is selected. The theorem states that the limit of $F(Y)$ is always 3, regardless of which m-sequence is chosen for a particular n.)

We shall need an upper bound on the aperiodic autocorrelation of truncated m-sequences. Given an m-sequence Y of length $n = 2^m - 1$, Sarwate [Sar84b] established that

$$|C_Y(u)| \leq 1 + \tfrac{2}{\pi}\sqrt{n+1}\log\left(\tfrac{4n}{\pi}\right) \quad \text{for } 1 \leq u < n. \tag{4}$$

We will now show that Lemma 1 (ii) implies that the same bound also holds for truncated m-sequences.

Lemma 4. *Let Y be an m-sequence of length $n = 2^m - 1$, and let ℓ be an integer satisfying $2 \leq \ell \leq n$. Then*

$$|C_{Y^{\ell/n}}(u)| \leq 1 + \tfrac{2}{\pi}\sqrt{n+1}\log\left(\tfrac{4n}{\pi}\right) \quad \textit{for } 1 \leq u < \ell.$$

Proof. Let α be the primitive element of $\mathrm{GF}(2^m)$ appearing in the definition of $Y = (y_0, y_1, \ldots, y_{n-1})$ given in (2), and let σ be the permutation determined by α satisfying (3). Now pick an integer u satisfying $1 \leq u < \ell$. Applying Lemma 1 (ii) twice, we find that

$$\begin{aligned} C_{Y^{\ell/n}}(u) &= \sum_{j=0}^{\ell-u-1} y_j y_{j+u} \\ &= \sum_{j=0}^{\ell-u-1} y_{(j+\sigma(u)) \bmod n} \\ &= \sum_{j=0}^{\ell-u-1} y_{(j+\sigma(u)-\sigma(n-\ell+u)) \bmod n}\, y_{(j+\sigma(u)-\sigma(n-\ell+u)+n-\ell+u) \bmod n} \\ &= C_{Y_{k/n}}(n-\ell+u) \qquad \text{for } k = \sigma(u) - \sigma(n-\ell+u). \end{aligned}$$

Since $Y_{k/n}$ is an m-sequence by Lemma 1 (i), the result follows from (4). $\square$

4 An Existence Result on the Merit Factor of Appended m-Sequences

In this section we prove a generalisation of Theorem 2 for appended m-sequences. We then conclude that, for all sufficiently large m, given a primitive element α of $\mathrm{GF}(2^m)$ there exists an m-sequence Y of length $n = 2^m - 1$ of the form (2) and a real number t such that $F(Y; Y^t) > 3.34$.

We begin by proving the following lemma on sums of elements of an m-sequence. This generalises to all nonnegative integers δ a result previously given by Lindholm [Lin68, Eq. (6e)] for $\delta \leq n$.

Lemma 5. *Let $Y = (y_0, y_1, \ldots, y_{n-1})$ be an m-sequence of length $n = 2^m - 1$. Given nonnegative integers k and δ, define*

$$S_Y(k, \delta) := \sum_{j=0}^{\delta-1} y_{(k+j) \bmod n}. \tag{5}$$

Then

$$n\,\mathbb{E}_k[(S_Y(k,\delta))^2] = \delta(n-\delta+1) + a(n+1)\,(2\delta - n(a+1))\,,$$

where $a = \lfloor \frac{\delta-1}{n} \rfloor$.

Proof. From the definition (5) of $S_Y(k, \delta)$ we have

$$\begin{aligned} n\,\mathbb{E}_k[(S_Y(k,\delta))^2] &= \sum_{k=0}^{n-1}\sum_{i=0}^{\delta-1}\sum_{j=0}^{\delta-1} y_{(k+i) \bmod n}\, y_{(k+j) \bmod n} \\ &= \sum_{i=0}^{\delta-1}\sum_{j=0}^{\delta-1} R_Y(i-j) \end{aligned}$$

by rearranging the summation and by the definition (1) of the periodic autocorrelation. Further manipulations give

