SEQUENCES WITH LOW CORRELATION

DANIEL J. KATZ

Abstract. Pseudorandom sequences are used extensively in communications and remote sensing. Correlation provides one measure of pseudorandomness, and low correlation is an important factor determining the performance of digital sequences in applications. We consider the problem of constructing pairs (f, g) of sequences such that both f and g have low mean square autocorrelation and f and g have low mean square mutual crosscorrelation. We focus on aperiodic correlation of binary sequences, and review recent contributions along with some historical context.

1. Introduction

Sequences with low correlation play many roles in technology, including remote sensing, design of scientific instruments, operation of communications networks, and acoustic design. The monographs of Golomb, Gong, and Schroeder [14, 15, 41] give some sense of the broad sweep of their applications. Golomb [14, p. 25] used correlation as a measure of pseudorandomness, a concept of significance for cryptography that has been developed extensively by Mauduit and Sárkozy in [34] and further works. Here we give an overview of recent progress on the problem of designing binary sequence pairs where both sequences have low aperiodic autocorrelation and the two sequences of the pair have low mutual aperiodic crosscorrelation.

This paper is organized as follows: Sections 2, 3, and 4 give the basic definitions (of sequences, correlation, and merit factors). Section 5 lists some constructions of sequence families with low mean square autocorrelation. Sections 6, 7, and 8 describe how the constructions are done, and provide more details about autocorrelation performance. Section 9 examines the question of low mean square crosscorrelation, and Section 10 discusses a combined measure (called the Pursley-Sarwate criterion) of autocorrelation and crosscorrelation performance of a sequence pair. Section 11 discusses families of sequence pairs with low Pursley-Sarwate criterion, and Section 12 concludes with open questions.

Date: 12 June 2018.

Key words and phrases. crosscorrelation, autocorrelation, aperiodic, merit factor, sequence.

This paper is based on work supported in part by the National Science Foundation under Grant DMS 1500856.

2. Sequences

If ℓ and m are positive integers, an *additive m-ary sequence of length ℓ* is an ℓ-tuple of elements of the additive group of $\mathbb{Z}/m\mathbb{Z}$, that is,

$$a = (a_0, a_1, \ldots, a_{\ell-1}) \in (\mathbb{Z}/m\mathbb{Z})^\ell. \tag{1}$$

When $m = 2$ we have an *additive binary sequence*, that is, an element of $\mathbb{F}_2^\ell$.

A *multiplicative m-ary sequence of length ℓ* is an ℓ-tuple of mth roots of unity in $\mathbb{C}$, that is,

$$b = (b_0, b_1, \ldots, b_{\ell-1}) \in \mu_m^\ell, \tag{2}$$

where $\mu_m = \{e^{2\pi i j/m} : 0 \leq j < m\}$ is the multiplicative group of mth roots of unity in $\mathbb{C}$. Most often we have $m = 2$, so $\mu_2 = \{1, -1\}$; this gives *multiplicative binary sequences*, which we shall just call *binary sequences.*

Consider the group homomorphism $\varepsilon \colon \mathbb{Z}/m\mathbb{Z} \to \mu_m$ with $\varepsilon(x) = e^{2\pi i x/m}$. If the sequences a and b of (1) and (2) are related by $b_k = \varphi(a_k)$ for every k, then we say that *b is the multiplicative version of a*, and equivalently, that *a is the additive version of b.*

For the purposes of this paper, it will be more convenient to consider sequences in their multiplicative guise. Furthermore, we shall identify the sequence $f = (f_0, \ldots, f_{\ell-1}) \in \mathbb{C}^\ell$ in multiplicative form with the polynomial $f(z) = f_0 + f_1 z + \cdots + f_{\ell-1} z^{\ell-1} \in \mathbb{C}[z]$, whose coefficients are the terms of the sequence f. This identification makes calculations easier and we shall see in Section 4 that it forms a bridge between the study of correlation and harmonic analysis that has proved fruitful in these studies.

3. Correlation

Correlation is a measure of the similarity between the various shifted versions of a pair of sequences. When the sequences of the pair are the same, we are comparing a sequence to shifted versions of itself, which is self-correlation, or autocorrelation. Truly random sequences should have low correlation with shifted versions of themselves (unless the shift is zero) and of each other, so we demand that our pseudorandom sequences also have low correlation.

Let us now define correlation precisely. For two sequences

$$\begin{aligned} f &= (f_0, f_1, \ldots, f_{\ell-1}) \in \mathbb{C}^\ell \\ g &= (g_0, g_1, \ldots, g_{\ell-1}) \in \mathbb{C}^\ell, \end{aligned} \tag{3}$$

and $s \in \mathbb{Z}$, the *aperiodic crosscorrelation of f with g at shift s*, denoted $C_{f,g}(s)$, is defined by

$$C_{f,g}(s) = \sum_{j \in \mathbb{Z}} f_{j+s} \overline{g_j},$$

where we use the convention that $f_j = g_j = 0$ when $j \notin \{0, 1, \ldots, \ell - 1\}$, so that the above sum only has a finite number of nonzero entries. We index over $\mathbb{Z}$ because the underlying translation operation involved in aperiodic crosscorrelation is a non-cyclic shift. We can view the aperiodic correlation of f with g at shift s as the inner product between the overlapping portions of f and g when g is shifted s places to the right relative to f, as shown in Figure 1.

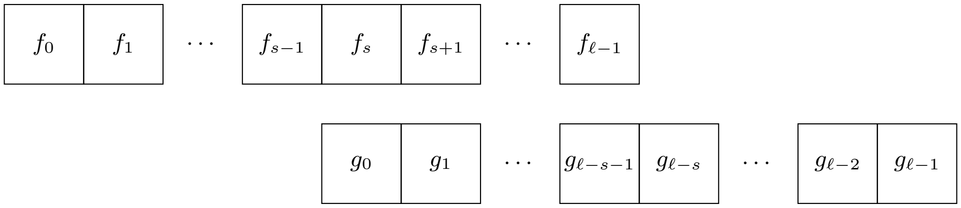

FIGURE 1. Aperiodic correlation of f with g at shift $s > 0$

Let us identify f and g of (3) with the polynomials $f(z) = f_0 + f_1 z + \cdots + f_{\ell-1} z^{\ell-1}$ and $g(z) = g_0 + g_1 z + \cdots + g_{\ell-1} z^{\ell-1}$, respectively, as discussed at the end of Section 2. Furthermore, let us adopt the convention that for any Laurent polynomial

$$a(z) = \sum_{j \in \mathbb{Z}} a_j z^j,$$

in the ring $\mathbb{C}[z, z^{-1}]$ of Laurent polynomials over $\mathbb{C}$, the *conjugate of* $a(z)$ is defined to be

$$\overline{a(z)} = \sum_{j \in \mathbb{Z}} \overline{a_j} z^{-j}, \tag{4}$$

where $\overline{a_j}$ is the usual complex conjugate of a_j. Then it is not difficult to show that

$$f(z)\overline{g(z)} = \sum_{s \in \mathbb{Z}} C_{f,g}(s) z^s,$$

that is, the crosscorrelation of f with g at shift s is the coefficient of z^s in the product $f(z)\overline{g(z)}$. This interpretation allows us to discover quite easily the following basic symmetry of aperiodic correlation:

$$C_{f,g}(s) = \overline{C_{g,f}(-s)}. \tag{5}$$

There is also a periodic version of correlation that treats our sequences (3) as periodically repeating every ℓ terms. In this case, $\mathbb{Z}/\ell\mathbb{Z}$ is the natural set for indexing sequence terms and expressing shifts, reflecting the cyclic nature of the sequences and the shifting. Then for any $s \in \mathbb{Z}/\ell\mathbb{Z}$, the *periodic crosscorrelation of* f *with* g *at shift* s, denoted $\mathrm{PC}_{f,g}(s)$, is defined by

$$\mathrm{PC}_{f,g}(s) = \sum_{j \in \mathbb{Z}/\ell\mathbb{Z}} f_{j+s} \overline{g_j}.$$

We can view the periodic correlation of f with g at shift s as the inner product of f with g when g is cyclically shifted s places to the right relative to f, as shown in Figure 2.

