

MERIT FACTORS OF POLYNOMIALS DERIVED FROM DIFFERENCE SETS

CHRISTIAN GÜNTHER AND KAI-UWE SCHMIDT

ABSTRACT. The problem of constructing polynomials with all coefficients 1 or -1 and large merit factor (equivalently with small L^4 norm on the unit circle) arises naturally in complex analysis, condensed matter physics, and digital communications engineering. Most known constructions arise (sometimes in a subtle way) from difference sets, in particular from Paley and Singer difference sets. We consider the asymptotic merit factor of polynomials constructed from other difference sets, providing the first essentially new examples since 1991. In particular we prove a general theorem on the asymptotic merit factor of polynomials arising from cyclotomy, which includes results on Hall and Paley difference sets as special cases. In addition, we establish the asymptotic merit factor of polynomials derived from Gordon-Mills-Welch difference sets and Sidelnikov almost difference sets, proving two recent conjectures.

1. INTRODUCTION

The problem of constructing polynomials having all coefficients in the set $\{-1, 1\}$ (frequently called *Littlewood polynomials*) with small L^α norm on the complex unit circle arises naturally in complex analysis [27], [28], [6], [12], condensed matter physics [3], and the design of sequences for communications devices [13], [2].

Recall that, for $1 \leq \alpha < \infty$, the L^α norm on the unit circle of a polynomial $f \in \mathbb{C}[z]$ is

$$\|f\|_\alpha = \left(\frac{1}{2\pi} \int_0^{2\pi} |f(e^{i\phi})|^\alpha d\phi \right)^{1/\alpha}.$$

The L^4 norm has received particular attention because it is easier to calculate than most other L^α norms. Specifically, the L^4 norm of $f \in \mathbb{C}[z]$ is exactly the sum of the squared magnitudes of the coefficients of $f(z)\overline{f(z^{-1})}$. It is customary (see [6], for example) to measure the smallness of the L^4 norm of a polynomial f by its *merit factor* $F(f)$, defined by

$$F(f) = \frac{\|f\|_2^4}{\|f\|_4^4 - \|f\|_2^4},$$

provided that the denominator is nonzero. Note that, if f is a Littlewood polynomial of degree $n - 1$, then $\|f\|_2 = \sqrt{n}$ and so a large merit factor means that the L^4 norm is small.

Date: 20 April 2015 (revised 16 August 2016).

The authors are supported by German Research Foundation (DFG).

We note that Golay's original equivalent definition [13] of the merit factor involves the aperiodic autocorrelations (which are precisely the coefficients of $f(z)\overline{f(z^{-1})}$) of the sequence formed by the coefficients of f .

In spite of substantial progress on the merit factor problem in the last fifty years (see [18], [16], [7] for surveys and [19] for a brief review of more recent work), modulo generalisations and variations, only three nontrivial families of Littlewood polynomials are known, for which we can compute the asymptotic merit factor. These are: Rudin-Shapiro polynomials and polynomials whose coefficients are derived either from multiplicative or additive characters of finite fields. As shown by Littlewood [28], Rudin-Shapiro polynomials are constructed recursively in such a way that their merit factor satisfies a simple recurrence, which gives an asymptotic value of 3. The largest asymptotic merit factors that have been obtained from the other two families equal cubic algebraic numbers $6.342061\dots$ and $3.342065\dots$, respectively [20], [19] (see Corollary 2.4 and Theorem 2.1 in this paper for precise statements).

The latter two families of polynomials are closely related to classical difference sets, namely Paley and Singer difference sets. Recall that a *difference set* with parameters (n, k, λ) is a k -subset D of a finite group G of order n such that the $k(k-1)$ nonzero differences of elements in D hit every nonzero element of G exactly λ times (so that $k(k-1) = \lambda(n-1)$). We are interested in the case that the group G is cyclic. In this case, we fix a generator θ of G and associate with a subset D of G the Littlewood polynomial

$$(1) \quad f_{r,t}(z) = \sum_{j=0}^{t-1} \mathbb{1}_D(\theta^{j+r})z^j,$$

where r and t are integers with $t \geq 0$ and

$$\mathbb{1}_D(y) = \begin{cases} 1 & \text{for } y \in D \\ -1 & \text{for } y \in G \setminus D. \end{cases}$$

If n is the group order, then $f_{0,n}$ captures the information about D . We call this polynomial a *characteristic polynomial* of D (which is unique up to the choice of θ) and the polynomials $f_{r,n}$ *shifted characteristic polynomials*.

The results of this paper are mainly motivated by the 1991 paper of Jensen, Jensen, and Høholdt [21], in which the authors asked for the merit factor of polynomials derived from families of difference sets. It was shown in [21] that, among the known families of difference sets, only those with Hadamard parameters, namely

$$(4h-1, 2h-1, h-1)$$

for a positive integer h , can give a nonzero asymptotic merit factor for their shifted characteristic polynomials. As of 1991, five families of such difference sets were known [21]:

(A) Paley difference sets,

- (B) Singer difference sets,
- (C) Twin-prime difference sets,
- (D) Gordon-Mills-Welch difference sets,
- (E) Hall difference sets.

While in the first three cases, the asymptotic merit factors of the shifted characteristic polynomials have been determined in [17] and [21] and those of the more general polynomials (1) in [20] and [19], the last two cases were left as open problems in [21]. More specifically, the asymptotic merit factor of the polynomials derived from a subclass of the Gordon-Mills-Welch difference sets is subject to a conjecture [19, Conjecture 7.1]. In this paper, we prove this conjecture and solve the problems concerning Gordon-Mills-Welch and Hall difference sets posed in [21] (see Theorem 2.1 and Corollary 2.6, respectively). In addition, we obtain the asymptotic merit factor of polynomials related to a construction of Sidelnikov [30] (see also [25]). This explains numerical observations in [15] and proves in the affirmative [19, Conjecture 7.2].

In fact, the result for Hall difference sets arises from a much more general theorem concerning polynomials derived from cyclotomy (see Theorem 2.3). This result considers polynomials constructed from subsets of \mathbb{F}_p obtained by joining $m/2$ of the m cyclotomic classes of (even) order m , where m satisfies $p \equiv 1 \pmod{m}$. The cases $m \in \{2, 4, 6\}$ are examined in detail. For $m = 2$, we obtain the asymptotic merit factor of polynomials arising from Paley difference sets (see Corollary 2.4), which is the main result of [20]. For $m = 4$, we obtain the asymptotic merit factor of polynomials arising from Ding-Helleseth-Lam almost difference sets [11] (see Corollary 2.5). For $m = 6$, we obtain, among other things, the asymptotic merit factor of polynomials arising from Hall difference sets (see Corollary 2.6).

Some comments on our result for Gordon-Mills-Welch difference sets follow. In the cyclic case, such sets have parameters

$$(2^m - 1, 2^{m-1} - 1, 2^{m-2} - 1),$$

which are typically called *Singer* parameters. The Gordon-Mills-Welch construction produces difference sets in a cyclic group G of order $2^m - 1$ from difference sets with Singer parameters in a subgroup of G . Hence this construction is very general and can in particular be iterated. Our result on Gordon-Mills-Welch difference sets (Theorem 2.1) requires no knowledge about the smaller difference sets that are used as building blocks. Thus Singer, Paley, or Hall difference sets (in groups whose order is a Mersenne number) can be used as building blocks. In addition, since 1991, further families of difference sets in cyclic groups with Singer parameters have been found:

- (F) Maschietti difference sets [29],
- (G) Dillon-Dobbertin difference sets [10],
- (H) No-Chung-Yun difference sets [10].

Our results include the cases when these difference sets are used as building blocks in the Gordon-Mills-Welch construction. However we have not been able to determine the asymptotic merit factors of the polynomials associated with these difference sets themselves. We conjecture that they have the same behaviour as those of Singer and Gordon-Mills-Welch difference sets, given in Theorem 2.1.

