A Survey of the Merit Factor Problem for Binary Sequences

Jonathan Jedwab*
Department of Mathematics, Simon Fraser University,
Burnaby, BC, Canada V5A 1S6

23 December 2004

Abstract

A classical problem of digital sequence design, first studied in the 1950s but still not well understood, is to determine those binary sequences whose aperiodic autocorrelations are collectively small according to some suitable measure. The merit factor is an important such measure, and the problem of determining the best value of the merit factor of long binary sequences has resisted decades of attack by mathematicians and communications engineers. In equivalent guise, the determination of the best asymptotic merit factor is an unsolved problem in complex analysis proposed by Littlewood in the 1960s that until recently was studied along largely independent lines. The same problem is also studied in theoretical physics and theoretical chemistry as a notoriously difficult combinatorial optimisation problem.

The best known value for the asymptotic merit factor has remained unchanged since 1988. However recent experimental and theoretical results strongly suggest a possible improvement. This survey describes the development of our understanding of the merit factor problem by bringing together results from several disciplines, and places the recent results within their historical and scientific framework.

1 Introduction

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

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

Since the 1950s, digital communications engineers have sought binary sequences whose aperiodic autocorrelations are collectively small according to some suitable measure of "goodness" (see Section 2.1). This survey deals with an important such measure, defined by Golay [30] in 1972: the *merit factor* of a binary sequence A of length n is given by

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

*I am grateful for support from NSERC of Canada via Discovery Grant # 31-611394.

and the best binary sequences are those with the largest merit factor.

Let $\mathcal{A}_n$ be the set of all binary sequences of length n. We define F_n to be the optimal value of the merit factor for sequences of length n:

$$F_n := \max_{A \in \mathcal{A}_n} F(A).$$

The principal problem in the study of the merit factor is to determine the asymptotic behaviour of F_n:

The Merit Factor Problem. Determine the value of $\limsup_{n \longrightarrow \infty} F_n$.

Golay's publications reveal a fascination with the Merit Factor Problem spanning a period of nearly twenty years [30], [31], [32], [33], [34], [35]; the closing words of [35], published after Golay's death, refer to the study of the merit factor as "...this challenging and charming problem".

Prior to Golay's definition of merit factor in 1972, Littlewood [54] and other analysts studied questions concerning the norms of polynomials with ± 1 coefficients on the unit circle of the complex plane. As we describe in Section 2.2, the Merit Factor Problem is precisely equivalent to a natural such question involving the L_4 norm. This survey traces the historical development of the two (mostly independent) streams of investigation: the merit factor of binary sequences, and the L_4 norm of complex-valued polynomials with ± 1 coefficients on the unit circle.

A benchmark result on the asymptotic behaviour of the merit factor was given by Newman and Byrnes [62] in 1990:

Proposition 1.1. *The mean value of $1/F$, taken over all sequences of length n, is* $\dfrac{n-1}{n}$.

Proposition 1.1 shows that the asymptotic mean value of $1/F$ over all sequences of length n is 1. We cannot follow [38] in concluding that the asymptotic mean value of F itself over all sequences of length n is 1 [68], but we expect that "good" sequences will have an asymptotic value of F greater than 1. Indeed, the best known asymptotic results to date are given by explicitly constructed families of sequences whose merit factor tends to 6 (see Theorems 4.1, 4.6 and 4.7). The current state of knowledge regarding the Merit Factor Problem can therefore be summarised as:

$$6 \leq \limsup_{n \longrightarrow \infty} F_n \leq \infty. \tag{3}$$

Both of the extreme values in (3) have been conjectured to be the true value of the lim sup:

Conjecture 1.2 (Høholdt and Jensen, 1988 [39])**.** $\limsup_{n \longrightarrow \infty} F_n = 6$.

Conjecture 1.3 (Littlewood, 1966 [53, §6])**.** $\limsup_{n \longrightarrow \infty} F_n = \infty$.

Littlewood [53] also proposed stronger versions of Conjecture 1.3:

(i) $\lim_{n \longrightarrow \infty} F_n = \infty$

(ii) $1/F_n = O(1/\sqrt{n})$ for infinitely many n

(iii) $1/F_n = O(1/\sqrt{n})$ for all n.

My impression is that most researchers are reluctant to take seriously even the weakest of Littlewood's proposals, Conjecture 1.3, perhaps because the identity of their originator does not seem to be widely known.

Considerable computational evidence has been amassed regarding the value of F_n for specific values of n, in order to shed light on the Merit Factor Problem. Where computationally feasible, the actual value of F_n has been calculated; for larger values of n we have lower bounds on F_n via the identification of good, though not necessarily optimal, sequences (see Section 3). Indeed, Conjectures 1.2 and 1.3 are both based at least partially on numerical data. Conjecture 1.2 was made in light of Theorem 4.1 and its proof in [39], together with an examination of large values of F found in [4] for sequences of odd length between 100 and 200. Conjecture 1.3 and the stronger versions (i), (ii) and (iii) listed above were based primarily on calculation of F_n for $7 \leq n \leq 19$; Littlewood [53] asserted that "the evidence seems definitely in favour of [these conjectures]", and reiterated in 1968 [54] that "the numerical evidence for [these conjectures] is very strong". In terms of the computational power readily available nowadays, the range of Littlewood's calculations from the 1960s appears woefully inadequate! By 1996 Mertens [58] had calculated the value of F_n for $n \leq 48$ and reached the "tentative conclusion" that $\lim_{n\longrightarrow\infty} F_n > 9$. Currently the value of F_n has been calculated [59] for $n \leq 60$, and large values of F are known [45] for $61 \leq n \leq 271$ (see Figure 1).

Some authors seem to have conjectured that $\limsup_{n\longrightarrow\infty} F_n$ is given by the largest merit factor value known to be consistently achievable for long sequences at the time of writing. For example, Newman and Byrnes [62] incorrectly conjectured in 1990 that $\lim_{n\longrightarrow\infty} F_n = 5$, "... based on extensive numerical evidence employing the Bose-Einstein statistics methodology of statistical mechanics". Likewise, as noted above, Høholdt and Jensen [39] based Conjecture 1.2 in part on the best known merit factors reported in 1985 in [4] for sequences of odd length between 100 and 200, which they described as "either strictly smaller than or suspiciously close to 6"; however the current data underlying Figure 1 shows that the best merit factor is actually greater than 8 for all of these odd sequence lengths. In contrast, Golay [33] proposed in 1982 that $\limsup_{n\longrightarrow\infty} F_n \simeq 12.32$ (see Section 4.7) and yet in 1983 wrote that [34] "... the eventuality must be considered that no systematic synthesis will ever be found which will yield higher merit factors [than 6]"!

Recent work of Borwein, Choi and Jedwab [13] provides numerical evidence, from sequences up to millions of elements in length, that $\limsup_{n\longrightarrow\infty} F_n > 6.34$ (see Section 5). This conclusion, which would increase the best known asymptotic merit factor for the first time since 1988, is implied by Conjecture 5.3 on the behaviour of a specified infinite family of sequences.

The remainder of this survey is organised as follows. Section 2 gives a detailed practical motivation for the Merit Factor Problem from digital sequence design, together with a theoretical motivation from complex analysis. Section 3 describes various experimental computational approaches that have been used to gather numerical data, including exhaustive search and stochastic algorithms. Section 4 explains the main theoretical approaches

that have been used to analyse the Merit Factor Problem. Section 5 outlines the method and results of [13], which suggest a new lower bound for $\limsup_{n\longrightarrow\infty} F_n$. Section 6 is a selection of challenges for future study.

This survey is concerned only with binary sequences, although the definition of merit factor has been extended to real-valued sequences (see for example [1]) as well as to binary arrays of dimension larger than 1 (see for example [8]). I have found the earlier surveys of Jensen and Høholdt [41] and Høholdt [38] to be helpful in preparing this paper, particularly when writing Section 4.

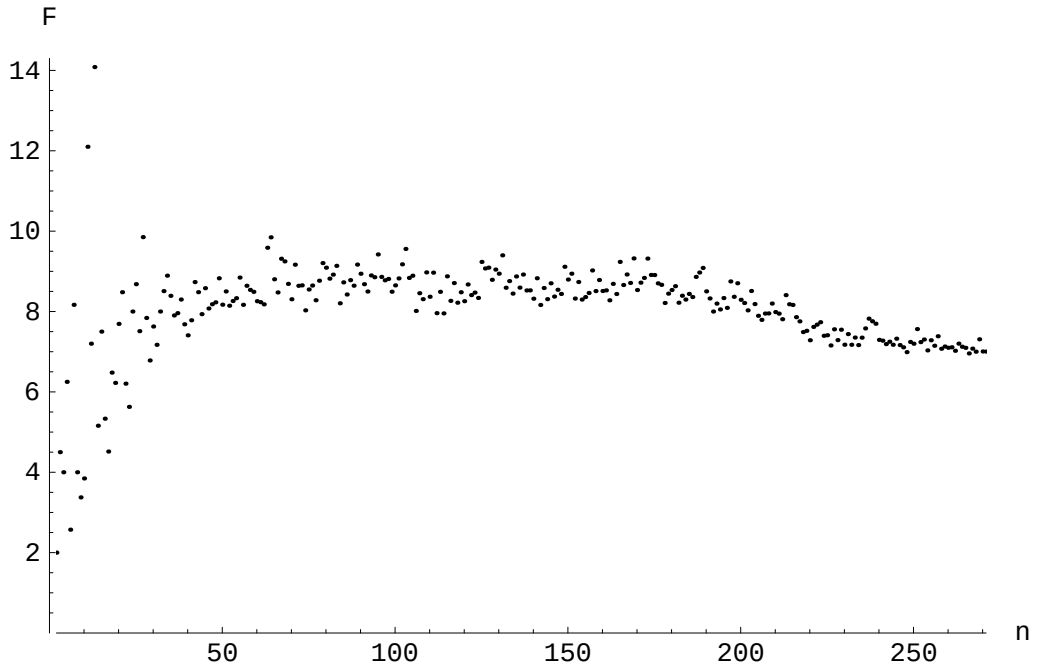

Figure 1: The optimal merit factor (for $2 \leq n \leq 60$) and the best known merit factor (for $61 \leq n \leq 271$) for binary sequences of length n.

