The Peak Sidelobe Level of Families of Binary Sequences

Jonathan Jedwab   Kayo Yoshida

17 September 2005 (revised 2 February 2006)

Abstract

A numerical investigation is presented for the peak sidelobe level (PSL) of Legendre sequences, maximal length shift register sequences (m-sequences), and Rudin-Shapiro sequences. The PSL gives an alternative to the merit factor for measuring the collective smallness of the aperiodic autocorrelations of a binary sequence. The growth of the PSL of these infinite families of binary sequences is tested against the desired growth rate $o(\sqrt{n \ln n})$ for sequence length n. The claim that the PSL of m-sequences grows like $O(\sqrt{n})$, which appears frequently in the radar literature, is concluded to be unproven and not currently supported by data. Notable similarities are uncovered between the PSL and merit factor behaviour under cyclic rotations of the sequences.

Keywords aperiodic autocorrelation, peak sidelobe level, binary sequence, merit factor, Legendre sequence, maximal length shift register sequence, Rudin-Shapiro sequence

1 Introduction

A *binary sequence* of length n is an n-tuple $A = (a_0, a_1, \ldots, a_{n-1})$ where $a_i = 1$ or -1 for each $i = 0, 1, \ldots, n-1$. The *aperiodic autocorrelation* of A at shift u is defined as

$$C_A(u) := \sum_{i=0}^{n-u-1} a_i a_{i+u}. \tag{1}$$

It has long been of interest in the study of sequence design to find binary sequences whose aperiodic autocorrelations are, in some suitable sense, collectively small. Two principal

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

measures of “smallness” have been used. One measure (surveyed in [16]) is the *merit factor*, introduced by Golay in 1972 [11]:

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

The other measure, and our main interest here, is the *peak sidelobe level* (PSL):

$$M(A) := \max_{1\le u\le n-1} |C_A(u)|\,.$$

Let $\mathcal{A}_n$ denote the set of all binary sequences of length n. We would like ultimately to understand the behaviour, as $n \to \infty$, of

$$M_n := \min_{A\in\mathcal{A}_n} M(A), \tag{2}$$

and to compare its asymptotic behaviour with that of $1/F_n$, where $F_n := \max_{A\in\mathcal{A}_n} F(A)$.

In order to compute M_n numerically for a given length n, in the most naive manner, requires testing 2^n different sequences. More efficient algorithms reduce the exponential term of the time complexity from $O(2^n)$ to roughly $O(1.4^n)$ [6], [7], [8]. (We will use the notation o, O, Ω and Θ to compare the growth rates of functions $f(n)$ and $g(n)$ from $\mathbb{N}$ to $\mathbb{R}^+$ in the following standard way: f is $o(g)$ means that $f(n)/g(n) \to 0$ as $n \to \infty$; f is $O(g)$ means that there is a constant c, independent of n, for which $f(n) \le cg(n)$ for all sufficiently large n; f is $\Omega(g)$ means that g is $O(f)$; and f is $\Theta(g)$ means that f is $O(g)$ and $\Omega(g)$.) The value of M_n has been computed up to $n = 70$, and it has been found that:

(i) $M_n \le 2$ for $n \le 21$ (Turyn, 1968 [32]), where $M_n = 1$ is achieved for $n = 2, 3, 4, 5, 7, 11$ and 13 by *Barker sequences*

(ii) $M_n \le 3$ for $n \le 48$ (Lindner, 1975 [20] for $n \le 40$; Cohen, Fox and Baden, 1990 [6] for $n \le 48$)

(iii) $M_n \le 4$ for $n \le 70$ (Elders-Boll, Schotten and Busboom, 1997 [9] for $49 \le n \le 61$; Coxson and Russo, 2005 [8] for $61 \le n \le 70$, correcting some errors in [7]).

Levanon and Mozeson [18, Table 6.3] list an example sequence attaining M_n for all values of $n \le 69$ (except those corresponding to lengths of Barker sequences in (i) above).

Theoretical bounds on the asymptotic behaviour of M_n were also known as early as 1968:

Theorem 1.1 (Moon and Moser [26]) *If $K(n)$ is any function of n such that $K(n) = o(\sqrt{n})$, then the proportion of sequences $A \in \mathcal{A}_n$ for which $M(A) > K(n)$ approaches 1 as $n \to \infty$.*

Theorem 1.2 (Moon and Moser [26]) *For any fixed $\epsilon > 0$, the proportion of sequences $A \in \mathcal{A}_n$ such that $M(A) \le (2+\epsilon)\sqrt{n\ln n}$ approaches 1 as $n \to \infty$.*

It is clear from Theorem 1.2 that for any fixed $\epsilon > 0$, $M_n \leq (2+\epsilon)\sqrt{n \ln n}$ when n is sufficiently large. The constant in this bound has recently been improved:

Theorem 1.3 (Mercer [25]) *For any fixed $\epsilon > 0$, $M_n \leq (\sqrt{2}+\epsilon)\sqrt{n \ln n}$ when n is sufficiently large.*

We note that there are sequence families for which the PSL grows faster than $\Theta(\sqrt{n \ln n})$, exceeding the upper bound in Theorems 1.2 and 1.3. An example is the sequence family $\mathcal{F} = \{A_n : n \in \mathbb{N}\}$ such that each of the n elements of A_n is 1. However, it is not currently known whether there exists any sequence family whose PSL grows like the lower bound $o(\sqrt{n})$ of Theorem 1.1, nor even like $\Theta(\sqrt{n})$. Nonetheless, even these lower bounds appear to be weak considering the known numerical results for M_n for $n \leq 70$. This apparent gap between the numerical data and the theoretical bounds motivates us to attempt to exhibit an infinite family of binary sequences whose PSL grows like $o(\sqrt{n \ln n})$ (more slowly than the upper bound of Theorems 1.2 and 1.3), and preferably like $O(\sqrt{n})$.

This rest of this paper is organised as follows. Section 2 introduces three infinite families of binary sequences whose merit factor behaviour is well understood, at least asymptotically. Section 3 explains known bounds on the PSL of these families of sequences. Sections 4, 5 and 6 present numerical results and observations on the PSL of Legendre sequences, maximal length shift register sequences, and Rudin-Shapiro sequences respectively. Section 7 presents some conclusions and suggestions for further work.

2 Three Families of Sequences

The theoretical approach to the merit factor problem includes the study of specific infinite families of sequences. We shall be concerned with the families of Legendre sequences, maximal length shift register sequences, and Rudin-Shapiro sequences. For more detailed information on these families, see [16] for example.

2.1 Legendre Sequences

The *Legendre sequence* (also called a *quadratic residue sequence*) $X = (x_0, x_1, \ldots, x_{n-1})$ of prime length n is defined so that

$$x_i := \begin{cases} 1 & \text{if } i \text{ is a quadratic residue mod } n \\ -1 & \text{otherwise.} \end{cases}$$

By convention, we take $x_0 = 1$. A Legendre sequence is equivalent to a cyclic difference set with parameters from the Hadamard family for $n \equiv 3 \pmod 4$ (see [1] or [28] for background on difference sets) and to a partial difference set for $n \equiv 1 \pmod 4$ [22, Theorem 2.1].