2. RESULTS

To state our results, we require the function $\varphi_\nu : \mathbb{R} \times \mathbb{R}^+ \rightarrow \mathbb{R}$, defined for real ν by

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

where \mathbb{N} is the set of positive integers. This function satisfies $\varphi_\nu(R, T) = \varphi_\nu(R + \frac{1}{2}, T)$ on its entire domain. It will be useful to know the global maximum of φ_ν for certain values of ν . The function φ_1 was maximised in [19, Corollary 3.2]. Using the same approach, we find that, for all $\nu \in [0, 1]$, the global maximum of $\varphi_\nu(R, T)$ exists and equals the largest root of

$$(\nu^4 - 2\nu^3 - 3\nu^2 - 50\nu + 112)X^3 + (12\nu^3 + 36\nu^2 - 18\nu - 528)X^2 + (24\nu^2 + 282\nu + 528)X - 6\nu - 48.$$

The location (R, T) of the global maximum is unique for $R \in [0, \frac{1}{2})$ and is attained when T is the middle root of

$$(2\nu + 2)X^3 - (6\nu + 24)X + 3\nu + 24$$

and $R = 3/4 - T/2$.

We begin with stating our results for Gordon-Mills-Welch difference sets [14] whose ambient group is \mathbb{F}_q^* , where $q > 2$ is a power of two¹. Let \mathbb{F}_s be a proper subfield of \mathbb{F}_q and let A contain all elements $a \in \mathbb{F}_q$ with $\text{Tr}_{q,s}(a) = 1$, where $\text{Tr}_{u,v}$ is the trace from \mathbb{F}_u to \mathbb{F}_v . Let B be a difference set in \mathbb{F}_s^* with $|B| = s/2$ (so that, for $s > 2$, the complement of B in \mathbb{F}_s^* has Singer parameters). We also allow $s = 2$, in which case B is a trivial difference set. A set of the form

$$(2) \quad \{ab : a \in A, b \in B\}$$

is a *Gordon-Mills-Welch difference set* in \mathbb{F}_q^* (whose complement has Singer parameters). They generalise the Singer difference sets, which arise for

¹We note that [14] defines more general difference sets, which are also called Gordon-Mills-Welch difference sets. The sets considered in this paper are only those with Hadamard parameters.

$s = 2$. We have the following result for the asymptotic merit factor of polynomials obtained by Gordon-Mills-Welch difference sets.

Theorem 2.1. *Let $q > 2$ be a power of two and let f be a characteristic polynomial of a Gordon-Mills-Welch difference set in \mathbb{F}_q^* . Let $T > 0$ be real. If $t/q \rightarrow T$, then $F(f_{r,t}) \rightarrow \varphi_0(0, T)$ as $q \rightarrow \infty$.*

In the particular case of Singer difference sets, Theorem 2.1 reduces to [19, Theorem 2.2 (i)]. The case that the Gordon-Mills-Welch difference sets in Theorem 2.1 are of the form (2) when B is a Singer difference set proves [19, Conjecture 7.1]².

Next we consider subsets of \mathbb{F}_q^* for an odd prime power q , which are related to a construction of Sidelnikov [30]. We call a set of the form

$$(3) \quad \{x \in \mathbb{F}_q^* : x + 1 \text{ is zero or a square in } \mathbb{F}_q^*\}$$

a *Sidelnikov set* in \mathbb{F}_q^* . Such a set gives rise to a so-called almost difference set [1, Theorem 4]. We have the following result for the asymptotic merit factor of the associated polynomials, proving [19, Conjecture 7.2].

Theorem 2.2. *Let q be an odd prime power and let f be a characteristic polynomial of a Sidelnikov set in \mathbb{F}_q^* . Let $T > 0$ be real. If $t/q \rightarrow T$, then $F(f_{r,t}) \rightarrow \varphi_0(0, T)$ as $q \rightarrow \infty$.*

The maximum asymptotic merit factor that can be obtained in Theorems 2.1 and 2.2 is $3.342065\dots$, the largest root of

$$7X^3 - 33X^2 + 33X - 3.$$

Next we construct Littlewood polynomials using cyclotomy. Let m be a positive integer and let p be a prime satisfying $p \equiv 1 \pmod{m}$. Let ω be a fixed primitive element in \mathbb{F}_p . Let C_0 be the set of m -th powers in \mathbb{F}_p^* and write $C_s = \omega^s C_0$ for $s \in \mathbb{Z}$. The sets C_0, C_1, \dots, C_{m-1} partition \mathbb{F}_p^* and are called the *cyclotomic classes* of \mathbb{F}_p of order m .

We construct subsets D of the additive group \mathbb{F}_p by joining some of these classes. This method provides a rich source of difference sets (see [23] for a survey). We may take 1 as a generator for \mathbb{F}_p , in which case the polynomials associated with D are

$$f_{r,t}(z) = \sum_{j=0}^{t-1} \mathbb{1}_D(j+r)z^j$$

and a characteristic polynomial is $f_{0,p}$ (this is no loss of generality; if the generator is v , then replace D by $v^{-1}D$). It follows from [21, Theorem 2.1] that the shifted characteristic polynomials associated with D have a nonzero asymptotic merit factor only if $|D|/p$ approaches $1/2$ as $p \rightarrow \infty$, thus m

²Conjecture 7.1 of [19] also involves “negaperiodic” and “periodic” extensions of the polynomials associated with Gordon-Mills-Welch difference sets. The corresponding assertions can be obtained as direct consequences of Proposition 5.3 and [19, Theorem 4.2], but are omitted here for the sake of simplicity.

must be even and D must be a union of $m/2$ cyclotomic classes. Two families of difference sets arise in this way, namely the Paley difference sets for $m = 2$ and the Hall difference sets for $m = 6$ [22, Theorem 2.2]. If D is a union of $m/2$ cyclotomic classes of order m , then $|D| = (p-1)/2$, so if D is a difference set, then it must have Hadamard parameters. Equivalently, $|(D+u) \cap D| = (p-3)/4$ for every $u \in \mathbb{F}_p^*$. Our next theorem applies not only to such difference sets, but requires this condition to hold asymptotically (in a precise sense).

Theorem 2.3. *Let m be an even positive integer and let S be an $m/2$ -element subset of $\{0, 1, \dots, m-1\}$. Let p take values in an infinite set of primes satisfying $p \equiv 1 \pmod{m}$. Let D be the union of the $m/2$ cyclotomic classes C_s with $s \in S$ of \mathbb{F}_p of order m and suppose that, as $p \rightarrow \infty$,*

$$(4) \quad \frac{(\log p)^3}{p^2} \sum_{u \in \mathbb{F}_p^*} \left(|(D+u) \cap D| - \frac{p}{4} \right)^2 \rightarrow 0.$$

Let f be a characteristic polynomial of D and let R and $T > 0$ be real. If $r/p \rightarrow R$ and $t/p \rightarrow T$, then the following hold as $p \rightarrow \infty$:

(i) If $\frac{p-1}{m}$ is even for every p , then $F(f_{r,t}) \rightarrow \varphi_1(R, T)$.

(ii) If $\frac{p-1}{m}$ is odd for every p , then $F(f_{r,t}) \rightarrow \varphi_\nu(R, T)$, where $\nu = (\frac{4N}{m} - 1)^2$ and

$$N = |\{(s, s') \in S \times S : s - s' = m/2\}|.$$

Several remarks on Theorem 2.3 follow. It is readily verified that ν in Theorem 2.3 satisfies $\nu \in [0, 1]$. The condition (4) is essentially necessary since

$$\frac{1}{F(f)} \geq \frac{8}{p^2} \sum_{u \in \mathbb{F}_p^*} \left(|(D+u) \cap D| - \frac{p-2}{4} \right)^2.$$

This can be deduced from the proof of Theorem 2.3 and the inequality

$$\|f\|_4^4 \geq \frac{1}{2p} \sum_{k \in \mathbb{F}_p} |f(e^{2\pi ik/p})|^4 + \frac{p^2}{2},$$

which can be obtained from [17, (2.3)] with an extra step involving the Cauchy-Schwarz inequality. In fact, this is a refinement of the Marcinkiewicz-Zygmund inequality [32, Chapter X, Theorem 7.5] for the L^4 norm.