$$\begin{aligned} n\,\mathbb{E}_k[(S_Y(k,\delta))^2] &= \sum_{v=-(\delta-1)}^{\delta-1} (\delta - |v|)\, R_Y(v) \\ &= \delta\, R_Y(0) + 2\sum_{v=1}^{\delta-1} v\, R_Y(\delta - v) \end{aligned}$$

since for every binary sequence A we have $R_A(v) = R_A(-v)$ for all v. Now from Lemma 1 (iii) we find that

$$\begin{aligned} n\,\mathbb{E}_k[(S_Y(k,\delta))^2] &= \delta n - 2\sum_{v=1}^{\delta-1} v + 2(n+1) \sum_{\substack{v=1 \\ v\equiv\delta \pmod n}}^{\delta-1} v \\ &= \delta n - \delta(\delta-1) + 2(n+1) \sum_{\substack{v=1 \\ v\equiv\delta \pmod n}}^{\delta-1} v. \end{aligned} \tag{6}$$

Writing $a = \lfloor \frac{\delta-1}{n} \rfloor$, we have

$$\begin{aligned} \sum_{\substack{v=1 \\ v\equiv\delta \pmod n}}^{\delta-1} v &= \sum_{j=1}^{a} (\delta - jn) \\ &= a\delta - \tfrac{1}{2} na(a+1), \end{aligned}$$

which after combination with (6) proves the lemma. □

We now apply the preceding lemma to prove the following result, in which the sequence $Y_{k/n}; (Y_{k/n})^{\ell/n}$ is obtained by rotating the m-sequence Y by k elements and then appending the resulting first ℓ elements.

Theorem 6. *Let Y be an m-sequence of length $n = 2^m - 1$, and let ℓ be an integer satisfying $0 \le \ell \le n$. Then*

$$\mathbb{E}_k\left[\frac{1}{F(Y_{k/n}; (Y_{k/n})^{\ell/n})}\right] = \frac{(n+\ell)(n+\ell-1)(n-2\ell+4) + 12(n+1)\ell(\ell-1)}{3n(n+\ell)^2}.$$

Proof. Let α be the primitive element of $\mathrm{GF}(2^m)$ appearing in the definition of $Y = (y_0, y_1, \dots, y_{n-1})$ given in (2), and let σ be the permutation determined by α satisfying (3). Then, by Lemma 1 (ii), for each u satisfying $1 \le u < n + \ell$ and $u \neq \ell$, we have

$$\begin{aligned} C_{Y_{k/n};(Y_{k/n})^{\ell/n}}(n+\ell-u) &= \sum_{j=0}^{u-1} y_{(k+j) \bmod n}\, y_{(k+j+n+\ell-u) \bmod n} \\ &= \sum_{j=0}^{u-1} y_{(\tau(k)+j) \bmod n} \\ &= S_Y(\tau(k), u), \end{aligned} \tag{7}$$

where $\tau(k) := k + \sigma((n+\ell-u) \bmod n)$ and $S_Y(k,\delta)$ is defined in (5). We also have

$$C_{Y_{k/n};(Y_{k/n})^{\ell/n}}(n) = \ell, \tag{8}$$

using the convention that $C_A(n) = 0$ for all binary sequences A of length n. Now, since $k \mapsto \tau(k) \bmod n$ is a permutation of $\{0, 1, \dots, n-1\}$ for each u, (8) and application of Lemma 5 to (7) give

$$n\,\mathbb{E}_k\left[\left(C_{Y_{k/n};(Y_{k/n})^{\ell/n}}(n+\ell-u)\right)^2\right] = \begin{cases} n\ell^2 & \text{for } u = \ell \\ u(n-u+1) & \text{for } 1 \le u \le n \text{ and } u \neq \ell \\ u(n-u+1) + 2(n+1)(u-n) & \text{for } n < u < n+\ell. \end{cases}$$

