

# ADVANCES IN THE MERIT FACTOR PROBLEM FOR BINARY SEQUENCES

JONATHAN JEDWAB, DANIEL J. KATZ, AND KAI-UWE SCHMIDT

ABSTRACT. The identification of binary sequences with large merit factor (small mean-squared aperiodic autocorrelation) is an old problem of complex analysis and combinatorial optimization, with practical importance in digital communications engineering and condensed matter physics. We establish the asymptotic merit factor of several families of binary sequences and thereby prove various conjectures, explain numerical evidence presented by other authors, and bring together within a single framework results previously appearing in scattered form. We exhibit, for the first time, families of skew-symmetric sequences whose asymptotic merit factor is as large as the best known value (an algebraic number greater than 6.34) for all binary sequences; this is interesting in light of Golay's conjecture that the subclass of skew-symmetric sequences has asymptotically optimal merit factor. Our methods combine Fourier analysis, estimation of character sums, and estimation of the number of lattice points in polyhedra.

## 1. INTRODUCTION

Let  $A = (a_0, a_1, \dots, a_{t-1})$  be an element of  $\{-1, 1\}^t$  with  $t > 1$ . We call  $A$  a *binary sequence of length  $t$* . The *aperiodic autocorrelation* of  $A$  at shift  $u$  is

$$c_u = \sum_{j=0}^{t-u-1} a_j a_{j+u} \quad \text{for } u \in \{0, 1, \dots, t-1\}.$$

Following Golay [14], we define the *merit factor* of  $A$  to be

$$F(A) = \frac{t^2}{2 \sum_{u=1}^{t-1} c_u^2}.$$

---

*Date:* 03 May 2012 (revised 22 January 2013).

*Key words and phrases.* Merit factor; binary sequence; asymptotic; skew-symmetric; Fourier analysis; character sum; lattice point.

J. Jedwab and D.J. Katz are with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada. K.-U. Schmidt was with Department of Mathematics, Simon Fraser University and is now with Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany. Email: jed@sfu.ca, dkatz@sfu.ca, kaiuwe.schmidt@ovgu.de.

J. Jedwab is supported by NSERC.

K.-U. Schmidt was supported by German Research Foundation.

A large merit factor means that the sum of squares of the autocorrelations at nonzero shifts is small when compared to the squared autocorrelation at shift zero (which always equals  $t^2$ ).

The determination of the largest possible merit factor of long binary sequences is of considerable importance in various disciplines (see [24] and [19] for surveys, and [25] for background on related problems). In digital communications, binary sequences with large merit factor correspond to signals whose energy is very uniformly distributed over frequency [1]. In theoretical physics, binary sequences achieving the largest merit factor for their length correspond to the ground states of Bernasconi's Ising spin model [2]. The growth rate of the optimal merit factor of binary sequences, as the sequence length increases, is related to classical conjectures due to Littlewood [36], [37] and Erdős [11, Problem 22], [12], [40] on the asymptotic behavior of norms of polynomials on the unit circle. This relationship arises because, when the binary sequence  $A$  is represented as a polynomial  $A(z) = \sum_{j=0}^{t-1} a_j z^j$ , its merit factor  $F(A)$  satisfies

$$(1.1) \quad \frac{1}{F(A)} = -1 + \frac{1}{2\pi t^2} \int_0^{2\pi} |A(e^{i\theta})|^4 d\theta$$

(see [36, pp. 370–371] or [20, eq. (4.1)], for example).

Littlewood [37, Chapter III, Problem 19] proved in 1968 that the merit factor of Rudin-Shapiro sequences tends to 3 as their length tends to infinity. Høholdt and Jensen [20], building on studies due to Turyn and Golay [17], proved in 1988 that the merit factor of Legendre sequences rotated by a quarter of their length is asymptotically 6, and conjectured that 6 is asymptotically the largest possible merit factor for binary sequences. But the present authors [26] recently disproved this conjecture by showing that a certain family of binary sequences attains an asymptotic merit factor  $F_a = 6.342061\dots$ , which is the largest root of  $29x^3 - 249x^2 + 417x - 27$ . These sequences, called *appended rotated Legendre sequences*, had been studied numerically by Kirilusha and Narayanaswamy [33] and Borwein, Choi, and Jedwab [8].

Prior to the paper [26], only two methods were known for calculating the asymptotic merit factor of a family of binary sequences [19]. The first is direct calculation, particularly in the case that the polynomials are recursively defined [37]. The second, introduced by Høholdt and Jensen [20] in 1988, is more widely applicable [30], [31], [5], [6], [4], [7], [44], [28], [29]. The new approach of [26] made it possible for the first time to handle appended rotated Legendre sequences, thereby showing that an asymptotic merit factor of 6 can be exceeded. In this paper, we elaborate and further develop the method of [26] to deal with other highly-studied binary sequence families, including Galois sequences (also known as m-sequences), Jacobi sequences, and sequences formed using Parker's periodic and negaperiodic constructions [41]. This allows us to explain several previous numerical results and prove a series of conjectures [42], [52], [49], [27] (see Section 3). Moreover,

we give simple unifying proofs, as well as generalizations, of the main results of [20], [30], [31], [41], [8], [49], [44], [28], [29] and [26].

The binary sequences we consider in this paper fall into two classes. The largest achievable asymptotic merit factor for the first class, based on Legendre sequences, is  $F_a = 6.342061\dots$  mentioned above, whereas that for the second class, based on Galois sequences, is  $F_b = 3.342065\dots$ , the largest root of  $7x^3 - 33x^2 + 33x - 3$ .

A binary sequence  $(a_0, a_1, \dots, a_{2s})$  of odd length  $2s + 1$  is called *skew-symmetric* if

$$a_{s+j} = (-1)^j a_{s-j} \quad \text{for all } j \in \{1, 2, \dots, s\}.$$

Historically, skew-symmetric binary sequences have been considered good candidates for a large merit factor (see [24, Section 3.1] for background), in part because half of their aperiodic autocorrelations are zero [14]. Computer calculations indicate [15, Table III], [39] that skew-symmetric binary sequences have largest possible merit factor among all binary sequences of their length, for all odd lengths between 2 and 60 except 19, 23, 25, 31, 33, 35, and 37. Golay conjectured [15], [16], based on a heuristic argument, that the largest asymptotic merit factor among all binary sequences is attained by skew-symmetric sequences. It is interesting, in light of Golay's conjecture, that Corollary 2.4 provides the first known families of skew-symmetric binary sequences with asymptotic merit factor  $F_a = 6.342061\dots$ .

To the authors' knowledge, this paper contains all currently known results on the asymptotic merit factor of nontrivial families of binary sequences, except for Rudin-Shapiro sequences [37] and related binary sequence families [21], [9], and certain modifications of Jacobi sequences [29], [51], [50].

## 2. RESULTS

Let  $A(z) = \sum_{j=0}^{n-1} a_j z^j$  be a polynomial of degree  $n - 1$  with coefficients in  $\{-1, 1\}$ ; we call  $(a_0, a_1, \dots, a_{n-1})$  the *coefficient sequence* of  $A$ , and write  $F(A)$  for its merit factor. Let  $r$  and  $t$  be integers that can depend on  $n$ , where  $t \geq 0$ , and define the polynomial

$$A^{r,t}(z) = \sum_{j=0}^{t-1} a_{j+r} z^j,$$

where henceforth we extend the definition of  $a_j$  so that  $a_{j+n} = a_j$  for all  $j \in \mathbb{Z}$ . The coefficient sequence of  $A^{r,t}$  is derived from that of  $A$  by cyclically permuting (rotating) the sequence elements through  $r$  positions, and then truncating when  $t < n$  or periodically extending (appending) when  $t > n$ . We follow Parker [41, Lemma 3] by applying a "negaperiodic" construction to  $A$  to give the polynomial

$$N(A)(z) = \sum_{j=0}^{4n-1} (-1)^{j(j-1)/2} a_j z^j,$$

whose coefficient sequence is the element-wise product of the coefficient sequence of  $A^{0,4n}$  with the sequence  $(+, +, -, -, +, +, -, -, \dots, +, +, -, -)$  of length  $4n$ . We also follow Parker [41, Lemma 4] by applying a “periodic” construction to  $A$  to give the polynomial

$$P(A)(z) = \sum_{j=0}^{4n-1} (-1)^{j(j-1)^2/2} a_j z^j,$$

whose coefficient sequence is the element-wise product of the coefficient sequence of  $A^{0,4n}$  with the sequence  $(+, +, -, +, +, +, -, +, \dots, +, +, -, +)$  of length  $4n$ .<sup>1</sup> The advantage of interpreting Parker’s constructions in terms of product sequences was recognized by Xiong and Hall [49] in the negaperiodic case, and by Yu and Gong [52] in the periodic case.

Let  $p$  be an odd prime. The *Legendre symbol*  $(j|p)$  is given by

$$(j|p) = \begin{cases} 0 & \text{if } j \equiv 0 \pmod{p}, \\ -1 & \text{if } j \text{ not a square modulo } p, \\ +1 & \text{otherwise,} \end{cases}$$

and the coefficient sequence of

$$(2.1) \quad X_p(z) = 1 + \sum_{j=1}^{p-1} (j|p) z^j$$

is a binary sequence called the *Legendre sequence* of length  $p$ .

Define the function  $g : \mathbb{R} \times \mathbb{R}^+ \rightarrow \mathbb{R}$  by

$$\frac{1}{g(R, T)} = 1 - \frac{4T}{3} + 4 \sum_{m \in \mathbb{N}} \max\left(0, 1 - \frac{m}{T}\right)^2 + \sum_{m \in \mathbb{Z}} \max\left(0, 1 - \left|1 + \frac{2R - m}{T}\right|\right)^2,$$

where  $\mathbb{N}$  is the set of positive integers. Then we have the following asymptotic merit factor result for Legendre sequences, and their negaperiodic and periodic versions.

**Theorem 2.1.** *Let  $X_p$  be the Legendre sequence of length  $p$  and let  $R$  and  $T > 0$  be real. Then the following hold, as  $p \rightarrow \infty$ :*

- (i) *If  $r/p \rightarrow R$  and  $t/p \rightarrow T$ , then  $F(X_p^{r,t}) \rightarrow g(R, T)$ .*
- (ii) *If  $r/(2p) \rightarrow R$  and  $t/(2p) \rightarrow T$ , then  $F(N(X_p)^{r,t}) \rightarrow g(R + \frac{1}{4}, T)$ .*
- (iii) *If  $r/(4p) \rightarrow R$  and  $t/(4p) \rightarrow T$ , then  $F(P(X_p)^{r,t}) \rightarrow g(R, T)$ .*

Theorem 2.1 (i) is the main result of [26]. The function  $g$  satisfies  $g(R, T) = g(R + \frac{1}{2}, T)$  on its entire domain. As shown in [26, Corollary 3.2], the global

---

<sup>1</sup>Our constructions are cyclically permuted versions of those of Parker [41], and our  $N(A)$  is defined to be twice as long as Parker’s; we address all cyclic shifts and lengths in our results, but the definitions above give the most convenient reference point for subsequent calculations.

maximum of  $g(R, T)$  exists and equals

$$(2.2) \quad F_a = 6.342061 \dots, \text{ the largest root of } 29x^3 - 249x^2 + 417x - 27.$$

The global maximum is unique for  $R \in [0, \frac{1}{2})$ , and is attained when  $T = 1.057827 \dots$  is the middle root of  $4x^3 - 30x + 27$  and  $R = \frac{3}{4} - \frac{T}{2}$ .

Now let  $\mathbb{F}_{2^d}$  be the finite field with  $2^d$  elements and write  $n = 2^d - 1$ . Let  $\psi : \mathbb{F}_{2^d} \rightarrow \{-1, 1\}$  be the canonical additive character of  $\mathbb{F}_{2^d}$ , given by

$$\psi(y) = (-1)^{\text{Tr}(y)},$$

where  $\text{Tr}(y) = \sum_{j=0}^{d-1} y^{2^j}$  is the absolute trace on  $\mathbb{F}_{2^d}$ . Let  $\theta$  be a primitive element of  $\mathbb{F}_{2^d}$  and define the polynomial

$$(2.3) \quad Y_{n,\theta}(z) = \sum_{j=0}^{n-1} \psi(\theta^j) z^j.$$

The coefficient sequence of  $Y_{n,\theta}$  is a binary sequence which we call the *Galois sequence* of length  $n$  with respect to  $\theta$  (cf. [46] for this terminology).<sup>2</sup>

Define the function  $h : \mathbb{R}^+ \rightarrow \mathbb{R}$  by

$$\frac{1}{h(T)} = 1 - \frac{2T}{3} + 4 \sum_{m \in \mathbb{N}} \max\left(0, 1 - \frac{m}{T}\right)^2.$$

Then we have the following asymptotic merit factor result for Galois sequences, and their negaperiodic and periodic versions.