The condition (4) can be checked using the cyclotomic numbers of order m , which are the m^2 numbers

$$|(C_i + 1) \cap C_j|$$

for $0 \leq i, j < m$. These numbers are known explicitly for all even $m \leq 20$ and for $m = 24$ (see [4, p. 152] for a list of references). Also note that the conclusion of Theorem 2.3 remains unchanged if we replace S by $h + S$ reduced modulo m for an integer h (which changes D to $\omega^h D$).

We now consider in detail the cases $m \in \{2, 4, 6\}$ of Theorem 2.3. If $m = 2$, then D consists of either the squares or the nonsquares of \mathbb{F}_p^* . In both cases, D is a Paley difference set for $p \equiv 3 \pmod{4}$. As remarked above, we can assume without loss of generality that D is the set of squares in \mathbb{F}_p^* . Then we have (see [4, Theorem 2.2.2], for example)

$$4|(D + u) \cap D| = \begin{cases} p - 4 - (-1)^{\frac{p-1}{2}} & \text{for } u \text{ a square in } \mathbb{F}_p^* \\ p - 2 + (-1)^{\frac{p-1}{2}} & \text{for } u \text{ a nonsquare in } \mathbb{F}_p^*. \end{cases}$$

Noting that $\nu = 1$ for $m = 2$, we obtain the following corollary, which is essentially the main result of [20] (see also [19, Theorem 2.1]).

Corollary 2.4. *Let p take values in an infinite set of odd primes, let D be either the set of squares or the set of nonsquares of \mathbb{F}_p^* and let f be a characteristic polynomial of D . Let R and $T > 0$ be real. If $r/p \rightarrow R$ and $t/p \rightarrow T$, then $F(f_{r,t}) \rightarrow \varphi_1(R, T)$ as $p \rightarrow \infty$.*

We now look at the case $m = 4$. Here, we only need to consider two cases for joining two cyclotomic classes of order four, namely $C_0 \cup C_2$ and $C_0 \cup C_1$. The first case brings us back to $m = 2$. When p is of the form $x^2 + 4$ for $x \in \mathbb{Z}$ and $(p - 1)/4$ is odd, the second case gives rise to the Ding-Helleseth-Lam almost difference sets [11, Theorem 4]. By inspecting the cyclotomic numbers of order four (see Section 7), we obtain the following.

Corollary 2.5. *Let p take values in an infinite set of primes of the form $x^2 + 4y^2$ for $x, y \in \mathbb{Z}$ such that $y^2(\log p)^3/p \rightarrow 0$ as $p \rightarrow \infty$. Let D be the union of two cyclotomic classes of \mathbb{F}_p of order four and let f be a characteristic polynomial of D . Let R and $T > 0$ be real. If $r/p \rightarrow R$ and $t/p \rightarrow T$, then $F(f_{r,t}) \rightarrow \varphi_1(R, T)$ as $p \rightarrow \infty$.*

Recall from elementary number theory that primes of the form $x^2 + 4y^2$ for $x, y \in \mathbb{Z}$ are exactly the primes that are congruent to 1 modulo 4. It is also known [8] that there are infinitely many primes satisfying the hypothesis of the corollary.

The case $m = 6$ is the first situation, where different limiting functions occur. In this case, there are four different sets D to consider, namely

$$(5) \quad C_0 \cup C_2 \cup C_4, \quad C_0 \cup C_1 \cup C_2, \quad C_0 \cup C_1 \cup C_3, \quad C_0 \cup C_1 \cup C_4.$$

Again, the first set brings us back to $m = 2$. When p is of the form $x^2 + 27$ for $x \in \mathbb{Z}$ and $(p - 1)/6$ is odd, then either the third or the fourth set in (5) gives rise to Hall difference sets [22] (the choice depends on the primitive element ω). We shall see that Theorem 2.3 gives two possible limiting functions for the sixth cyclotomic classes, which is our motivation for the following definition. Let D be a union of three cyclotomic classes of order six. If there is a $\gamma \in \mathbb{F}_p^*$ such that γD equals one of the first two sets in (5), then we say that D is of *Paley type*. Otherwise, we say that D is of *Hall type*.

Corollary 2.6. *Let p take values in an infinite set of primes of the form $x^2 + 27y^2$ for $x, y \in \mathbb{Z}$ such that $y^2(\log p)^3/p \rightarrow 0$ as $p \rightarrow \infty$. Let D be the union of three cyclotomic classes of \mathbb{F}_p of order six and let f be a characteristic polynomial of D . Let R and $T > 0$ be real. If $r/p \rightarrow R$ and $t/p \rightarrow T$, then the following hold as $p \rightarrow \infty$:*

- (i) *If, for each p , D is of Paley type or $\frac{p-1}{6}$ is even, then $F(f_{r,t}) \rightarrow \varphi_1(R, T)$.*
- (ii) *If, for each p , D is of Hall type and $\frac{p-1}{6}$ is odd, then $F(f_{r,t}) \rightarrow \varphi_{1/9}(R, T)$.*

It is known that primes of the form $x^2 + 27y^2$ for $x, y \in \mathbb{Z}$ are exactly the primes p for which $p \equiv 1 \pmod{6}$ and 2 is a cube modulo p [4, Corollary 2.6.4]. Again, it is also known [8] that there are infinitely many primes satisfying the hypothesis of the corollary.

The largest asymptotic merit factor that can be obtained in Corollaries 2.4, 2.5, and 2.6 (i) is $6.342061\dots$, the largest root of

$$29X^3 - 249X^2 + 417X - 27,$$

which equals the best known asymptotic value for Littlewood polynomials. The largest asymptotic merit factor that can be obtained in Corollary 2.6 (ii) is $3.518994\dots$, the largest root of

$$349061X^3 - 1737153X^2 + 1835865X - 159651.$$

It is also of interest to look at the case $T = 1$ in our results, which concerns just the shifted characteristic polynomials, as considered in [17] and [21] for Paley and Singer difference sets, respectively. Since

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

the global maximum of $g_\nu(R, 1)$ equals $6/(2 - \nu)$. Hence, for $T = 1$, Theorems 2.1 and 2.2 give an asymptotic merit factor of 3, Corollaries 2.4, 2.5, and 2.6 (i) give a maximum asymptotic merit factor of 6 and Corollary 2.6 (ii) gives a maximum asymptotic merit factor of $54/17$.

We note that there are also “negaperiodic” and “periodic” versions of Theorem 2.1, Theorem 2.3, and its corollaries, as considered in [19] (but not of Theorem 2.2 since in this case the characteristic polynomials have odd degree). These follow directly from our results and a generalisation of Theorem 3.1 in the vein of parts (ii) and (iii) of Theorems 4.1 and 4.2 in [19]. We omit their statements for the sake of simplicity.

We shall prove Theorems 2.1 and 2.2 in Sections 5 and 6, respectively. Theorem 2.3 and Corollaries 2.5 and 2.6 will be proved in Section 7.

3. ASYMPTOTIC MERIT FACTOR CALCULATION

Let $f(z) = \sum_{j=0}^{n-1} a_j z^j$ be a Littlewood polynomial of degree $n - 1$ and let r and t be integers with $t \geq 0$. Define the polynomial

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

where we extend the definition of a_j so that $a_{j+n} = a_j$ for all $j \in \mathbb{Z}$. Write $\epsilon_k = e^{2\pi i k/n}$. From [19] it is known that $F(f_{r,t})$ depends only on the function $L_f : (\mathbb{Z}/n\mathbb{Z})^3 \rightarrow \mathbb{Z}$, defined by

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

Define the functions $I_n, J_n : (\mathbb{Z}/n\mathbb{Z})^3 \rightarrow \mathbb{Z}$ by

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

and

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

and, for even n , the function $K_n : (\mathbb{Z}/n\mathbb{Z})^3 \rightarrow \mathbb{Z}$ by

$$K_n(a, b, c) = \begin{cases} 1 & \text{if } a = n/2 \text{ and } b = c + n/2 \text{ and } bc \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

In order to prove Theorems 2.1, 2.2, and 2.3 we shall show that the corresponding function L_f is well approximated by either $I_n + \nu J_n$ for an appropriate real ν or by $I_n + K_n$ and then apply one of the following two theorems. Our first theorem is a slight generalisation of Theorems 4.1 (i) and 4.2 (i) of [19], which arise by setting $\nu = 1$ and $\nu = 0$, respectively. This theorem can be proved by applying straightforward modifications to the proof of [19, Theorem 4.1].