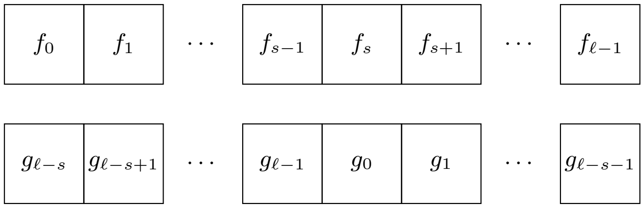

FIGURE 2. Periodic correlation of f with g at shift s

If $s \in \mathbb{Z}$, then we interpret $\mathrm{PC}_{f,g}(s)$ as $\mathrm{PC}_{f,g}(\sigma)$ where $\sigma \in \mathbb{Z}/\ell\mathbb{Z}$ is the congruence class of s modulo ℓ. In this case one can see that for any $s \in \mathbb{Z}$, we have

$$\mathrm{PC}_{f,g}(s) = \sum_{\substack{t \in \mathbb{Z} \\ t \equiv s \pmod{\ell}}} C_{f,g}(t),$$

where at most two of these terms can be nonzero, and in particular, if $0 \leq s < \ell$, then

$$\mathrm{PC}_{f,g}(s) = C_{f,g}(s) + C_{f,g}(s-\ell). \tag{6}$$

One can obtain a polynomial interpretation of periodic crosscorrelation by regarding our sequences as lying in the ring $\mathbb{C}[z]/(z^\ell - 1)$ rather than $\mathbb{C}[z]$. The notion of a conjugate of a Laurent polynomial from (4) carries over naturally to $\mathbb{C}[z]/(z^\ell - 1)$: negative powers of z can be reinterpreted as positive powers since $z^\ell = 1$ in this ring, and the ideal $(z^\ell - 1)$ is closed under our conjugation since $\overline{z^\ell - 1} = -z^{-\ell}(z^\ell - 1)$. Then one can show that

$$f(z)\overline{g(z)} \equiv \sum_{s \in \mathbb{Z}/\ell\mathbb{Z}} \mathrm{PC}_{f,g}(s) z^s \pmod{z^\ell - 1},$$

and from this prove the symmetry

$$\mathrm{PC}_{f,g}(s) = \overline{\mathrm{PC}_{g,f}(-s)}.$$

Periodic correlation is more mathematically tractable than aperiodic correlation. For example, when we consider sequences derived from finite field characters (see Sections 6 and 7), the periodic correlation values are complete character sums, while the aperiodic correlation values are incomplete character sums, which are much more difficult to handle. Equation (6) shows that the magnitude of any periodic correlation cannot be more than twice as large as the largest magnitude of any aperiodic correlation value. In consequence of this, Boehmer [1, p. 157] points out that having low periodic correlation at all shifts is a necessary but not sufficient condition for having low aperiodic correlation at all shifts. She then enunciates a design technique that has been used widely in attempts to design sequences with low aperiodic correlation: design sequences with low periodic correlation and hope that some of these will also have low aperiodic correlation.

Earlier we had mentioned autocorrelation, or correlation of a sequence with itself. If f is the sequence in (3) and $s \in \mathbb{Z}$, then the *aperiodic autocorrelation of f at shift s* is just the aperiodic crosscorrelation of f with itself at shift s, that is,

$$C_{f,f}(s) = \sum_{j \in \mathbb{Z}} f_{j+s}\overline{f_j}.$$

And for $s \in \mathbb{Z}/\ell\mathbb{Z}$, the *periodic autocorrelation of f at shift s* is just the periodic crosscorrelation of f with itself at shift s, that is,

$$\mathrm{PC}_{f,f}(s) = \sum_{j \in \mathbb{Z}/\ell\mathbb{Z}} f_{j+s}\overline{f_j}.$$

Note that if the shift is zero in either the aperiodic or periodic case, then

$$C_{f,f}(0) = \mathrm{PC}_{f,f}(0) = \sum_{j=0}^{\ell-1} |f_j|^2, \tag{7}$$

which is the squared Euclidean norm of f if it is regarded as a vector in $\mathbb{C}^\ell$. If all the terms of f are of unit magnitude, we say that f is a *unimodular sequence.* For example, all m-ary sequences are unimodular, since their terms are roots of unity. If f is unimodular, then

$$C_{f,f}(0) = \mathrm{PC}_{f,f}(0) = \ell,$$

which is the length of the sequence, and is naturally as large as a correlation value involving unimodular sequences of length ℓ could possibly be. On the other hand, what we know about random walks suggests that typical correlation values for randomly selected binary sequences of length ℓ (with uniform probability distribution) should not have magnitudes much larger than $\sqrt{\ell}$.

4. Demerit factors and merit factors

In a multi-user communications network, one can modulate the messages of the various users with different signature sequences. For efficient operation, it is desirable that the family of signature sequences used should have the following properties:

(i) Each sequence f should have low magnitude autocorrelation $|C_{f,f}(s)|$ at all nonzero shifts (all $s \neq 0$).

(ii) Each pair (f, g) of sequences should have low magnitude crosscorrelation $|C_{f,g}(s)|$ at all shifts s.

Notice that it is the magnitude of the correlation value that is typically considered, since often the argument is not discernible in our systems. In view of our comments on random sequences at the conclusion of the previous section, a typical correlation value can be considered small if it does not have magnitude much larger than the square root of the length of the sequences involved. Condition (i) helps the communications system maintain synchronization with the user represented by sequence f: the sharp difference between correlation of at shift 0 (when the sequence is aligned with a reference copy of itself) and at nonzero shifts (when it is not aligned) allows one to obtain very accurate timings. Condition (ii) prevents the output from the user represented by sequence f from being confused with any output from the user represented by sequence g, regardless of any delays between these two signals.

In this paper, we consider the simplest possible case of this design problem for sequences with low autocorrelation and crosscorrelation, that is, we ask for pairs of sequences such that $|C_{f,f}(s)|$ and $|C_{g,g}(s)|$ are low for all $s \neq 0$ and $|C_{f,g}(s)|$ is low for all s. We could rate overall smallness of correlation in various ways. One method is to rate crosscorrelation performance for a sequence pair (f,g) by the worst case: the *peak crosscorrelation of f with g* is

$$\max_{s\in\mathbb{Z}} |C_{f,g}(s)|,$$

and we would want this to be small.

After studying this and some other common measures of smallness of crosscorrelation, Kärkkäinen [25, p. 149] expresses the view that one gets a better notion of likely performance from a mean square measure. Accordingly, for sequence pair (f,g), we define the *crosscorrelation demerit factor of f and g* as

$$\mathrm{CDF}(f,g) = \frac{\sum_{s\in\mathbb{Z}} |C_{f,g}(s)|^2}{|C_{f,f}(0)|\cdot|C_{g,g}(0)|},$$

which, in view of (7), is the sum of squared magnitudes of crosscorrelation values for the sequence pair we obtain from f and g if we scale each of them to have unit Euclidean magnitude. We should note that $\mathrm{CDF}(f,g) = \mathrm{CDF}(g,f)$ because of (5). Normally f and g are unimodular sequences of the same length ℓ, so the denominator of the CDF is simply ℓ^2. Since we want every term in the numerator to be as small as possible, a large CDF indicates poor performance. If one wants a measure that is larger for good sequence pairs, one defines the *crosscorrelation merit factor of f and g* to be

$$\mathrm{CMF}(f,g) = \frac{1}{\mathrm{CDF}(f,g)}.$$

We have analogous measures for autocorrelation. If f is a sequence, then the *autocorrelation demerit factor of f* is defined to be

$$\mathrm{ADF}(f) = \frac{\sum_{\substack{s\in\mathbb{Z}\\ s\neq 0}} |C_{f,f}(s)|^2}{|C_{f,f}(0)|^2} = \mathrm{CDF}(f,f) - 1, \tag{8}$$

where one should note that we omit the autocorrelation at shift 0 in the numerator. This is because $C_{f,f}(0)$ is always large, and we want it to be large, so that it should not be construed as contributing to the demerit factor. And the *autocorrelation merit factor of f* is just the reciprocal of the demerit factor,

$$\mathrm{AMF}(f) = \frac{1}{\mathrm{ADF}(f)}.$$

Naturally we want to make the autocorrelation demerit factor small, or equivalently, to make the autocorrelation merit factor large.

Recall from the end of Section 2 that we always identify the sequence $f = (f_0, \ldots, f_{\ell-1}) \in \mathbb{C}^\ell$ with the polynomial $f(z) = f_0 + f_1 z + \cdots + f_{\ell-1} z^{\ell-1} \in \mathbb{C}[z]$. We shall now see how this point of view relates to merit factors. For any real number $r \geq 1$ and any function f defined on the complex unit circle, we define the *L^r norm of f on the complex unit circle* to be

$$\|f\|_r = \left(\frac{1}{2\pi} \int_0^{2\pi} |f(e^{i\theta})|^r d\theta \right)^{1/r},$$

provided that this integral exists (as it certainly will when f is a Laurent polynomial).

Then one can show that the crosscorrelation demerit factor is

$$\mathrm{CDF}(f,g) = \frac{\|fg\|_2^2}{\|f\|_2^2 \|g\|_2^2}$$

and the autocorrelation demerit factor is

$$\mathrm{ADF}(f) = \frac{\|f\|_4^4}{\|f\|_2^4} - 1 \tag{9}$$

This links the work of Littlewood (see [32] and [33, Problem 19]) on flatness of polynomials on the complex unit circle with the work of Golay [8, 9] on merit factors.