**Theorem 2.2.** *For each  $n = 2^d - 1$ , choose an integer  $r$  and a primitive  $\theta \in \mathbb{F}_{2^d}$ , and let  $Y_{n,\theta}$  be the Galois sequence of length  $n$  with respect to  $\theta$ . Let  $T > 0$  be real. Then the following hold, as  $n \rightarrow \infty$ :*

- (i) *If  $t/n \rightarrow T$ , then  $F(Y_{n,\theta}^{r,t}) \rightarrow h(T)$ .*
- (ii) *If  $t/(2n) \rightarrow T$ , then  $F(N(Y_{n,\theta})^{r,t}) \rightarrow h(T)$ .*
- (iii) *If  $t/(4n) \rightarrow T$ , then  $F(P(Y_{n,\theta})^{r,t}) \rightarrow h(T)$ .*

Elementary calculus shows that  $h(T)$  is strictly decreasing on the intervals  $[2, 3]$ ,  $[3, 4]$ ,  $\dots$ , and so one can confine the optimization problem to  $[0, 2]$ , where it is not hard to show that the global maximum of  $h(T)$  is unique and is attained for  $T = 1.115749 \dots$ , which is the middle root of  $x^3 - 12x + 12$ . The maximum value attained there is

$$F_b = 3.342065 \dots, \text{ the largest root of } 7x^3 - 33x^2 + 33x - 3.$$

We find it rather curious that, if  $(R_a, T_a)$  is the pair  $(R, T)$  that maximizes  $g(R, T)$  and  $T_b$  is the  $T$  that maximizes  $h(T)$ , then the algebraic numbers

$$g(R_a, T_a) - 6 = 0.342061 \dots$$

<sup>2</sup>The *m-sequences* associated with  $\theta$  are the  $n$  cyclic permutations of this Galois sequence. Their corresponding polynomials are  $Y_{n,\theta}^{r,n}$  for  $r = 0, 1, \dots, n-1$ , all of which we handle in Theorem 2.2.

and

$$h(T_b) - 3 = 0.342065\dots$$

are distinct, but first differ in only the sixth decimal place. Likewise, the algebraic numbers

$$T_a - 1 = 0.057827\dots$$

and

$$\frac{1}{2}(T_b - 1) = 0.057874\dots$$

are distinct, but first differ in only the fifth decimal place.

Our third main result is a far-reaching generalization of Theorem 2.1. For  $j$  an integer and  $n$  a positive odd integer, the *Jacobi symbol*  $(j|n)$  extends the Legendre symbol via  $(j|1) = 1$  and  $(j|n_1)(j|n_2) = (j|n_1n_2)$  for positive odd integers  $n_1, n_2$ . For  $n$  a positive odd square-free integer, the coefficient sequence of

$$X_n(z) = \sum_{j=0}^{n-1} (j | \frac{n}{\gcd(j,n)}) z^j$$

is a binary sequence called the *Jacobi sequence* of length  $n$ . When  $n$  is prime, then  $X_n$  is the Legendre sequence of length  $n$ .

We denote by  $\omega(n)$  and  $\kappa(n)$  the number of distinct prime divisors of  $n$  and the smallest prime divisor of  $n$ , respectively. Then the merit factor for Jacobi sequences, and their negaperiodic and periodic versions, has the same asymptotic form as that for Legendre sequences as presented in Theorem 2.1.

**Theorem 2.3.** *Let  $n > 1$  take values in an infinite set of positive odd square-free integers such that*

$$(2.4) \quad \frac{\max(4^{\omega(n)}(\log n)^6, 5^{\omega(n)})}{\kappa(n)} \rightarrow 0 \quad \text{as } n \rightarrow \infty.$$

*Let  $X_n$  be the Jacobi sequence of length  $n$  and let  $R$  and  $T > 0$  be real. Then the following hold, as  $n \rightarrow \infty$ .*

- (i) *If  $r/n \rightarrow R$  and  $t/n \rightarrow T$ , then  $F(X_n^{r,t}) \rightarrow g(R, T)$ .*
- (ii) *If  $r/(2n) \rightarrow R$  and  $t/(2n) \rightarrow T$ , then  $F(N(X_n)^{r,t}) \rightarrow g(R + \frac{1}{4}, T)$ .*
- (iii) *If  $r/(4n) \rightarrow R$  and  $t/(4n) \rightarrow T$ , then  $F(P(X_n)^{r,t}) \rightarrow g(R, T)$ .*

In the special case where each  $n$  is prime, Theorem 2.3 reduces to Theorem 2.1.

The following corollary is an immediate consequence of Theorem 2.3, and the fact that  $(j|d) = (-j|d)$  when  $d \equiv 1 \pmod{4}$ .

**Corollary 2.4.** *Let  $n > 1$  take values in an infinite set of positive odd square-free integers such that each prime divisor of  $n$  is congruent to 1 modulo 4 and such that*

$$\frac{\max(4^{\omega(n)}(\log n)^6, 5^{\omega(n)})}{\kappa(n)} \rightarrow 0 \quad \text{as } n \rightarrow \infty.$$

*Let  $X_n$  be the Jacobi sequence of length  $n$ . Then the coefficient sequence of each of the polynomials  $N(X_n)^{n-s, 2s+1}$  and  $P(X_n)^{n-s, 2s+1}$  is skew-symmetric for each nonnegative integer  $s$ , and for real  $T > 0$  the following hold, as  $n \rightarrow \infty$ :*

- (i) *If  $s/n \rightarrow T$ , then  $F(N(X_n)^{n-s, 2s+1}) \rightarrow g(\frac{1}{4} - \frac{T}{2}, T)$ .*
- (ii) *If  $s/(2n) \rightarrow T$ , then  $F(P(X_n)^{n-s, 2s+1}) \rightarrow g(\frac{1}{4} - \frac{T}{2}, T)$ .*

Since the global maximum  $F_a$  of  $g(R, T)$  (see (2.2)) occurs when  $R = \frac{1}{4} - \frac{T}{2}$ , Corollary 2.4 shows that the largest known asymptotic merit factor for a family of binary sequences can be achieved by families of skew-symmetric binary sequences. This is of particular interest in view of Golay's conjecture (see the final paragraph of Section 1).

The rest of the paper is organized as follows. Section 3 describes some consequences of our results, including the resolution of several conjectures, the explanation of numerical evidence due to other authors, and the encompassing of numerous special cases that have previously appeared in scattered form. Section 4 presents our general method for calculating the asymptotic merit factor of a family of binary sequences and their negaperiodic and periodic versions. Section 5 applies this method to Legendre and Galois sequences to establish Theorems 2.1 and 2.2, respectively, using estimates on character sums. Section 6 extends the analysis for Legendre sequences to Jacobi sequences and so proves Theorem 2.3, using counting results for lattice points in polyhedra. (We have chosen to present the proof of Theorem 2.1 separately, even though it is a special case of Theorem 2.3, in order to introduce ideas progressively and maintain clarity of explanation.) Section 7 discusses what underlies the negaperiodic and periodic constructions, extends the results of the paper to other binary sequence families, and proposes conjectures for the asymptotic merit factor behavior of two further binary sequence families.

### 3. RELATIONSHIP TO PREVIOUS RESULTS

The results where  $T \neq 1$  in Theorem 2.1 (ii), (iii), Theorems 2.2 and 2.3, and Corollary 2.4 are all new, and prove various conjectures posed in the literature. Theorem 2.1 (ii) shows how  $N(X_p)^{r,t}$  can achieve an asymptotic merit factor  $F_a$ , as defined in (2.2), proving a conjecture due to Parker [42, Conjecture 4], and how  $N(X_p)^{0,t}$  can achieve an asymptotic merit factor greater than 6.17, explaining numerical results presented by Xiong and Hall [49, Section VI]. Theorem 2.1 (iii) shows how  $P(X_p)^{r,t}$  can achieve an asymptotic merit factor  $F_a$ , proving a conjecture due to Yu and Gong [52,

Conjecture 3]. Theorem 2.2 (i) proves the conjecture of Jedwab and Schmidt [27, Conjecture 9, Corollary 10] that for all  $\theta$  and  $r$ , the asymptotic merit factor of  $Y_{n,\theta}^{r, \lfloor nT \rfloor}$  is  $h(T)$  when  $0 < T \leq 2$ . Theorem 2.3 (i) shows how  $X_n^{r,t}$  can attain an asymptotic merit factor  $F_a$  for composite  $n$ , explaining numerical evidence reported by Parker [42, p. 82].

Various special cases of Theorems 2.1, 2.2, 2.3, and Corollary 2.4 have appeared in scattered form in the literature. The case  $T = 1$  of Theorem 2.1 (i) implies that  $X_p^{r,p}$  has asymptotic merit factor  $g(R, 1)$  if  $r/p \rightarrow R$  as  $p \rightarrow \infty$ . Since

$$\frac{1}{g(R, 1)} = \frac{1}{6} + 8\left(R - \frac{1}{4}\right)^2 \quad \text{for } 0 \leq R \leq \frac{1}{2},$$

the maximum asymptotic merit factor that can be attained in this way is  $g(\frac{1}{4}, 1) = 6$ . This was proved by Høholdt and Jensen [20]. Theorem 2.1 (i) was proved for general  $R$  and  $T$  by the present authors [26].

The case  $T = 1$  of Theorem 2.1 (ii) implies that  $N(X_p)^{\lfloor 2pR \rfloor, 2p}$  has asymptotic merit factor  $g(R + \frac{1}{4}, 1)$ , and so the largest asymptotic merit factor that can be attained in this way is 6. Xiong and Hall [49, Theorem 3.3] proved this result for  $R = 0$ . Schmidt, Jedwab, and Parker [44, Theorem 5] then proved the result for general  $R$ . The case  $T = 1$  of Theorem 2.1 (iii) shows that  $P(X_p)^{\lfloor 4pR - p \rfloor, 4p}$  also has asymptotic merit factor  $g(R + \frac{1}{4}, 1)$ , as was proved by Schmidt, Jedwab, and Parker [44, Theorem 8].

The case  $T = 1$  of Theorem 2.2 (i) implies that  $Y_{n,\theta}^{r,n}$  has asymptotic merit factor  $h(1) = 3$  for all  $\theta$  and  $r$ . This was proved by Jensen and Høholdt [30, Section 5] (see also Jensen, Jensen, and Høholdt [31, Theorem 2.2]). The case  $T = 1$  of Theorem 2.2 (ii) and (iii) implies a corresponding result for  $N(Y_{n,\theta})^{r, 2n}$  and  $P(Y_{n,\theta})^{r, 4n}$ , respectively, which was proved by Jedwab and Schmidt [28, Theorems 11 and 12]. Jedwab and Schmidt [27, Corollary 7] proved that, for  $1 \leq T \leq 2$  and for all  $\theta$ , there is a choice of  $r$  for each  $n$  such that the infimum limit of  $F(Y_{n,\theta}^{r, \lfloor nT \rfloor})$  is at least  $h(T)$ . The question as to whether the limit of  $F(Y_{n,\theta}^{r, \lfloor nT \rfloor})$  equals  $h(T)$  for all choices of  $\theta$  and  $r$  was left as an open problem [27, Section 5] and is answered in the affirmative by Theorem 2.2 (i).

The case  $T = 1$  of Theorem 2.3 (i) was proved by Jedwab and Schmidt [29, Theorem 2.5] under conditions on the growth rate of  $\omega(n)$  that are different from (2.4). The case  $T = 1$  of Theorem 2.3 (ii) was proved by Xiong and Hall [49, Theorem 5.2] for  $n = pq$  and  $R = 0$ , where  $p$  and  $q$  are odd primes satisfying  $p \equiv q \equiv 1 \pmod{4}$ , under a more restrictive condition than (2.4). The case  $T = 1$  of Corollary 2.4 implies that, for  $n \equiv 1 \pmod{4}$ , both  $N(X_n)^{0, 2n+1}$  and  $P(X_n)^{-n, 4n+1}$  are skew-symmetric binary sequences, each having asymptotic merit factor 6. This was proved by Schmidt, Jedwab, and Parker for prime  $n$  [44, Corollaries 6 and 9].



