Universität Paderborn

Flat polynomials, low autocorrelation sequences, and difference sets

Christian Günther

Dissertation

zur Erlangung des Grades
„Doktor der Naturwissenschaften“ (Dr. rer. nat.)

vorgelegt dem Institut für Mathematik
der Fakultät für Elektrotechnik, Informatik und Mathematik
der Universität Paderborn

Dezember 2018

Gutachter: Prof. Dr. Kai-Uwe Schmidt
Univ.-Doz. Dr. Arne Winterhof
Prof. Dr. Tor Helleseth

betreut von Prof. Dr. Kai-Uwe Schmidt

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my thesis advisor Prof. Kai-Uwe Schmidt for the continuous support of my doctoral studies, for his patience and motivation, for his immense knowledge, for the opportunities to attend various top-level conferences all over the world, and for providing excellent working conditions at Otto von Guericke University of Magdeburg and at Paderborn University. I would like to thank him as well for writing one of the three reviews of this thesis.

I wish to thank Univ.-Doz. Arne Winterhof from the Johann Radon Institute for Computational and Applied Mathematics in Linz and Prof. Helleseth from the University of Bergen for writing the other reviews.

I also want to thank all the former and present fellow students, colleagues, and friends at Magdeburg and Paderborn. I am especially thankful to Sascha, Dariusz, Josefin, and Stephan. I couldn't have done it without you.

Last but not least, I would like to thank my parents for supporting me spiritually throughout studying mathematics and my whole life in general.

Paderborn, December 2018.

To my parents and Sascha.

Kurzfassung

Die vorliegende Dissertation beschäftigt sich mit den aperiodischen Korrelationseigenschaften binärer und unimodularer Folgen endlicher Länge. Die aperiodische Kreuzkorrelation ist ein Maß für die Ähnlichkeit einer Folge zu einer verschobenen Kopie einer anderen Folge. Wenn beide Folgen gleich sind, wird die Kreuzkorrelation auch Autokorrelation genannt. Von besonderem Interesse sind lange Folgen, deren sämtliche aperiodische Korrelationen betragsmäßig klein sind, da sie zahlreiche Anwendungen, unter anderem in der digitalen Nachrichtentechnik, haben.

Der Merit-Faktor und das Peak-Sidelobe-Level sind die beiden wichtigsten Maße dafür, dass die aperiodischen Autokorrelationen einer Folge klein sind. Wir untersuchen den asymptotischen Merit-Faktor und das asymptotische Peak-Sidelobe-Level von Familien binärer Folgen. Dabei liefern wir, unter anderem, erstmals seit 1991 wesentlich neue Beispiele für Familien binärer Folgen, für die wir den asymptotischen Merit-Faktor bestimmen können.

In der Funktionentheorie tauchen aperiodische Autokorrelationen naturgemäß bei der Untersuchung von L^α-Normen von Polynomen auf. Polynome, die eine kleine L^α-Norm haben und deren Koeffizienten nur die Werte -1 und 1 annehmen, sind von besonderem Interesse. Wir bestimmen explizite und rekursive Formeln für das asymptotische Verhältnis von L^α-Norm und L^2-Norm zweier spezifischer Familien von Polynomen mit Koeffizienten aus $\{-1, 1\}$ für unendlich viele α.

Schließlich betrachten wir ein kombiniertes Maß dafür, dass sämtliche aperiodische Auto- und Kreuzkorrelationen eines Paares von Folgen klein sind. Insbesondere konstruieren wir Paare unimodularer Folgen, die in Hinsicht auf dieses Maß asymptotisch optimal sind.

Abstract

The thesis at hand deals with the aperiodic correlation properties of binary and unimodular sequences. The aperiodic crosscorrelation is a measure for the similarity of a sequence to a possibly shifted copy of another sequence. If both sequences are equal, then the aperiodic crosscorrelation reduces to the aperiodic autocorrelation. Of particular interest are long sequences whose correlations are small in magnitude, mainly because such sequences have natural applications in digital communications.

The two most important measures for the collective smallness of the aperiodic autocorrelations of a sequence are the merit factor and the peak sidelobe level. We examine the merit factor and the peak sidelobe level of families of binary sequences. Among other things, we determine the asymptotic merit factors of several families of binary sequences, providing the first essentially new examples since 1991.

For complex analysts, the aperiodic autocorrelations arise naturally in the study of L^α norms of polynomials. Of particular interest are polynomials that have a small L^α norm and whose coefficients are either -1 or 1. We provide explicit and recursive formulas for the asymptotic ratio of L^α and L^2 norm of two specific families of polynomials with coefficients in $\{-1, 1\}$ for infinitely many α.

Finally, we study a combined measure for the collective smallness of aperiodic auto- and crosscorrelations of sequence pairs. In particular, we exhibit pairs of unimodular sequences which are, in view of this measure, asymptotically optimal.

Table of contents

Chapter 1

Introduction and thesis overview

1.1 Aperiodic correlations

A *sequence* A of length n is an n-tuple $(a_0, a_1, \ldots, a_{n-1})$ where each a_j is a complex number. It is convenient to extend the definition and write $a_{j+n} = a_j$ for all integers j.

Let $A = (a_0, a_1, \ldots, a_{n-1})$ and $B = (b_0, b_1, \ldots, b_{n-1})$ be two sequences of length n. The *aperiodic crosscorrelation* of A and B at shift $u \in \mathbb{Z}$ is given by

$$C_{A,B}(u) = \sum_{0 \le j,\, j+u < n} a_j \overline{b_{j+u}}.$$

The *aperiodic autocorrelation* of A at shift u is $C_{A,A}(u)$, which we abbreviate as $C_A(u)$. Notice that $C_{A,B}(u)$ and $C_A(u)$ can only be nonzero for $-n < u < n$. Furthermore, it is not hard to show that

$$C_{A,B}(u) = \overline{C_{B,A}(-u)} \quad \text{for each } u \in \mathbb{Z},$$

and, in particular,

$$C_A(u) = \overline{C_A(-u)} \quad \text{for each } u \in \mathbb{Z}. \tag{1.1}$$

Thus, when considering magnitudes of aperiodic correlations, it is sufficient to consider only shifts u in the set $\{0, 1, \ldots, n-1\}$.

Since the 1950s there is sustained interest in long sequences with small correlations (see [127], [60], and [113] for excellent surveys), mainly because small correlation helps to separate a useful signal from noise or unwanted signals. In particular, small cross-correlation is usually required to ensure that sequences can be distinguished well from each other, and small autocorrelation is usually required to keep the transmitter and the receiver synchronised. Therefore, such sequences have natural applications in digital communications.

For applications, of particular interest are sequences whose entries have the same magnitude and lie within a small set. A sequence is called *binary* if each entry is -1 or 1 and it is called *unimodular* if each entry has unit magnitude. Below, we summarise two of the meta problems that are considered within this thesis. The first problem is one of the most challenging problems in sequence design.

Problem 1.1. *Find binary (unimodular) sequences A of large length n for which the elements in the set $\{|C_A(u)|\colon 0 < u < n\}$ are collectively as small as possible.*

For a unimodular sequence A of length n, we always have $C_A(0) = n$. Therefore, we call $C_A(0)$ the *trivial* aperiodic autocorrelation of A and omitted it in the set in Problem 1.1. For integral u with $0 < |u| < n$, the values $C_A(u)$ are called *nontrivial* aperiodic autocorrelations of A.

Another problem that is examined within this thesis is the following.

Problem 1.2. *Find binary (unimodular) sequences A and B of large length n for which the elements in the set*

$$\{|C_A(u)|\colon 0 < u < n\} \cup \{|C_B(u)|\colon 0 < u < n\} \cup \{|C_{A,B}(u)|\colon 0 \le u < n\}$$

are collectively as small as possible.

1.2 The L^α norm of polynomials

Sequences can be identified with polynomials and vice versa. Given a sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n, we can represent A via the polynomial

$$f_A(z) = \sum_{j=0}^{n-1} a_j z^j \in \mathbb{C}[z]$$

and call A the *coefficient sequence* of f_A.

For real $\alpha \ge 1$, the L^α *norm* of a polynomial f in $\mathbb{C}[z]$ on the complex unit circle is

$$\|f\|_\alpha = \left(\frac{1}{2\pi}\int_0^{2\pi} |f(e^{i\theta})|^\alpha \, d\theta\right)^{1/\alpha}, \tag{1.2}$$

and its supremum norm is $\|f\|_\infty = \max_{\theta\in[0,2\pi]}|f(e^{i\theta})|$. There are various extremal problems, originally raised by Erdős, Littlewood, and others, concerning the behaviour of such norms for polynomials with all coefficients in $\{-1, 1\}$, which are today called *Littlewood polynomials* (see Littlewood [87], Borwein [11], and Erdélyi [32] for surveys on selected problems). Roughly speaking, such problems ask for Littlewood polynomials f that provide a good approximation to a function that is constant on the complex unit circle, and in particular have small L^α norm on the complex unit circle. Notice that this constant is

necessarily $\|f\|_2 = \sqrt{1+\deg f}$ since, for a polynomial f_A in $\mathbb{C}[z]$ of degree $n-1$ with coefficient sequence $A = (a_0, a_1, \ldots, a_{n-1})$, we have

$$\|f_A\|_2^2 = \frac{1}{2\pi} \sum_{j,k=0}^{n-1} a_j \overline{a_k} \int_0^{2\pi} e^{i(j-k)\theta}\, d\theta = \sum_{j=0}^{n-1} |a_j|^2. \tag{1.3}$$

Therefore, another meta problem that is considered within this thesis is the following.

Problem 1.3. *Find Littlewood polynomials f of large degree n such that $\|f\|_\alpha$ is as small as possible.*

Of particular interest is the L^4 norm of Littlewood polynomials, since it is easier to compute than most other norms. In fact, there is a close relationship between the L^4 norm of a polynomial and the aperiodic autocorrelations of its coefficient sequence.

Proposition 1.2.1. *Let $f_A \in \mathbb{C}[z]$ be a polynomial of degree $n-1$ with coefficient sequence A.*

(i) For all z on the complex unit circle, we have

$$|f_A(z)|^2 = \sum_{u=-n+1}^{n-1} \overline{C_A(u)} z^u.$$

(ii) We have

$$\|f_A\|_4^4 = 2\sum_{u=1}^{n-1} |C_A(u)|^2 + C_A(0)^2.$$

Proof. Write $A = (a_0, \ldots, a_{n-1})$. Then, for all z with $|z| = 1$, we have

$$\begin{aligned} |f_A(z)|^2 &= \sum_{j,k=0}^{n-1} a_j \overline{a_k} z^{j-k} \\ &= \sum_{u=-n+1}^{n-1} \sum_{0 \le k,\, k+u < n} a_{k+u} \overline{a_k} z^u \\ &= \sum_{u=-n+1}^{n-1} \overline{C_A(u)} z^u, \end{aligned}$$

where we put $u = j-k$ in third step. This proves (i). From (i) we then find that

$$\|f_A\|_4^4 = \frac{1}{2\pi} \int_0^{2\pi} \sum_{u,v=-n+1}^{n-1} \overline{C_A(u) C_A(v)} e^{i\theta(u+v)}\, d\theta.$$

Interchange integration and summations to obtain

$$\|f_A\|_4^4 = \sum_{u=-n+1}^{n-1} \overline{C_A(u)C_A(-u)}.$$

Applying (1.1) twice leads to

$$\|f_A\|_4^4 = 2\sum_{u=1}^{n-1}|C_A(u)|^2 + |C_A(0)|^2,$$

from which part (ii) follows by noting that $C_A(0)$ is real. □

From Proposition 1.2.1 (ii) we find that the problem of searching for Littlewood polynomials with small L^4 norm (Problem 1.3 with $\alpha = 4$) is closely related to the problem of searching for binary sequences whose aperiodic autocorrelations are small in magnitude (Problem 1.1). In fact, we shall see in Section 1.5 that both problems are, in a certain sense, equivalent.

1.3 Barker sequences

By a simple parity argument not all nontrivial aperiodic autocorrelations of a binary sequence of length greater than 1 can be zero. Therefore, in view of Problem 1.1, an ideal binary sequence A has the property that $|C_A(u)|$ is either 0 or 1 for all nonzero shifts u. Such sequences are called *Barker sequences*[1].

It is straightforward to show that if $A = (a_0, a_1, \ldots, a_{n-1})$ is a Barker sequence of length n and $s, t \in \{0, 1\}$ are fixed, then the sequence $B = (b_0, b_1, \ldots, b_{n-1})$ given by

$$b_j = (-1)^{s+tj} a_j \quad \text{for} \quad 0 \le j < n$$

is also a Barker sequence. Therefore, without loss of generality, we may always assume that a Barker sequence of length greater than 1 starts with two ones. In Figure 1.1 we see a complete list of all known such Barker sequences, where here and throughout, we write + for 1 and − for −1.

At least since 1960 [125] it has been conjectured that there exists no Barker sequence of length greater than 13.

Conjecture 1.3.1 ([125])**.** *There exists no Barker sequence of length greater than* 13*.*

In 1961 Turyn and Storer [126] proved that this conjecture is true for odd lengths by showing that any putative Barker sequence of odd length has some repeating structure

[1]We note that in 1953 Barker [6] originally asked for binary sequences with the property that all nontrivial aperiodic autocorrelations lie in $\{0, -1\}$, but over the years (see for example [131] and [127]) it became customary to relax Barkers condition slightly.

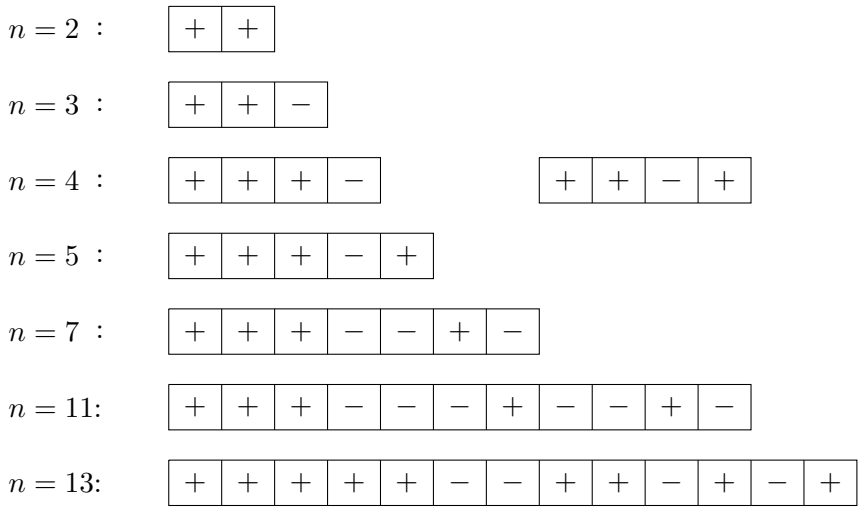

Figure 1.1: Barker sequences of length n starting with two ones.

from which it follows that the sequence must be short. Although their proof is elementary, it is somewhat complicated. Schmidt and Willms [114] gave a very nice and simple proof.

Theorem 1.3.2 ([126], [114])**.** *There exists no Barker sequence of odd length greater than* 13*.*

Also strong partial results on the length of a putative Barker sequence of even length are known. For example, we have the following theorem.

Theorem 1.3.3 ([31])**.** *If A is a Barker sequence of even length n, then n has no prime divisor that is congruent to* 3 *modulo* 4*.*

The latest results of Leung and Schmidt [84] lead to:

Theorem 1.3.4 ([84])**.** *There is no Barker sequence of length n for $13 < n < 4 \cdot 10^{33}$.*

However, although there is overwhelming evidence that no long Barker sequences exist, Conjecture 1.3.1 is still unsettled. In view of the apparent nonexistence of long Barker sequences, several authors have studied different measures for the collective smallness of the aperiodic autocorrelations of binary sequences. The two most important such measures are the *peak sidelobe level* and the *merit factor*.

1.4 The peak sidelobe level of binary sequences

Let A be a binary sequence of length $n > 1$. The *peak sidelobe level* of A is given by

$$\mathrm{M}(A) = \max_{0<u<n} |C_A(u)|,$$

and the most appreciated sequences are of course those with a small peak sidelobe level. By a parity argument the peak sidelobe level of a binary sequence is at least 1. In particular, a binary sequence has peak sidelobe level 1 if and only if it is a Barker sequence.

Define M_n to be the minimum of $\mathrm{M}(A)$ taken over all 2^n binary sequences A of length n. The principal problem concerning the peak sidelobe level of binary sequences is to understand the behaviour of M_n as $n \to \infty$:

Problem 1.4. *Determine the asymptotic behaviour of M_n as $n \to \infty$.*

It is conjectured (see for example [113, Conjecture 3.4.1]) that M_n grows like a small constant times $\sqrt{n}$. It is easy to see that the correctness of this conjecture would imply that there are only finitely many Barker sequences.

We consider an example.

Example 1.4.1. Let

$$A = (+ + + + + - + - - + - + + + - - + +).$$

All nontrivial aperiodic autocorrelations of A are in the set $\{-2, 0, 1, 2\}$, so that $\mathrm{M}(A) = 2$. Thus, in view of the nonexistence of a Barker sequence of length 18 (see Theorem 1.3.4), we know $M_{18} = 2$.

Known results

We now briefly review known results on the peak sidelobe level of binary sequences. Already in 1968 Turyn [127] knew that $M_n \leq 2$ for $n \leq 21$. Over the years an enormous amount of (computational) effort has been invested in finding binary sequences with small peak sidelobe level, which leads to the determination of M_n via exhaustive search up to $n = 84$ (see [82] for the latest results). In particular, it has been shown (see also [113, Section 3.4]) that M_n satisfies:

$$\begin{aligned} M_n &= 1 \quad \text{for each } n \in \{2, 3, 4, 5, 7, 11, 13\}, \\ M_n &\leq 2 \quad \text{for each } n \leq 21, \\ M_n &\leq 3 \quad \text{for each } n \leq 48, \\ M_n &\leq 4 \quad \text{for each } n \leq 82, \\ M_n &\leq 5 \quad \text{for each } n \leq 105. \end{aligned}$$

Recall that a sequence $X_1, X_2, X_3, \ldots$ of random variables converges *in probability* to a constant c if, for all $\epsilon > 0$, we have

$$\Pr[|X_n - c| > \epsilon] \to 0$$

as $n \to \infty$. The following theorem gives the peak sidelobe level of random binary sequences.

Theorem 1.4.2 ([112]). *For each integer $n > 1$, let A_n be drawn uniformly at random from $\{-1, 1\}^n$. Then, as $n \to \infty$,*

$$\frac{\mathrm{M}(A_n)}{\sqrt{2n \log n}} \to 1 \quad \textit{in probability}$$

and

$$\frac{\mathrm{E}(\mathrm{M}(A_n))}{\sqrt{2n \log n}} \to 1.$$

Theorem 1.4.2 says that the peak sidelobe level of "most" binary sequences of length n is close to $\sqrt{2n \log n}$. However, there could exist "rare" binary sequences whose peak sidelobe level grows like $O(\sqrt{n} \log \log n)$ or $O(\sqrt{n})$. It is even possible that M_n grows more slowly than $c\sqrt{n}$ for each $c > 0$, which would be an earth-shattering result.

Although the peak sidelobe level of almost all binary sequences grows like $\sqrt{2n \log n}$, there is only one known *specific* family of binary sequences whose peak sidelobe level is of order $O(\sqrt{n \log n})$. This family was constructed by Schmidt [110] using techniques from probabilistic combinatorics. We briefly review his construction.

Construction 1.4.3 ([110]). Let n be a positive integer and write $\omega = \sqrt{2 \log(2n)/n}$. Construct the binary sequence $B_n = (b_0, b_1, \ldots, b_{n-1})$ of length n recursively via

$$b_j = -\operatorname{sign}\left(\sum_{k=1}^{j-1} b_{j-k} \sinh\left(\omega \sum_{\ell=0}^{j-k-1} b_\ell b_{\ell+k} \right) \right) \quad \text{for each } j = 0, 1, \ldots, n-1,$$

where, by convention, $\operatorname{sign}(0) = -1$.

Notice that the first two entries of the sequence B_n are always equal to 1.

Example 1.4.4. The first few nontrivial sequences that arise from Construction 1.4.3 are:

$$\begin{aligned} B_3 &= (+\,+\,-), \\ B_4 &= (+\,+\,-\,+), \\ B_5 &= (+\,+\,-\,+\,+), \\ B_6 &= (+\,+\,-\,+\,+\,-). \end{aligned}$$

From this pattern one could guess that B_n is always an initial segment of B_{n+1}. It is remarked in [110] that this is in general not the case. Indeed, we have

$$\begin{aligned} B_{18} &= (+\,+\,-\,+\,+\,+\,-\,-\,-\,-\,+\,-\,+\,-\,-\,-\,-\,-), \\ B_{19} &= (+\,+\,-\,+\,+\,+\,-\,-\,-\,-\,+\,-\,+\,+\,-\,-\,+\,-\,+), \end{aligned}$$

which differ at the 14-th and the 17-th entry.

We have the following theorem, which gives the best known upper bound on infinitely many values of M_n.

Theorem 1.4.5 ([110])**.** *Let $n > 1$ and let B_n be the binary sequence of length n that arises from Construction 1.4.3. Then*

$$\mathrm{M}(B_n) \leq \sqrt{2n \log(2n)}.$$

One of the most challenging research problems concerning the peak sidelobe level of binary sequences can therefore be summarised as follows:

Problem 1.5. *Find a family of binary sequences of length n whose peak sidelobe level grows more slowly than $c\sqrt{n \log n}$ for each constant $c > 0$.*

We note that there are also some partial results on the peak sidelobe level of other specific families of binary sequences (see [109], [58], and [89]), which however only guarantee a peak sidelobe level that is worse than that of a typical binary sequence given in Theorem 1.4.2. For excellent surveys on the topic we refer to Jedwab [60, Section 5] and Schmidt [113, Sections 3.3 and 3.4].

In the radar literature appears frequently the claim that the peak sidelobe level of a specific family of binary sequences, namely the so-called *Galois sequences*, grows like $O(\sqrt{n})$ (see [63, Section 3] for a list of references). Additionally, numerically [28] it seems that the peak sidelobe level of almost all Galois sequences grows like $O(\sqrt{n})$ (see also the forthcoming Conjecture 5.1.2). Therefore, Galois sequences seem to be very promising candidates in order to attack Problem 1.5. However, there is also numerical evidence [63] that not all Galois sequences have a "small" peak sidelobe level, so that the claim from the radar literature seems to be wrong. Also in order to learn more on the asymptotic behaviour of M_n in Problem 1.4, we examine in Chapter 5 the peak sidelobe level of Galois sequences. In particular, we give theoretical evidence that there exists a family of Galois sequences whose peak sidelobe level grows at least with order $\sqrt{n} \log \log \log n$.

1.5 The merit factor of binary sequences

Let A be a binary sequence of length $n > 1$. We now consider our second measure for the collective smallness of the aperiodic autocorrelations of A, which was defined by Golay [41] in 1972: the *merit factor* of A, which is given by

$$\mathrm{F}(A) = \frac{n^2}{\sum_{u \in \mathbb{Z} \setminus \{0\}} C_A(u)^2}.$$

By (1.1) the merit factor of A can alternatively be written as

$$\mathrm{F}(A) = \frac{n^2}{2\sum_{u=1}^{n-1} C_A(u)^2}.$$

In view of Problem 1.1 the best sequences are those with a large merit factor, which means that the sum of squared nontrivial aperiodic autocorrelations of the sequence is small when compared to the squared trivial aperiodic autocorrelation (which always equals n^2 for binary sequences of length n). Such sequences have applications in digital communications [7] and in condensed matter physics [8], for example.

Define F_n to be the maximum of $\mathrm{F}(A)$ taken over all 2^n binary sequences A of length n. It is not hard to show that if A is a Barker sequence of length n, then $\mathrm{F}(A) = F_n$. The intrinsic goal concerning the merit factor of binary sequences is to understand the behaviour of F_n as $n \to \infty$:

Problem 1.6. *Determine the asymptotic behaviour of F_n as $n \to \infty$. In particular, determine*

$$\limsup_{n\to\infty} F_n.$$

We consider an example.

Example 1.5.1. Let $A = (+++++--+-+-+)$ be a Barker sequence of length 13. Then we have

$$C_A(u)^2 = \begin{cases} 0 & \text{for } u \in \{1, 3, \ldots, 11\} \\ 1 & \text{for } u \in \{2, 4, \ldots, 12\}, \end{cases}$$

so that $\mathrm{F}(A) = 13^2/12 = 14.0833\ldots$, and therefore $F_{13} = 14.0833\ldots$.

In fact there is no binary sequence known that has a larger merit factor than that obtained in Example 1.5.1.

Old conjectures

Several conjectures concerning Problem 1.6 appeared in the literature. We state two contradicting conjectures, the first is due to Littlewood [86] in 1966 and the second is due to Golay [42] in 1982.

Conjecture 1.5.2 ([86])**.** *We have*

$$\limsup_{n\to\infty} F_n = \infty.$$

Conjecture 1.5.3 ([42])**.** *We have*

$$\limsup_{n\to\infty} F_n = 12.32\ldots.$$

Connections to the peak sidelobe level and the L^4 norm

There is a close relationship between the merit factor and the peak sidelobe level of a binary sequence, which is straightforward to prove.

Proposition 1.5.4. *Let A be a binary sequence of length $n > 1$. Then*

$$\mathrm{F}(A) > \frac{n}{2\,\mathrm{M}(A)^2}.$$

The next result is a consequence of Proposition 1.5.4.

Corollary 1.5.5. *Let n take values in an infinite set of positive integers. For each n, let A_n be a binary sequence of length n.*

(i) If $\liminf_{n\to\infty} \mathrm{M}(A_n)/\sqrt{n} = 0$, then $\limsup_{n\to\infty} \mathrm{F}(A_n) = \infty$.