2 Practical and Theoretical Motivation

This section shows how the Merit Factor Problem arises independently in digital sequence design and complex analysis.

2.1 Digital Sequence Design

Since the 1950s, digital communications engineers have sought to identify those binary sequences whose aperiodic autocorrelations are collectively as small as possible, for application in synchronisation, pulse compression and especially radar [74]. This classical

problem of digital sequence design remains largely unsolved. In 1953 Barker [2] proposed that an ideal binary sequence of length n is one for which

$$C(u) = -1 \text{ or } 0 \quad \text{for } 0 < u < n,$$

but could find examples only for lengths $n = 3$, 7 and 11. Subsequent authors relaxed Barker's condition to:

$$|C(u)| = 1 \text{ or } 0 \quad \text{for } 0 < u < n, \tag{4}$$

and binary sequences satisfying (4) became known as *Barker sequences*. By a parity argument, no binary sequence can have a smaller value of $|C(u)|$ than a Barker sequence for any u. However the only non-trivial lengths for which Barker sequences are known to exist are 2, 3, 4, 5, 7, 11 and 13, and it has long been conjectured that no other sequence lengths n are possible:

Conjecture 2.1. *There is no Barker sequence of length $n > 13$.*

I do not know who first proposed Conjecture 2.1 but it is implied by Ryser's Conjecture [67] of 1963 on cyclic difference sets (see [48] for recent progress on this conjecture), and Turyn [74] declared in 1968: "There is overwhelming evidence that there are no Barker sequences [with $n > 13$]". A weaker version of Conjecture 2.1, alluded to in [74], states that there are only finitely many lengths n for which a Barker sequence of length n exists. In order to continue the historical account we introduce some further definitions.

The *periodic autocorrelation* of a binary sequence $A = (a_0, a_1, \ldots, a_{n-1})$ at shift u is given by

$$R_A(u) := \sum_{i=0}^{n-1} a_i a_{(i+u) \bmod n} \qquad \text{for } u = 0, 1, \ldots, n-1, \tag{5}$$

so that

$$R_A(u) = C_A(u) + C_A(n-u) \qquad \text{for } 0 < u < n. \tag{6}$$

A (v, k, λ) *cyclic difference set* is a k-element subset D of the cyclic group $\mathbb{Z}_v$ for which the multiset of differences $\{d_1 - d_2 : d_1, d_2 \in D,\ d_1 \neq d_2\}$ contains each non-zero element of $\mathbb{Z}_v$ exactly λ times (see [6] for background on difference sets, including generalisation to non-cyclic groups). The following is well-known (see for example [3]):

Proposition 2.2. *A (v, k, λ) cyclic difference set D is equivalent to a binary sequence $A = (a_0, a_1, \ldots, a_{v-1})$ having k elements -1 and constant periodic autocorrelation $R_A(u) = v - 4(k - \lambda)$ for $0 < u < v$, via the relationship*

$$i \in D \text{ if and only if } a_i = -1, \quad \text{for } 0 \leq i < v.$$

Turyn and Storer [72] showed in 1961 that Conjecture 2.1 is true for odd n, and that if a Barker sequence A of even length $n > 2$ exists then it satisfies $R_A(u) = 0$ for $0 < u < n$. Therefore, by Proposition 2.2, if there is a Barker sequence of length $v > 13$ then there is a

cyclic difference set in $\mathbb{Z}_v$ satisfying $v = 4(k - \lambda)$. Difference sets satisfying this condition are known as *Hadamard* difference sets, and [73] must satisfy

$$(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N) \quad \text{for integer } N. \tag{7}$$

(See [20] for a survey of difference sets with parameters (7); note that the difference set parameters (v, k, λ) given in (17) are unfortunately *also* called Hadamard.)

In his celebrated 1965 paper [73], Turyn showed that if there is a cyclic difference set with parameters (7) in $\mathbb{Z}_{4N^2}$ having $N \neq 1$, then $N \geq 55$. The paper [73] established the systematic use of algebraic number theory in the study of difference sets, which is now a standard and much-used technique. (See [6] for an overview of this technique, and some precursors to [73]; see [49] for dramatic improvements to the smallest open case for a Barker sequence and for a cyclic difference set with parameters (7).) R. Turyn has confirmed [personal communication, May 2003] that the chain of reasoning presented here, beginning with the search for binary sequences with small aperiodic autocorrelations, was the principal motivation behind [73]. I find it noteworthy that there has been a striking expansion of knowledge regarding difference sets since the publication of [73] and yet we still have not reached a comparably deep understanding of the original motivating problem.

Once it became apparent that the ideal behaviour given by a Barker sequence is unlikely to be achieved beyond length 13, attention turned [69], [74] to two measures of how closely the aperiodic autocorrelations of a binary sequence A of length n can collectively approach the ideal behaviour. These two measures are:

$$\sum_{u=1}^{n-1} [C_A(u)]^2 \tag{8}$$

and

$$M(A) := \max_{0<u<n} |C_A(u)|. \tag{9}$$

The first measure (8) is simply $n^2/(2F(A))$, which was actually used by communications engineers as a measure of the "goodness" of a binary sequence several years before Golay [30] defined the merit factor in 1972 (see Section 3.2 for mention of Lunelli's work [55] of 1965 in this context).

The second measure (9) has been less well studied. By analogy with F_n, define

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

to be the optimal value of $M(A)$ for sequences of length n. By exhaustive search, Turyn [74] showed that $M_n \leq 2$ for $n \leq 21$ in 1968 and Lindner [51] determined M_n for $n \leq 40$ in 1975 using specialised hardware. In 1990 Cohen, Fox and Baden [18] found M_n for $n \leq 48$ by fixing sequence elements one pair at a time, working from the endpoints towards the centre and retaining only sequences with a prescribed maximum value of $|C(u)|$. Further calculations along similar lines by Coxson, Hirschel and Cohen [19] in 2001 found M_n for $n \leq 69$. From [18] and [19] we have $M_n \leq 3$ for all $n \leq 48$ and $M_n \leq 4$ for all $n \leq 69$; the value of M_n broadly increases with n, but not monotonically. In 1968 Moon and Moser [61] used elementary counting arguments to establish an (apparently weak) upper bound on M_n:

Theorem 2.3. *For any fixed* $\epsilon > 0$, $M_n \leq (2+\epsilon)(n \log n)^{1/2}$.

I can see three possible explanations for the relative popularity of the measure (8) over (9). The first is that we have a more developed theoretical framework for studying the merit factor (see Section 4). The second is that the merit factor is a natural measure of the energy efficiency of a binary sequence used for physical transmission of information (see (13) and the comments following it). The third was offered by Turyn [74, p. 199] in 1968: "Intuitively one would expect [determination of $\limsup_{n\longrightarrow\infty} F_n$] to be easier [than determination of $\liminf_{n\longrightarrow\infty} M_n$]"!

2.2 Complex Analysis

We now describe an equivalent formulation of the Merit Factor Problem from complex analysis. Let $P_A(z) := \sum_{i=0}^{n-1} a_i z^i$ be the complex-valued polynomial whose coefficients are the elements of the binary sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n. The L_4 *norm* of the polynomial $P_A(z)$ on the unit circle of the complex plane is defined to be

$$||P_A(z)||_4 := \left(\int_0^1 |P_A(\exp(2\pi\theta\sqrt{-1}))|^4 d\theta \right)^{1/4}, \tag{10}$$

and it is straightforward to show [53] that

$$||P_A(z)||_4^4 = n^2 + 2\sum_{u=1}^{n-1} [C_A(u)]^2. \tag{11}$$

Therefore the merit factor of the sequence A is related to the L_4 norm of the corresponding polynomial of degree $n-1$ by

$$||P_A(z)||_4^4 = n^2 \left(1 + \frac{1}{F(A)}\right), \tag{12}$$

and a large merit factor corresponds to a small L_4 norm. (See [17] for a survey of extremal problems involving the L_4 norm and other norms of complex-valued polynomials with ± 1 coefficients.)