When a sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n is *rotated* by a rotational fraction r, we obtain a new sequence $A_r = (b_0, b_1, \ldots, b_{n-1})$ such that

$$b_i := a_{(i+\lfloor rn \rfloor) \bmod n}.$$

In 1988 Høholdt and Jensen [14], building on earlier work of Turyn (reported in [12]) and Golay [12], established:

Theorem 2.1 (Høholdt and Jensen [14]) *Let X be a Legendre sequence of prime length n. Then*

$$\frac{1}{\lim_{n\to\infty} F(X_r)} = \begin{cases} \frac{1}{6} + 8(r - \frac{1}{4})^2 & \text{for } 0 \le r \le \frac{1}{2} \\ \frac{1}{6} + 8(r - \frac{3}{4})^2 & \text{for } \frac{1}{2} \le r < 1. \end{cases}$$

It follows that the maximum asymptotic merit factor of any rotation of a Legendre sequence is 6, and is achieved when the rotational fraction r is 1/4 and 3/4. Although this value 6 is the greatest proven asymptotic result for the merit factor of binary sequences, Borwein, Choi and Jedwab [3] gave strong numerical evidence that there are binary sequences whose asymptotic merit factor exceeds 6.34. Their construction involves sequences given by appending the initial elements of some rotation of a Legendre sequence to itself.

2.2 Maximal Length Shift Register Sequences

A *maximal length shift register sequence*, also called an *m-sequence*, *ML-sequence*, or *pseudonoise sequence*, is a binary sequence $Y = (y_0, y_1, \ldots, y_{2^m-2})$ of length $2^m - 1$ for which

$$y_i := (-1)^{\mathrm{tr}(\beta\alpha^i)} \quad \text{for all } 0 \le i < 2^m - 1, \tag{3}$$

where α is a primitive element of the finite field $\mathrm{GF}(2^m)$, β is any fixed nonzero element from the same field, and tr() is the trace function from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$ defined by $\mathrm{tr}() : x \mapsto \sum_{i=0}^{m-1} x^{2^i}$ (see [24], for example). An m-sequence of a given length $2^m - 1$ is not unique, since the choice of nonzero β and primitive α are arbitrary.

Alternatively we can define an m-sequence Y using a linear recurrence relation. Let $f(x) = 1 + \sum_{i=1}^{m} c_i x^i$ be a primitive polynomial of degree m over $\mathrm{GF}(2)$. Define a 0/1 sequence $(a_0, a_1, \ldots, a_{2^m-2})$ so that $a_0, a_1, \ldots, a_{m-1}$ take arbitrary values that are not all 0's, and

$$a_i := \left(\sum_{j=1}^{m} c_j a_{i-j} \right) \bmod 2 \quad \text{for } m \le i < 2^m - 1.$$

Then set $y_i = (-1)^{a_i}$ for $0 \le i \le 2^m - 2$ to yield a $+1/-1$ sequence Y of length $2^m - 1$: this gives an m-sequence. This alternative definition can be physically implemented using a shift register with m stages [13].

The "window property" of m-sequences [13] implies that, if we fix a primitive polynomial $f(x)$ and take all $2^m - 1$ permitted values of the initial elements $(a_0, a_1, \ldots, a_{m-1})$, we obtain

$2^m - 1$ different m-sequences that are all possible cyclic shifts of an m-sequence generated by $f(x)$. Since there are exactly $\frac{\phi(2^m-1)}{m}$ primitive polynomials of degree m over GF(2) [19, Chapter 3, Theorem 3.15], there are a total of $\frac{\phi(2^m-1)}{m} \cdot (2^m - 1)$ distinct m-sequences of length $2^m - 1$.

A third equivalent representation of an m-sequence is as a cyclic Singer difference set [24]. In 1989 this equivalence was used to prove:

Theorem 2.2 (Jensen and Høholdt [17]) *The asymptotic merit factor of any rotation of an m-sequence is* 3.

Figure 1 contrasts the difference between the behaviour of the asymptotic merit factor of Legendre sequences (Theorem 2.1) and m-sequences (Theorem 2.2) as the rotational fraction r varies.

2.3 Rudin-Shapiro Sequences

Given sequences $A = (a_0, a_1, \ldots, a_{n-1})$ of length n and $A' = (a'_0, a'_1, \ldots, a'_{n'-1})$ of length n', let $A; A'$ denote the sequence $(b_0, b_1, \ldots, b_{n+n'-1})$ of length $n + n'$ given by *appending* A' to A:

$$b_i := \begin{cases} a_i & \text{for } 0 \le i < n \\ a'_{i-n} & \text{for } n \le i < n + n'. \end{cases}$$

The *Rudin-Shapiro sequence pair* $X^{(m)}$ and $Y^{(m)}$ of length 2^m is defined recursively so that $X^{(0)} = Y^{(0)} := (1)$, and

$$\left.\begin{array}{rcl} X^{(m)} & := & X^{(m-1)}; Y^{(m-1)}, \\ Y^{(m)} & := & X^{(m-1)}; -Y^{(m-1)} \end{array}\right\} \text{ for } m > 0.$$

In 1968 Littlewood determined the exact merit factor of a Rudin-Shapiro sequence of any length 2^m:

Theorem 2.3 (Littlewood [21, p. 28]) *The merit factor of both sequences $X^{(m)}$ and $Y^{(m)}$ of a Rudin-Shapiro sequence pair of length 2^m is* $\dfrac{3}{1-(-1/2)^m}$.

Consequently, the asymptotic merit factor of both sequences of a Rudin-Shapiro sequence pair is 3. Rudin-Shapiro sequences differ from Legendre sequences and m-sequences in that they have no known periodic property (under sequence rotations), such as equivalence to a difference set or partial difference set. This distinction will be of importance in Section 6.

3 Bounds on the Peak Sidelobe Level of Families of Sequences

In Section 1 we presented some general bounds on the PSL. In this section we consider bounds on the PSL of specific families of binary sequences.

We begin with a connection between the merit factor and the PSL of a family of sequences. Let $\mathcal{F}$ be a family of binary sequences and let each $A_n \in \mathcal{F}$ have length n. Suppose $\liminf_{n\to\infty}(M(A_n)/\sqrt{n}) = 0$. Then, for each n,

$$0 < \frac{1}{\sqrt{2F(A_n)}} = \frac{\sqrt{\sum_{u=1}^{n-1}[C_A(u)]^2}}{n} \leq \frac{\sqrt{(n-1)[M(A_n)]^2}}{n} < \frac{M(A_n)}{\sqrt{n}}.$$

It follows that $\liminf_{n\to\infty}(1/\sqrt{2F(A_n)}) = 0$ and therefore $\limsup_{n\to\infty} F(A_n) = \infty$. The converse of this statement is useful:

Proposition 3.1 *Let $\mathcal{F}$ be a family of binary sequences and let each $A_n \in \mathcal{F}$ have length n. If $\{F(A_n) : A_n \in \mathcal{F}\}$ is bounded, then $M(A_n) = \Omega(\sqrt{n})$.*

By Proposition 3.1 and Theorems 2.1, 2.2, and 2.3, the PSL of any rotation of a Legendre sequence, of any m-sequence, and of a Rudin-Shapiro sequence all grow at least as fast as $\sqrt{n}$.