Sarwate [38, eqs. (13),(38)] calculated expected values of demerit factors for randomly selected binary sequences (where each term is independent of the others and has equal probability of being $+1$ or -1). For a randomly selected sequence f of length ℓ, Sarwate calculated the expected value of the autocorrelation demerit factor to be

$$E[\mathrm{ADF}(f)] = 1 - \frac{1}{\ell}. \tag{10}$$

For a randomly selected pair (f,g) of sequences of length ℓ, Sarwate calculated the expected value of the crosscorrelation demerit factor to be

$$E[\mathrm{CDF}(f,g)] = 1. \tag{11}$$

So typical values of both autocorrelation and crosscorrelation demerit factors will be about 1 when the length ℓ is large, as it quite often is. For example, Gold sequences of length 1023 are used in the Global Positioning System (GPS), and code division multiple access communications (CMDA) protocols use even longer sequences. Thus we want constructions that produce families of low correlation sequence pairs of various lengths. Typically, our constructions produce families with unbounded lengths, and we rate a family by the *asymptotic demerit factors*, that is, the limit of the autocorrelation or crosscorrelation demerit factor as the length of the sequences tends to infinity. For sequences derived from finite field characters, it has been observed in many cases [27, 2] that the limiting behavior of families is approached quite rapidly, so that even sequences of quite modest length (of the order of a hundred or more) already have demerit factors close to the limiting values.

5. High asymptotic autocorrelation merit factor

In this section we shall discuss constructions that give infinite families of binary sequences with high asymptotic autocorrelation merit factor. Recall (10), which says that randomly selected binary sequences of length ℓ have an average autocorrelation demerit factor of $1-1/\ell$, which is close to 1 for large ℓ. It is possible to obtain families where the asymptotic demerit factor is considerably lower. It is relatively rare to find such families, and to the author's best knowledge, the first one that was discovered derives from the Rudin-Shapiro polynomials, which shall be discussed further in Section 8. It was Littlewood who originally proved a result tantamount to showing that this family of polynomials has asymptotic demerit factor 1/3 [33, pp. 27–28]. At the time, the concept of merit factor for correlation had not yet been defined: the formula for the autocorrelation merit factor would appear as a “factor” in a 1972 paper by Golay [8], who later called this the “merit factor” in another paper a few years later [9]. What Littlewood actually proved [33, p. 28] is a formula for the ratio of L^4 norm to L^2 norm of the Rudin-Shapiro polynomials, which via (9) is equivalent to finding the asymptotic autocorrelation demerit factor. The Rudin-Shapiro sequence family has one sequence f_n of length 2^n for each nonnegative integer n, and Littlewood's result shows that $\mathrm{ADF}(f_n) = (1-(-1/2)^n)/3$, which tends to 1/3 in the limit as n tends to infinity.

If we consider Littlewood's result as the first low asymptotic demerit factor record, then this record was broken by Høholdt and Jensen [17] with cyclically shifted Legendre sequences, and that record was again broken by Jedwab, Katz, and Schmidt [20, Theorem 1.1] with Legendre sequences that are cyclically shifted and appended (periodically extended). The Legendre sequences and their modifications shall be discussed in more detail in Section 7. We summarize these records in Table 1, which in addition to listing the asymptotic demerit factor also lists its reciprocal, the asymptotic merit factor, which is the way these results are usually presented in the literature. The asymptotic demerit factor of $0.157\ldots$ listed for the shifted and appended Legendre sequences is the smallest real root of the polynomial $27x^3-417x^2+249x-29$. It should also be noted that, in addition to the records on Table 1, an important advance was the determination by Jensen and Høholdt [23, §5] of the asymptotic merit factor of a class of sequences known as maximal linear recursive sequences (m-sequences). These sequences shall be described in the next section, but they are of great

Table 1. Records for high asymptotic autocorrelation merit factor

	Asymptotic		
Sequence family	AMF	ADF	Proved by
Rudin-Shapiro	3	0.333 . . .	Littlewood (1968) [33, pp. 28]
Legendre, shifted	6	0.166 . . .	Høholdt-Jensen (1988) [17]
Legendre, shifted and appended	6.342 . . .	0.157 . . .	Jedwab-Katz-Schmidt (2013) [20, Theorem 1.1]

interest because it is easy to generate large families of them for use in communications networks. Jensen and Høholdt showed that any infinite family of m-sequences has asymptotic autocorrelation demerit factor 1/3, which equals the performance of the Rudin-Shapiro polynomials.

6. Sequences from additive characters

In this section, we shall discuss sequences derived from additive characters of finite fields, of which the most fundamental are the *maximum length linear recursive shift register sequences*, which are also called *maximal linear recursive sequences*, or just *m-sequences*. Let $\mathbb{F}_q$ be a finite field of characteristic p and order $q = p^n$. An *additive character* is a homomorphism from the additive group $\mathbb{F}_q$ to the multiplicative group $\mathbb{C}^*$. We use $\operatorname{Tr}\colon \mathbb{F}_q \to \mathbb{F}_p$ to denote the absolute trace from $\mathbb{F}_q$ to its prime field $\mathbb{F}_p$. Then for each $a \in \mathbb{F}_q$, the map $\varepsilon_a\colon \mathbb{F}_q \to \mathbb{C}^*$ with $\varepsilon_a(x) = \exp(2\pi i \operatorname{Tr}(ax)/p)$ is an additive character of $\mathbb{F}_q$, and $\{\varepsilon_a : a \in \mathbb{F}_q\}$ is the entire group of q additive characters from $\mathbb{F}_q$ into $\mathbb{C}^*$, with ε_0 being the trivial character (that maps every element of $\mathbb{F}_q$ to 1), while ε_1 is called the *canonical additive character*.

Let α be a primitive element of $\mathbb{F}_q$. Let us list the nonzero elements of $\mathbb{F}_q$ as powers of the primitive element α, that is, as

$$\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{q-2},$$

and then apply a nontrivial additive character ψ to obtain a sequence

$$\left(\psi(\alpha^0), \psi(\alpha^1), \ldots, \psi(\alpha^{q-2})\right). \tag{12}$$

An *m-sequence* is any sequence obtained in this way. Any nontrivial additive character of a finite field of characteristic p has the complex pth roots of unity as its outputs, so the m-sequences produced from fields of characteristic p are p-ary sequences. We shall mainly be interested in binary m-sequences, which derive from fields of characteristic 2.

Changing the nontrivial character ψ in (12) simply causes a cyclic shift of the m-sequence, and each of the $q-1$ nontrivial additive characters of $\mathbb{F}_q$ produces a different cyclic shift, and the $q-1$ different cyclically shifted versions of our m-sequence are all distinct. If the character ψ we use is the canonical additive character, we call the m-sequence produced in (12) a *Galois sequence* or a *naturally shifted m-sequence*.

Changing the primitive element α in (12) to another primitive element $\beta = \alpha^d$ (where $\gcd(d, q-1) = 1$ to maintain primitivity) causes the m-sequence (12) to be decimated by d, that is, the new m-sequence based on β is what one obtains by selecting every dth element from the original sequence (starting at the beginning and proceeding cyclically modulo the length $q-1$). If β is a Galois conjugate of α over the prime field $\mathbb{F}_p$, that is, if d is a power of p modulo $q-1$, then one just gets back the original sequence (up to some cyclic shift); otherwise one gets a sequence that is distinct from every cyclic shift of the original sequence. Thus decimations d that are a power of p modulo $q-1$ are said to be *degenerate*. When the original sequence is a Galois sequence, decimation by a degenerate d yields back the original sequence exactly (not even cyclically shifted). Another type of decimation that will become useful later in Section 11 is a *reversing decimation*, which is any decimation d for which there is an integer k such that $d \equiv -p^k \pmod{q-1}$. If we decimate an m-sequence by such a d, one obtains the reverse of the original sequence (up to a cyclic shift).

We can now count the total number of m-sequences, based on our freedom to choose the character (cyclic shifting) and the primitive element modulo Galois conjugacy (decimation). If we organize m-sequences of length $p^n - 1$ into classes of sequences modulo cyclic shifting (with $p^n - 1$ sequences per class), the number of classes of m-sequences will be equal to the number of classes of primitive elements of $\mathbb{F}_q = \mathbb{F}_{p^n}$ modulo Galois conjugacy (with n Galois conjugates per class). Since the number of primitive elements in $\mathbb{F}_q = \mathbb{F}_{p^n}$ is $\varphi(p^n - 1)$, where φ is Euler's φ-function, the total number of m-sequences of length p^n is $(p^n - 1)\varphi(p^n - 1)/n$. If α is a primitive element of our field $\mathbb{F}_q$, then α^{-1} will also be a primitive element and will not be a Galois conjugate of α unless $q \leq 4$ (in which case all primitive elements in $\mathbb{F}_q$ are Galois conjugates of each other). So $\varphi(p^n - 1)/n > 1$ whenever $p^n > 4$, in which case it is possible to obtain at least two cyclically distinct m-sequences (related by a nondegenerate decimation) of length $p^n - 1$.