Theorem 3.1. *Let ν be a real number and let n take values in an infinite set of positive integers. For each n , let f be a Littlewood polynomial of degree $n - 1$ and suppose that, as $n \rightarrow \infty$,*

$$(\log n)^3 \max_{a,b,c \in \mathbb{Z}/n\mathbb{Z}} |L_f(a, b, c) - (I_n(a, b, c) + \nu J_n(a, b, c))| \rightarrow 0.$$

Let R and $T > 0$ be real. If $r/n \rightarrow R$ and $t/n \rightarrow T$, then $F(f_{r,t}) \rightarrow \varphi_\nu(R, T)$ as $n \rightarrow \infty$.

There is a similar generalisation of parts (ii) and (iii) of Theorems 4.1 and 4.2 in [19], which we do not consider in this paper.

Our second theorem is a more subtle modification of Theorem 4.1 (i) in [19]. We include a proof that highlights the required modifications of the proof of [19, Theorem 4.1 (i)].

Theorem 3.2. *Let n take values in an infinite set of even positive integers. For each n , let f be a Littlewood polynomial of degree $n - 1$ and suppose that, as $n \rightarrow \infty$,*

$$(6) \quad (\log n)^3 \max_{a,b,c \in \mathbb{Z}/n\mathbb{Z}} |L_f(a, b, c) - (I_n(a, b, c) + K_n(a, b, c))| \rightarrow 0.$$

Let $T > 0$ be real. If $t/n \rightarrow T$, then $F(f_{r,t}) \rightarrow \varphi_0(0, T)$ as $n \rightarrow \infty$.

Proof. The first part of the proof is identical to that of [19, Theorem 4.1 (i)], giving

$$(7) \quad \frac{1}{F(f_{r,t})} = -1 + \frac{1}{t^2 n} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \sum_{a,b,c \in \mathbb{Z}/n\mathbb{Z}} L_f(a, b, c) \epsilon_a^{-j_2-r} \epsilon_b^{j_3+r} \epsilon_c^{j_4+r},$$

where $\epsilon_k = e^{2\pi i k/n}$. Write

$$(8) \quad L_f(a, b, c) = I_n(a, b, c) + K_n(a, b, c) + M_n(a, b, c),$$

where $M_n(a, b, c)$ is an error term, which can be controlled using (6). 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) $b = c + n/2$ and $a = n/2$. Then $I_n(a, b, c) + K_n(a, b, c)$ equals 1 if at least one of these conditions is satisfied and $I_n(a, b, c) + K_n(a, b, c)$ equals 0 otherwise. There are exactly three tuples (a, b, c) that satisfy more than one of these conditions, namely $(0, 0, 0)$, $(n/2, n/2, 0)$, and $(n/2, 0, n/2)$.

We now substitute (8) into (7) and break the sum involving $I_n(a, b, c) + K_n(a, b, c)$ into six parts: three sums corresponding to the three cases and three sums to correct for the double counting of $(0, 0, 0)$, $(n/2, n/2, 0)$, and $(n/2, 0, n/2)$. Noting that the sums arising in cases (1) and (2) have the same value, as have the sums arising for the compensation of the double count of $(n/2, n/2, 0)$ and $(n/2, 0, n/2)$, we obtain

$$\frac{1}{F(f_{r,t})} = -1 + A + B + C - D_1 - D_2 - D_3 + E,$$

where

$$\begin{aligned}
A = B &= \frac{1}{t^2 n} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \sum_{b \in \mathbb{Z}/n\mathbb{Z}} \epsilon_b^{j_3 - j_2}, \\
C &= \frac{1}{t^2 n} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} (-1)^{j_3 - j_2} \sum_{c \in \mathbb{Z}/n\mathbb{Z}} \epsilon_c^{j_3 + j_4 + 2r}, \\
D_1 &= \frac{1}{t^2 n} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} 1, \\
D_2 = D_3 &= \frac{1}{t^2 n} \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} (-1)^{j_3 - j_2}, \\
E &= \frac{1}{t^2 n} \sum_{a, b, c \in \mathbb{Z}/n\mathbb{Z}} M_n(a, b, c) \epsilon_{-a+b+c}^r \sum_{\substack{0 \leq j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \epsilon_a^{-j_2} \epsilon_b^{j_3} \epsilon_c^{j_4}.
\end{aligned}$$

As in the proof of [19, Theorem 4.2], we have $-1 + A + B - D_1 + E \rightarrow 1/\varphi_0(0, T)$ if $t/n \rightarrow T$. Hence it remains to show that $C - D_2 - D_3 \rightarrow 0$ if $t/n \rightarrow T$.

Since there are contributions to the first sum in C only when $j_3 + j_4 = mn - 2r$ for some $m \in \mathbb{Z}$, we obtain

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

Therefore we have $|C| \leq 1/(tn)$ and so $C \rightarrow 0$ if $t/n \rightarrow T$. By writing $j_3 = j_1 + m$ for some $m \in \mathbb{Z}$ we find that

$$D_2 = \frac{1}{t^2 n} \sum_{m \in \mathbb{Z}} \left(\sum_{0 \leq j, j+m < t} (-1)^j \right)^2.$$

Hence $|D_2| \leq 1/(tn)$ and therefore $D_2 + D_3 \rightarrow 0$ if $t/n \rightarrow T$. This completes the proof. \square

4. SOME BACKGROUND ON GAUSS AND JACOBI SUMS

Let χ be a multiplicative character of \mathbb{F}_q . Throughout this paper, we use the common convention

$$\chi(0) = \begin{cases} 0 & \text{if } \chi \text{ is nontrivial} \\ 1 & \text{if } \chi \text{ is trivial.} \end{cases}$$

We define the *canonical Gauss sum* of χ to be

$$(9) \quad G(\chi) = \sum_{y \in \mathbb{F}_q^*} \chi(y) e^{2\pi i \operatorname{Tr}_{q,p}(y)/p},$$

where p is the characteristic of \mathbb{F}_q and $\text{Tr}_{q,p}$ is the trace from \mathbb{F}_q to \mathbb{F}_p . Below we summarise some basic facts about such Gauss sums (see [26, Chapter 5] or [4, Chapter 1], for example).

Lemma 4.1. *Let χ be a multiplicative character of \mathbb{F}_q . Then the following hold.*

- (i) $G(\chi) = -1$ if χ is trivial.
- (ii) $|G(\chi)| = \sqrt{q}$ if χ is nontrivial.
- (iii) $G(\chi)G(\bar{\chi}) = \chi(-1)q$.

We also require the following deep result due to Katz [24, pp. 161–162].

Lemma 4.2. *Let $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s$ be multiplicative characters of \mathbb{F}_q such that $\alpha_1, \dots, \alpha_r$ do not arise by permuting β_1, \dots, β_s . Then*

$$\left| \sum_{\chi} G(\chi\alpha_1) \cdots G(\chi\alpha_r) \overline{G(\chi\beta_1)} \cdots \overline{G(\chi\beta_s)} \right| \leq \max(r, s) q^{(r+s+1)/2},$$

where the sum runs over all multiplicative characters χ of \mathbb{F}_q .

Now let ψ and χ be multiplicative characters of \mathbb{F}_q . The *Jacobi sum* corresponding to ψ and χ is defined to be

$$J(\psi, \chi) = \sum_{y \in \mathbb{F}_q} \psi(y)\chi(1-y).$$

Below we summarise some basic facts about Jacobi sums (see [26, Chapter 5] or [4, Chapter 2], for example).

