What can be used instead of a Barker sequence?

Jonathan Jedwab

Abstract. A classical problem of digital sequence design, first studied in the 1950s but still not well understood, is to determine long binary sequences for which the absolute values of the aperiodic autocorrelations are collectively as small as possible. The ideal sequence from this point of view is a Barker sequence, but there is overwhelming evidence that no Barker sequence of length greater than 13 exists.

Since a Barker sequence of length greater than 13 must have constant periodic autocorrelations at all non-zero shifts, it is equivalent to a difference set in a cyclic group. The rich structure of the group setting allows the application of techniques and tools from finite field theory, algebraic number theory, character theory, and elsewhere. This has stimulated much research on difference sets, whose study has matured into a fertile body of theory.

However the motivating practical problem remains firmly in the aperiodic domain, and has attracted renewed interest in recent years. We survey various responses to the presumed nonexistence of long Barker sequences, namely: multi-dimensional Barker arrays; the peak sidelobe level of binary sequences; the merit factor of binary sequences; Barker sequences over a non-binary alphabet; and pairs of Golay complementary sequences and arrays.

1. The Barker Sequence Conjecture

We consider a *length s binary sequence* to be a one-dimensional matrix $\mathcal{A} = (A[i])$ whose elements satisfy

$$A[i] = \begin{cases} -1 \text{ or } 1 & \text{for } 0 \le i < s \\ 0 & \text{otherwise.} \end{cases}$$

The *aperiodic autocorrelation function* of a length s binary sequence $\mathcal{A} = (A[i])$ is given by

$$C_{\mathcal{A}}(u) := \sum_i A[i]A[i+u] \quad \text{for integer } u, \tag{1.1}$$

and measures the extent to which a binary sequence resembles a shifted copy of itself.

2000 *Mathematics Subject Classification.* Primary 94A55, 68P30; Secondary 05B10, 05B20.

Key words and phrases. aperiodic, array, autocorrelation, Barker, binary, difference set, Golay, quaternary, merit factor, peak sidelobe level, sequence.

Date. November 13, 2007 (revised February 10, 2008).

The author is supported by NSERC of Canada.

Barker [**Bar53**] proposed a group synchronisation digital system in 1953, based on the use of binary sequences $\mathcal{A}$ of length s for which $C_{\mathcal{A}}(u)$ is small (not necessarily in magnitude) for each $u \neq 0$. The purpose of this constraint was to ensure a large difference between the system output $C_{\mathcal{A}}(0)$ at the moment of synchronisation and the maximum possible system output $C_{\mathcal{A}}(u) + |u|$ when synchronisation is delayed by u time units, for $|u| < s$ [**Bar53**, Figure 6a]. Consideration of the probability of false synchronisation at each value of u led Barker to seek solutions for large s to the problem:

$$\text{minimise } \max_{0<u<s} C_{\mathcal{A}}(u) \text{ over all length } s \text{ binary sequences } \mathcal{A}. \tag{1.2}$$

Now by summing (1.1) over all integers u, we find that $2\sum_{0<u<s} C_{\mathcal{A}}(u) = (\sum_i A[i])^2 - s \geq -s + (s \bmod 2)$. But since $C_{\mathcal{A}}(u)$ is the sum of exactly $s - |u|$ terms, each of which is ± 1, we also have $C_{\mathcal{A}}(u) \equiv s-u \pmod 2$. It follows that $\max_{0<u<s} C_{\mathcal{A}}(u) \geq 0$ for $s > 2$ (since otherwise $C_{\mathcal{A}}(u) \leq -1$ when $s-u$ is odd and $C_{\mathcal{A}}(u) \leq -2$ when $s-u$ is even), and that equality is achieved if and only if

$$C_{\mathcal{A}}(u) = 0 \text{ or } -1 \quad \text{for all } u \neq 0 \tag{1.3}$$

(where $C_{\mathcal{A}}(u) = -1$ for u in the range $0 < u < s$ exactly when $s-u$ is odd). Barker therefore proposed that, for this synchronisation application, an ideal binary sequence $\mathcal{A}$ is one satisfying (1.3) for large s. He gave examples of such sequences for lengths $s = 3$, 7 and 11, but speculated (correctly, by Theorem 1.2 and (1.5)) that examples for larger values of s do not exist.

Subsequent authors recognised that several additional application contexts, including pulse compression and especially radar, would benefit from the use of long binary sequences for which $|C_{\mathcal{A}}(u)|$, rather than $C_{\mathcal{A}}(u)$, is small for each $u \neq 0$ [**Wel60**], [**Boe67**], [**Tur68**]. This motivates the fundamental sequence design problem:

Problem 1.1. *Find binary sequences $\mathcal{A}$ of large length s for which the elements of the set $\{|C_{\mathcal{A}}(1)|, |C_{\mathcal{A}}(2)|, \ldots, |C_{\mathcal{A}}(s-1)|\}$ are collectively as small as possible.*

The importance of Problem 1.1 is that it deals with the aperiodic domain, which is the natural physical setting in which many autocorrelation processes arise. An ideal solution of Problem 1.1 is a long binary sequence for which

for each $u \neq 0$ independently, $|C_{\mathcal{A}}(u)|$ takes its smallest possible value.

Barker's condition was therefore relaxed from (1.3) to

$$|C_{\mathcal{A}}(u)| = 0 \text{ or } 1 \quad \text{for all } u \neq 0 \tag{1.4}$$

(where $|C_{\mathcal{A}}(u)| = 1$ for u in the range $0 < u < s$ exactly when $s-u$ is odd), and a binary sequence satisfying (1.4) became known as a *Barker sequence.*

Using the symbols + and − to represent the sequence elements 1 and −1 respectively, the following are examples of Barker sequences of length $s > 1$:

$$\begin{aligned}
s = 2 :&\quad [+\ +]\\
s = 3 :&\quad [+\ +\ -]\\
s = 4 :&\quad [+\ +\ +\ -]\\
s = 5 :&\quad [+\ +\ +\ -\ +]\\
s = 7 :&\quad [+\ +\ +\ -\ -\ +\ -]\\
s = 11 :&\quad [+\ +\ +\ -\ -\ -\ +\ -\ -\ +\ -]\\
s = 13 :&\quad [+\ +\ +\ +\ +\ -\ -\ +\ +\ -\ +\ -\ +].
\end{aligned}$$

No Barker sequence of length greater than 13 is known, and Turyn and Storer established in 1961 by elementary methods that such a sequence cannot occur for odd length:

Theorem 1.2 ([**TS61**]). *There is no Barker sequence of odd length $s > 13$.*

Theorem 1.2 was proved by showing that any odd-length Barker sequence has some repeating structure, and therefore that it must be short. The material in [**TS61**] was contained in the earlier report [**Tur60**], produced by Turyn in 1960 under contract to the U.S. Air Force. This report also includes nonexistence results for Barker sequences for some even lengths, leading the author to remark [**Tur60**, p. II-2] that "The existence of a [Barker sequence with length greater than 13] is thus not completely resolved, though, of course, in view of the results stated above, it seems extremely improbable." We formalise this statement as:

Conjecture 1.3 (Barker Sequence Conjecture). *There is no Barker sequence of length $s > 13$.*

(It is not entirely clear to whom the Barker Sequence Conjecture should be attributed. To my knowledge, it was first suggested in print in the statement from [**Tur60**] quoted above, although R. Turyn reports [personal communication, October 2007] that he intended this remark not as a conjecture in the mathematical sense, but as the likely conclusion of known facts, in particular his joint work with J. Storer.)

The Barker Sequence Conjecture remains unproven, although a great deal of evidence has been accumulated in its favour, as we now review. The Conjecture holds for odd s, by Theorem 1.2, so suppose that $\mathcal{A} = (A[i])$ is a Barker sequence of even length $s > 13$. Turyn and Storer [**TS61**] pointed out that this implies the *periodic autocorrelation function* $C_{\mathcal{A}}(u) + C_{\mathcal{A}}(u - s)$ of $\mathcal{A}$ satisfies

$$C_{\mathcal{A}}(u) + C_{\mathcal{A}}(u - s) = 0 \quad \text{for each } u \text{ satisfying } 0 < u < s, \tag{1.5}$$

in other words that $\mathcal{A}$ is a *perfect binary sequence*. In 1965, Turyn proved:

Theorem 1.4 ([**Tur65**]). *If there exists a perfect binary sequence of length $s > 4$ then $s = 4S^2$ for some odd integer $S \geq 55$ that is not a prime power.*

Turyn's method was to show that (1.5) is equivalent to the set $D := \{i \in \mathbb{Z}_s \mid A[i] = -1\}$ forming a $(4S^2, 2S^2 - S, S^2 - S)$-difference set in the cyclic group $\mathbb{Z}_s$, where $s = 4S^2$ for some integer S (see for example [**BJL99**] for background on difference sets); and that the existence of this difference set is in turn equivalent to the *character sum* $\chi(D) := \sum_{i \in D} \eta^i$, where η is any s-th root of unity, satisfying

$$|\chi(D)| = S. \tag{1.6}$$

Application of algebraic number theory to (1.6), taking advantage of the fact that S must be integer, then gives the constraints on S of Theorem 1.4. In particular there is no perfect binary, and therefore no Barker, sequence of length s for $13 < s < 4 \cdot 55^2 = 12,100$. This result saw no improvement for the next 25 years.

In 1990, Eliahou, Kervaire and Saffari found a new constraint on the possible lengths of a Barker sequence, as a corollary to Theorem 8.4:

Theorem 1.5 ([**EKS90**]). *If there exists a Barker sequence of even length s then s has no prime factor congruent to* 3 *modulo* 4*.*

By combining Theorem 1.5 with the algebraic number theoretic constraints of Turyn's method, it follows [**JL92**], [**EK92**] that there is no Barker sequence of length $4S^2$ for $1 < S < 689$. We cannot reach the same conclusion for a perfect binary sequence (defined via the periodic autocorrelation function) because the proof of Theorem 1.5, in contrast to that of Theorem 1.4, relies crucially on aperiodic properties.

The next improvement was due to Schmidt [**Sch99**], who in 1999 introduced the method of field descent to restrict the possible solutions of equations of the form

$$X\overline{X} = n \quad \text{and} \quad X \in \mathbb{Z}[\exp(2\pi\sqrt{-1}/m)],$$

where bar represents complex conjugation and n, m are positive integers; (1.6) has this form for $4n = m = s$. This allowed an increase in the size of the smallest open case for a perfect binary sequence from $S = 55$ to $S = 165$, and an increase in the corresponding size for a Barker sequence (after combining with constraints from Theorem 1.5) from $S = 689$ to $S = 10^6$. Refinements to the field descent method [**Sch02**], [**LS05**] gave a further increase in the size of the smallest open case for a perfect binary sequence to $S = 11715$, and (after combination with Theorem 1.5) a dramatic increase in the corresponding size for a Barker sequence to $S = 5 \cdot 10^{10}$:

Theorem 1.6 ([**LS05**]). *There is no Barker sequence of length s for $13 < s < 10^{22}$.*

2. Responses to the presumed nonexistence of long Barker sequences

To a mathematician, the verification of the Barker Sequence Conjecture up to length 10^{22} in Theorem 1.6, while suggestive, is far from conclusive. Indeed, a proof of the Conjecture remains both elusive and highly desirable. But to a digital systems engineer, the matter was effectively settled decades ago: even if a Barker sequence of enormous length were to exist, it is most unlikely that it could ever be implemented in a practical system. This naturally prompts the question:

What can be used instead of a Barker sequence to solve Problem 1.1?