As described in Section 1, we would like to identify a family of sequences whose PSL grows like $o(\sqrt{n \ln n})$. Among the three families of sequences introduced in Section 2, the largest asymptotic merit factor is achieved by rotated Legendre sequences. We might therefore expect that, if any of these families has a PSL that grows like $o(\sqrt{n \ln n})$, the family of Legendre sequences (and their rotations) is the most likely candidate; we might even hope that the PSL of some rotation grows like $O(\sqrt{n})$. This is investigated in Section 4.

The PSL of m-sequences Y of length n has been much discussed in the literature. In 1980, McEliece [23] showed that $\sqrt{n+1}\ln(en)$ is an upper bound for $M(Y)$. In 1984 Sarwate improved this bound:

Theorem 3.2 (Sarwate [30]) *Let Y be an m-sequence of length n. Then*

$$M(Y) < 1 + \frac{2}{\pi}\sqrt{n+1}\ln\left(\frac{4n}{\pi}\right).$$

Theorem 3.2 does not tell us whether the PSL of (some or all) m-sequences grows like $o(\sqrt{n \ln n})$. However, Cohen, Baden and Cohen [5, p. 62] state, without reference, that m-sequences "can achieve peak sidelobe levels (PSLs) on the order of $N^{1/2}$"! This is the most modest growth of the PSL that an m-sequence could possibly achieve (Proposition 3.1 and Theorem 2.2). It is not clear whether the statement in [5] is intended to apply to any rotation of an m-sequence generated by any primitive polynomial, or only to some (infinite) subset of

m-sequences. But even if it held for some infinite subset, this would imply that M_n (see (2)) grows like $O(\sqrt{n})$. This would greatly improve on Moon and Moser's Theorem 1.2, and indeed would render Mercer's improvement (Theorem 1.3) of little value.

However we were unable to find a proof or supporting numerical evidence for this claim. For example, Farnett and Stevens [10, 10.21] state that the PSL of m-sequences is "approximately" $\sqrt{n}$ for large n. Cohen [4, p. 486] makes the same statement, adding that "as N increases, the rule-of-thumb approximation improves". But neither author gives a reference. Likewise Vakman [33, p. 182–183] claims that the PSL of m-sequences grows like $O(\sqrt{n})$, and further states: "It has been noted repeatedly that either by empirical methods, by combining several M-sequences, or, finally, by constructing other types of sequences, it is possible to find [other long sequences for which the PSL grows like $O(\sqrt{n})$]". Once again, however, no reference is given, and [33] describes the proof for m-sequences as being "beyond the scope of this book". We therefore regard this claim to be unproven and currently unsupported.

We investigate the PSL of families of m-sequences numerically in Section 5, testing its growth against the claimed bounding function $\sqrt{n}$ and also against the function $\sqrt{n \ln n}$.

In Section 6 we study the PSL of Rudin-Shapiro sequences and their rotations, as an example of a sequence family with no known periodic property. Although an upper bound for the PSL of unrotated Rudin-Shapiro sequences is known, it is weak in comparison with the function $\sqrt{n \ln n}$:

Theorem 3.3 (Høholdt, Jensen and Justesen [15]) *The PSL of both sequences $X^{(m)}$ and $Y^{(m)}$ of a Rudin-Shapiro sequence pair of length $n = 2^m$ grows like $O(n^{0.9})$.*

4 The Peak Sidelobe Level of Legendre Sequences

In this section we compare the growth of the PSL of Legendre sequences with the functions $\sqrt{n}$ and $\sqrt{n \ln n}$ (see Section 3). Write $R = \{0, \frac{1}{n}, \dots, \frac{n-1}{n}\}$ and let X be a Legendre sequence of prime length n. We calculated $M(X_r)$ for all $r \in R$ for various values of n, using similar strategies to those described in [16, Section 3.2] for efficiency.

Figure 2 shows the variation of $M(X_r)$ with the rotational fraction r, for $n = 49,999$ and $n = 104,729$. Similar shapes of graph were obtained for all lengths tested. (After submitting this paper we became aware that in 2005, prior to the start of our investigation, Schotten and Lüke [31, Figure 2] presented a graph corresponding to Figure 2 for six values of n in the range $211 \leq n \leq 10007$.) The shape of the graphs closely resembles that of the graph of $1/\lim_{n\to\infty} F(X_r)$ against r (see Figure 1 left), in particular achieving a minimum value at approximately $r = 1/4$ and $r = 3/4$. The obvious difference between the shape of the graphs for M and asymptotic $1/F$ is that "fuzziness" seems to persist in the graph of $M(X_r)$ at all lengths.

Figure 3 shows the variation of $\min_{r\in R} M(X_r)$ with length n for the first 3500 prime lengths ($n \leq 32609$). (The data set underlying Figure 3 was previously calculated for primes n

in the much smaller ranges $7 \le n \le 113$ (Boehmer, 1967 [2]) and $67 \le n \le 1019$ (Rao and Reddy, 1986 [29]). Since the minimising value of r was found to be approximately $1/4$ for various lengths n, Figure 3 also shows the variation of $M(X_{1/4})$ with n for $n \le 41081$. Both graphs have a similar shape, although there is more variation in the second case.

We now compare the growth of the two functions, $\min_{r\in R} M(X_r)$ and $M(X_{1/4})$, with $\sqrt{n}$ and with $\sqrt{n \ln n}$. Figure 4 shows the variation of $\min_{r\in R} M(X_r)/\sqrt{n}$ and $M(X_{1/4})/\sqrt{n}$ with n. Both graphs show increasing functions, from which we conclude that the original two functions both grow at least as fast as $\sqrt{n}$. Figure 5 shows the variation of $\min_{r\in R} M(X_r)/\sqrt{n \ln n}$ and $M(X_{1/4})/\sqrt{n \ln n}$ with n. Both graphs now show functions that appear to approach a nonzero constant, which suggests that $\min_{r\in R} M(X_r)$ and $M(X_{1/4})$ both grow like $\Theta(\sqrt{n \ln n})$.

Based on the numerical evidence displayed in Figures 4 and 5, we conclude tentatively that $\min_{r\in R} M(X_r)$ and $M(X_{1/4})$ both grow like $\Theta(\sqrt{n \ln n})$. This is contrary to our initial expectation for the growth of the PSL of Legendre sequences.