(ii) If $\limsup_{n\to\infty} \mathrm{F}(A_n)$ is finite, then $\liminf_{n\to\infty} \mathrm{M}(A_n)/\sqrt{n} > 0$.

Corollay 1.5.5 implies that if M_n would grow more slowly than $c\sqrt{n}$ for each constant $c > 0$, then $\limsup_{n\to\infty} F_n = \infty$. On the other hand, if $\limsup_{n\to\infty} F_n$ is bounded, then M_n grows at least with order $\sqrt{n}$.

Let A be a binary sequence of length $n > 1$ and let f_A be the Littlewood polynomial of degree $n-1$ with coefficient sequence A. Then Proposition 1.2.1 (ii) simplifies to

$$\|f_A\|_4^4 = 2\sum_{u=1}^{n-1} C_A(u)^2 + n^2,$$

or equivalently,

$$\mathrm{F}(A) = \frac{n^2}{\|f_A\|_4^4 - n^2}. \tag{1.4}$$

That means that searching for Littlewood polynomials of large degree and small L^4 norm (Problem 1.3 with $\alpha = 4$) is the same problem as finding long binary sequences with large merit factor (Problem 1.6). In particular, combinatorialists and complex analysts studied independently the same problem over decades.

Known results

We now briefly review known results concerning the merit factor of binary sequences. As for the peak sidelobe level, much (computational) effort has been invested in finding long sequences with large merit factor. The values of F_n are determined via exhaustive search up to $n = 66$ (see [99] for the latest results), we visualise them in Figure 1.2. Effective methods have been developed to find large values for the merit factors of binary sequences

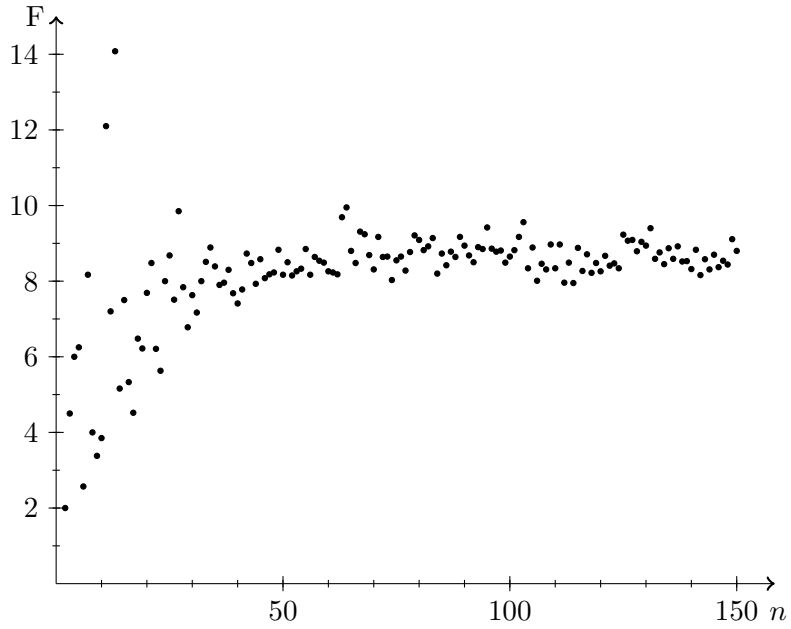

Figure 1.2: The largest merit factors (for $2 \leq n \leq 66$) and the best known merit factors (for $67 \leq n \leq 150$) of binary sequences of length n.

for larger lengths n (see [17] for the latest results). These values are listed in [16] and are visualised in Figure 1.2 up to $n = 150$.

The next result due to Sarwate [108] gives the merit factor of a typical binary sequence. It is a benchmark result in the asymptotic merit factor calculation.

Theorem 1.5.6 ([108])**.** *Let $n > 1$ and let A be drawn uniformly at random from $\{-1, 1\}^n$. Then*

$$\mathrm{E}\left(\frac{1}{\mathrm{F}(A)}\right) = 1 - \frac{1}{n}.$$

In particular, we deduce from Theorem 1.5.6 that the asymptotic mean value over the reciprocal merit factors over all binary sequences of length n is 1 as $n \to \infty$. Therefore, we expect that "good" binary sequences have a merit factor greater than 1.

An ultimate goal concerning the merit factor problem is to find infinite families of binary sequences with large merit factors such that we know the *exact* merit factor of each member in the family. This was done for the *Shapiro sequences* [87], which we consider next.

Construction 1.5.7 ([118])**.** Let $A_0 = B_0 = (1)$ and, for $m \geq 0$, define the *Shapiro sequences* A_m and B_m of length 2^m recursively via

$$A_m = (A_{m-1}, B_{m-1}) \quad \text{and} \quad B_m = (A_{m-1}, -B_{m-1}).$$

Example 1.5.8. The first few nontrivial Shapiro sequences of length 2^m are:

$$\begin{aligned} m = 1: &\qquad A_1 = (++), &&\qquad B_1 = (+-),\\ m = 2: &\qquad A_2 = (+++-), &&\qquad B_2 = (++-+),\\ m = 3: &\qquad A_3 = (+++-++-+), &&\qquad B_3 = (+++---+-). \end{aligned}$$

In 1968 Littlewood [87] determined the merit factor of Shapiro sequences.

Theorem 1.5.9 ([87])**.** *Let $m \geq 1$ and let A_m and B_m be the Shapiro sequences of length 2^m. We have*

$$\mathrm{F}(A_m) = \mathrm{F}(B_m) = \frac{3}{1-(-1/2)^m}.$$

In particular, Shapiro sequences have an asymptotic merit factor of 3.

Unfortunately, there is no other nontrivial infinite family of binary sequences for which we know the exact merit factor of each member in the family. Therefore, we are interested in asymptotic results; but also in this case, in spite of substantial progress on the merit factor problem in the last fifty years (see [59], [56], [14], [60, Section 6], and [113, Section 3.5] for surveys), modulo generalisations and variations, only two more nontrivial families of binary sequences are known, for which we can compute the asymptotic merit factor. These are *Legendre* and *Galois sequences*, which are closely related to *Paley* and *Singer difference sets*.

The following result due to Jedwab, Katz, and Schmidt [62] comes from Legendre sequences and gives the largest known asymptotic merit factor for binary sequences (see the forthcoming Corollary 3.5.4 for a precise statement). Here,

$$\Phi = 6.342061\ldots \text{ is the largest root of } 29x^3 - 249x^2 + 417x - 27.$$

Theorem 1.5.10 ([62])**.** *There exists a family of binary sequences whose asymptotic merit factor is equal to Φ.*

The largest asymptotic merit factor that has been obtained from Galois sequences equals the cubic algebraic number $3.342065\ldots$ [61] (see the forthcoming Corollary 3.4.5 for a precise statement). Therefore, in view of Problem 1.6, the current state of knowledge can be summarised as

$$\Phi \leq \limsup_{n\to\infty} F_n \leq \infty,$$

from which one of the most challenging research problems concerning the merit factor of binary sequences follows:

Problem 1.7. *Find a family of binary sequences whose asymptotic merit factor is greater than Φ.*

New results

Most known constructions of binary sequences with large merit factor arise (sometimes in a subtle way) from difference sets, in particular from Paley and Singer difference sets. In Chapter 3 we shall examine the merit factors of binary sequences that come from other difference sets, providing the first essentially new examples since 1991 [64]. In particular, we prove a very general theorem on the asymptotic merit factor of binary sequences that arise from cyclotomy, which includes results on *Hall* and Paley difference sets, and in particular includes Theorem 1.5.10 as special cases. In addition, we establish the asymptotic merit factors of sequences derived from *Gordon-Mills-Welch difference sets* and *Sidelnikov almost difference sets*, proving two conjectures from 2013 ([61, Conjectures 7.1 and 7.2]) in the affirmative and explaining numerical evidence made in [54].

1.6 Flat polynomials

This section is devoted to Problem 1.3. Let

$$A = (+ + + + + - - + + - + - +)$$

be a Barker sequence of length 13 and let

$$B = (- + + - + - + - - - + + +)$$

be a randomly chosen binary sequence of the same length. In Figure 1.3 we see the magnitudes of the Littlewood polynomials f_A and f_B (with coefficient sequences A and B, respectively) on the complex unit circle. The polynomial f_A approximates the function that is constant to $\sqrt{13}$ much better than f_B. In fact, f_A is, in a certain sense, the best possible approximation.

Old conjectures

Several conjectures have been posed that address Problem 1.3. In 1960, Newman [94] mentioned the following conjecture.

Conjecture 1.6.1 ([94])**.** *There exists a constant $c_1 > 0$ such that*

$$\frac{\|f\|_1}{\|f\|_2} \leq 1 - c_1$$

for every nonconstant Littlewood polynomial f.

A similar conjecture concerning the L^4 norm is due to Golay [42].

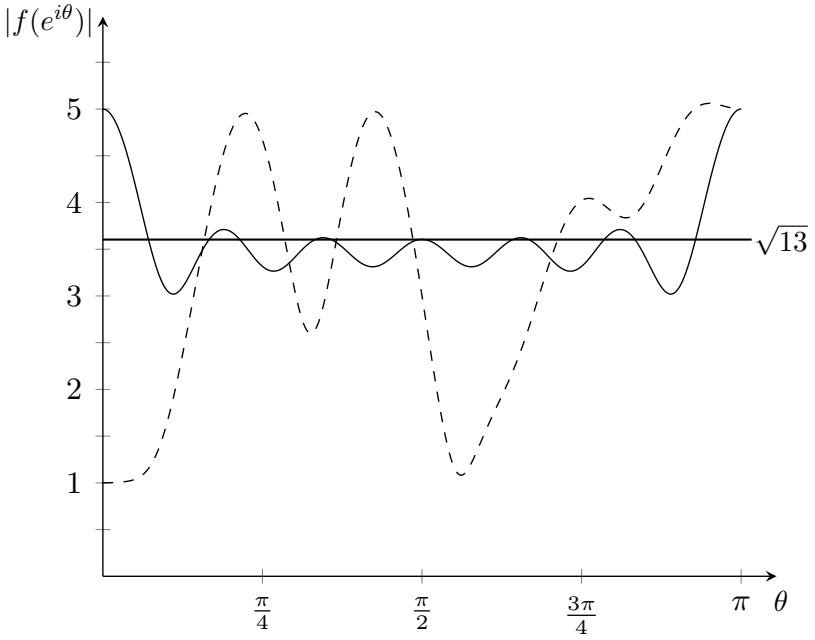

Figure 1.3: The magnitudes of the polynomials f_A (solid line) and f_B (dashed line) of degree 12 on the complex unit circle, where $A = (+ + + + + - - + + - + - +)$ and $B = (- + + - + - + - - - + + +)$.

Conjecture 1.6.2 ([42])**.** *There exists a constant $c_4 > 0$ such that*

$$\frac{\|f\|_4}{\|f\|_2} \geq 1 + c_4$$

for every nonconstant Littlewood polynomial f.

Notice that, in view of (1.4) and (1.3), this is just Conjecture 1.5.3 in a weak form. Littlewood [86] conjectured that there is no such constant as in Conjecture 1.6.2 (see also Conjecture 1.5.2). Golay's Conjecture 1.6.2 implies another famous conjecture due to Erdős [33], [96].

Conjecture 1.6.3 ([33], [96])**.** *There exists a constant $c_\infty > 0$ such that*

$$\frac{\|f\|_\infty}{\|f\|_2} \geq 1 + c_\infty$$

for every nonconstant Littlewood polynomial f.

All these conjectures are wide open. In fact, if any of the Conjectures 1.6.1, 1.6.2, or 1.6.3 is true, then there are only finitely many Barker sequences.

Known results

The following result on the monotonicity of L^α norms is well known.

Proposition 1.6.4. *Let $f \in \mathbb{C}[z]$.*

(i) For $\alpha \geq \beta \geq 1$, we have $\|f\|_\alpha \geq \|f\|_\beta$.

(ii) We have $\lim_{\alpha\to\infty}\|f\|_\alpha = \|f\|_\infty$.

We now briefly review known results concerning the L^α norm of Littlewood polynomials. In the next theorem we extend the definition of $\|\cdot\|_\alpha$ in (1.2) to all real $\alpha > 0$, although it is only a norm for $\alpha \geq 1$. The first result is due to Halász [51] and the second due to Borwein and Lockhart [15], in which

$$\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}dt$$

denotes the *Gamma function*, satisfying $\Gamma(n+1) = n!$ for nonnegative integers n.

Theorem 1.6.5 ([51], [15])**.** *For each positive integer n, let f_n be a Littlewood polynomial of degree $n-1$ whose coefficient sequence is drawn uniformly at random from $\{-1,1\}^n$. Then the following hold as $n \to \infty$.*

(i) We have

$$\frac{\|f_n\|_\infty}{\sqrt{n\log n}} \to 1 \quad \textit{in probability.}$$

(ii) Let $0 < \alpha < \infty$. Then

$$\left(\frac{\|f_n\|_\alpha}{\sqrt{n}}\right)^\alpha \to \Gamma(1+\alpha/2) \quad \textit{in probability.}$$

In particular, Theorem 1.6.5 says that if α is a positive integer, then for random Littlewood polynomials f_n of degree $n-1$ we have, as $n \to \infty$,

$$\left(\frac{\|f_n\|_{2\alpha}}{\sqrt{n}}\right)^{2\alpha} \to \alpha! \quad \text{in probability.}$$

For $\alpha = 2$, this result can also be obtained from Theorem 1.5.6. For more results on L^α norms of random Littlewood polynomials see also Choi and Erdélyi [20].

New results

Until 2017, there was no known nontrivial *specific* family of Littlewood polynomials for which we can determine the asymptotic behaviour of its L^α norm for infinitely many α. In Chapter 4 we shall examine two families of Littlewood polynomials, namely *Fekete polynomials* (whose coefficient sequences are Legendre sequences) and *Galois polynomials* (whose coefficient sequences are Galois sequences). We give explicit and recursive formulas for the limit of the ratio of L^α and L^2 norm of Fekete and Galois polynomials when α is

an even positive integer and the degree of the polynomials tends to infinity. These results vastly generalise earlier results on the L^4 norm of these polynomials.

After a preprint of our results on the L^α norm of Fekete and Galois polynomials [48] appeared on the arXiv, Rodgers published results on the L^α norm of *Shapiro polynomials* in a preprint of [105] on the arXiv. We now briefly explain his results. Let A_m and B_m be the Shapiro sequences of length 2^m (see Construction 1.5.7). Define the *Shapiro polynomials* s_m and t_m to be the Littlewood polynomials of degree $2^m - 1$ with coefficient sequences A_m and B_m, respectively. Rodgers [105] determined the asymptotic normalised L^α norm of Shapiro polynomials when α is an even positive integer, thereby proving a conjecture attributed in [29] to Saffari.

Theorem 1.6.6 ([105])**.** *Let α be a positive integer and let s_m and t_m be the Shapiro polynomials of degree $2^m - 1$. Then*

$$\lim_{m\to\infty} \left(\frac{\|s_m\|_{2\alpha}}{\sqrt{2^m}} \right)^{2\alpha} = \lim_{m\to\infty} \left(\frac{\|t_m\|_{2\alpha}}{\sqrt{2^m}} \right)^{2\alpha} = \frac{2^\alpha}{\alpha+1}.$$

Since $2^\alpha/(\alpha+1) < \alpha!$ for $\alpha > 1$, the normalised asymptotic L^α norm of Shapiro polynomials is smaller than that of random Littlewood polynomials. The case that $\alpha = 2$ together with (1.4) reproves the fact that the asymptotic merit factor of Shapiro sequences is 3 (see Theorem 1.5.9). In fact, Rodgers [105] proved a more general result: Let X be a random variable which is uniformly distributed on the complex unit circle. Then

$$\frac{s_m(X)}{\sqrt{2^m}} \quad \text{and} \quad \frac{t_m(X)}{\sqrt{2^m}}$$

are asymptotically uniformly distributed in the complex disc of radius $\sqrt{2}$.

1.7 The Pursley-Sarwate criterion of sequences

This section is devoted to Problem 1.2. Let A and B be unimodular sequences of length $n > 1$. The collective smallness of the aperiodic crosscorrelations of A and B is measured by the *crosscorrelation merit factor* of A and B, which is defined to be

$$\mathrm{CF}(A, B) = \frac{n^2}{\sum_{u\in\mathbb{Z}} |C_{A,B}(u)|^2},$$

and good sequence pairs are those with a large crosscorrelation merit factor. Accordingly, extending the definition of the merit factor from binary to unimodular sequences, the collective smallness of the aperiodic autocorrelations of A is measured by the *(autocorrelation) merit factor* of A, which is given by

$$\mathrm{F}(A) = \frac{n^2}{\sum_{u\in\mathbb{Z}\setminus\{0\}} |C_A(u)|^2}.$$

Notice that $1/\mathrm{F}(A) = 1/\mathrm{CF}(A, A) - 1$. In order to motivate the next definition, we consider an example which is also given in [71, Section 9].

Example 1.7.1. For even n, consider the binary sequences

$$A_n = (+ + \cdots +)$$
$$B_n = (+ - + - \cdots + -)$$

of length n. It is easy to see that

$$\mathrm{CF}(A_n, B_n) = n,$$

so that $\mathrm{CF}(A_n, B_n) \to \infty$ as $n \to \infty$. On the other hand, it is also not difficult to show that

$$\mathrm{F}(A_n) = \mathrm{F}(B_n) = \frac{3n}{2n^2 + 1},$$

so that $\mathrm{F}(A_n) \to 0$ and $\mathrm{F}(B_n) \to 0$ as $n \to \infty$. Therefore, it is not interesting to search for pairs of sequences with large crosscorrelation merit factor in isolation from the merit factor of each sequence in the pair.

The best sequence pairs (A, B) are those where $\mathrm{F}(A)$, $\mathrm{F}(B)$, and $\mathrm{CF}(A, B)$ are collectively large. A fundamental relationship between these three quantities is given by

$$1 - (\mathrm{F}(A)\,\mathrm{F}(B))^{-1/2} \leq \mathrm{CF}(A, B)^{-1} \leq 1 + (\mathrm{F}(A)\,\mathrm{F}(B))^{-1/2}, \tag{1.5}$$

as proved by Pursley and Sarwate [104] for binary sequences and generalised by Katz and Moore [73] for unimodular sequences. Following Boothby and Katz [10], we define the *Pursley-Sarwate criterion* of A and B to be

$$\mathrm{PSC}(A, B) = (\mathrm{F}(A)\,\mathrm{F}(B))^{-1/2} + \mathrm{CF}(A, B)^{-1}.$$

From (1.5) we obtain $\mathrm{PSC}(A, B) \geq 1$. Hence, in order to design pairs of sequences (A, B) with simultaneously small aperiodic autocorrelations and crosscorrelations, we would like to have $\mathrm{PSC}(A, B)$ close to 1.

Known results and Golay pairs

We now briefly review known results on the Pursley-Sarwate criterion of sequence pairs (see also [71, Section 11] for a recent survey). Katz [70], Boothby and Katz [10], and Katz, Lee, and Trunov [72] studied the Pursley-Sarwate criterion of sequence pairs derived from Galois, Legendre, Shapiro-like, and related sequences. This gives pairs of unimodular and binary sequences whose Pursley-Sarwate criterion is close to 1, but strictly bounded away from 1, as the sequence length tends to infinity.

In fact, pairs of unimodular sequences (A, B) with $\mathrm{PSC}(A, B) = 1$ were recently classified by Katz and Moore [73] to be exactly the *Golay pairs*. These are pairs of unimodular sequences (A, B) of the same length that satisfy

$$C_A(u) + C_B(u) = 0 \quad \text{for all } u \neq 0.$$

We have the following result.

Theorem 1.7.2 ([73])**.** *Let A and B be unimodular sequences of length $n > 1$. Then $\mathrm{PSC}(A, B) = 1$ if and only if (A, B) is a Golay pair.*

Golay pairs were first studied by Golay [40]. For example, the two sequences $(+++-)$ and $(++-+)$ form a Golay pair. It is surprisingly easy to construct Golay pairs for infinitely many lengths. Indeed, there is a recursive construction that produces a Golay pair of length mn from two Golay pairs of length m and n [128]. In particular, it follows from this construction that the Shapiro sequences of length 2^m form a Golay pair for each m.

The classification in Theorem 1.7.2 does however not say anything about the individual quantities $\mathrm{F}(A)$, $\mathrm{F}(B)$, and $\mathrm{CF}(A, B)$ for a Golay pair (A, B). These values are known for the Shapiro sequences A_m and B_m of length 2^m. From Theorem 1.5.9 we know

$$\mathrm{F}(A_m) = \mathrm{F}(B_m) = \frac{3}{1 - (-1/2)^m}.$$

Since (A_m, B_m) is a Golay pair, we know $\mathrm{PSC}(A_m, B_m) = 1$, so that

$$\mathrm{CF}(A_m, B_m) = \frac{3}{2 + (-1/2)^m}$$

by the definition of the Pursley-Sarwate criterion. Therefore, we have $\mathrm{F}(A_m) \to 3$ and $\mathrm{F}(B_m) \to 3$ and $\mathrm{CF}(A_m, B_m) \to 3/2$ as $m \to \infty$.

New results

In Chapter 6 we exhibit pairs of unimodular sequences for which the Pursley-Sarwate criterion tends to 1 as the sequence length tends to infinity and for which (unlike for general Golay pairs) we can control the autocorrelation and the crosscorrelation merit factor. In particular, we show that there exist unimodular sequence pairs (A_n, B_n) such that

$$\lim_{n\to\infty} \mathrm{F}(A_n) = \lim_{n\to\infty} \mathrm{F}(B_n) = \infty \quad \text{and} \quad \lim_{n\to\infty} \mathrm{CF}(A_n, B_n) = 1.$$

We remark that it is known [95] that there exist unimodular sequences whose merit factor grows without bound. This is very different from the binary case (see Theorem 1.5.10 and Problem 1.7).

In our second result we construct unimodular sequence pairs (A_n, B_n) with asymptotic Pursley-Sarwate criterion equal to 1 such that the autocorrelation and crosscorrelation merit factors are asymptotically balanced, which means that

$$\lim_{n\to\infty} \mathrm{F}(A_n) = \lim_{n\to\infty} \mathrm{F}(B_n) = \lim_{n\to\infty} \mathrm{CF}(A_n, B_n) = 2.$$

Chapter 2

Difference sets and characteristic sequences

2.1 Introduction and chapter overview

We begin with examining Problem 1.1 and focus ourselves on searching for long binary sequences whose aperiodic autocorrelations are small in magnitude. Such sequences must satisfy two conditions, which we give next.

Let $A = (a_0, a_1, \ldots, a_{n-1})$ be a sequence of length n. In order to state a first necessary condition for small aperiodic autocorrelations, we define the *periodic autocorrelation* of A at shift $u \in \mathbb{Z}$ to be

$$R_A(u) = \sum_{j=0}^{n-1} a_j \overline{a_{j+u}}.$$

Recall that the indices of a_{j+u} are taken modulo n if necessary. As for the aperiodic autocorrelations in (1.1), it is not hard to show that

$$R_A(-u) = \overline{R_A(u)} \quad \text{for each } u \in \mathbb{Z}.$$

Furthermore, for nonnegative integers u_1 and u_2 with $u_1 \equiv u_2 \pmod{n}$, we have $R_A(u_1) = R_A(u_2)$, so that it is sufficient to consider only shifts u in the set $\{0, 1, \ldots, n-1\}$ when considering magnitudes of periodic autocorrelations. We have the following well known relationship between the periodic and aperiodic autocorrelations of A:

$$R_A(u) = C_A(u) + \overline{C_A(n-u)} \quad \text{for each } u = 0, 1, \ldots, n-1. \tag{2.1}$$

From this relationship it follows that a sequence whose aperiodic autocorrelations are small in magnitude must have small magnitudes of periodic autocorrelations. Since the periodic autocorrelations of a sequence are often much easier to study than their aperiodic counterparts, it is a typical attempt to look for sequences with good periodic autocorrelation

properties and then study their aperiodic autocorrelations.

The next theorem due to Jensen, Jensen, and Høholdt [64] provides a necessary condition on families of binary sequences to have a nonzero asymptotic merit factor. Its proof uses the readily verified equation

$$\sum_{u=0}^{n-1} R_A(u) = \left| \sum_{j=0}^{n-1} a_j \right|^2 \tag{2.2}$$

for a sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n, and the Cauchy-Schwarz inequality.

Theorem 2.1.1 ([64])**.** *Let n take values in an infinite set of positive integers. For each n, let A_n be a binary sequence of length n and let k_n be its number of ones. Suppose that $k_n/n \to d$ as $n \to \infty$. If $d \neq 1/2$, then $\mathrm{F}(A_n) \to 0$ as $n \to \infty$.*

A binary sequence of length n is called *balanced*, if its number of ones (and also of minus ones) is as close to $n/2$ as possible. In view of (2.1) and Theorem 2.1.1 it might be a good starting point to find balanced binary sequences whose periodic autocorrelations are small in magnitude, and then examine their aperiodic autocorrelations.

The remainder of this chapter is structured as follows. In Section 2.3 we shall see that binary sequences with good periodic autocorrelations are closely related to two combinatorial objects, namely *difference sets* and *almost difference sets*, which are specific subsets of abelian groups.

Many constructions of difference sets and almost difference sets arise from finite fields; in fact all known constructions that are of interest for our concerns arise from finite fields. Therefore, in Section 2.2 we recall some basic facts on finite fields. We also introduce *characters*, which are homomorphisms from a group into $\mathbb{C}^*$. Since a field consists of an additive and a multiplicative group, there are two types of characters to consider, namely *additive* and *multiplicative* characters. Among other things, characters provide a condition that allow us to check whether a given set is a difference set. This is done using so-called *character sums*. Arguably the most important character sums over finite fields are *Gauss sums*, which are mighty tools to transit from additive to multiplicative characters of a finite field and vice versa. These sums appear in various contexts in algebra and number theory. Also of interest are the closely related *Jacobi sums*, which are important in the study of the number of solutions of equations over finite fields, for example. We conclude Section 2.2 with two useful and highly nontrivial bounds on specific types of character sums over finite fields.