Statements such as Proposition 1.1 and Conjecture 1.3 were originally made in terms of the L_4 norm of ± 1 polynomials, but have been expressed here in terms of the merit factor using (12). (Results that are recast in terms of the merit factor in this way often appear initially to be different from their original L_4 formulation because complex analysis usually considers polynomials of degree n, whereas (11) and (12) involve a polynomial of degree $n-1$.) However the results from the sequence design literature have not always been known to the complex analysis community, and vice-versa. For example, Littlewood [53] stated the correspondence (11) in 1966 without naming the aperiodic autocorrelation coefficients, and highlighted the lengths $n = 7$, 11 and 13 as supporting binary sequences satisfying (4) without mentioning Barker sequences (see Section 2.1). If Littlewood had been aware of the nonexistence results for Barker sequences already found by Turyn and Storer [72] in 1961 and by Turyn [73] in 1965, I do not believe he would have proposed

Conjecture 1.3 in 1966 [53], repeated it in 1968 [54, Problem 19], and on both occasions cited as strong evidence the calculated value of F_n for $7 \leq n \leq 19$. Likewise, in 1988 Høholdt and Jensen [39] restated the correspondence (11) and explicitly linked the merit factor of binary sequences to complex-valued polynomials with ± 1 coefficients on the unit circle (to my knowledge, for the first time). But they then declared: "Unfortunately, there have been no results on [integrals of the type (10)], which can give new information on the behavior of the merit factor", whereas Littlewood [54] had given Theorem 4.2 in 1968.

Since $\int_0^1 |P_A(\exp(2\pi\theta\sqrt{-1}))|^2 d\theta = \sum_{i=0}^{n-1} a_i^2 = n$, we deduce from (2), (10) and (11) that

$$\int_0^1 \left\{ \left| P_A(\exp(2\pi\theta\sqrt{-1})) \right|^2 - n \right\}^2 d\theta = \frac{n^2}{F(A)}. \tag{13}$$

The left-hand side of (13) measures, in terms of power, how much the amplitude spectrum of the continuous-time signal corresponding to the sequence A deviates from its mean value n [4]. Therefore a larger merit factor corresponds to a more uniform distribution of the signal energy over the frequency range, which is of particular importance in spread-spectrum radio communications.

We have seen in Proposition 2.2 that a cyclic difference set is equivalent to a binary sequence A having constant periodic autocorrelation at all non-zero shifts. In terms of the corresponding polynomial $P_A(z)$, it is equivalent to the value $|P_A(z)|$ being constant at all complex nth roots of unity except 1.

Conjecture 1.3 is related to another old conjecture from complex analysis involving the supremum norm of ± 1 polynomials on the unit circle:

Conjecture 2.4 (Erdös, 1957 [24, Problem 22])**.** *There exists a constant $c > 0$ such that, for all n and for all binary sequences $A = (a_0, a_1, \ldots a_{n-1})$ of length n,*

$$\sup_{|z|=1} |P_A(z)| \geq (1+c)\sqrt{n}$$

where $P_A(z) := \sum_{i=0}^{n-1} a_i z^i$.

(Conjecture 2.4 was posed in [24] as a question as to whether a suitable $c > 0$ exists for complex-valued sequences satisfying $|a_i| = 1$ for all i, and restated [25] in 1962 as a conjecture. Kahane [43] showed that the conjecture is false for complex-valued sequences, but the restriction of the question to binary sequences remains open.) Since $\sup_{|z|=1} |P_A(z)| \geq ||P_A(z)||_4$, we deduce from (12) that if Conjecture 1.3 is false then Conjecture 2.4 is true.

Furthermore, by (2) and (4), a Barker sequence of even length n must have merit factor n, so if Conjecture 1.3 is false then the weaker version of Conjecture 2.1 (that there are only finitely many Barker sequences) is also true. So determining whether $\limsup_{n \longrightarrow \infty} F_n$ is unbounded would be of great significance: if so then a 1966 conjecture due to Littlewood is established; and if not then both a 1957 conjecture due to Erdös and a forty-year-old conjecture on the finiteness of the number of Barker sequences are true!

3 Computational Approaches

An experimental approach to mathematics has long provided "... a compelling way to generate understanding and insight; to generate and confirm or confront conjectures; and generally to make mathematics more tangible, lively and fun..." [9]. The view of mathematics as an experimental science has become more prominent as computers of steadily increasing power have become widely accessible to perform the role of "laboratory". In this spirit, considerable computational evidence has been collected regarding the value of F_n for specific values of n, in order to better understand the Merit Factor Problem.

The value of F_n has been calculated for $n \leq 60$ using exhaustive computation (see Section 3.2). A lower bound on F_n has been found for $61 \leq n \leq 271$ using stochastic search algorithms to identify good, though not necessarily optimal, sequences (see Section 3.3). The available evidence for $n \leq 271$ is summarised in Figure 1. The two largest known values of F_n are $F_{13} \simeq 14.1$ and $F_{11} = 12.1$, both of which arise from Barker sequences (see Section 2.1); no other values of $F_n \geq 10$ are known. The known lower bounds for F_n suffer a reduction for values of n beyond about 200. However one would expect a reduction of this sort owing to the increased computational burden for larger n and the large number of local optima in the search landscape (see Section 3.3). Indeed, previous versions of Figure 1, representing less extensive computational effort, have exhibited a similar phenomenon but at smaller values of n.

3.1 Skew-Symmetric Sequences

A common strategy for extending the reach of merit factor computations (both exhaustive and stochastic) is to impose restrictions on the structure of the sequence. The most popular of these historically has been the restriction to a *skew-symmetric* binary sequence, defined by Golay [30] in 1972 as a binary sequence $(a_0, a_1, \ldots, a_{2m})$ of odd length $2m+1$ for which

$$a_{m+i} = (-1)^i a_{m-i} \quad \text{for } i = 1, 2, \ldots, m. \tag{14}$$

(Condition (14) had also been noted by Littlewood [53], [54] in relation to a question involving the supremum norm of ± 1 polynomials on the unit circle).

Skew-symmetric sequences are known to attain the optimal merit factor value F_n for the following odd values of $n < 60$: 3, 5, 7, 9, 11, 13, 15, 17, 21, 27, 29, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57 and 59. Indeed, Golay [32] used the observation that all odd length Barker sequences are skew-symmetric to propose the skew-symmetric property as a sieve in searching for sequences with large merit factor. The computational advantage of this sieve is that it roughly doubles the sequence length that can be searched with given computational resources. Furthermore, as noted by Golay [30], half the aperiodic autocorrelations of a skew-symmetric sequence are 0:

Proposition 3.1. *A skew-symmetric binary sequence A of odd length has $C_A(u) = 0$ for all odd u.*

Golay [32] proposed that the asymptotic optimal merit factor of the set of skew-symmetric sequences is equal to $\limsup_{n \longrightarrow \infty} F_n$, so that nothing is lost by restricting

attention to this set. Although Golay's argument was heuristic and relied on the unproven "Postulate of Mathematical Ergodicity" (see Section 4.7), we know [10, p. 33] that the asymptotic value of the *mean* merit factor does not change when we restrict to skew-symmetric sequences (by comparison with Proposition 1.1):

Proposition 3.2. *The mean value of* $1/F$*, taken over all skew-symmetric sequences of odd length* n*, is* $\dfrac{(n-1)(n-2)}{n^2}$.

The optimal merit factor over all skew-symmetric sequences of odd length n was calculated by Golay [32] for $n \leq 59$ in 1977. It was then calculated independently by Golay and Harris [35] for $n \leq 69$ in 1990 and by de Groot, Würtz and Hoffmann [22] for $n \leq 71$ in 1992. It would be feasible, using the methods of Section 3.2, to extend these results to lengths up to around 119 (involving 60 arbitrary sequence elements), although it is not clear to me that this would represent a useful investment of computational resources.

In 1990 Golay and Harris [35] found good skew-symmetric sequences for odd lengths n in the range $71 \leq n \leq 117$ by regarding a skew-symmetric sequence as the interleaving of two constrained sequences: one symmetric and the other anti-symmetric. They formed candidate sets S_1 of symmetric sequences and S_2 of anti-symmetric sequences, each of whose members had large merit factor relative to other sequences of the same type, and then found the largest merit factor over all interleavings of a sequence from S_1 with a sequence from S_2.

3.2 Exhaustive Computation

The value of F_n has been calculated:

(i) for "small n" in 1965 by Lunelli [55], as referenced in [74] (and expressed in terms of minimising (8))

(ii) for $7 \leq n \leq 19$ by Swinnerton-Dyer, as presented by Littlewood [54] in 1966 (and expressed in terms of minimising (11))

(iii) for $n \leq 32$ by Turyn, as presented by Golay [33] in 1982

(iv) for $n \leq 48$ in 1996 by Mertens [58]

(v) for $n \leq 60$ (the current record) by Mertens and Bauke [59].

The merit factor of a binary sequence of length n can be calculated from (1) and (2) in $O(n^2)$ operations. The computations for a given sequence can be re-used to calculate the merit factor of other sequences of the same length by changing one sequence element at a time and updating the aperiodic autocorrelations in $O(n)$ operations for each such change. The determination of F_n by calculating the merit factor in this way for all 2^n sequences of length n, for example by using a Gray code, requires $O(n2^n)$ operations. However the algorithm of [58] and [59] reduces the exponential term of the complexity of determining F_n from 2^n to roughly 1.85^n by means of a branch-and-bound algorithm. The principle is to fix the sequence elements one pair at a time, working from the endpoints towards

the centre and pruning the search tree by bounding $\sum_{u>0}[C(u)]^2$. (See Section 2.1 for a a similar idea applied to the calculation of M_n in [18] and [19], reducing the exponential term of the complexity of that calculation from 2^n to roughly 1.4^n.)