Our p-ary m-sequence (12) of length $p^n - 1$ follows a linear recursion of depth n whose characteristic polynomial is the minimal polynomial of the primitive element α over the prime field $\mathbb{F}_p$. Because of this, our m-sequence of length $p^n - 1$ can be generated using a linear feedback shift register of length n. This efficient generation of very long sequences with rather small circuits makes m-sequences very popular in applications. Furthermore, from two m-sequences of length $p^n - 1$ related by a nondegenerate decimation d, one can construct a family of $p^n + 1$ Gold sequences of length $p^n - 1$. Gold's original construction [13, §IV] uses carefully chosen decimations d to produce families where all the sequences have low periodic autocorrelation and all the pairs have low periodic crosscorrelation.

We now give an overview of findings on the asymptotic aperiodic autocorrelation merit factor of binary m-sequences and their relatives. As mentioned in the previous section, Jensen and Høholdt [23, §5] proved that m-sequences have asymptotic autocorrelation demerit factor 1/3. Jedwab and Schmidt [21, Theorems 11 and 12] applied some constructions described by Parker [35, Lemmas 3 and 4] to m-sequences to produce families of related sequences that also have asymptotic autocorrelation demerit factor 1/3. Parker gave two constructions, each of which takes a sequence as an input and gives a longer sequence as an output. The first construction, called the *negaperiodic construction*, doubles the length of the sequence, so we shall call it *Parker's doubling construction*. The second construction, called the *periodic construction*, quadruples the length of the sequence, so we shall call it *Parker's quadrupling construction*.

Another technique that was used to modify m-sequences is *appending*, which originates with studies by Kirilusha and Narayanaswamy [31]. We let $f(z) = \sum_{j=0}^{\ell-1} f_j z^j$ be a sequence of length ℓ (represented in polynomial form), and extend the definition of f_j so that $f_{j+\ell} = f_j$ for all $j \in \mathbb{Z}$. Then we can truncate or periodically extend f simply by changing the range of summation. For example if $m < \ell$, then $g(z) = \sum_{j=0}^{m-1} f_j z^j$ is a truncated version of f, while if $m > \ell$, then it is an periodically extended version of f. In these respective cases, we say that this new sequence g is f *truncated to* m/ℓ *times its usual length* or f *appended to* m/ℓ *times its usual length*. Jedwab, Katz, and Schmidt [19, Theorem 2.2] proved that if one applies this procedure to m-sequences, one can produce families with an asymptotic autocorrelation demerit factor of $0.299\ldots$, which is the smallest real root of the polynomial $3x^3 - 33x^2 + 33x - 7$. To achieve this, one should use m-sequences appended to about $1.115\ldots$ times their usual length, where $1.115\ldots$ is the middle root of $x^3 - 12x + 12$. Jedwab, Katz, and Schmidt also combined the appending procedure with Parker's constructions to produce further families with asymptotic autocorrelation demerit factor $0.299\ldots$.

The concept of an m-sequence can be generalized to a produce a larger family of sequences called the *Gordon-Mills-Welch sequences* [40]. The construction of Gordon-Mills-Welch sequences differs from that of m-sequences in that the character ψ used in the m-sequence construction (12) is replaced with a "twisted" version. Günther and Schmidt [16, p. 344–345] have recently shown Gordon-Mills-Welch sequences attain the same asymptotic autocorrelation demerit factors that m-sequences do: 1/3 for natural length and $0.299\ldots$ if appended.

7. Sequences from multiplicative characters

Now we describe a sequence construction that is in some sense dual to the construction of m-sequences. The pseudorandom behavior of m-sequences can be traced to the fact that we form them by listing the nonzero elements of a finite field $\mathbb{F}_q$ in an order based on the *multiplicative structure* of the field (that is, as powers of a primitive element) and then apply an *additive character* to them (see (12) and the commentary preceding it). Our next construction is dual in the sense that we shall devise a listing of the elements of a finite field based on the *additive structure* of the field and then apply a *multiplicative character* to them.

To make a multiplicative character sequence, let us start with a finite field $\mathbb{F}_p$ of prime order p, and write its elements in an order based on the additive structure of the field. We can take 1 as our additive generator, and then the additive analogue of taking increasing powers of this element is to form sums of increasing numbers of 1, that is, we list the elements of $\mathbb{F}_p$ in the order

$$0, 1, 1+1=2, 1+1+1=3, \ldots, p-1. \tag{13}$$

Now let $\chi\colon \mathbb{F}_p \to \mathbb{C}^*$ be a multiplicative character, that is, a group homomorphism from $\mathbb{F}_p^*$ to $\mathbb{C}^*$, and make sure that χ is nontrivial, that is, does not map every element to 1. Normally one extends a multiplicative character χ by setting $\chi(0) = 0$. Then we apply our nontrivial multiplicative character χ to our list (13) of elements of $\mathbb{F}_p$ to obtain the sequence

$$(\chi(0), \chi(1), \chi(2), \ldots, \chi(p-1))\,.^1 \tag{14}$$

The multiplicative characters of $\mathbb{F}_p$ form a cyclic group of order $p-1$ under multiplication. If χ is a character whose order is m in this group, then all terms except $\chi(0) = 0$ are mth roots of unity. Normally, we replace the initial $\chi(0) = 0$ term with a complex number mth root of unity (typically one just uses 1) to get a true m-ary sequence.

If p is an odd prime, then the group of multiplicative characters of $\mathbb{F}_p$ always contains one and only one character of order 2, which is called the *quadratic character* or *Legendre symbol.* If we use this as our character χ in the construction above (and replace $\chi(0)$ with 1), then we obtain a binary sequence $h = (h_0, h_1, \ldots, h_{p-1})$, called a *Legendre sequence*, where

$$h_j = \begin{cases} +1 & \text{if } j \text{ is the square of some element in } \mathbb{F}_p, \\ -1 & \text{if } j \text{ is not the square of any element in } \mathbb{F}_p. \end{cases} \tag{15}$$

Since there is only one character of order 2 over each prime field $\mathbb{F}_p$ of odd order, this construction gives us only one binary sequence of length p for each odd prime p. Contrast this with the construction of m-sequences in Section 6, which often produces many sequences of the same length that are not related to each other by cyclic shifting.

One might ask why we only used prime fields in the construction of multiplicative character sequences, while we used arbitrary finite fields to construct m-sequences. The reason is that prime fields are the only finite fields that are cyclic groups under addition, so they are the only finite fields where

[1] This sequence was formed using the specific choice of 1 as the additive generator of $\mathbb{F}_p$. We could have replaced 1 with any other $a \in \mathbb{F}_p^*$ to form the list $0, a, 2a, \ldots, (p-1)a$ of elements of $\mathbb{F}_p$ instead of (13), and then apply χ to every term to get $(\chi(0), \chi(a), \chi(2a), \ldots, \chi((p-1)a))$. This would just give the sequence in (14) multiplied by the unimodular scalar $\chi(a)$. This scalar multiplciation has no effect on the magnitudes of correlation values.

one can generate a list of all the elements using a single additive generator. A finite field $\mathbb{F}_{p^n}$ of characteristic p and order p^n is an n-dimensional vector space over $\mathbb{F}_p$, so $\mathbb{F}_{p^n}$ can be generated by an $\mathbb{F}_p$-basis consisting of n elements. Using this n-dimensional description of $\mathbb{F}_{p^n}$, we can generalize our construction to create n-dimensional arrays whose entries are given by evaluations of multiplicative characters, and there are natural definitions of correlation for these arrays, with many results analogous to what we present about sequences in this paper, for example, see [26].

As noted above, the standard multiplicative character construction only gives one binary sequence of length p for each odd prime p. This is not very satisfactory if we are interested in finding pairs or larger families of binary sequences with low crosscorrelation. Boothby and Katz [2] discovered that one can often obtain sequences with good aperiodic autocorrelation and crosscorrelation properties using linear combinations of multiplicative characters. Among the sequences formed from linear combinations of multiplicative characters that Boothby and Katz studied are the *cyclotomic sequences*, whose periodic and aperiodic autocorrelation properties had been studied by Boehmer [1], and whose periodic autocorrelation and periodic crosscorrelation properties had been studied by Ding, Helleseth, and Lam [5, 6].