In Section 2.4 we then define *optimal* and *optimal balanced* binary sequences, which are promising candidates when searching for binary sequences with good aperiodic autocorrelation properties. We provide some fundamental results by showing that optimal and optimal balanced binary sequences are equivalent to specific difference and almost difference sets.

We conclude with Section 2.5, where we consider examples of families of optimal

balanced binary sequences. In particular, we shall see that such sequences exist for infinitely many lengths for each congruence class modulo 4.

2.2 Finite fields and character sums

Characters

Let $(G, \cdot)$ be a finite abelian group. A *character* χ of G is a homomorphism from G into the multiplicative group $\mathbb{C}^*$ of the complex numbers. Some readily verified properties of characters are:

- $\chi(e) = 1$, where e is the neutral element of G.
- $\chi(g)$ is a root of unity for each $g \in G$.
- $\chi(g^{-1}) = \overline{\chi(g)}$ for each $g \in G$.

We denote the set of characters of G by $\widehat{G}$. For $\chi, \lambda \in \widehat{G}$, the *product* $\chi\lambda$ is the character defined by

$$\chi\lambda(g) = \chi(g)\lambda(g) \quad \text{for each } g \in G.$$

Then $\widehat{G}$ together with this operation forms a group, which is called the *character group* of G. The neutral element χ_0 of $\widehat{G}$ is the homomorphism that maps every element of G to 1. Therefore, we call χ_0 the *trivial character* of G. The other characters of G are called *nontrivial*. It is well known that $\widehat{G}$ is isomorphic to G, and in particular $|\widehat{G}| = |G|$.

The following lemma provides orthogonality properties of characters, which are proved for example in [85, Chapter 5].

Lemma 2.2.1. *Let G be an abelian group of order n.*

(i) Let $\chi, \lambda \in \widehat{G}$. Then

$$\frac{1}{n}\sum_{g\in G} \chi(g)\overline{\lambda(g)} = \begin{cases} 0 & \text{if } \chi \neq \lambda \\ 1 & \text{if } \chi = \lambda. \end{cases}$$

(ii) Let $g, h \in G$. Then

$$\frac{1}{n}\sum_{\chi\in\widehat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} 0 & \text{if } g \neq h \\ 1 & \text{if } g = h. \end{cases}$$

The trace function

For a prime power q, we denote by $\mathbb{F}_q$ the field with q elements, and write $\mathbb{F}_q^*$ for its multiplicative group. Recall that $\mathbb{F}_q^*$ is cyclic and a generator of $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$.

For a positive integer m, the *trace function* $\mathrm{Tr}_{q^m/q}$ from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ is given by

$$\mathrm{Tr}_{q^m/q}(x) = \sum_{j=0}^{m-1} x^{q^j} \quad \text{for each } x \in \mathbb{F}_{q^m}.$$

Below we summarise some well known facts on the trace function. The proofs are straightforward, most of them can be found in [85, Chapter 2], for example.

Lemma 2.2.2. *The trace function $\mathrm{Tr}_{q^m/q}$ has the following properties:*

(i) $\mathrm{Tr}_{q^m/q}$ *is a linear mapping from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, where both $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$ are viewed as $\mathbb{F}_q$ vector spaces.*

(ii) $\mathrm{Tr}_{q^m/q}(v) = mv$ *for each $v \in \mathbb{F}_q$.*

(iii) $\mathrm{Tr}_{q^m/q}(x^q) = \mathrm{Tr}_{q^m/q}(x)$ *for each $x \in \mathbb{F}_{q^m}$.*

(iv) Let ℓ be a divisor of m. Then

$$\mathrm{Tr}_{q^m/q}(x) = \mathrm{Tr}_{q^\ell/q}\left(\mathrm{Tr}_{q^m/q^\ell}(x)\right) \quad \text{for each } x \in \mathbb{F}_{q^m}.$$

(v) For each $v \in \mathbb{F}_q$, we have

$$\left|\{x \in \mathbb{F}_{q^m} : \mathrm{Tr}_{q^m/q}(x) = v\}\right| = q^{m-1}.$$

Characters of finite fields

Since $\mathbb{F}_q$ consists of an additive and a multiplicative group, there are two types of characters to consider, namely *additive* and *multiplicative* characters of $\mathbb{F}_q$.

Let p be the characteristic of $\mathbb{F}_q$. The *additive* characters of $\mathbb{F}_q$ are given by

$$\psi_v : (\mathbb{F}_q, +) \to \mathbb{C}^*, \ x \mapsto e^{2\pi i \,\mathrm{Tr}_{q/p}(vx)/p}, \quad \text{for each } v \in \mathbb{F}_q. \tag{2.3}$$

The additive character ψ_1 is called the *canonical* additive character of $\mathbb{F}_q$.

Now fix a primitive element θ of $\mathbb{F}_q$. The *multiplicative* characters of $\mathbb{F}_q$ are given by

$$\chi_k : \mathbb{F}_q^* \to \mathbb{C}^*, \ \theta^j \mapsto e^{2\pi i kj/(q-1)}, \quad \text{for each } k \in \{0, 1, \ldots, q-2\}.$$

A generator of $\widehat{\mathbb{F}_q^*}$ is called a *primitive* multiplicative character of $\mathbb{F}_q$. For odd q, the multiplicative character that corresponds to $k = (q-1)/2$ is called the *quadratic* character of $\mathbb{F}_q$. For the quadratic character we usually reserve the symbol η; the name comes from the identity

$$\eta(x) = \begin{cases} 1 & \text{if } x \text{ is a square in } \mathbb{F}_q^* \\ -1 & \text{if } x \text{ is a nonsquare in } \mathbb{F}_q^*. \end{cases}$$

Throughout this thesis, we extend a multiplicative character χ of $\mathbb{F}_q$ to a mapping on $\mathbb{F}_q$ by defining

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

Gauss sums

Let χ be a multiplicative and let ψ be an additive character of $\mathbb{F}_q$. The *Gauss sum* of χ and ψ is

$$G(\chi, \psi) = \sum_{x \in \mathbb{F}_q^*} \chi(x)\psi(x).$$

For the canonical additive character ψ_1 of $\mathbb{F}_q$, we call $G(\chi, \psi_1)$ the *canonical* Gauss sum of χ, which we abbreviate as $G(\chi)$. Below we summarise some basic facts on Gauss sums (see [85, Chapter 5] or [9, Chapter 1], for example).

Lemma 2.2.3. *Let χ be a multiplicative and let ψ be an additive character of $\mathbb{F}_q$. Then the following hold.*

(i) $G(\chi, \psi) = q - 1$ *if χ and ψ are trivial.*

(ii) $G(\chi, \psi) = -1$ *if χ is trivial and ψ is nontrivial.*

(iii) $G(\chi, \psi) = 0$ *if χ is nontrivial and ψ is trivial.*

(iv) $|G(\chi, \psi)| = \sqrt{q}$ *if χ and ψ are nontrivial.*

(v) $G(\chi)G(\overline{\chi}) = \chi(-1)q$ *if χ is nontrivial.*

Let ψ_v be the additive character of $\mathbb{F}_q$ given in (2.3)*. Then the following hold.*

(vi) $G(\chi, \psi_{vw}) = \overline{\chi(v)}G(\chi, \psi_w)$ *for each $v \in \mathbb{F}_q^*$ and each $w \in \mathbb{F}_q$.*

(vii) $G(\chi^p, \psi_v) = G(\chi, \psi_{\sigma(v)})$ *for each $v \in \mathbb{F}_q$, where p is the characteristic of $\mathbb{F}_q$ and $\sigma(v) = v^p$.*

Also for certain nontrivial characters the associated Gauss sums can be evaluated explicitly. For example, we have the following result (see [85, Theorem 5.15], for example).

Proposition 2.2.4. *Let p be an odd prime and let η be the quadratic character of $\mathbb{F}_{p^m}$. Then*

$$G(\eta) = \begin{cases} (-1)^{m-1}p^{m/2} & \text{if } p \equiv 1 \pmod 4 \\ (-1)^{m-1}i^m p^{m/2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Jacobi sums

Let χ and λ be multiplicative characters of $\mathbb{F}_q$. The *Jacobi sum* corresponding to χ and λ is defined to be

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

Below we summarise some basic facts about Jacobi sums (see [85, Chapter 5] or [9, Chapter 2], for example).

Lemma 2.2.5. *Let χ and λ be multiplicative characters of $\mathbb{F}_q$. Then the following hold.*

(i) $J(\chi,\lambda) = 0$ *if exactly one of χ or λ is trivial.*

(ii) $|J(\chi,\lambda)| = 1$ *if χ and λ are nontrivial, but $\chi\lambda$ is trivial.*

(iii) $|J(\chi,\lambda)| = \sqrt{q}$ *if all of χ, λ, and $\chi\lambda$ are nontrivial.*

(iv) $J(\chi,\lambda)\, q = G(\chi)G(\lambda)\overline{G(\chi\lambda)}$ *if χ and λ are nontrivial.*

(v) $J(\chi,\lambda)J(\overline{\chi},\lambda\chi) = \chi(-1)q$ *if χ and λ are nontrivial.*

Bounds on character sums

In order to prove our results, we usually have to deal with error terms which consist of various types of character sums. We now summarise two deep results which will allow us to bound the occurring error terms.

We shall require the Weil bound for sums of multiplicative characters with polynomial arguments (see [85, Theorem 5.41] or [93, Lemma 9.25], for example).

Lemma 2.2.6. *Let χ be a multiplicative character of $\mathbb{F}_q$ of order $k > 1$, and let $f \in \mathbb{F}_q[x]$ be a monic polynomial of degree greater than zero that is not a k-th power. Let m be the number of distinct roots of f in its splitting field over $\mathbb{F}_q$. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leq (m-1)\sqrt{q}.$$

We also require the following deep result due to Katz [74, pp. 161–162].

Lemma 2.2.7 ([74])**.** *Let $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s$ be multiplicative characters of $\mathbb{F}_q$ such that $\alpha_1, \ldots, \alpha_r$ do not arise by permuting $\beta_1, \ldots, \beta_s$. Then*

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

2.3 Difference sets and almost difference sets

Difference sets

We begin with the definition of a *difference set*.

Definition (Difference set)**.** Let $(G,+)$ be a finite abelian group of order n. A *difference set* D with parameters (n,k,λ) is a k-set $D \subseteq G$ (which is a set with k elements) such that

the multiset $\{x - y \colon x, y \in D, x \neq y\}$ contains every non-identity element of G exactly λ times. If G is cyclic, then we call D *cyclic*.

We remark that the definition of a difference set also applies to nonabelian finite groups. However, we restrict ourselves to abelian groups. Notice that the parameters of an (n, k, λ) difference set are necessarily related as follows:

$$k(k-1) = \lambda(n-1). \tag{2.4}$$

Another way to look at difference sets is via the *difference function*.

Definition (Difference function)**.** Let $(G, +)$ be a finite abelian group and $D \subseteq G$. The *difference function* of D is

$$d_D(g) = |(g + D) \cap D| \quad \text{for each } g \in G,$$

where $g + D = \{g + d : d \in D\}$.

The following properties of the difference function are readily verified.

Lemma 2.3.1. *Let $(G, +)$ be an abelian group of order n and let $D \subseteq G$ be a k-subset. Then the following hold.*

(i) $d_D(g) = d_D(-g)$ *for each* $g \in G$.

(ii) $\sum_{g \in G \setminus \{0\}} d_D(g) = k(k-1)$.

(iii) $d_D(g)$ *is the number of times that* g *occurs in the list of nontrivial differences of* D *for each* $g \in G$.

(iv) D *is an* (n, k, λ) *difference set if and only if* $d_D(g) = \lambda$ *for each* $g \in G \setminus \{0\}$.

There are certain obvious difference sets D of a group G, namely:

- $D = \varnothing$ and $D = G$.
- $D = \{g\}$ and $D = G \setminus \{g\}$ for each $g \in G$.

These difference sets are called *trivial*.

Remark. If D is an (n, k, λ) difference set in a group G, then $G \setminus D$ is an $(n, n-k, n-2k+\lambda)$ difference set in G. Hence, we may restrict ourselves to the case that $k \leq n/2$.

We consider an example.

Example 2.3.2. Let $G = (\mathbb{Z}/11\mathbb{Z}, +)$ and let $D = \{1, 3, 4, 5, 9\}$. The list of differences of D is:

	1	3	4	5	9
1	0	9	8	7	3
3	2	0	10	9	5
4	3	1	0	10	6
5	4	2	1	0	7
9	8	6	5	4	0

Here, the entry (i, j) in the inner part of the table is obtained by calculating entry i of the left column minus entry j of the top row for each $i, j \in \{1, \ldots, 5\}$. For example entry $(1, 2)$ is $1 - 3 = 9$. Every nonzero element of G occurs exactly twice in the table. Hence, D is a (cyclic) difference set in G with parameters $(11, 5, 2)$. On the other hand, $G \setminus D = \{0, 2, 6, 7, 8, 10\}$ has the following list of differences:

	0	2	6	7	8	10
0	0	9	5	4	3	1
2	2	0	7	6	5	3
6	6	4	0	10	9	7
7	7	5	1	0	10	8
8	8	6	2	1	0	9
10	10	8	4	3	2	0

Every nonzero element of G occurs exactly three times in the table. Therefore, $G \setminus D$ is a $(11, 5, 3)$ difference set, which is compatible with the relation between the parameters of a difference set and its complement.

For a subset D of a finite abelian group G and a character ψ of G, we write

$$\psi(D) = \sum_{d \in D} \psi(d),$$

and we call $\psi(D)$ a *character value* of D. The following lemma gives a characterisation of difference sets using the magnitudes of their character values.

Lemma 2.3.3. *Let $(G, +)$ be an abelian group of order n and let $D \subseteq G$ be a k-subset. Then D is a difference set if and only if*

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

for every nontrivial character ψ of G.

Proof. If $n = 1$, then there is nothing to show, hence we may assume that $n > 1$. First, assume that D is an (n, k, λ) difference set in G and let ψ be a nontrivial character of G.

Then

$$\begin{aligned}|\psi(D)|^2 &= \psi(D)\overline{\psi(D)}\\ &= \sum_{d_1,\, d_2 \in D} \psi(d_1 - d_2)\\ &= k + \lambda \sum_{g \in G\setminus\{0\}} \psi(g)\\ &= k - \lambda\\ &= \frac{k(n-k)}{n-1},\end{aligned}$$

where we have used Lemma 2.2.1 (i) in the penultimate step, and (2.4) in the ultimate step.

Now assume that

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

for every nontrivial character ψ of G. For each $g \in G$, put

$$S(g) = \frac{1}{n} \sum_{\psi \in \widehat{G}} |\psi(D)|^2 \overline{\psi(g)}.$$

We shall compute $S(g)$ in two different ways. We have

$$\begin{aligned}S(g) &= \frac{1}{n} \sum_{\psi \in \widehat{G}} \overline{\psi(g)} \sum_{d_1,\, d_2 \in D} \psi(d_1 - d_2)\\ &= \sum_{d_1,\, d_2 \in D} \frac{1}{n} \sum_{\psi \in \widehat{G}} \psi(d_1 - d_2)\overline{\psi(g)}.\end{aligned}$$

Hence, by Lemma 2.2.1 (ii),

$$S(g) = \big|\{(d_1, d_2) \in D \times D \colon d_1 - d_2 = g\}\big|. \tag{2.5}$$

On the other hand, using the assumption of the lemma and $|\psi_0(D)|^2 = k^2$ for the trivial character ψ_0 of G, we have

$$S(g) = \frac{k^2}{n} + \frac{k(n-k)}{n(n-1)} \sum_{\substack{\psi \in \widehat{G}\\ \psi \neq \psi_0}} \overline{\psi(g)}.$$

From Lemma 2.2.1 (ii) it follows that

$$\sum_{\substack{\psi \in \widehat{G}\\ \psi \neq \psi_0}} \overline{\psi(g)} = \begin{cases} -1 & \text{for } g \neq 0\\ n-1 & \text{for } g = 0,\end{cases}$$

so that

$$S(g) = \begin{cases} \lambda & \text{for } g \neq 0 \\ k & \text{for } g = 0. \end{cases}$$

Comparing this with (2.5) proves the lemma. □

As an application of Lemma 2.3.3, we consider the following classical result due to Paley [100].

Theorem 2.3.4 ([100])**.** *Let q be an odd prime power with $q \equiv 3 \pmod 4$, and let D be the set of squares in $\mathbb{F}_q^*$. Then D is a $(q, (q-1)/2, (q-3)/4)$ difference set in $(\mathbb{F}_q, +)$.*

Proof. Let ψ be a nontrivial additive character of $\mathbb{F}_q$ and notice that $|D| = (q-1)/2$. Therefore, if D is a difference set, then D has parameters $(q, (q-1)/2, (q-3)/4)$. In order to prove that D is a difference set, we want to make use of Lemma 2.3.3. Thus, we have to show that

$$|\psi(D)|^2 = \frac{q+1}{4}. \tag{2.6}$$

Let η be the quadratic character of $\mathbb{F}_q$. We have

$$\frac{1}{2}\big(\eta(x)+1\big) = \begin{cases} 1 & \text{for } x \in D \\ 0 & \text{for } x \in \mathbb{F}_q^* \setminus D, \end{cases}$$

so that

$$\psi(D) = \frac{1}{2} \sum_{x \in \mathbb{F}_q^*} \big(\eta(x)+1\big)\psi(x).$$

By Lemma 2.2.1 (i) we have

$$\psi(D) = -\frac{1}{2} + \frac{1}{2} G(\eta, \psi).$$

Using Lemma 2.2.3 (vi) and then Proposition 2.2.4, we obtain

$$\psi(D) = -\frac{1}{2} \pm \frac{1}{2} i\sqrt{q},$$

which proves (2.6). □

The difference sets constructed in Theorem 2.3.4 are called *Paley difference sets*.

For more details on difference sets we refer the interested reader to the book of Lander [79] and to the articles [65], [68], [66].

Almost difference sets

For applications, the main issues concerning difference sets are the existence and the construction problem. It is an immediate consequence of (2.4) that for certain parameters

no difference sets can exist. For example if $n \equiv 1 \pmod 4$, then there is no $(n, (n-1)/2, \lambda)$ difference set (and also no $(n, (n+1)/2, \lambda)$ difference set) since 4 does not divide $n-3$. Therefore, for our concerns it is customary to relax the properties of a difference set slightly.

Definition (Almost difference set)**.** Let $(G, +)$ be an abelian group of order n. An *almost difference set* D with parameters (n, k, λ, t) is a k-set $D \subseteq G$ such that the multiset $\{x - y \colon x, y \in D, x \neq y\}$ represents exactly t of the non-identity elements of G exactly λ times and every other of the $n-1-t$ non-identity elements of G exactly $\lambda+1$ times. As for difference sets, we call D *cyclic* if G is cyclic.

Notice that each difference set with parameters (n, k, λ) is an almost difference set with parameters $(n, k, \lambda, n-1)$ and also with parameters $(n, k, \lambda - 1, 0)$. The parameters of an (n, k, λ, t) almost difference set are necessarily related as follows:

$$k(k-1) = \lambda t + (\lambda + 1)(n - 1 - t).$$

Remark. If D is an (n, k, λ, t) almost difference set in a group G, then $G \setminus D$ is an $(n, n-k, n-2k+\lambda, t)$ almost difference set in G. Hence, we may restrict ourselves again to the case that $k \leq n/2$.

We consider an example.

Example 2.3.5. Let $G = (\mathbb{Z}/13\mathbb{Z}, +)$ and let $D = \{0, 2, 3, 8, 9, 11\}$. The list of differences of D is:

	0	2	3	8	9	11
0	0	11	10	5	4	2
2	2	0	12	7	6	4
3	3	1	0	8	7	5
8	8	6	5	0	12	10
9	9	7	6	1	0	11
11	11	9	8	3	2	0

Hence, the list of nontrivial differences of D is:

$$\{1, 1, 3, 3, 4, 4, 9, 9, 10, 10, 12, 12, 2, 2, 2, 5, 5, 5, 6, 6, 6, 7, 7, 7, 8, 8, 8, 11, 11, 11\}.$$

Therefore, D is a $(13, 6, 2, 6)$ almost difference set in G, so that $G \setminus D$ is a $(13, 7, 3, 6)$ almost difference set.

We have the following easily verified connection between an almost difference set and its difference function.

Lemma 2.3.6. *Let $(G,+)$ be an abelian group of order n and let $D \subseteq G$ be a k-subset. Then D is an (n,k,λ,t) almost difference set if and only if $d_D(g) = \lambda$ has exactly t solutions $g \in G \setminus \{0\}$ and $d_D(g) = \lambda + 1$ has exactly $n-1-t$ solutions $g \in G \setminus \{0\}$.*

For more details on almost difference sets see for example [4].

Characteristic sequences

It turns out that cyclic difference and almost difference sets can be used to construct binary sequences with good correlation properties. The next definition provides a connection between sequences and subsets of cyclic groups.

Definition (Characteristic sequence)**.** Let $(G,\cdot)$ be a cyclic group of order n and let $D \subseteq G$. Fix a generator θ of G and define

$$\mathbb{1}_D(x) = \begin{cases} 1 & \text{for } x \in D \\ -1 & \text{for } x \notin D \end{cases}$$

to be the *indicator function* function of D. Then we call the sequence $A = (a_0, a_1, \ldots, a_{n-1})$ with $a_j = \mathbb{1}_D(\theta^j)$ for each $j = 0, 1, \ldots, n-1$ the *characteristic sequence* of D (with respect to θ).

Notice that, assuming the notation of the definition, the difference function $d_D(\theta^u)$ counts the number of pairs $(a_j, a_{j+u}) = (+,+)$ when j ranges over $\{0,1,\ldots,n-1\}$. Furthermore, every binary sequence of length n is a characteristic sequence of a subset of $(\mathbb{Z}/n\mathbb{Z},+)$ using the generator 1.

We consider an example.

Example 2.3.7 (Legendre sequence)**.** Let p be an odd prime and let D be the set of squares in $\mathbb{F}_p^*$ (so that D is a Paley difference set if $p \equiv 3 \pmod 4$). The characteristic sequence of D corresponding to the generator 1 of $(\mathbb{F}_p,+)$ is called the *Legendre sequence* of length p. The first few Legendre sequences of length p are:

$$\begin{aligned} p = 3 &: (-+-), \\ p = 5 &: (-+--+), \\ p = 7 &: (-++-+--), \\ p = 11 &: (-+-+++---+-), \\ p = 13 &: (-+-++----++-+). \end{aligned}$$

We have the following relationship between the periodic autocorrelations of a characteristic sequence A of a set D and the difference function of D.

Lemma 2.3.8. *Let $(G, \cdot)$ be a cyclic group of order n with generator θ, and let $D \subseteq G$ be a k-subset. Let A be the characteristic sequence of D with respect to θ. Then*

$$R_A(u) = n - 4(k - d_D(\theta^u)) \quad \textit{for each } u = 0, 1, \ldots, n-1.$$

Proof. Write $A = (a_0, \ldots, a_{n-1})$ and let $u \in \{0, \ldots, n-1\}$. There are $k - d_D(\theta^u)$ pairs $(a_j, a_{j+u}) = (+, -)$ and also $k - d_D(\theta^u)$ pairs $(a_j, a_{j+u}) = (-, +)$ when j ranges over $\{0, \ldots, n-1\}$. Thus, there are

$$n - d_D(\theta^u) - 2(k - d_D(\theta^u)) = n - 2k + d_D(\theta^u)$$

pairs $(a_j, a_{j+u}) = (-, -)$ when j ranges over $\{0, \ldots, n-1\}$. Recalling that $R_A(u)$ counts the number of agreements minus the number of disagreements of A with a by u entries cyclically shifted copy of A, we have

$$\begin{aligned} R_A(u) &= d_D(\theta^u) + (n - 2k + d_D(\theta^u)) - 2(k - d_D(\theta^u)) \\ &= n - 4(k - d_D(\theta^u)). \end{aligned}$$

□

Combining Lemma 2.3.1 (iv) with Lemma 2.3.8, and Lemma 2.3.6 with Lemma 2.3.8, we obtain a characterisation of cyclic difference and almost difference sets in terms of the periodic autocorrelations of their characteristic sequences.

Proposition 2.3.9. *Let A be a characteristic sequence of length n of a k-set D. Then the following hold.*

(i) D is an (n, k, λ) difference set if and only if $R_A(u) = n - 4(k - \lambda)$ for each $u \in \{1, 2, \ldots, n-1\}$.

(ii) D is an (n, k, λ, t) almost difference set if and only if $R_A(u) = n - 4(k - \lambda)$ has exactly t solutions $u \in \{1, 2, \ldots, n-1\}$ and $R_A(u) = n - 4(k - \lambda - 1)$ has exactly $n - 1 - t$ solutions $u \in \{1, 2, \ldots, n-1\}$.

2.4 Optimal binary sequences

We are interested in binary sequences whose periodic autocorrelations are small in magnitude. The next corollary, which follows easily from Lemma 2.3.8, lays the foundation for a first theoretical bound on how small the magnitudes of the periodic autocorrelations can collectively be.