Lemma 4.3. *Let ψ and χ be multiplicative characters of \mathbb{F}_q . Then the following hold.*

- (i) $J(\psi, \chi) = 0$ if exactly one of ψ or χ is trivial.
- (ii) $|J(\psi, \chi)| = 1$ if ψ and χ are nontrivial, but $\psi\chi$ is trivial.
- (iii) $|J(\psi, \chi)| = \sqrt{q}$ if all of ψ , χ , and $\psi\chi$ are nontrivial.
- (iv) $J(\psi, \chi)q = G(\psi)G(\chi)\overline{G(\psi\chi)}$ if ψ and χ are nontrivial.
- (v) $J(\psi, \chi)J(\bar{\psi}, \chi\psi) = \psi(-1)q$ if ψ and χ are nontrivial.

5. GORDON-MILLS-WELCH DIFFERENCE SETS

In this section we prove Theorem 2.1. If D is a subset of a finite abelian group G and χ is a character of G , we write

$$\chi(D) = \sum_{d \in D} \chi(d).$$

The following lemma is standard (and easily verified).

Lemma 5.1. *A k -subset D of a finite abelian group G of order n is a difference set if and only if*

$$|\chi(D)|^2 = \frac{k(n-k)}{n-1}$$

for all nontrivial characters χ of G .

The following lemma gives the character values of Gordon-Mills-Welch difference sets and in particular gives an alternative proof of the main result of [14] (although, for simplicity, we restrict q to be even).

Lemma 5.2. *Let $q > 2$ be a power of two and let \mathbb{F}_s be a subfield of \mathbb{F}_q . Let A contain all elements $a \in \mathbb{F}_q$ with $\text{Tr}_{q,s}(a) = 1$, let B be a subset of \mathbb{F}_s^* , and write $D = \{ab : a \in A, b \in B\}$. Let χ be a nontrivial character of \mathbb{F}_q^* and let χ^* be its restriction to \mathbb{F}_s^* . Then*

$$\chi(D) = \begin{cases} \frac{\chi^*(B)}{G(\chi^*)} G(\chi) & \text{for } \chi^* \text{ nontrivial} \\ -\frac{\chi^*(B)}{s} G(\chi) & \text{for } \chi^* \text{ trivial.} \end{cases}$$

In particular, if B is a difference set in \mathbb{F}_s^* and $|B| = s/2$, then D is a difference set with parameters $(q-1, q/2, q/4)$.

Proof. We have

$$\chi(D) = \sum_{\substack{a \in \mathbb{F}_q \\ \text{Tr}_{q,s}(a)=1}} \sum_{b \in B} \chi(ab) = E(\chi) \chi^*(B),$$

where

$$E(\chi) = \sum_{\substack{a \in \mathbb{F}_q \\ \text{Tr}_{q,s}(a)=1}} \chi(a)$$

is an Eisenstein sum. It is known [4, pp. 391/400] that

$$E(\chi) = \begin{cases} G(\chi)/G(\chi^*) & \text{for } \chi^* \text{ nontrivial} \\ -G(\chi)/s & \text{for } \chi^* \text{ trivial,} \end{cases}$$

which proves the first statement of the lemma. The second statement follows from Lemmas 5.1 and 4.1. \square

We now prove Theorem 2.1 by combining Theorem 3.1 with the following result.

Proposition 5.3. *Let $q > 2$ be a power of two and let f be a characteristic polynomial of a Gordon-Mills-Welch difference set in \mathbb{F}_q^* . Then*

$$|L_f(a, b, c) - I_{q-1}(a, b, c)| \leq \frac{2q^{5/2}}{(q-1)^3}$$

for all $a, b, c \in \mathbb{Z}/(q-1)\mathbb{Z}$.

Proof. By definition, there exists a proper subfield \mathbb{F}_s of \mathbb{F}_q such that the underlying Gordon-Mills-Welch difference set is

$$D = \{ab : a \in A, b \in B\},$$

where A contains all elements $a \in \mathbb{F}_q$ with $\text{Tr}_{q,s}(a) = 1$ and B is a difference set in \mathbb{F}_s^* with $|B| = s/2$. Let θ be a generator for \mathbb{F}_q^* such that

$$f(z) = \sum_{j=0}^{q-2} \mathbb{1}_D(\theta^j) z^j.$$

Let ξ be the multiplicative character of \mathbb{F}_q given by $\xi(\theta) = e^{2\pi i/(q-1)}$. It is readily verified that

$$f(e^{2\pi i k/(q-1)}) = \begin{cases} 1 & \text{for } k \equiv 0 \pmod{q-1} \\ 2\xi^k(D) & \text{for } k \not\equiv 0 \pmod{q-1}. \end{cases}$$

It then follows from Lemmas 5.2 and 4.1 (i) that

$$f(e^{2\pi i k/(q-1)}) = C_k G(\xi^k),$$

where C_k has unit magnitude for all k and depends only on k modulo $q-1$. Therefore

$$(10) \quad L_f(a, b, c) = \frac{1}{(q-1)^3} \sum_{\chi} G(\chi) G(\chi \xi^a) \overline{G(\chi \xi^b) G(\chi \xi^c)} C_{\chi}(a, b, c),$$

where the sum is over all multiplicative characters χ of \mathbb{F}_q and $C_{\chi}(a, b, c)$ has unit magnitude. Using Lemma 4.1, we obtain

$$L_f(a, b, c) = \begin{cases} 1 + \frac{q-2}{(q-1)^2} & \text{for } a = b = c = 0 \\ 1 - \frac{1}{(q-1)^2} & \text{for } \{0, a\} = \{b, c\} \text{ and } a \neq 0, \end{cases}$$

which proves the desired result in the case that $I_{q-1}(a, b, c) = 1$.

Now assume that $\{0, a\} \neq \{b, c\}$, so that $I_{q-1}(a, b, c) = 0$. We need to show that

$$(11) \quad |L_f(a, b, c)| \leq \frac{2q^{5/2}}{(q-1)^3}.$$

Let H be the subgroup of index $s-1$ of the character group of \mathbb{F}_q^* and note that H is not the trivial group since, by assumption, $s < q$. Then $C_{\chi}(a, b, c)$ is constant when χ ranges over a coset of H . Since $C_{\chi}(a, b, c)$ has unit magnitude, we find from (10) and the triangle inequality that

$$(12) \quad |L_f(a, b, c)| \leq \frac{s-1}{(q-1)^3} \max_{\phi} \left| \sum_{\chi \in H} G(\chi \phi) G(\chi \phi \xi^a) \overline{G(\chi \phi \xi^b) G(\chi \phi \xi^c)} \right|,$$

where the maximum is over all multiplicative characters ϕ of \mathbb{F}_q . By the definition (9) of a Gauss sum over \mathbb{F}_q , the inner sum can be written as

$$\sum_{w,x,y,z \in \mathbb{F}_q^*} (-1)^{\text{Tr}_{q,2}(w+x+y+z)} \xi^a(x) \overline{\xi^b(y) \xi^c(z)} \phi\left(\frac{wx}{yz}\right) \sum_{\chi \in H} \chi\left(\frac{wx}{yz}\right).$$

For each $w, x, y, z \in \mathbb{F}_q^*$, we have

$$\frac{s-1}{q-1} \sum_{\chi \in H} \chi\left(\frac{wx}{yz}\right) = \frac{1}{q-1} \sum_{\chi} \chi\left(\frac{wx}{yz}\right),$$

where the sum on the right-hand side is over all multiplicative characters of \mathbb{F}_q , since both sides equal either 0 or 1 depending on whether $wx = yz$ or not. Therefore, we can rewrite the inner sum of (12) as

$$\frac{1}{s-1} \sum_{\chi} G(\chi\phi) G(\chi\phi\xi^a) \overline{G(\chi\phi\xi^b) G(\chi\phi\xi^c)},$$

where χ now runs over all multiplicative characters of \mathbb{F}_q . The magnitude of this expression is at most $\frac{2}{s-1} q^{5/2}$ by Lemma 4.2. Substitute into (12) to conclude that (11) holds, as required. \square

6. SIDELNIKOV SETS

In this section we prove Theorem 2.2 by combining Theorem 3.2 with the following result.

Proposition 6.1. *Let q be an odd prime power and let f be a characteristic polynomial of a Sidelnikov set in \mathbb{F}_q^* . Then*

$$\left| L_f(a, b, c) - (I_{q-1}(a, b, c) + K_{q-1}(a, b, c)) \right| \leq \frac{23q^{5/2}}{(q-1)^3}$$

for all $a, b, c \in \mathbb{Z}/(q-1)\mathbb{Z}$.