I argue that a historical reading of the literature would class many combinatorial objects, that have been studied for their favourable aperiodic autocorrelation properties, as responses to this question.

A first group of responses addresses Problem 1.1 directly, by specifying an interpretation for "collectively as small as possible" that relaxes the Barker sequence condition (1.4) for an ideal binary sequence. The two most well-studied interpretations involve minimising the maximum, or the sum of squares, of the values $|C_{\mathcal{A}}(u)|$:

- **Minimise** $\max_{0<u<s}|C_{\mathcal{A}}(u)|$ **over all length s binary sequences $\mathcal{A}$.**
  This is the obvious modification of Barker's original design problem (1.2). The quantity $\max_{0<u<s}|C_{\mathcal{A}}(u)|$ is called the *peak sidelobe level* of the sequence $\mathcal{A}$ (see Section 5).
- **Minimise** $\sum_{0<u<s}[C_{\mathcal{A}}(u)]^2$ **over all length s binary sequences $\mathcal{A}$.**
  This places more emphasis on the collective smallness of the values $|C_{\mathcal{A}}(u)|$. The quantity $s^2/(2\sum_{0<u<s}[C_{\mathcal{A}}(u)]^2)$ is called the *merit factor* of the sequence $\mathcal{A}$ (see Section 6).

A second group of responses modifies Problem 1.1 to allow more general objects than binary sequences, and then seeks an ideal solution. Responses in this group include:

- **Two or more dimensions.**
  The sequence $\mathcal{A}$ is replaced by a multi-dimensional array, and the definition of aperiodic autocorrelation is suitably modified (see Sections 3 and 4).
- **A sequence pair.**
  The sequence $\mathcal{A}$ is replaced by a sequence pair $\mathcal{A}$ and $\mathcal{B}$ with the property that $C_{\mathcal{A}}(u) + C_{\mathcal{B}}(u) = 0$ for all $u \neq 0$, known as a *Golay complementary sequence pair* (see Section 8).
- **Non-binary alphabet.**
  The alphabet $\{1, -1\}$ of the sequence elements is replaced by a larger alphabet, often a set of complex roots of unity, and the definition of aperiodic autocorrelation is suitably modified. The ideal condition on the modified problem can then be relaxed in order to generate further examples (see Sections 3 and 7).

These responses can be combined in various ways, for example by studying Golay complementary array pairs over a non-binary alphabet. Sections 4 to 8 of this survey examine responses of each of the above five types, together with some combinations. Section 3 introduces some definitions and notation, and Section 9 is the conclusion.

3. Definitions and notation

We define an $s_1 \times \ldots \times s_r$ *array* to be an r-dimensional matrix $\mathcal{A} = (A[i_1, \ldots, i_r])$ of complex-valued entries, where $i_1, \ldots, i_r$ are integer, for which

$$A[i_1, \ldots, i_r] = 0 \;\text{ if, for any } k \in \{1, \ldots, r\},\ i_k < 0 \text{ or } i_k \geq s_k.$$

In the case $r = 1$, $\mathcal{A} = (A[i_1])$ reduces to a length s_1 sequence. The array is defined over an *alphabet* $W \subseteq \mathbb{C}$ if each array element $A[i_1, \ldots, i_r]$, where $0 \leq i_k < s_k$ for each k, takes values in W. The alphabet is *unimodular* if $|w| = 1$ for all $w \in W$. Write $\xi := \exp(2\pi\sqrt{-1}/H)$ for some integer H. A unimodular alphabet is *H-phase* if $W = \{1, \xi, \xi^2, \ldots, \xi^{H-1}\}$. A 2-phase array has $W = \{1, -1\}$ and is called *binary*; a 4-phase array has $W = \{1, \sqrt{-1}, -1, -\sqrt{-1}\})$ and is called *quaternary*. The usage of *ternary* is ambiguous: in some contexts it is used to mean the 3-phase alphabet $W = \{1, (-1 + \sqrt{-3})/2, (-1 - \sqrt{-3})/2\}$, but in others it is reserved for the non-unimodular alphabet $W = \{1, 0, -1\}$.

The *aperiodic autocorrelation function* of an $s_1 \times \cdots \times s_r$ array $\mathcal{A} = (A[i_1, \ldots, i_r])$ is given by

$$C_{\mathcal{A}}(u_1, \ldots, u_r) := \sum_{i_1} \cdots \sum_{i_r} A[i_1, \ldots, i_r] \overline{A[i_1 + u_1, \ldots, i_r + u_r]} \quad \text{for integer } u_1, \ldots, u_r,$$

where bar represents complex conjugation. This definition reduces to (1.1) when $\mathcal{A}$ is a binary sequence.

We will examine three infinite families of binary sequences with specific structure. A *maximal length shift register sequence* (often abbreviated to m-sequence, and also known as an *ML-sequence* or *pseudonoise sequence*) is a binary sequence $(Y[i])$ of length $2^m - 1$ defined by

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

where α is a primitive element of the field $\mathrm{GF}(2^m)$, β is a fixed non-zero element of the same field, and tr() is the trace function from $\mathrm{GF}(2^m)$ to $GF(2)$. For each primitive element α we can choose $2^m - 1$ different values of β, each of which corresponds to a cyclic shift of the m-sequence for which $\beta = 1$; in particular, any cyclic shift of an m-sequence is also an m-sequence. (The k-th *cyclic shift* of a length s sequence $(A[i])$ is the length s sequence whose i-th entry is $A[(i+k) \bmod s]$ for $0 \le i < s$.) The name "maximal-length shift register sequence" 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 (see for example [**GG05**] for background on m-sequences).

A *Legendre sequence* is a binary sequence $(X[i])$ of prime length s defined by

$$X[i] := \left(\frac{i}{s} \right) \quad \text{for } 0 \le i < s,$$

where $\left(\frac{i}{s}\right)$ is the Legendre symbol (which takes the value 1 if i is a quadratic residue modulo s and the value -1 if not; we choose the convention that $\left(\frac{i}{s}\right) := 1$ if $i = 0$).

Given sequences $\mathcal{A} = (A[i])$ of length s and $\mathcal{B} = (B[i])$ of length s' we write $\mathcal{A}; \mathcal{B}$ for the sequence $(C[i])$ of length $s + s'$ given by *concatenating* $\mathcal{A}$ and $\mathcal{B}$:

$$C[i] := \begin{cases} A[i] & \text{for } 0 \le i < s \\ B[i - s] & \text{for } s \le i < s + s'. \end{cases}$$

The *Rudin-Shapiro sequence pair* $A^{(m)}$, $B^{(m)}$ of length 2^m is defined recursively [**Sha51**], [**Rud59**] by:

$$\begin{cases} A^{(m)} := & A^{(m-1)}; B^{(m-1)}, \\ B^{(m)} := & A^{(m-1)}; -B^{(m-1)}. \end{cases} \tag{3.1}$$

where $A^{(0)} = B^{(0)} := [+]$. Rudin-Shapiro sequence pairs are a special case of binary Golay complementary sequence pairs (see Section 8). A *Rudin-Shapiro sequence* is a sequence that is a member of some Rudin-Shapiro sequence pair.

We 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 $f(n) \le c g(n)$ 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 $\Omega(g)$.

4. Multi-dimensional Barker arrays

In this section we examine the generalisation of the Barker sequence condition to two or more dimensions. An $s_1 \times \cdots \times s_r$ *Barker array* is defined to be an $s_1 \times \cdots \times s_r$ binary array for which

$$|C_{\mathcal{A}}(u_1, \ldots, u_r)| = 0 \text{ or } 1 \quad \text{for all } (u_1, \ldots, u_r) \neq (0, \ldots, 0).$$

In the case $r = 1$, this condition reduces to the Barker sequence condition (1.4). Alquaddoomi and Scholtz introduced two-dimensional Barker arrays in 1989, describing how large examples could be used as an alternative to long Barker sequences for high resolution radar applications [**AS89**]. However, apart from the size 2×2 (for example the array $\begin{bmatrix} + & + \\ + & - \end{bmatrix}$), they could find no examples of $s_1 \times s_2$ Barker arrays having $s_1, s_2 > 1$. Their conjecture that no such arrays exist was proved in 2007 by Davis, Jedwab and Smith:

Theorem 4.1 ([**DJS07**]). *There are no $s_1 \times s_2$ Barker arrays having $s_1, s_2 > 1$ except when $s_1 = s_2 = 2$.*

We now outline the proof of Theorem 4.1 which, like that of Theorem 1.5, depends crucially on aperiodic properties. By adapting the method of proof of (1.5), we find that the two-dimensional periodic autocorrelation function

$$C_{\mathcal{A}}(u_1, u_2) + C_{\mathcal{A}}(u_1, u_2 - s_2) + C_{\mathcal{A}}(u_1 - s_1, u_2) + C_{\mathcal{A}}(u_1 - s_1, u_2 - s_2) \tag{4.1}$$

takes the constant value -1, 0 or 1 for all $(u_1, u_2) \neq (0, 0)$ satisfying $0 \leq u_1 < s_1$, $0 \leq u_2 < s_2$ (where the constant is determined by the value of $s_1 s_2$ modulo 4). However Alquaddoomi and Scholtz [**AS89**] recognised that a stronger condition holds, namely that the "hybrid" autocorrelation function

$$C_{\mathcal{A}}(u_1, u_2) + C_{\mathcal{A}}(u_1, u_2 - s_2) \tag{4.2}$$

(aperiodic in the first index but periodic in the second) also takes the constant value -1, 0 or 1 for all $(u_1, u_2) \neq (0, 0)$ satisfying $-s_1 < u_1 < s_1$, $0 \leq u_2 < s_2$. This is sufficient to determine the aperiodic autocorrelation function of the length s_1 sequence $\mathcal{R} = (R[i_1])$ defined by $R[i_1] := \sum_{i_2} A[i_1, i_2]\xi^{i_2}$, where ξ is a primitive s_2-th root of unity, from which Theorem 4.1 can then be derived. Knowledge of the aperiodic, rather than the periodic, autocorrelation function of the sequence $\mathcal{R}$ is a consequence of working with the hybrid autocorrelation function (4.2) rather than the full periodic autocorrelation function (4.1). We can visualise this distinction as corresponding to whether the array $\mathcal{A}$ is written on the surface of a cylinder or on the surface of a torus.