Corollary 2.4.1. *Let A be a binary sequence of length n. Then*

$$R_A(u) \equiv n \pmod 4 \quad \textit{for each } u = 0, 1, \ldots, n-1.$$

From Corollary 2.4.1 we deduce that every binary sequence A of length $n > 1$ satisfies

$$\max_{0<u<n} |R_A(u)| \geq \begin{cases} 0 & \text{for } n \equiv 0 \pmod 4 \\ 1 & \text{for } n \equiv 1 \pmod 4 \\ 2 & \text{for } n \equiv 2 \pmod 4 \\ 1 & \text{for } n \equiv 3 \pmod 4. \end{cases} \tag{2.7}$$

Therefore, we call a binary sequence *optimal* if it satisfies (2.7) with equality. For excellent surveys on optimal binary sequences the interested reader is referred to [67], [18], and to [113, Section 2].

If the length $n > 1$ is congruent to 0 modulo 4, then optimal sequences are only known for $n = 4$ (for example the Barker sequence $(+++-)$ is optimal) and there is overwhelming evidence that there exists no optimal binary sequences of greater length (see [107, p. 134] for an old conjecture due to Ryser and [83] for the latest results concerning that topic).

If the length $n > 1$ is congruent to 1 modulo 4, then optimal sequences are only known for $n = 5$ and $n = 13$. For example the Barker sequences

$$(+++-+) \quad \text{and} \quad (+++++--++-+-+)$$

are optimal sequences of length 5 and 13, respectively. There is evidence (see [67, Corollary 2.5], [113, Conjecture 2.3.11], and [97, Section 2]) that there exists no optimal binary sequence of length $n > 13$ with n congruent to 1 modulo 4.

We shall see in Section 2.5 that there are constructions that provide infinitely many optimal binary sequences with lengths congruent to 2 and 3 modulo 4, respectively.

Binary sequences with two-level periodic autocorrelation

Besides searching for binary sequences whose periodic autocorrelations are small in magnitude, a second goal in sequence design is to minimise the total number of distinct periodic autocorrelation values (see for example [68, Section 7]). To characterise this number, we say that a sequence has *k-level* periodic autocorrelation if all of its periodic autocorrelations lie within a set of k elements. Since the trivial periodic autocorrelation of a binary sequence is always equal to its length, binary sequences with a two-level periodic autocorrelation are the most appreciated. We have the following well known characterisation of optimal binary sequences with two-level periodic autocorrelation.

Theorem 2.4.2. *Let A be a characteristic sequence of length n of a set D.*

(i) If $n \equiv 0 \pmod 4$, then $R_A(u) = 0$ for each $u = 1, 2, \ldots, n-1$ if and only if D or its complement is an

$$\left(n, \frac{n-\sqrt{n}}{2}, \frac{n-2\sqrt{n}}{4}\right)$$

difference set.

(ii) *If* $n \equiv 1 \pmod 4$, *then* $R_A(u) = 1$ *for each* $u = 1, 2, \ldots, n-1$ *if and only if* D *or its complement is an*

$$\left(n, \frac{n - \sqrt{2n-1}}{2}, \frac{n + 1 - 2\sqrt{2n-1}}{4}\right)$$

difference set.

(iiia) *If* $n \equiv 2 \pmod 4$, *then* $R_A(u) = -2$ *for each* $u = 1, 2, \ldots, n-1$ *if and only if* D *or its complement is an*

$$\left(n, \frac{n - \sqrt{2-n}}{2}, \frac{n - 2 - 2\sqrt{2-n}}{4}\right)$$

difference set.

(iiib) *If* $n \equiv 2 \pmod 4$, *then* $R_A(u) = 2$ *for each* $u = 1, 2, \ldots, n-1$ *if and only if* D *or its complement is an*

$$\left(n, \frac{n - \sqrt{3n-2}}{2}, \frac{n + 2 - 2\sqrt{3n-2}}{4}\right)$$

difference set.

(iv) *If* $n \equiv 3 \pmod 4$, *then* $R_A(u) = -1$ *for each* $u = 1, 2, \ldots, n-1$ *if and only if* D *or its complement is an*

$$\left(n, \frac{n-1}{2}, \frac{n-3}{4}\right)$$

difference set.

Proof. Exemplarily we prove (i), the proofs of the other parts are analogous. Write $k = |D|$ and notice that k is the number of ones of A. Let θ be the generator of the underlying cyclic group that corresponds to A. We have by Lemma 2.3.8

$$R_A(u) = -1 \quad \text{for each } u = 1, \ldots, n-1$$

if and only if

$$n - 4(k - d_D(\theta^u)) = -1 \quad \text{for each } u = 1, \ldots, n-1,$$

which, by Lemma 2.3.1 (iv), is true if and only if D is an $(n, k, (4k - n - 1)/4)$ difference set. Using (2.4) straightforward computations complete the proof. □

Notice that the only difference sets with parameters as in Theorem 2.4.2 (iiia) are the trivial $(2, 1, 0)$ difference sets, which correspond to the sequences $(+\,-)$ and $(-\,+)$. There are no known difference sets with $n > 4$ corresponding to case (i), and there are only finitely many known difference sets that correspond to the cases (ii) and (iiib). For a discussion of those cases, we refer to [67]. From Theorem 2.3.4 (with q being a prime so that $(\mathbb{F}_q, +)$ is cyclic) we already know that there exist infinitely many difference sets that correspond to case (iv).

Optimal balanced binary sequences

Recall that a *balanced* binary sequence is a sequence of length n with the property that its number of ones is as close to $n/2$ as possible. From Theorem 2.1.1 we already know that only those binary sequences that are at least "nearly" balanced can perform well when considering asymptotic merit factors. In view of Theorem 2.4.2 (i) a balanced binary sequence whose length is divisible by 4 cannot be optimal. By Theorem 2.4.2 (ii) there are no sequences of length congruent to 1 modulo 4 greater than 1 that are optimal and balanced. Also in view of the apparent nonexistence of long optimal binary sequences with lengths congruent to 0 or 1 modulo 4, it is natural to construct balanced binary sequences A of length $n > 1$ that satisfy

$$\max_{0<u<n} |R_A(u)| \leq \begin{cases} 4 & \text{for } n \equiv 0 \pmod 4 \\ 3 & \text{for } n \equiv 1 \pmod 4 \\ 2 & \text{for } n \equiv 2 \pmod 4 \\ 1 & \text{for } n \equiv 3 \pmod 4. \end{cases} \tag{2.8}$$

We call a balanced binary sequence A of length greater than 1 that satisfies (2.8) *optimal balanced*. We now show that certain almost difference sets are closely related to optimal balanced binary sequences (see also [18, Theorem 2.1] for a similar result without the restriction to balance).

Theorem 2.4.3. *Let A be a characteristic sequence of length n of a set D.*

(i) If $n \equiv 0 \pmod 4$, then $R_A(u) \in \{-4, 0\}$ for each $u = 1, 2, \ldots, n-1$ if and only if D is an

$$\left(n, \frac{n}{2}, \frac{n-4}{4}, \frac{n}{4}\right) \tag{2.9}$$

almost difference set.

(ii) If $n \equiv 1 \pmod 4$, then $R_A(u) \in \{-3, 1\}$ for each $u = 1, 2, \ldots, n-1$ if and only if D or its complement is an

$$\left(n, \frac{n-1}{2}, \frac{n-5}{4}, \frac{n-1}{2}\right) \tag{2.10}$$

almost difference set.

(iii) If $n \equiv 2 \pmod 4$, then $R_A(u) \in \{-2, 2\}$ for each $u = 1, 2, \ldots, n-1$ if and only if D is an

$$\left(n, \frac{n}{2}, \frac{n-2}{4}, \frac{3n-2}{4}\right) \tag{2.11}$$

almost difference set.

(iv) If $n \equiv 3 \pmod 4$*, then* $R_A(u) = -1$ *for each* $u = 1, 2, \ldots, n-1$ *if and only if* D *or its complement is an*

$$\left(n, \frac{n-1}{2}, \frac{n-3}{4}\right) \tag{2.12}$$

difference set.

Proof. Exemplarily we prove (i), the proofs for (ii) and (iii) are analogous, and part (iv) is (basically) the same as Theorem 2.4.2 (iv).

Notice that the number of ones in A is $n/2$ if and only if $|D| = n/2$. Let θ be the generator of the underlying cyclic group that corresponds to A. From Lemma 2.3.8 we know that $R_A(u) = -4$ for exactly $n/4$ values of u and $R_A(u) = 0$ for exactly $3n/4 - 1$ values of u when u ranges over $\{1, \ldots, n-1\}$ if and only if $-4 = n - 4(n/2 - d_D(\theta^u))$ for exactly $n/4$ values of u and $0 = n - 4(n/2 - d_D(\theta^u))$ for exactly $3n/4 - 1$ values of u when u ranges over $\{1, \ldots, n-1\}$. By Lemma 2.3.6 this is true if and only if D is an $(n, n/2, (n-4)/4, n/4)$ almost difference set, which proves (i). □

Theorem 2.4.3 (iv) is just stated for the sake of completeness (it is basically the same as Theorem 2.4.2 (iv)). The parameters (2.12) are called *Hadamard parameters* and the corresponding difference sets are often called *(Paley-)Hadamard difference sets* (see [65, p. 244]).

Let A be a balanced binary sequence of length n. First, suppose that n is congruent to 0 modulo 4. We note that the case that $R_A(u) \in \{-4, 4\}$ for each $u = 1, 2, \ldots, n-1$ is not desirable since we want that all nontrivial periodic autocorrelations of A are as small as possible in magnitude. The case that $R_A(u) \in \{0, 4\}$ for each $u = 1, 2, \ldots, n-1$ cannot occur by (2.2).

Now suppose that n is congruent to 2 modulo 4. We note that the case that $R_A(u) = 2$ for each $u = 1, 2, \ldots, n-1$ cannot occur by (2.2), and the only balanced binary sequences that satisfy $R_A(u) = -2$ for each $u = 1, 2, \ldots, n-1$ are $(+-)$ and $(-+)$ by (2.2).

We shall see in Section 2.5 that optimal balanced binary sequences exist for infinitely many lengths n for each congruence class modulo 4.

2.5 Examples of optimal balanced binary sequences

In this section we review three constructions of optimal balanced binary sequences.

The Sidelnikov construction

We now describe a construction due to Sidelnikov [119] that produces optimal balanced binary sequences of even lengths.

Theorem 2.5.1 ([119], [81]). *Let q be an odd prime power and define*

$$D = \{x \in \mathbb{F}_q^* \colon x + 1 \text{ is zero or a square in } \mathbb{F}_q\}.$$

If $q-1$ is congruent to 0 modulo 4, then D is an almost difference set in $\mathbb{F}_q^*$ with parameters (2.9). *If $q-1$ is congruent to 2 modulo 4, then D is an almost difference set in $\mathbb{F}_q^*$ with parameters* (2.11). *Equivalently, a characteristic sequence of D is optimal balanced.*

We call the set D in Theorem 2.5.1 the *Sidelnikov almost difference set* in $\mathbb{F}_q^*$, and a characteristic sequence of D a *Sidelnikov sequence* of length $q-1$. It is mentioned in [113], Sidelnikov sequences were first studied by Turyn [127] and were later examined apparently independently by Sidelnikov [119] and Lempel, Cohn, and Eastman [81]. We consider an example.

Example 2.5.2. The set of squares of $\mathbb{F}_{13}$ is $\{1, 3, 4, 9, 10, 12\}$, so that the Sidelnikov almost difference set in $\mathbb{F}_{13}^*$ is $\{2, 3, 8, 9, 11, 12\}$. Choosing the primitive element 2 of $\mathbb{F}_{13}$, we can write the elements of $\mathbb{F}_{13}^*$ in the following way:

$$\begin{array}{llllll} 2^0 = 1, & 2^1 = 2, & 2^2 = 4, & 2^3 = 8, & 2^4 = 3, & 2^5 = 6, \\ 2^6 = 12, & 2^7 = 11, & 2^8 = 9, & 2^9 = 5, & 2^{10} = 10, & 2^{11} = 7. \end{array}$$

Therefore, the Sidelnikov sequence A of length 12 with respect to the generator 2 is

$$A = (- + - - + + - + + + - - -).$$

It is readily verified that

$$R_A(u) = \begin{cases} -4 & \text{for } u \in \{4, 6, 8\} \\ 0 & \text{for } u \in \{1, 2, 3, 5, 7, 9, 10, 11\}, \end{cases}$$

in accordance with Theorem 2.5.1.

We note that more known constructions of optimal balanced binary sequences of even length are described in [18, Sections 4 and 5].

The Paley construction

We now review a classical construction which is due to Paley, who studied related objects [100]. By combining Theorem 2.3.4 with Theorem 2.4.3 (iv) we know already that the Legendre sequence of length p, where p is a prime with $p \equiv 3 \pmod 4$, is optimal balanced. We now consider an example for the case that $p \equiv 1 \pmod 4$.

Example 2.5.3. Recall from Example 2.3.7 the Legendre sequence $A = (- + - - +)$ of length 5. It is readily verified that

$$R_A(u) = \begin{cases} -3 & \text{for } u \in \{1,4\} \\ 1 & \text{for } u \in \{2,3\}, \end{cases}$$

so that A is optimal balanced, and the set $\{1,4\}$ is a $(5,2,0,2)$ almost difference set in $(\mathbb{F}_5,+)$ by Theorem 2.4.3 (ii).

In accordance with Example 2.5.3, we have the following result, which is closely related to Theorem 2.3.4 and tailored to sequences.

Theorem 2.5.4 ([100])**.** *Let p be an odd prime and let D be the set of squares in $\mathbb{F}_p^*$. If $p \equiv 3 \pmod 4$, then D is a Paley difference set in $(\mathbb{F}_p,+)$, and if $p \equiv 1 \pmod 4$, then D is an almost difference set in $(\mathbb{F}_p,+)$ with parameters (2.10). Equivalently, a characteristic sequence of D is optimal balanced. In particular, Legendre sequences are optimal balanced.*

The Singer construction

In our next construction we build cyclic difference sets in the multiplicative group of a finite field of characteristic two. The following classical result is due to Singer, who studied related structures in finite geometry [120]. We include a short proof.

Theorem 2.5.5 ([120])**.** *Let $m \geq 1$ and let $v \in \mathbb{F}_{2^m}^*$. Define*

$$D = \{x \in \mathbb{F}_{2^m}^* \colon \operatorname{Tr}_{2^m/2}(vx) = 0\}.$$

Then D is a difference set in $\mathbb{F}_{2^m}^*$ with Hadamard parameters. Equivalently, a characteristic sequence of D is optimal balanced.

Proof. Let ψ_v be the additive character of $\mathbb{F}_{2^m}$ given in (2.3). Let θ be a primitive element of $\mathbb{F}_{2^m}$ and define the sequence $A = (a_0, \ldots, a_{n-1})$ via

$$a_j = \psi_v(\theta^j) \quad \text{for each } j = 0, \ldots, n-1.$$

Notice that A is the characteristic sequence of D with respect to θ. For each $u = 1, \ldots, n-1$, we have

$$\begin{aligned} R_A(u) &= \sum_{j=0}^{n-1} \psi_v(\theta^j)\psi_v(\theta^{j+u}) \\ &= \sum_{j=0}^{n-1} \psi_{v(1+\theta^u)}(\theta^j) \\ &= -1 \end{aligned}$$

by Lemma 2.2.1 (i) since $v(1+\theta^u) \neq 0$. Theorem 2.4.3 (iv) completes the proof. □

Numbers of the form 2^m-1 are called *Mersenne numbers*. The set D in Theorem 2.5.5 is called *Singer difference set* (with respect to v), and its parameters $(2^m-1, 2^{m-1}-1, 2^{m-2}-1)$ are typically called *Singer parameters*. A characteristic sequence of D is called an *m-sequence* or a *Galois sequence* of length 2^m-1 (see also [116]). Below we summarise some well known facts about Galois sequences (see for example [43]):

- There are exactly $n\,\varphi(n)/m$ Galois sequences of length $n = 2^m-1$, where φ is *Euler's totient function* given by

  $$\varphi(n) = |\{d \in \{1, 2, \ldots, n\} \colon \gcd(d, n) = 1\}|.$$

  This can be deduced as follows: Two sequences A and B are called *cyclically distinct* if A is not a cyclic shift of B. For example the sequences $(+--+-)$ and $(++--)$ are cyclically distinct, whereas $(++--)$ and $(+---+)$ are not cyclically distinct.

  Let θ be a primitive element of $\mathbb{F}_{2^m}$. For $v \in \mathbb{F}_{2^m}^*$ and an integer d with $\gcd(d, n) = 1$, let $A(v, \theta^d)$ be the characteristic sequence of

  $$\{x \in \mathbb{F}_{2^m}^* \colon \operatorname{Tr}_{2^m/2}(vx) = 0\}$$

  with respect to θ^d. It is not hard to show that the sequences $A(1, \theta)$ and $A(1, \theta^d)$ are cyclically distinct if and only if d is not a power of 2. By noting that the sequences $A(v, \theta^d)$ are cyclic shifts of the sequence $A(1, \theta^d)$ when v ranges over $\mathbb{F}_{2^m}^*$, we deduce that there are exactly $\varphi(n)/m$ cyclically distinct Galois sequences of length n. We are done by checking that $A(v, \theta^d) \neq A(w, \theta^d)$ whenever $v \neq w$.

- Galois sequences can be generated efficiently using linear feedback shift registers.

- Every cyclic shift of a Galois sequence is a Galois sequence.

The last two properties make Galois sequences especially useful for practical applications. We consider an example.

Example 2.5.6. We construct $\mathbb{F}_8$ using the irreducible polynomial $x^3 + x + 1 \in \mathbb{F}_2[x]$, so that

$$\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1).$$

Taking α to be a root of $x^3 + x + 1$, we can write the elements of $\mathbb{F}_8$ in the following way:

Element of $\mathbb{F}_8$	Trace
0	0
$\alpha^0 = 1$	1
$\alpha^1 = \alpha$	0
$\alpha^2 = \alpha^2$	0
$\alpha^3 = \alpha + 1$	1
$\alpha^4 = \alpha^2 + \alpha$	0
$\alpha^5 = \alpha^2 + \alpha + 1$	1
$\alpha^6 = \alpha^2 + 1$	1

Hence, the Singer difference set corresponding to $v = 1$ is $\{\alpha, \alpha^2, \alpha^4\}$, so that

$$A = (- + + - + - -)$$

is a Galois sequence of length 7 (with respect to the generator α). It is readily verified that, in accordance with Theorem 2.5.5, all nontrivial periodic autocorrelations of A are equal to -1.

Chapter 3

The merit factor of binary sequences

3.1 Introduction and chapter overview

Recall from Chapter 1 that the *merit factor* of a binary sequence A of length $n > 1$ is given by

$$\mathrm{F}(A) = \frac{n^2}{2\sum_{u=1}^{n-1} C_A(u)^2}.$$

In spite of substantial progress on the merit factor problem in the last fifty years, modulo generalisations and variations, only three nontrivial families of binary sequences are known, for which we can compute the asymptotic merit factor, namely Shapiro (see Theorem 1.5.9), Legendre, and Galois sequences (see the forthcoming Corollaries 3.5.4 and 3.4.5, respectively). We consider the merit factor of other families of binary sequences, providing the first essentially new examples since 1991. The results of this chapter are mainly motivated by the paper [64] of Jensen, Jensen, and Høholdt from 1991, in which the authors asked for the merit factors of sequences that arise from difference sets.

The chapter is structured as follows. In Section 3.2 we prove two general theorems on the asymptotic merit factor of binary sequences. We shall apply these theorems to specific families of binary sequences to deduce our results. In Section 3.3 we determine the asymptotic merit factor of Sidelnikov sequences, proving [61, Conjecture 7.2] in the affirmative and explaining numerical evidence made in [54]. In Section 3.4 we determine the asymptotic merit factor of characteristic sequences of *Gordon-Mills-Welch difference sets*. In particular, we obtain the results on the merit factor behaviour of Galois sequences proved in [61] as a corollary. In Section 3.5 we then provide a very general theorem on the asymptotic merit factor of binary sequences that arise from cyclotomy, which includes results on Legendre sequences, and on the characteristic sequences of *Hall difference sets* and *Ding-Helleseth-Lam almost difference sets* as special cases.

Since 1991, further cyclic difference sets with Singer parameters have been found,

namely:

- *Maschietti difference sets* [88];
- *Dillon-Dobbertin difference sets* [25];
- *No-Chung-Yun difference sets* [25].

We remark that we have not been able to determine the asymptotic merit factors of the characteristic sequences of those difference sets. In Section 3.6 we discuss the occurring problems. We conclude with Section 3.7, where we give a list of open problems concerning the merit factor of binary sequences.

The results of this chapter are also published in [49].

3.2 Asymptotic merit factor calculation

In this section we prove two theorems on the asymptotic merit factor of binary sequences, which are the foundations for the proofs of our main results.

Modifications of a sequence

Let $A = (a_0, a_1, \ldots, a_{n-1})$ be a binary sequence of length $n > 1$. We wish to modify A in such a way that its merit factor becomes larger. Therefore, for integers r and $t > 0$ that can depend on n, we define $A^{r,t}$ to be the coefficient sequence of the polynomial

$$\sum_{j=0}^{t-1} a_{j+r} z^j. \tag{3.1}$$

Informally speaking, the sequence $A^{r,t}$ is obtained from A by cyclically shifting its entries by r elements to the left and then truncating when $t < n$ or periodically appending when $t > n$. Notice that $A^{0,n} = A$, and we have $A^{r_1,t} = A^{r_2,t}$ for all $t > 0$ whenever $r_1 \equiv r_2 \pmod{n}$. For example, if $A = (+++-)$, then $A^{1,3} = (++-)$ and $A^{3,10} = (-+++-+++-+)$.

Let A be the Legendre sequence of length 101. In order to motivate the study of aperiodic autocorrelations (and in particular the study of merit factors) of the sequences $A^{r,t}$, we compute $\mathrm{F}(A^{r,t})$ for various r and t. In Figure 3.1 we observe that the merit factor of $A^{r,101}$ depends heavily on the rotation r. In particular, we have

$$\max_{0 \le r < 101} \mathrm{F}\left(A^{r,101}\right) = \mathrm{F}\left(A^{25,101}\right) = \mathrm{F}\left(A^{77,101}\right) = 5.4609\ldots. \tag{3.2}$$

Therefore, an appropriate rotation of A enlarges its merit factor vastly.

We now consider truncations and appendices of a corresponding optimal rotation of A. In Figure 3.2 we see the merit factors of $A^{r,t}$ when t ranges over $\{50, 51, \ldots, 150\}$ and r is

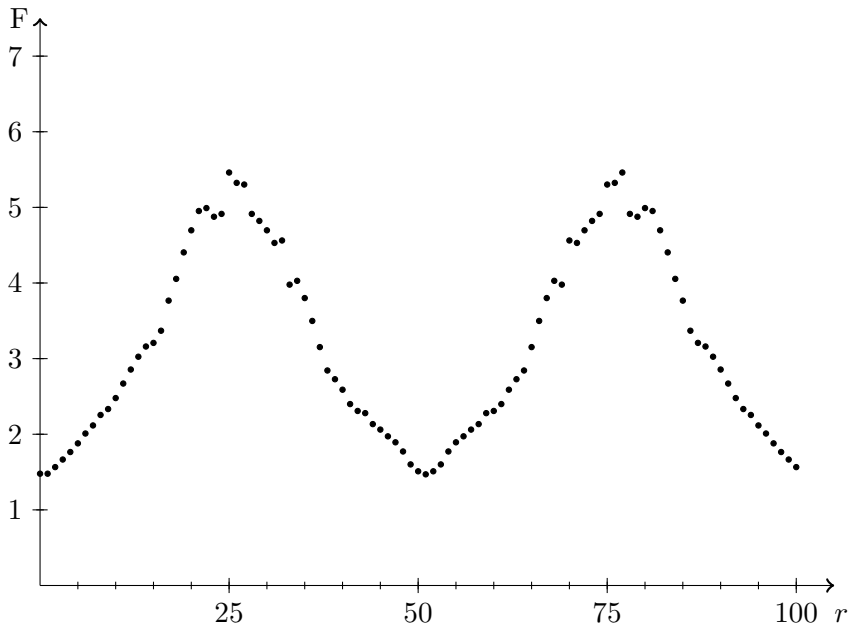

Figure 3.1: The merit factors of $A^{r,101}$ for $r = 0, 1, \ldots, 100$, where A is the Legendre sequence of length 101.

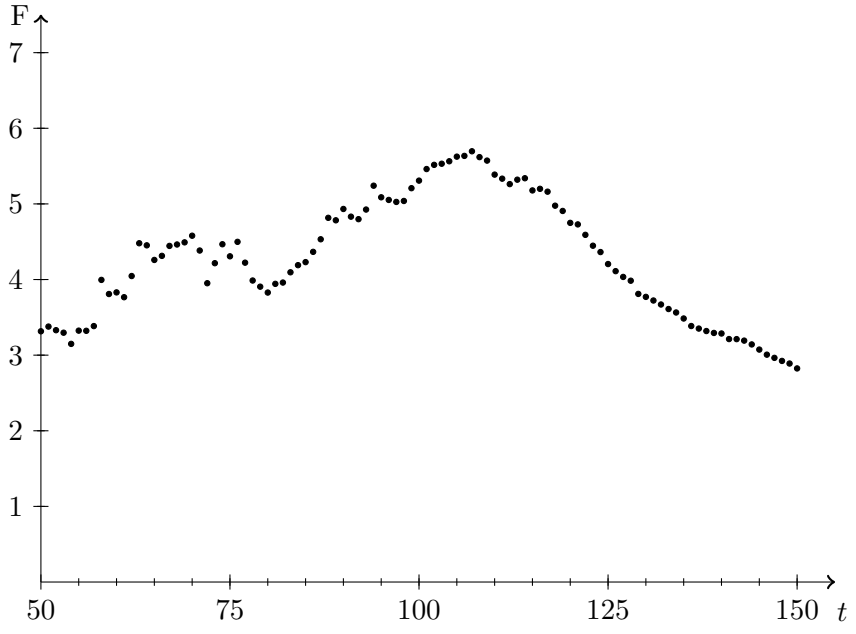

Figure 3.2: The merit factors of $A^{r,t}$ for $t = 50, 51, \ldots, 150$, where A is the Legendre sequence of length 101 and r is an optimal rotation.

an optimal rotation. In particular, we have

$$\max_{\substack{50\le t<151\\ 0\le r<101}} \mathrm{F}\left(A^{r,t}\right) = \mathrm{F}\left(A^{21,107}\right) = 5.6960\ldots,$$

which is a slight improvement of the merit factor of an optimal rotation of A given in (3.2).