Proof. Let η be the quadratic character of \mathbb{F}_q . By the definition of a Sidelnikov set (3), there exists a generator θ of \mathbb{F}_q^* such that

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

where, as usual, $\eta(0) = 0$. Let ξ be the multiplicative character of \mathbb{F}_q given by $\xi(\theta) = e^{2\pi i/(q-1)}$. Then we have, for all $k \not\equiv 0 \pmod{q-1}$,

$$\begin{aligned} f(e^{2\pi ik/(q-1)}) &= (-1)^k + \sum_{j=0}^{q-2} \eta(\theta^j + 1) \xi^k(\theta^j) \\ &= (-1)^k + \sum_{y \in \mathbb{F}_q} \eta(y + 1) \xi^k(y) \\ &= (-1)^k + \xi^k(-1) \sum_{y \in \mathbb{F}_q} \eta(y) \xi^k(1 - y) \\ &= (-1)^k (1 + J(\eta, \xi^k)). \end{aligned}$$

On the other hand we have $f(1) = 1 - \eta(1) = 0$. Therefore

$$(13) \quad L_f(a, b, c) = \frac{(-1)^{a+b+c}}{(q-1)^3} \sum_{\chi} J(\eta, \chi) J(\eta, \chi \xi^a) \overline{J(\eta, \chi \xi^b) J(\eta, \chi \xi^c)} + \Delta,$$

where the sum is over all multiplicative characters χ of \mathbb{F}_q and $|\Delta| \leq 15q^{3/2}/(q-1)^2$, using Lemma 4.3. If one of b and c equals a and the other is zero, then by Lemma 4.3 the sum in (13) is between $(q-5)q^2$ and $(q-2)q^2$. If $a = (q-1)/2$ and $b = c + (q-1)/2$, then $\xi^a = \eta$ and $\xi^b = \xi^c \eta$ and by Lemma 4.3 (in particular (v)) the sum (13) is again at least $(q-5)q^2$ and at most $(q-2)q^2$. Since

$$\frac{(q-5)q^2}{(q-1)^3} = 1 - \frac{2q^2 + 3q - 1}{(q-1)^3},$$

this establishes the cases in which either $I_{q-1}(a, b, c)$ or $K_{q-1}(a, b, c)$ equals 1.

Now assume that (a, b, c) is such that $I_{q-1}(a, b, c)$ and $K_{q-1}(a, b, c)$ are both zero. Equivalently, the multisets

$$(14) \quad \{\xi^0, \xi^a, \xi^b \eta, \xi^c \eta\} \quad \text{and} \quad \{\eta, \xi^a \eta, \xi^b, \xi^c\}$$

are distinct. Use Lemmas 4.3 and 4.1 to see that the sum in (13) equals

$$(15) \quad \frac{1}{q^2} \sum_{\chi} G(\chi) G(\chi \xi^a) G(\chi \eta \xi^b) G(\chi \eta \xi^c) \overline{G(\chi \eta) G(\chi \eta \xi^a) G(\chi \xi^b) G(\chi \xi^c)}$$

plus an error term of magnitude at most $4q^{3/2}$, where the sum is over all multiplicative characters χ of \mathbb{F}_q . Since the multisets (14) are distinct, we can apply Lemma 4.2 to see that (15) is at most $4q^{5/2}$. This shows that

$$|L_f(a, b, c)| \leq \frac{23q^{5/2}}{(q-1)^3},$$

as required. □

7. CYCLOTOMIC CONSTRUCTIONS

In this section we prove Theorem 2.3 and Corollaries 2.5 and 2.6. We shall use the following notation. Let m be an even positive integer and let p be a prime satisfying $p \equiv 1 \pmod{m}$. Let ω be a primitive element of \mathbb{F}_p and let C_0, C_1, \dots, C_{m-1} be the cyclotomic classes of \mathbb{F}_p of order m with respect to ω . Let S be an $m/2$ -element subset of $\{0, 1, \dots, m-1\}$ and let D be the union of the $m/2$ cyclotomic classes C_s with $s \in S$. Taking 1 as a generator for the additive group of \mathbb{F}_p , a characteristic polynomial of D is

$$(16) \quad f(z) = \sum_{j=0}^{p-1} \mathbb{1}_D(j) z^j.$$

The following lemma gives the evaluations of f at p -th roots of unity.

Lemma 7.1. *Assume the notation as above and let χ be a multiplicative character of \mathbb{F}_p of order m . Then*

$$f(e^{2\pi i k/p}) = \frac{2}{m} \sum_{j=1}^{m-1} G(\chi^j) \overline{\chi^j(k)} \sum_{s \in S} \overline{\chi^j(\omega^s)} - 1.$$

Proof. Since $f(1) = |D| - |\mathbb{F}_p \setminus D| = -1$, the result holds for $k \equiv 0 \pmod{p}$, so assume that $k \not\equiv 0 \pmod{p}$. By definition we have

$$\begin{aligned} f(e^{2\pi i k/p}) &= \sum_{y \in D} e^{2\pi i k y/p} - \sum_{y \in \mathbb{F}_p \setminus D} e^{2\pi i k y/p} \\ &= 2 \sum_{y \in D} e^{2\pi i k y/p} - \sum_{y \in \mathbb{F}_p} e^{2\pi i k y/p} \\ &= 2 \sum_{y \in D} e^{2\pi i k y/p} \\ &= 2 \sum_{s \in S} \sum_{y \in C_s} e^{2\pi i k y/p}. \end{aligned}$$

Writing $h = \frac{p-1}{m}$, the inner sum can be written as

$$\begin{aligned} \sum_{y \in C_s} e^{2\pi i k y/p} &= \sum_{j=0}^{h-1} e^{2\pi i k \omega^{m j + s}/p} \\ &= \frac{1}{m} \left(\sum_{y \in \mathbb{F}_p} e^{2\pi i k \omega^s y^m/p} - 1 \right). \end{aligned}$$

Since $\sum_{j=0}^{m-1} \chi^j(y)$ equals m if y is an m -th power and equals zero otherwise, we have, for each $a \in \mathbb{F}_p^*$,

$$\begin{aligned} \sum_{y \in \mathbb{F}_p} e^{2\pi i a y^m / p} &= \sum_{y \in \mathbb{F}_p} e^{2\pi i a y / p} \sum_{j=0}^{m-1} \chi^j(y) \\ &= \sum_{j=0}^{m-1} \sum_{y \in \mathbb{F}_p} e^{2\pi i y / p} \chi^j(y) \overline{\chi^j(a)}. \end{aligned}$$

For $j = 0$, the inner sum equals zero, so we can let the outer sum start with $j = 1$. Then all involved multiplicative characters are nontrivial and we can restrict the summation range of the inner sum to \mathbb{F}_p^* . Therefore

$$\sum_{y \in \mathbb{F}_p} e^{2\pi i a y^m / p} = \sum_{j=1}^{m-1} G(\chi^j) \overline{\chi^j(a)},$$

which gives the desired result. \square

Our next result estimates L_f for f given in (16) at all points, but $(0, 0, 0)$.