We now describe the construction of cyclotomic sequences. Let m be an even positive integer and let p be a prime with $m \mid p-1$. Then let $\mathbb{F}_p^{*m}$ be the set $\{a^m : a \in \mathbb{F}_p^*\}$ of mth powers, which is a subgroup of order $(p-1)/m$ in the group in $\mathbb{F}_p^*$. We form the quotient group $\mathbb{F}_p^*/\mathbb{F}_p^{*m}$ of order m, which consists of m cosets of $\mathbb{F}_p^{*m}$ in $\mathbb{F}_p^*$. Partition $\mathbb{F}_p$ into two sets, A and B as follows: A contains 0 along with the union of $m/2$ cosets of $\mathbb{F}_p^{*m}$, while B contains the union of the other $m/2$ cosets of $\mathbb{F}_p^{*m}$. Then we define a sequence $f = (f_0, f_1, \ldots, f_{p-1})$ where $f_j = 1$ if $j \in A$ and $f_j = -1$ if $j \in B$. The choices that we make when allocating cosets to A or B can influence the correlation behavior of the sequences.

Let us consider cyclotomic sequences in some of the simplest cases , that is, when m is small. When $m = 2$ and when we define A to be $\{0\} \cup \mathbb{F}_p^{*2}$, we recover the Legendre sequence h defined above (cf. (15)). When $m = 4$, we define two new sequences in this manner: let α be a primitive element of $\mathbb{F}_p$ and list the four cosets of $\mathbb{F}_p^{*4}$ as $R_j = \alpha^j \mathbb{F}_p^{*4}$ for $j \in \{0, 1, 2, 3\}$. Then define $f = (f_0, f_1, \ldots, f_{p-1})$ by

$$f_j = \begin{cases} +1 & \text{if } j \in R_0 \cup R_1 \cup \{0\} \\ -1 & \text{if } j \in R_2 \cup R_3, \end{cases} \tag{16}$$

and define $g = (g_0, g_1, \ldots, g_{p-1})$ by

$$g_j = \begin{cases} +1 & \text{if } j \in R_0 \cup R_3 \cup \{0\} \\ -1 & \text{if } j \in R_1 \cup R_2. \end{cases} \tag{17}$$

The Legendre sequence defined in (15) reappears in this formalism as $h = (h_0, h_1, \ldots, h_{p-1})$, where

$$h_j = \begin{cases} +1 & \text{if } j \in R_0 \cup R_2 \cup \{0\} \\ -1 & \text{if } j \in R_1 \cup R_3, \end{cases} \tag{18}$$

because $R_0 \cup R_2 = \mathbb{F}_p^{*2}$.

As mentioned above, these sequences are all formed by applying linear combinations of multiplicative characters to the list (13). In the case of our Legendre sequence h, the linear combination is just the single quadratic character. For sequences f and g, we let θ be the multiplicative character of $\mathbb{F}_p$ of order 4 defined by $\theta(\alpha^j) = e^{\pi i j/2} = i^j$, where we recall that α is the primitive element of $\mathbb{F}_p$ used to define the cosets R_j. The other multiplicative character of $\mathbb{F}_p$ of order 4 is $\overline{\theta}$, which has $\overline{\theta}(\alpha^j) = (-i)^j$. To get the sequence f, one first applies the linear combination of characters

$$\lambda(x) = \frac{1-i}{2}\theta(x) + \frac{1+i}{2}\overline{\theta}(x)$$

to the elements of the list (13) to get the sequence

$$(\lambda(0) = 0, \lambda(1), \ldots, \lambda(p-1)),$$

and then one replaces $\lambda(0) = 0$ with 1. To get the sequence g, one uses the same procedure, but with

$$\mu(x) = \frac{1+i}{2}\theta(x) + \frac{1-i}{2}\overline{\theta}(x)$$

in place of λ.

Now that we have introduced our sequences, we need to discuss the modified versions of them that have been found to have good correlation properties. First of all, unlike the definition of m-sequences in Section 6, the above definitions of sequences derived from multiplicative characters do not embrace all cyclic shifts of a given sequence. Instead each sequence comes defined with a particular cyclic shift. We will want to cyclically shift our multiplicative character sequences, but then we call them *shifted multiplicative character sequences* to distinguish them from the originals. For example, Golay [12] reported Turyn's discovery that one can significantly increase the autocorrelation merit factor of Legendre sequences if one cyclically shifts them. We can also apply Parker's doubling and quadrupling constructions, as well as the appending technique described in Section 6 to sequences produced from the constructions mentioned above.

As mentioned in Section 5, Høholdt and Jensen [17] proved that appropriately cyclically shifted Legendre sequences achieve asymptotic autocorrelation demerit factor 1/6. One can also obtain the same asymptotic demerit factor with sequences formed from Legendre sequences with Parker's doubling construction, as proved by Xiong and Hall [45, Theorem 3.3], or with Parker's quadrupling construction (combined with appropriate shifting), as proved by Schmidt, Jedwab, and Parker [39, Theorem 8].

If one also allows appending (with or without Parker's constructions and with appropriate shifting) of Legendre sequences, then Jedwab, Katz, and Schmidt (in [20, Theorem 1.1] an [19, Theorem 2.1]) showed that one can achieve an asymptotic autocorrelation demerit factor of $0.157\ldots$, which is the smallest real root of the polynomial $27x^3 - 417x^2 + 249x - 29$. To achieve this, one appends the sequences to be about $1.057\ldots$ times their usual length, where $1.057\ldots$ is the middle root of $4x^3 - 30x + 27$.

We note that one can generalize the notion of Legendre sequences, which are based on quadratic characters of prime fields, to *Jacobi sequences*, which are based on quadratic characters of integer residue rings (which allows for composite lengths). Jacobi sequences and their modifications (using shifting, Parker's constructions, and appending) often behave similarly to Legendre sequences, and are able to achieve the same asymptotic autocorrelation demerit factor of $1/6$ in their natural lengths and $0.157\ldots$ when appended. Although there are some detailed conditions that must be respected to obtain this behavior, Jacobi sequences provide good autocorrelation at a wider variety of lengths than one could obtain with Legendre sequences alone. See the papers of Jensen, Jensen, and Høholdt [24, Theorem 2.4, §§IV–V]; Xiong and Hall [45, §V], [46]; Jedwab and Schmidt [22]; and Jedwab, Katz, and Schmidt [19, Theorem 2.3, Corollary 2.4, and §6] for the principal results.

Boothby and Katz [2, Theorem 19] and Günther and Schmidt [16, p. 347] show that carefully selected families of the cyclotomic sequences can produce asymptotic demerit factor $1/6$ when suitably cyclically shifted, and if one also appends appropriately, this can be improved to the same $0.157\ldots$ value as for appended Legendre sequences. When designing a particular family of such sequences it is necessary to make judicious choices of which cyclotomic classes to assign $+1$ values and which cyclotomic classes to assign -1 values, otherwise the demerit factors will be bounded away from $0.157\ldots$. Boothby and Katz [2, Theorem 10] give conditions under which one can achieve limiting autocorrelation demerit factor $0.157\ldots$ for sequences derived from linear combinations of multiplicative characters, which includes the binary cyclotomic sequences as a proper subclass. Boothby and Katz's conditions are met by the cyclotomic sequences derived from quartic characters described at (16) and (17), and these sequences were used by both Boothby and Katz [2, Theorem 19] and Günther and Schmidt [16, p. 347] as examples showing that one can achieve asymptotic demerit factor $0.157\ldots$. Günther and Schmidt also give examples of sequence designs from six cyclotomic classes, and exhibit families that achieve limiting demerit factor $0.157\ldots$ and families that do not.

Even if one uses sequence designs from four or six cyclotomic classes that can achieve asymptotic autocorrelation demerit factor $0.157\ldots$, one must restrict one's sequence family to contain only sequences derived from fields $\mathbb{F}_p$ whose orders fulfill exacting number-theoretic conditions (see [2, Theorem 19] and [16, Corollaries 2.5 and 2.6]). As such, if one adopts one of these cyclotomic sequence designs, the sequences produced will, at most lengths, fall short of Legendre sequences in terms of autocorrelation performance. Accordingly Boothby and Katz [2, p. 6162] point out that there is little reason to use these cyclotomic sequences in applications where one wants a single sequence with good autocorrelation performance; rather, the real interest of cyclotomic sequences is that there is more than one of them of a given length, so they can be used in applications where crosscorrelation is important. We shall discuss this further in Section 11.

Günther and Schmidt [16, p. 344–345] also studied another family of pseudorandom sequences called the *Sidel′nikov sequences* [43]. These sequences are derived from quadratic characters of finite fields, but in a different way than Legendre sequences. Günther and Schmidt proved that Sidel′nikov sequences have the same asymptotic autocorrelation demerit factors as m-sequences: $1/3$ in their natural length, and $0.299\ldots$ for appropriately appended versions.