Functions for the behaviour of the asymptotic merit factor

To state our results on the asymptotic merit factors of binary sequences, we shall require the function $\varphi_\nu\colon \mathbb{R}\times\mathbb{R}^+\to\mathbb{R}$, 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, and the involved sums consist of only finitely many nonzero summands for all (R,T).

It will be useful to know the global maximum of φ_ν for certain values of ν. The function φ_1 was maximised in [62, Corollary 3.2]. Using the same approach, we find that, for all $\nu\in[0,1]$, the global maximum of φ_ν 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 $R = 3/4 - T/2$.

Throughout the remainder of this chapter the functions φ_0, φ_1, and $\varphi_{1/9}$ are of particular interest. Therefore, we visualise these functions in Figure 3.3 for $T\in[0.9,1.3]$ and $R = 3/4 - T/2$.

Two theorems on the asymptotic merit factor

We wish to exploit the method of [61] and [62]. It involves Fourier analysis, counting lattice points in polyhedra, and estimation of error terms. We now explain and slightly generalise this method.

Let $A = (a_0, a_1, \ldots, a_{n-1})$ be a binary sequence of length n and let f_A be the Littlewood

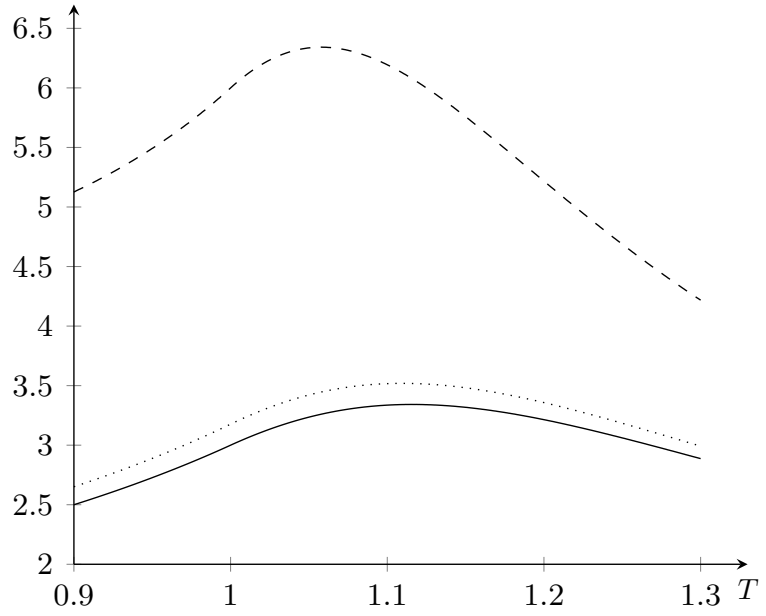

Figure 3.3: The functions φ_0 (solid line), φ_1 (dashed line), and $\varphi_{1/9}$ (dotted line) for $T \in [0.9, 1.3]$ and $R = 3/4 - T/2$.

polynomial with coefficient sequence A. Let r and t be integers with $t > 1$, and write $\epsilon_n(k) = e^{2\pi ik/n}$. From [61] it is known that $\mathrm{F}(A^{r,t})$ depends only on the function $L_A\colon (\mathbb{Z}/n\mathbb{Z})^3 \to \mathbb{Z}$, defined by

$$L_A(a,b,c) = \frac{1}{n^3} \sum_{k \in \mathbb{Z}/n\mathbb{Z}} f_A\big(\epsilon_n(k)\big) f_A\big(\epsilon_n(k+a)\big) \overline{f_A\big(\epsilon_n(k+b)\big) f_A\big(\epsilon_n(k+c)\big)}. \tag{3.3}$$

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

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

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 $K_n\colon (\mathbb{Z}/n\mathbb{Z})^3 \to \mathbb{Z}$ 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 our results on the asymptotic merit factor of binary sequences, we shall

show that the corresponding function L_A 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 [61, Theorem 4.1 (i)] and [61, Theorem 4.2 (i)], which arise by setting $\nu = 1$ and $\nu = 0$, respectively.

Theorem 3.2.1. *Let ν be a real number and let n take values in an infinite set of positive integers. For each n, let A_n be a binary sequence of length n. Suppose that, as $n \to \infty$,*

$$(\log n)^3 \max_{a,b,c \in \mathbb{Z}/n\mathbb{Z}} \left| L_{A_n}(a,b,c) - \big(I_n(a,b,c) + \nu J_n(a,b,c)\big) \right| \to 0. \tag{3.4}$$

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

Proof. For each n, write $A_n = (a_0, \ldots, a_{n-1})$, and let $f_{A_n}(z) = \sum_{j=0}^{n-1} a_j z^j$ be the Littlewood polynomial with coefficient sequence A_n. For each integer u, we have

$$C_{A_n^{r,t}}(u) = \sum_{\substack{0 \le j_1, j_2 < t \\ j_2 = j_1 + u}} a_{j_1+r} a_{j_2+r},$$

so that

$$\sum_{u \in \mathbb{Z}} C_{A_n^{r,t}}(u)^2 = \sum_{\substack{0 \le j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} a_{j_1+r} a_{j_2+r} a_{j_3+r} a_{j_4+r}.$$

Therefore,

$$\frac{1}{\mathrm{F}(A_n^{r,t})} = -1 + \frac{1}{t^2} \sum_{\substack{0 \le j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} a_{j_1+r} a_{j_2+r} a_{j_3+r} a_{j_4+r}. \tag{3.5}$$

It is readily verified that

$$a_j = \frac{1}{n} \sum_{k \in \mathbb{Z}/n\mathbb{Z}} f_{A_n}(\epsilon_n(k)) \epsilon_n(-jk).$$

Therefore, if j_1, j_2, j_3, j_4 are integers with $j_1 + j_2 = j_3 + j_4$, then $a_{j_1} a_{j_2} a_{j_3} a_{j_4}$ equals

$$\frac{1}{n^4} \sum_{k_1,k_2,k_3,k_4 \in \mathbb{Z}/n\mathbb{Z}} f_{A_n}\big(\epsilon_n(k_1)\big) f_{A_n}\big(\epsilon_n(k_2)\big) f_{A_n}\big(\epsilon_n(k_3)\big) f_{A_n}\big(\epsilon_n(k_4)\big) \times \epsilon_n\big((j_2 - j_3 - j_4)k_1 - j_2 k_2 - j_3 k_3 - j_4 k_4\big).$$

Re-indexing with

$$k_1 = k,\ k_2 = k + a,\ k_3 = -k - b,\ k_4 = -k - c$$

leads to

$$a_{j_1}a_{j_2}a_{j_3}a_{j_4} = \frac{1}{n}\sum_{a,b,c\in\mathbb{Z}/n\mathbb{Z}} L_{A_n}(a,b,c)\epsilon_n(-j_2a + j_3b + j_4c).$$

Substitution into (3.5) shows that $1/\operatorname{F}(A_n^{r,t})$ equals

$$-1 + \frac{1}{nt^2}\sum_{\substack{0\le j_1,j_2,j_3,j_4<t\\ j_1+j_2=j_3+j_4}}\ \sum_{a,b,c\in\mathbb{Z}/n\mathbb{Z}} L_{A_n}(a,b,c)\epsilon_n\big((-j_2-r)a + (j_3+r)b + (j_4+r)c\big). \tag{3.6}$$

Write

$$L_{A_n}(a,b,g) = I_n(a,b,c) + \nu J_n(a,b,c) + M_n(a,b,c), \tag{3.7}$$

where $M_n(a,b,c)$ is an error term which can be controlled using (3.4). We now consider three cases for the triple $(a,b,c) \in (\mathbb{Z}/n\mathbb{Z})^3$:

(1) $a = b$ and $c = 0$;

(2) $a = c$ and $b = 0$;

(3) $a = 0$ and $b = c \neq 0$.

Then $I_n(a,b,c) = 1$ if (1) or (2) is satisfied, and $I_n(a,b,c) = 0$ otherwise; and $J_n(a,b,c) = 1$ if (3) is satisfied, and $J_n(a,b,c) = 0$ otherwise. The only triple (a,b,c) that satisfies more than one of these conditions is $(0,0,0)$, which satisfies both (1) and (2).

We now substitute (3.7) into (3.6) and break the sum involving $I_n(a,b,c) + \nu J_n(a,b,c)$ into four parts: three sums corresponding to the three cases, and a fourth sum to correct for the double counting of $(0,0,0)$. Noting that the sums arising in cases (1) and (2) have the same value, we obtain

$$\frac{1}{\operatorname{F}(A_n^{r,t})} = -1 + X + Y + \nu Z - D + E,$$

where

$$X = Y = \frac{1}{t^2n}\sum_{\substack{0\le j_1,j_2,j_3,j_4<t\\ j_1+j_2=j_3+j_4}}\ \sum_{b\in\mathbb{Z}/n\mathbb{Z}} \epsilon_n\big((j_3-j_2)b\big),$$

$$Z = \frac{1}{t^2n}\sum_{\substack{0\le j_1,j_2,j_3,j_4<t\\ j_1+j_2=j_3+j_4}}\ \sum_{\substack{c\in\mathbb{Z}/n\mathbb{Z}\\ c\neq 0}} \epsilon_n\big((j_3+j_4+2r)c\big),$$

$$D = \frac{1}{t^2n}\sum_{\substack{0\le j_1,j_2,j_3,j_4<t\\ j_1+j_2=j_3+j_4}} 1,$$

$$E = \frac{1}{t^2n}\sum_{a,b,c\,\in\,\mathbb{Z}/n\mathbb{Z}} M_n(a,b,c)\,\epsilon_n\big(r(-a+b+c)\big)\sum_{\substack{0\le j_1,j_2,j_3,j_4<t\\ j_1+j_2=j_3+j_4}} \epsilon_n(-j_2a + j_3b + j_4c).$$

If $t/n \to T$, then (3.4) combined with the forthcoming Lemma 3.2.4 implies that $E \to 0$. Therefore, it remains to determine the asymptotic behaviour of the sums X, Z, and D to complete the proof.

There are contributions in X only when $j_3 = j_2 + mn$ for some integer m. In this case, we also have $j_1 = j_4 + mn$ since $j_1 + j_2 = j_3 + j_4$, so that

$$X = \frac{1}{t^2} \sum_{m \in \mathbb{Z}} \Bigg(\sum_{0 \le j,\, j+mn<t} 1 \Bigg)^2$$

Make use of the elementary counting identity

$$\sum_{0 \le j,\, j+u<s} 1 = \max(0, s - |u|) \quad \text{for all } u, s \in \mathbb{Z},$$

to obtain

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

Analogously, using $j_3 = j_2 + m$ instead of $j_3 = j_2 + mn$, we have

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

which simplifies to

$$\begin{aligned} D &= \frac{1}{n} + \frac{2}{t^2 n} \sum_{m=1}^{t-1} m^2 \\ &= \frac{2t^2 + 1}{3tn} \end{aligned}$$

using

$$\sum_{j=1}^{s} j^2 = \frac{s(s+1)(2s+1)}{6}$$

for all nonnegative integers s.

We now write $Z = Z_1 - D$, where

$$Z_1 = \frac{1}{t^2 n} \sum_{\substack{0 \le j_1, j_2, j_3, j_4 < t \\ j_1 + j_2 = j_3 + j_4}} \sum_{c \in \mathbb{Z}/n\mathbb{Z}} \epsilon_n\big((j_3 + j_4 + 2r)c\big).$$

Similarly as for X, there are contributions in Z_1 only when $j_4 = mn - 2r - j_3$ for some integer m, so that

$$Z_1 = \frac{1}{t^2} \sum_{m \in \mathbb{Z}} \Bigg(\sum_{0 \le j,\, mn - 2r - j < t} 1 \Bigg)^2.$$

Now make use of the elementary counting identity

$$\sum_{0\le j,\, u-j<s} 1 = \max(0, s-|s-1-u|) \quad \text{for all } u, s \in \mathbb{Z},$$

to obtain

$$Z_1 = \frac{1}{t^2}\sum_{m\in\mathbb{Z}} \max(0, t-|t-1-mn+2r|)^2.$$

Therefore,

$$Z = \frac{1}{t^2}\sum_{m\in\mathbb{Z}} \max(0, t-|t-1-mn+2r|)^2 - \frac{2t^2+1}{3tn}.$$

Since X, Y, and Z are continuous functions of r and t, we obtain

$$-1 + X + Y + \nu Z - D \to \frac{1}{\varphi_\nu(R,T)}$$

if $r/n \to R$ and $t/n \to T$, as required. □

Our second theorem is a more subtle modification of [61, Theorem 4.1 (i)]. Its proof is similar to the proof of Theorem 3.2.1. We include a proof that highlights the required modifications.

Theorem 3.2.2. *Let n take values in an infinite set of even positive integers. For each n, let A_n be a binary sequence of length n. Suppose that, as $n \to \infty$,*

$$(\log n)^3 \max_{a,b,c\in\mathbb{Z}/n\mathbb{Z}} \big|L_{A_n}(a,b,c) - (I_n(a,b,c) + K_n(a,b,c))\big| \to 0. \tag{3.8}$$

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

Proof. The first part of the proof is identical to that of Theorem 3.2.1, showing that $1/\mathrm{F}(A_n^{r,t})$ equals

$$-1 + \frac{1}{nt^2} \sum_{\substack{0\le j_1,j_2,j_3,j_4<t \\ j_1+j_2=j_3+j_4}} \sum_{a,b,c\in\mathbb{Z}/n\mathbb{Z}} L_{A_n}(a,b,c)\epsilon_n\big((-j_2-r)a + (j_3+r)b + (j_4+r)c\big). \tag{3.9}$$

Write

$$L_{A_n}(a,b,c) = I_n(a,b,c) + K_n(a,b,c) + M_n(a,b,c), \tag{3.10}$$

where $M_n(a,b,c)$ is an error term which can be controlled using (3.8). Consider three cases for the triple $(a,b,c) \in (\mathbb{Z}/n\mathbb{Z})^3$:

(1) $c = a$ and $b = 0$;

(2) $a = b$ and $c = 0$;

(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 (3.10) into (3.9) 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

$$\frac{1}{\mathrm{F}(A_n^{r,t})} = -1 + X + Y + Z - D_1 - D_2 - D_3 + E,$$

where

$$X = Y = \frac{1}{t^2 n} \sum_{\substack{0 \le j_1,j_2,j_3,j_4 < t \\ j_1+j_2=j_3+j_4}} \sum_{b \in \mathbb{Z}/n\mathbb{Z}} \epsilon_n\big((j_3-j_2)b\big),$$

$$Z = \frac{1}{t^2 n} \sum_{\substack{0 \le j_1,j_2,j_3,j_4 < t \\ j_1+j_2=j_3+j_4}} (-1)^{j_3-j_2} \sum_{c \in \mathbb{Z}/n\mathbb{Z}} \epsilon_n\big((j_3+j_4+2r)c\big),$$

$$D_1 = \frac{1}{t^2 n} \sum_{\substack{0 \le j_1,j_2,j_3,j_4 < t \\ j_1+j_2=j_3+j_4}} 1,$$

$$D_2 = D_3 = \frac{1}{t^2 n} \sum_{\substack{0 \le j_1,j_2,j_3,j_4 < t \\ j_1+j_2=j_3+j_4}} (-1)^{j_3-j_2},$$

$$E = \frac{1}{t^2 n} \sum_{a,b,c \in \mathbb{Z}/n\mathbb{Z}} M_n(a,b,c)\, \epsilon_n\big(r(-a+b+c)\big) \sum_{\substack{0 \le j_1,j_2,j_3,j_4 < t \\ j_1+j_2=j_3+j_4}} \epsilon_n(-j_2 a + j_3 b + j_4 c).$$

As in the proof of Theorem 3.2.1, we have

$$-1 + X + Y - D_1 + E \to \frac{1}{\varphi_0(0,T)}$$

if $t/n \to T$. Hence, it remains to show that $Z - D_2 - D_3 \to 0$ if $t/n \to T$.

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

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

Therefore, we have $|Z| \le 1/(tn)$ and so $Z \to 0$ if $t/n \to T$.

By writing $j_3 = j_1 + m$ for some $m \in \mathbb{Z}$, we find that

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

Hence, $|D_2| \le 1/(tn)$ and therefore $D_2 + D_3 \to 0$ if $t/n \to T$, which completes the proof. $\square$

We close this section by proving the bound used in Theorems 3.2.1 and 3.2.2. We deduce it from a more general result, which we shall also need in Chapter 4.

Lemma 3.2.3. *Let α be a positive integer and write $\epsilon_n(j) = e^{2\pi i j/n}$. There exists a constant c_α which only depends on α such that, for all positive integers n and t, we have*

$$\sum_{s_1,\dots,s_{2\alpha-1} \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{\substack{0 \le j_1,\dots,j_{2\alpha} < t \\ j_1 + \cdots + j_{2\alpha} = \alpha(t-1)}} \epsilon_n(s_1 j_1 + \cdots + s_{2\alpha-1} j_{2\alpha-1}) \right| \le c_\alpha \max(n,t)^{2\alpha-1} (1 + \log t)^{2\alpha-1}.$$

Proof. Put $d = 2\alpha - 1$. For a polyhedron $P \subseteq [0,1]^d$, let

$$F_t(z_1, \dots, z_d) = \sum_{(j_1,\dots,j_d) \in \mathbb{Z}^d \cap (t-1)P} z_1^{j_1} \cdots z_d^{j_d}$$

be a polynomial in $\mathbb{C}[z_1, \dots, z_d]$. Write

$$S_n = \sum_{s_1,\dots,s_d \in \mathbb{Z}/n\mathbb{Z}} \left| F_t(e^{2\pi i s_1/n}, \dots, e^{2\pi i s_d/n}) \right|.$$

We shall see at the end of the proof that the left-hand side of the statement of the lemma equals S_n for a particular choice of the polyhedron P.

The L^1 norm of F_t is defined to be

$$\|F_t\|_1 = \frac{1}{(2\pi)^d} \int_0^{2\pi} \cdots \int_0^{2\pi} \left| F_t(e^{i\theta_1}, \dots, e^{i\theta_d}) \right| d\theta_1 \cdots d\theta_d.$$

It is known (see [124, 9.2.1], for example) that

$$\|F_t\|_1 \le \gamma(P)(1 + \log t)^d, \tag{3.11}$$

where $\gamma(P)$ depends only on the polyhedron P. We shall find an upper bound for S_n in terms of $\|F_t\|_1$.

Let f be a polynomial in $\mathbb{C}[z]$. By the mean value theorem there exist real numbers

$\theta_0, \ldots, \theta_{n-1}$ with $\theta_s \in [2\pi s/n, 2\pi(s+1)/n]$ for all s such that

$$\begin{aligned} \|f\|_1 &= \frac{1}{2\pi} \sum_{s=0}^{n-1} \int_{2\pi s/n}^{2\pi(s+1)/n} \left|f(e^{i\theta})\right| d\theta \\ &= \frac{1}{n} \sum_{s=0}^{n-1} \left|f(e^{i\theta_s})\right|. \end{aligned} \tag{3.12}$$

By the triangle inequality we have

$$\begin{aligned} \left| \sum_{s=0}^{n-1} \left|f(e^{i\theta_s})\right| - \sum_{s=0}^{n-1} \left|f(e^{2\pi is/n})\right| \right| &\leq \sum_{s=0}^{n-1} \left|f(e^{i\theta_s}) - f(e^{2\pi is/n})\right| \\ &= \sum_{s=0}^{n-1} \left| \int_{2\pi s/n}^{\theta_s} f'(e^{i\theta})\, d\theta \right| \\ &\leq \int_0^{2\pi} \left|f'(e^{i\theta})\right| d\theta \\ &= 2\pi \|f'\|_1. \end{aligned} \tag{3.13}$$

Now suppose that f has degree at most $t-1$. Then $\|f'\|_1 \leq (t-1)\,\|f\|_1$ by a Bernstein-type inequality (see [11, p. 143] or [133, p. 11], for example). Combination of (3.12) and (3.13) then gives

$$\sum_{s=0}^{n-1} \left|f(e^{2\pi is/n})\right| \leq (1+2\pi) \max(n,t)\, \|f\|_1.$$

Since $F_t(z_1, \ldots, z_d)$ has degree at most $t-1$ in each indeterminate, we find by a straightforward induction that

$$S_n \leq (1+2\pi)^d \max(n,t)^d\, \|F_t\|_1,$$

and then with (3.11),

$$S_n \leq (1+2\pi)^d \gamma(P) \max(n,t)^d (1+\log t)^d. \tag{3.14}$$

Recalling that $d = 2\alpha - 1$, we now take

$$P = \left\{ (x_1, \ldots, x_{2\alpha-1}) \in \mathbb{R}^{2\alpha-1} : \begin{array}{c} 0 \leq x_1, \ldots, x_{2\alpha-1} \leq 1, \\ \alpha - 1 \leq x_1 + \cdots + x_{2\alpha-1} \leq \alpha \end{array} \right\}.$$

Set $j_{2\alpha} = \alpha(t-1) - j_1 - \cdots - j_{2\alpha-1}$ to see that the left-hand side of the statement of the lemma equals S_n, so that (3.14) completes the proof. □

We have the following corollary.

Corollary 3.2.4. *Write $\epsilon_n(j) = e^{2\pi ij/n}$. There exists a constant c such that, for all positive integers n and t, we have*

$$\sum_{a,b,c\in\mathbb{Z}/n\mathbb{Z}} \left| \sum_{\substack{0\le j_1,j_2,j_3,j_4<t \\ j_1+j_2=j_3+j_4}} \epsilon_n(-j_2a + j_3b + j_4c) \right| \le c\max(n,t)^3(1+\log t)^3.$$

Proof. After re-indexing with

$$k_1 = t-1-j_2,\ k_2 = j_3,\ k_3 = j_4,\ k_4 = t-1-j_1,$$

the statement of the lemma is equivalent to

$$\sum_{a,b,c\in\mathbb{Z}/n\mathbb{Z}} \left| \sum_{\substack{0\le k_1,k_2,k_3,k_4<t \\ k_1+k_2+k_3+k_4=2(t-1)}} \epsilon_n(k_1a + k_2b + k_3c) \right| \le c\max(n,t)^3(1+\log t)^3,$$

so that Lemma 3.2.3 with $\alpha = 2$ completes the proof. □

We remark that a bound similar to that in Corollary 3.2.4 was given by Jedwab, Katz, and Schmidt [62, Lemma 2.2]. The authors of [62] proved [62, Lemma 2.2] by direct calculation. Their bound holds with $c = 64$ and the $\log t$ term in the statement of Corollary 3.2.4 is replaced by $\log n$, which however does not make a big difference in the asymptotic merit factor calculation since we always assume that t/n is bounded as $n \to \infty$.

3.3 Sidelnikov sequences

In this section we examine the asymptotic merit factor of Sidelnikov sequences. In 2010, Hare and Yazdani [54] wrote:

"An obvious question is, what happens with Fekete-like polynomials? [...] Computationally it appears that the merit factors of these polynomials is tending to 3 *for large n."*

Hare and Yazdani called the polynomials that correspond to Sidelnikov sequences *Fekete-like polynomials*[1]. Their numerical observations suggest that the asymptotic merit factor of Sidelnikov sequences is 3, which is also subject to a conjecture due to Jedwab, Katz, and Schmidt [61, Conjecture 7.2] (which also involves the generalised Sidelnikov sequences). We shall prove this conjecture in the affirmative. We need the following proposition, which states that, if A is a Sidelnikov sequence of length n, then the corresponding function L_A is well approximated by $I_n + K_n$.

[1] In fact the coefficient sequence of a Fekete-like polynomial is a slightly modified Sidelnikov sequence in the sense that its first entry is zero instead of minus one. However, this modification does not effect the asymptotic merit factor.

Proposition 3.3.1. *Let q be an odd prime power and let A be a Sidelnikov sequence of length $q-1$. Then*

$$\big|L_A(a,b,c) - \big(I_{q-1}(a,b,c) + K_{q-1}(a,b,c)\big)\big| \le \frac{23q^{5/2}}{(q-1)^3}$$

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

Proof. Let f_A be the polynomial with coefficient sequence A, and let η be the quadratic character of $\mathbb{F}_q$. By the definition of a Sidelnikov sequence (see Theorem 2.5.1), there exists a primitive element θ of $\mathbb{F}_q$ such that

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

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

$$\begin{aligned} f_A\big(e^{2\pi i k/(q-1)}\big) &= (-1)^k + \sum_{j=0}^{q-2} \eta(\theta^j+1)\lambda^k(\theta^j) \\ &= (-1)^k + \sum_{x\in\mathbb{F}_q} \eta(x+1)\lambda^k(x) \\ &= (-1)^k + \lambda^k(-1) \sum_{x\in\mathbb{F}_q} \eta(x)\lambda^k(1-x) \\ &= (-1)^k\big(1 + J(\eta,\lambda^k)\big), \end{aligned}$$

where $J(\eta,\lambda^k)$ is a Jacobi sum. On the other hand, we have $f(1) = 1 - \eta(1) = 0$.