3.3 Stochastic Search Algorithms

For a given sequence length n, the search for a good lower bound for F_n can be viewed as a combinatorial optimisation problem over the space of 2^n binary sequences. This problem, often referred to as the "low autocorrelated binary string problem", has been studied in theoretical physics in connection with quantum models of magnetism as well as in theoretical chemistry. Early results [4], [5], [22] from the application of simulated annealing and evolutionary algorithms to the optimisation problem were rather disappointing, finding merit factor values no larger than about 6 for sequence lengths of around 200 and often failing to find previously known large merit factor values. Bernasconi [5] predicted from computational experiments that "... stochastic search procedures will not yield merit factors higher than about $F = 5$ for long sequences" (referring to lengths greater than about 200), and the problem was declared [22] to be "... amongst the most difficult optimization problems".

Several authors [5], [58], [60] suggested that the combinatorial landscape of the search space exhibits "golf-hole" behaviour, in the sense that the sequences attaining F_n are extremely isolated within the landscape (see [65] for an overview of combinatorial landscapes). This suggestion appears to have originated with an unfavourable comparison between empirically obtained merit factor values and the value of approximately 12.32... conjectured by Golay [33] for $\limsup_{n\longrightarrow\infty} F_n$, even though Golay's value depends on an unproven hypothesis (see Section 4.7). But, while the landscape has an exceptionally large number of local optima [23], after detailed analysis Ferreira, Fontanari and Stadler [27] found no evidence of "golf-hole" behaviour and suggested that the difference in difficulty between this and other problems of combinatorial optimisation is quantitative rather than qualitative.

As recognised in [22], the performance of stochastic search algorithms can vary significantly according to the care with which the algorithm parameters are tuned. In 1998 Militzer, Zamparelli and Beule [60] used an evolutionary algorithm to obtain more encouraging numerical results for sequence lengths up to about 200 — although they still considered that the search for a binary sequence attaining the optimal value F_n "... resembles the search for a needle in the haystack"! The best currently known stochastic search results, on which Figure 1 is based, are due to Borwein, Ferguson and Knauer [14] (with possible updates listed at [45]). These results rely on a combination of algorithmic improvements and extended use of considerable computational resources.

The basic method underlying many of the stochastic search algorithms is to move through the search space of sequences by changing only one, or sometimes two, sequence elements at a time. This method was suggested by Golay [31] as early as 1975, in relation to skew-symmetric sequences. The merit factor of any close neighbour sequence can be calculated in $O(n)$ operations from knowledge of the aperiodic autocorrelations of the current sequence. The search algorithm specifies when it is acceptable to move to a neighbour

sequence, for example when it has merit factor no smaller than the current sequence, or when it has the largest merit factor amongst all close neighbours not previously visited. The search algorithm must also specify how to choose a new sequence when no acceptable neighbour sequence can be found. The method of [14] augments this search strategy to allow the addition or removal of one outer sequence element at a time.

Many authors [4], [22], [32], [35] [60] have applied stochastic search algorithms only to skew-symmetric sequences in order to obtain results for lengths that would otherwise be out of computational reach (see Section 3.1). The results of [14] for all lengths $n \geq 103$ (both odd and even) are based on searches for which the initial sequence is skew-symmetric.

Despite recent improvements, no stochastic search algorithm has yet been found that reliably produces binary sequences with merit factor greater than 6 in reasonable time for large n. Therefore such algorithms cannot yet shed light on whether the known range for $\limsup_{n\longrightarrow\infty} F_n$ given in (3) can be narrowed.

4 Theoretical Approaches

In this section we consider theoretical approaches to the Merit Factor Problem, based mostly on infinite families of binary sequences with specified structure.

4.1 Legendre Sequences

We begin with the strongest proven asymptotic result. The *Legendre sequence* $X = (x_0, x_1, \ldots, x_{n-1})$ of prime length n is defined by:

$$x_i := \left(\frac{i}{n}\right) \quad \text{for } 0 \leq i < n,$$

where $\left(\frac{i}{n}\right)$ is the Legendre symbol (which takes the value 1 if i is a quadratic residue modulo n and the value -1 if not; we choose the convention that $\left(\frac{i}{n}\right) := 1$ if $i = 0$). Given a sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n and a real number r, we write A_r for the sequence $(b_0, b_1, \ldots, b_{n-1})$ obtained by *rotating* (equivalently, cyclically shifting) the sequence A by a multiple r of its length:

$$b_i := \; a_{(i+\lfloor rn \rfloor) \bmod n} \quad \text{for } 0 \leq i < n. \tag{15}$$

In 1981 Turyn calculated the merit factor of the rotation X_r of the Legendre sequence X for sequence lengths up to 10,000, as reported in [34]. Based on Turyn's work Golay [34] gave a derivation of the asymptotic value of this merit factor, which accorded with Turyn's calculations but relied on heuristic arguments as well as the "Postulate of Mathematical Ergodicity" (see Section 4.7). In 1988 Høholdt and Jensen [39] proved that the expression derived by Golay is in fact correct:

Theorem 4.1. *Let X be a Legendre sequence of prime length n. Then*

$$\frac{1}{\lim\limits_{n\longrightarrow\infty} F(X_r)} = \begin{cases} \frac{1}{6} + 8(r - \frac{1}{4})^2 & \text{for } 0 \leq r \leq \frac{1}{2} \\ \frac{1}{6} + 8(r - \frac{3}{4})^2 & \text{for } \frac{1}{2} \leq r \leq 1. \end{cases} \tag{16}$$

Therefore the asymptotic merit factor of the optimal rotation of a Legendre sequence is 6 and occurs for $r = 1/4$ and $r = 3/4$. Borwein and Choi [12] subsequently determined the exact, rather than the asymptotic, value of $F(X_r)$ for all r. In the optimal cases $r = 1/4$ and $r = 3/4$, this exact value involves the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$.

The analytical method used by Høholdt and Jensen [39], and its refinement in [12], applies only to odd-length sequences and depends crucially on the relationship of the sequence to a cyclic difference set, in this case belonging to the parameter class

$$(v, k, \lambda) = (n, (n-1)/2, (n-3)/4) \quad \text{for integer } n \equiv 3 \pmod 4. \tag{17}$$

(Many constructions for difference sets with parameters (17) are known; see [75] for a survey and [37] for an important recent result. The parameter class (17) is referred to as *Hadamard*, but unfortunately so is another parameter class (7).)

It is well known (see for example [6]) that, for $n \equiv 3 \pmod 4$, a Legendre sequence X of length n is equivalent to a cyclic difference set in $\mathbb{Z}_n$ with parameters from the class (17), known as a *quadratic residue* or *Paley* difference set. By Proposition 2.2 this is equivalent to X having constant periodic autocorrelation at all non-zero shifts, and this property is retained under all rotations of the sequence:

$$R_{X_r}(u) = -1 \quad \text{for } 0 \le r \le 1 \text{ and } 0 < u < n. \tag{18}$$

Therefore, from (6), every rotation of a Legendre sequence of length $n \equiv 3 \pmod 4$ has the property that its aperiodic autocorrelations sum in pairs to -1. Of course this does not imply that the individual aperiodic autocorrelations will themselves have small magnitude but one might hope that, for some rotation, the full set of aperiodic autocorrelations will have a small sum of squares. Indeed, R. Turyn has indicated [personal communication, May 2003] that this was exactly his rationale for investigating these sequences. (Similar reasoning was used by Boehmer [7] in seeking binary sequences A with a small value of $M(A)$, as defined in (9), from sequences having small periodic autocorrelation at all non-zero shifts.) For $n \equiv 1 \pmod 4$, all rotations of a Legendre sequence are equivalent to a *partial difference set* in $\mathbb{Z}_n$ [56, Theorem 2.1] and can be dealt with in a similar manner to the case $n \equiv 3 \pmod 4$, for example [13] by slight modification to the sequence.

An asymptotic merit factor of 6, as given by the family of Legendre sequences in Theorem 4.1, is the largest so far proven. We shall see in Section 5 that there is strong evidence, although not a proof, that an asymptotic merit factor greater than 6.34 can be achieved via a related family of sequences. I find it remarkable that both of these constructions, as well as others described in this section, rely directly on special *periodic* autocorrelation properties of the sequences. In my opinion this is a reflection of the current paucity of powerful tools for analysing aperiodic autocorrelations independently of their periodic properties. Indeed, while periodic behaviour lends itself readily to mathematical investigation via techniques from algebra and analysis based on an underlying cyclic group or finite field, it remains the case [26, p. 269] that "... the aperiodic correlation properties of sequences are notoriously difficult to analyse"; see [64] for further discussion of this point. Given the appropriate mathematical tools, I believe we might uncover asymptotic merit factors significantly greater than those suggested by the results of Section 5.

The method introduced by Høholdt and Jensen [39] to calculate the asymptotic merit factor of rotated Legendre sequences was subsequently applied to further families of odd-length binary sequences corresponding to cyclic difference sets with parameters in the class (17) (see Sections 4.4 and 4.6).