## 4. ASYMPTOTIC MERIT FACTOR CALCULATION

Let  $A$  be a binary sequence of length  $n$  with associated polynomial  $A(z)$  and write  $\epsilon_k = e^{2\pi ik/n}$ . It turns out that  $F(A^{r,t})$ ,  $F(N(A)^{r,t})$ , and  $F(P(A)^{r,t})$  depend only on the function  $L_A$  defined, for  $a, b, c \in \mathbb{Z}/n\mathbb{Z}$ , by

$$L_A(a, b, c) = \frac{1}{n^3} \sum_{k \in \mathbb{Z}/n\mathbb{Z}} A(\epsilon_k) A(\epsilon_{k+a}) \overline{A(\epsilon_{k+b}) A(\epsilon_{k+c})}.$$

In the following two theorems, we shall determine the asymptotic behavior of  $F(A^{r,t})$ ,  $F(N(A)^{r,t})$ , and  $F(P(A)^{r,t})$  when  $L_A$  approximates either of the functions  $I_n$  and  $J_n$  defined, for  $a, b, c \in \mathbb{Z}/n\mathbb{Z}$ , by

$$I_n(a, b, c) = \begin{cases} 1 & \text{if one of } a, b, c \text{ is zero and the other two are equal,} \\ 0 & \text{otherwise,} \end{cases}$$

and

$$J_n(a, b, c) = \begin{cases} 1 & \text{if } (c = a \text{ and } b = 0) \text{ or } (a = b \text{ and } c = 0), \\ 0 & \text{otherwise.} \end{cases}$$

In Section 5, we shall establish that the error of this approximation for  $L_A$  vanishes asymptotically for Legendre and Galois sequences, thereby proving Theorems 2.1 and 2.2. We shall make repeated use of the elementary counting identities

$$(4.1) \quad \sum_{0 \leq j, j+u < t} 1 = \max(0, t - |u|),$$

$$(4.2) \quad \sum_{0 \leq j, u-j < t} 1 = \max(0, t - |t - 1 - u|).$$

**Theorem 4.1.** *Let  $n$  take values in an infinite set of positive integers. For each  $n$ , let  $V_n$  be a binary sequence of length  $n$  and suppose that, as  $n \rightarrow \infty$ ,*

$$(4.3) \quad (\log n)^3 \max_{a, b, c \in \mathbb{Z}/n\mathbb{Z}} |L_{V_n}(a, b, c) - I_n(a, b, c)| \rightarrow 0.$$

*Let  $R$  and  $T > 0$  be real. Then the following hold, as  $n \rightarrow \infty$ :*

- (i) *If  $r/n \rightarrow R$  and  $t/n \rightarrow T$ , then  $F(V_n^{r,t}) \rightarrow g(R, T)$ .*
- (ii) *If each  $n$  is odd,  $r/(2n) \rightarrow R$ , and  $t/(2n) \rightarrow T$ , then  $F(N(V_n)^{r,t}) \rightarrow g(R + \frac{1}{4}, T)$ .*
- (iii) *If each  $n$  is odd,  $r/(4n) \rightarrow R$ , and  $t/(4n) \rightarrow T$ , then  $F(P(V_n)^{r,t}) \rightarrow g(R, T)$ .*

*Proof.* Let  $V_n(z) = \sum_{j=0}^{n-1} v_{n,j} z^j$  be the polynomial associated with  $V_n$  and write  $v_{n,j+n} = v_{n,j}$  for all  $j$ . We treat the three parts of the theorem together by letting the binary sequence  $U_n$  be one of  $V_n$ ,  $N(V_n)$ , or  $P(V_n)$ . In all three

parts,  $U_n$  can be written in polynomial form as

$$U_n(z) = \sum_{j=0}^{sn-1} w_j v_{n,j} z^j,$$

where  $s \in \{1, 4\}$  and  $w_j \in \{-1, 1\}$  for all  $j$ . After elementary manipulations, we find from (1.1) that  $1 + 1/F(U_n^{r,t})$  equals

$$(4.4) \quad \frac{1}{t^2} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} (w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r}) (v_{n, j_1+r} v_{n, j_2+r} v_{n, j_3+r} v_{n, j_4+r}).$$

Write  $\epsilon_k = e^{2\pi i k/n}$ . It is readily verified that, for all integers  $j$ ,

$$v_{n,j} = \frac{1}{n} \sum_{k \in \mathbb{Z}/n\mathbb{Z}} V_n(\epsilon_k) \epsilon_k^{-j}.$$

A straightforward calculation then shows that, if  $j_1, j_2, j_3, j_4$  are integers satisfying  $j_1 + j_2 = j_3 + j_4$ , then

$$(4.5) \quad v_{n, j_1} v_{n, j_2} v_{n, j_3} v_{n, j_4} = \frac{1}{n} \sum_{a, b, c \in \mathbb{Z}/n\mathbb{Z}} L_{V_n}(a, b, c) \epsilon_a^{-j_2} \epsilon_b^{j_3} \epsilon_c^{j_4}.$$

Note that  $I_n(a, b, c)$  approximates  $L_{V_n}(a, b, c)$  via (4.3). Consider three cases for the tuple  $(a, b, c) \in \mathbb{Z}/n\mathbb{Z}$ : (1)  $c = a$  and  $b = 0$ , (2)  $a = b$  and  $c = 0$ , and (3)  $b = c$  and  $a = 0$ . Then  $I_n(a, b, c) = 1$  if at least one of these conditions is satisfied, and  $I_n(a, b, c) = 0$  otherwise. The only tuple  $(a, b, c)$  that satisfies more than one of these conditions is  $(0, 0, 0)$ . We now substitute (4.5) into (4.4) and reorganize (4.4) by writing  $L_{V_n}(a, b, c)$  as  $I_n(a, b, c)$  plus an error term, and then break the sum involving  $I_n(a, b, c)$  into four parts: three sums corresponding to the three cases, and a fourth sum to correct for the triple counting of  $(a, b, c) = (0, 0, 0)$ . We keep the sum  $E$  over the error term entire, and thus have

$$\frac{1}{F(U_n^{r,t})} = -1 + A + B + C - 2D + E,$$

where

$$\begin{aligned} A &= \frac{1}{t^2 n} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \sum_{a \in \mathbb{Z}/n\mathbb{Z}} \epsilon_a^{j_4 - j_2}, \\ B &= \frac{1}{t^2 n} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \sum_{b \in \mathbb{Z}/n\mathbb{Z}} \epsilon_b^{j_3 - j_2}, \\ C &= \frac{1}{t^2 n} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \sum_{c \in \mathbb{Z}/n\mathbb{Z}} \epsilon_c^{j_3 + j_4 + 2r}, \end{aligned}$$

$$\begin{aligned}
D &= \frac{1}{t^2 n} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r}, \\
E &= \frac{1}{t^2 n} \sum_{a, b, c \in \mathbb{Z}/n\mathbb{Z}} [L_{V_n}(a, b, c) - I_n(a, b, c)] \epsilon_{-a+b+c}^t \\
&\quad \times \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \epsilon_a^{-j_2} \epsilon_b^{j_3} \epsilon_c^{j_4}.
\end{aligned}$$

Notice that  $A = B$  and there are contributions in  $A$  only when  $j_4 = j_2 + mn$  for some  $m \in \mathbb{Z}$ . When this occurs, we also have  $j_1 = j_3 + mn$  since  $j_1 + j_2 = j_3 + j_4$ , so that

$$(4.6) \quad A + B = \frac{2}{t^2} \sum_{m \in \mathbb{Z}} \left( \sum_{0 \leq j, j+mn < t} w_{j+r} w_{j+r+mn} \right)^2.$$

Likewise (using  $j_4 = j_2 + m$  instead of  $j_4 = j_2 + mn$ ), we obtain

$$D = \frac{1}{t^2 n} \sum_{m \in \mathbb{Z}} \left( \sum_{0 \leq j, j+m < t} w_{j+r} w_{j+r+m} \right)^2.$$

Similarly, there are contributions in  $C$  only when  $j_4 = mn - 2r - j_3$  for some  $m \in \mathbb{Z}$ , and therefore

$$(4.7) \quad C = \frac{1}{t^2} \sum_{m \in \mathbb{Z}} \left( \sum_{0 \leq j, mn-2r-j < t} w_{j+r} w_{mn-(j+r)} \right)^2.$$

If  $t/n$  tends to a positive real number as  $n \rightarrow \infty$ , then assumption (4.3), combined with Lemma 4.3 (with  $v_j = w_{j+r}$ ) stated below, implies that  $E \rightarrow 0$ . Thus it remains to determine the asymptotic behavior of the sums  $A + B$ ,  $C$ , and  $D$  for the three parts of the theorem. We shall use the notation  $x_n \sim y_n$  to mean that  $x_n - y_n \rightarrow 0$  as  $n \rightarrow \infty$ .

(i)  $U_n = V_n$ : Here we have  $s = 1$  and  $w_j = 1$  for all  $j$ , and we suppose that  $r/n \rightarrow R$  and  $t/n \rightarrow T$  as  $n \rightarrow \infty$ . Identities (4.1) and (4.2) give

$$\begin{aligned}
A + B &= \frac{2}{t^2} \sum_{m \in \mathbb{Z}} \max(0, t - |m|n)^2, \\
D &= \frac{1}{t^2 n} \sum_{m \in \mathbb{Z}} \max(0, t - |m|)^2, \\
C &= \frac{1}{t^2} \sum_{m \in \mathbb{Z}} \max(0, t - |t - 1 - mn + 2r|)^2,
\end{aligned}$$

and we can then evaluate  $D$  exactly as  $(2t^2 + 1)/(3tn)$ . Then, since  $A + B$  and  $C$  are continuous functions of  $t$  and  $r$ , we obtain  $-1 + A + B + C - 2D \rightarrow 1/g(R, T)$ , as required.

(ii)  $U_n = N(V_n)$ : Here we have  $s = 4$  and  $w_j = (-1)^{j(j-1)/2}$  for all  $j$ , and we suppose that each  $n$  is odd and  $r/(2n) \rightarrow R$  and  $t/(2n) \rightarrow T$  as  $n \rightarrow \infty$ .

Since  $w_{j+2k} = (-1)^k w_j$  for all  $j$ , by (4.1) the contribution to  $A + B$  arising by restricting the outer sum in (4.6) to even  $m$  is

$$\frac{2}{t^2} \sum_{m \in \mathbb{Z}} \max(0, t - 2|m|n)^2.$$

Now, for all  $j$  and for all odd  $u$  we have  $w_j w_{j+u} + w_{j+1} w_{j+1+u} = 0$ , and therefore if  $S$  is a finite set of consecutive integers, we have

$$(4.8) \quad \left| \sum_{j \in S} w_j w_{j+u} \right| \leq 1 \quad \text{for odd } u.$$

The terms in the outer sum of  $A + B$  are zero whenever  $|m|n > t - 1$ , so that the number of nonzero terms in the outer sum of  $A + B$  is bounded by  $1 + 2(t - 1)/n$ . Using (4.8) and the assumption that  $n$  is odd, we then find that the contribution to  $A + B$  arising by restricting the outer sum to odd  $m$  is at most  $2/t^2 + 4/(tn)$ , and therefore

$$A + B \sim \frac{2}{t^2} \sum_{m \in \mathbb{Z}} \max(0, t - 2|m|n)^2.$$

Likewise,

$$D \sim \frac{1}{t^2 n} \sum_{m \in \mathbb{Z}} \max(0, t - 2|m|)^2$$

and therefore  $D \sim t/(3n)$ . We proceed similarly to estimate  $C$ . Here we use that  $w_{1-j} = w_j$  for all  $j$ . It then follows from (4.8) that, if  $S$  is a finite set of consecutive integers, then

$$\left| \sum_{j \in S} w_j w_{u-j} \right| \leq 1 \quad \text{for even } u.$$

We now split the outer sum of  $C$  in (4.7) into sums over odd and even  $m$ , noting that we may neglect contributions arising from the sum over even  $m$  as  $n \rightarrow \infty$ . Since  $w_{2k+1-j} = (-1)^k w_j$  for all  $j$ , by (4.2) this gives

$$C \sim \frac{1}{t^2} \sum_{m \in \mathbb{Z}} \max(0, t - |t - 1 - (2m - 1)n + 2r|)^2.$$

We conclude that  $-1 + A + B + C - 2D \rightarrow 1/g(R + \frac{1}{4}, T)$ , as required.