8. Rudin-Shapiro-like sequences

In his master's thesis [42, p. 42], Shapiro devised a construction of a family $f_0, f_1, f_2, \ldots$ of sequences, where f_n is a binary sequence of length 2^n. Shapiro's construction is easier to understand when one introduces a companion family of sequences, $g_0, g_1, g_2, \ldots$. Recall from Section 2 our identification of sequences with polynomials. The construction is the recursion with

$$\begin{aligned} f_0(z) &= g_0(z) = 1 \\ f_{n+1}(z) &= f_n(z) + z^{2^n} g_n(z) \\ g_{n+1}(z) &= f_n(z) - z^{2^n} g_n(z). \end{aligned} \tag{19}$$

In terms of sequences, this says that f_{n+1} is the concatenation of f_n and g_n, while g_{n+1} is the concatenation of f_n and $-g_n$. Shapiro's sequences (polynomials) are what one gets when one retains $f_0, f_1, f_2, \ldots$ and discards the companion sequences. These sequences were rediscovered by Rudin [37, eq. (1.5)] somewhat later, and are now known as *Rudin-Shapiro sequences* (or *Rudin-Shapiro polynomials*).

Around the same time as Shapiro, Golay [7] discovered an equivalent construction that produced what he called *complementary pairs* (now called *Golay complementary pairs* or just *Golay pairs*). These are pairs (f, g) of sequences of the same length with $C_{f,f}(s) + C_{g,g}(s) = 0$ for all $s \neq 0$, and Golay originally devised them for use in multislit spectrometry. We say that a Golay pair has length ℓ to mean that it consists of two sequences, each of length ℓ. If one pairs the Shapiro sequences with their companions, that is, if one considers $(f_0, g_0), (f_1, g_1), (f_2, g_2), \ldots$, then one obtains one infinite family of complementary pairs constructed by Golay. As mentioned in Section 5 above, Littlewood [33, pp. 27–28] performed a calculation tantamount to showing that $\mathrm{ADF}(f_n) = (1 - (-1/2)^n)/3$, which proves that the family $f_0, f_1, f_2, \ldots$ of Rudin-Shapiro sequences has asymptotic demerit factor $1/3$.

Brillhart and Carlitz [4, Theorem 1] showed that the companion sequences in the construction (19) were related to the main sequences by

$$g_n(z) = (-1)^n z^{2^n-1} f_n(-1/z)$$

for every n. For any polynomial $h(z) \in \mathbb{C}[z]$, we define the *reciprocal polynomial of* $h(z)$, denoted $h^*(z)$, to be $z^{\deg h} h(1/z)$, that is, the polynomial obtained from h by writing the coefficients in reverse order. Then the result of Brillhart and Carlitz becomes $g_n(z) = (-1)^{2^n+n-1} f_n^*(-z)$, so that we could restate the construction without the companion sequences:

$$\begin{aligned} f_0(z) &= 1 \\ f_{n+1}(z) &= f_n(z) + (-1)^{2^n+n-1} z^{\deg f_n + 1} f_n^*(-z). \end{aligned} \tag{20}$$

It turns out that one gets similar asymptotic autocorrelation behavior no matter how the sign is chosen on the second term, as observed by Høholdt, Jensen, and Justesen [18, Theorem 2.3], so we may generalize construction (20) to

$$\begin{aligned} f_0(z) &= 1 \\ f_{n+1}(z) &= f_n(z) + \sigma_n z^{\deg f_n + 1} f_n^*(-z), \end{aligned} \tag{21}$$

where $\sigma_0, \sigma_1, \ldots$ is any sequence of values in $\{+1, -1\}$, called the *sign sequence* for our construction. Høholdt, Jensen, and Justesen show [18, Theorem 2.3] that regardless of the choice of sign sequence, one still obtains $\mathrm{ADF}(f_n) = (1 - (-1/2)^n)/3$, so the asymptotic autocorrelation demerit factor is $1/3$.

Construction (21) was further generalized by Borwein and Mossinghoff [3, pp. 1159 and 1161], by allowing much more freedom at the start:

$$\begin{aligned} f_0(z) &= \text{any polynomial with coefficients in } \{+1, -1\} \\ f_{n+1}(z) &= f_n(z) + \sigma_n z^{\deg f_n + 1} f_n^*(-z), \end{aligned} \tag{22}$$

where again $\sigma_0, \sigma_1, \ldots$ is any sequence of values in $\{+1, -1\}$, called the *sign sequence* for our construction. We call f_0 the *seed* of the construction, and we call the family $f_0, f_1, f_2, \ldots$ of polynomials the *stem* generated by that seed and sign sequence. Following Borwein and Mossinghoff, we call families of sequences (polynomials) generated from construction (22) *Rudin-Shapiro-like sequences (polynomials).*

Borwein and Mossinghoff found a precise formula [3, Theorem 1] for the autocorrelation demerit factor of Rudin-Shapiro-like polynomials produced by their construction (22). That is, they have a formula for computing $\mathrm{ADF}(f_n)$ for every n, and from this they compute the asymptotic autocorrelation merit factor, which depends on the seed but not the sign sequence. They show that the asymptotic autocorrelation demerit factor is always greater than or equal to $1/3$, but only achieves a value of $1/3$ for certain seeds, which we call *optimal seeds.* Borwein and Mossinghoff performed a computer search (informed by some of their theoretical results) over all binary sequences of length 40 or less, and found optimal seeds of lengths 1, 2, 4, 8, 16, 20, 32, and 40, and no optimal seeds of other lengths in this range. Later Katz, Lee, and Trunov [28, Table 1] performed a larger search that extended to all seeds of length 52 or less, and found new optimal seeds at length 52 (but at no other length between 40 and 52). This data was explained by the following classification of optimal seeds [30, Theorem 1]: a seed of length greater than 1 is optimal if and only if it is the interleaving of a Golay complementary pair, where the *interleaving* of two sequences $a = (a_0, a_1, \ldots, a_{\ell-1})$ and $b = (b_0, b_1, \ldots, b_{\ell-1})$ of length ℓ is the the sequence $(a_0, b_0, a_1, b_1, \ldots, a_{\ell-1}, b_{\ell-1})$ of length 2ℓ. In polynomial terms, the interleaving is $a(z^2) + zb(z^2)$. This result, along with the known fact that the two seeds ($+1$ and -1) of length 1 are optimal, gives a full classification of the optimal seeds. A construction of Turyn [44, Corollary to Lemma 5] shows that there is a Golay complementary pair of length $2^a 10^b 26^c$ for every choice of nonnegative integers a, b, c. Thus there are infinitely many optimal seeds.

9. High asymptotic crosscorrelation merit factor

Consider the sequences

$$\begin{aligned} f_\ell &= (+1, +1, +1, +1, \ldots, +1, +1) \\ g_\ell &= (+1, -1, +1, -1, \ldots, +1, -1) \end{aligned}$$

of even length ℓ. It is not difficult to calculate that

$$\mathrm{CDF}(f_\ell, g_\ell) = \frac{1}{\ell},$$

so that the asymptotic crosscorrelation demerit factor of the family of pairs $\{(f_\ell, g_\ell) : \ell \in 2\mathbb{Z}\}$ is zero (so asymptotic crosscorrelation merit factor is infinite). But it is also not difficult to calculate that

$$\mathrm{ADF}(f_\ell) = \mathrm{ADF}(g_\ell) = \frac{2\ell^2 + 1}{3\ell},$$

so that the families $\{f_\ell : \ell \in 2\mathbb{Z}\}$ and $\{g_\ell : \ell \in 2\mathbb{Z}\}$ both have infinite asymptotic autocorrelation demerit factor (so asymptotic autocorrelation merit factor is 0). Thus it is not interesting to seek families of sequence pairs with low asymptotic crosscorrelation demerit factor in isolation from the asymptotic autocorrelation demerit factor of the constituent sequences. What we really want to know is whether there is a way to make asymptotic autocorrelation and crosscorrelation demerit factors small at the same time. In the next section we explore a measure that will help us quantify this goal.

10. Pursley-Sarwate Criterion

Pursley and Sarwate [36, eqs. (3),(4)] proved that any pair (f, g) of binary sequences has

$$1 - \sqrt{\mathrm{ADF}(f)\,\mathrm{ADF}(g)} \le \mathrm{CDF}(f, g) \le 1 + \sqrt{\mathrm{ADF}(f)\,\mathrm{ADF}(g)}. \tag{23}$$

Their proof is based on the Cauchy-Schwarz inequality. We define the *Pursley-Sarwate criterion* for a pair (f, g) of sequences to be

$$\mathrm{PSC}(f,g)=\sqrt{\mathrm{ADF}(f)\,\mathrm{ADF}(g)}+\mathrm{CDF}(f,g),$$

and then the bound (23) tells us that

$$\mathrm{PSC}(f,g)\geq 1. \tag{24}$$

We would like sequence pairs (f, g) with $\mathrm{ADF}(f)$, $\mathrm{ADF}(g)$, and $\mathrm{CDF}(f, g)$ as small as possible, but the bound (24) shows that we cannot make them all simultaneously close to zero. In view of Sarwate's expected values of demerit factors for randomly selected binary sequences in (10) and (11), we expect a typical randomly selected pair (f, g) of sequences to have $\mathrm{PSC}(f, g)$ of about 2. We would like to construct sequence pairs (f, g) with $\mathrm{PSC}(f, g)$ as close to 1 as possible. We often consider *asymptotic* PSC of families of sequence pairs, that is, the limiting value of PSC as the length of the sequences tends to infinity.