In 1992, Dymond [**Dym92**] investigated the existence of r-dimensional Barker arrays for $r > 2$, and conjectured that no such arrays (whose representation requires all r dimensions) exist. Her conjecture was proved in 2007 by Jedwab and Parker:

Theorem 4.2 ([**JP07b**]). *There are no $s_1 \times \cdots \times s_r$ Barker arrays having $r > 2$ and each $s_k > 1$.*

A key auxiliary result in the proof of Theorem 4.2 is given by applying a "projection mapping" (see Section 8) to a Barker array in order to obtain a Barker array with one dimension fewer:

Theorem 4.3 ([**JP07b**]). *If there exists an $s \times t \times s_1 \times \ldots \times s_r$ Barker array, where $r \geq 0$, then there exists an $st \times s_1 \times \ldots \times s_r$ Barker array.*

Theorem 4.2 is a straightforward corollary of Theorem 4.3: we apply Theorem 4.3 repeatedly to reduce the number of dimensions to 2, and then use Theorem 4.1. (Theorem 4.3 can also be applied in the case $r = 0$ to show that the existence of a two-dimensional Barker array implies the existence of a Barker sequence with the same number of elements. However this result is not as strong as Theorem 4.1, because Conjecture 1.3 remains unproved.)

Theorems 4.1 and 4.2 show that the generalisation of Barker sequences to two or more dimensions, while giving a mathematically satisfying result, does not provide practically useful examples having large numbers of elements.

5. The peak sidelobe level of binary sequences

In this section we examine a first relaxation of the Barker sequence criterion (1.4) for an ideal binary sequence. The *peak sidelobe level* (PSL) of a binary sequence $\mathcal{A}$ of length $s > 1$ is

$$M(\mathcal{A}) := \max_{0<u<s} |C_{\mathcal{A}}(u)|. \tag{5.1}$$

The maximum value of the PSL of a length s binary sequence is $s-1$, which is attained by the sequence $[+ \quad + \quad \cdots \quad +]$. The optimal value of the PSL over the set $\mathcal{L}_s$ of all 2^s binary sequences of length s is

$$M_s := \min_{\mathcal{A} \in \mathcal{L}_s} M(\mathcal{A}),$$

and our objective is to understand the behaviour of M_s as $s \to \infty$. In my opinion, this is the most natural modification of Barker's original design problem (1.2) and should be described before the merit factor modification (see Section 6), even though the historical order of study has often been the reverse. Indeed, when binary sequences are used as pulse compression codes for radar scenarios in which the target must be distinguished from a few large objects rather than many smaller objects, the peak sidelobe level is a more important criterion than the merit factor [**Nun05**], [**SLX07**].

No technique is currently known for studying the asymptotic behaviour of M_s directly; instead we rely on indirect approaches and experimental results. The value of M_s has been calculated by exhaustive search for $s \le 61$ [**CFB90**], [**EBSB97**] and $s = 64$ [**CR05**], using a branch-and-bound algorithm with an apparent time complexity of approximately $\Theta(1.4^s)$. The plot of these calculated values in Figure 1 shows that the function M_s is broadly, though not monotonically, increasing for s in the range $s \le 61$. Figure 1 also shows the best known, though not necessarily optimal, values of M for $61 < s \le 105$, $s \ne 64$ [**CR05**], [**NC08a**]. (Note that the PSL values for $61 < s \le 70$, $s \ne 64$ given in [**CR05**] are not necessarily optimal, because the possibility that $M_s = 2$ in that range has not been ruled out and because [**KMB86**] was mistakenly cited as establishing that $M_s \ne 3$ for $s > 51$.)

An indirect approach, and the only proven PSL result for general binary sequences, is to examine the growth rate of the peak sidelobe level of <u>almost all</u> binary sequences. Moon and Moser used elementary counting arguments in 1968 to show that this growth rate lies between order $\sqrt{s}$ and order $\sqrt{s \log s}$:

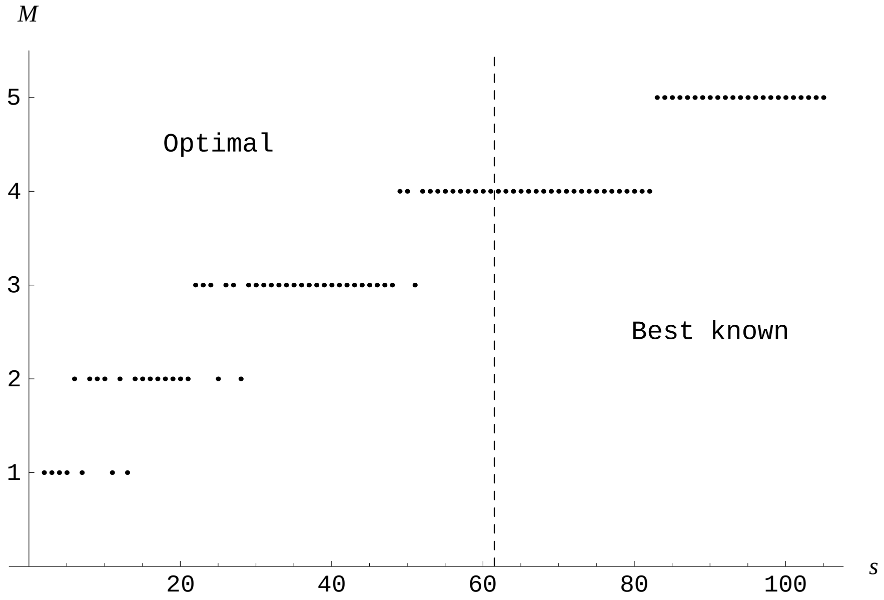

FIGURE 1. The optimal PSL (for $s \leq 61$ and $s = 64$) and the best known PSL (for $61 < s \leq 105$, $s \neq 64$) for binary sequences of length s.

THEOREM 5.1 ([**MM68**]).

(*i*) *If $K(s)$ is any function of s such that $K(s) = o(\sqrt{s})$, then the proportion of sequences $\mathcal{A} \in \mathcal{L}_s$ for which $M(\mathcal{A}) > K(s)$ approaches 1 as $s \to \infty$.*

(*ii*) *For any fixed $\epsilon > 0$, the proportion of sequences $\mathcal{A} \in \mathcal{L}_s$ such that $M(\mathcal{A}) \leq (2+\epsilon)\sqrt{s \log s}$ approaches 1 as $s \to \infty$.*

In 2007, Dmitriev and Jedwab presented experimental evidence that the "upper bound" $\sqrt{s \log s}$ on the order of the growth rate of the PSL in Theorem 5.1 is attained by almost all binary sequences:

EXPERIMENTAL RESULT 5.2 ([**DJ07**]). *The PSL of almost all binary sequences of length s appears to grow like $\Theta(\sqrt{s \log s})$.*

Assuming Experimental Result 5.2 to be correct, the challenge is then to find binary sequences (necessarily forming a set of density zero) whose PSL grows more slowly than order $\sqrt{s \log s}$. Three candidate families of binary sequences and all their cyclic shifts have been investigated, each (by Corollary 6.7) having a PSL growth rate of at least order $\sqrt{s}$: Rudin-Shapiro sequences, Legendre sequences, and m-sequences. We have the following theoretical result due to Høholdt, Jensen and Justesen for Rudin-Shapiro sequences, and experimental results due to Jedwab and Yoshida for Legendre sequences and m-sequences:

THEOREM 5.3 ([**HJJ85**]). *The PSL of a Rudin-Shapiro sequence of length $s = 2^m$ grows like $O(s^{0.9})$.*

EXPERIMENTAL RESULT 5.4 ([**JY06**]). *The PSL of an optimal cyclic shift of a Legendre sequence of prime length s appears to grow like $\Theta(\sqrt{s \log s})$.*

Experimental Result 5.5 ([**JY06**]). *The mean value of the PSL of all m-sequences of length $s = 2^m - 1$ appears to grow like $O(\sqrt{s \log s})$.*

The upper bounding function $s^{0.9}$ for the PSL of a Rudin-Shapiro sequence in Theorem 5.3 is weak compared with $\sqrt{s \log s}$, but data (summarised in [**JY06**, Figure 10]) suggest that the actual PSL grows like $\Omega(\sqrt{s \log s})$. Furthermore, assuming Experimental Results 5.2 and 5.4 to be correct, the growth rate of the PSL of an optimal cyclic shift of a Legendre sequence is no different from that of almost all binary sequences. This leaves m-sequences as the most promising candidate of the three families, as we now examine in detail.

In 1980 McEliece [**McE80**] showed that the PSL of m-sequences grows like $O(\sqrt{s} \cdot \log s)$, and Sarwate later improved the growth constant:

Theorem 5.6 ([**Sar84**]). *The PSL of an m-sequence of length s is at most $1 + (2/\pi)\sqrt{s+1}\log(4s/\pi)$.*

The method of [**McE80**] and [**Sar84**] involved estimation of the maximum absolute value of an incomplete exponential sum, using results obtained in 1918 by Vinogradov and by Pólya (see Tietäväinen [**Tie99**] for an overview of this method). It is an indication of the difficulty of analysing the peak sidelobe level that we have known for nearly 40 years (via Theorem 5.1) that the PSL of almost all binary sequences grows like $O(\sqrt{s \log s})$, and yet the strongest known result on the growth rate of the PSL of any $\underline{\text{specific}}$ family of binary sequences is $O(\sqrt{s} \cdot \log s)$ (via Theorem 5.6)!

On the other hand, the radar literature from the 1960s onwards tells a different story, with repeated statements that the PSL of some or all m-sequences of length $s = 2^m - 1$ grows like $O(\sqrt{s})$ (and therefore like $\Theta(\sqrt{s})$, by Corollary 6.7). Jedwab and Yoshida [**JY06**] were unable to trace any published theoretical basis for these claims, and could not reach a stronger conclusion than Experimental Result 5.5 from exhaustive calculation for $m \leq 15$. But Dmitriev and Jedwab showed in 2007 that these claims, while previously unsupported both theoretically and experimentally, appear to be correct for almost all m-sequences:

Experimental Result 5.7 ([**DJ07**]). *The PSL of almost all m-sequences of length s appears to grow like $\Theta(\sqrt{s})$.*

Experimental Result 5.7 is the first numerical evidence of $\Theta(\sqrt{s})$ growth in the PSL of any family of binary sequences. It relies on an algorithm for calculating the maximum PSL over all cyclic shifts of an m-sequence generated by a given primitive element α of $\mathrm{GF}(s+1)$ (see Section 3), that requires only $\Theta(s)$ operations instead of the previous $\Theta(s^2)$. This reduction in time complexity extends the range of exhaustive calculation to $m \leq 25$, revealing behaviour that would not otherwise be apparent. In particular, the mean (taken over all primitive elements α of $\mathrm{GF}(s+1)$) of the maximum PSL over all cyclic shifts appears to be approximately $1.31\sqrt{s}$ for large s. Data from the new algorithm also imply the following improvement on Experimental Result 5.5:

Experimental Result 5.8 ([**DJ07**]). *The PSL of all m-sequences of length s appears to grow like $O(\sqrt{s} \cdot \log\log s)$*

Figure 2 is a schematic summary of the strongest known theoretical and experimental results on the peak sidelobe level of binary sequences. Experimental Results 5.2, 5.7 and 5.8 provide clear directions for future research.