(iii)  $U_n = P(V_n)$ : Here we have  $s = 4$  and  $w_j = (-1)^{j(j-1)^2/2}$  for all  $j$ , and we suppose that each  $n$  is odd and  $r/(4n) \rightarrow R$  and  $t/(4n) \rightarrow T$  as  $n \rightarrow \infty$ . This can be treated similarly to part (ii). We have  $w_{j+4} = w_j$  and  $\sum_{j=0}^3 w_j w_{j+u} = 0$  for  $u \not\equiv 0 \pmod{4}$ , from which we can conclude by (4.1) that

$$A + B \sim \frac{2}{t^2} \sum_{m \in \mathbb{Z}} \max(0, t - 4|m|n)^2,$$

and

$$D \sim \frac{1}{t^2 n} \sum_{m \in \mathbb{Z}} \max(0, t - 4|m|)^2,$$

so that  $D \sim t/(6n)$ . In order to estimate  $C$ , we use  $w_{-j} = w_j$  and (4.2) to obtain

$$C \sim \frac{1}{t^2} \sum_{m \in \mathbb{Z}} \max(0, t - |t - 1 - 4mn + 2r|)^2.$$

We conclude that  $-1 + A + B + C - 2D \rightarrow 1/g(R, T)$ , as required.  $\square$

**Theorem 4.2.** *Let  $n$  take values in an infinite set of positive integers. For each  $n$ , let  $V_n$  be a binary sequence of length  $n$  and suppose that, as  $n \rightarrow \infty$ ,*

$$(4.9) \quad (\log n)^3 \max_{a, b, c \in \mathbb{Z}/n\mathbb{Z}} |L_{V_n}(a, b, c) - J_n(a, b, c)| \rightarrow 0.$$

*Let  $T > 0$  be real. Then the following hold, as  $n \rightarrow \infty$ :*

- (i) *If  $t/n \rightarrow T$ , then  $F(V_n^{r,t}) \rightarrow h(T)$ .*
- (ii) *If each  $n$  is odd and  $t/(2n) \rightarrow T$ , then  $F(N(V_n)^{r,t}) \rightarrow h(T)$ .*
- (iii) *If each  $n$  is odd and  $t/(4n) \rightarrow T$ , then  $F(P(V_n)^{r,t}) \rightarrow h(T)$ .*

*Proof.* The proof of the theorem is similar to the proof of Theorem 4.1, though slightly simpler. Here we consider only two cases for the tuple  $(a, b, c) \in \mathbb{Z}/n\mathbb{Z}$ : (1)  $c = a$  and  $b = 0$ , and (2)  $a = b$  and  $c = 0$ , so that  $J_n(a, b, c) = 1$  if at least one of these conditions is satisfied and  $J_n(a, b, c) = 0$  otherwise. Letting  $U_n$  be one of the sequences  $V_n$ ,  $N(V_n)$ , or  $P(V_n)$ , we then have

$$\frac{1}{F(U_n^{r,t})} = -1 + A + B - D + E,$$

where  $A$ ,  $B$ , and  $D$  are the same expressions (and have the same asymptotic evaluations) as in the proof of Theorem 4.1, but now

$$E = \frac{1}{t^2 n} \sum_{a, b, c \in \mathbb{Z}/n\mathbb{Z}} [L_{V_n}(a, b, c) - J_n(a, b, c)] e_{-a+b+c}^r \times \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \epsilon_a^{-j_2} \epsilon_b^{j_3} \epsilon_c^{j_4}.$$

The term  $C$  never arises because we have no analogue of case (3) following (4.5) in the proof of the previous theorem; and we subtract  $D$ , rather than  $2D$  as previously, because the tuple  $(a, b, c) = (0, 0, 0)$  is doubly counted in cases (1) and (2) rather than trebly counted. When  $U_n = V_n$ ,  $N(V_n)$ , or  $P(V_n)$ , the proof is completed by observing that, as  $n \rightarrow \infty$ , we have  $-1 + A + B - D \rightarrow 1/h(T)$ , and if  $t/n$  tends to a positive real number then  $E \rightarrow 0$  by the assumption (4.9) and Lemma 4.3.  $\square$

We close this section by proving the result used in the proof of Theorems 4.1 and 4.2, which is similar to Lemma 2.2 of [26] but more widely applicable.

**Lemma 4.3.** *Let  $n$  be a positive integer and write  $\epsilon_k = e^{2\pi ik/n}$ . Let  $s$  be a positive integer coprime to  $n$ , and let  $v_j \in \mathbb{C}$  be such that  $|v_j| \leq 1$  and  $v_{j+s} = v_j$  for all  $j \in \mathbb{Z}$ . Then*

$$\sum_{a,b,c \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} v_{j_1} v_{j_2} v_{j_3} v_{j_4} \epsilon_a^{-j_2} \epsilon_b^{j_3} \epsilon_c^{j_4} \right| \leq 936s^3 \max(n, \lceil t/s \rceil)^3 (1 + \log n)^3.$$

*Proof.* Since  $|v_j| \leq 1$  for all  $j$ , and the value of  $v_j$  depends only on the congruence class of  $j$  modulo  $s$ , the sum to be bounded is at most

$$\sum_{a,b,c \in \mathbb{Z}/n\mathbb{Z}} \sum_{k_2, k_3, k_4=0}^{s-1} \left| \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4 \\ (j_2, j_3, j_4) \equiv (k_2, k_3, k_4) \pmod{s}}} \epsilon_a^{-j_2} \epsilon_b^{j_3} \epsilon_c^{j_4} \right|.$$

Reparameterize the inner sum by  $(j_1, j_2, j_3, j_4) = (i_1, i_2, i_3, i_4)s + (k_3 + k_4 - k_2, k_2, k_3, k_4)$  and  $(x, y, z) = (-a, b, c)s$ . Since  $s$  is coprime to  $n$ , we obtain

$$\sum_{k_2, k_3, k_4=0}^{s-1} \sum_{x,y,z \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{\substack{(i_1, i_2, i_3, i_4) \in I_1 \times I_2 \times I_3 \times I_4 \\ i_1 + i_2 = i_3 + i_4}} \epsilon_x^{i_2} \epsilon_y^{i_3} \epsilon_z^{i_4} \right|,$$

where each of  $I_1, I_2, I_3$ , and  $I_4$  is a set of at most  $\lceil t/s \rceil$  consecutive integers (depending on  $k_2, k_3$ , and  $k_4$ ). Apply Lemma 4.4 to the sum over  $x, y, z$ .  $\square$

**Lemma 4.4.** *Let  $n$  be a positive integer and write  $\epsilon_k = e^{2\pi ik/n}$ . Let each of  $I_1, I_2, I_3, I_4$  be a finite set of at most  $L$  consecutive integers. Then*

$$\sum_{a,b,c \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{\substack{(i_1, i_2, i_3, i_4) \in I_1 \times I_2 \times I_3 \times I_4 \\ i_1 + i_2 = i_3 + i_4}} \epsilon_a^{i_2} \epsilon_b^{i_3} \epsilon_c^{i_4} \right| \leq 936 \max(n, L)^3 (1 + \log n)^3.$$

*Proof.* We may assume that each of the sets  $I_1, I_2, I_3, I_4$  is nonempty, otherwise the result is trivial. By reparameterizing, we may also assume that  $|I_1| \leq |I_2|$  and  $|I_3| \leq |I_4|$ . Translate  $I_1, I_2, I_3$ , and  $I_4$  to sets  $H_1, H_2, H_3$ , and  $H_4$ , respectively, each of whose least element is zero. Then for some  $\lambda \in \mathbb{Z}$  the sum to be bounded is

$$(4.10) \quad \sum_{a,b,c \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{\substack{(h_1, h_2, h_3, h_4) \in H_1 \times H_2 \times H_3 \times H_4 \\ h_1 + h_2 = h_3 + h_4 + \lambda}} \epsilon_a^{h_2} \epsilon_b^{h_3} \epsilon_c^{h_4} \right|.$$

Set  $u = 2L$ . We may assume that  $|\lambda| < u$ , otherwise the inner sum is empty and the desired bound is immediate.

Let  $H_1 = \{0, 1, \dots, f\}$  and  $H_2 = \{0, 1, \dots, g\}$ ; note that  $0 \leq f \leq g$ . Then for a function  $S$  of two variables, the sum  $\sum_{(h_1, h_2) \in H_1 \times H_2} S(h_1, h_2)$  equals

$$\sum_{v=0}^{f-1} \sum_{h_1=0}^v S(h_1, v - h_1) + \sum_{v=f}^g \sum_{h_1=0}^f S(h_1, v - h_1) + \sum_{v=g+1}^{f+g} \sum_{h_1=v-g}^f S(h_1, v - h_1).$$

The range of each of the three inner sums over  $h_1$  has the form  $ju - w \leq h_1 \leq kv + x$ , where  $w \in \{0, |H_2| - 1\}$ ,  $x \in \{0, |H_1| - 1\}$ , and  $j, k \in \{0, 1\}$ . Apply the same rationale to sums over  $(h_3, h_4) \in H_3 \times H_4$  to break the inner sum of (4.10) into nine sums (some of which may be empty), each of the form

$$\sum_{v \in V} \sum_{h_1 = ju - w}^{kv + x} \sum_{h_3 = \ell(v - \lambda) - \beta}^{m(v - \lambda) + \gamma} \epsilon_a^{v - h_1} \epsilon_b^{h_3} \epsilon_c^{v - \lambda - h_3}$$

where  $V$  is a set of consecutive integers in  $[0, u)$ , the integers  $w, x, \beta, \gamma$  satisfy  $0 \leq w + x < u$  and  $0 \leq \beta + \gamma < u$ , and  $j, k, \ell, m \in \{0, 1\}$ . By the triangle inequality and some reparameterization, it suffices to show that

$$G = \sum_{a, b, c \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{v \in V} \sum_{h_1 = ju - w}^{kv + x} \sum_{h_3 = \ell v - y}^{mv + z} \epsilon_a^v \epsilon_b^{h_1} \epsilon_c^{h_3} \right|$$

is at most  $104 \max(n, L)^3 (1 + \log n)^3$ , where  $V$  is a set of consecutive integers lying in  $[0, u)$ , the integers  $w, x, y, z$  satisfy  $0 \leq w + x < u$  and  $|y + z| < 2u$ , and  $j, k, \ell, m \in \{0, 1\}$ .

Now separate  $G$  into four sums according to whether each of  $b$  and  $c$  is 0 to obtain  $G = G_1 + G_2 + G_3 + G_4$ , where

$$\begin{aligned} G_1 &= \sum_{\substack{a, b, c \in \mathbb{Z}/n\mathbb{Z} \\ b, c \neq 0}} \left| \sum_{v \in V} \frac{\epsilon_a^v (\epsilon_b^{ju - w} - \epsilon_b^{x + kv}) (\epsilon_c^{\ell v - y} - \epsilon_c^{z + mv})}{(1 - \epsilon_b)(1 - \epsilon_c)} \right|, \\ G_2 &= \sum_{\substack{a, b \in \mathbb{Z}/n\mathbb{Z} \\ b \neq 0}} \left| \sum_{v \in V} ((y + z + 1) + (m - \ell)v) \frac{\epsilon_a^v (\epsilon_b^{ju - w} - \epsilon_b^{x + kv})}{1 - \epsilon_b} \right|, \\ G_3 &= \sum_{\substack{a, c \in \mathbb{Z}/n\mathbb{Z} \\ c \neq 0}} \left| \sum_{v \in V} ((w + x + 1) + (k - j)v) \frac{\epsilon_a^v (\epsilon_c^{\ell v - y} - \epsilon_c^{z + mv})}{1 - \epsilon_c} \right|, \\ G_4 &= \sum_{a \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{v \in V} ((w + x + 1) + (k - j)v) ((y + z + 1) - (m - \ell)v) \epsilon_a^v \right|. \end{aligned}$$

By the triangle inequality, the constraints  $|w + x| < u$  and  $|y + z| < 2u$  and  $j, k, \ell, m \in \{0, 1\}$ , and some reparameterization, we have

$$\begin{aligned} G_1 &\leq \sum_{\substack{b, c, d \in \mathbb{Z}/n\mathbb{Z} \\ b, c \neq 0}} \frac{4}{|1 - \epsilon_b| \cdot |1 - \epsilon_c|} \left| \sum_{v \in V} \epsilon_d^v \right|, \\ G_2, G_3 &\leq \sum_{\substack{b, d \in \mathbb{Z}/n\mathbb{Z} \\ b \neq 0}} \frac{1}{|1 - \epsilon_b|} \left( 4u \left| \sum_{v \in V} \epsilon_d^v \right| + 2 \left| \sum_{v \in V} v \epsilon_d^v \right| \right), \end{aligned}$$

$$G_4 \leq \sum_{\substack{a \in \mathbb{Z}/n\mathbb{Z} \\ a \neq 0}} \left( 2u^2 \left| \sum_{v \in V} \epsilon_a^v \right| + 3u \left| \sum_{v \in V} v \epsilon_a^v \right| + \left| \sum_{v \in V} v^2 \epsilon_a^v \right| \right).$$

We next prove by induction on  $h \geq 0$  that, for a set  $V$  of consecutive integers in  $[0, u)$ ,

$$(4.11) \quad \sum_{\substack{a \in \mathbb{Z}/n\mathbb{Z} \\ a \neq 0}} \left| \sum_{v \in V} v^h \epsilon_a^v \right| \leq 2u^h n \log n,$$