5 The Peak Sidelobe Level of m-Sequences

In this section we compare the growth of the PSL of m-sequences with the functions $\sqrt{n}$ and $\sqrt{n \ln n}$. Our main interests are in testing the claim that the PSL of m-sequences grows like $O(\sqrt{n})$, and in identifying a family of sequences for which the growth of the PSL is $o(\sqrt{n \ln n})$ (see Section 3).

Let $R = \{0, \frac{1}{n}, \ldots, \frac{n-1}{n}\}$ as before, and let Y be an m-sequence of length $n = 2^m - 1$. We used the recurrence relation definition of an m-sequence (see Section 2.2) to calculate $M(Y_r)$ for all $r \in R$. This was done for all $\frac{\phi(2^m-1)}{m}$ primitive polynomials $f(x)$ of degree m over GF(2) for $m \le 15$ (length $n \le 32,767$), and for selected primitive polynomials of degree m over GF(2) for $16 \le m \le 20$ (length $n \le 1,048,575$). The computational burden was reduced by a factor of 2 for $m > 2$ by noting that the $2^m - 1$ m-sequences generated by $f(x)$ are the reverse of those generated by its reciprocal polynomial $x^m f(x^{-1})$ (which is distinct from $f(x)$), and that sequence reversal does not affect the aperiodic autocorrelations defined in (1). For example, the exhaustive computation for $m = 15$ was completed using 900 primitive polynomials obtained from Appendix C of [27], each generating a sequence that was examined at each of its 32,767 distinct rotations.

Figure 6 shows the variation of $M(Y_r)$ with the rotational fraction r, for two specific m-sequences. The shape of both graphs resembles that of the graph of $1/\lim_{n\to\infty} F(Y_r)$ against r (see Figure 1 right), but with "fuzziness" appearing to persist in the graph of $M(Y_r)$ at all sequence lengths. This similarity between the graphs of M and asymptotic $1/F$ mirrors the behaviour for Legendre sequences noted in Section 4.

Our initial analysis of the exhaustive m-sequence data (for $m \le 15$) kept the results for each primitive polynomial separate, and calculated the minimum, mean and maximum value of the PSL over all rotations $r \in R$. However we were unable to explain the variation of these values in terms of the primitive polynomial, and so we pooled the PSL data for all rotations of all m-sequences of the same length.

Indeed, let $\mathcal{Y}_m$ be the set of all $\frac{\phi(2^m-1)}{m} \cdot (2^m-1)$ m-sequences of length 2^m-1. Table 1 shows the variation with m of the minimum, mean and maximum value of $M(Y)$ over all m-sequences $Y \in \mathcal{Y}_m$ for $m \leq 15$, together with partial data for $16 \leq m \leq 20$. Figure 7 displays these values, taking ln of both co-ordinates in order to spread out the data points. Table 1 also compares the calculated PSL values for m-sequences for $2 \leq m \leq 6$ with the known optimal value M_{2^m-1} (see (2)).

We now compare the growth of the minimum, mean and maximum value of $M(Y)$ with $\sqrt{n}$ and $\sqrt{n \ln n}$. Figure 8 shows the variation of these values with $\ln n$, after division by $\sqrt{n}$ (left) and $\sqrt{n \ln n}$ (right). For the mean values $\sum_{Y \in \mathcal{Y}_m} M(Y)/|\mathcal{Y}_m|$, the left graph shows a (broadly) increasing function while the right graph shows a strictly decreasing function. We conclude that the mean value of the PSL over all m-sequences of length 2^m-1 grows like $\Omega(\sqrt{n})$ (as we already knew from Proposition 3.1 and Theorem 2.2), and like $O(\sqrt{n \ln n})$ (which, if true, would improve on the upper bound of Theorem 3.2). This empirical conclusion implies that the minimum PSL of m-sequences also grows like $O(\sqrt{n \ln n})$.

In light of the numerical evidence presented, we consider the claim that the PSL of m-sequences grows like $O(\sqrt{n})$ is not currently supported by data. We believe it would be challenging to collect sufficient computational data to settle this question with reasonable confidence. Nonetheless, it seems that the mean value of the PSL of m-sequences is more likely to achieve the desired growth rate of $o(\sqrt{n \ln n})$ than the PSL of Legendre sequences (see Section 4).

6 The Peak Sidelobe Level of Rudin-Shapiro Sequences

In this section we pursue the apparent similarity between the shape of the graphs of M and asymptotic $1/F$ as the rotational fraction r varies, as observed in the case of Legendre sequences in Section 4 and m-sequences in Section 5. We assumed that this similarity depends on an underlying periodic property, the property in these cases being equivalence to a difference set or partial difference set. We tested this assumption using the Rudin-Shapiro sequences, which have no known periodic property.

To our knowledge the merit factor of Rudin-Shapiro sequences under cyclic rotation has not previously been studied; all that is known regarding the merit factor is Theorem 2.3. Let $(X^{(m)}, Y^{(m)})$ be a Rudin-Shapiro sequence pair of length $n = 2^m$. Figure 9 shows the variation of $1/F((X^{(m)})_r)$ with the rotational fraction $r \in R$, for $m = 10$ and for $m = 16$. Similar shapes of graph were obtained for all values $9 \leq m \leq 16$ (whereas for $m \leq 8$ there are too few data points to discern such a clear shape). $F((X^{(m)})_r)$ appears to lie between $3/2$ and 3 for all r, when m is large.

The PSL of the unrotated sequence $X^{(m)}$ grows like $O(n^{0.9})$, by Theorem 3.3. Figure 10 shows the variation of $M((X^{(m)})_r)$ with $r \in R$ for $m = 10$, 12, and 16. The shape of the graphs becomes more regular as m increases, apparently approaching a piecewise linear function composed of 12 pieces with minima at $r = 0$, 1/4, 3/8, 1/2, 3/4, and 7/8. Unlike the case of Legendre sequences (Figure 2) and m-sequences (Figure 6), there appears to be no "fuzziness" in the graph of M at large lengths. Perhaps more surprisingly, there is still a considerable similarity between the graphs of M and $1/F$ as r varies (comparing Figure 10 to Figure 9). We conclude that this phenomenon is not restricted to sequences having an underlying periodic property.

We performed the same calculations for the other sequence $Y^{(m)}$ of the Rudin-Shapiro pair. The corresponding graphs, both for M and $1/F$, appeared to be the reflection of those for $X^{(m)}$ about the line $r = 1/2$.

7 Conclusions

We summarise our main conclusions as:

(i) The PSL of the optimal rotation of a Legendre sequence of prime length n appears to grow like $\Theta(\sqrt{n \ln n})$, contrary to our initial expectation of $o(\sqrt{n \ln n})$ growth.

(ii) The mean value of the PSL of m-sequences of length $n = 2^m - 1$ seems to grow like $\Omega(\sqrt{n})$ and like $O(\sqrt{n \ln n})$. We consider the claim that the PSL of m-sequences grows like $O(\sqrt{n})$ to be unproven and not currently supported by data.