4.2 Rudin-Shapiro Sequences

We next consider the earliest asymptotic merit factor result of which I am aware. 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' we write $A; A'$ for the sequence $(b_0, b_1, \ldots, b_{n+n'-1})$ given by *appending* A' to A:

$$b_i := \begin{cases} a_i & \text{for } 0 \le i < n \\ a'_{i-n} & \text{for } n \le i < n + n'. \end{cases} \tag{19}$$

The *Rudin-Shapiro sequence pair* $X^{(m)}$, $Y^{(m)}$ of length 2^m is defined recursively [66], [71] by:

$$X^{(m)} := X^{(m-1)}; Y^{(m-1)}, \tag{20}$$

$$Y^{(m)} := X^{(m-1)}; -Y^{(m-1)}. \tag{21}$$

where $X^{(0)} = Y^{(0)} := [1]$. In 1968 Littlewood [54, p. 28] proved (in the language of complex-valued polynomials — see Section 2.2):

Theorem 4.2. *The merit factor of both sequences $X^{(m)}$, $Y^{(m)}$ of a Rudin-Shapiro pair of length 2^m is* $\dfrac{3}{(1 - (-1/2)^m)}$.

Therefore the asymptotic merit factor of both sequences of a Rudin-Shapiro pair is 3. To my knowledge, Theorem 4.2 is the first explicit construction of an infinite family of binary sequences, each with known merit factor, whose asymptotic merit factor is non-zero. It is not surprising that such constructions exist, because by Proposition 1.1 the expected asymptotic value of $1/F$ for a *randomly-chosen* binary sequence is 1. Nonetheless such a construction did not appear in the digital sequence design literature until Theorem 4.2 was rediscovered in generalised form as Theorem 4.3 in 1985. (In fact Littlewood [52, p. 334] performed the "straightforward calculations" leading to Theorem 4.2 as early as 1961, but the stated values in [52] are incorrect.)

Rudin-Shapiro sequence pairs are a special case of binary Golay complementary sequence pairs. (H. Shapiro suggests [70] that, in terms of historical precedence, a more suitable name than "Rudin-Shapiro" would be "Golay-Shapiro"; the confusion seems to have arisen from several mistaken citations of [71] as having been published in 1957, only two years prior to [66], rather than 1951.) Golay complementary pairs were introduced by Golay [28], [29] in 1949 in connection with a problem in infrared multislit spectroscopy and have seen repeated practical application since then, most recently in multicarrier wireless transmission (see [21] for details and recent results).

4.3 Generalisations of the Rudin-Shapiro Sequences

We now describe two generalisations of the Rudin-Shapiro sequences. Unfortunately neither improves on the asymptotic merit factor of 3 achieved in Theorem 4.2.

A first generalisation involves binary sequences $X^{(m)} = (x_0, x_1, \ldots, x_{2^m-1})$ of length 2^m that are defined recursively via:

$$x_{2^i+j} := (-1)^{j+f(i)} x_{2^i-j-1} \quad \text{for } 0 \le j < 2^i \text{ and } 0 \le i < m, \tag{22}$$

where $x_0 := 1$ and f is any function from $\mathbb{N}$ to $\{0, 1\}$. If we take

$$f(i) \quad = \quad \begin{cases} 0 & \text{if } i = 0 \text{ or } i \text{ is odd} \\ 1 & \text{if } i > 0 \text{ is even} \end{cases}$$

then the resulting sequence $X^{(m)}$ satisfies (20), and if we take the same function f but switch the value of $f(m-1)$ then the resulting sequence $Y^{(m)}$ satisfies (21); so the sequences of a Rudin-Shapiro pair are special cases of (22).

In 1985 Høholdt, Jensen and Justesen [40] established:

Theorem 4.3. *The merit factor of the sequence $X^{(m)}$ defined in* (22) *is* $\dfrac{3}{(1-(-1/2)^m)}$ *for any function f.*

Therefore the asymptotic merit factor of this family of sequences is 3.

Using polynomial notation, we can further generalise the Rudin-Shapiro sequences by regarding (22) as the special case $X^{(0)} = 1$ of the recursive construction

$$P_{X^{(m)}}(z) := P_{X^{(m-1)}}(z) \pm z^{2^{m-1}} P^*_{X^{(m-1)}}(-z), \tag{23}$$

where $P^*(z)$ is defined to be $z^{n-1}P(1/z)$ for a polynomial $P(z)$ of degree $n-1$. In 2000 Borwein and Mossinghoff [15] considered choices for the initial polynomial other than $X^{(0)} = 1$, having unrestricted degree, but concluded that the asymptotic merit factor achievable from (23) in this way is never more than 3.

The asymptotic merit factor results of Sections 4.2 and 4.3 are unusual in that they do not rely on special periodic autocorrelation properties. Instead, the merit factor is calculated directly from the defining recurrence relations.

4.4 Maximal Length Shift Register Sequences

A *maximal length shift register sequence* (often abbreviated to an ML-sequence or m-sequence) $X = (x_0, x_1, \ldots, x_{2^m-2})$ of length $2^m - 1$ is defined by:

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

where α is a primitive element of the field $\mathbb{F}_{2^m}$, β is a fixed element of the same field, and tr() is the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. The name given to these sequences arises from an alternative definition involving a linear recurrence relation of period $2^m - 1$ that can be

physically implemented using a shift register with m stages [36]. A maximal length shift register sequence is equivalent to a type of cyclic difference set with parameters from the class (17), known as a *Singer difference set*.

Sarwate [68] showed in 1984 that:

Theorem 4.4. *The mean value of* $1/F$*, taken over all* n *rotations of a maximal length shift register sequence of length* $n = 2^m - 1$*, is* $\dfrac{(n-1)(n+4)}{3n^2}$.

([40] points out that Theorem 4.4 could be derived from much earlier results due to Lindholm [50].) Theorem 4.4 implies that for any length $n = 2^m - 1$ there is some rotation of a maximal length shift register sequence of length n with merit factor of *at least* $3n^2/((n-1)(n+4))$, which asymptotically equals 3. This suggests the possibility of achieving an asymptotic merit factor greater than 3 by choosing a suitable rotation of a maximal length shift register sequence, but in 1989 Jensen and Høholdt [41] used the method introduced in [39] to show that this is not possible:

Theorem 4.5. *The asymptotic merit factor of any rotation of a maximal length shift register sequence is* 3.

4.5 Jacobi Sequences

A *Jacobi sequence* $X = (x_0, x_1, \ldots, x_{n-1})$ of length $n = p_1 p_2 \ldots p_r$, where $p_1 < p_2 < \ldots < p_r$ and each p_j is prime, is defined by:

$$x_i := \left(\frac{i}{p_1}\right)\left(\frac{i}{p_2}\right)\ldots\left(\frac{i}{p_r}\right) \quad \text{for } 0 \le i < n.$$

We can regard Jacobi sequences as the "product" of r Legendre sequences; for $r > 1$ such sequences do not correspond to difference sets.

In 2001 Borwein and Choi [11] proved:

Theorem 4.6. *Let* X *be a Jacobi sequence of length* $n = p_1 p_2 \ldots p_r$*, where* $p_1 < p_2 < \ldots p_r$ *and each* p_j *is prime. Then, provided that* $n^\epsilon/p_1 \longrightarrow 0$ *for any fixed* $\epsilon > 0$ *as* $n \longrightarrow \infty$*,* $1/\lim_{n\longrightarrow\infty} F(X_r)$ *is given by* (16).

Therefore, provided that (roughly speaking) p_1 does not grow significantly more slowly than n, the asymptotic merit factor of the optimal rotation of a Jacobi sequence is 6. The case $r = 2$ of Theorem 4.6, subject to a more restrictive condition on the growth of p_1, was given earlier by Jensen, Jensen and Høholdt [42].

4.6 Modified Jacobi Sequences

We next consider a modification of the Jacobi sequences of Section 4.5 for the case $r = 2$, as introduced by Jensen, Jensen and Høholdt [42]. A *modified Jacobi sequence* $X =$

$(x_0, x_1, \ldots, x_{n-1})$ of length $n = pq$, where p and q are distinct primes, is defined by:

$$x_i := \begin{cases} 1 & \text{for } i \equiv 0 \pmod{q} \\ -1 & \text{for } i > 0 \text{ and } i \equiv 0 \pmod{p} \\ \left(\frac{i}{p}\right)\left(\frac{i}{q}\right) & \text{for all other } i \text{ for which } 0 \leq i < n. \end{cases}$$

In the case $q = p + 2$, a modified Jacobi sequence is called a *Twin Prime sequence* and corresponds to a type of cyclic difference set with parameters from the class (17), known as a *Twin Prime difference set*.

In 1991 Jensen, Jensen and Høholdt [42] used the method introduced in [39] to prove:

Theorem 4.7. *Let X be a modified Jacobi sequence of length pq, where p and q are distinct primes. Then, provided that $((p+q)^5 \log^4(n))/n^3 \longrightarrow 0$ as $n \longrightarrow \infty$, $1/\lim_{n\longrightarrow\infty} F(X_r)$ is given by* (16).

Therefore, provided that p grows roughly as fast as q, the asymptotic merit factor of the optimal rotation of a modified Jacobi sequence (and in particular a Twin Prime sequence) is 6.