We therefore obtain

$$\begin{aligned} \mathbb{E}_k\left[\frac{n(n+\ell)^2}{2F(Y_{k/n}; (Y_{k/n})^{\ell/n})}\right] &= \sum_{u=1}^{n+\ell-1} n\,\mathbb{E}_k\left[\left(C_{Y_{k/n};(Y_{k/n})^{\ell/n}}(n+\ell-u)\right)^2\right] \\ &= \sum_{\substack{u=1 \\ u \neq \ell}}^{n+\ell-1} u(n-u+1) + n\ell^2 + \sum_{u=n+1}^{n+\ell-1} 2(n+1)(u-n) \\ &= \tfrac{1}{6}(n+\ell)(n+\ell-1)(n-2\ell+4) + 2(n+1)\ell(\ell-1), \end{aligned}$$

proving the theorem. ∎

Notice that Theorem 2 arises as the special case $\ell = 0$ of Theorem 6. It follows from Theorem 6 that, for every m-sequence Y and integer ℓ satisfying $0 \le \ell \le n$, there exists an integer k such that

$$F(Y_{k/n}; (Y_{k/n})^{\ell/n}) \ge \frac{3n(n+\ell)^2}{(n+\ell)(n+\ell-1)(n-2\ell+4)+12(n+1)\ell(\ell-1)}.$$

Writing $t = \frac{\ell}{n}$, taking the infimum limit as $n \longrightarrow \infty$, and using Lemma 1 (i), we obtain the following asymptotic result.

Corollary 7. *Let $t \in [0,1]$ be a real number. For each integer m and for each primitive element α of $\mathrm{GF}(2^m)$, there exists a nonzero $\beta \in \mathrm{GF}(2^m)$ such that the m-sequence Y of length $n = 2^m - 1$ defined in* (2) *satisfies*

$$\liminf_{n \longrightarrow \infty} F(Y; Y^t) \ge \frac{3(1+t)^2}{1+9t^2-2t^3}.$$

In particular,

$$\liminf_{n \longrightarrow \infty} F(Y; Y^t) > 3.3420653 \quad \textit{for } t = 0.1157494.$$

The second statement in the corollary implies that, for all sufficiently large m, given a primitive element α of $\mathrm{GF}(2^m)$, we can pick an m-sequence Y of length $n = 2^m - 1$ of the form (2) such that $F(Y; Y^t) > 3.34$ for $t = 0.1157494$.

5 A Conjecture on the Merit Factor of Appended m-Sequences

The results of the previous section imply that, for each sufficiently large $n = 2^m - 1$, we can choose an m-sequence Y of length n such that the maximum of $F(Y; Y^t)$ over $t \in [0,1]$ is greater than 3.34. In this section and in the following section we shall present compelling evidence, and therefore conjecture, that

$$\lim_{n \longrightarrow \infty} F(Y; Y^t) = \frac{3(1+t)^2}{1+9t^2-2t^3} \quad \text{for } t \in [0,1), \tag{9}$$

regardless of the choice of the m-sequence Y for each particular n. Subject to this conjecture, the asymptotic maximum of $F(Y; Y^t)$ over $t \in [0,1)$ is approximately 3.34, regardless of the choice of the m-sequence Y for each particular n.

We shall first prove the following theorem, which allows us to replace the conjecture (9) by a simpler one. A result similar to Theorem 8, namely [BCJ04, Thm. 6.4], is known to hold for Legendre sequences.

Theorem 8. *Let Y be an m-sequence of length $n = 2^m - 1$, and let $t \in (0,1)$ be a real number. Then, as $n \longrightarrow \infty$,*

$$\frac{1}{F(Y; Y^t)} \sim 2\left(\frac{t}{1+t}\right)^2 \left(\frac{1}{F(Y^t)} + 1\right) + \left(\frac{1-t}{1+t}\right)^2 \frac{1}{F((Y_t)^{1-t})}.$$

Proof. Write $Y = (y_0, y_1, \dots, y_{n-1})$ and $\ell := \lfloor tn \rfloor$. By definition we have $Y^t = (y_0, y_1, \dots, y_{\ell-1})$. Now define $Y' = (y_\ell, y_{\ell+1}, \dots, y_{n-1})$, so that $Y = Y^t; Y'$. Then by the definition (1) of the periodic autocorrelation we have

$$C_{Y;Y^t}(u) = \begin{cases} R_Y(u) + C_{Y^t}(u) & \text{for } 1 \le u < \ell \\ R_Y(\ell) & \text{for } u = \ell \\ R_Y(u) - C_{Y'}(n-u) & \text{for } \ell < u < n \\ \ell & \text{for } u = n \\ C_{Y^t}(u-n) & \text{for } n < u < n+\ell. \end{cases}$$