For the base case  $h = 0$ , we note that  $|\sum_{v \in V} \epsilon_a^v| \leq 2|1 - \epsilon_a|^{-1}$  and use the standard bound [10, p. 136]

$$(4.12) \quad \sum_{a=1}^{n-1} \frac{1}{|1 - \epsilon_a|} \leq n \log n.$$

For  $h > 0$ , write  $V = \{\sigma, \sigma + 1, \dots, \tau - 1\}$  and note that

$$\sum_{v \in V} v^h \epsilon_a^v = \sum_{i=\sigma}^{\tau-2} \sum_{v=i+1}^{\tau-1} v^{h-1} \epsilon_a^v + \sigma \sum_{v=\sigma}^{\tau-1} v^{h-1} \epsilon_a^v.$$

Apply the triangle inequality and the inductive hypothesis to obtain

$$\sum_{\substack{a \in \mathbb{Z}/n\mathbb{Z} \\ a \neq 0}} \left| \sum_{v \in V} v^h \epsilon_a^v \right| \leq ((\tau - \sigma - 1) + \sigma) 2u^{h-1} n \log n,$$

which completes the proof of (4.11) since  $\tau \leq u$ . From (4.11), we find

$$\sum_{a \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{v \in V} v^h \epsilon_a^v \right| \leq u^{h+1} + 2u^h n \log n,$$

and we apply this and (4.12) to the bounds for  $G_1, G_2, G_3$ , and  $G_4$  to obtain

$$G_1 \leq 4(n \log n)^2(u + 2n \log n)$$

$$G_2, G_3 \leq 4u(n \log n)(u + 2n \log n) + 2n \log n(u^2 + 2un \log n)$$

$$G_4 \leq 2u^2(u + 2n \log n) + 3u(u^2 + 2un \log n) + (u^3 + 2u^2 n \log n).$$

Since  $u = 2L$  and  $G = G_1 + G_2 + G_3 + G_4$ , we conclude that  $G \leq 104 \max(n, L)^3(1 + \log n)^3$  as required.  $\square$

## 5. LEGENDRE AND GALOIS SEQUENCES

At the beginning of Section 4, it was noted one can compute the merit factor of a binary sequence  $A$  of length  $n$  from the function  $L_A$  defined, for  $a, b, c \in \mathbb{Z}/n\mathbb{Z}$ , by

$$L_A(a, b, c) = \frac{1}{n^3} \sum_{k \in \mathbb{Z}/n\mathbb{Z}} A(\epsilon_k) A(\epsilon_{k+a}) \overline{A(\epsilon_{k+b})} \overline{A(\epsilon_{k+c})},$$



where  $\epsilon_k = e^{2\pi ik/n}$ . In this section, we combine Theorem 4.1 with an estimate of  $L_A(a, b, c)$  for Legendre sequences in order to complete the proof of Theorem 2.1, and combine Theorem 4.2 with an estimate of  $L_A(a, b, c)$  for Galois sequences in order to complete the proof of Theorem 2.2.

Theorem 2.1 is obtained by combining the following lemma with Theorem 4.1, taking  $V_n = X_n$  for odd prime  $n$ .

**Lemma 5.1.** *Let  $X_p$  be the Legendre sequence of prime length  $p$ , as defined in (2.1). Then*

$$\max_{a,b,c \in \mathbb{Z}/p\mathbb{Z}} |L_{X_p}(a, b, c) - I_p(a, b, c)| \leq 18p^{-1/2}.$$

*Proof.* For  $\epsilon_k = e^{2\pi ik/p}$ , from (2.1) we have

$$X_p(\epsilon_k) - 1 = \sum_{j=1}^{p-1} (j | p) \epsilon_k^j,$$

which is a quadratic Gauss sum and evaluates to  $i^{(p-1)^2/4} p^{1/2} (k | p)$  [13], [3]. It follows from the multiplicativity of the Legendre symbol that

$$L_{X_p}(a, b, c) = \frac{1}{p} \sum_{x \in \mathbb{F}_p} (x(x+a)(x+b)(x+c) | p) + \Delta,$$

where  $|\Delta| \leq 15p^{-1/2}$ . The Weil bound [48], [35, Theorem 5.41] shows that the sum over  $x$  has magnitude at most  $3p^{1/2}$  when  $x(x+a)(x+b)(x+c)$  is not a square in  $\mathbb{F}_p[x]$ . This polynomial is a square in  $\mathbb{F}_p[x]$  if and only if it either has two distinct double roots, in which case the sum over  $x$  equals  $p-2$ , or else has a quadruple root, in which case the sum is  $p-1$ .  $\square$

Theorem 2.2 is obtained by combining the following lemma with Theorem 4.2, taking  $V_n = Y_{n,\theta}$ .

**Lemma 5.2.** *Let  $Y_{n,\theta}$  be the Galois sequence of length  $n = 2^d - 1$  with respect to a primitive element  $\theta \in \mathbb{F}_{2^d}$ , as defined in (2.3). Then*

$$\max_{a,b,c \in \mathbb{Z}/n\mathbb{Z}} |L_{Y_{n,\theta}}(a, b, c) - J_n(a, b, c)| \leq \frac{(n+1)^{3/2}}{n^2}.$$

*Proof.* Write  $q = 2^d = n+1$  and  $\epsilon_k = e^{2\pi ik/n}$ . Let  $\chi: \mathbb{F}_q^* \rightarrow \mathbb{C}$  be the multiplicative character of order  $q-1$  given by  $\chi(\theta^j) = \epsilon_j$ , so that  $\chi^k(\theta^j) = \epsilon_j^k$ . Then from (2.3),

$$Y_{n,\theta}(\epsilon_k) = \sum_{x \in \mathbb{F}_q^*} \psi(x) \chi^k(x)$$

is a Gauss sum. We use the following facts [35, Theorems 5.11 and 5.12]: (i)  $Y_{n,\theta}(1) = -1$ ; and (ii)  $Y_{n,\theta}(\epsilon_k)$  and  $Y_{n,\theta}(\epsilon_{-k})$  are complex conjugates, each of magnitude  $q^{1/2}$ , when  $k \not\equiv 0 \pmod{n}$ .

Now  $L_{Y_{n,\theta}}(a, b, c)$  can be written as

$$\frac{1}{n^3} \sum_{k \in \mathbb{Z}/n\mathbb{Z}} \sum_{w,x,y,z \in \mathbb{F}_q^*} \psi(w+x+y+z) \chi^k(w) \chi^{k+a}(x) \overline{\chi^{k+b}(y) \chi^{k+c}(z)}.$$

Since  $\sum_{k \in \mathbb{Z}/n\mathbb{Z}} \chi^k(v)$  equals  $n$  for  $v = 1$  and equals zero otherwise, we have

$$L_{Y_{n,\theta}}(a, b, c) = \frac{1}{n^2} \sum_{\substack{w,x,y,z \in \mathbb{F}_q^* \\ wx=yz}} \psi(w+x+y+z) \chi^a(x) \overline{\chi^b(y) \chi^c(z)}.$$

Set  $v = w/y = z/x$ , and separate out terms with  $v = 1$  to obtain

$$L_{Y_{n,\theta}}(a, b, c) = \delta_b \delta_{a-c} + \frac{1}{n^2} \sum_{\substack{v,x,y \in \mathbb{F}_q^* \\ v \neq 1}} \psi((v+1)(x+y)) \chi^{a-c}(x) \chi^{-b}(y) \chi^{-c}(v),$$

where  $\delta_0 = 1$  and  $\delta_u = 0$  for nonzero  $u$ , and we have used the fact that  $\sum_{s \in \mathbb{F}_q^*} \chi^u(s) = n\delta_u$  for  $u \in \mathbb{Z}/n\mathbb{Z}$ . Reparameterize with  $t = (v+1)x$  and  $u = (v+1)y$  to get

$$\begin{aligned} L_{Y_{n,\theta}}(a, b, c) &= \delta_b \delta_{a-c} + \frac{1}{n^2} \sum_{\substack{t,u,v \in \mathbb{F}_q^* \\ v \neq 1}} \psi(t) \psi(u) \chi^{a-c}(t) \chi^{-b}(u) \chi(v^{-c}(v+1)^{b+c-a}), \\ &= \delta_b \delta_{a-c} + \frac{1}{n^2} Y_{n,\theta}(\epsilon_{a-c}) Y_{n,\theta}(\epsilon_{-b}) \sum_{v \in \mathbb{F}_q^* \setminus \{1\}} \chi(v^{-c}(v+1)^{b+c-a}). \end{aligned}$$

Using facts (i) and (ii), we get the explicit evaluation

$$L_{Y_{n,\theta}}(a, b, c) = \begin{cases} 1 + \frac{n-1}{n^2} & \text{if } a = b = c = 0, \\ 1 - \frac{1}{n^2} & \text{if } \{0, a\} = \{b, c\} \text{ and } a \neq 0, \end{cases}$$

which gives the desired result in the case that  $J_n(a, b, c) = 1$ .

Otherwise we have  $\{0, a\} \neq \{b, c\}$  (so that  $J_n(a, b, c) = 0$ ). Then  $\delta_b \delta_{a-c}$  vanishes, and the exponents  $-c$  and  $b+c-a$  in the last sum over  $v$  cannot simultaneously vanish. Thus the Weil bound [48], [35, Theorem 5.41] shows that the sum over  $v$  has magnitude at most  $q^{1/2}$ . This, along with facts (i) and (ii), shows that  $|L_{Y_{n,\theta}}(a, b, c)| \leq \frac{(n+1)^{3/2}}{n^2}$ .  $\square$

## 6. JACOBI SEQUENCES

In this section, we prove Theorem 2.3. We shall give a detailed proof of part (i) of Theorem 2.3, making use of the machinery developed in the proof of Theorem 4.1 together with Lemma 5.1. We shall then describe how to modify the proof to establish parts (ii) and (iii).

The condition (2.4) is given, and we suppose that  $r/n \rightarrow R$  and  $t/n \rightarrow T$  as  $n \rightarrow \infty$ . Let

$$X_n(z) = \sum_{j=0}^{n-1} x_{n,j} z^j$$

be the polynomial associated with the Jacobi sequence of length  $n$  and write  $x_{n,j+n} = x_{n,j}$  for all  $j$ . Let  $P(n)$  be the set of prime divisors of  $n$ , so that  $n = \prod_{p \in P(n)} p$  since  $n$  is square-free. The crucial ingredient of the proof is the representation

$$(6.1) \quad x_{n,j} = \prod_{p \in P(n)} x_{p,j},$$

which is an immediate consequence of the definition of the Jacobi symbol. Then, by the same reasoning as in the beginning of the proof of Theorem 4.1, we find that

$$(6.2) \quad 1 + \frac{1}{F(X_n^{r,t})} = \frac{1}{t^2} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \prod_{p \in P(n)} x_{p, j_1+r} x_{p, j_2+r} x_{p, j_3+r} x_{p, j_4+r}.$$

Also, writing  $\zeta_d = e^{2\pi i/d}$ , we see from (4.5) that, if  $j_1, j_2, j_3, j_4$  are integers satisfying  $j_1 + j_2 = j_3 + j_4$ , then

$$x_{p, j_1} x_{p, j_2} x_{p, j_3} x_{p, j_4} = \frac{1}{p} \sum_{a, b, c \in \mathbb{Z}/p\mathbb{Z}} L_{X_p}(a, b, c) \zeta_p^{-aj_2} \zeta_p^{bj_3} \zeta_p^{cj_4}.$$

Substitute into (6.2) and write  $P(n) = \{p_1, p_2, \dots, p_\ell\}$  (where  $\ell = \omega(n)$  is the number of prime divisors of  $n$ ) to see that  $1 + 1/F(X_n^{r,t})$  equals

$$(6.3) \quad \frac{1}{t^2 n} \sum_{a_1, b_1, c_1 \in \mathbb{Z}/p_1\mathbb{Z}} \cdots \sum_{a_\ell, b_\ell, c_\ell \in \mathbb{Z}/p_\ell\mathbb{Z}} \left( \prod_{k=1}^{\ell} L_{X_{p_k}}(a_k, b_k, c_k) \right) \\ \times \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \prod_{k=1}^{\ell} \zeta_{p_k}^{-a_k(j_2+r)} \zeta_{p_k}^{b_k(j_3+r)} \zeta_{p_k}^{c_k(j_4+r)}.$$