4.7 Golay's "Postulate of Mathematical Ergodicity"

The aperiodic autocorrelations $C(1), C(2), \ldots, C(n-1)$ of a sequence that is chosen at random from the 2^n binary sequences of length n are clearly dependent random variables. However in 1977 Golay [32] proposed, with an appeal to intuition and by analogy with statistical mechanics, a "Postulate of Mathematical Ergodicity" that states roughly:

> The correct value of $\limsup_{n\longrightarrow\infty} F_n$ can be found by treating $C(1), C(2), \ldots, C(n-1)$ as *independent* random variables for large n.

(The statement of the Postulate in [32] and its restatement in [33] are not entirely precise; indeed, Massey disclosed [57] that he was asked to mediate a dispute between Golay and the referees over the level of rigour of [33].)

Assuming the Postulate, Golay argued in [32] that $\lim_{n\longrightarrow\infty} F_n = 2e^2 \simeq 14.78$. In 1982 Golay [33] identified a "convenient, but faulty, approximation" in [32] and, by refining its heuristic arguments, concluded instead that the Postulate implies:

Conjecture 4.8 (Golay, 1982 [33])**.** $\lim_{n\longrightarrow\infty} F_n = 12.32\ldots$

Golay [33] also argued that:

(i) restriction to skew-symmetric sequences (see Section 3.1) does not change the asymptotic optimal merit factor

(ii) it is "most likely" that $F_n \leq 12.32\ldots$ for all $n \neq 13$.

Bernasconi [5] gave a more transparent derivation of the value 12.32... as an estimate for the asymptotic optimal merit factor, based on "an uncontrolled approximation for the partition function". Although the underlying assumption in [5] and [33] is clearly identified as unproven, its derived consequences are sometimes quoted as fact (for example, conclusion (ii) above and Conjecture 4.8 are treated in [4] and [16] respectively as proven results). Massey [57] wrote that he "would not want to bet on the contrary [to Conjecture 4.8]".

Golay [34] used the Postulate to predict correctly the asymptotic merit factor of a rotated Legendre sequence (see Section 4.1). Further evidence in support of the Postulate was given by Ferreira, Fontanari and Stadler [27], who found unexpectedly good agreement between experimentally determined parameters of the combinatorial search landscape (see Section 3.3) and those predicted by the Postulate. Nonetheless I am sceptical about its use: I do not find the arguments proposed in its favour in [33] to be convincing, and it seems not to be falsifiable except by direct disproof of Conjecture 4.8 or conclusion (i) above.

5 Periodic Appending

This section contains an overview of recent results of Borwein, Choi and Jedwab [13] that strongly suggest that $\limsup_{n\longrightarrow\infty} F_n > 6$. These results were motivated by the discoveries of A. Kirilusha and G. Narayanaswamy in 1999, working as summer students under the supervision of J. Davis at the University of Richmond.

We shall make use of the definition of rotation and appending of sequences as given in (15) and (19). Given a sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n and a real number t satisfying $0 \leq t \leq 1$, we write A^t for the sequence $(b_0, b_1, \ldots, b_{\lfloor tn \rfloor - 1})$ obtained by *truncating* A to a fraction t of its length:

$$b_i := \ a_i \quad \text{for } 0 \leq i < \lfloor tn \rfloor.$$

Let X be a Legendre sequence of prime length n. We know from Theorem 4.1 that $\lim_{n\longrightarrow\infty} F(X_{\frac{1}{4}}) = 6$. Kirilusha and Narayanaswamy [44] investigated how the merit factor of $X_{\frac{1}{4}}$ changes as sequence elements are successively appended. They observed:

Proposition 5.1. *Let $\{A_n\}$ and $\{B_n\}$ be sets of binary sequences, where each A_n has length n and each B_n has length $o(\sqrt{n})$. Then*

$$\frac{1}{F(A_n; B_n)} = \frac{1}{F(A_n)} + o(1).$$

It follows that up to $o(\sqrt{n})$ *arbitrary* sequence elements ± 1 can be appended to $X_{\frac{1}{4}}$ without changing the asymptotic merit factor of 6. Kirilusha and Narayanaswamy [44] then asked which choice of *specific* sequence elements yields the best merit factor when appended to $X_{\frac{1}{4}}$. To considerable surprise, they found that when the appended sequence elements are identical to some truncation of $X_{\frac{1}{4}}$, the merit factor appears to increase to a value consistently greater than 6.2!

This phenomenon was studied in detail in [13]. A key realisation was that the number of appended elements should take the form $\lfloor tn \rfloor$ for some fixed t, rather than the form $\lfloor n^\alpha \rfloor$ for fixed $\alpha < 1$ as suggested in [44]. Figure 2 shows the variation of $F(X_r; (X_r)^t)$ with r for the optimal value of t, for a large fixed length $n = 259499$. Extensive numerical evidence was presented in [13] to suggest that:

(i) for large n, the merit factor of the appended sequence $X_{\frac{1}{4}}; (X_{\frac{1}{4}})^t$ is greater than 6.2 when $t \simeq 0.03$

(ii) for large n, the merit factor of the appended sequence $X_r; (X_r)^t$ is greater than 6.34 for $r \simeq 0.22$ and $r \simeq 0.72$, when $t \simeq 0.06$.

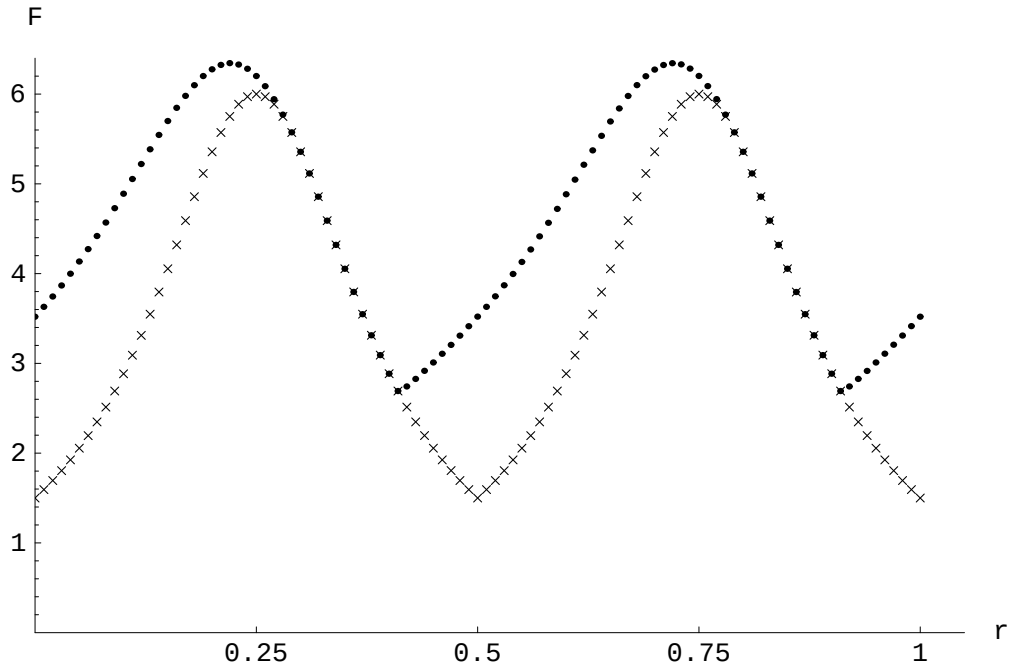

Figure 2: The merit factor of the r-rotated Legendre sequence of length 259499 before ($\times$) and after ($^\bullet$) appending of the optimal number of its own initial elements, for varying r.

I do not have a complete explanation for these apparent properties but they appear to rely on X_r having small periodic autocorrelation at all non-zero shifts, as given by (18). It seems that this causes the aperiodic autocorrelations of the appended sequence $X_r; (X_r)^t$ to be collectively small (for some values of $r \neq 0$ and for an appropriate value of t). In fact the process of successively appending initial elements of the sequence to itself would give a progressively larger merit factor if not for the single shift $u = n$. At this shift, the initial $\lfloor tn \rfloor$ elements of X_r are mapped onto copies of themselves and the resulting contribution of $(\lfloor tn \rfloor)^2$ to $\sum [C(u)]^2$ cannot be allowed to grow too large.