11. Pairs with low asymptotic Pursley-Sarwate criterion

One should recall the sequence constructions described in Sections 6, 7, and 8 above: we now consider pairs of such sequences that have low Pursley-Sarwate criterion. Table 2 lists some constructions that produce families of binary sequence pairs with low asymptotic PSC.

Table 2. Families of sequence pairs with low asymptotic PSC

Sequence pair (f,g)	Asymptotic Values		
construction	$\mathrm{ADF}(f)=\mathrm{ADF}(g)$	$\mathrm{CDF}(f,g)$	$\mathrm{PSC}(f,g)$
Katz (2016) [27, pp. 5240, 5247]			
m-sequences, typical	1/3	1	4/3
m-sequence, reversing	1/3	5/6	7/6
half Legendre	7/12	7/12	7/6
Boothby-Katz (2017) [2, pp. 6160–6161]			
quartic cyclotomics	in $[1/6, 5/6]$	in $[1/3, 1]$	7/6
Legendre + quartic	1/6	1	7/6
Katz-Lee-Trunov [28, Table 3]			
Rudin-Shapiro-like	1/3	77/100	331/300
Katz-Moore [29, Theorem 1.1]			
Golay pair	1/3	2/3	1

Let us provide some context and details for the table entries. If we fix a $d \in \mathbb{Z}$ with $|d|$ not a power of 2 and produce an infinite family of binary m-sequence pairs (f_n, g_n) where g_n is (up to cyclic shift) a decimation of f_n by

d, then Katz [27, Theorem 1] showed that the asymptotic crosscorrelation demerit factor will tend to 1. Since we have seen in Section 6 that the autocorrelation demerit factor tends to $1/3$, this produces a sequence family with asymptotic PSC of $4/3$. We call this a *typical m-sequence construction.* If we instead use $d = -2^k$ for some nonnegative integer k, then we produce a family of binary m-sequence pairs (f_n, g_n) where g_n is related to f_n by the reversing decimation, and then Katz [27, Theorem 2] showed that one can lower the asymptotic crosscorrelation demerit factor to $5/6$ by appropriately cyclically shifting the sequences. This results in families with asymptotic PSC of $7/6$. We call this a *reversing m-sequence construction.* (We never allow d to be a power of 2, since that will give degenerate decimations, and we will be correlating an m-sequence with cyclic shifts of itself.)

Another construction of Katz [27, p. 5247] takes a Legendre sequence (which has length equal to some odd prime p), cyclically shifts it in a certain way, discards the last term, and cuts the remaining sequence into a pair of two sequences of length $(p-1)/2$. In this way one can obtain a family of sequence pairs (f_n, g_n) with asymptotic $\mathrm{ADF}(f_n)$, $\mathrm{ADF}(g_n)$, and $\mathrm{CDF}(f_n, g_n)$ all equal to $7/12$, and thus asymptotic PSC equal to $7/6$. We call this the *half Legendre construction.*

Boothby and Katz [2, Theorem 21] crosscorrelated the two cyclotomic sequences (16) and (17) derived from quartic characters, and also the cyclically shifted versions of these two sequences. As mentioned in Section 7, one obtains very low asymptotic autocorrelation demerit factor only for certain lengths, depending on a number-theoretic criterion. It turns out that the crosscorrelation demerit factor of our sequence pairs tends to decrease as their autocorrelation demerit factor increases. In fact, for any real number A with $1/6 \leq A \leq 5/6$, there is an infinite family of pairs (f_n, g_n) of these cyclically shifted cyclotomic sequences such that asymptotic $\mathrm{ADF}(f_n)$ and $\mathrm{ADF}(g_n)$ are A, asymptotic $\mathrm{CDF}(f_n, g_n)$ is $7/6 - A$, and asymptotic PSC is $7/6$.

One can also crosscorrelate cyclically shifted Legendre sequences (see (15), or equivalently (18)) with cyclically shifted versions of either of our quartic cyclotomic sequences (see (16) or (17)). In this case Boothby and Katz [2, Theorem 20] show that one always obtains asymptotic CDF of 1, so one should choose the shifted Legendre sequences and shifted quartic cyclotomic sequences to have limiting ADF of $1/6$, and thus obtain limiting PSC of $7/6$.

It should be noted that all the constructions of Katz and Boothby-Katz discussed here employ sequences in their usual length, but their results allow for the possibility of truncating and appending the sequences. They showed [2, eq. (7)] that modest appending can be used to produce families of sequence pairs with asymptotic PSC slightly lower than $7/6$.

Katz, Lee, and Trunov crosscorrelated pairs of Rudin-Shapiro-like polynomials [28, Theorem 2.4], by beginning with two different seeds, f_0 and g_0, and applying recursion (22) to produce two stems $f_0, f_1, \ldots$ and $g_0, g_1, \ldots$ (using the same sign sequence in recursion (22) to produce the two stems).

They derive a precise formula for $\mathrm{CDF}(f_n, g_n)$ for each n. This reduces to Borwein and Mossinghoff's precise formula [3, Theorem 1] for $\mathrm{ADF}(f_n)$ when we set $g_n = f_n$ and subtract 1 (see (8)). From this one can compute $\mathrm{PSC}(f_n, g_n)$ precisely and from this determine the limiting PSC. Katz, Lee, and Trunov [28, Table 3] found a pair of seeds, each of length 40, that yield stems with limiting ADF of 1/3 and limiting CDF of 77/100, for a limiting PSC of $331/300 = 1.10\overline{3}$.

Finally, Katz and Moore [29, Theorem 1.1] proved that a pair (f, g) of binary sequences has $\mathrm{PSC}(f, g) = 1$ if and only if (f, g) is a Golay complementary pair. In Section 8, we noted that there are known to be Golay pairs of lengths $2^a 10^b 26^c$ for all nonnegative integers a, b, and c, so we have infinitely many binary sequence pairs with PSC exactly equal to 1. Thus we obtain an asymptotic PSC of 1 with the Golay pairs. We note that if (f, g) is a Golay pair, then $\mathrm{ADF}(f) = \mathrm{ADF}(g)$. The Golay pairs (f_n, g_n) produced by recursion (19) have Rudin-Shapiro sequences as the first sequence in each pair. Thus they have asymptotic $\mathrm{ADF}(f_n)$ equal to 1/3 by the result of Littlewood described in Sections 5 and 8. So asymptotic $\mathrm{ADF}(g_n)$ is also 1/3 for these pairs, and thus asymptotic $\mathrm{CDF}(f_n, g_n)$ is 2/3.

We note that the families of sequence pairs on Table 2 all have equal asymptotic autocorrelation demerit factors for the first and second elements of the pairs. While this must be the case for Golay complementary pairs, is not always observed in other constructions with low asymptotic PSC. For example, Katz, Lee, and Trunov [28, Table 2] exhibit constructions of families $(f_0, g_0), (f_1, g_1), \ldots$ of pairs of Rudin-Shapiro-like sequences with low asymptotic $\mathrm{PSC}(f_n, g_n)$ where the asymptotic $\mathrm{ADF}(f_n)$ is not equal to the asymptotic $\mathrm{ADF}(g_n)$.

12. Open questions

We present two open questions that arise naturally from the considerations above.

Question 1. *What is the lowest asymptotic autocorrelation demerit factor for binary sequences?*

Or equivalently, what is the highest asymptotic autocorrelation merit factor for binary sequences? Littlewood [33, pp. 28–29] made a conjecture that there is a infinite family of binary sequences with autocorrelation demerit tending to zero, or equivalently, autocorrelation merit factor tending to infinity. Golay, on the other hand, conjectured that autocorrelation merit factor is bounded, and he proposed [10] that asymptotic merit factor can never exceed $2e^2 = 14.77\ldots$. Later [11] he revised his proposed upper bound on asymptotic merit factor to a value of about 12.32.

We saw in Section 9 a construction of sequence pairs with asymptotic crosscorrelation demerit factor of zero, but at the expense of poor autocorrelation performance. It would be interesting to know how low asymptotic crosscorrelation demerit factor can be made without having poor autocorrelation demerit factors.