(iii) For large n, the graphs of the variation of $M(A_r)$ and $1/F(A_r)$ with rotational fraction r have a similar shape, where A is a Legendre sequence, an m-sequence, or a Rudin-Shapiro sequence of length n. This phenomenon does not seem to be restricted to sequence families having an underlying periodic property.

We suggest the following would be of interest for future work:

(i) Determine theoretically if the PSL of an optimal rotation of a Legendre sequence is really given by $\Theta(\sqrt{n \ln n})$.

(ii) Determine the actual rate of growth of the mean PSL of m-sequences. Prove or disprove the claim that the PSL of some or all m-sequences grows like $O(\sqrt{n})$.

(iii) Explain the apparent similarity, for large n, between the graphs of the variation of $M(A_r)$ and $1/F(A_r)$ with r for various sequence families $\{A\}$.

(iv) Explain the apparent behaviour of $M((X^{(m)})_r)$ for a Rudin-Shapiro sequence $X^{(m)}$ for large m, as described in Section 6 and illustrated in Figure 10.

References

[1] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory.* Cambridge University Press, Cambridge, 1986.

[2] A.M. Boehmer. Binary pulse compression codes. *IEEE Trans. Inform. Theory*, **IT-13**:156–167, 1967.

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

[4] M.N. Cohen. Pulse compression in radar systems. In J.L. Eaves and E.K. Reedy, editors, *Principles of Modern Radar*, pages 465–501. Van Nostrand Reinhold, New York, 1987.

[5] M.N. Cohen, J.M. Baden, and P.E. Cohen. Biphase codes with minimum peak sidelobes. In *IEEE National Radar Conference*, pages 62–66. IEEE, 1989.

[6] M.N. Cohen, M.R. Fox, and J.M. Baden. Minimum peak sidelobe pulse compression codes. In *IEEE International Radar Conference*, pages 633–638. IEEE, 1990.

[7] G.E. Coxson, A. Hirschel, and M.N. Cohen. New results on minimum-PSL binary codes. In *IEEE Radar Conference*, pages 153–156. IEEE, 2001.

[8] G.E. Coxson and J. Russo. Efficient exhaustive search for optimal-peak-sidelobe binary codes. *IEEE Trans. Aerospace and Electron. Systems*, **41**:302–308, 2005.

[9] H. Elders-Boll, H. Schotten, and A. Busboom. A comparative study of optimization methods for the synthesis of binary sequences with good correlation properties. In *5th IEEE Symposium on Communication and Vehicular Technology in the Benelux*, pages 24–31. IEEE, 1997.

[10] E.C. Farnett and G.H. Stevens. Pulse compression radar. In M.I. Skolnik, editor, *Radar Handbook*, chapter 10. Van Nostrand Reinhold, New York, 1987.

[11] M.J.E. Golay. A class of finite binary sequences with alternate autocorrelation values equal to zero. *IEEE Trans. Inform. Theory*, **IT-18**:449–450, 1972.

[12] M.J.E. Golay. The merit factor of Legendre sequences. *IEEE Trans. Inform. Theory*, **IT-29**:934–936, 1983.

[13] S.W. Golomb. *Shift Register Sequences.* Aegean Park Press, California, revised edition, 1982.

[14] T. Høholdt and H.E. Jensen. Determination of the merit factor of Legendre sequences. *IEEE Trans. Inform. Theory*, **34**:161–164, 1988.

[15] T. Høholdt, H.E. Jensen, and J. Justesen. Aperiodic correlations and the merit factor of a class of binary sequences. *IEEE Trans. Inform. Theory*, **IT-31**:549–552, 1985.

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

[17] H.E. Jensen and T. Høholdt. Binary sequences with good correlation properties. In L. Huguet and A. Poli, editors, *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.

[18] N. Levanon and E. Mozeson. *Radar Signals.* IEEE Press, Wiley-Interscience, Hoboken, New Jersey, 2004.

[19] R. Lidl and G. Pilz. *Applied Abstract Algebra.* Springer-Verlag, New York, 1984.

[20] J. Lindner. Binary sequences up to length 40 with best possible autocorrelation function. *Electron. Lett.*, **11**:507, 1975.

[21] J.E. Littlewood. *Some Problems in Real and Complex Analysis.* Heath Mathematical Monographs. D.C. Heath and Company, Massachusetts, 1968.

[22] S.L. Ma. A survey of partial difference sets. *Designs, Codes and Cryptography*, **4**:221–261, 1994.

[23] R.J. McEliece. Correlation properties of sets of sequences derived from irreducible cyclic codes. *Inform. Contr.*, **45**:18–25, 1980.

[24] R.J. McEliece. *Finite Fields for Computer Scientists and Engineers.* Kluwer Academic, Boston, 1987.

[25] I.D. Mercer. Autocorrelations of random binary sequences. 2004. Preprint.

[26] J.W. Moon and L. Moser. On the correlation function of random binary sequences. *SIAM J. Appl. Math.*, **16**:340–343, 1968.

[27] W.W. Peterson and E.J. Weldon, Jr. *Error-Correcting Codes.* MIT Press, Cambridge, MA and London, England, 2nd edition, 1972.

[28] A. Pott. *Finite Geometry and Character Theory.* Lecture Notes in Mathematics 1601. Springer-Verlag, Berlin, 1995.

[29] K.V. Rao and V.U. Reddy. Biphase sequence generation with low sidelobe autocorrelation function. *IEEE Trans. Aerospace and Electron. Systems*, **AES-22**:128–133, 1986.

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

[31] H.D. Schotten and H.D. Lüke. On the search for low correlated binary sequences. *AEU — Int. J. of Electronics and Communications*, **59**:67–78, 2005.

[32] R.J. Turyn. Sequences with small correlation. In H.B. Mann, editor, *Error Correcting Codes*, pages 195–228. Wiley, New York, 1968.

[33] D.E. Vakman. *Sophisticated Signals and the Uncertainty Principle in Radar*. Springer-Verlag, New York, 1968.