For each  $p \in P(n)$ , write  $L_{X_p}(a, b, c) = I_p(a, b, c) + N_p(a, b, c)$ . From Lemma 5.1, we have

$$\max_{a, b, c \in \mathbb{Z}/p\mathbb{Z}} |N_p(a, b, c)| \leq 18p^{-1/2} \leq 18\kappa(n)^{-1/2}$$

(where  $\kappa(n)$  is the smallest prime divisor of  $n$ ). Henceforth, let  $n \geq n_0$ , where  $n_0$  is the smallest  $n$  such that  $18\kappa(n)^{-1/2} \leq 1$  for all  $n \geq n_0$ . Such an  $n_0$  exists since  $\kappa(n) \rightarrow \infty$ , by (2.4). Then, expanding the first product in (6.3) into  $2^\ell$  terms, all but one of which contains at least one factor

$N_{p_k}(a_k, b_k, c_k)$ , we see that  $1 + 1/F(X_n^{r,t})$  equals

$$(6.4) \quad \frac{1}{t^2 n} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \prod_{p \in P(n)} \sum_{a, b, c \in \mathbb{Z}/p\mathbb{Z}} I_p(a, b, c) \zeta_p^{-a(j_2+r)} \zeta_p^{b(j_3+r)} \zeta_p^{c(j_4+r)},$$

plus an error term whose magnitude is bounded by

$$\frac{18(2^\ell - 1)}{t^2 n \kappa(n)^{1/2}} \sum_{a_1, b_1, c_1 \in \mathbb{Z}/p_1\mathbb{Z}} \cdots \sum_{a_\ell, b_\ell, c_\ell \in \mathbb{Z}/p_\ell\mathbb{Z}} \left| \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \prod_{k=1}^{\ell} \zeta_{p_k}^{-a_k j_2} \zeta_{p_k}^{b_k j_3} \zeta_{p_k}^{c_k j_4} \right|.$$

By the Chinese Remainder Theorem, and replacing  $2^\ell$  by  $2^{\omega(n)}$ , this error term equals

$$(6.5) \quad \frac{18(2^{\omega(n)} - 1)}{t^2 n \kappa(n)^{1/2}} \sum_{a, b, c \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \zeta_n^{-a j_2} \zeta_n^{b j_3} \zeta_n^{c j_4} \right|.$$

Now we turn back to the main term (6.4). Proceeding with three cases for  $(a, b, c)$ , as in the proof of Theorem 4.1, we find that, for integral  $j, k$ , and  $\ell$ ,

$$\frac{1}{p} \sum_{a, b, c \in \mathbb{Z}/p\mathbb{Z}} I_p(a, b, c) \zeta_p^{-a j} \zeta_p^{b k} \zeta_p^{c \ell} = \delta_p(\ell - j) + \delta_p(k - j) + \delta_p(k + \ell) - \frac{2}{p},$$

where, for integral  $m$  and  $j$ ,

$$\delta_m(j) = \begin{cases} 1 & \text{if } m \mid j \\ 0 & \text{otherwise.} \end{cases}$$

Hence, (6.4) equals

$$\frac{1}{t^2} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \prod_{p \in P(n)} \left( \delta_p(j_4 - j_2) + \delta_p(j_3 - j_2) + \delta_p(j_3 + j_4 + 2r) - \frac{2}{p} \right).$$

By expanding the product, this expression can be written as

$$\sum_{[P_0 : P_1 : P_2 : P_3] = P(n)} \frac{(-2)^{|P_0|}}{t^2 P_0^\times} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \delta_{P_1^\times}(j_4 - j_2) \delta_{P_2^\times}(j_3 - j_2) \delta_{P_3^\times}(j_3 + j_4 + 2r),$$

where we write the sum over  $[P_0 : P_1 : P_2 : P_3] = P(n)$  to mean the sum over all ordered partitions of  $P(n)$  into sets  $P_0, P_1, P_2, P_3$ , and where we write  $P_k^\times$  to mean  $\prod_{p \in P_k} p$ . We partition this sum by separating the three summands where  $P_1, P_2$ , or  $P_3$  equals  $P(n)$  and so have

$$\frac{1}{F(X_n^{r,t})} = -1 + A + B + C + D + E,$$

where

$$\begin{aligned}
A &= \frac{1}{t^2} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \delta_n(j_4 - j_2), \\
B &= \frac{1}{t^2} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \delta_n(j_3 - j_2), \\
C &= \frac{1}{t^2} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \delta_n(j_3 + j_4 + 2r), \\
D &= \sum_{\substack{[P_0: P_1: P_2: P_3] = P(n) \\ P_1, P_2, P_3 \neq P(n)}} \frac{(-2)^{|P_0|}}{t^2 P_0^\times} \\
&\quad \times \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \delta_{P_1^\times}(j_4 - j_2) \delta_{P_2^\times}(j_3 - j_2) \delta_{P_3^\times}(j_3 + j_4 + 2r),
\end{aligned}$$

and  $E$  is an error term whose magnitude is bounded by (6.5). The sums  $A$ ,  $B$ , and  $C$  are identical to those in the proof of Theorem 4.1 (i), and  $E \rightarrow 0$  by Lemma 4.3 and (2.4), because  $t/n$  tends to a positive real number. We now show that  $D \rightarrow -4T/3$ , and therefore  $-1 + A + B + C + D \rightarrow 1/g(R, T)$ , which completes the proof of part (i).

Lemma 6.2 (i) (to be proved below) shows that the inner sum of  $D$  equals

$$\frac{2t^3}{3P_1^\times P_2^\times P_3^\times},$$

plus an error term whose magnitude is at most

$$\frac{4572 \max(t, P_1^\times, P_2^\times, P_3^\times)^2 \max(P_1^\times, P_2^\times, P_3^\times)}{P_1^\times P_2^\times P_3^\times}.$$

All partitions involved in the outer sum of  $D$  satisfy  $\max(P_1^\times, P_2^\times, P_3^\times) \leq n/\kappa(n)$ , because none of  $P_1$ ,  $P_2$ , and  $P_3$  equals  $P(n)$ . We further assume that  $n \geq n_1$ , where  $n_1$  is the smallest  $n$  such that  $n/\kappa(n) \leq t$  for all  $n \geq n_1$ . Such an  $n_1$  exists since  $t/n$  tends to a positive real number and  $\kappa(n) \rightarrow \infty$  as  $n \rightarrow \infty$  by (2.4). Therefore  $\max(t, P_1^\times, P_2^\times, P_3^\times) = t$ , and the error term for the inner sum of  $D$  has magnitude at most

$$\frac{4572 t^2 n}{P_1^\times P_2^\times P_3^\times \kappa(n)}.$$

Therefore each summand of the outer sum of  $D$  equals

$$\frac{2t}{3n} (-2)^{|P_0|},$$

plus an error term whose magnitude is at most

$$(6.6) \quad \frac{4572 \cdot 2^{|P_0|}}{\kappa(n)}.$$

Hence  $D$  equals

$$\frac{2t}{3n} \left( \sum_{[P_0:P_1:P_2:P_3]=P(n)} (-2)^{|P_0|} - 3 \right),$$

plus  $4^{\omega(n)} - 3$  error terms each with magnitude at most (6.6). The principal term for  $D$  then evaluates to

$$\frac{2t}{3n} \left( \sum_{j=0}^{\omega(n)} \binom{\omega(n)}{j} 3^j (-2)^{\omega(n)-j} - 3 \right) = -\frac{4t}{3n},$$

which tends to  $-4T/3$ , while the sum over the  $4^{\omega(n)} - 3$  error terms has magnitude smaller than

$$\frac{4572}{\kappa(n)} \sum_{j=0}^{\omega(n)} \binom{\omega(n)}{j} 3^j 2^{\omega(n)-j} = \frac{4572 \cdot 5^{\omega(n)}}{\kappa(n)},$$

which by (2.4) tends to zero as  $n \rightarrow \infty$ . Therefore  $D \rightarrow -4T/3$ , as required.

We now sketch how to prove parts (ii) and (iii). We treat both cases together by letting  $U_n$  be either  $N(X_n)$  or  $P(X_n)$ . The condition (2.4) is given; for part (ii) we suppose that  $r/(2n) \rightarrow R$  and  $t/(2n) \rightarrow T$  as  $n \rightarrow \infty$ , and for part (iii) we suppose that  $r/(4n) \rightarrow R$  and  $t/(4n) \rightarrow T$  as  $n \rightarrow \infty$ . In polynomial form, we have

$$U_n(z) = \sum_{j=0}^{4n-1} w_j \left( \prod_{p \in P(n)} x_{p,j} \right) z^j,$$

where  $w_j = (-1)^{j(j-1)/2}$  for  $U_n = N(X_n)$  and  $w_j = (-1)^{j(j-1)^2/2}$  for  $U_n = P(X_n)$ . Then, proceeding as in the proof of part (i), we arrive at

$$\frac{1}{F(U_n^{r,t})} = -1 + A + B + C + D + E,$$

where

$$\begin{aligned}
A &= \frac{1}{t^2} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \delta_n(j_4 - j_2), \\
B &= \frac{1}{t^2} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \delta_n(j_3 - j_2), \\
C &= \frac{1}{t^2} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \delta_n(j_3 + j_4 + 2r), \\
D &= \sum_{\substack{[P_0:P_1:P_2:P_3]=P(n) \\ P_1, P_2, P_3 \neq P(n)}} \frac{(-2)^{|P_0|}}{t^2 P_0^\times} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \\
&\quad \times \delta_{P_1^\times}(j_4 - j_2) \delta_{P_2^\times}(j_3 - j_2) \delta_{P_3^\times}(j_3 + j_4 + 2r),
\end{aligned}$$

and  $E$  is an error term whose magnitude is, for all sufficiently large  $n$ , bounded by

$$\frac{18(2^{\omega(n)} - 1)}{t^2 n \kappa(n)^{1/2}} \sum_{a, b, c \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \zeta_n^{-aj_2} \zeta_n^{bj_3} \zeta_n^{cj_4} \right|.$$

The sums  $A$ ,  $B$ , and  $C$  are the same as in the corresponding parts of the proof of Theorem 4.1, and  $E \rightarrow 0$  by Lemma 4.3 and (2.4) because  $t/n$  tends to a positive real number. By invoking Lemma 6.2 (ii) and (iii), we can show, by proceeding as in the proof of part (i), that  $D \sim -2t/(3n)$  for  $U_n = N(X_n)$  and  $D \sim -t/(3n)$  for  $U_n = P(X_n)$ , from which parts (ii) and (iii) follow.  $\square$

To prove Lemma 6.2, which was invoked in the proof of Theorem 2.3, we require the following lemma.

**Lemma 6.1.** *Let  $t$  be a nonnegative real number and define the half-open polyhedron*

$$C = \{(x, y, z) \in \mathbb{R}^3 : 0 \leq x, y, z, y + z - x < t\}.$$

*Let  $a$ ,  $b$ , and  $c$  be positive integers of the same parity. Define the lattice*

$$\Lambda = \{(x, y, z) \in \mathbb{Z}^3 : x \equiv y \pmod{a}, x \equiv z \pmod{b}, y \equiv -z \pmod{c}\}$$

*and let  $K$  be a translation of  $\Lambda$ . Then*

$$\left| |K \cap C| - \frac{2t^3}{3abc} \right| \leq \frac{4572 \max(t, a, b, c)^2 \max(a, b, c)}{abc}$$

*if  $a$ ,  $b$ , and  $c$  are odd, and*

$$\left| |K \cap C| - \frac{4t^3}{3abc} \right| \leq \frac{1332 \max(t, a, b, c)^2 \max(a, b, c)}{abc}$$

if  $a$ ,  $b$ , and  $c$  are even.

*Proof.* A standard calculation shows that the volume of  $C$  is  $\text{vol}(C) = 2t^3/3$ . For positive real  $d$ , let  $C_d^-$  be the set of points within  $C$  that are at distance more than  $d$  from the boundary of  $C$ , and let  $C_d^+$  be the set of points lying within  $C$  or no further than distance  $d$  from some point in  $C$ . Then  $C_d^- \subseteq C \subseteq C_d^+$ , and by translating the planes bounding  $C$  inward or outward, it can be shown that

$$(6.7) \quad \text{vol}(C_d^-) \geq \frac{2}{3}(t - 2\sqrt{3}d)^3 \quad \text{and} \quad \text{vol}(C_d^+) \leq \frac{2}{3}(t + 2\sqrt{3}d)^3.$$

Let  $v$  and  $\ell$  be the volume and the largest diagonal of the fundamental parallelepiped of  $\Lambda$ , respectively. Then  $|K \cap C|$  is at least the number of parallelepipeds of  $K$  wholly contained in  $C$ , which is at least the number intersecting  $C_\ell^-$ , so that  $|K \cap C|$  is at least  $\text{vol}(C_\ell^-)/v$ . Likewise,  $|K \cap C|$  is at most the number of parallelepipeds of  $K$  intersecting  $C$ , which is at most the number wholly contained in  $C_\ell^+$ , and so  $|K \cap C|$  is at most  $\text{vol}(C_\ell^+)/v$ .