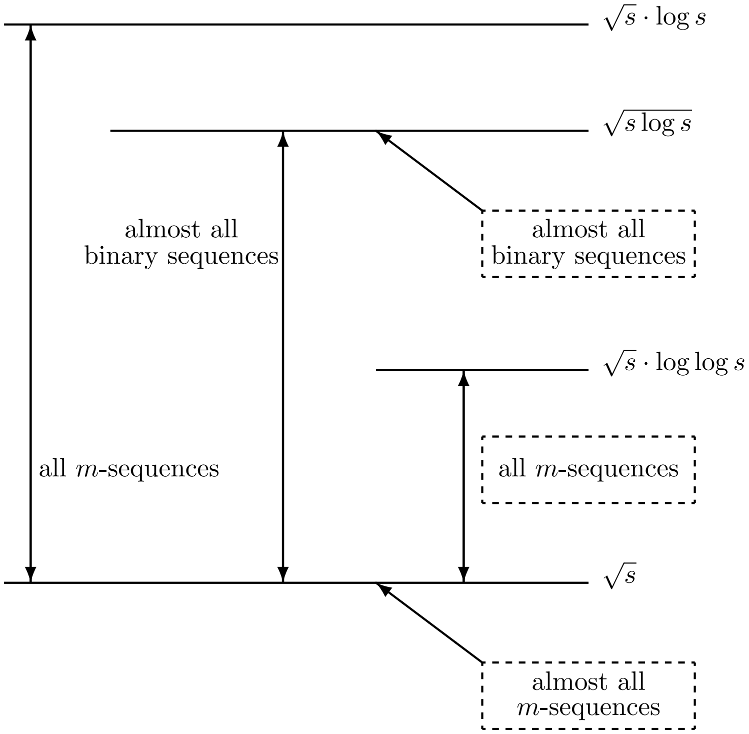

FIGURE 2. Growth rate of the peak sidelobe level of binary sequences (dashed box around text indicates an experimental result)

6. The merit factor of binary sequences

In this section we examine a second relaxation of the Barker sequence criterion (1.4) for an ideal binary sequence (see [**Jed05**] for a more detailed exploration). The *merit factor* of a binary sequence $\mathcal{A}$ of length $s > 1$ is defined to be

$$F(\mathcal{A}) := \frac{s^2}{2\sum_{0<u<s}[C_{\mathcal{A}}(u)]^2}, \tag{6.1}$$

which places more emphasis on the collective smallness of the values $|C_{\mathcal{A}}(u)|$ than the peak sidelobe level (5.1) does. The name "merit factor" was coined in 1972 by Golay [**Gol72**], although equivalent quantities had been studied several years earlier by communications engineers such as Lunelli [**Lun65**] and by complex analysts such as Littlewood [**Lit68**]. The optimal value of the merit factor over the set $\mathcal{L}_s$ of all 2^s binary sequences of length s is

$$F_s := \max_{\mathcal{A} \in \mathcal{L}_s} F(\mathcal{A}),$$

and our objective is to understand the behaviour of F_s as $s \to \infty$. Since the mean value of $1/F(\mathcal{A})$, taken over all binary sequences $\mathcal{A} \in \mathcal{L}_s$, is $(s-1)/s$ [**NB90**], we immediately have $F_s > 1$ for all s.

The merit factor is a natural measure of the energy efficiency of a binary sequence used to transmit information by modulating a carrier signal, which is of particular importance in spread-spectrum communication [**BCH85**]. The larger the merit factor of the sequence, the more uniformly the signal energy is distributed over the frequency range. The merit factor occurs in equivalent guise in complex analysis, as the study of the L_4 norm of complex-valued polynomials with ±1 coefficients on the unit circle (see [**Bor02**] for background on this and other norms), although the connection seems not to have been recognised until 1988 [**HJ88**]. Maximisation of the merit factor is also studied in statistical mechanics, in terms of finding the minimum energy states (ground states) of a quantum Ising spin model [**Ber87**]. Within theoretical physics and theoretical chemistry, maximisation of the merit factor is recognised as a notoriously difficult combinatorial optimisation problem [**MZB98**]. The merit factor is a useful sequence design criterion for radar scenarios in which the target must be distinguished from a large number of comparably sized smaller objects (although it has recently been argued [**SLX07**] that a more complex criterion is preferable for this scenario).

The value of F_s has been calculated by exhaustive search for $s \leq 60$ by Mertens and Bauke [**MB07**], using a branch-and-bound algorithm with an apparent time complexity of approximately $\Theta(1.85^s)$. Several authors have used stochastic algorithms to find large, though not necessarily optimal, values of F for sequences of length $s > 60$. Figure 3 shows the current best known value of F for $60 < s \leq 200$ [**BFK07**], together with the value of F_s for $s \leq 60$.

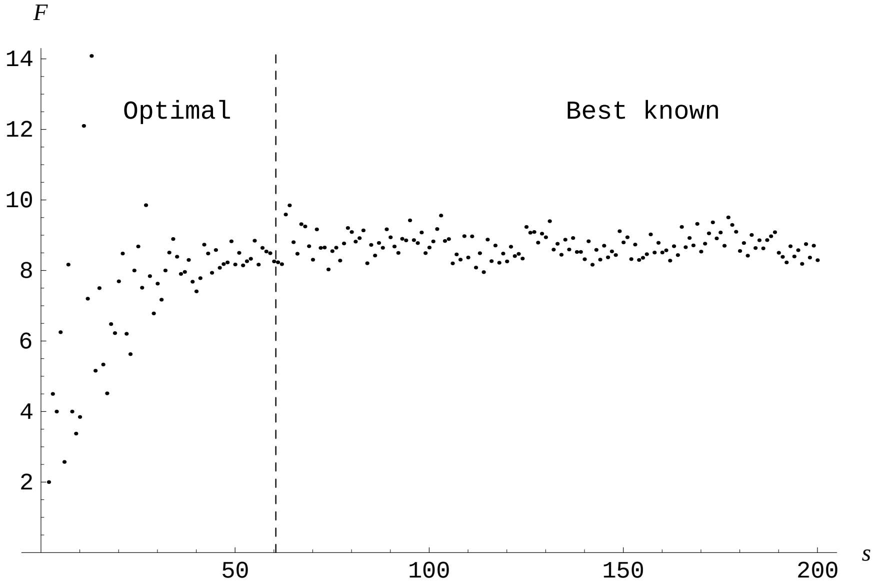

Figure 3. The optimal merit factor (for $s \leq 60$) and the best known merit factor (for $60 < s \leq 200$) for binary sequences of length s.

The asymptotic merit factor has been calculated for the following families of binary sequences: Rudin-Shapiro sequences and their generalisations; Legendre sequences and their generalisations; and m-sequences. In each case the asymptotic merit factor is an integer, although we do not yet have a good explanation as to why. The earliest of these calculations was given by Littlewood in 1968:

Theorem 6.1 ([**Lit68**]). *The asymptotic merit factor of a Rudin-Shapiro sequence is* 3.

Theorem 6.1 was generalised to two other recursively defined families of binary sequences whose asymptotic merit factor is also 3 [**HJJ85**], [**BM00**]. Høholdt and Jensen, building on a numerical investigation by Turyn and a heuristic derivation due to Golay [**Gol83**], showed in 1988:

Theorem 6.2 ([**HJ88**]). *The asymptotic merit factor of any cyclic shift of a Legendre sequence is at most* 6*, and equality is attained when the cyclic shift is* $1/4$ *and* $3/4$ *of the sequence length.*

Several generalisations of Legendre sequences also attain an asymptotic merit factor of 6 under optimal cyclic shifts [**JJH91**], [**BC01**], [**XH08**]. Jensen and Høholdt showed in 1989:

Theorem 6.3 ([**JH89**]). *The asymptotic merit factor of an* m*-sequence is* 3.

Legendre sequences and m-sequences, unlike Rudin-Shapiro sequences, are known to have a highly structured periodic autocorrelation function. This periodic structure was used crucially in the proof of Theorems 6.2 and 6.3, whereas Theorem 6.1 was proved directly from the recurrence relation (3.1).

Theorem 6.2 implies that $\limsup_{s\to\infty} F_s \geq 6$, and after nearly 20 years this remains the strongest proven result on the asymptotic behaviour of F_s. Nonetheless, in 2004 Borwein, Choi and Jedwab, building on a numerical investigation by Kirilusha and Narayanaswamy [**KN99**], showed experimentally that a merit factor greater than 6.34 seems to be achievable:

Experimental Result 6.4 ([**BCJ04**]). *A merit factor greater than* 6.34 *appears to be obtainable consistently, by concatenating a long Legendre sequence and a suitable initial portion of a suitable cyclic shift of itself.*

The appropriate amount of cyclic shift and length of initial portion were derived exactly in [**BCJ04**], subject to a conjecture on the asymptotic merit factor of any truncation of any cyclic shift of a Legendre sequence. The value 6.34... then arises as a function of a solution to a cubic equation. Certain generalisations of the construction of [**BCJ04**] also appear to attain a merit factor greater than 6.34 [**YG07**].

The value of $\limsup_{s\to\infty} F_s$ has been variously conjectured to be: 6 [**HJ88**], based on numerical data available in the late 1980s for $s < 200$; greater than 7, and perhaps greater than 8 or 9 [**BFK07**], based on recent numerical data for $s \leq 200$; 12.32... [**Gol82**], based on heuristic arguments and the "Postulate of Mathematical Ergodicity" (see [**Jed05**, Section 4.7] for discussion of this unproven assumption); and ∞, conjectured by Littlewood in 1966:

Conjecture 6.5 ([**Lit66**, §6]). $\limsup_{s\to\infty} F_s = \infty$.

The conjectured value 6 no longer seems plausible, in view of Experimental Result 6.4. At the other extreme, the value ∞ in Conjecture 6.5 was based on the calculation of F_s in the very limited range $s \leq 19$ in 1966. The much more extensive data now available, shown in Figure 3, do not suggest that the merit factor can grow without bound.

Some directions for future research are:

1. Investigate Experimental Result 6.4 theoretically.
2. Seek a family of binary sequences which reduces or eliminates the gap between the apparent limiting merit factor of at least 8 suggested by Figure 3, and the largest merit factor value 6.34... so far shown experimentally to be obtainable consistently for long sequences. In view of the known asymptotic results of Theorems 6.1, 6.2 and 6.3, one might hope that the asymptotic merit factor of such a family would take an integer value, namely 7 or larger.
3. Settle the fundamental question as to whether Conjecture 6.5 is correct, which relates to several other conjectures (see [**Jed05**, Section 2.2]).