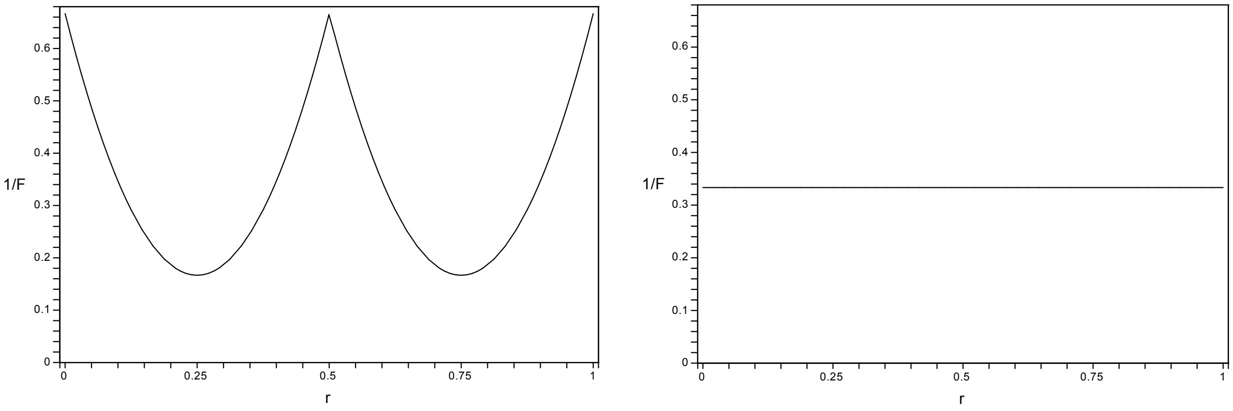

Figure 1: Variation of $1/[\lim_{n\to\infty} F(X_r)]$ with r for a Legendre sequence X (left) and variation of $1/[\lim_{n\to\infty} F(Y_r)]$ with r for an m-sequence Y (right)

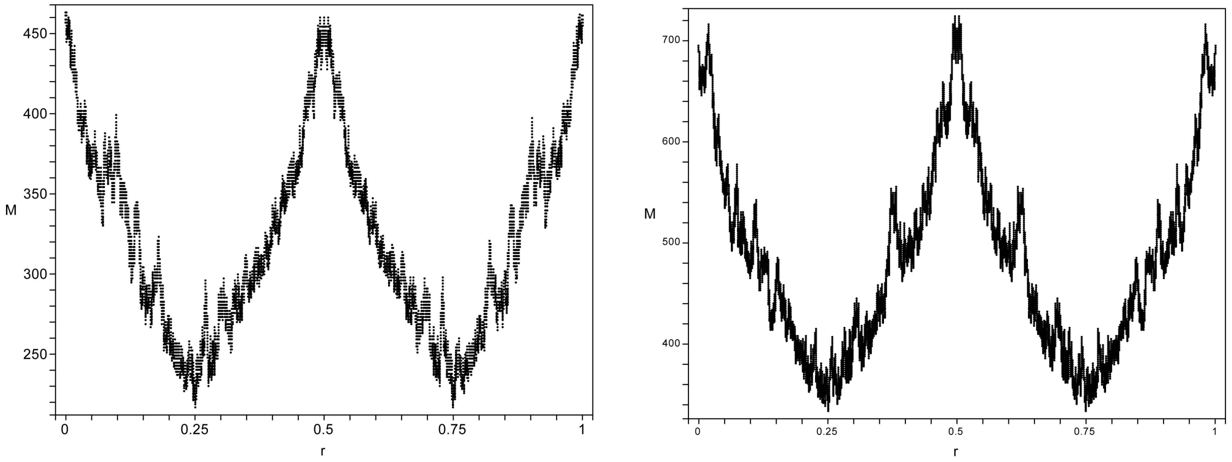

Figure 2: Variation of $M(X_r)$ with r for Legendre sequences of length $n =$ 49,999 (left) and $n =$ 104,729 (right)

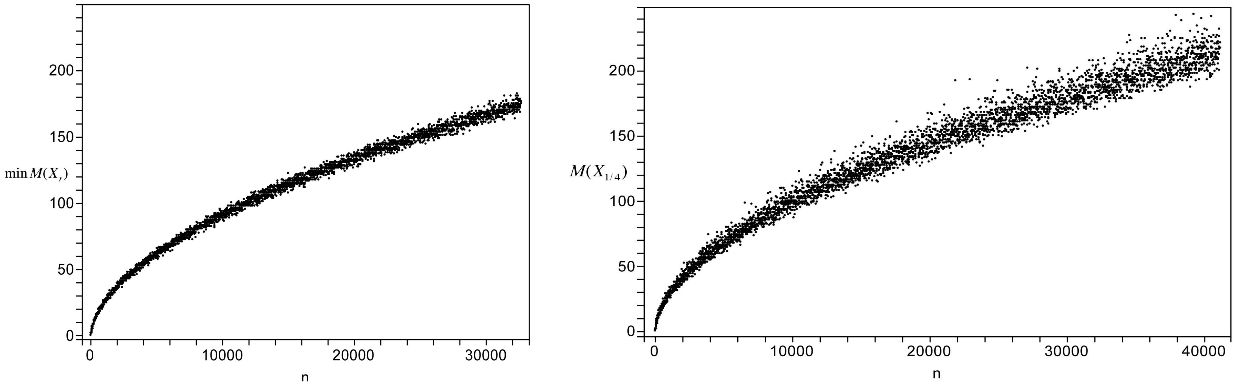

Figure 3: Variation of $\min_{r \in R} M(X_r)$ with n (left), and $M(X_{1/4})$ with n (right)

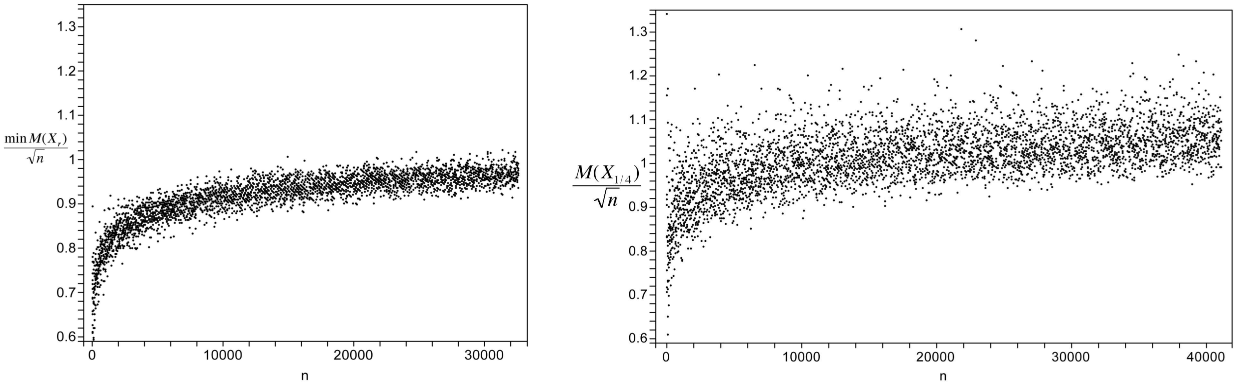

Figure 4: Variation of $\frac{\min_{r \in R} M(X_r)}{\sqrt{n}}$ with n (left), and $\frac{M(X_{1/4})}{\sqrt{n}}$ with n (right)

(Some function values for very small n lie outside the plotted range)