This intuition was formalised in [13], leading to an asymptotic relationship between the merit factor of the appended sequence $X_r;(X_r)^t$ and the merit factor of two truncated sequences $(X_r)^t$ and $(X_{r+t})^{1-t}$:

Theorem 5.2 ([13, Theorem 6.4 and equation (20)]). *Let X be a Legendre sequence of prime length n and let r, t satisfy $0 \le r \le 1$ and $0 < t \le 1$. Then, for large n,*

$$\frac{1}{F(X_r;(X_r)^t)} \sim \begin{cases} 2\left(\frac{t}{1+t}\right)^2\left(\frac{1}{F((X_r)^t)}+1\right)+\left(\frac{1-t}{1+t}\right)^2\left(\frac{1}{F((X_{r+t})^{1-t})}\right) & \text{for } t<1 \\ \frac{1}{2}\left(\frac{1}{F(X_r)}+1\right). & \text{for } t=1. \end{cases} \tag{24}$$

(The single shift $u = n$ is responsible for a contribution of $2\left(\frac{t}{1+t}\right)^2$ to the right-hand side of (24) for $t \le 1$; if this contribution were zero for $t = 1$ we would have $F(X_r;X_r) = 2F(X_r)$.) Given Theorem 5.2, it is sufficient to determine an asymptotic form for the function $t^2/F((X_r)^t)$ for any (r,t) satisfying $0 \le r \le 1$ and $0 < t \le 1$; this asymptotic form is already known for $t = 1$ from Theorem 4.1. Numerical evidence from sequences up to millions of elements in length leads to:

Conjecture 5.3 ([13, Conjecture 7.5]). *Let X be a Legendre sequence of prime length n. Then*

$$g(r,t) := \begin{cases} \lim\limits_{n\longrightarrow\infty}\left(\dfrac{t^2}{F((X_r)^t)}\right) & \text{for } 0<t\le 1 \\ 0 & \text{for } t=0 \end{cases} \tag{25}$$

is well-defined for any $r,t \in [0,1]$ and is given by

$$g(r,t) = t^2(1-\tfrac{4}{3}t) + h(r,t),$$

where

$$h(r+\tfrac{1}{2},t) := h(r,t) \quad \text{for } 0 \le r \le \tfrac{1}{2} \text{ and } 0 \le t \le 1$$

and $h(r,t)$ is defined for $0 \le r \le 1/2$ and $0 \le t \le 1$ in Figure 3.

By Proposition 7.6 of [13], the definition of $h(r,t)$ given in Figure 3 is needed for only one of the regions R_2 and R_3, because if the definition holds in either one then it holds in the other.

Support for Conjecture 5.3 is given by calculations [13] showing that for

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

the maximum discrepancy between the conjectured and actual value of $t^2/F((X_r)^t)$ is

$$\max_{(r,t)\in G}\left|\frac{t^2}{F((X_r)^t)} - g(r,t)\right| = \begin{cases} 0.00484 & \text{for } n = 22783 \\ 0.00122 & \text{for } n = 259499 \\ 0.00025 & \text{for } n = 4433701. \end{cases} \tag{26}$$

Subject to Conjecture 5.3, Theorem 5.2 implies that the maximum value of $\lim_{n\longrightarrow\infty} F(X_r;(X_r)^t)$ over $r,t \in [0,1]$ is approximately 6.3421, occurring at $r \simeq 0.2211$ and 0.7211 and $t \simeq 0.0578$,

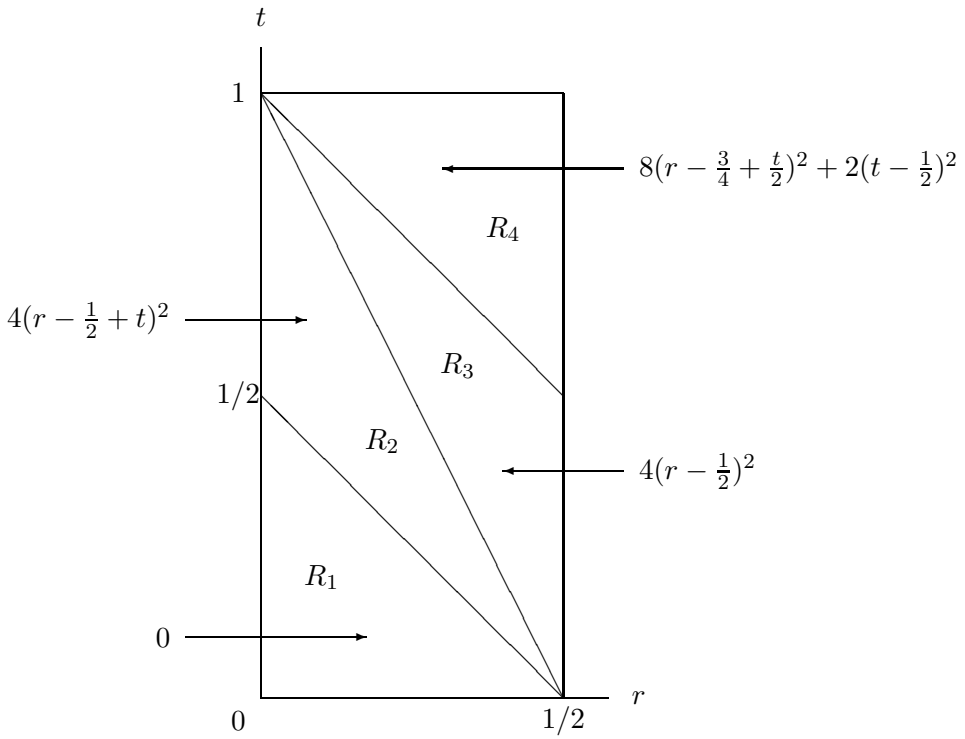

Figure 3: The function $h(r, t)$ for the range $0 \leq r \leq 1/2$ and $0 \leq t \leq 1$, in regions R_1, R_2, R_3 and R_4.

and the maximum value of $\lim_{n \longrightarrow \infty} F(X_{\frac{1}{4}}; (X_{\frac{1}{4}})^t)$ over $t \in [0, 1]$ is approximately 6.2018, occurring at $t \simeq 0.0338$ [13]. These values are in excellent agreement with calculated data.

Furthermore, experimental results [13] suggest that, provided p and q grow roughly as fast as each other, appending the initial elements of a modified Jacobi sequence of length $n = pq$ (see Section 4.6) to itself produces the same asymptotic behaviour as for Legendre sequences. Likewise, M. Parker [personal communication, June 2003] has found numerical evidence that the same is true for a family of sequences described in [63], provided that the sign of sequence elements is reversed under rotation and under appending.

Independently of [13], Kristiansen [46] presented sequences of length up to 20,000 having merit factor greater than 6.3, also inspired by Kirilusha and Narayanaswamy [44]. Each of the sequences in [46] is obtained by searching over a set of sequences derived from a Legendre sequence. [46] gives an approximate value for the total number of sequence elements resulting from the search but does not contain a theoretical explanation of the merit factor properties of the sequences. In response to a preprint of [13], Kristiansen and Parker [47] recognised that the sequences in [46] could more easily be viewed as an appending of a rotated Legendre sequence.

6 Challenges

I conclude with a personal selection of challenges concerning the Merit Factor Problem, arranged in order of increasing significance.

(6) Find a binary sequence X of length $n > 13$ for which $F(X) \geq 10$.

Such a sequence would give the largest known merit factor, with the exception of Barker sequences of length 11 and 13 (see Section 3).

(5) Find a binary sequence X for which $F(X) > 14.1$.

Regarding such a possibility, Massey [57] wrote in 1990: "Golay always regarded the length 13 Barker Sequences, whose merit factor is 14.08... as a singularity of nature whose goodness would never again be attained". Attractive though such a result would be, I have not placed it any higher on the list of challenges because I believe the study of the merit factor is fundamentally concerned with asymptotic behaviour, not the identification of a particular sequence with an unusually large value of F.

(4) Prove that Conjecture 1.2 is false.

This might be achieved, for example, by determining the asymptotic value of $t^2/F((X_r)^t)$ for a Legendre sequence X for appropriate r and t (see Conjecture 5.3). A disproof of Conjecture 1.2 would give a proven new lower bound on $\limsup_{n\longrightarrow\infty} F_n$ for the first time since 1988.

(3) Find a binary sequence family X for which $\lim_{n\longrightarrow\infty} F(X) > 6.3421\ldots$

The apparent lower bound of 6.3421... implied by Conjecture 5.3 arises by reference to periodic properties of Legendre sequences. I believe that better bounds might be found from a direct analysis of aperiodic behaviour (see Section 4.1).

(2) Find a binary sequence family X for which $\lim_{n\longrightarrow\infty} F(X)$ is an integer greater than 6.

Although I do not have a satisfying explanation, I find it remarkable that the Legendre, Rudin-Shapiro, generalised Rudin-Shapiro (22), maximal length shift register, Jacobi, and modified Jacobi sequences all have an asymptotic merit factor that takes an integer value (see Section 4). One might expect that some other infinite families of sequences behave similarly.

(1) Determine whether $\limsup_{n\longrightarrow\infty} F_n$ is finite and, if so, determine its value.

This is a restatement of the Merit Factor Problem. If $\limsup_{n\longrightarrow\infty} F_n$ is infinite then Conjecture 1.3 from 1966 is true, whereas if it is finite then Conjecture 2.4 from 1957 is true and furthermore there are only finitely many Barker sequences (see Section 2.2). If $\limsup_{n\longrightarrow\infty} F_n$ takes any value other than 12.32... then Golay's "Postulate of Mathematical Ergodicity" is false (see Section 4.7).

Acknowledgements

I am grateful to R. Turyn for generously sharing insights into the historical background of the Merit Factor Problem, and to L. Goddyn for suggesting the use of Figure 3 to represent the function $h(r,t)$.

References

[1] M. Antweiler and L. Bömer. Merit factor of Chu and Frank sequences. *Electron. Lett.*, **26**:2068–2070, 1990.

[2] R.H. Barker. Group synchronizing of binary digital systems. In W. Jackson, editor, *Communication Theory*, pages 273–287. Academic Press, New York, 1953.

[3] L.D. Baumert. *Cyclic Difference Sets*. Lecture Notes in Mathematics 182. Springer-Verlag, New York, 1971.