In what follows, we will assume that n is large enough such that $2 \le \ell \le n-2$, in which case all of the above ranges for u are nonempty. Since by Lemma 1 (iii), $R_Y(u) = -1$ for $1 \le u < n$, we then obtain

$$\begin{aligned} \frac{(n+\ell)^2}{2F(Y;Y^t)} &= \sum_{u=0}^{n+\ell-1} [C_{Y;Y^t}(u)]^2 \\ &= \sum_{u=1}^{\ell-1} [C_{Y^t}(u) - 1]^2 + 1 + \sum_{u=1}^{n-\ell-1} [C_{Y'}(u) + 1]^2 + \ell^2 + \sum_{u=1}^{\ell-1} [C_{Y^t}(u)]^2 \\ &= \frac{\ell^2}{F(Y^t)} + \frac{(n-\ell)^2}{2F(Y')} + \ell^2 + n - 1 - 2\sum_{u=1}^{\ell-1} C_{Y^t}(u) + 2\sum_{u=1}^{n-\ell-1} C_{Y'}(u). \end{aligned} \tag{10}$$

Now by comparing Y' with $(Y_t)^{1-t}$, we find that

$$Y' = \begin{cases} (Y_t)^{1-t} & \text{if } tn \text{ is integer} \\ (Y_t)^{1-t}; y_{n-1} & \text{otherwise.} \end{cases}$$

This gives

$$\left| C_{Y'}(u) - C_{(Y_t)^{1-t}}(u) \right| \le 1 \quad \text{for } 0 \le u < n - \ell \tag{11}$$

with the convention that $C_A(s) = 0$ for each length s binary sequence A. Thus, since Y_t is an m-sequence, we conclude from Lemma 4 that the last two sums in (10) are $O(n^{\frac{3}{2}} \log n)$ as $n \longrightarrow \infty$. Also from (11) and Lemma 4 we find that, as $n \longrightarrow \infty$,

$$\frac{(n-\ell)^2}{2F(Y')} = \frac{(\lfloor (1-t)n \rfloor)^2}{2F((Y_t)^{1-t})} + O(n^{\frac{3}{2}} \log n).$$

Hence, since $\ell \sim tn$, we obtain from (10) the asymptotic relationship

$$\frac{(1+t)^2 n^2}{2F(Y;Y^t)} \sim \frac{t^2 n^2}{F(Y^t)} + \frac{(1-t)^2 n^2}{2F((Y_t)^{1-t})} + t^2 n^2,$$

as required. □

Theorem 8 and Lemma 1 (i) imply that, in order to find the asymptotic merit factor of an appended m-sequence $Y; Y^t$ for all $t \in (0,1)$, it is sufficient to know the asymptotic value of $t^2/F(Z^t)$ for all m-sequences Z and for all $t \in (0,1)$. Numerical computations suggest that, for each long m-sequence Y, the curve $1/F(Y^t)$ for $t \in (0,1]$ can be fitted very well by a linear function. This leads us to the following conjecture.

Conjecture 9. *Let Y be an m-sequence of length $n = 2^m - 1$, and let $t \in (0, 1]$ be a real number. Then, $\lim_{n\to\infty}(t^2/F(Y^t))$ is well-defined and*

$$\lim_{n \longrightarrow \infty} \frac{t^2}{F(Y^t)} = t^2(1 - \tfrac{2}{3}t).$$

We now use Theorem 8 to show that the conjectured asymptotic form (9) of the merit factor of appended m-sequences is implied by Conjecture 9.