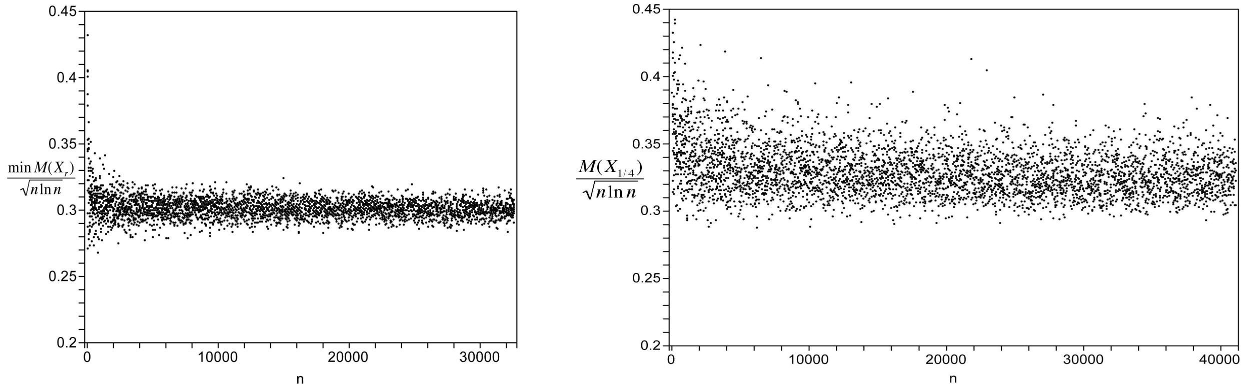

Figure 5: Variation of $\frac{\min_{r \in R} M(X_r)}{\sqrt{n \ln n}}$ with n (left), and $\frac{M(X_{1/4})}{\sqrt{n \ln n}}$ with n (right)

(Some function values for very small n lie outside the plotted range)

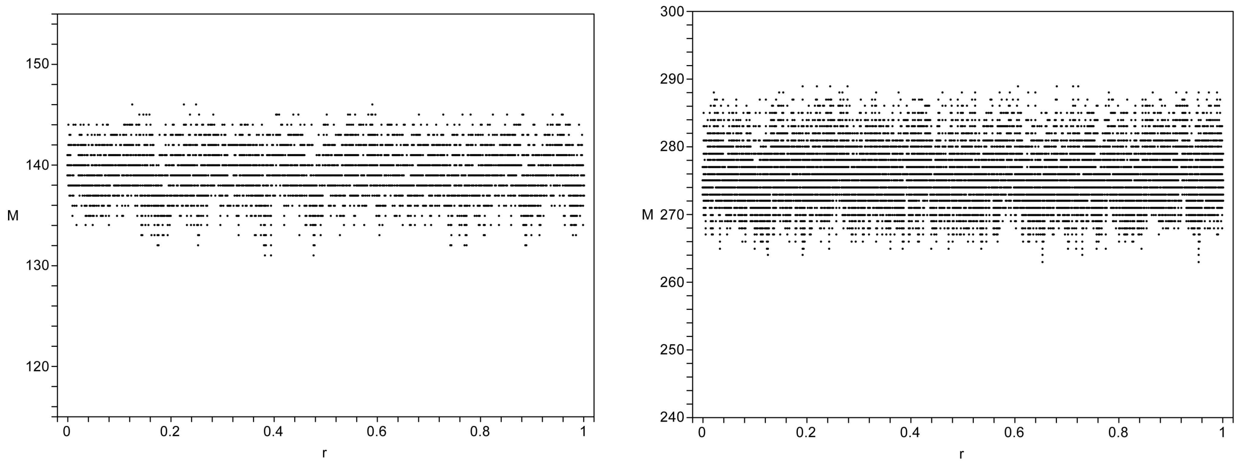

Figure 6: Variation of $M(Y_r)$ with r for m-sequences Y, for $m = 14$ and the primitive polynomial $f(x) = x^{14} + x^{13} + x^{10} + x^6 + x^2 + x + 1$ (left), and $m = 16$ and the primitive polynomial $f(x) = x^{16} + x^{15} + x^{14} + x^{12} + x^{11} + x^9 + x^8 + x^7 + x^5 + x + 1$ (right)

m	2^m-1	M_{2^m-1}	$\min\limits_{Y\in\mathcal{Y}_m} M(Y)$	$\sum\limits_{Y\in\mathcal{Y}_m} M(Y)/\lvert\mathcal{Y}_m\rvert$	$\max\limits_{Y\in\mathcal{Y}_m} M(Y)$
2	3	1	1	1.33	2
3	7	1	1	2.14	3
4	15	2	3	3.60	5
5	31	3	4	5.16	7
6	63	4	6	7.84	11
7	127	—	8	11.71	16
8	255	—	13	16.88	22
9	511	—	19	24.89	34
10	1023	—	29	35.93	46
11	2047	—	42	52.20	68
12	4095	—	61	76.45	107
13	8191	—	85	108.74	144
14	16383	—	125	156.08	207
15	32767	—	175	222.28	295
16	65535	—	(260)	—	(358)
17	131071	—	(379)	—	(547)
18	262143	—	(560)	—	(779)
19	524287	—	(790)	—	(1135)
20	1048575	—	(1221)	—	(1422)

Table 1: Summary of results on the PSL of m-sequences Y: exhaustive data for $2 \leq m \leq 15$, selected data for $16 \leq m \leq 20$. ($\mathcal{Y}_m$ is the set of all m-sequences of length 2^m-1. Numbers within round brackets indicate the min / max from partial computation for that m.)

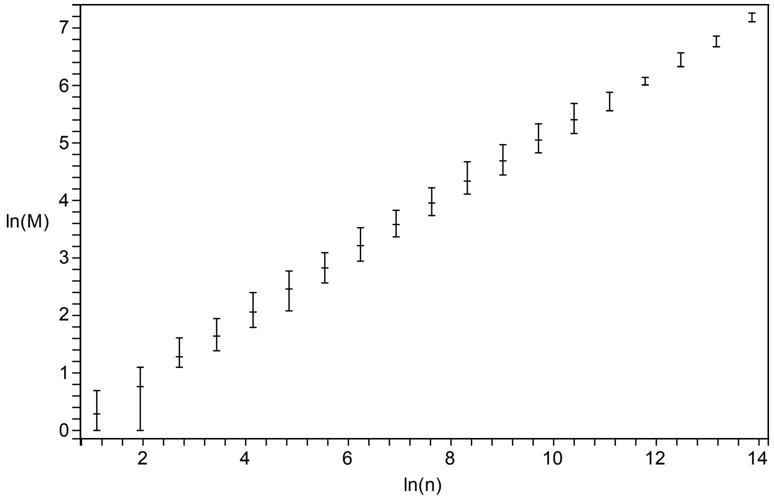

Figure 7: Summary of results on the PSL of m-sequences Y from Table 1: Variation of min / mean / max of $\ln M(Y)$ with $\ln n = \ln(2^m - 1)$