Now, if  $a$ ,  $b$ , and  $c$  are odd, it is readily verified that  $\Lambda$  is generated by

$$\frac{1}{2}(c+a, c-a, c+a), \quad \frac{1}{2}(c+b, c+b, c-b), \quad (c, c, c),$$

from which we find that  $v = abc$  and (by the triangle inequality)  $\ell \leq 3\sqrt{3} \max(a, b, c)$ , and the result follows from (6.7). On the other hand, if  $a$ ,  $b$ , and  $c$  are even,  $\Lambda$  is generated by

$$\frac{1}{2}(a, -a, a), \quad \frac{1}{2}(b, b, -b), \quad \frac{1}{2}(c, c, c),$$

and  $v = abc/2$  and  $\ell \leq 3\sqrt{3} \max(a, b, c)/2$ .  $\square$

We now prove the lemma that was invoked in the proof of Theorem 2.3.

**Lemma 6.2.** *Let  $r$  be an integer, let  $t$  be a nonnegative integer, and let  $a$ ,  $b$ , and  $c$  be odd positive integers. For some  $w_j$  with  $j \in \mathbb{Z}$ , consider the sum*

$$(6.8) \quad \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} w_{j_1+r} w_{j_2+r} w_{j_3+r} w_{j_4+r} \delta_a(j_4 - j_2) \delta_b(j_3 - j_2) \delta_c(j_3 + j_4 + 2r),$$

where  $\delta_m(j)$  equals 1 if  $m \mid j$  and equals 0 otherwise.

(i) *Let  $S_1(a, b, c)$  be the sum (6.8), where  $w_j = 1$  for all  $j \in \mathbb{Z}$ . Then*

$$\left| S_1(a, b, c) - \frac{2t^3}{3abc} \right| \leq \frac{4572 \max(t, a, b, c)^2 \max(a, b, c)}{abc}.$$

(ii) *Let  $S_2(a, b, c)$  be the sum (6.8), where  $w_j = (-1)^{j(j-1)/2}$  for all  $j \in \mathbb{Z}$ . Then*

$$\left| S_2(a, b, c) - \frac{t^3}{3abc} \right| \leq \frac{42624 \max(t, a, b, c)^2 \max(a, b, c)}{abc}.$$



(iii) Let  $S_3(a, b, c)$  be the sum (6.8), where  $w_j = (-1)^{j(j-1)^2/2}$  for all  $j \in \mathbb{Z}$ . Then

$$\left| S_3(a, b, c) - \frac{t^3}{6abc} \right| \leq \frac{42624 \max(t, a, b, c)^2 \max(a, b, c)}{abc}.$$

*Proof.* For part (i), let  $C$  and  $\Lambda$  be as in Lemma 6.1 and let  $K = \Lambda - (r, r, r)$ . Then

$$S_1(a, b, c) = |K \cap C|,$$

and (i) follows from Lemma 6.1 since  $a$ ,  $b$ , and  $c$  have the same parity.

For parts (ii) and (iii), we claim that when  $h_1 + h_2 = h_3 + h_4$ , the value of  $w_{h_1} w_{h_2} w_{h_3} w_{h_4}$  depends only on the congruence class modulo 4 of  $h_4 - h_2$ ,  $h_3 - h_2$ , and  $h_3 + h_4$ . Indeed, for part (ii) we have

$$w_{h_1} w_{h_2} w_{h_3} w_{h_4} = (-1)^{(h_4 - h_2)(h_3 - h_2)}$$

whenever  $h_1 + h_2 = h_3 + h_4$ , while for part (iii) we have

$$w_{h_1} w_{h_2} w_{h_3} w_{h_4} = \begin{cases} (-1)^{(h_4 - h_2)(h_3 - h_2)/2} & \text{if } (h_4 - h_2)(h_3 - h_2) \text{ is even,} \\ (-1)^{(h_3 + h_4)/2} & \text{otherwise} \end{cases}$$

whenever  $h_1 + h_2 = h_3 + h_4$ . For either part, define  $\sigma: \mathbb{Z}^3 \rightarrow \{-1, 1\}$  so that  $w_{h_1} w_{h_2} w_{h_3} w_{h_4} = \sigma(h_4 - h_2, h_3 - h_2, h_3 + h_4)$  whenever  $h_1 + h_2 = h_3 + h_4$ , and reparameterize (6.8) to obtain

$$(6.9) \quad \sum_{\substack{0 \leq k, \ell, m < 4 \\ m \equiv k + \ell \pmod{2}}} \sigma(k, \ell, m) \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4 \\ j_4 - j_2 \equiv k \pmod{4} \\ j_3 - j_2 \equiv \ell \pmod{4} \\ j_3 + j_4 + 2r \equiv m \pmod{4}}} \delta_a(j_4 - j_2) \delta_b(j_3 - j_2) \delta_c(j_3 + j_4 + 2r).$$

Since  $a$ ,  $b$ , and  $c$  are odd, by the Chinese Remainder Theorem each of the 32 inner sums counts the number of points of some translate of the lattice

$$\Lambda = \{(x, y, z) \in \mathbb{Z}^3 : x \equiv y \pmod{4a}, x \equiv z \pmod{4b}, y \equiv -z \pmod{4c}\}$$

lying within the half-open polyhedron  $C$  defined in Lemma 6.1. By Lemma 6.1, each of these 32 inner sums equals  $t^3/(48abc)$  plus an error term of magnitude at most

$$(6.10) \quad \frac{1332 \max(t, a, b, c)^2 \max(a, b, c)}{abc}.$$

In part (ii),  $\sigma(k, \ell, m)$  equals  $+1$  for 24 of the triples  $(k, \ell, m)$  in the summation and equals  $-1$  for the remaining 8 triples, so (6.9) equals  $t^3/(3abc)$  plus an error term whose magnitude is at most 32 times (6.10). In part (iii),  $\sigma(k, \ell, m)$  equals  $+1$  for 20 of the triples  $(k, \ell, m)$  in the summation and equals  $-1$  for the remaining 12 triples, so (6.9) equals  $t^3/(6abc)$  plus an error term whose magnitude is at most 32 times (6.10).  $\square$

## 7. CLOSING COMMENTS

We close with a discussion of what underlies the negaperiodic and periodic constructions, some generalizations of our results to other binary sequence families involving combinations of Legendre and Galois sequences, and some conjectures on the asymptotic merit factor behavior of two binary sequence families examined by other authors. We hope this will stimulate further research.

**7.1. What underlies the negaperiodic and periodic constructions?**

Let  $V = (v_0, v_1, \dots, v_{n-1})$  and  $W = (w_0, w_1, \dots, w_{s-1})$  be binary sequences of length  $n$  and  $s$ , respectively, and write  $v_{j+n} = v_j$  and  $w_{j+s} = w_j$  for all  $j \in \mathbb{Z}$ . Define the *product sequence* formed from  $V$  and  $W$  to be the length  $ns$  coefficient sequence of

$$(V \otimes W)(z) = \sum_{j=0}^{ns-1} v_j w_j z^j.$$

Then we can write  $V = V \otimes (+)$  and  $N(V) = V \otimes (+, +, -, -)$  and  $P(V) = V \otimes (+, +, -, +)$ , and it is natural to ask whether the methods of this paper can be applied to  $V \otimes W$  when  $W$  is not one of  $(+)$ ,  $(+, +, -, -)$ , and  $(+, +, -, +)$ .

Indeed, it is readily shown that the same method used to prove Theorem 4.2 (ii) for  $N(V)$  can be applied to  $V \otimes W$  for general  $W$ , under the sufficient conditions that  $s$  is even,  $\gcd(n, s) = 1$ , and

$$(7.1) \quad \sum_{j=0}^{s-1} w_j w_{j+u} = \begin{cases} s & \text{for } u \equiv 0 \pmod{s}, \\ -s & \text{for } u \equiv s/2 \pmod{s}, \\ 0 & \text{otherwise.} \end{cases}$$

The sequence  $(+, +, -, -)$  satisfies these conditions, and gives rise to the negaperiodic construction  $N(V) = V \otimes (+, +, -, -)$ . The sequence  $(+, -)$  also satisfies these conditions, but the resulting product sequence  $V \otimes (+, -)$  trivially has the same merit factor properties as  $V$ .<sup>3</sup> Since the existence of a binary sequence satisfying (7.1) for even  $s > 2$  is equivalent to the existence of a  $(s/2, 2, s/2, s/4)$  relative difference set  $R$  in  $\mathbb{Z}/s\mathbb{Z}$  (via the correspondence  $j \in R$  if and only if  $w_j = -1$ ), standard nonexistence results for relative difference sets in cyclic groups show that there are no such binary sequences for even  $s > 4$  [23, Result 4.8], [43, Corollary 6]; see [38, Appendix VI] for a direct proof. Therefore there are no binary sequences  $W$  satisfying the sufficient conditions for  $s > 4$ .

Likewise, the same method used to prove Theorem 4.1 (ii) for  $N(V)$  can be applied to  $V \otimes W$  for general  $W$ , under the same sufficient conditions as

<sup>3</sup>Let  $U = V \otimes (+, -)$ . Then  $U^{r,t}$  arises by negating every other element of  $V^{r,t}$ , so that the aperiodic autocorrelation of  $U^{r,t}$  is obtained from that of  $V^{r,t}$  by negating the values at odd shifts, thus preserving the merit factor.

above together with the additional condition

$$(7.2) \quad w_{k-j} = w_j \quad \text{for all } j \in \mathbb{Z} \text{ and some integer } k.$$

This enlarged set of conditions is satisfied by all the sequences that satisfy the original set of conditions, namely the sequences  $(+, +, -, -)$ ,  $(+, -)$ , and their cyclic shifts.

The same method used to prove Theorem 4.2 (iii) for  $P(V)$  can be applied to  $V \otimes W$  for general  $W$ , under the sufficient conditions that  $\gcd(n, s) = 1$  and

$$(7.3) \quad \sum_{j=0}^{s-1} w_j w_{j+u} = \begin{cases} s & \text{for } u \equiv 0 \pmod{s}, \\ 0 & \text{otherwise.} \end{cases}$$

The sequences  $(+, +, -, +)$  and  $(+)$  satisfy these conditions, and give rise to the periodic construction  $P(V) = V \otimes (+, +, -, +)$  and the trivial construction  $V = V \otimes (+)$ , respectively. The existence of a binary sequence satisfying (7.3) for  $s > 1$  is equivalent to the existence of an  $(s, (s - \sqrt{s})/2, (s - 2\sqrt{s})/4)$ -difference set in  $\mathbb{Z}/s\mathbb{Z}$ , and there are no such binary sequences for  $4 < s < 4 \cdot 11715^2$  [34, Corollary 4.5].

Likewise, the same method used to prove Theorem 4.1 (iii) for  $P(V)$  can be applied to  $V \otimes W$  for general  $W$ , under the same sufficient conditions from the previous paragraph together with the additional condition (7.2). This additional condition constrains the difference set to have multiplier  $-1$ , and a classical nonexistence result on difference set multipliers shows that there are no such sequences for  $s > 4$  [32, Corollary 3.7].

**7.2. Product of Legendre and Galois sequences.** Using the operator  $\otimes$  defined in Section 7.1, we consider product sequences involving Legendre and Galois sequences. As previously, we write  $X_p$  for the Legendre sequence of length  $p$ , and  $Y_{n,\theta}$  for the Galois sequence of length  $n = 2^d - 1$  with respect to a primitive  $\theta \in \mathbb{F}_{2^d}$ .

Let  $P$  be a set of odd primes, and let  $M$  be a set of Mersenne numbers (having the form  $2^d - 1$  for integral  $d$ ) such that  $P$  and  $M$  are disjoint and the elements of  $P \cup M$  are pairwise coprime. For each  $2^d - 1 \in M$ , choose a primitive element  $\theta \in \mathbb{F}_{2^d}$  and consider the product sequence

$$(7.4) \quad \left( \bigotimes_{p \in P} X_p \right) \otimes \left( \bigotimes_{n \in M} Y_{n,\theta} \right)$$

of length  $(\prod_{p \in P} p)(\prod_{n \in M} n)$ . If  $M$  is empty, then by (6.1) the product sequence (7.4) is a Jacobi sequence and its asymptotic merit factor behavior is the same as that of a Legendre sequence (see Theorem 2.3). Otherwise, the product sequence involves at least one Galois sequence. In that case, a straightforward (albeit notationally cumbersome) generalization of the proof of Theorem 2.3 shows that, under suitable conditions on the growth rate of  $|P \cup M|$  and  $\min(P \cup M)$ , the asymptotic merit factor behavior of the product

sequence (7.4) and its negaperiodic and periodic versions is the same as that of a Galois sequence (see Theorem 2.2).