Corollary 10. *Let Y be an m-sequence of length $2^m - 1$, and let $t \in [0, 1)$ be a real number. Then, subject to Conjecture 9,*

$$\lim_{n \longrightarrow \infty} F(Y; Y^t) = \frac{3(1+t)^2}{1 + 9t^2 - 2t^3}.$$

Proof. The case $t = 0$ follows directly from Conjecture 9 (and is known to be correct by Theorem 3). Subject to Conjecture 9 we conclude from Theorem 8 that, for $t \in (0, 1)$,

$$\lim_{n \longrightarrow \infty} F(Y; Y^t) = \frac{(1+t)^2}{2t^2(1 - \frac{2}{3}t + 1) + (1-t)^2(1 - \frac{2}{3}(1-t))},$$

which proves the corollary. □

Under the assumption that Conjecture 9 is correct, elementary calculus gives the maximum asymptotic merit factor achievable by appending to m-sequences.

Corollary 11. *Let Y be an m-sequence of length $n = 2^m - 1$, and assume Conjecture 9 to be correct. Then the maximum of $\lim_{n\to\infty} F(Y; Y^t)$ over $t \in [0, 1)$ is given by*

$$\lim_{n \longrightarrow \infty} F(Y; Y^{\hat{t}}) = \frac{3(1+\hat{t})^2}{1 + 9\hat{t}^2 - 2\hat{t}^3},$$

where $\hat{t}$ is the solution of

$$t^3 + 3t^2 - 9t + 1 = 0 \quad \text{for } 0 < t < 1.$$

Approximately we have

$$\lim_{n \longrightarrow \infty} F(Y; Y^{\hat{t}}) \simeq 3.3420653 \quad \text{and} \quad \hat{t} \simeq 0.1157494.$$

6 Evidence in Favour of Conjecture 9

Conjecture 9 implies that, given an m-sequence Y of length $n = 2^m - 1$,

$$\mathbb{E}_k\left[\frac{t^2}{F((Y_{k/n})^t)}\right] \sim t^2(1 - \tfrac{2}{3}t) \quad \text{for } t \in (0, 1] \text{ as } n \longrightarrow \infty. \tag{12}$$

This asymptotic relation is implied by setting $\ell = tn$ and letting $n \longrightarrow \infty$ in the following result, which therefore provides evidence in favour of Conjecture 9.

Proposition 12. *Let Y be an m-sequence of length $n = 2^m - 1$, and let ℓ be an integer satisfying $2 \le \ell \le n$. Then*

$$\mathbb{E}_k\left[\frac{1}{F((Y_{k/n})^{\ell/n})}\right] = \frac{(\ell-1)(3n - 2\ell + 4)}{3n\ell}.$$

Proof. The proof is similar to that of Theorem 6. Let α be the primitive element of $\mathrm{GF}(2^m)$ appearing in the definition of Y given in (2), and let σ be the permutation determined by α satisfying (3). By Lemma 1 (ii), for each u satisfying $1 \le u < \ell$, we have

$$C_{(Y_{k/n})^{\ell/n}}(\ell - u) = S_Y(k + \sigma(\ell - u), u),$$

where $S_Y(k, \delta)$ is defined in (5). Then by Lemma 5

$$n\,\mathbb{E}_k\left[\left(C_{(Y_{k/n})^{\ell/n}}(\ell - u)\right)^2\right] = u(n - u + 1) \quad \text{for } 1 \le u < \ell,$$

so that

$$\begin{aligned}\mathbb{E}_k\left[\frac{n\ell^2}{2F((Y_{k/n})^{\ell/n})}\right] &= \sum_{u=1}^{\ell-1} n\,\mathbb{E}_k\left[\left(C_{(Y_{k/n})^{\ell/n}}(\ell - u)\right)^2\right] \\ &= \sum_{u=1}^{\ell-1} u(n - u + 1) \\ &= \tfrac{1}{6}\ell(\ell - 1)(3n - 2\ell + 4),\end{aligned}$$

as required. □

Notice that Theorem 2 arises as the special case $\ell = n$ of Proposition 12. Proposition 12 and its consequence (12) still leave the possibility that, given an m-sequence Y of length $n = 2^m - 1$ and a real $t \in (0, 1]$, the asymptotic form of $t^2/F((Y_r)^t)$ varies as r ranges over $[0, 1]$. However, we now present numerical data showing that this is apparently not the case, therefore providing further evidence in favour of Conjecture 9.