[4] 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.

[5] J. Bernasconi. Low autocorrelation binary sequences: statistical mechanics and configuration state analysis. *J. Physique*, **48**:559–567, 1987.

[6] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory*. Cambridge University Press, Cambridge, 2nd edition, 1999. Volumes I and II.

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

[8] L. Bömer and M. Antweiler. Optimizing the aperiodic merit factor of binary arrays. *Signal Processing*, **30**:1–13, 1993.

[9] J. Borwein and D. Bailey. *Mathematics by Experiment: Plausible Reasoning in the 21st Century*. A.K. Peters, Natick, 2004.

[10] P. Borwein. *Computational Excursions in Analysis and Number Theory*. CMS Books in Mathematics. Springer-Verlag, New York, 2002.

[11] P. Borwein and K.-K.S. Choi. Merit factors of polynomials formed by Jacobi symbols. *Canad. J. Math.*, **53**:33–50, 2001.

[12] P. Borwein and K.-K.S. Choi. Explicit merit factor formulae for Fekete and Turyn polynomials. *Trans. Amer. Math. Soc.*, **354**:219–234, 2002.

[13] 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.

[14] P. Borwein, R. Ferguson, and J. Knauer. The merit factor of binary sequences. In preparation.

[15] P. Borwein and M. Mossinghoff. Rudin-Shapiro-like polynomials in L_4. *Math. of Computation*, **69**:1157–1166, 2000.

[16] F. Brglez, X.Y. Li, M.F. Stallman, and B. Militzer. Evolutionary and alternative algorithms: reliable cost predictions for finding optimal solutions to the LABS problem. *Information Sciences*, 2004. To appear.

[17] K.-K.S. Choi. Extremal problems about norms of Littlewood polynomials. 2004. Preprint.

[18] 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.

[19] 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.

[20] J.A. Davis and J. Jedwab. A survey of Hadamard difference sets. In K.T. Arasu et al., editors, *Groups, Difference Sets and the Monster*, pages 145–156. de Gruyter, Berlin-New York, 1996.

[21] J.A. Davis and J. Jedwab. Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes. *IEEE Trans. Inform. Theory*, **45**:2397–2417, 1999.

[22] C. de Groot, D. Würtz, and K.H. Hoffmann. Low autocorrelation binary sequences: exact enumeration and optimization by evolutionary strategies. *Optimization*, **23**:369–384, 1992.

[23] V.M. de Oliveira, J.F. Fontanari, and P.F. Stadler. Metastable states in high order short-range spin glasses. *J. Phys. A: Math. Gen.*, **32**:8793–8802, 1999.

[24] P. Erdös. Some unsolved problems. *Mich. Math. J.*, **4**:291–300, 1957.

[25] P. Erdös. An inequality for the maximum of trigonometric polynomials. *Ann. Polon. Math.*, **12**:151–154, 1962.

[26] P. Fan and M. Darnell. *Sequence Design for Communications Applications*. Communications Systems, Techniques and Applications. Research Studies Press, Taunton, 1996.

[27] F.F. Ferreira, J.F. Fontanari, and P.F. Stadler. Landscape statistics of the low autocorrelated binary string problem. *J. Phys. A: Math. Gen.*, **33**:8635–8647, 2000.

[28] M.J.E. Golay. Multislit spectroscopy. *J. Opt. Soc. Amer.*, **39**:437–444, 1949.

[29] M.J.E. Golay. Static multislit spectrometry and its application to the panoramic display of infrared spectra. *J. Opt. Soc. Amer.*, **41**:468–472, 1951.

[30] 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.

[31] M.J.E. Golay. Hybrid low autocorrelation sequences. *IEEE Trans. Inform. Theory*, **IT-21**:460–462, 1975.

[32] M.J.E. Golay. Sieves for low autocorrelation binary sequences. *IEEE Trans. Inform. Theory*, **IT-23**:43–51, 1977.

[33] M.J.E. Golay. The merit factor of long low autocorrelation binary sequences. *IEEE Trans. Inform. Theory*, **IT-28**:543–549, 1982.

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

[35] M.J.E. Golay and D.B. Harris. A new search for skewsymmetric binary sequences with optimal merit factors. *IEEE Trans. Inform. Theory*, **36**:1163–1166, 1990.

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

[37] T. Helleseth, P.V. Kumar, and H. Martinsen. A new family of ternary sequences with ideal two-level autocorrelation function. *Designs, Codes and Cryptography*, **23**:157–166, 2001.

[38] T. Høholdt. The merit factor of binary sequences. In A. Pott et al., editors, *Difference Sets, Sequences and Their Correlation Properties*, volume 542 of *NATO Science Series C*, pages 227–237. Kluwer Academic Publishers, Dordrecht, 1999.

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

[40] 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.

[41] 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.

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

[43] J.-P. Kahane. Sur les polynômes á coefficients unimodulaires. *Bull. London Math. Soc.*, **12**:321–342, 1980.

[44] A. Kirilusha and G. Narayanaswamy. Construction of new asymptotic classes of binary sequences based on existing asymptotic classes. Summer Science Program Technical Report, Dept. Math. Comput. Science, University of Richmond, July 1999.

[45] J. Knauer. Merit Factor Records. Online. Available: <http://www.cecm.sfu.ca/~jknauer/labs/records.html>, November 2004.

[46] R.A. Kristiansen. On the Aperiodic Autocorrelation of Binary Sequences. Master's thesis, University of Bergen, March 2003.

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

[48] K.H. Leung, S.L. Ma, and B. Schmidt. Nonexistence of abelian difference sets: Lander's conjecture for prime power orders. *Trans. Amer. Math. Soc.*, **356**:4343–4358, 2004.

[49] K.H. Leung and B. Schmidt. The field descent method. *Designs, Codes and Cryptography*. To appear.

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

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

[52] J.E. Littlewood. On the mean values of certain trigonometrical polynomials. *J. London Math. Soc.*, **36**:307–334, 1961.

[53] J.E. Littlewood. On polynomials $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta i}$. *J. London Math. Soc.*, **41**:367–376, 1966.

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

[55] L. Lunelli. Tabelli di sequenze $(+1, -1)$ con autocorrelazione troncata non maggiore di 2. Politecnico di Milano, 1965.

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

[57] J.L. Massey. Marcel J.E. Golay (1902-1989). Obituary, in: *IEEE Information Theory Society Newsletter*, June 1990.

[58] S. Mertens. Exhaustive search for low-autocorrelation binary sequences. *J. Phys. A: Math. Gen.*, **29**:L473–L481, 1996.

[59] S. Mertens and H. Bauke. Ground States of the Bernasconi Model with Open Boundary Conditions. Online. Available: `<http://odysseus.nat.uni-magdeburg.de/~mertens/bernasconi/open.dat>`, November 2004.

[60] B. Militzer, M. Zamparelli, and D. Beule. Evolutionary search for low autocorrelated binary sequences. *IEEE Trans. Evol. Comput.*, **2**:34–39, 1998.

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

[62] D.J. Newman and J.S. Byrnes. The L^4 norm of a polynomial with coefficients ± 1. *Amer. Math. Monthly*, **97**:42–45, 1990.

[63] M.G. Parker. Even length binary sequence families with low negaperiodic autocorrelation. In S. Boztas and I. E. Shparlinski, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-14 Proceedings*, volume 2227 of *Lecture Notes in Computer Science*, pages 200–210. Springer-Verlag, 2001.

[64] K.G. Paterson. Applications of exponential sums in communications theory. In M. Walker, editor, *Cryptography and Coding*, volume 1746 of *Lecture Notes in Computer Science*, pages 1–24. Springer-Verlag, Berlin, 1999.

[65] C.M. Reidys and P.F. Stadler. Combinatorial landscapes. *SIAM Review*, **44**:3–54, 2002.

[66] W. Rudin. Some theorems on Fourier coefficients. *Proc. Amer. Math. Soc.*, **10**:855–859, 1959.

[67] H.J. Ryser. *Combinatorial Mathematics*. Carus Mathematical Monographs No. 14. Mathematical Association of America, Washington, DC, 1963.

[68] D.V. Sarwate. Mean-square correlation of shift-register sequences. *IEE Proceedings Part F*, **131**:101–106, 1984.

[69] M.R. Schroeder. Synthesis of low peak-factor signals and binary sequences with low autocorrelation. *IEEE Trans. Inform. Theory*, **IT-16**:85–89, 1970.

[70] H. Shapiro. Harold Shapiro's Research Interests. Online. Available: `<http://www.math.kth.se/~shapiro/profile.html>`, November 2004.

[71] H.S. Shapiro. Extremal Problems for Polynomials and Power Series. Master's thesis, Mass. Inst. of Technology, 1951.

[72] R. Turyn and J. Storer. On binary sequences. *Proc. Amer. Math. Soc.*, **12**:394–399, 1961.

[73] R.J. Turyn. Character sums and difference sets. *Pacific J. Math.*, **15**:319–346, 1965.

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

[75] Q. Xiang. Recent results on difference sets with classical parameters. In A. Pott et al., editors, *Difference Sets, Sequences and Their Correlation Properties*, volume 542 of *NATO Science Series C*, pages 419–437. Kluwer Academic Publishers, Dordrecht, 1999.