Therefore,

$$L_A(a,b,c) = \frac{(-1)^{a+b+c}}{(q-1)^3} \sum_{\chi\in\widehat{\mathbb{F}_q^*}} J(\eta,\chi)J(\eta,\chi\lambda^a)\overline{J(\eta,\chi\lambda^b)J(\eta,\chi\lambda^c)} + \Delta, \tag{3.15}$$

where $|\Delta| \le 15q^{3/2}/(q-1)^2$ using Lemma 2.2.5. If $\{b,c\} = \{0,a\}$, then by Lemma 2.2.5 the sum in (3.15) is between $(q-5)q^2$ and $(q-2)q^2$. If $a = (q-1)/2$ and $b = c + (q-1)/2$, then $\lambda^a = \eta$ and $\lambda^b = \lambda^c\eta$ and by Lemma 2.2.5 (in particular (v)) the sum (3.15) 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

$$\{\lambda^0, \lambda^a, \lambda^b\eta, \lambda^c\eta\} \quad \text{and} \quad \{\eta, \lambda^a\eta, \lambda^b, \lambda^c\} \tag{3.16}$$

are distinct. Use Lemmas 2.2.5 and 2.2.3 to see that the sum in (3.15) equals

$$\frac{1}{q^2}\sum_{\chi\in\widehat{\mathbb{F}_q^*}} G(\chi)G(\chi\lambda^a)G(\chi\eta\lambda^b)G(\chi\eta\lambda^c)\overline{G(\chi\eta)G(\chi\eta\lambda^a)G(\chi\lambda^b)G(\chi\lambda^c)} \tag{3.17}$$

plus an error term of magnitude at most $4q^{3/2}$. Since the multisets (3.16) are distinct, we can apply Lemma 2.2.7 to see that (3.17) is at most $4q^{5/2}$. This shows that

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

as required. □

The following result on the asymptotic merit factor of Sidelnikov sequences is obtained by combining Proposition 3.3.1 with Theorem 3.2.2.

Theorem 3.3.2. *For each odd prime power q, let A_{q-1} be a Sidelnikov sequence of length $q-1$. Let $T > 0$ be real. If $t/q \to T$ as $q \to \infty$, then $\mathrm{F}(A_{q-1}^{r,t}) \to \varphi_0(0,T)$ as $q \to \infty$.*

The largest merit factor that can be attained in Theorem 3.3.2 is $3.342065\ldots$, which is the largest root of

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

The global maximum is unique and it is attained for $T = 1.115749\ldots$, which is the middle root of

$$x^3 - 12x + 12.$$

To explain Hare and Yazdani's numerical observations on the asymptotic merit factor of Sidelnikov sequences [54], we have to look at the case $T = 1$ in Theorem 3.3.2. This case concerns just the shifted Sidelnikov sequences, as considered in [57] and [64] for Legendre and Galois sequences, respectively. In this case, Theorem 3.3.2 gives an asymptotic merit factor of 3.

3.4 Gordon-Mills-Welch difference sets

We now consider a construction of difference sets with Singer parameters which is due to Gordon, Mills, and Welch [45]. In the literature, this construction is often called the *GMW construction*. It produces cyclic difference sets in $\mathbb{F}_{2^m}^*$ from difference sets in the multiplicative group of a subfield of $\mathbb{F}_{2^m}$. Therefore, it is very general and can in particular be iterated.

Construction 3.4.1 (Gordon-Mills-Welch [45])**.** Let m and s be integers with $1 \leq s < m$ such that s divides m (so that $\mathbb{F}_{2^s}$ is a subfield of $\mathbb{F}_{2^m}$). Let B contain all elements $b \in \mathbb{F}_{2^m}$ with $\mathrm{Tr}_{2^m/2^s}(b) = 1$, and let C be a difference set in $\mathbb{F}_{2^s}^*$ of size 2^{s-1} (so that, for $s > 1$, the complement of C has Singer parameters). The set

$$D = \{bc \colon b \in B, c \in C\}$$

is a *Gordon-Mills-Welch difference set*[2] in $\mathbb{F}_{2^m}^*$ (whose complement has Singer parameters). Equivalently, a characteristic sequence of D is optimal balanced (by Theorem 2.4.3).

If the set C in Construction 3.4.1 is a Singer difference set, then a characteristic sequence of D is also called *GMW sequence* [115]. Gordon-Mills-Welch difference sets generalise the Singer difference sets, which arise for $s = 1$ (in which case C is a trivial difference set).

In their 1991 paper, Jensen, Jensen, and Høholdt [64] wrote:

"It is currently an open problem to find the asymptotic merit factor for sequences constructed from GMW and Hall difference sets."

In the remainder of this section we examine the asymptotic merit factor of the characteristic sequences of Gordon-Mills-Welch difference sets. In the next section we consider the asymptotic merit factor of binary sequences that arise from cyclotomy, which give results on Hall difference sets as special cases.

The following lemma gives the character values of Gordon-Mills-Welch difference sets. In particular, it gives an alternative proof for them to be difference sets.

Lemma 3.4.2. *Let m and s be integers with $1 \leq s < m$ such that s divides m. Let B contain all elements $b \in \mathbb{F}_{2^m}$ with $\mathrm{Tr}_{2^m/2^s}(b) = 1$, and let C be a subset of $\mathbb{F}_{2^s}^*$. Write $D = \{bc \colon b \in B, c \in C\}$. Let χ be a nontrivial multiplicative character of $\mathbb{F}_{2^m}$ and let χ^* be its restriction to $\mathbb{F}_{2^s}$. Then*

$$\chi(D) = \begin{cases} \dfrac{\chi^*(C)}{G(\chi^*)} G(\chi) & \text{if } \chi^* \text{ is nontrivial} \\ -\dfrac{\chi^*(C)}{s} G(\chi) & \text{if } \chi^* \text{ is trivial.} \end{cases}$$

In particular, if C is a difference set in $\mathbb{F}_{2^s}^*$ of size 2^{s-1}, then D is a difference set whose complement has Singer parameters.

Proof. We have

$$\begin{aligned} \chi(D) &= \sum_{\substack{b \in \mathbb{F}_{2^m} \\ \mathrm{Tr}_{2^m/2^s}(b)=1}} \sum_{c \in C} \chi(bc) \\ &= E(\chi)\, \chi^*(C), \end{aligned}$$

[2]We note that [45] defines more general differences sets, which are also called Gordon-Mills-Welch difference sets. However, in Construction 3.4.1 only those with Hadamard parameters are considered.

where

$$E(\chi) = \sum_{\substack{b \in \mathbb{F}_{2^m} \\ \mathrm{Tr}_{2^m/2^s}(b)=1}} \chi(b)$$

is an *Eisenstein sum*. It is known [9, pp. 391/400] that

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

which proves the first statement of the lemma. The second statement follows from Lemmas 2.3.3 and 2.2.3. □

In order to prove the main result of this section we need the following proposition, which states that, if A is a characteristic sequence of a Gordon-Mills-Welch difference set of length n, then the corresponding function L_A is well approximated by I_n.

Proposition 3.4.3. *Let $m > 1$ be an integer, and let A be a characteristic sequence of a Gordon-Mills-Welch difference set in $\mathbb{F}_{2^m}^*$ of length $2^m - 1$. Then*

$$\left|L_A(a,b,c) - I_{2^m-1}(a,b,c)\right| \le \frac{2^{5m/2+1}}{(2^m-1)^3}$$

for all $a, b, c \in \mathbb{Z}/(2^m-1)\mathbb{Z}$.

Proof. By definition, there exists a proper subfield $\mathbb{F}_{2^s}$ of $\mathbb{F}_{2^m}$ such that the underlying Gordon-Mills-Welch difference set is

$$D = \{bc \colon b \in B, c \in C\},$$

where B contains all elements $b \in \mathbb{F}_{2^m}$ with $\mathrm{Tr}_{2^m/2^s}(b) = 1$ and C is a difference set in $\mathbb{F}_{2^s}^*$ of size 2^{s-1}. Let f_A be the Littlewood polynomial with coefficient sequence A, and let θ be a primitive element of $\mathbb{F}_{2^m}$ such that

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

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

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

It then follows from Lemmas 3.4.2 and 2.2.3 (ii) that, for all integers k,

$$f_A\big(e^{2\pi ik/(2^m-1)}\big) = C_k G(\lambda^k),$$

where C_k has unit magnitude for all k and depends only on k modulo $2^s - 1$.

Therefore,

$$L_A(a,b,c) = \frac{1}{(2^m-1)^3} \sum_{\chi \in \widehat{\mathbb{F}_{2^m}^*}} G(\chi)G(\chi\lambda^a)\overline{G(\chi\lambda^b)G(\chi\lambda^c)}\, C_\chi(a,b,c), \tag{3.18}$$

where $C_\chi(a,b,c)$ has unit magnitude. Using Lemma 2.2.3, we obtain

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

which proves the desired result in the case that $I_{2^m-1}(a,b,c) = 1$.

Now assume that $\{0,a\} \neq \{b,c\}$, so that $I_{2^m-1}(a,b,c) = 0$. We have to show that

$$|L_A(a,b,c)| \leq \frac{2^{5m/2+1}}{(2^m-1)^3}. \tag{3.19}$$

Let H be the subgroup of index $2^s - 1$ of the character group of $\mathbb{F}_{2^m}^*$ and note that H is not the trivial group since, by assumption, $s < m$. 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 (3.18) and the triangle inequality that

$$|L_A(a,b,c)| \leq \frac{2^s-1}{(2^m-1)^3} \max_{\phi \in \widehat{\mathbb{F}_{2^m}^*}} \left| \sum_{\chi \in H} G(\chi\phi)G(\chi\phi\lambda^a)\overline{G(\chi\phi\lambda^b)G(\chi\phi\lambda^c)} \right|. \tag{3.20}$$

By the definition of a canonical Gauss sum over $\mathbb{F}_{2^m}$, the sum can be written as

$$\sum_{w,x,y,z \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}_{2^m/2}(w+x+y+z)}\, \lambda^a(x)\overline{\lambda^b(y)\lambda^c(z)}\, \phi\Big(\frac{wx}{yz}\Big) \sum_{\chi \in H} \chi\Big(\frac{wx}{yz}\Big).$$

For all $w, x, y, z \in \mathbb{F}_{2^m}^*$, we have

$$\frac{2^s-1}{2^m-1} \sum_{\chi \in H} \chi\Big(\frac{wx}{yz}\Big) = \frac{1}{2^m-1} \sum_{\chi \in \widehat{\mathbb{F}_{2^m}^*}} \chi\Big(\frac{wx}{yz}\Big),$$

since both sides equal either 0 or 1, depending on whether $wx = yz$, by Lemma 2.2.1 (ii). Therefore, we can rewrite the sum in (3.20) as

$$\frac{1}{s-1} \sum_{\chi \in \widehat{\mathbb{F}_{2^m}^*}} G(\chi\phi)G(\chi\phi\lambda^a)\overline{G(\chi\phi\lambda^b)G(\chi\phi\lambda^c)}.$$

The magnitude of this expression is at most $\frac{2}{2^s-1}2^{5m/2}$ by Lemma 2.2.7. Substitute into (3.20) to conclude that (3.19) holds, as required. □

The following result on the asymptotic merit factor of characteristic sequences of Gordon-Mills-Welch difference sets is obtained by combining Proposition 3.4.3 with Theorem 3.2.1 taking $\nu = 0$.

Theorem 3.4.4. *For each $n = 2^m - 1$ with $m > 1$, let A_n be a characteristic sequence of a Gordon-Mills-Welch difference set in $\mathbb{F}_{2^m}$ of length n. Let $T > 0$ be real. If $t/n \to T$ as $n \to \infty$, then $\mathrm{F}(A_n^{r,t}) \to \varphi_0(0,T)$ as $n \to \infty$.*

In particular, the asymptotic merit factor of characteristic sequences of Gordon-Mills-Welch difference sets behaves in the same way as those of Sidelnikov sequences. The case that the Gordon-Mills-Welch difference sets in Theorem 3.4.4 arise from Construction 3.4.1 with C being a Singer difference set proves [61, Conjecture 7.1][3] in the affirmative.

It is remarkable that Theorem 3.4.4 requires no knowledge about the smaller difference sets that are used as building blocks to construct the Gordon-Mills-Welch difference sets. Although we have not been able to determine the asymptotic merit factors of the characteristic sequences of Maschietti, Dillon-Dobbertin, and No-Chung-Yun difference sets themselves (see Section 3.6), these difference sets can be used as building blocks. Furthermore, even Paley and Hall difference sets (in groups whose order is a Mersenne number) can be used as building blocks.

In the particular case that $s = 1$ and $C = \{1\}$ in Construction 3.4.1, Theorem 3.4.4 reduces to:

Corollary 3.4.5 ([61])**.** *For each $n = 2^m - 1$ with $m > 1$, let A_n be a Galois sequence of length n. Let $T > 0$ be real. If $t/n \to T$ as $n \to \infty$, then $\mathrm{F}(A_n^{r,t}) \to \varphi_0(0,T)$.*

The case $T = 1$ in Corollary 3.4.5 is due to Jensen, Jensen, and Høholdt [64]. In particular, the asymptotic merit factor of Galois sequences behaves in the same way as those of Sidelnikov sequences.

3.5 Cyclotomic constructions

In this section we examine the asymptotic merit factor of sequences that arise from cyclotomy. We shall use the following notation. Let $m > 1$ be an integer, let p be a prime satisfying $p \equiv 1 \pmod{m}$, and let ω be a fixed primitive element of $\mathbb{F}_p$. Define C_0 to be the set of m-th powers in $\mathbb{F}_p^*$, and write $C_s = \omega^s C_0$ for each $s \in \mathbb{Z}$. The sets $C_0, C_1, \ldots, C_{m-1}$ partition $\mathbb{F}_p^*$ and are called the *cyclotomic classes* of $\mathbb{F}_p$ of order m (corresponding to ω).

We construct subsets D of the additive group of $\mathbb{F}_p$ by joining some of these classes. This method provides a rich source of difference sets (see [65] for a survey). From Theorem 2.1.1 we already know that the characteristic sequences of D can only have a nonzero asymptotic

[3] We remark that [61, Conjecture 7.1] also involves "negaperiodic" and "periodic" extensions of the sequences associated with Gordon-Mills-Welch difference sets. The corresponding assertions can be obtained as direct consequences of Proposition 3.4.3 and [61, Theorem 4.2], but are omitted here for the sake of simplicity.

merit factor if $|D|/p$ approaches $1/2$ as $p \to \infty$, so that we are interested in the case that m is even and D is the union of $m/2$ of the cyclotomic classes of order m. Two families of difference sets arise in this way, namely the Paley difference sets for $m = 2$ (see Theorem 2.3.4) and the Hall difference sets for $m = 6$ (see the forthcoming Theorem 3.5.8). Notice that, if D is a difference set in $(\mathbb{F}_p, +)$, then it must have Hadamard parameters. Equivalently, $d_D(u) = (p-3)/4$ for each $u \in \mathbb{F}_p^*$, where d_D is the difference function defined in Section 2.3.

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 $C_0, C_1, \ldots, C_{m-1}$ be the cyclotomic classes of $\mathbb{F}_p$ of order m with respect to ω. Let S be an $m/2$-element subset of $\{0, 1, \ldots, m-1\}$ and let D be the union of the $m/2$ cyclotomic classes C_s with $s \in S$. We may take 1 as a generator of $(\mathbb{F}_p, +)$, in which case the characteristic sequence A of D is

$$A = \big(\mathbb{1}_D(0), \mathbb{1}_D(1), \ldots, \mathbb{1}_D(p-1)\big). \tag{3.21}$$

This is no loss of generality; if the generator is θ, then replace D by $\theta^{-1}D$. Let f_A be the Littlewood polynomial with coefficient sequence A. The following lemma gives the evaluations of f_A at p-th roots of unity.

Lemma 3.5.1. *Assume the notation as above and let χ be a multiplicative character of $\mathbb{F}_p$ of order m. Then, for each integer k,*

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

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

$$\begin{aligned} f_A(e^{2\pi ik/p}) &= \sum_{x \in D} e^{2\pi ikx/p} - \sum_{x \in \mathbb{F}_p \setminus D} e^{2\pi ikx/p} \\ &= 2 \sum_{x \in D} e^{2\pi ikx/p} - \sum_{x \in \mathbb{F}_p} e^{2\pi ikx/p} \\ &= 2 \sum_{x \in D} e^{2\pi ikx/p} \\ &= 2 \sum_{s \in S} \sum_{x \in C_s} e^{2\pi ikx/p}. \end{aligned}$$

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

$$\begin{aligned} \sum_{x \in C_s} e^{2\pi ikx/p} &= \sum_{j=0}^{h-1} e^{2\pi ik\omega^{mj+s}/p} \\ &= \frac{1}{m} \Bigg(\sum_{x \in \mathbb{F}_p} e^{2\pi ik\, \omega^s x^m/p} - 1 \Bigg). \end{aligned}$$

Since $\sum_{j=0}^{m-1} \chi^j(x)$ equals m if x is an m-th power and equals zero otherwise by Lemma 2.2.1 (ii), we have, for each $a \in \mathbb{F}_p^*$,

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

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,

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

which gives the desired result. □

Our next result estimates L_A for A given in (3.21) at all points, but $(0, 0, 0)$.

Proposition 3.5.2. *With the notation as above, we have*

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

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

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

and

$$\mu = \big|\{(s, s') \in S \times S \colon s - s' = m/2\}\big|.$$

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 3.5.1 we find that

$$f_A(e^{2\pi i k/p}) = \sum_{j=1}^{m-1} G(\chi^j) K(\chi^j) \overline{\chi^j(k)} - 1 \tag{3.22}$$

for each integer k. Hence, $L_A(a,b,c)$ equals

$$\frac{1}{p^3}\sum_{j_1,j_2,j_3,j_4=1}^{m-1} G(\chi^{j_1})G(\chi^{j_2})\overline{G(\chi^{j_3})G(\chi^{j_4})}\,K(\chi^{j_1})K(\chi^{j_2})\overline{K(\chi^{j_3})K(\chi^{j_4})} \times \sum_{k\in\mathbb{F}_p} \overline{\chi^{j_1}(k)\chi^{j_2}(k+a)}\chi^{j_3}(k+b)\chi^{j_4}(k+c) + \Delta, \tag{3.23}$$

where $|\Delta| \le 15(m-1)^4 p^{-1/2}$, using that the magnitude of the sum on the right-hand side of (3.22) is at most $(m-1)\sqrt{p}$ by Lemma 2.2.3.

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 (3.23) 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 Lemma 2.2.6 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, $L_A(a,0,a)$ equals

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

plus an error term of magnitude at most $16(m-1)^4 p^{-1/2}$. Then we find from Lemma 2.2.3 and

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

that the desired result holds for $b = 0$ and $c = a \neq 0$.

The case that $c = 0$ 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 (3.23) 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, $L_A(0,b,b)$ equals

$$\frac{1}{p^2}\left|\sum_{j=1}^{m-1} G(\chi^j)G(\overline{\chi^j})\,K(\chi^j)K(\overline{\chi^j})\right|^2 \tag{3.24}$$

plus an error term of magnitude at most $16(m-1)^4 p^{-1/2}$. From Lemma 2.2.3 we find

that (3.24) equals

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

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 Lemma 2.2.6 again to conclude that the inner sum in (3.23) is at most $3\sqrt{p}$ in magnitude. Therefore, by Lemma 2.2.3 we have

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

which completes the proof. □

Our next theorem is the main result of this section. It applies not only to the characteristic sequences of difference sets, but requires this condition to hold asymptotically (in a precise sense).

Theorem 3.5.3. *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 $p\equiv 1 \pmod m$. For each p, let D_p be the union of the $m/2$ cyclotomic classes C_s with $s\in S$ of $\mathbb{F}_p$ of order m, and let A_p be a characteristic sequence of D_p. Suppose that, as $p\to\infty$,*

$$\frac{(\log p)^3}{p^2}\sum_{u=1}^{p-1}R_{A_p}(u)^2 \to 0. \tag{3.25}$$

Let R and $T>0$ be real. If $r/p\to R$ and $t/p\to T$ as $p\to\infty$, then the following hold as $p\to\infty$:

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

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

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

Proof. Without loss of generality, we may choose 1 as a generator of $(\mathbb{F}_p,+)$ and take $A_p=(\mathbb{1}_D(0),\mathbb{1}_D(1),\dots,\mathbb{1}_D(p-1))$ as a characteristic sequence of D_p as in (3.21). We shall deduce Theorem 3.5.3 from Theorem 3.2.1. Proposition 3.5.2 takes care of all values of $L_{A_p}(a,b,c)$ in the condition of Theorem 3.2.1, except when $(a,b,c)=(0,0,0)$. We shall show that our assumption (3.25) takes care of the latter case.

Let f_{A_p} be the Littlewood polynomial with characteristic sequence A_p. By Proposi-

tion 1.2.1 (i) we have, for each integer k,

$$\begin{aligned}\left|f_{A_p}(e^{2\pi ik/p})\right|^2 &= \sum_{u=-p+1}^{p-1} C_{A_p}(u)e^{2\pi iku/p} \\ &= p + \sum_{u=1}^{p-1} C_{A_p}(u)e^{-2\pi iku/p} + \sum_{u=1}^{p-1} C_{A_p}(p-u)e^{2\pi ik(p-u)/p} \\ &= \sum_{u\in\mathbb{F}_p} R_{A_p}(u)e^{-2\pi iku/p},\end{aligned}$$

where we have used (2.1) in the ultimate step. Thus, by Parseval's theorem,

$$\frac{1}{p}\sum_{k\in\mathbb{F}_p}\left|f_{A_p}(e^{2\pi ik/p})\right|^4 = \sum_{u\in\mathbb{F}_p} R_{A_p}(u)^2.$$

Since $R_{A_p}(0) = p$, we find that $L_f(0,0,0)$ equals

$$\frac{1}{p^3}\sum_{k\in\mathbb{F}_p}\left|f_{A_p}(e^{2\pi ik/p})\right|^4 = 1 + \frac{1}{p^2}\sum_{u=1}^{p-1} R_{A_p}(u)^2.$$

Now our assumption (3.25) together with Proposition 3.5.2 imply that the condition of Theorem 3.2.1 is satisfied, which proves the theorem. □

Several remarks on Theorem 3.5.3 follow. It is readily verified that ν in Theorem 3.5.3 satisfies $\nu \in [0,1]$. The condition (3.25) is essentially necessary since

$$\frac{1}{\mathrm{F}(A_p)} \geq \frac{1}{2p^2}\sum_{u=1}^{p-1} R_{A_p}(u)^2,$$

which can be deduced from (2.1) and the Cauchy-Schwarz inequality.

Let A_p be defined as in (3.21). The condition (3.25) can be checked using

$$R_{A_p}(u) = 4d_{D_p}(u) - (p-2) \quad \text{for each } u = 0,1,\ldots,p-1, \tag{3.26}$$

which follows from Lemma 2.3.8. To compute the values of the difference function in (3.26) one can use the cyclotomic numbers of order m, which are the m^2 numbers

$$|(C_i+1)\cap C_j| \quad \text{for } i,j \in \{0,1,\ldots,m-1\}.$$

These numbers can be expressed in terms of Jacobi sums (see [9, Theorem 2.5.1]) and are known explicitly for all even $m \leq 20$ and for $m = 24$ (see [9, p. 152] for a list of references).

Also note that the conclusion of Theorem 3.5.3 remains unchanged if we replace S by $h + S$ reduced modulo m for an integer h (which changes D_p to $\omega^h D_p$), so that we do not have to consider all $\binom{m}{m/2}$ choices for forming the set S. In fact, it can be shown that

the number of sets S that we have to consider is only

$$\frac{1}{m}\sum_{d\,|\,\frac{m}{2}}\varphi(d)\binom{m/d}{m/(2d)},$$

which can be deduced from [122, Problem 7.112 b].

We note that some results related to Theorem 3.5.3 and Corollary 3.5.7 have been obtained independently by Boothby and Katz [10], which appeared in preprint form after the submission of [49]. In [10] the authors study the crosscorrelations between two sequences derived from linear combinations of multiplicative characters of finite fields, which in particular applies to sequences derived from cyclotomy, as in Theorem 3.5.3. If these two sequences are equal, the crosscorrelations reduce to autocorrelations, in which case the combination of [10, Corollary 2] and [10, Lemma 15] leads to a result similar to Theorem 3.5.3. The difference is that the condition (3.25) is removed, but the limit contains an extra term involving combinations of Gauss sums. The authors of [10] could evaluate this extra term in the cases $m = 2$ and $m = 4$.

We now consider the cases $m \in \{2, 4, 6\}$ of Theorem 3.5.3 in detail and we also look briefly at the case $m = 8$.

The case $m = 2$

Let $m = 2$ and let p be an odd prime. Here, D_p consists of either the squares or the nonsquares of $\mathbb{F}_p^*$. As remarked above, we can assume without loss of generality that D_p is the set of squares in $\mathbb{F}_p^*$. From Theorem 2.5.4 we know already that D_p is a Paley difference set for $p \equiv 3 \pmod 4$, and an almost difference set with parameters (2.10) for $p \equiv 1 \pmod 4$.

Notice that the characteristic sequence A_p of D_p with respect to the generator 1 of $(\mathbb{F}_p, +)$ is the Legendre sequence of length p. Using the cyclotomic numbers of order 2 (see [9, Theorem 2.2.2], for example), we have

$$R_{A_p}(u) = \begin{cases} -2 - (-1)^{\frac{p-1}{2}} & \text{if } u \text{ is a square in } \mathbb{F}_p^* \\ (-1)^{\frac{p-1}{2}} & \text{if } u \text{ is a nonsquare in } \mathbb{F}_p^*, \end{cases} \tag{3.27}$$

which reproves Theorem 2.5.4.

Noting that $\nu = 1$ for $m = 2$ and using (3.27) to check the condition (3.25), we obtain the following corollary, which is essentially the main result of [62] (see also [61, Theorem 2.1]).