We conclude this section by examining the relationship between the peak sidelobe level and the merit factor. We know that if the peak sidelobe level of a family of binary sequences were to grow more slowly than order $\sqrt{s}$, then the merit factor of that family would grow without bound and so Conjecture 6.5 would be true:

Proposition 6.6 (Jedwab and Yoshida 2006 [**JY06**]). *Let $\mathcal{B}$ be a family of binary sequences and let each $\mathcal{A}_s \in \mathcal{B}$ have length s. If $\liminf_{s\to\infty}(M(\mathcal{A}_s)/\sqrt{s}) = 0$ then $\limsup_{s\to\infty} F(\mathcal{A}_s) = \infty$.*

Assuming that Conjecture 6.5 is false (which most researchers appear to believe), Proposition 6.6 demonstrates the strength of Experimental Result 5.7, because the apparent growth rate $\Theta(\sqrt{s})$ of that result is then the optimal growth rate for the peak sidelobe level of all binary sequences. Application of Proposition 6.6 to Theorems 6.1, 6.2 and 6.3 gives:

Corollary 6.7. *The PSL of a length s sequence that is a Rudin-Shapiro sequence, any cyclic shift of a Legendre sequence, or an m-sequence, grows like $\Omega(\sqrt{s})$.*

Proposition 6.6 is an extreme instance of a more general phenomenon, whereby small values of the peak sidelobe level M are often associated with large values of the merit factor F. Indeed, for the three binary sequence families discussed in this section (Rudin-Shapiro sequences, Legendre sequences, and m-sequences), the graphs of the variation of M and of $1/F$ over all cyclic shifts of the sequence appear to have broadly similar shape [**JY06**]. Since this similarity of graphs includes Rudin-Shapiro sequences, it is not restricted to sequences having a highly structured periodic autocorrelation function. However the association between small M and large F is not perfect: whereas suitable cyclic shifts of Legendre sequences perform better than m-sequences with respect to the merit factor (compare Theorems 6.2 and 6.3), all cyclic shifts of Legendre sequences appear to perform worse than m-sequences with respect to the peak sidelobe level (compare Experimental Results 5.4 and 5.8).

7. Barker sequences over a non-binary alphabet

This section deals with the modification of Problem 1.1 in which the binary alphabet is replaced by an H-phase or unimodular alphabet (see Section 3 for the definition of these alphabets and the associated aperiodic autocorrelation function).

We are interested firstly in an ideal solution to the modified Problem 1.1, and secondly in relaxations of the ideal condition that produce further examples.

What property should an H-phase sequence $\mathcal{A}$ of length s possess to be called Barker? In the binary case $H = 2$, we saw in Section 1 that it should be an ideal solution of Problem 1.1 in the sense that

$$\text{for each } u \neq 0 \text{ independently, } |C_{\mathcal{A}}(u)| \text{ takes its smallest possible value,} \tag{7.1}$$

which for $H = 2$ implies that

$$|C_{\mathcal{A}}(u)| = 0 \text{ or } 1 \quad \text{for all } u \neq 0. \tag{7.2}$$

In the case $H > 2$, the same reasoning applied to the H-phase version of Problem 1.1 indicates that the sequence should likewise be ideal according to (7.1). While I believe that (7.1) is the natural criterion for an H-phase Barker sequence, it is not the generally accepted one. Instead, Golomb and Scholtz [**GS65**] defined a *generalised Barker sequence* to be a unimodular sequence $\mathcal{A}$ for which

$$|C_{\mathcal{A}}(u)| \leq 1 \quad \text{for all } u \neq 0. \tag{7.3}$$

(An alternative name is a *polyphase Barker sequence*, although the literature is inconsistent about whether and how "generalised" and "polyphase" should distinguish the unimodular case from the more constrained H-phase case.)

The relationship between the criteria (7.1), (7.2), and (7.3) for an H-phase sequence depends on the value of H, as we now examine. We shall see that, as a definition for an H-phase (or unimodular) generalised Barker sequence: (7.1) is of theoretical interest but apparently too restrictive for practical purposes; (7.2) is inappropriate except for specific small values of H; and (7.3) is too relaxed to identify the best sequences, and should be used in conjunction with some other condition.

- $H = 2$**,** 3 **and** 4**.**
  In this case the three conditions (7.1), (7.2), and (7.3) coincide: for u satisfying $0 < u < s$, they are equivalent in the cases $H = 2$ and 4 to
  $$|C_{\mathcal{A}}(u)| = \begin{cases} 1 & \text{for } s-u \text{ odd} \\ 0 & \text{for } s-u \text{ even,} \end{cases}$$
  and in the case $H = 3$ to
  $$|C_{\mathcal{A}}(u)| = \begin{cases} 1 & \text{for } s-u \equiv 1 \text{ or } 2 \pmod 3 \\ 0 & \text{for } s-u \equiv 0 \pmod 3. \end{cases}$$
  In particular, for these values of H we can regard (7.3) as a convenient shorthand for (7.2), which is possibly why (7.3) was chosen in [**GS65**] as the definition of an H-phase generalised Barker sequence.

- $H = 6$**.**
  In this case (7.2) and (7.3) are again equivalent, and (7.1) implies (7.3), but (7.3) does not imply (7.1). For example, consider the 6-phase length 9 sequences $\mathcal{B} = (\exp(b[i]\pi\sqrt{-1}/3))$ and $\mathcal{C} = (\exp(c[i]\pi\sqrt{-1}/3))$, where $(b[i]) = [0, 0, 1, 1, 5, 4, 1, 3, 0]$ and $(c[i]) = [0, 0, 0, 2, 5, 1, 4, 3, 1]$. The aperiodic autocorrelations of these sequences have magnitude
  $$(|C_{\mathcal{B}}(u)| : 0 \leq u < 9) = (9, 0, 0, 0, 1, 0, 0, 0, 1)$$

and

$$(|C_{\mathcal{C}}(u)| : 0 \le u < 9) = (9,\, 1,\, 1,\, 1,\, 1,\, 1,\, 1,\, 1,\, 1),$$

so although $\mathcal{B}$ and $\mathcal{C}$ are both 6-phase generalised Barker sequences, $\mathcal{B}$ is a better sequence than $\mathcal{C}$. This suggests the use of the sum of squares $\sum_{0<u<s} |C_{\mathcal{A}}(u)|^2$ as an additional criterion to (7.3) for evaluating the fitness of an H-phase generalised Barker sequence $\mathcal{A}$ of length s.

- $H = 5$ **and** $H > 6$.
  For $H = 5$ and $H > 6$, (7.3) does not imply (7.2) because $|C_{\mathcal{A}}(u)|$ can take non-zero values strictly less than 1. For example, up to equivalence transformations, the unique 8-phase length 16 generalised Barker sequence is [**Mow93**]

  $$\mathcal{B} = [1,\, 1,\, 1,\, -i,\, -i,\, 1,\, i,\, i,\, -i,\, -1,\, i,\, -i,\, 1,\, -1,\, 1,\, e^{3\pi\sqrt{-1}/4}],$$

  and for u satisfying $0 < u < 16$ we have

  $$|C_{\mathcal{B}}(u)| = \begin{cases} 1 & \text{for } u \text{ odd} \\ \sqrt{2-\sqrt{2}} & \text{for } u \text{ even.} \end{cases}$$

  Since $\sqrt{2-\sqrt{2}} < 1$, (7.2) is not an appropriate criterion for an H-phase generalised Barker sequence, for general H. Furthermore, the generalised Barker sequence $\mathcal{B}$ does not achieve the smallest possible value of $|C_{\mathcal{A}}(u)|$ for each $u \neq 0$. Indeed, no 8-phase length 16 sequence $\mathcal{A}$ can do so, otherwise for u satisfying $0 < u < 16$ we would have

  $$|C_{\mathcal{A}}(u)| = \begin{cases} 1 & \text{for } u \text{ odd} \\ 0 & \text{for } u \text{ even,} \end{cases}$$

  and $\mathcal{B}$ would not be unique. Apparently (7.1) is too restrictive a criterion for practical purposes, although I believe it is of theoretical interest to classify the H-phase sequences satisfying this criterion.

Table 1 shows existence results for H-phase generalised Barker sequences up to length 19 for $H \in \{2, 3, 4, 6, 8\}$, taken from exhaustive searches reported in [**BF07**]. (Some of the table entries imply others, because an H-phase generalised Barker sequence can be considered as a kH-phase generalised Barker sequence of the same length, for any integer k. The entries for $H = 2$ were discussed in Section 1.) The suggestive existence pattern for $H = 6$ up to length 13 was known to Golomb and Scholtz in 1965 [**GS65**], motivating their conjecture that a 6-phase generalised Barker sequence exists for every length; however the length 16 provides a counterexample. (Chang and Golomb [**CG94**], [**CG96**] stated the nonexistence of 6-phase length 16 generalised Barker sequences earlier than [**BF07**], but gave other nonexistence results which disagree with those in [**BF07**]. In particular, they claimed there is no 6-phase length 18 generalised Barker sequence, whereas P. Borwein and R. Ferguson [personal communication, November 2007] provided the sequence $(\exp(a[i]\pi\sqrt{-1}/3))$ to verify their statement to the contrary in [**BF07**], where

$$(a[i]) = [0,\, 0,\, 1,\, 1,\, 4,\, 5,\, 5,\, 0,\, 4,\, 1,\, 5,\, 2,\, 2,\, 0,\, 1,\, 4,\, 4,\, 2].$$

I have therefore quoted the results in [**BF07**], in preference to those in [**CG94**] and [**CG96**].)

No H-phase generalised Barker sequence of length $s > 18$ has been found for $H \in \{3, 4, 6, 8\}$, and by exhaustive search P. Borwein and R. Ferguson [personal communication, February 2008] have established nonexistence for $H = 3$ and $20 \leq s \leq 76$, for $H = 4$ and $20 \leq s \leq 60$, for $H = 6$ and $20 \leq s \leq 29$, and for $H = 8$ and $20 \leq s \leq 25$. This suggests an extension of Conjecture 1.3 to these values of H and lengths $s > 18$. The only theoretical support for this conjecture of which I am aware is due to Turyn [**Tur74a**], for the cases $H = 3$ and 4.

For fixed H, numerical studies (including those described above) suggest that H-phase generalised Barker sequences become more scarce as the length s grows. In view of this, many authors have sought examples by instead fixing s, and either allowing the number of phases H to grow or else allowing the sequence alphabet to be unimodular. Extensive computational work by a succession of authors, ranging from a 1974 study for $s \leq 18$ [**SA74**] to recent work for $s \leq 63$ [**BF05**], $s = 64$ [**Nun05**], and $s \geq 65$ [**NC08b**], has established:

Proposition 7.1. *There exists a unimodular generalised Barker sequence for all lengths $s \leq 70$ and for $s \in \{72, 76, 77\}$.*

The method of these authors was either to restrict in advance to an H-phase alphabet for some large value of H and search stochastically, or else to perform numerical optimisation on continuous-valued phase variables followed by quantisation to a finite alphabet. The work leading to Proposition 7.1 is motivated by the question:

Question 7.2. *Does a unimodular generalised Barker sequence of length s exist for all s?*

Some authors, for example [**ZG93**] and [**Fri96**], concluded from computational studies that the answer to Question 7.2 is negative, but these conclusions were shown to be premature by later work, and it remains the case that "There is currently no evidence against a positive answer" [**Mow96**]. Ein-Dor, Kanter and Kinzel [**EDKK02**] argue that an H-phase generalised Barker sequence of length s exists for all $H \geq s$ and sufficiently large s, under the assumption of Golay's unproven "Postulate of Mathematical Ergodicity" (mentioned in Section 6; see also [**Jed05**, Section 4.7]).