Let α be a primitive element of $\mathrm{GF}(2^m)$, and let $Y = (y_0, y_1, \ldots, y_{n-1})$ be the m-sequence of length $n = 2^m - 1$ given by (2), where β is chosen such that $y_0 = y_1 = \cdots = y_{m-1} = 1$ (which can be done uniquely by the run property of m-sequences; see [Gol67, p. 44, Thm. 4.2] for example). We inspect the *discrepancy*

$$d(r, t) := \frac{t^2}{F((Y_r)^t)} - t^2(1 - \tfrac{2}{3}t)$$

for

$$(r, t) \in L := \{0, 1/64, 2/64, \ldots, 1\} \times \{1/64, 2/64, \ldots, 1\}.$$

We obtain the following example data for the maximum discrepancy on L:

$$\max_{(r,t)\in L} |d(r, t)| = \begin{cases} 0.018453 & \text{for } n = 2^{11} - 1 \text{ using } \alpha^{11} = \alpha^2 + 1 \\ 0.006677 & \text{for } n = 2^{15} - 1 \text{ using } \alpha^{15} = \alpha + 1 \\ 0.001363 & \text{for } n = 2^{19} - 1 \text{ using } \alpha^{19} = \alpha^5 + \alpha^2 + \alpha + 1 \\ 0.000395 & \text{for } n = 2^{23} - 1 \text{ using } \alpha^{23} = \alpha^5 + 1. \end{cases}$$

The data show that the discrepancy apparently tends to zero with increasing length n. We observed a similar behaviour for other choices for the primitive element α.

7 Comparison to Legendre Sequences

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 [HJ88].

Theorem 13 (Høholdt and Jensen [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*

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

The maximum asymptotic merit factor of a rotated Legendre sequence X_r is 6, which occurs for $r = \frac{1}{4}$ and $\frac{3}{4}$ and is the best proven asymptotic merit factor of a binary sequence family. Borwein, Choi, and Jedwab [BCJ04] presented an analysis of the effect of appending for rotated Legendre sequences, similar to the analysis for m-sequences given in Section 5. Extensive numerical data for the behaviour of $1/F((X_r)^t)$ were presented, leading to a conjecture on its asymptotic form. Using a result similar to Theorem 8, the authors of [BCJ04] showed that, subject to this conjecture, $\lim_{n\to\infty} F(X_r; (X_r)^t)$ exists for all $r, t \in [0, 1]$ and

$$\max_{r \in [0,1]} \lim_{n \longrightarrow \infty} F(X_r; (X_r)^t) = G(t) \quad \text{for } t \in [0, 1],$$

where

$$G(t) = \begin{cases} \dfrac{6(1+t)^2}{1 + 18t^2 - 8t^3} & \text{for } 0 \le t \le \frac{1}{2} \\[2ex] \dfrac{6(1+t)^2}{4 - 12t + 30t^2 - 8t^3} & \text{for } \frac{1}{2} \le t \le 1. \end{cases}$$

We now compare this function with

$$H(t) = \frac{3(1+t)^2}{1 + 9t^2 - 2t^3} \quad \text{for } t \in [0, 1],$$

which, subject to Conjecture 9, equals $\lim_{n\to\infty} F(Y; Y^t)$, where Y is an m-sequence of length $n = 2^m - 1$. The left plot of Figure 1 shows the graphs of $G(t)$ and $H(t)$. The maximum of $G(t)$ in the interval $t \in [0, 1]$ is given by

$$G(\hat{t}_L) \simeq 6.3420596 \quad \text{for } \hat{t}_L \simeq 0.0578279,$$

and, as in Corollary 11, the maximum of $H(t)$ in the interval $t \in [0, 1]$ is given by

$$H(\hat{t}_M) \simeq 3.3420653 \quad \text{for } \hat{t}_M \simeq 0.1157494.$$

Surprisingly (to us), we find $G(\hat{t}_L) - 6 \simeq H(\hat{t}_M) - 3$ and $2\hat{t}_L \simeq \hat{t}_M$, but certainly equality does not hold. Indeed, the right plot of Figure 1 shows that $G(t) - 6$ and $H(2t) - 3$ have very similar graphs in the range $t \in [0, \frac{1}{8}]$. It is doubtful these graphs could be distinguished for $t \simeq 0.058$ purely from numerical data.