Corollary 3.5.4 ([62])**.** *Let p take values in an infinite set of odd primes. For each p, let D_p be either the set of squares or the set of nonsquares of $\mathbb{F}_p^*$, and let A_p be a characteristic sequence of D_p. Let R and $T > 0$ be real. If $r/p \to R$ and $t/p \to T$ as $p \to \infty$, then $\mathrm{F}(A_p^{r,t}) \to \varphi_1(R, T)$ as $p \to \infty$.*

The case $T = 1$ of Corollary 3.5.4 is due to Høholdt and Jensen [57]. It implies that, if $r/p \to R$ as $p \to \infty$, then the merit factor of $A_p^{r,p}$ tends to $\varphi_1(R, 1)$ as $p \to \infty$. For $|R| \leq 1/2$, we have

$$\frac{1}{\varphi_1(R,1)} = \frac{1}{6} + 8\left(|R| - \frac{1}{4}\right)^2,$$

so that the largest asymptotic merit factor that can be attained in this case is $\varphi_1(1/4, 1) = 6$. The maximum asymptotic merit factor that can be attained in Corollary 3.5.4 is $6.342061\ldots$, the largest root of

$$29x^3 - 249x^2 + 417x - 27.$$

It is attained when $T = 1.057827\ldots$ is the middle root of

$$4x^3 - 30x + 27$$

and $R = 3/4 - T/2$. Recall that the value $6.342061\ldots$ is in fact the largest known asymptotic merit factor that is attained by any family of binary sequences.

The case $m = 4$

We now look at the case $m = 4$. Here, we only have 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 $m = 2$.

The cyclotomic numbers of order four have been already determined by Gauss and can be found, for example, in [9, Theorem 2.4.1]. Recall from elementary number theory that primes of the form $x^2 + 4y^2$ for integers x and y are exactly the primes that are congruent to 1 modulo 4. The cyclotomic numbers of order four 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 of $\mathbb{F}_p$ used to define the cyclotomic classes, but this is encapsulated in the fact that y is unique only up to sign.

Let p be a prime with $p \equiv 1 \pmod 4$ and write $p = x^2 + 4y^2$. Define A to be the characteristic sequence of $D = C_0 \cup C_1$ that corresponds to the generator 1 of $(\mathbb{F}_p, +)$. Using the cyclotomic numbers of order four, we can calculate the periodic autocorrelations of A, which are listed in Table 3.1. For example if $u \in C_1$, then $u^{-1} \in C_3$, so that

$$R_A(u) = 4\big(|(C_3+1) \cap C_3| + |(C_3+1) \cap C_0| + |(C_0+1) \cap C_3| + |(C_0+1) \cap C_0|\big) - p + 2.$$

From the data in Table 3.1 together with Proposition 2.3.9 we conclude the following result due to Ding, Helleseth, and Lam [27].

Theorem 3.5.5 ([27]). *Let p be a prime of the form $p = x^2 + 4y^2$ for integers x and y. Let C_0, C_1, C_2, C_3 be the cyclotomic classes of $\mathbb{F}_p$ of order four with respect to some primitive element of $\mathbb{F}_p$. Then $C_0 \cup C_1$ is an almost difference set in $(\mathbb{F}_p, +)$ with parameters* (2.10)

Table 3.1: The numbers $R_A(u)$ for the characteristic sequence A of $C_0 \cup C_1$ (corresponding to the generator 1) for primes p of the form $p = x^2 + 4y^2$.

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

(equivalently, a characteristic sequence of $C_0 \cup C_1$ is optimal balanced) if and only if $(p-1)/4$ is odd and $y \in \{-1, 1\}$.

We call the almost difference sets that arise from the theorem *Ding-Helleseth-Lam almost difference sets*. We consider an example that illustrates Theorem 3.5.5.

Example 3.5.6. Let $p = 29 = 5^2 + 4$ and choose the primitive element 2 of $\mathbb{F}_{29}$ to build cyclotomic classes of order four. Then

$$C_0 \cup C_1 = \{1, 2, 3, 7, 11, 14, 16, 17, 19, 20, 21, 23, 24, 25\}.$$

The characteristic sequence A of $C_0 \cup C_1$ with respect to the generator 1 of $(\mathbb{F}_{29}, +)$ is

$$A = (- + + + - - - + - - - + - - + - + + - + + + - + + + - - -).$$

In accordance with Theorem 3.5.5, we have

$$R_A(u) = \begin{cases} -3 & \text{for } u \in \{1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28\} \\ 1 & \text{for } u \in \{2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27\}. \end{cases}$$

However, it is not known whether there are infinitely many primes of the form $x^2 + 4$. The next corollary of Theorem 3.5.3 does not only apply to Ding-Helleseth-Lam almost difference sets.

Corollary 3.5.7. *Let p take values in an infinite set of primes of the form $x^2 + 4y^2$ for integers x and y with $y^2(\log p)^3/p \to 0$ as $p \to \infty$. For each p, let D_p be the union of two cyclotomic classes of $\mathbb{F}_p$ of order four, and let A_p be a characteristic sequence of D_p. Let R and $T > 0$ be real. If $r/p \to R$ and $t/p \to T$ as $p \to \infty$, then $\mathrm{F}(A_p^{r,t}) \to \varphi_1(R, T)$ as $p \to \infty$.*

Proof. From the data in Table 3.1 we conclude that the assumption $y^2(\log p)^3/p \to 0$ implies the condition (3.25) in Theorem 3.5.3. It is also readily verified that $\nu = 1$, which completes the proof. □

In particular, the asymptotic merit factor of the sequences considered in Corollary 3.5.7 behaves in the same way as those of Legendre sequences. It is known (see [22, Theorem 1], for example) that there are infinitely many primes satisfying the hypothesis of Corollary 3.5.7. This can also be deduced from the fact that the normalised Gauss sum $G(\chi)/\sqrt{p}$, where χ is a multiplicative character of order four of $\mathbb{F}_p$, becomes equidistributed on the complex unit circle when p runs through the set of primes congruent to 1 modulo 4 [55], [102].

We note that Boothby and Katz [10] proved a more general version of Corollary 3.5.7. In particular, [10, Theorem 19] (together with [10, Theorem 18]) generalises Corollary 3.5.7 in the sense that the asymptotic merit factor, as $p \to \infty$, is given in terms of a limit point of γ, where $\tan(\gamma) = 2y/x$ and $p = x^2 + 4y^2$. Corollary 3.5.7 is essentially the case $\gamma \to 0$, which maximises the asymptotic merit factor.

The case $m = 6$

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

$$C_0 \cup C_2 \cup C_4, \quad C_0 \cup C_1 \cup C_2, \quad C_0 \cup C_1 \cup C_3, \quad C_0 \cup C_1 \cup C_4. \tag{3.28}$$

Again, the first set brings us back to $m = 2$.

The cyclotomic numbers of order six have been determined by Dickson [24] (see also [52] for $(p-1)/6$ odd and [132] 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), on the cubic character of 2, and on the parity of $(p-1)/6$. It is known [9, Corollary 2.6.4] that primes p of the form $p = x^2 + 27y^2$ for integers x and y are exactly the primes for which $p \equiv 1 \pmod 6$ and 2 is a cube modulo p.

Let p be a prime of the form $p = x^2 + 27y^2$. Define A to be the characteristic sequence of D that corresponds to the generator 1 of $(\mathbb{F}_p, +)$, where D is either the second, third, or fourth set in (3.28). The numbers $R_A(u)$ can be calculated using the cyclotomic numbers of order six and are given in Tables 3.2 and 3.3 (as in the case $m = 4$, the integer y is only unique up to sign, corresponding to different primitive elements of $\mathbb{F}_p$).

From the data in Table 3.2 we conclude the following result due to Hall [52].

Theorem 3.5.8 ([52])**.** *Let p be a prime of the form $p = 4x^2 + 27$ for some integer x. Let $C_0, C_1, \ldots, C_5$ be the cyclotomic classes of $\mathbb{F}_p$ of order six with respect to some primitive element of $\mathbb{F}_p$. If $3 \in C_1$, then write $D = C_0 \cup C_1 \cup C_3$, and if $3 \in C_5$, then write $D = C_0 \cup C_1 \cup C_4$[4]. Then D is a difference set in $(\mathbb{F}_p, +)$ with Hadamard parameters. Equivalently, a characteristic sequence of D is optimal balanced.*

The difference sets that arise from Theorem 3.5.8 are called *Hall difference sets*.

[4] We always have $3 \in C_1 \cup C_5$ by quadratic and cubic reciprocity laws.

Moreover, Hall [52] proved that each union of three different cyclotomic classes of order six that is a difference set is either equivalent to the set of squares or to the Hall difference set.

Table 3.2: The numbers $R_A(u)$ for the characteristic sequence A of D (corresponding to the generator 1) for primes p of the form $p = x^2 + 27y^2$ and $(p-1)/6$ odd.

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

Table 3.3: The numbers $R_A(u)$ for the characteristic sequence A of D (corresponding to the generator 1) for primes p of the form $p = x^2 + 27y^2$ and $(p-1)/6$ even.

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

We consider an example that illustrates Theorem 3.5.8.

Example 3.5.9. Let $p = 31$ and choose the primitive element 3 of $\mathbb{F}_{31}$. Then

$$C_0 \cup C_1 \cup C_3 = \{1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30\}.$$

The characteristic sequence A of $C_0 \cup C_1 \cup C_3$ with respect to the generator 1 of $(\mathbb{F}_p, +)$ is

$$A = (- + + + + - + - + - - - + - - + + + - - - - - + + - - + - + +).$$

In accordance with Theorem 3.5.8, all nontrivial periodic autocorrelations of A are equal to -1.

Again, it is not known whether there are infinitely primes of the form $4x^2 + 27$. The next corollary of Theorem 3.5.3 does not only apply to Hall difference sets. In fact, we

shall see that Theorem 3.5.3 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 (3.28), then we say that D is of *Paley type*. Otherwise, we say that D is of *Hall type*.

Corollary 3.5.10. *Let p take values in an infinite set of primes of the form $x^2 + 27y^2$ for some integers x and y with $y^2(\log p)^3/p \to 0$ as $p \to \infty$. For each p, let D_p be the union of three cyclotomic classes of $\mathbb{F}_p$ of order six, and let A_p be a characteristic sequence of D_p. Let R and $T > 0$ be real. If $r/p \to R$ and $t/p \to T$ as $p \to \infty$, then the following hold as $p \to \infty$:*

(i) If, for each p, D_p is of Paley type or $\frac{p-1}{6}$ is even, then $\mathrm{F}(A_p^{r,t}) \to \varphi_1(R,T)$.

(ii) If, for each p, D_p is of Hall type and $\frac{p-1}{6}$ is odd, then $\mathrm{F}(A_p^{r,t}) \to \varphi_{1/9}(R,T)$.

Proof. From the data in Tables 3.2 and 3.3 we conclude that the assumption $y^2(\log p)^3/p \to 0$ implies the condition (3.25) in Theorem 3.5.3. The proof is completed by checking that $\nu = 1$ if D_p is of Paley type and $\nu = 1/9$ if D_p is of Hall type. □

Again, it is known [22] that there are infinitely many primes satisfying the hypothesis of Corollary 3.5.10.

The largest asymptotic merit factor that can be attained in Corollary 3.5.10 (ii) is $3.518994\ldots$, the largest root of

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

In the case that $T = 1$, Corollary 3.5.10 (ii) gives a maximum asymptotic merit factor of $54/17$.

The case $m = 8$

We now look briefly at the case $m = 8$. In this case, there are ten different choices for the set S in Theorem 3.5.3 to consider, namely

$$\begin{array}{lllll} \{0,2,4,6\}, & \{0,1,4,5\}, & \{0,1,2,3\}, & \{0,1,2,4\}, & \{0,1,2,5\}, \\ \{0,1,2,6\}, & \{0,1,3,4\}, & \{0,1,3,5\}, & \{0,1,3,6\}, & \{0,1,4,6\}. \end{array} \tag{3.29}$$

Again, the first set brings us back to $m = 2$, and the second set brings us back to $m = 4$. The cyclotomic numbers of order eight have been determined by Lehmer [80]. However, from those numbers we deduce that the merit factor of sequences that correspond to one of the remaining sets in (3.29) tends to zero as the sequence lengths tend to infinity.

3.6 Further difference sets with Singer parameters

As mentioned at the end of Section 3.1, there are further families of cyclic difference sets with Singer parameters. We have not been able to determine the asymptotic merit factors of the characteristic sequences of those difference sets. We now review the constructions and discuss the problems that occur in the merit factor calculation.

Maschietti difference sets

Maschietti [88] established a link between so-called monomial hyperovals in finite projective planes and difference sets with Singer parameters. His construction is strikingly simple: If the set

$$\{(1, x, x^\ell)\colon x \in \mathbb{F}_{2^m}\} \cup \{(0,1,0), (0,0,1)\}$$

forms a hyperoval in the projective plane of order 2^m, then $\{x + x^\ell\colon x \in \mathbb{F}_{2^m}\} \setminus \{0\}$ is a difference set in $\mathbb{F}_{2^m}^*$ with Singer parameters. We state Maschietti's result in a (for our concerns) more convenient way which follows [34] and [113], and which does not require any background on hyperovals. We include a short proof that relies on Lemma 2.3.3.

Theorem 3.6.1 ([88])**.** *Let ℓ and m be positive integers with $m > 1$ and ℓ coprime to $2^m - 1$, such that the map $x \mapsto x + x^\ell$ from $\mathbb{F}_{2^m}$ to itself is two-to-one. Then the set*

$$D_\ell = \{x + x^\ell\colon x \in \mathbb{F}_{2^m}\} \setminus \{0\}$$

is a difference set in $\mathbb{F}_{2^m}^*$ with Singer parameters. Equivalently, a characteristic sequence of D_ℓ is optimal balanced.

Proof. Let χ be a nontrivial multiplicative character of $\mathbb{F}_{2^m}$ and notice that $|D_\ell| = 2^{m-1} - 1$. Therefore, if D_ℓ is a difference set, then D_ℓ has Singer parameters. In order to prove that D_ℓ is a difference set, we want to make use of Lemma 2.3.3. Thus, we have to show that

$$|\chi(D_\ell)|^2 = 2^{m-2}. \tag{3.30}$$

Since the map $x \mapsto x + x^\ell$ is two-to-one and $\chi(0) = 0$, we have

$$\begin{aligned}\chi(D_\ell) &= \frac{1}{2} \sum_{x \in \mathbb{F}_{2^m}} \chi(x + x^\ell) \\ &= \frac{1}{2} \sum_{x \in \mathbb{F}_{2^m}} \chi(x)\chi(1 + x^{\ell-1}).\end{aligned}$$

Since the map $x \mapsto x + x^\ell$ is two-to-one, the only solutions of $x(1 + x^{\ell-1}) = 0$ are 0 and 1. Therefore, there is no $(\ell-1)$-th root of unity distinct from 1 in $\mathbb{F}_{2^m}$, which implies that $\ell - 1$

is coprime to $2^m - 1$. Let h be the multiplicative inverse of $\ell - 1$ modulo $2^m - 1$. Then

$$\begin{aligned}\chi(D_\ell) &= \frac{1}{2} \sum_{x \in \mathbb{F}_{2^m}} \chi^h(x)\chi(1+x) \\ &= \frac{1}{2} J(\chi^h, \chi).\end{aligned}$$

Noting that $\chi^{(h+1)(\ell-1)} = \chi^\ell$ is nontrivial, we deduce that χ^{h+1} is nontrivial, so that (3.30) follows from Lemma 2.2.5 (iii). □

The difference sets that arise from Theorem 3.6.1 are called *Maschietti difference sets*. Up to equivalence, the only known choices for ℓ are:

(i) $\ell = 2^j$ for all j with $\gcd(j, m) = 1$ (in which case we obtain Singer difference sets again);

(ii) $\ell = 6$ for odd m [117];

(iii) $\ell = 3 \cdot 2^{(m+1)/2} + 4$ for odd m [39];

(iv) $\ell = 2^{(m+1)/2} + 2^{(3m+1)/4}$ for $m \equiv 1 \pmod 4$ and $\ell = 2^{(m+1)/2} + 2^{(m+1)/4}$ for $m \equiv 3 \pmod 4$ [39].

As proved by Evans, Hollmann, Krattenthaler, and Xiang [34], the Maschietti difference sets that arise in the cases (ii), (iii), and (iv) are inequivalent to other known difference sets.

Let D_ℓ be a Maschietti difference set in $\mathbb{F}_{2^m}^*$, let θ be a primitive element of $\mathbb{F}_{2^m}$, and let A be the characteristic sequence of D_ℓ with respect to θ. Define f_A to be the Littlewood polynomial with coefficient sequence A and write $n = 2^m - 1$. The next proposition gives the evaluations of f_A at n-th roots of unity.

Proposition 3.6.2. *Assume the notation as above and let χ be the multiplicative character of $\mathbb{F}_{2^m}$ given by $\chi(\theta) = e^{2\pi i/n}$. Let h be the multiplicative inverse of $\ell - 1$ modulo n and let k be an integer. Then*

$$f_A\big(e^{2\pi i k/n}\big) = \begin{cases} -1 & \text{if } k \equiv 0 \pmod n \\ J(\chi^{hk}, \chi^k) & \text{if } k \not\equiv 0 \pmod n. \end{cases}$$

Proof. Since $f_A(1) = |D_\ell| - |\mathbb{F}_{2^m}^* \setminus D_\ell| = -1$, the result holds for $k \equiv 0 \pmod n$, so assume

that $k \not\equiv 0 \pmod{n}$. By definition we have

$$\begin{aligned} f_A(e^{2\pi ik/n}) &= \sum_{\substack{0\le j<n \\ \theta^j \in D_\ell}} e^{2\pi ikj/n} - \sum_{\substack{0\le j<n \\ \theta^j \in \mathbb{F}_{2^m}^* \setminus D_\ell}} e^{2\pi ikj/n} \\ &= 2\sum_{\substack{0\le j<n \\ \theta^j \in D_\ell}} e^{2\pi ikj/n} - \sum_{0\le j<n} e^{2\pi ikj/n} \\ &= 2\sum_{\substack{0\le j<n \\ \theta^j \in D_\ell}} \chi^k(\theta^j) \\ &= 2\chi^k(D_\ell). \end{aligned}$$

From the proof of Theorem 3.6.1 we already know that

$$2\chi^k(D_\ell) = J(\chi^{hk}, \chi^k),$$

which completes the proof. □

Therefore, for the corresponding function L_A of A, we obtain

$$L_A(a,b,c) = \frac{1}{n^3} \sum_{\substack{k\in\mathbb{Z}/n\mathbb{Z} \\ k\notin\{0,-a,-b,-c\}}} J\big(\chi^{hk},\chi^k\big)J\big(\chi^{h(k+a)},\chi^{k+a}\big)\overline{J\big(\chi^{h(k+b)},\chi^{k+b}\big)J\big(\chi^{h(k+c)},\chi^{k+c}\big)} + \Delta,$$

where $|\Delta| \le 4(n+1)^{3/2}/n^3$ using Lemma 2.2.5 (iii). By Lemma 2.2.5 (iii) we also see that the function L_A is well approximated by I_n in the cases that $a = b$ and $c = 0$, or $a = c$ and $b = 0$. However, it seems to hard to estimate L_A in the remaining cases. Even applying Lemma 2.2.5 (iv), which allows us to re-write the occurring Jacobi sums as normalised products of Gauss sums, produces sums which cannot be bounded using Lemma 2.2.7.

Dillon-Dobbertin difference sets

The next construction is due to Dillon and Dobbertin [25]. Their proof uses Fourier analysis in the additive group of $\mathbb{F}_{2^m}$ and Dickson polynomials.

Theorem 3.6.3 ([25])**.** *Let ℓ and m be positive and coprime integers with $\ell < m/2$, and write $d = 4^\ell - 2^\ell + 1$. Let*

$$D_\ell = \{(x+1)^d + x^d + 1 \colon x \in \mathbb{F}_{2^m}\} \setminus \{0\}.$$

Then D_ℓ is a difference set in $\mathbb{F}_{2^m}^*$ with Singer parameters. Equivalently, a characteristic sequence of D_ℓ is optimal balanced.

The difference sets that arise from Theorem 3.6.3 are called *Dillon-Dobbertin difference*

sets. In the case that $\ell = 1$ we obtain Singer difference sets again.

Let D_ℓ be a Dillon-Dobbertin difference set in $\mathbb{F}_{2^m}^*$, let θ be a primitive element of $\mathbb{F}_{2^m}$, and let A be the characteristic sequence of D_ℓ with respect to θ. Define f_A to be the Littlewood polynomial with coefficient sequence A and write $n = 2^m - 1$. The next proposition gives the evaluations of f_A at n-th roots of unity.

Proposition 3.6.4. *Assume the notation as above and let χ be the multiplicative character of $\mathbb{F}_{2^m}$ given by $\chi(\theta) = e^{2\pi i/n}$. Let k be an integer. Then*

$$f_A\big(e^{2\pi ik/n}\big) = \frac{G(\chi^k)G(\chi^{(2^\ell+1)k})}{G(\chi^{3k})}.$$

Proof. Since $f_A(1) = |D_\ell| - |\mathbb{F}_{2^m}^* \setminus D_\ell| = -1$, the result holds for $k \equiv 0 \pmod{n}$, so assume that $k \not\equiv 0 \pmod{n}$. As in the proof of Proposition 3.6.2, we have

$$f_A(e^{2\pi ik/n}) = 2\chi^k(D_\ell).$$

The character values of Dillon-Dobbertin difference sets have been determined in [26] and are given by

$$2\chi^k(D_\ell) = \frac{G(\chi^k)G(\chi^{(2^\ell+1)k})}{G(\chi^{3k})},$$

which completes the proof. □

Again, in the cases that $a = b$ and $c = 0$, or $a = c$ and $b = 0$ it is readily verified that the to A corresponding function L_A is well approximated by I_n. However, it seems to hard to bound L_A in the remaining cases.

No-Chung-Yun difference sets

The last known construction of cyclic difference sets with Singer parameters was given by No, Chung, and Yun [98], but they could not prove that their construction provides infinitely many difference sets. This was proved by Dillon and Dobbertin [25] by using Fourier analysis in the additive group of $\mathbb{F}_{2^m}$ and by exploiting the theory of quadratic forms over fields of characteristic two.

Theorem 3.6.5 ([25])**.** *Let m be a positive integer that is not divisible by 3. If $m \equiv 1 \pmod 3$, then write $k = (m-1)/3$, and if $m \equiv 2 \pmod 3$, then write $k = (m+1)/3$. Write $d = 4^k - 2^k + 1$ and define*

$$C = \{(x+1)^d + x^d \colon x \in \mathbb{F}_{2^m}\}.$$

If m is even, then put $D = C$. If m is odd, then let D be the complement of C in $\mathbb{F}_{2^m}^*$. Then D is a difference set in $\mathbb{F}_{2^m}^*$ with Singer parameters. Equivalently, a characteristic sequence of D is optimal balanced.

We call the difference sets that arise from Theorem 3.6.5 *No-Chung-Yun difference sets*. We remark that although Dillon-Dobbertin difference sets are closely related to No-Chung-Yun difference sets, they are not equivalent and the proofs given in [25] are completely different. Adding 1 to a polynomial changes the multiplicative structure of its image a lot.

However, the character values of No-Chung-Yun difference sets are not known. Therefore, in order to apply the methods of this chapter to the characteristic sequences of those difference sets, one first has to determine its character values.

A conjecture on the asymptotic merit factor

We conjecture that the asymptotic merit factor of the characteristic sequences of Maschietti, Dillon-Dobbertin, and No-Chung-Yun difference sets behaves in the same way as those of Sidelnikov sequences, Galois sequences, and the characteristic sequences of Gordon-Mills-Welch difference sets (see Theorem 3.3.2, Corollary 3.4.5, and Theorem 3.4.4, respectively).

Conjecture 3.6.6. *Let m take values in an infinite set of positive integers. For each m, write $n = 2^m - 1$ and suppose that A_n is a characteristic sequence of length n of a Maschietti, Dillon-Dobbertin, or No-Chung-Yun difference set in $\mathbb{F}_{2^m}^*$. If $t/n \to T$ as $n \to \infty$, then $\mathrm{F}(A_n^{r,t}) \to \varphi_0(0,T)$ as $n \to \infty$.*

One could conjecture that the asymptotic merit factor of the characteristic sequences of all cyclic difference sets with Singer parameters behaves in the same way. However since Paley, Hall, and Singer difference sets have the same parameters in groups whose order is a *Mersenne prime* (which is a prime of the form $2^m - 1$), this claim seems to be false (it is not known whether there exist infinitely many Mersenne primes).

3.7 Conclusion and open problems

Most known constructions of binary sequences with large merit factor arise (sometimes in a subtle way) from difference sets, in particular from Paley and Singer difference sets. We considered the merit factors of sequences constructed from other difference sets, thereby providing the first essentially new examples since 1991. In particular, we proved the general Theorem 3.5.3 on the asymptotic merit factor of binary sequences arising from cyclotomy, which includes results on Hall and Paley difference sets, and also on Ding-Helleseth-Lam almost difference sets as special cases (see Corollaries 3.5.4, 3.5.7, and 3.5.10). We established the asymptotic merit factor of Sidelnikov sequences in Theorem 3.3.2, proving [61, Conjecture 7.2] in the affirmative and explaining numerical evidence made in [54]. In addition, we determined the asymptotic merit factor of the characteristic sequences of Gordon-Mills-Welch difference sets in Theorem 3.4.4, proving that [61, Conjecture 7.1] is true.