We have seen that the generalised Barker sequence condition (7.3) is too relaxed to identify the best unimodular sequences $\mathcal{A}$ of length s, and that it should be used in conjunction with some other distinguishing condition. One alternative for this condition is to minimise the number of phases H required to represent the sequence.

		s																	
		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
H	2	✓	✓	✓	✓	×	✓	×	×	×	✓	×	✓	×	×	×	×	×	×
	3	✓	✓	✓	✓	×	✓	×	✓	×	×	×	×	×	×	×	×	×	×
	4	✓	✓	✓	✓	×	✓	×	×	×	✓	×	✓	×	✓	×	×	×	×
	6	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×	✓	×
	8	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	×	×	×

Table 1. Existence pattern for H-phase generalised Barker sequences of length s (where ✓ indicates existence and × nonexistence)

This has the significant advantage of simplifying the practical implementation: with each increase in H, the phase resolution required from the digital signalling becomes physically more difficult, and for very large values of H or for unimodular sequences the signalling becomes effectively analogue. A second alternative is to minimise the sum of squares $\sum_{0<u<s}|C_{\mathcal{A}}(u)|^2$ (see the earlier discussion of the case $H = 6$), or equivalently to maximise the merit factor

$$F(\mathcal{A}) := \frac{s^2}{2\sum_{0<u<s}|C_{\mathcal{A}}(u)|^2}, \tag{7.4}$$

which reduces to (6.1) in the binary case. A third alternative is to minimise the peak sidelobe level; since $|C_{\mathcal{A}}(s-1)| = 1$ for any unimodular sequence $\mathcal{A}$ of length $s > 1$, we exclude the value $u = s-1$ by writing (for $s > 2$)

$$M(\mathcal{A}) := \max_{0<u<s-1}|C_{\mathcal{A}}(u)|, \tag{7.5}$$

which reduces to (5.1) in the binary case. A sequence that is optimal according to one condition is not necessarily optimal according to another, although good performance as measured by different conditions is often associated (as noted at the end of Section 6 in the case of binary sequences). Borwein and Ferguson [**BF05**] used a stochastic algorithm to search for H-phase generalised Barker sequences of length up to 63 that are optimal with respect to each of these three conditions (smallest number of phases H, smallest sum of squares $\sum_{0<u<s}|C_{\mathcal{A}}(u)|^2$, and smallest peak sidelobe level) in turn. Although they argued on statistical grounds that the best values found in [**BF05**] for the smallest sum of squares are "good candidates for global minima ... up to length 45," the value found for length 43 (and for several lengths greater than 45) was improved in [**NC08b**].

Some directions for future research are:

1. Find theoretical nonexistence results for H-phase generalised Barker sequences with small values of H, for example by developing arguments in [**Tur74a**].
2. Approach Question 7.2 theoretically, perhaps by weakening or removing the statistical assumptions used in [**EDKK02**] (rather than seeking to extend Proposition 7.1 to larger values of s numerically).
3. Classify the H-phase sequences satisfying the ideal criterion (7.1). The classification is known when H is a multiple of 6, because (7.1) then requires

$$C_{\mathcal{A}}(u) = 0 \quad \text{for each } u \text{ satisfying } 0 < u < s-1, \tag{7.6}$$

and no unimodular sequence of length $s > 3$ satisfies (7.6) [**WHD77**].

Finally, we mention that the merit factor (7.4) of H-phase sequences with $H > 2$ appears to exhibit very different behaviour from that of binary sequences, as the length s grows. For example, a *Frank sequence* is a $\sqrt{s}$-phase sequence of square length s whose merit factor appears to grow like $O(\sqrt{s})$ [**AB90**], whereas no binary sequence family is known whose merit factor grows without bound (see Section 6). Furthermore, the peak sidelobe level (7.5) of Frank sequences has been proved to grow like $O(\sqrt{s})$ [**Tur67**] (and appears to grow like $\Theta(\sqrt{s})$ [**AB90**]), whereas a growth rate of $\Theta(\sqrt{s})$ is apparently achievable but has not yet been proved for any binary sequence family (see Section 5).

8. Pairs of Golay complementary sequences and arrays

In this section we deal with the modification of Problem 1.1 in which a binary sequence is replaced by a pair of binary sequences whose aperiodic autocorrelation functions sum to zero at all non-zero shifts. Unlike the case of non-binary Barker sequences (see Section 7), it is clear how to extend this modification to a complex alphabet, as well as to multi-dimensional arrays. The resulting objects are of interest both practically and theoretically.

A *Golay (complementary) sequence pair* is a pair of length s sequences $\mathcal{A}$ and $\mathcal{B}$ over some alphabet $W \subseteq \mathbb{C}$, for which

$$C_{\mathcal{A}}(u) + C_{\mathcal{B}}(u) = 0 \quad \text{for all } u \neq 0. \tag{8.1}$$

In higher dimensions, an $s_1 \times \cdots \times s_r$ *Golay (complementary) array pair* is a pair of $s_1 \times \cdots \times s_r$ arrays $\mathcal{A}$ and $\mathcal{B}$ over $W \subseteq \mathbb{C}$, for which

$$C_{\mathcal{A}}(u_1, \ldots, u_r) + C_{\mathcal{B}}(u_1, \ldots, u_r) = 0 \quad \text{for all } (u_1, \ldots, u_r) \neq (0, \ldots, 0).$$

We call an array $\mathcal{A}$ a *Golay array* if it forms a Golay array pair with some array $\mathcal{B}$; and similarly for sequences. Golay sequences and arrays are particularly useful in digital information processing because their summed autocorrelations are precisely zero, rather than just having small magnitude, and their defining property (8.1) resides in the aperiodic domain that is the natural setting for many physical processes. They have been applied in such diverse areas as infrared multislit spectrometry [**Gol51**], X-ray and gamma-ray coded aperture imaging [**OHT78**], optical time domain reflectometry [**NNG$^+$89**], power control for multicarrier wireless transmission [**DJ99**], and medical ultrasound [**NSL$^+$03**]. The central theoretical questions are: for what sizes $s_1 \times \cdots \times s_r$ does a Golay array pair exist, and how many distinct Golay array pairs of a given size are there?

The earliest results are for binary Golay sequence pairs, as introduced in 1951 by Golay [**Gol51**]. (Although the paper [**Gol51**] predates Barker's [**Bar53**], to my knowledge all other research on Golay sequence pairs occurred in 1960 [**Wel60**] or 1961 [**Gol61**] or later, and so can be considered a response to the presumed nonexistence of long Barker sequences as suggested in Section 2.) Binary Golay sequence pairs $(\mathcal{A}, \mathcal{B})$ exist for lengths 2 and 10 [**Gol51**] and 26 [**Gol62**], for example:

$$\begin{array}{rrl}
s = 2: & \mathcal{A} = & [+\,+] \\
 & \mathcal{B} = & [+\,-] \\
s = 10: & \mathcal{A} = & [+\,+\,+\,+\,+\,-\,+\,-\,-\,+] \\
 & \mathcal{B} = & [+\,+\,-\,-\,+\,+\,+\,-\,+\,-] \\
s = 26: & \mathcal{A} = & [+\,+\,+\,+\,-\,+\,+\,-\,-\,+\,-\,+\,-\,+\,-\,-\,+\,-\,+\,+\,+\,-\,-\,+\,+\,+] \\
 & \mathcal{B} = & [+\,+\,+\,+\,-\,+\,+\,-\,-\,+\,-\,+\,+\,+\,+\,+\,-\,+\,-\,-\,-\,+\,+\,-\,-\,-].
\end{array}$$

Binary Golay sequence pairs therefore exist for infinitely many lengths, by Turyn's 1974 composition construction:

Theorem 8.1 ([**Tur74b**]). *If there exist binary Golay sequence pairs of length s_1 and s_2 then there exists a binary Golay sequence pair of length $s_1 s_2$.*

Corollary 8.2. *There exists a binary Golay sequence pair of length $2^a 10^b 26^c$ for all integer $a, b, c \geq 0$.*

The following results, discovered nearly 40 years apart, together contain all known general nonexistence results for binary Golay sequence pairs:

Proposition 8.3 ([**Gol51**], proved in [**Gol61**]). *If there exists a binary Golay sequence pair of length $s > 1$ then s is even.*

Theorem 8.4 ([**EKS90**]). *If there exists a binary Golay sequence pair of length $s > 1$ then s has no prime factor congruent to 3 modulo 4.*

Theorem 8.4 was re-proved elegantly by Eliahou, Kervaire and Saffari in [**EKS91**], by representing the sequences of the Golay pair as polynomials and analysing the possible divisors of the polynomial version of (8.1). Theorem 8.4 implies Theorem 1.5, because if $(A[i])$ is a Barker sequence of even length then $(A[i])$ and $((-1)^i A[i])$ form a Golay sequence pair. The number of distinct binary Golay sequence pairs has been determined by exhaustive search for all lengths less than 100; the smallest length for which existence is open is 106 [**BF03**].

Golay sequence pairs have been studied over many non-binary alphabets, including: ternary [**GL94**], [**CK01**] (meaning the alphabet $\{1, 0, -1\}$ rather than the 3-phase alphabet); quaternary [**CHK02**]; 2^h-phase [**DJ99**]; H-phase [**Pat00**] (where H must be even for $s > 1$, otherwise (8.1) fails for $u = s - 1$); unimodular [**Bud90**]; and QAM (quadrature amplitude modulation) [**CVT03**]. The richest known structure for H-phase Golay sequences occurs at lengths 2^m, which are also usually the most convenient lengths for implementation. In 1999 Davis and Jedwab gave an explicit construction, using algebraic normal form, for 2^h-phase Golay sequence pairs of length 2^m:

Theorem 8.5. [**DJ99**] *For any integers $m, h \geq 1$, there are at least $2^{h(m+1)} \cdot m!/2$ distinct 2^h-phase Golay sequences of length 2^m (and at least twice as many for $m = 1$), which form at least $2^{h(m+2)} m!$ ordered Golay sequence pairs.*

In the binary case $h = 1$, the Golay sequences described in Theorem 8.5 occur as $m!/2$ complete cosets of the first-order Reed-Muller code $\mathrm{RM}(1, m)$ within the second-order Reed-Muller code $\mathrm{RM}(2, m)$; the same is true for the non-binary cases $h > 1$ under suitable generalisation of the Reed-Muller code. These Golay sequences can therefore be used in multicarrier wireless transmission, where the Golay property allows tight control of variations in power output, the Reed-Muller code property allows strong error correction, and the required modulation and demodulation is carried out using Fourier transform processing [**DJ99**]. Paterson [**Pat00**] showed that the algebraic normal forms of the construction described in Theorem 8.5 hold without modification when 2^h is replaced by any even H.