Proposition 7.2. *With the notation as above, we have*

$$|L_f(a, b, c) - (I_p(a, b, c) + \nu J_p(a, b, c))| \leq 18(m-1)^4 p^{-1/2}$$

for all $a, b, c \in \mathbb{Z}/p\mathbb{Z}$ with $(a, b, c) \neq (0, 0, 0)$, where

$$\nu = \begin{cases} 1 & \text{for } \frac{p-1}{m} \text{ even} \\ \left(\frac{4N}{m} - 1\right)^2 & \text{for } \frac{p-1}{m} \text{ odd} \end{cases}$$

and

$$N = |\{(s, s') \in S \times S : s - s' = m/2\}|.$$

Proof. Let χ be a multiplicative character of \mathbb{F}_p of order m and write

$$K(\chi^j) = \frac{2}{m} \sum_{s \in S} \overline{\chi^j(\omega^s)}.$$

From Lemma 7.1 we find that

$$(17) \quad f(e^{2\pi i k / p}) = \sum_{j=1}^{m-1} G(\chi^j) K(\chi^j) \overline{\chi^j(k)} - 1.$$

Hence $L_f(a, b, c)$ equals

$$(18) \quad \frac{1}{p^3} \sum_{j_1, j_2, j_3, j_4=1}^{m-1} G(\chi^{j_1}) G(\chi^{j_2}) \overline{G(\chi^{j_3}) G(\chi^{j_4})} K(\chi^{j_1}) K(\chi^{j_2}) \overline{K(\chi^{j_3}) K(\chi^{j_4})} \\ \times \sum_{k \in \mathbb{F}_p} \overline{\chi^{j_1}(k) \chi^{j_2}(k+a) \chi^{j_3}(k+b) \chi^{j_4}(k+c)} + \Delta,$$

where $|\Delta| \leq 15(m-1)^4 p^{-1/2}$, using that the magnitude of the sum on the right-hand side of (17) is at most $(m-1)p^{1/2}$ by Lemma 4.1. First consider the case that $b = 0$ and $c = a \neq 0$, so that $I_p(a, b, c) = 1$ and $J_p(a, b, c) = 0$. Then the inner sum in (18) is

$$\sum_{k \in \mathbb{F}_p} \chi^{j_3 - j_1}(k) \chi^{j_4 - j_2}(k + a).$$

This sum either has magnitude at most \sqrt{p} by the Weil bound (see [26, Theorem 5.41], for example) or equals p . Since $a \neq 0$, the latter case occurs if and only if $j_1 \equiv j_3 \pmod{m}$ and $j_2 \equiv j_4 \pmod{m}$. Therefore $L_f(a, 0, a)$ equals

$$\frac{1}{p^2} \left(\sum_{j=1}^{m-1} |G(\chi^j)|^2 |K(\chi^j)|^2 \right)^2$$

plus an error term of magnitude at most $16(m-1)^4 p^{-1/2}$. Then we find from Lemma 4.1 and

$$\sum_{j=1}^{m-1} |K(\chi^j)|^2 = 1$$

that the desired result holds for $b = 0$ and $c = a \neq 0$. The case $c = 0$ and $b = a \neq 0$ is completely analogous.

Now assume that $a = 0$ and $c = b \neq 0$, so that $I_p(a, b, c) = 0$ and $J_p(a, b, c) = 1$. Then the inner sum in (18) equals

$$\sum_{k \in \mathbb{F}_p} \overline{\chi^{j_1 + j_2}(k)} \chi^{j_3 + j_4}(k + b).$$

As before, this sum either has magnitude at most \sqrt{p} or equals p , where the latter case occurs if and only if $j_1 \equiv -j_2 \pmod{m}$ and $j_3 \equiv -j_4 \pmod{m}$. Hence $L_f(0, b, b)$ equals

$$(19) \quad \frac{1}{p^2} \left| \sum_{j=1}^{m-1} G(\chi^j) G(\overline{\chi^j}) K(\chi^j) K(\overline{\chi^j}) \right|^2$$

plus an error term of magnitude at most $16(m-1)^4 p^{-1/2}$. From Lemma 4.1 we find that (19) equals

$$\left| \sum_{j=1}^{m-1} \chi^j(-1) |K(\chi^j)|^2 \right|^2 = \left(\sum_{j=1}^{m-1} (-1)^{\frac{j(p-1)}{m}} \left| \frac{2}{m} \sum_{s \in S} e^{2\pi i j s / m} \right|^2 \right)^2.$$

A standard calculation then shows that this expression equals ν . This proves the desired result in the case that $a = 0$ and $c = b \neq 0$.

Now assume that $0, a, b, c$ do not form two pairs of equal elements. In this case, we invoke the Weil bound again to conclude that the inner sum in (18) is at most $3\sqrt{p}$ in magnitude. Therefore we have by Lemma 4.1

$$|L_f(a, b, c)| \leq 18(m-1)^4 p^{-1/2},$$

which completes the proof. \square

Proof of Theorem 2.3. Without loss of generality, we may choose 1 as a generator for the additive group of \mathbb{F}_p and take (16) as a characteristic polynomial of D (if the generator is v , then replace D by $v^{-1}D$).

We shall deduce Theorem 2.3 from Theorem 3.1. Proposition 7.2 takes care of all values of $L_f(a, b, c)$ in the condition of Theorem 3.1, except when $(a, b, c) = (0, 0, 0)$. We shall show that our assumption (4) takes care of the latter case. Writing

$$R_u = \sum_{y \in \mathbb{F}_p} \mathbb{1}_D(y) \mathbb{1}_D(y + u),$$

a standard calculation gives

$$|f(e^{2\pi ik/p})|^2 = \sum_{u \in \mathbb{F}_p} R_u e^{-2\pi iku/p}$$

and therefore, by Parseval's identity,

$$\frac{1}{p} \sum_{k \in \mathbb{F}_p} |f(e^{2\pi ik/p})|^4 = \sum_{u \in \mathbb{F}_p} R_u^2.$$

A counting argument shows that

$$R_u = 4|(D + u) \cap D| - (p - 2).$$

Therefore, since $2|D| = p - 1$, we find that $L_f(0, 0, 0)$ equals

$$\frac{1}{p^3} \sum_{k \in \mathbb{F}_p} |f(e^{2\pi ik/p})|^4 = 1 + \frac{1}{p^2} \sum_{u \in \mathbb{F}_p^*} (4|(D + u) \cap D| - (p - 2))^2.$$

Now our assumption (4) together with Proposition 7.2 imply that the condition of Theorem 3.1 is satisfied, which proves Theorem 2.3. \square

Next we show how to deduce Corollaries 2.5 and 2.6 from Theorem 2.3. First consider Corollary 2.5. As explained in Section 2, we just need to consider the case that $D = C_0 \cup C_1$. The cyclotomic numbers of order four have been already determined by Gauss and can be found, for example, in [4, Theorem 2.4.1]. These numbers depend on the representation $p = x^2 + 4y^2$ and on the parity of $(p - 1)/4$. They also depend on the choice of the primitive element in \mathbb{F}_p used to define the cyclotomic classes, but this is encapsulated in the fact that y is unique only up to sign. Using the cyclotomic numbers of order four, we obtain the numbers $|(D + u) \cap D|$, shown in Table 1. For example, if $u \in C_1$, then $u^{-1} \in C_3$ and $|(D + u) \cap D|$ equals

$$|(C_3 + 1) \cap C_3| + |(C_3 + 1) \cap C_0| + |(C_0 + 1) \cap C_3| + |(C_0 + 1) \cap C_0|.$$

From the data in Table 1 we conclude that the assumption $y^2(\log p)^3/p \rightarrow 0$ as $p \rightarrow \infty$ in Corollary 2.5 implies the condition (4) in Theorem 2.3. It is also readily verified that $\nu = 1$, which proves Corollary 2.5.

TABLE 1. The numbers $4|(D+u)\cap D|-(p-2)$ for $D = C_0\cup C_1$ and primes p of the form $p = x^2 + 4y^2$.

D	$\frac{p-1}{4}$ even	$\frac{p-1}{4}$ odd
$u \in C_0$	$-3 + 2y$	$-1 - 2y$
$u \in C_1$	$-3 - 2y$	$-1 + 2y$
$u \in C_2$	$1 + 2y$	$-1 - 2y$
$u \in C_3$	$1 - 2y$	$-1 + 2y$

TABLE 2. The numbers $4|(D+u)\cap D|-(p-2)$ for primes of the form $x^2 + 27y^2$ and $(p-1)/6$ odd.