Question 2. *Among infinite families of binary sequence pairs (f, g) such that* $\mathrm{ADF}(f)$*,* $\mathrm{ADF}(g)$*, and* $\mathrm{CDF}(f, g)$ *tend to limits as the length of the sequences tends to infinity, and such that the limiting values for* $\mathrm{ADF}(f)$ *and* $\mathrm{ADF}(g)$ *are not greater than* 1*, what is the lowest possible limiting value for* $\mathrm{CDF}(f, g)$*?*

In Section 11 we saw that the construction of Boothby-Katz [2, p. 6160] involving pairs of cyclotomic sequences derived from quartic characters furnishes families of sequence pairs (f, g) with asymptotic $\mathrm{CDF}(f, g)$ of $1/3$ and asymptotic $\mathrm{ADF}(f)$ and $\mathrm{ADF}(g)$ of $5/6$ (so limiting $\mathrm{PSC}(f, g)$ is $7/6$). If one wants to get even lower asymptotic CDF, then one can use appending. One would use Theorems 19 and 21 of [2] with the following parameters: one would let $\gamma = \pi/2$, let $\Lambda = 1.207\ldots$ be the middle root of $4x^3 - 36x^2 + 60x - 27$, and let $R = (1 - 2\Lambda)/4$. This would produce a family of pairs of quartic cyclotomic sequences that are cyclically shifted and then appended to $\Lambda = 1.207\ldots$ times their normal length. The limiting ADF of these sequences is 1 and the limiting CDF is $0.254\ldots$, the middle root of $729x^3 + 981x^2 - 1245x + 241$. Note that the PSC for this family is $1.254\ldots$, which is considerably worse than the $7/6$ that one obtains without appending, so a considerable sacrifice in autocorrelation performance is being made for this increase in crosscorrelation performance. One should note that when one appends like this, there will be a rather large value in the autocorrelation spectrum when the appended portion on one copy of the sequence comes into alignment with the initial portion of the other copy. The magnitude of this large autocorrelation value will be about equal to the length of the appended sequence times $1 - 1/\Lambda = 0.172\ldots$.

This paper has confined itself to analyzing the autocorrelation and crosscorrelation demerit factors of sequence pairs. In many applications one needs larger families of sequences with low mutual correlation, and it would be interesting to extend the concepts here to that more general setting.

Acknowledgement

The author thanks Yakov Sapozhnikov for his careful reading of this paper and his helpful suggestions.

References

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

[2] K. T. R. Boothby and D. J. Katz. Low correlation sequences from linear combinations of characters. *IEEE Trans. Inform. Theory*, **63**(10):6158–6178 (2017).

[3] P. Borwein and M. Mossinghoff. Rudin-Shapiro-like polynomials in L_4. *Math. Comp.*, **69**(231):1157–1166 (2000).

[4] J. Brillhart and L. Carlitz. Note on the Shapiro polynomials. *Proc. Amer. Math. Soc.*, **25**:114–118 (1970).

[5] C. Ding, T. Helleseth, and K. Y. Lam. Several classes of binary sequences with three-level autocorrelation. *IEEE Trans. Inform. Theory*, **45**(7):2606–2612 (1999).

[6] C. Ding, T. Helleseth, and K. Y. Lam. Duadic sequences of prime lengths. *Discrete Math.*, **218**(1-3):33–49 (2000).

[7] M. J. E. Golay. Static multislit spectrometry and its application to the panoramic display of infrared spectra. *J. Opt. Soc. Am.*, **41**(7):468–472 (1951).

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

[9] M. J. E. Golay. Hybrid low autocorrelation sequences. *IEEE Trans. Inform. Theory*, **21**:460–462 (1975).

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

[11] M. J. E. Golay. The merit factor of long low autocorrelation binary sequences. *IEEE Trans. Inform. Theory*, **28**(3):543–549 (1982).

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

[13] R. Gold. Optimal binary sequences for spread spectrum multiplexing. *IEEE Trans. Inform. Theory*, **13**(4):619–621 (1967).

[14] S. W. Golomb. *Shift register sequences.* With portions co-authored by Lloyd R. Welch, Richard M. Goldstein, and Alfred W. Hales. Holden-Day, Inc., San Francisco, Calif.-Cambridge-Amsterdam (1967).

[15] S. W. Golomb and G. Gong. *Signal design for good correlation.* Cambridge University Press, Cambridge (2005).

[16] C. Günther and K.-U. Schmidt. Merit factors of polynomials derived from difference sets. *J. Combin. Theory Ser. A*, **145**:340–363 (2017).

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

[18] T. Høholdt, H. E. Jensen, and J. Justesen. Aperiodic correlations and the merit factor of a class of binary sequences. *IEEE Trans. Inform. Theory*, **31**(4):549–552 (1985).

[19] J. Jedwab, D. J. Katz, and K.-U. Schmidt. Advances in the merit factor problem for binary sequences. *J. Combin. Theory Ser. A*, **120**(4):882–906 (2013).

[20] J. Jedwab, D. J. Katz, and K.-U. Schmidt. Littlewood polynomials with small L^4 norm. *Adv. Math.*, **241**:127–136 (2013).

[21] J. Jedwab and K.-U. Schmidt. The merit factor of binary sequence families constructed from m-sequences. In *Finite fields: theory and applications*, volume 518 of *Contemp. Math.*, pages 265–278. Amer. Math. Soc., Providence, RI (2010).

[22] J. Jedwab and K.-U. Schmidt. The L_4 norm of Littlewood polynomials derived from the Jacobi symbol. *Pacific J. Math.*, **257**(2):395–418 (2012).

[23] H. E. Jensen and T. Høholdt. Binary sequences with good correlation properties. In *Applied algebra, algebraic algorithms and error-correcting codes (Menorca, 1987)*, volume 356 of *Lecture Notes in Comput. Sci.*, pages 306–320. Springer, Berlin (1989).

[24] J. M. Jensen, H. E. Jensen, and T. Høholdt. The merit factor of binary sequences related to difference sets. *IEEE Trans. Inform. Theory*, **37**(3, part 1):617–626 (1991).

[25] K. H. A. Kärkkäinen. Mean-square cross-correlation as a performance measure for department of spreading code families. In *IEEE Second International Symposium on Spread Spectrum Techniques and Applications*, pages 147–150 (1992).

[26] D. J. Katz. Asymptotic L^4 norm of polynomials derived from characters. *Pacific J. Math.*, **263**(2):373–398 (2013).

[27] D. J. Katz. Aperiodic crosscorrelation of sequences derived from characters. *IEEE Trans. Inform. Theory*, **62**(9):5237–5259 (2016).

[28] D. J. Katz, S. Lee, and S. A. Trunov. Crosscorrelation of Rudin-Shapiro-like polynomials. Preprint, arXiv:1702.07697 (2017).

[29] D. J. Katz and E. Moore. Sequence pairs with lowest combined autocorrelation and crosscorrelation. Preprint, arXiv:1711.02229 (2017).

[30] D. J. Katz and S. A. Trunov. Rudin-Shapiro-like polynomials with maximum asymptotic merit factor. Preprint, arXiv:1711.02233 (2017).

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

[32] 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).

[33] J. E. Littlewood. *Some problems in real and complex analysis.* D. C. Heath and Co. Raytheon Education Co., Lexington, Mass. (1968).

[34] C. Mauduit and A. Sárközy. On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol. *Acta Arith.*, **82**(4):365–377 (1997).

[35] M. G. Parker. Even length binary sequence families with low negaperiodic autocorrelation. In *Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001)*, volume 2227 of *Lecture Notes in Comput. Sci.*, pages 200–209. Springer, Berlin (2001).

[36] M. B. Pursley and D. V. Sarwate. Bounds on aperiodic cross-correlation for binary sequences. *Electronics Letters*, **12**(12):304–305 (1976).

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

[38] D. V. Sarwate. Mean-square correlation of shift-register sequences. *Communications, Radar and Signal Processing, IEE Proceedings F*, **131**(2):101–106 (1984).

[39] K.-U. Schmidt, J. Jedwab, and M. G. Parker. Two binary sequence families with large merit factor. *Adv. Math. Commun.*, **3**(2):135–156 (2009).

[40] R. A. Scholtz and L. R. Welch. GMW sequences. *IEEE Trans. Inform. Theory*, **30**(3):548–553 (1984).

[41] M. R. Schroeder. *Number theory in science and communication*, volume 7 of *Springer Series in Information Sciences.* Springer-Verlag, Berlin, fourth edition (2006). With applications in cryptography, physics, digital information, computing, and self-similarity.

[42] H. S. Shapiro. Extremal problems for polynomials and power series. Master's thesis, Massachusetts Institute of Technology, Cambridge (1951).

[43] V. M. Sidel′nikov. Some k-valued pseudo-random sequences and nearly equidistant codes. *Problemy Peredači Informacii*, **5**(1):16–22 (1969). English translation in *Problems of Information Transmission*, **5**:12–16 (1969).

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

[45] T. Xiong and J. I. Hall. Construction of even length binary sequences with asymptotic merit factor 6. *IEEE Trans. Inform. Theory*, **54**(2):931–935 (2008).

[46] T. Xiong and J. I. Hall. Modifications of modified Jacobi sequences. *IEEE Trans. Inform. Theory*, **57**(1):493–504 (2011).

Department of Mathematics, California State University, Northridge, United States