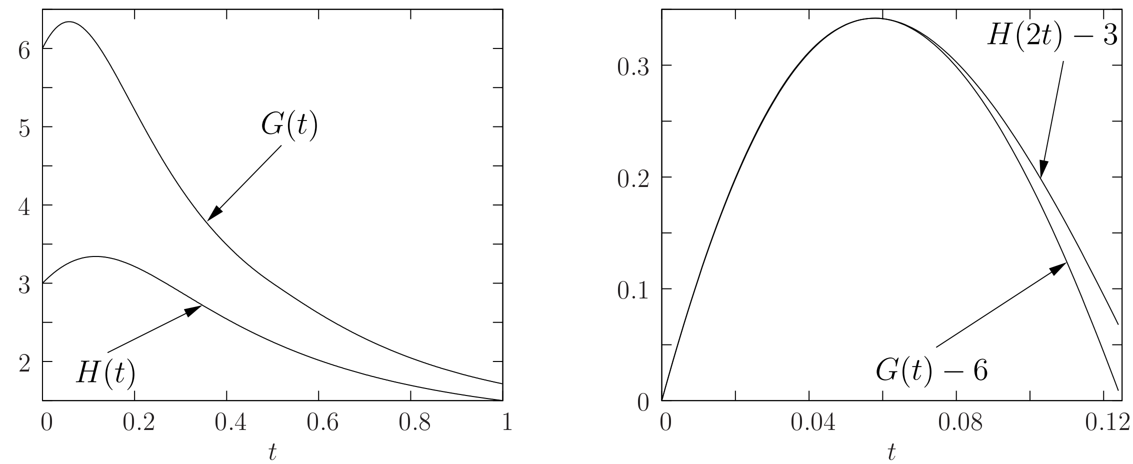

Figure 1: Comparison of the graphs of $G(t)$ and $H(t)$.

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.*, 40:289–304, 1985.

[BCJ04] P. Borwein, K. K. S. Choi, and J. Jedwab. Binary sequences with merit factor greater than 6.34. *IEEE Trans. Inf. Theory*, 50(12):3234–3249, 2004.

[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 Francicso, CA, 1967.

[HJ88] T. Høholdt and H. E. Jensen. Determination of the merit factor of Legendre sequences. *IEEE Trans. Inf. Theory*, 34(1):161–164, 1988.

[Jed05] J. Jedwab. A survey of the merit factor problem for binary sequences. In *Proc. of Sequences and Their Applications (SETA)*, volume 3486 of *Lecture Notes in Computer Science*, pages 30–55. New York: Springer Verlag, 2005.

[Jed08] J. Jedwab. What can be used instead of a Barker sequence? *Contemp. Math.*, 461:153–178, 2008.

[JH89] H. E. Jensen and T. Høholdt. Binary sequences with good correlation properties. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-5 Proceedings*, volume 356 of *Lecture Notes in Computer Science*, pages 306–320. Springer-Verlag, Berlin, 1989.

[KN99] A. Kirilusha and G. Narayanaswamy. Construction of new asymptotic classes of binary sequences based on existing asymptotic classes. Summer Science Program Tech. Report, Dept. Math. Comput. Sci., Univ. Richmond, Richmond, VA, 1999.

[KP04] R. A. Kristiansen and M. G. Parker. Binary sequences with merit factor > 6.3. *IEEE Trans. Inf. Theory*, 50(12):3385–3389, 2004.

[Lin68] J. H. Lindholm. An analysis of the pseudo-randomness properties of subsequences of long m-sequences. *IEEE Trans. Inf. Theory*, IT-14(4):569–576, 1968.

[Sar84a] D. V. Sarwate. Mean-square correlation of shift-register sequences. *IEE Proc.*, 131, Part F(2):101–106, 1984.

[Sar84b] D. V. Sarwate. An upper bound on the aperiodic autocorrelation function for a maximal-length sequence. *IEEE Trans. Inf. Theory*, IT-30(4):685–687, 1984.