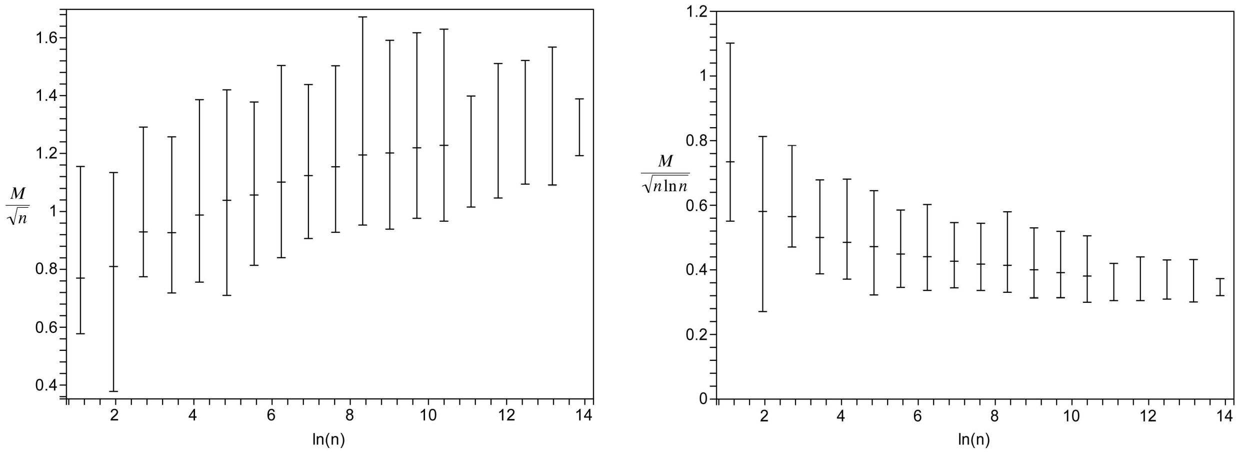

Figure 8: Min / mean / max of $M(Y)$ divided by $\sqrt{n}$ (left) and $\sqrt{n \ln n}$ (right)

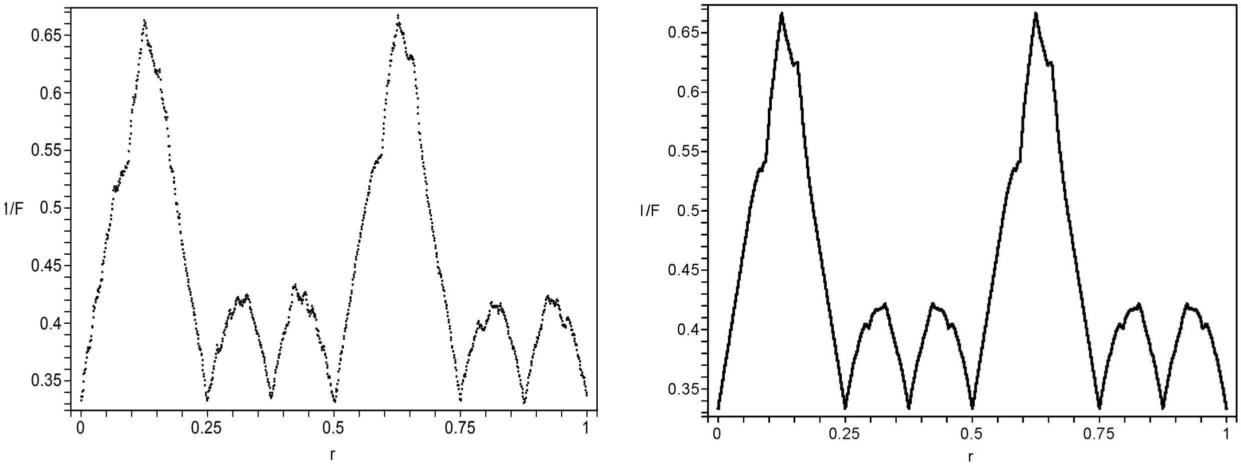

Figure 9: Variation of $1/F((X^{(m)})_r)$ with r for a Rudin-Shapiro sequence $X^{(m)}$, for $m = 10$ (left) and $m = 16$ (right)

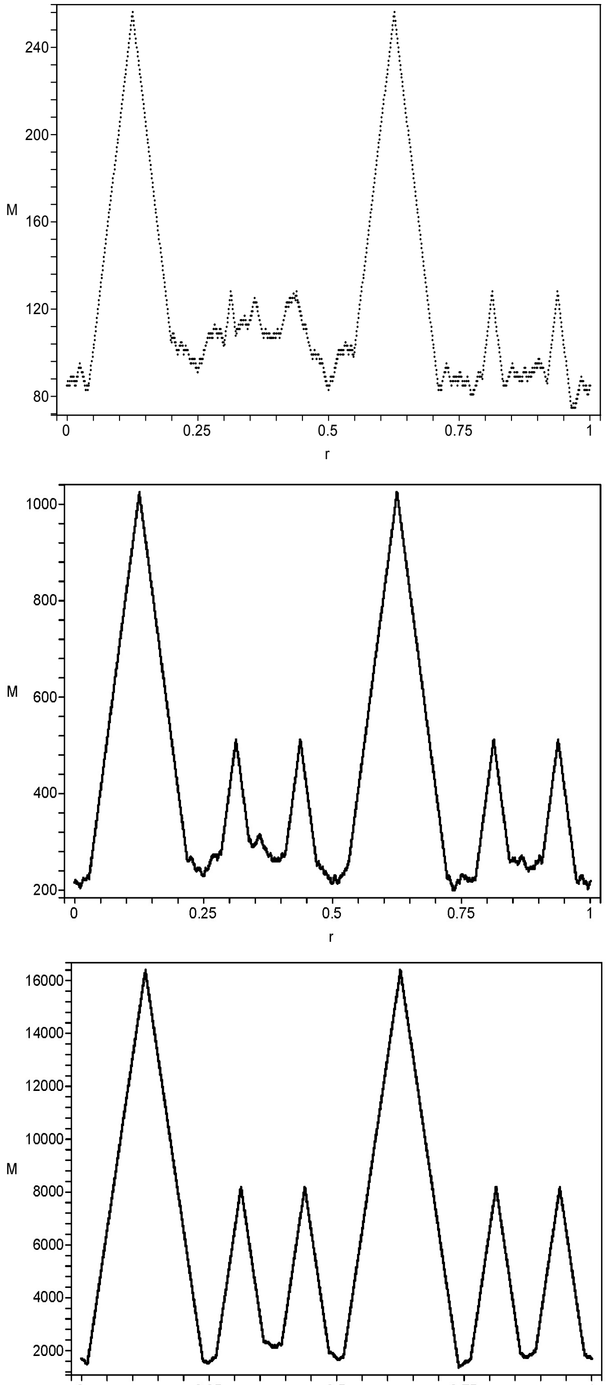

Figure 10: Variation of $M((X^{(m)})_r)$ with r for a Rudin-Shapiro sequence $X^{(m)}$, for $m = 10$ (top), $m = 12$ (middle), and $m = 16$ (bottom)