For six years after Theorem 8.5 was known, it appeared that the underlying construction might account for all 2^h-phase Golay sequences of length 2^m. But in 2005, Li and Chu [**LC05**] discovered 1024 additional quaternary Golay sequences of length 16 by computer search, lying in the (quaternary generalisation of the) third-order Reed-Muller code. The origin of these additional 1024 Golay sequences was shown to be the quaternary length 8 Golay sequences

$$[1, 1, 1, -1, 1, 1, -1, 1] \quad \text{and} \quad [1, \sqrt{-1}, -\sqrt{-1}, 1, 1, -\sqrt{-1}, \sqrt{-1}, 1], \tag{8.2}$$

which share the same autocorrelation function even though they do not lie in the same equivalence class under standard equivalence transformations [**FJ06**]. Li and Chu's discovery prompted the question as to which further Golay sequences of length greater than 16 (not described in Theorem 8.5) can be derived, under known recursive constructions such as concatenation and interleaving, from the 1024 additional length 16 Golay sequences. This question was answered from the viewpoint of Golay array pairs, as we now describe.

In 2007, Jedwab and Parker proposed that a Golay array pair, constructed in as many dimensions as possible, is a fundamental object of study, and that Golay sequence pairs should be viewed as derived objects under repeated reduction of the number of dimensions by one:

Theorem 8.6 ([**JP07a**]). *If there exists an $s \times t \times s_1 \times \cdots \times s_r$ Golay array pair over an alphabet $W \subseteq \mathbb{C}$, where $r \geq 0$, then there exists an $st \times s_1 \times \cdots \times s_r$ Golay array pair over W.*

Theorem 8.6 is proved by applying a "projection mapping" to each array of the higher-dimensional Golay pair, replacing each $s \times t$ "slice" formed from the first two dimensions of the array by the sequence obtained when the elements of the slice are listed column by column. (Projection mappings, combined with a parity argument, were also used to establish Theorem 4.3.) In 2008, Fiedler, Jedwab and Parker showed [**FJP08**] that the array viewpoint leads to a three-stage process for constructing and enumerating Golay sequence and array pairs:

1. construct suitable Golay array pairs from lower-dimensional Golay array pairs, using a generalisation of Theorem 8.1;
2. apply transformations to these Golay array pairs to generate a larger set of Golay array pairs; and
3. take all possible images of the resulting Golay array pairs under successive projection mappings.

This process simplifies previous approaches, by separating the construction of Golay arrays in Steps 1 and 2 from the enumeration of all possible projections of these arrays to lower dimensions in Step 3. In particular, it constructs all 2^h-phase Golay sequences of length 2^m obtainable under any known method. In the quaternary case, it constructs all Golay sequences of length 2^m derivable from Li and Chu's examples [**LC05**], leading to the following counts:

Theorem 8.7 ([**FJP08**]). *Let $m > 3$ be an integer. There are at least*

$$\sum_{c=0}^{\lfloor (m+1)/4 \rfloor} 2^{2m-c+1} \binom{m-3c+1}{c} (m-2c)!$$

quaternary Golay sequences of length 2^m, and at least 8 times this number of quaternary Golay sequence pairs of length 2^m.

By combining Theorem 8.6, a generalisation of Theorem 8.1, and computer search results from [**BF03**], the sizes for which there exists a binary Golay array pair with fewer than 100 elements can be determined:

Proposition 8.8 ([**JP07a**]). *Up to reordering of dimensions, an $s_1 \times \cdots \times s_r$ binary Golay array pair with $1 < \prod_{k=1}^{r} s_k < 100$ exists for precisely the following sizes, together with the derived sizes arising from Theorem 8.6:*

2, 2×2, $2 \times 2 \times 2$, $2 \times 2 \times 2 \times 2$, $2 \times 2 \times 2 \times 2 \times 2$, $2 \times 2 \times 2 \times 2 \times 2 \times 2$,
10, 2×10, $2 \times 2 \times 10$, $2 \times 2 \times 2 \times 10$, 26, 2×26.

The introduction of the Golay array viewpoint suggests some questions for future research:

1. Only two ingredients are needed in the three-stage construction process to construct all known 2^h-phase Golay sequences of length 2^m [**FJP08**]: trivial Golay sequence pairs ([1], [1]), together with 512 ordered quaternary length 8 "cross-over" Golay sequence pairs resulting from the shared autocorrelation function of the sequences (8.2). Can we find other ingredients for the construction process that produce new 2^h-phase Golay sequences of length 2^m?
2. How can the three-stage construction process be used to simplify or extend known results on the construction of Golay sequences in other contexts, such as QAM alphabets, the ternary alphabet $\{1, 0, -1\}$, or quaternary sequences whose length is not a power of 2?

9. Conclusion

There is overwhelming numerical evidence in favour of the Barker Sequence Conjecture (see Theorem 1.6), though still no proof despite nearly 50 years of effort. In this survey, I argue that many of the combinatorial objects that have been studied for their favourable aperiodic autocorrelation properties can be viewed as responses to the presumed nonexistence of long Barker sequences, including: multidimensional Barker arrays; binary sequences with small peak sidelobe level; binary sequences with large merit factor; Barker sequences over a non-binary alphabet; and pairs of Golay complementary sequences and arrays. The existence question for Barker arrays in two or more dimensions has now been completely solved. Recent results have opened up new research directions for each of the other listed responses.

Further combinations of responses are possible, apart from those considered here. Some of these, with illustrative references, are: the merit factor of binary arrays [**BA93**]; the peak sidelobe level of binary arrays [**AS89**], [**SL05**]; and sets of more than two sequences whose autocorrelations sum to zero [**Gol51**], [**Pat00**], [**Sch07**].

The aperiodic autocorrelation function arises naturally in many physical settings, and so is more practically useful than its periodic counterpart. At the same time, the aperiodic autocorrelation function is often thought to possess little intrinsic structure. I believe there is much evidence to the contrary, both classical and modern, including:

- Theorem 5.1 on the asymptotic behaviour of the peak sidelobe level of almost all binary sequences.
- Theorems 6.1, 6.2 and 6.3 on the integer-valued asymptotic merit factor of Rudin-Shapiro sequences, the optimal cyclic shift of Legendre sequences, and m-sequences, and similar results on generalisations of these families.
- Theorem 8.5, whose proof links Golay sequence pairs of length 2^m to Reed-Muller codes.
- The three-stage construction process for Golay sequence and array pairs described in Section 8, showing that some operations that appear to behave differently on Golay sequences can be viewed as the same operation on a Golay array but followed by different projections.

Note added in proof

Litsyn and Shpunt have recently proved the conclusion of Experimental Result 5.2:

THEOREM 9.1 ([**LS08**]). *The PSL of almost all binary sequences of length s grows like $\Theta(\sqrt{s \log s})$, and the growth constant lies in the interval $[1, \sqrt{2}]$.*

Acknowledgements

I am grateful to R. Turyn for generously providing many insights into the early history of the subject, and to Kai-Uwe Schmidt for pointing out the reference [**WHD77**]. P. Borwein and R. Ferguson kindly supplied the data corresponding to Figure 5 of [**BFK07**], which are displayed in Figure 3 of this paper.

References

[AB90] M. Antweiler and L. Bömer, *Merit factor of Chu and Frank sequences*, Electron. Lett. **26** (1990), 2068–2070.

[AS89] S. Alquaddoomi and R.A. Scholtz, *On the nonexistence of Barker arrays and related matters*, IEEE Trans. Inform. Theory **35** (1989), 1048–1057.

[BA93] L. Bömer and M. Antweiler, *Optimizing the aperiodic merit factor of binary arrays*, Signal Processing **30** (1993), 1–13.

[Bar53] R.H. Barker, *Group synchronizing of binary digital systems*, Communication Theory (W. Jackson, ed.), Academic Press, New York, 1953, pp. 273–287.

[BC01] P. Borwein and K.-K.S. Choi, *Merit factors of polynomials formed by Jacobi symbols*, Canad. J. Math. **53** (2001), 33–50.

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

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

[Ber87] J. Bernasconi, *Low autocorrelation binary sequences: statistical mechanics and configuration state analysis*, J. Physique **48** (1987), 559–567.

[BF03] P.B. Borwein and R.A. Ferguson, *A complete description of Golay pairs for lengths up to 100*, Mathematics of Computation **73** (2003), 967–985.

[BF05] P. Borwein and R. Ferguson, *Polyphase sequences with low autocorrelation*, IEEE Trans. Inform. Theory **51** (2005), 1564–1567.

[BF07] ———, *Barker sequences*, June 2007, poster presented at CMS-MITACS Joint Conference 2007, Winnipeg, MB.

[BFK07] P. Borwein, R. Ferguson, and J. Knauer, *The merit factor problem*, preprint.

[BJL99] T. Beth, D. Jungnickel, and H. Lenz, *Design theory*, 2nd ed., Cambridge University Press, Cambridge, 1999, Volumes I and II.

[BM00] P. Borwein and M. Mossinghoff, *Rudin-Shapiro-like polynomials in L_4*, Math. of Computation **69** (2000), 1157–1166.

[Boe67] A.M. Boehmer, *Binary pulse compression codes*, IEEE Trans. Inform. Theory **IT-13** (1967), 156–167.

[Bor02] P. Borwein, *Computational excursions in analysis and number theory*, CMS Books in Mathematics, Springer-Verlag, New York, 2002.

[Bud90] S.Z. Budišin, *New complementary pairs of sequences*, Electron. Lett. **26** (1990), 881–883.

[CFB90] M.N. Cohen, M.R. Fox, and J.M. Baden, *Minimum peak sidelobe pulse compression codes*, IEEE International Radar Conference, IEEE, 1990, pp. 633–638.

[CG94] N. Chang and S.W. Golomb, *On n-phase Barker sequences*, IEEE Trans. Inform. Theory **40** (1994), 1251–1253.

[CG96] ———, 7200-*phase generalized Barker sequences*, IEEE Trans. Inform. Theory **42** (1996), 1236–1238.

[CHK02] R. Craigen, W. Holzmann, and H. Kharaghani, *Complex Golay sequences: structure and applications*, Discrete Math. **252** (2002), 73–89.

[CK01] R. Craigen and C. Koukouvinos, *A theory of ternary complementary pairs*, J. Combin. Theory (Series A) **96** (2001), 358–375.

[CR05] G.E. Coxson and J. Russo, *Efficient exhaustive search for optimal-peak-sidelobe binary codes*, IEEE Trans. Aerospace and Electron. Systems **41** (2005), 302–308.

[CVT03] C.V. Chong, R. Venkataramani, and V. Tarokh, *A new construction of 16-QAM Golay complementary sequences*, IEEE Trans. Inform. Theory **49** (2003), 2953–2959.

[DJ99] 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** (1999), 2397–2417.