D	$C_0 \cup C_1 \cup C_2$	$C_0 \cup C_1 \cup C_3$	$C_0 \cup C_2 \cup C_3$
$u \in C_0$	$-1 + 8y$	$-3 + 2y$	$-3 - 2y$
$u \in C_1$	-1	-1	$1 + 2y$
$u \in C_2$	$-1 - 8y$	$1 - 2y$	-1
$u \in C_3$	$-1 + 8y$	$-3 + 2y$	$-3 - 2y$
$u \in C_4$	-1	-1	$1 + 2y$
$u \in C_5$	$-1 - 8y$	$1 - 2y$	-1

Now consider Corollary 2.6. Then it suffices to consider the cases that D is one of the following sets

$$C_0 \cup C_1 \cup C_2, \quad C_0 \cup C_1 \cup C_3, \quad C_0 \cup C_1 \cup C_4.$$

The cyclotomic numbers of order six have been determined by Dickson [9] (see also [22] for $(p-1)/6$ odd and [31] for $(p-1)/6$ even). These numbers depend on the representation of p as a sum of a square and three times a square (every prime congruent to 1 modulo 3 can be represented in this way) and on the cubic character of 2. Since p is of the form $x^2 + 27y^2$, we know [4, Theorem 2.6.4] that 2 is a cube in \mathbb{F}_p . In this case, the numbers $|(D+u)\cap D|$ are given in Tables 2 and 3 (again y is only unique up to sign, corresponding to different primitive elements in \mathbb{F}_p). We again conclude that the assumption $y^2(\log p)^3/p \rightarrow 0$ as $p \rightarrow \infty$ in Corollary 2.6 implies the condition (4) in Theorem 2.3. The proof of Corollary 2.6 is completed by checking that $\nu = 1$ if D is of Paley type and $\nu = 1/9$ if D is of Hall type.

8. CLOSING REMARK

We note that some results related to Theorem 2.3 and Corollary 2.5 have been obtained (apparently independently) by Boothby and Katz in [5], which appeared in preprint form after the submission of this paper. In [5] the authors study the crosscorrelations between two sequences derived from linear combinations of multiplicative characters of finite fields, which in particular

TABLE 3. The numbers $4|(D + u) \cap D| - (p - 2)$ for primes of the form $x^2 + 27y^2$ and $(p - 1)/6$ even.

D	$C_0 \cup C_1 \cup C_2$	$C_0 \cup C_1 \cup C_3$	$C_0 \cup C_2 \cup C_3$
$u \in C_0$	$-3 + 8y$	$-3 + 6y$	$-3 + 2y$
$u \in C_1$	-3	$-3 - 4y$	$1 - 2y$
$u \in C_2$	$-3 - 8y$	$1 + 2y$	$-3 + 4y$
$u \in C_3$	$1 + 8y$	$-3 - 2y$	$-3 - 6y$
$u \in C_4$	1	$1 + 4y$	$1 + 6y$
$u \in C_5$	$1 - 8y$	$1 - 6y$	$1 - 4y$

applies to sequences derived from cyclotomy, as in Theorem 2.3. If these two sequences are equal, the crosscorrelations reduce to autocorrelations, in which case the combination of [5, Corollary 4.2] and [5, Lemma 7.4] leads to a result similar to Theorem 2.3. The difference is that the condition (4) is removed, but the limit contains an extra term involving combinations of Gauss sums. The authors of [5] could evaluate this extra term in the cases $m = 2$ and $m = 4$, thereby obtaining Corollary 2.4 again and generalising Corollary 2.5. In particular, [5, Theorem 8.3] (together with [5, Theorem 8.2]) generalises Corollary 2.5 in the sense that the asymptotic merit factor, as $p \rightarrow \infty$, is given in terms of a limit point of γ , where $\tan(\gamma) = 2y/x$ and $p = x^2 + 4y^2$. Corollary 2.5 is essentially the case $\gamma \rightarrow 0$, which maximises the asymptotic merit factor.

REFERENCES

- [1] K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar, and H. M. Martinsen, *Almost difference sets and their sequences with optimal autocorrelation*, IEEE Trans. Inform. Theory **47** (2001), no. 7, 2934–2943.
- [2] 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), no. 5, 289–304.
- [3] J. Bernasconi, *Low autocorrelation binary sequences: statistical mechanics and configuration state analysis*, J. Physique **48** (1987), no. 4, 559–567.
- [4] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, Inc., New York, 1998, A Wiley-Interscience Publication.
- [5] T. Boothby and D. J. Katz, *Low correlation sequences from linear combinations of characters*, arXiv:1602.04514 [cs.IT], 14 Feb 2016.
- [6] 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.
- [7] P. Borwein, R. Ferguson, and J. Knauer, *The merit factor problem*, Number theory and polynomials, London Math. Soc. Lecture Note Ser., vol. 352, Cambridge Univ. Press, Cambridge, 2008, pp. 52–70.
- [8] M. D. Coleman, *The Rosser-Iwaniec sieve in number fields, with an application*, Acta Arith. **65** (1993), no. 1, 53–83.

- [9] L. E. Dickson, *Cyclotomy, Higher Congruences, and Waring's Problem*, Amer. J. Math. **57** (1935), no. 2, 391–424.
- [10] J. F. Dillon and H. Dobbertin, *New cyclic difference sets with Singer parameters*, Finite Fields Appl. **10** (2004), no. 3, 342–389.
- [11] C. Ding, T. Hellesest, and K. Y. Lam, *Several classes of binary sequences with three-level autocorrelation*, IEEE Trans. Inform. Theory **45** (1999), no. 7, 2606–2612.
- [12] T. Erdélyi, *Polynomials with Littlewood-type coefficient constraints*, Approximation theory, X (St. Louis, MO, 2001), Innov. Appl. Math., Vanderbilt Univ. Press, Nashville, TN, 2002, pp. 153–196.
- [13] M. J. E. Golay, *A class of finite binary sequences with alternate autocorrelation values equal to zero*, IEEE Trans. Inform. Theory **IT-18** (1972), no. 3, 449–450.
- [14] B. Gordon, W. H. Mills, and L. R. Welch, *Some new difference sets*, Canad. J. Math. **14** (1962), 614–625.
- [15] K. G. Hare and S. Yazdani, *Fekete-like polynomials*, J. Number Theory **130** (2010), 2198–2213.
- [16] 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.
- [17] T. Høholdt and H. E. Jensen, *Determination of the merit factor of Legendre sequences*, IEEE Trans. Inform. Theory **34** (1988), no. 1, 161–164.
- [18] 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.
- [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** (2013), no. 4, 882–906.
- [20] ———, *Littlewood polynomials with small L^4 norm*, Adv. Math. **241** (2013), 127–136.
- [21] 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), no. 3, 617–626.
- [22] M. Hall Jr., *A survey of difference sets*, Proc. Amer. Math. Soc. **7** (1956), 975–986.
- [23] D. Jungnickel, *Difference sets*, Contemporary design theory, Wiley-Intersci. Ser. Discrete Math. Optim., Wiley, New York, 1992, pp. 241–324.
- [24] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of Mathematics Studies, vol. 116, Princeton University Press, Princeton, NJ, 1988.
- [25] A. Lempel, M. Cohn, and W. L. Eastman, *A class of balanced binary sequences with optimal autocorrelation properties*, IEEE Trans. Inform. Theory **IT-23** (1977), no. 1, 38–42.
- [26] R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.
- [27] 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), no. 1, 367–376.
- [28] ———, *Some problems in real and complex analysis*, D. C. Heath and Co. Raytheon Education Co., Lexington, Mass., 1968.
- [29] A. Maschietti, *Difference sets and hyperovals*, Des. Codes Cryptogr. **14** (1998), no. 1, 89–98.
- [30] V. M. Sidel'nikov, *Some k -valued pseudo-random sequences and nearly equidistant codes*, Probl. Inform. Transm. **5** (1969), 12–16.
- [31] A. L. Whiteman, *The cyclotomic numbers of order twelve*, Acta Arith. **6** (1960), 53–76.
- [32] A. Zygmund, *Trigonometric series. Vols. I, II*, 2nd ed., Cambridge University Press, New York, 1959.

DEPARTMENT OF MATHEMATICS, PADERBORN UNIVERSITY, WARBURGER STR. 100,
33098 PADERBORN, GERMANY.

E-mail address, Ch. Günther: chriguen@math.upb.de

DEPARTMENT OF MATHEMATICS, PADERBORN UNIVERSITY, WARBURGER STR. 100,
33098 PADERBORN, GERMANY.

E-mail address, K.-U. Schmidt: kus@math.upb.de