**7.3. Gordon-Mills-Welch sequences and Sidelnikov sequences.** Let  $F = \mathbb{F}_{2^d}$  be the finite field with  $2^d$  elements and let  $K$  be a subfield of  $F$  of size  $2^k$  (so that  $k$  divides  $d$ ). The *relative trace*  $\text{Tr}_{F/K} : F \rightarrow K$  is given by

$$\text{Tr}_{F/K}(y) = \sum_{j=0}^{d/k-1} y^{2^{jk}}.$$

Let  $\psi$  be the canonical additive character of  $K$ , let  $\theta$  be a primitive element of  $F$ , and let  $\ell$  be an integer coprime to  $2^k - 1$ . The coefficient sequence of the polynomial

$$\sum_{j=0}^{n-1} \psi(\text{Tr}_{F/K}(\theta^j)^\ell) z^j$$

is called a *Gordon-Mills-Welch sequence* of length  $n = 2^d - 1$  [45] with respect to  $\theta$ ,  $k$ ,  $\ell$ . The special case  $\ell = 1$  reduces to a Galois sequence. In 1991, Jensen, Jensen and Høholdt asked how the asymptotic merit factor of a Gordon-Mills-Welch sequence behaves [31]. Based on numerical evidence, we conjecture that the generalization from a Galois sequence to a Gordon-Mills-Welch sequence does not affect the asymptotic merit factor, and that the same holds for the negaperiodic and periodic versions of these sequences.

**Conjecture 7.1.** *For each  $n = 2^d - 1$ , choose a primitive  $\theta \in \mathbb{F}_{2^d}$ , and  $k$  dividing  $d$ , and  $\ell$  coprime to  $2^k - 1$ . Then the asymptotic merit factor of the Gordon-Mills-Welch sequence of length  $n$  (and its negaperiodic and periodic versions) with respect to  $\theta$ ,  $k$ ,  $\ell$  is the same as that of a Galois sequence as specified in Theorem 2.2.*

Now let  $q$  be an odd prime power, and let  $\theta$  be a primitive element of  $\mathbb{F}_q$ . Let  $\eta : \mathbb{F}_q \rightarrow \{1, -1\}$  be the quadratic character on the nonzero elements of  $\mathbb{F}_q$ , and extend  $\eta$  (in a nonstandard way) via  $\eta(0) = 1$ . The coefficient sequence of the polynomial

$$Z_{n,\theta}(z) = \sum_{j=0}^{q-2} \eta(\theta^j + 1) z^j$$

is called a *Sidelnikov sequence* of length  $q - 1$  with respect to  $\theta$  [47]. Based on numerical evidence, we conjecture that the asymptotic merit factor of a Sidelnikov sequence is the same as that of a Galois sequence as specified in

Theorem 2.2 (i).<sup>4</sup> (Since the length of a Sidelnikov sequence is even, there is no negaperiodic or periodic version to consider.)

**Conjecture 7.2.** *For each odd prime power  $q$ , choose an integer  $r$  and a primitive  $\theta \in \mathbb{F}_q$ , and let  $Z_{n,\theta}$  be the Sidelnikov sequence of length  $n = q - 1$  with respect to  $\theta$ . Let  $T > 0$  be real. If  $t/n \rightarrow T$  as  $n \rightarrow \infty$ , then  $F(Z_{n,\theta}^{r,t}) \rightarrow h(T)$  as  $n \rightarrow \infty$ .*

## REFERENCES

- [1] 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.
- [2] J. Bernasconi, *Low autocorrelation binary sequences: statistical mechanics and configuration state analysis*, J. Physique **48** (1987), 559–567.
- [3] B. C. Berndt and R. J. Evans, *The determination of Gauss sums*, Bull. Amer. Math. Soc. (N.S.) **5** (1981), 107–129.
- [4] P. Borwein, *Computational excursions in analysis and number theory*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, 10, Springer-Verlag, New York, 2002.
- [5] P. Borwein and K.-K. S. Choi, *Merit factors of character polynomials*, J. London Math. Soc. **61** (2000), 706–720.
- [6] ———, *Merit factors of polynomials formed by Jacobi symbols*, Canad. J. Math. **53** (2001), 33–50.
- [7] ———, *Explicit merit factor formulae for Fekete and Turyn polynomials*, Trans. Amer. Math. Soc. **354** (2002), 219–234.
- [8] P. Borwein, K.-K. S. Choi, and J. Jedwab, *Binary sequences with merit factor greater than 6.34*, IEEE Trans. Inf. Theory **50** (2004), 3234–3249.
- [9] P. Borwein and M. Mossinghoff, *Rudin-Shapiro-like polynomials in  $L_4$* , Math. Comp. **69** (2000), 1157–1166.
- [10] H. Davenport, revised by H. L. Montgomery, *Multiplicative number theory*, third ed., Springer-Verlag, New York, 2000.
- [11] P. Erdős, *Some unsolved problems*, Michigan Math. J. **4** (1957), 291–300.
- [12] ———, *An inequality for the maximum of trigonometric polynomials*, Ann. Polon. Math. **12** (1962), 151–154.
- [13] C. F. Gauss, *Summatio quarundam serierum singularium*, Comment. Soc. Reg. Sci. Gottingensis **1** (1811).
- [14] M. J. E. Golay, *A class of finite binary sequences with alternate autocorrelation values equal to zero*, IEEE Trans. Inf. Theory **IT-18** (1972), 449–450.
- [15] ———, *Sieves for low autocorrelation binary sequences*, IEEE Trans. Inf. Theory **IT-23** (1977), 43–51.
- [16] ———, *The merit factor of long low autocorrelation binary sequences*, IEEE Trans. Inf. Theory **IT-28** (1982), 543–549.
- [17] ———, *The merit factor of Legendre sequences*, IEEE Trans. Inf. Theory **29** (1983), 934–936.
- [18] K. G. Hare and S. Yazdani, *Fekete-like polynomials*, J. Number Theory **130** (2010), 2198–2213.

---

<sup>4</sup>Huo [22] presents numerical evidence suggesting that the merit factor of the nonbinary analogues of the Sidelnikov sequences (which use multiplicative characters of higher order in place of the quadratic character) might also have the same asymptotic behavior. In their paper on Fekete-like polynomials, Hare and Yazdani [18] present numerical evidence suggesting that a particular cyclic shift of a Sidelnikov sequence (namely the coefficient sequence of  $\sum_{j=0}^{q-2} \eta(\theta^j - 1)z^j$ ) has asymptotic merit factor 3.

- [19] T. Høholdt, *The merit factor problem for binary sequences*, Applied algebra, algebraic algorithms and error-correcting codes, Lecture Notes in Comput. Sci., vol. 3857, Springer, Berlin, 2006, pp. 51–59.
- [20] T. Høholdt and H. E. Jensen, *Determination of the merit factor of Legendre sequences*, IEEE Trans. Inf. Theory **34** (1988), 161–164.
- [21] T. Høholdt, H. E. Jensen, and J. Justesen, *Aperiodic correlations and the merit factor of a class of binary sequences*, IEEE Trans. Inf. Theory **IT-31** (1985), 549–552.
- [22] F. Huo, *Sequences design for OFDM and CDMA systems*, Master’s thesis, University of Waterloo, 2011.
- [23] J. Jedwab, *Generalized perfect arrays and Menon difference sets*, Des. Codes Cryptogr. **2** (1992), 19–68.
- [24] J. Jedwab, *A survey of the merit factor problem for binary sequences*, Proc. of Sequences and Their Applications, Lecture Notes in Comput. Sci., vol. 3486, New York: Springer Verlag, 2005, pp. 30–55.
- [25] J. Jedwab, *What can be used instead of a Barker sequence?*, Finite fields and applications, Contemp. Math., vol. 461, Amer. Math. Soc., Providence, RI, 2008, pp. 153–178.
- [26] J. Jedwab, D. J. Katz, and K.-U. Schmidt, *Littlewood polynomials with small  $L^4$  norm*, arXiv:1205.0260v1 [math.NT] (2011).
- [27] J. Jedwab and K.-U. Schmidt, *Appended  $m$ -sequences with merit factor greater than 3.34*, Sequences and Their Applications (C. Carlet and A. Pott, eds.), Lecture Notes in Comput. Sci., vol. 6338, Springer, 2010, pp. 204–216.
- [28] J. Jedwab and K.-U. Schmidt, *The merit factor of binary sequence families constructed from  $m$ -sequences*, Finite fields: theory and applications, Contemp. Math., vol. 518, Amer. Math. Soc., Providence, RI, 2010, pp. 265–278.
- [29] ———, *The  $L_4$  norm of Littlewood polynomials derived from the Jacobi symbol*, Pac. J. Math. **257** (2012), 395–418.
- [30] H. E. Jensen and T. Høholdt, *Binary sequences with good correlation properties*, Applied algebra, algebraic algorithms and error-correcting codes, Lecture Notes in Comput. Sci., vol. 356, Springer, Berlin, 1989, pp. 306–320.
- [31] 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.
- [32] E. C. Johnsen, *The inverse multiplier for abelian group difference sets*, Canad. J. Math. **16** (1964), 787–796.
- [33] A. Kirilusha and G. Narayanaswamy, *Construction of new asymptotic classes of binary sequences based on existing asymptotic classes*, Summer Science Program Tech. Rep., Dept. Math. Comput. Sci., Univ. Richmond, VA, 1999.
- [34] K. H. Leung and B. Schmidt, *The field descent method*, Des. Codes Cryptogr. **36** (2005), 171–188.
- [35] R. Lidl and H. Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.
- [36] 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.
- [37] ———, *Some problems in real and complex analysis*, D. C. Heath and Co. Raytheon Education Co., Lexington, Mass., 1968.
- [38] H.D. Lüke, H.D. Schotten, and H. Hadinejad-Mahram, *Binary and quadriphase sequences with optimal autocorrelation properties: a survey*, IEEE Trans. Inform. Theory **49** (2003), 3271–3282.
- [39] S. Mertens, *Ground states of the Bernasconi model with open boundary conditions*, <http://www-e.uni-magdeburg.de/mertens/research/labs/open.dat>, 2001.
- [40] D. J. Newman and J. S. Byrnes, *The  $L^4$  norm of a polynomial with coefficients  $\pm 1$* , Amer. Math. Monthly **97** (1990), 42–45.

- [41] M. G. Parker, *Even length binary sequence families with low negaperiodic autocorrelation*, Applied algebra, algebraic algorithms and error-correcting codes, Lecture Notes in Comput. Sci., vol. 2227, Springer, Berlin, 2001, pp. 200–209.
- [42] M. G. Parker, *Univariate and multivariate merit factors*, Proc. of Sequences and Their Applications, Lecture Notes in Computer Science, vol. 3486, New York: Springer Verlag, 2005, pp. 72–100.
- [43] A. Pott, *Two applications of relative difference sets: difference triangles and negaperiodic autocorrelation functions*, Discrete Math. **308** (2008), no. 13, 2854–2861.
- [44] K.-U. Schmidt, J. Jedwab, and M. G. Parker, *Two binary sequence families with large merit factor*, Adv. Math. Commun. **3** (2009), 135–156.
- [45] R. A. Scholtz and L. R. Welch, *GMW sequences*, IEEE Trans. Inf. Theory **30** (1984), 548–553.
- [46] M. R. Schroeder, *Number theory in science and communication*, fifth ed., Springer-Verlag, Berlin, 2009.
- [47] V. M. Sidelnikov, *Some  $k$ -valued pseudo-random sequences and nearly equidistant codes*, Probl. Inf. Transm. **5** (1969), 12–16.
- [48] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U. S. A. **34** (1948), 204–207. MR 0027006 (10,234e)
- [49] T. Xiong and J. I. Hall, *Construction of even length binary sequences with asymptotic merit factor 6*, IEEE Trans. Inf. Theory **54** (2008), 931–935.
- [50] T. Xiong and J. I. Hall, *Modifications on character sequences and construction of large even length binary sequences*, preprint (2010).
- [51] ———, *Modifications of modified Jacobi sequences*, IEEE Trans. Inf. Theory **57** (2011), 493–504.
- [52] N. Y. Yu and G. Gong, *The perfect binary sequence of period 4 for low periodic and aperiodic autocorrelations*, Sequences, subsequences, and consequences, Lecture Notes in Comput. Sci., vol. 4893, Springer, Berlin, 2007, pp. 37–49.