[DJ07] D. Dmitriev and J. Jedwab, *Bounds on the growth rate of the peak sidelobe level of binary sequences*, Advances in Mathematics of Communications **1** (2007), 461–475.

[DJS07] J.A. Davis, J. Jedwab, and K.W. Smith, *Proof of the Barker array conjecture*, Proc. Amer. Math. Soc. **135** (2007), 2011–2018.

[Dym92] M. Dymond, *Barker arrays: existence, generalization and alternatives*, Ph.D. thesis, University of London, 1992.

[EBSB97] H. Elders-Boll, H. Schotten, and A. Busboom, *A comparative study of optimization methods for the synthesis of binary sequences with good correlation properties*, 5th IEEE Symposium on Communication and Vehicular Technology in the Benelux, IEEE, 1997, pp. 24–31.

[EDKK02] L. Ein-Dor, I. Kanter, and W. Kinzel, *Low autocorrelated multiphase sequences*, Physical Review E **65** (2002), 020102.

[EK92] S. Eliahou and M. Kervaire, *Barker sequences and difference sets*, L'Enseign. Math. **38** (1992), 345–382.

[EKS90] S. Eliahou, M. Kervaire, and B. Saffari, *A new restriction on the lengths of Golay complementary sequences*, J. Combin. Theory (A) **55** (1990), 49–59.

[EKS91] S. Eliahou, M. Kervaire, and B. Saffari, *On Golay polynomial pairs*, Advances App. Math. **12** (1991), 235–292.

[FJ06] F. Fiedler and J. Jedwab, *How do more Golay sequences arise?*, IEEE Trans. Inform. Theory **52** (2006), 4261–4266.

[FJP08] F. Fiedler, J. Jedwab, and M.G. Parker, *A multi-dimensional approach to the construction and enumeration of Golay complementary sequences*, J. Combin. Theory (A) (2008), to appear.

[Fri96] M. Friese, *Polyphase Barker sequences up to length 36*, IEEE Trans. Inform. Theory **42** (1996), 1248–1250.

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

[GL94] A. Gavish and A. Lempel, *On ternary complementary sequences*, IEEE Trans. Inform. Theory. **40** (1994), 522–526.

[Gol51] M.J.E. Golay, *Static multislit spectrometry and its application to the panoramic display of infrared spectra*, J. Opt. Soc. Amer. **41** (1951), 468–472.

[Gol61] ———, *Complementary series*, IRE Trans. Inform. Theory **IT-7** (1961), 82–87.

[Gol62] ———, *Note on "Complementary series"*, Proc. IRE **50** (1962), 84.

[Gol72] ———, *A class of finite binary sequences with alternate autocorrelation values equal to zero*, IEEE Trans. Inform. Theory **IT-18** (1972), 449–450.

[Gol82] ———, *The merit factor of long low autocorrelation binary sequences*, IEEE Trans. Inform. Theory **IT-28** (1982), 543–549.

[Gol83] ———, *The merit factor of Legendre sequences*, IEEE Trans. Inform. Theory **IT-29** (1983), 934–936.

[GS65] S.W. Golomb and R.A. Scholtz, *Generalized Barker sequences*, IEEE Trans. Inform. Theory **IT-11** (1965), 533–537.

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

[HJJ85] 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** (1985), 549–552.

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

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

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

[JL92] J. Jedwab and S. Lloyd, *A note on the nonexistence of Barker sequences*, Designs, Codes and Cryptography **2** (1992), 93–97.

[JP07a] J. Jedwab and M.G. Parker, *Golay complementary array pairs*, Designs, Codes and Cryptography **44** (2007), 209–216.

[JP07b] ———, *There are no Barker arrays having more than two dimensions*, Designs, Codes and Cryptography **43** (2007), 79–84.

[JY06] J. Jedwab and K. Yoshida, *The peak sidelobe level of families of binary sequences*, IEEE Trans. Inform. Theory **52** (2006), 2247–2254.

[KMB86] A.M. Kerdock, R. Mayer, and D. Bass, *Longest binary pulse compression codes with given peak sidelobe levels*, Proceedings of the IEEE **74** (1986), 366.

[KN99] 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.

[LC05] Y. Li and W.B. Chu, *More Golay sequences*, IEEE Trans. Inform. Theory **51** (2005), 1141–1145.

[Lit66] 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** (1966), 367–376.

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

[LS05] K.H. Leung and B. Schmidt, *The field descent method*, Designs, Codes and Cryptography **36** (2005), 171–188.

[LS08] S. Litsyn and A. Shpunt, *Typical peak sidelobe level of binary sequences*, preprint.

[Lun65] L. Lunelli, *Tabelli di sequenze* $(+1, -1)$ *con autocorrelazione troncata non maggiore di* 2, Politecnico di Milano, 1965.

[MB07] S. Mertens and H. Bauke, *Ground States of the Bernasconi Model with Open Boundary Conditions*, online. Available: `<http://www-e.uni-magdeburg.de/mertens/research/labs/open.dat>`, October 2007.

[McE80] R.J. McEliece, *Correlation properties of sets of sequences derived from irreducible cyclic codes*, Inform. Contr. **45** (1980), 18–25.

[MM68] J.W. Moon and L. Moser, *On the correlation function of random binary sequences*, SIAM J. Appl. Math. **16** (1968), 340–343.

[Mow93] W.H. Mow, *Enumeration techniques for best* N*-phase codes*, Electron. Lett. **29** (1993), 907–908.

[Mow96] ———, *General limit theorem for* n *phase Barker sequences*, Electron. Lett. **32** (1996), 1364–1365.

[MZB98] B. Militzer, M. Zamparelli, and D. Beule, *Evolutionary search for low autocorrelated binary sequences*, IEEE Trans. Evol. Comput. **2** (1998), 34–39.

[NB90] D.J. Newman and J.S. Byrnes, *The* L^4 *norm of a polynomial with coefficients* ±1, Amer. Math. Monthly **97** (1990), 42–45.

[NC08a] C. Nunn and G.E. Coxson, *Best-known autocorrelation peak sidelobe levels for binary codes of length* 71 *to* 105, IEEE Trans. Aerospace and Electron. Systems (2008), to appear.

[NC08b] ———, *Polyphase pulse compression codes with optimal peak and integrated sidelobes*, preprint.

[NNG$^+$89] M. Nazarathy, S.A. Newton, R.P. Giffard, D.S. Moberly, F. Sischka, W.R. Trutna, Jr., and S. Foster, *Real-time long range complementary correlation optical time domain reflectometer*, IEEE J. Lightwave Technology **7** (1989), 24–38.

[NSL$^+$03] A. Nowicki, W. Secomski, J. Litniewski, I. Trots, and P.A. Lewin, *On the application of signal compression using Golay's codes sequences in ultrasonic diagnostic*, Arch. Acoustics **28** (2003), 313–324.

[Nun05] C. Nunn, *Constrained optimization applied to pulse compression codes, and filters*, IEEE International Radar Conference, IEEE, 2005, pp. 190–194.

[OHT78] N. Ohyama, T. Honda, and J. Tsujiuchi, *An advanced coded imaging without side lobes*, Optics Comm. **27** (1978), 339–344.

[Pat00] K.G. Paterson, *Generalized Reed-Muller codes and power control in OFDM modulation*, IEEE Trans. Inform. Theory **46** (2000), 104–120.

[Rud59] W. Rudin, *Some theorems on Fourier coefficients*, Proc. Amer. Math. Soc. **10** (1959), 855–859.

[SA74] U. Somaini and M.H. Ackroyd, *Uniform complex codes with low autocorrelation sidelobes*, IEEE Trans. Inform. Theory **20** (1974), 689–691.

[Sar84] D.V. Sarwate, *An upper bound on the aperiodic autocorrelation function for a maximal-length sequence*, IEEE Trans. Inform. Theory **IT-30** (1984), 685–687.

[Sch99] B. Schmidt, *Cyclotomic integers and finite geometry*, J. Am. Math. Soc. **12** (1999), 929–952.

[Sch02] ———, *Characters and cyclotomic fields in finite geometry*, Lecture Notes in Mathematics, vol. 1797, Springer, Berlin, 2002.

[Sch07] K.-U. Schmidt, *Complementary sets, generalized Reed-Muller codes, and power control for OFDM*, IEEE Trans. Inform. Theory **53** (2007), 808–814.

[Sha51] H.S. Shapiro, *Extremal problems for polynomials and power series*, Master's thesis, Mass. Inst. of Technology, 1951.

[SL05] H.D. Schotten and H.D. Lüke, *On the search for low correlated binary sequences*, AEU — Int. J. of Electronics and Communications **59** (2005), 67–78.

[SLX07] P. Stoica, J. Li, and M. Xue, *On sequences with good correlation properties: a new perspective*, 2007 IEEE Information Theory Workshop on Information Theory for Wireless Networks (T. Helleseth et al., eds.), IEEE, 2007.

[Tie99] A. Tietäväinen, *Vinogradov's method and some applications*, Number Theory and its Applications (C.Y. Yildirim and S.A. Stepanov, eds.), Lecture Notes in Pure and Applied Mathematics, vol. 204, Marcel Dekker, New York, 1999, pp. 261–282.

[TS61] R. Turyn and J. Storer, *On binary sequences*, Proc. Amer. Math. Soc. **12** (1961), 394–399.

[Tur60] R. Turyn, *Optimum codes study*, Final Report. Contract AF19(604)-5473, Sylvania Electronic Systems, 29 January 1960.

[Tur65] R.J. Turyn, *Character sums and difference sets*, Pacific J. Math. **15** (1965), 319–346.

[Tur67] R. Turyn, *The correlation function of a sequence of roots of 1*, IEEE Trans. Inform. Theory **IT-13** (1967), 524–525.

[Tur68] R.J. Turyn, *Sequences with small correlation*, Error Correcting Codes (H.B. Mann, ed.), Wiley, New York, 1968, pp. 195–228.

[Tur74a] ———, *Four-phase Barker codes*, IEEE Trans. Inform. Theory **IT-20** (1974), 366–371.

[Tur74b] ———, *Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings*, J. Combin. Theory (A) **16** (1974), 313–333.

[Wel60] G.R. Welti, *Quaternary codes for pulsed radar*, IRE Trans. Inf. Theory **IT-6** (1960), 400–408.

[WHD77] D.J. White, J.N. Hunt, and L.A.G. Dresel, *Uniform Huffman sequences do not exist*, Bull. London Math. Soc. **9** (1977), 193–198.

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

[YG07] N.Y. Yu and G. Gong, *The perfect binary sequence of period* 4 *for low periodic and aperiodic autocorrelations*, Sequences, Subsequences, and Consequences (S.W. Golomb et al., eds.), Lecture Notes in Computer Science, vol. 4893, Springer-Verlag, Berlin, 2007, pp. 37–49.

[ZG93] N. Zhang and S.W. Golomb, *Polyphase sequences with low autocorrelation*, IEEE Trans. Inform. Theory **39** (1993), 1085–1089.

Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC, Canada V5A 1S6

E-mail address: jed@sfu.ca