Define $\Phi = 6.342061\ldots$ to be the largest root of

$$29x^3 - 249x^2 + 417x - 27.$$

The largest asymptotic merit factor that has been obtained from any family of binary sequences is Φ (see Corollary 3.5.4). Let F_n be the maximum of $\mathrm{F}(A)$ taken over all binary sequences A of length n (as in Chapter 1). In view of Problem 1.6, the current state of knowledge can be summarised as:

$$\Phi \leq \limsup_{n\to\infty} F_n \leq \infty.$$

However, there is strong numerical evidence [5] that the value of Φ can be improved. We conclude with a list of open problems concerning the merit factor of binary sequences.

- Determine the asymptotic merit factor of the characteristic sequences of Maschietti and Dillon-Dobbertin difference sets (see also Conjecture 3.6.6).

  In order to attack this problem with the methods of this chapter one needs a more general version of Lemma 2.2.7.

- Determine the character values of No-Chung-Yun difference sets.

  This is the first step to determine the asymptotic merit factor of the characteristic sequences of those difference sets. If the character values are "nice enough", then the methods of this chapter could apply.

- Find other infinite families of cyclic difference sets with Hadamard parameters. Find other infinite families of binary sequences with large merit factor.

  Of course the ultimate goal is not to find more and more families, but rather to gain a better understanding of the asymptotic merit factor behaviour.

- Find a family of binary sequences whose asymptotic merit factor is greater than Φ.

  This is of course a very challenging problem. A good starting point might be the work of Baden [5]. He applied a steep descent algorithm to binary sequences with large merit factor and "optimised" the sequences to produce higher merit factors. In particular, he applied his algorithm to optimally rotated and appended Legendre sequences, and obtained (numerically) an asymptotic merit factor of 6.3758, which is slightly larger than Φ. More interestingly, applying the algorithm to optimally rotated and appended *Jacobi sequences* (which are generalisations of Legendre sequences to composite sequence lengths) whose length is a product of two primes, seems to produce an asymptotic merit factor of 6.4382. Even more strikingly it seems that applying the algorithm to Jacobi sequences whose length is a product of three, four, or more primes enlarges the asymptotic merit factor.

- Solve Problem 1.6, that is, determine

$$\limsup_{n\to\infty} F_n.$$

  This is arguably the most important and challenging problem concerning the merit factor of binary sequences and is just included for the sake of completeness.

Chapter 4

The L^α norm of Littlewood polynomials

4.1 Introduction and chapter overview

Recall from Chapter 1 that, for real $\alpha \geq 1$, the L^α *norm* of a polynomial f in $\mathbb{C}[z]$ on the complex unit circle is

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

and its supremum norm is $\|f\|_\infty = \max_{\theta\in[0,2\pi]}|f(e^{i\theta})|$. Until 2017, there was no known nontrivial *specific* family of Littlewood polynomials for which we can determine the asymptotic behaviour of its L^α norm for infinitely many α. In this chapter we generalise methods of Chapter 3 and consider the L^α norm of two families of Littlewood polynomials whose coefficient sequences come from difference sets, namely the *Fekete polynomials* and the *Galois polynomials*.

Let p be an odd prime and let η be the quadratic character of $\mathbb{F}_p$. The polynomial

$$f_p(z) = \sum_{j=1}^{p-1} \eta(j) z^j$$

is called the *Fekete polynomial* of degree $p-1$. Notice that $z^{-1}f_p(z)$ is a Littlewood polynomial which has the same L^α norm as $f_p(z)$, and that the coefficient sequence of f_p is the Legendre sequence of length p with initial element 0 instead of -1. Fekete polynomials appear frequently in the context of extremal polynomial problems (see [92], [23], [13], [12] and [69], for example) and have been studied extensively now for over a century [35].

In 1980 Montgomery [92] proved that for all sufficiently large primes p, we have

$$\frac{2}{\pi}\log\log p \leq \frac{\|f_p\|_\infty}{\sqrt{p}} \leq \frac{2}{\pi}\log p + 2,$$

and he conjectured that the upper bound can be improved to some constant times $\log\log p$. Combining (1.4) with Corollary 3.5.4, we have

$$\lim_{p\to\infty}\left(\frac{\|f_p\|_4}{\sqrt{p}}\right)^4 = \frac{5}{3}. \tag{4.1}$$

In fact, Borwein and Choi [12] established exact expressions for $\|f_p\|_4$ in terms of the class number of $\mathbb{Q}(\sqrt{-p})$.

We also consider the *shifted* Fekete polynomials

$$f_p^r(z) = \sum_{j=0}^{p-1} \eta(j+r)\, z^j,$$

where r is an integer that can depend on p. Notice that the coefficient sequences of shifted Fekete polynomials are again essentially shifted Legendre sequences. Combining (1.4) with Corollary 3.5.4, if $r/p \to R$ as $p \to \infty$, then

$$\lim_{p\to\infty}\left(\frac{\|f_p^r\|_4}{\sqrt{p}}\right)^4 = \frac{7}{6} + \frac{1}{2}(4|R|-1)^2 \quad \text{for } |R| \le \frac{1}{2}. \tag{4.2}$$

A shifted Fekete polynomial is not necessarily a Littlewood polynomial since one of its first p coefficients is zero. However, changing this coefficient to -1 or 1 does not affect the asymptotic behaviour of the L^α norm.

For a Mersenne number $n = 2^m - 1$, a *Galois polynomial* of degree $n-1$ is the Littlewood polynomial

$$g_n(z) = \sum_{j=0}^{n-1} \psi(\theta^j)\, z^j,$$

where θ is a primitive element of $\mathbb{F}_{2^m}$ and ψ is a nontrivial additive character of $\mathbb{F}_{2^m}$. Therefore, the coefficient sequence of g_n is a Galois sequence of length n. Again, combining (1.4) with Corollary 3.4.5, we obtain

$$\lim_{n\to\infty}\left(\frac{\|g_n\|_4}{\sqrt{n}}\right)^4 = \frac{4}{3}. \tag{4.3}$$

We shall see that (4.1), (4.2), and (4.3) are in fact special cases of our main results (see the forthcoming Theorems 4.3.7, 4.3.6, and 4.4.4).

The remainder of this chapter is structured as follows. In Section 4.2 we prove a general result on the L^α norm of a polynomial that lays the foundation to prove our main results. In Sections 4.3 and 4.4 we calculate the L^α norm of Fekete and Galois polynomials, respectively. We give explicit and recursive formulas for the limit of the ratio of L^α and L^2 norm of Fekete and Galois polynomials when α is an even positive integer and the degree of the polynomials tends to infinity. Similar results are given for the shifted Fekete polynomials. Our results vastly generalise earlier results on the L^4 norm of these

polynomials. To our knowledge, these are the first results that give these limiting values for specific families of nontrivial Littlewood polynomials and infinitely many α. We conclude with Section 4.5, where give a list of open problems concerning the L^α norm of Littlewood polynomials.

The results of this chapter are also published in [48].

4.2 Calculation of $L^{2\alpha}$ norms

We begin with establishing some notation that will be used throughout this chapter. For a positive integer n, write $\epsilon_n(x) = e^{2\pi i x/n}$. Let $f(z) = \sum_{j=0}^{n-1} a_j z^j$ be a polynomial in $\mathbb{C}[z]$ of degree $n-1$ and let r be an integer. Define the *shifted* polynomial

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

where, as for sequences, we extend the definition of a_j so that $a_{j+n} = a_j$ for all $j \in \mathbb{Z}$. Informally speaking, the coefficient sequence of f^r is obtained from the coefficient sequence of f by cyclically shifting its entries by r elements to the left. Notice that f^r is the same polynomial as that given in (3.1) with $t = n$.

We shall express the $L^{2\alpha}$ norm of the polynomial f^r, where α is a positive integer, in a form that will be convenient for us later. To do so, we associate with f the function $L_f\colon (\mathbb{Z}/n\mathbb{Z})^{2\alpha} \to \mathbb{C}$ given by

$$L_f(t_1, \dots, t_{2\alpha}) = \frac{1}{n^{\alpha+1}} \sum_{m \in \mathbb{Z}/n\mathbb{Z}} \prod_{k=1}^{\alpha} f\big(\epsilon_n(m+t_k)\big)\overline{f\big(\epsilon_n(m+t_{\alpha+k})\big)}.$$

Let A be the coefficient sequence of f. The function L_f is closely related to the function L_A given in (3.3). In fact, for $\alpha = 2$, we have $L_f(0, a, b, c) = L_A(a, b, c)$. We shall see that introducing a fourth variable (and, for higher norms, a 2α-th variable) in the definition of L_f will make the arising combinatorics easier. Define another function $h_{n,r}\colon (\mathbb{Z}/n\mathbb{Z})^{2\alpha} \to \mathbb{C}$ by

$$h_{n,r}(t_1, \dots, t_{2\alpha}) = \sum_{\substack{0 \le j_1, \dots, j_{2\alpha} < n \\ j_1 + \dots + j_\alpha = j_{\alpha+1} + \dots + j_{2\alpha}}} \prod_{k=1}^{\alpha} \overline{\epsilon_n\big(t_k(j_k + r)\big)}\epsilon_n\big(t_{\alpha+k}(j_{\alpha+k} + r)\big).$$

The following proposition will be the starting point of our considerations.

Proposition 4.2.1. *Let α be a positive integer, let f be a polynomial in $\mathbb{C}[z]$ of degree $n-1$, and let r be an integer. Then*

$$\|f^r\|_{2\alpha}^{2\alpha} = \frac{1}{n^\alpha} \sum_{\boldsymbol{t} \in (\mathbb{Z}/n\mathbb{Z})^{2\alpha}} L_f(\boldsymbol{t})\, h_{n,r}(\boldsymbol{t}).$$

Proof. Write $f(z) = \sum_{j=0}^{n-1} a_j z^j$. From

$$\|f^r\|_{2\alpha}^{2\alpha} = \frac{1}{2\pi} \int_0^{2\pi} \left(f^r(e^{i\theta}) \overline{f^r(e^{i\theta})} \right)^\alpha d\theta$$

we obtain

$$\|f^r\|_{2\alpha}^{2\alpha} = \sum_{\substack{0 \le j_1, \dots, j_{2\alpha} < n \\ j_1 + \cdots + j_\alpha = j_{\alpha+1} + \cdots + j_{2\alpha}}} \prod_{k=1}^{\alpha} a_{j_k + r} \, \overline{a_{j_{\alpha+k}+r}}.$$

It is readily verified that

$$a_j = \frac{1}{n} \sum_{s \in \mathbb{Z}/n\mathbb{Z}} f\big(\epsilon_n(s)\big) \, \epsilon_n(-sj),$$

giving

$$\|f^r\|_{2\alpha}^{2\alpha} = \frac{1}{n^{2\alpha}} \sum_{s_1, \dots, s_{2\alpha} \in \mathbb{Z}/n\mathbb{Z}} h_{n,r}(s_1, \dots, s_{2\alpha}) \prod_{k=1}^{\alpha} f\big(\epsilon_n(s_k)\big) \, \overline{f\big(\epsilon_n(s_{\alpha+k})\big)}.$$

Re-index the summation with $s_i = m + t_i$ for all i and then sum over $m \in \mathbb{Z}/n\mathbb{Z}$ to obtain the statement in the proposition. □

We also need the following estimate, which we deduce from Lemma 3.2.3.

Corollary 4.2.2. *Let α be a positive integer. There exists a constant c_α which only depends on α such that, for all positive integers n and all integers r, we have*

$$\sum_{\boldsymbol{t} \in (\mathbb{Z}/n\mathbb{Z})^{2\alpha}} |h_{n,r}(\boldsymbol{t})| \le c_\alpha \, n^{2\alpha} (1 + \log n)^{2\alpha - 1}.$$

Proof. After re-indexing the summation in the definition of $h_{n,r}(\boldsymbol{t})$ with

$$j_i = n - 1 - \ell_i \quad \text{and} \quad j_{\alpha+i} = \ell_{\alpha+i} \quad \text{for all } i \in \{1, \dots, \alpha\},$$

the statement of the lemma is equivalent to

$$\sum_{t_1, \dots, t_{2\alpha} \in \mathbb{Z}/n\mathbb{Z}} \left| \sum_{\substack{0 \le \ell_1, \dots, \ell_{2\alpha} < n \\ \ell_1 + \cdots + \ell_{2\alpha} = \alpha(n-1)}} \epsilon_n(t_1\ell_1 + \cdots + t_{2\alpha}\ell_{2\alpha}) \right| \le c_\alpha \, n^{2\alpha} (1 + \log n)^{2\alpha - 1}. \tag{4.4}$$

Replace $\ell_{2\alpha} = \alpha(n-1) - \ell_1 - \cdots - \ell_{2\alpha-1}$ and re-index with $s_i = t_i - 1$ for all $i \in \{1, \dots, 2\alpha - 1\}$ to see that the left-hand side of (4.4) equals n times the left-hand side of the statement in Lemma 3.2.3 (with $t = n$), which completes the proof. □

4.3 Fekete polynomials

In this section we prove our results on the $L^{2\alpha}$ norm of (shifted) Fekete polynomials.

We begin with setting some notation. We say that a tuple $(t_1, t_2, \dots, t_{2\alpha})$ is *even* if there exists a permutation σ of $\{1, 2, \dots, 2\alpha\}$ such that $t_{\sigma(2k-1)} = t_{\sigma(2k)}$ for each $k \in \{1, 2, \dots, \alpha\}$. For example $(2, 1, 1, 3, 2, 3)$ is even, whereas $(2, 1, 1, 3, 1, 3)$ is not even. Let $\mathcal{E}_\alpha(n)$ be the set of even tuples in $(\mathbb{Z}/n\mathbb{Z})^{2\alpha}$.

We begin with the following lemma.

Lemma 4.3.1. *Let α be a positive integer and, for each odd prime p, let f_p^r be a shifted Fekete polynomial corresponding to the Fekete polynomial of degree $p-1$. Then*

$$\lim_{p\to\infty} \left(\frac{\|f_p^r\|_{2\alpha}}{\sqrt{p}}\right)^{2\alpha} = \lim_{p\to\infty} \frac{1}{p^{2\alpha}} \sum_{\boldsymbol{t}\in\mathcal{E}_\alpha(p)} h_{p,r}(\boldsymbol{t}), \tag{4.5}$$

provided that one of the limits exists.

Proof. Let f_p be the Fekete polynomial of degree $p-1$. For $\boldsymbol{t} \in (\mathbb{Z}/p\mathbb{Z})^{2\alpha}$, let $J_p(\boldsymbol{t})$ be the indicator function that equals one if $\boldsymbol{t}$ is even and is zero otherwise. From Proposition 4.2.1 we find that

$$\left(\frac{\|f_p^r\|_{2\alpha}}{\sqrt{p}}\right)^{2\alpha} = \frac{1}{p^{2\alpha}} \sum_{\boldsymbol{t}\in(\mathbb{Z}/p\mathbb{Z})^{2\alpha}} J_p(\boldsymbol{t}) h_{p,r}(\boldsymbol{t}) + \frac{1}{p^{2\alpha}} \sum_{\boldsymbol{t}\in(\mathbb{Z}/p\mathbb{Z})^{2\alpha}} \big(L_{f_p}(\boldsymbol{t}) - J_p(\boldsymbol{t})\big)\, h_{p,r}(\boldsymbol{t}).$$

We show that the second sum on the right-hand side tends to zero. This will prove the lemma since

$$\sum_{\boldsymbol{t}\in(\mathbb{Z}/p\mathbb{Z})^{2\alpha}} J_p(\boldsymbol{t}) h_{p,r}(\boldsymbol{t}) = \sum_{\boldsymbol{t}\in\mathcal{E}_\alpha(p)} h_{p,r}(\boldsymbol{t}).$$

Let η be the quadratic character of $\mathbb{F}_p$. Notice that $f_p(e^{2\pi i k/p})$ equals the canonical quadratic Gauss sum $G(\eta)$, whose explicit evaluation is

$$G(\eta) = i^{(p-1)^2/4} p^{1/2}\, \eta(k)$$

by Proposition 2.2.4. Therefore,

$$L_{f_p}(t_1, \dots, t_{2\alpha}) = \frac{1}{p} \sum_{m=0}^{p-1} \eta(m+t_1) \cdots \eta(m+t_{2\alpha}).$$

If $(t_1, \dots, t_{2\alpha})$ is even, then it is readily verified that

$$1 - \alpha/p \le L_{f_p}(t_1, \dots, t_{2\alpha}) \le 1 - 1/p.$$

On the other hand, if $(t_1, \dots, t_{2q})$ is not even, then we have

$$|L_{f_p}(t_1, \dots, t_{2\alpha})| \le (2\alpha - 1)p^{-1/2}$$

by Lemma 2.2.6. Therefore,

$$\big|L_{f_p}(\boldsymbol{t}) - J_p(\boldsymbol{t})\big| \le (2\alpha - 1)p^{-1/2} \quad \text{for all } \boldsymbol{t} \in (\mathbb{Z}/p\mathbb{Z})^{2\alpha}.$$

By the triangle inequality we then find that

$$\frac{1}{p^{2\alpha}}\left|\sum_{\boldsymbol{t}\in(\mathbb{Z}/p\mathbb{Z})^{2\alpha}} \big(L_{f_p}(\boldsymbol{t}) - J_p(\boldsymbol{t})\big)\, h_{p,r}(\boldsymbol{t})\right| \le \frac{2\alpha - 1}{p^{2\alpha+1/2}} \sum_{\boldsymbol{t}\in(\mathbb{Z}/p\mathbb{Z})^{2\alpha}} |h_{p,r}(\boldsymbol{t})|,$$

which tends by Lemma 3.2.3 to zero as $p \to \infty$, as required. □

Evaluation of the right-hand side of (4.5)

In what follows we shall evaluate the right-hand side of (4.5). First, we have to set some notation. For a positive integer m, let Π_m be the set of partitions of $\{1, 2, \dots, m\}$. For $\pi \in \Pi_m$, we refer to the elements of π as *blocks*. We shall need the following combinatorial principle (see [122, p. 5], for example), in which $\mathbb{N}$ is the set of positive integers.

Lemma 4.3.2. *Let K be a field of characteristic 0, let $f\colon \mathbb{N} \to K$ be arbitrary, and define a new function $g\colon \mathbb{N} \cup \{0\} \to K$ by $g(0) = 1$ and*

$$g(k) = \sum_{\pi\in\Pi_k} \prod_{B\in\pi} f(|B|) \quad \textit{for } k \ge 1.$$

Let $G(z) = \sum_{k\ge0} g(k)z^k/k!$ and $F(z) = \sum_{k\ge1} f(k)z^k/k!$ be the corresponding exponential generating functions. Then $G(z) = \exp(F(z))$. Moreover,

$$g(k) = \sum_{j=1}^{k} \binom{k-1}{j-1} f(j)g(k-j) \quad \textit{for } k \ge 1.$$

Proof. The first part of the lemma is a consequence of Faá di Bruno's generalisation of the chain rule (see [77, Theorem 1.3.2], for example), which states that, for a formal power series $E(z)$ and $k \ge 1$, we have

$$(E \circ F)^{(k)}(z) = \sum_{\pi\in\Pi_k} (E^{(|\pi|)} \circ F)(z) \prod_{B\in\pi} F^{(|B|)}(z).$$

Take $E(z) = \exp(z)$ and set $z = 0$ to see that the right-hand side equals $g(k)$, which proves the first part. The second part follows from $G'(z) = G(z)F'(z)$ by equating coefficients. □

We need some more notation. The *signed tangent numbers* $T(k)$ are defined by the

Maclaurin series

$$\log\cosh(z) = \sum_{k=1}^{\infty} \frac{T(k)}{(2k)!}\, z^{2k}. \tag{4.6}$$

They are scaled versions of Bernoulli numbers and $|T(k)| = (-1)^{k+1}T(k)$ are known as the *tangent* or *zag* numbers, which appear in [1] as

$$\texttt{A000182} = [1, 2, 16, 272, 7936, 353792, \dots].$$

The numbers $T(k)$ can be recursively determined via

$$T(k) = 1 - \sum_{j=1}^{k-1} \binom{2k-1}{2j-1} T(j) \quad \text{for } k \geq 1.$$

This can be deduced from Lemma 4.3.2, in which we choose $f\colon \mathbb{N} \to \mathbb{R}$ such that $F(z) = \log\cosh(z)$, which means that

$$f(k) = \begin{cases} T(k/2) & \text{if } k \text{ is even} \\ 0 & \text{if } k \text{ is odd.} \end{cases}$$

Note that then $g(k) = 1$ if k is even and $g(k) = 0$ if k is odd since $G(z) = \cosh(z)$.

Let $\pi \in \Pi_m$. We say that π is *even* if each block of π has even cardinality. For example the element $\{\{1,4\},\{2,3\}\} \in \Pi_4$ is even, whereas $\{\{1,3,4\},\{2\}\}$ is not even. For a tuple $\boldsymbol{t} = (t_1, t_2, \dots, t_m)$ in $(\mathbb{Z}/n\mathbb{Z})^m$ we define $\boldsymbol{t} \prec \pi$ to be true if and only if $t_j = t_k$ whenever j and k belong to the same block of π. For example, if $\boldsymbol{t} = (1,2,1)$ and $\pi = \{\{1,3\},\{2\}\}$, then $t \prec \pi$ holds.

Lemma 4.3.3. *Let α be a positive integer, $h\colon \mathcal{E}_\alpha(n) \to \mathbb{C}$ be an arbitrary function, and let $T(k)$ be the k-th signed tangent number. Then*

$$\sum_{\boldsymbol{t}\in\mathcal{E}_\alpha(n)} h(\boldsymbol{t}) = \sum_{\substack{\pi\in\Pi_{2\alpha} \\ \pi \text{ even}}} \sum_{\substack{\boldsymbol{t}\in\mathcal{E}_\alpha(n) \\ \boldsymbol{t}\prec\pi}} h(\boldsymbol{t}) \prod_{B\in\pi} T\big(\tfrac{1}{2}|B|\big). \tag{4.7}$$

Proof. Taking $F(z) = \log\cosh(z)$ in Lemma 4.3.2 (so that $G(z) = \cosh(z)$), we find with (4.6) and $\cosh(z) = \sum_{k\geq 0} z^{2k}/(2k)!$ that

$$\sum_{\substack{\pi\in\Pi_{2k} \\ \pi \text{ even}}} \prod_{B\in\pi} T\big(\tfrac{1}{2}|B|\big) = 1 \quad \text{for each } k \geq 1. \tag{4.8}$$

Let $\boldsymbol{s} \in \mathcal{E}_\alpha(n)$ be an even tuple, and let $\pi_{\boldsymbol{s}} \in \Pi_{2\alpha}$ be the coarsest partition of $\{1, 2, \dots, 2\alpha\}$ with the property $\boldsymbol{s} \prec \pi_{\boldsymbol{s}}$. Define $m_k(\boldsymbol{s})$ to be the number of blocks B in $\pi_{\boldsymbol{s}}$ such that $|B| = k$. For example, if $\boldsymbol{s} = (1,2,2,1,2,2)$, then $\pi_{\boldsymbol{s}}$ is $\{\{1,4\},\{2,3,5,6\}\}$, and

we have $m_2(\boldsymbol{s}) = m_4(\boldsymbol{s}) = 1$ and $m_k(\boldsymbol{s}) = 0$ for all $k \notin \{2, 4\}$.

By linearity it suffices to prove the lemma for the case that $h(\boldsymbol{x}) = 1$ for $\boldsymbol{x} = \boldsymbol{s}$ and $h(\boldsymbol{x}) = 0$ otherwise. Clearly, the left-hand side of (4.7) equals 1. On the other hand, the sum

$$\sum_{\substack{\boldsymbol{t} \in \mathcal{E}_\alpha(n) \\ \boldsymbol{t} \prec \pi}} h(t)$$

is just the indicator function of the event $s \prec \pi$, so that we can restrict the outer summation on the right-hand side of (4.7) to the even partitions that are refinements of π_s. Therefore, the right-hand side of (4.7) equals

$$\prod_{k=1}^{\alpha} \left(\sum_{\substack{\pi \in \Pi_{2k} \\ \pi \text{ even}}} \prod_{B \in \pi} T\left(\tfrac{1}{2}|B|\right) \right)^{m_k(s)},$$

which again equals 1 by (4.8). □

Evaluation of the inner sums on the right-hand side of (4.7)

Next we evaluate the inner sums on the right-hand side of (4.7) for $h = h_{n,r}$. We first have to set some notation.

For a positive integer n and real x, we define the *generalised Eulerian numbers* to be

$$\left\langle {n \atop x} \right\rangle = \sum_{j=0}^{\lfloor x+1 \rfloor} (-1)^j \binom{n+1}{j} (x+1-j)^n. \tag{4.9}$$

Note that $\left\langle {n \atop x} \right\rangle$ is nonzero only for $x \in (-1, n)$. If x is integral, then $\left\langle {n \atop x} \right\rangle$ is an Eulerian number in the usual sense. We refer to the book [103] for the combinatorial significance of Eulerian numbers and to [130] for a natural interpretation of generalised Eulerian numbers in terms of splines.

We have the following result.

Lemma 4.3.4. *Let $\pi = \{B_1, \dots, B_\ell\} \in \Pi_{2\alpha}$ be an even partition with ℓ blocks. Write $N_i = |B_i|/2$ and $P_i = |\{x \in B_i : x > \alpha\}|$ for all i. If $r/n \to R$ as $n \to \infty$, then*

$$\lim_{n\to\infty} \frac{1}{n^{2\alpha}} \sum_{\substack{\boldsymbol{t} \in \mathcal{E}_\alpha(n) \\ \boldsymbol{t} \prec \pi}} h_{n,r}(\boldsymbol{t}) = \sum_{\substack{a_1,\dots,a_\ell \in \mathbb{Z} \\ a_1+\cdots+a_\ell = \alpha}} \prod_{i=1}^{\ell} \frac{1}{(2N_i-1)!} \left\langle {2N_i - 1 \atop 2R(N_i - P_i) + a_i - 1} \right\rangle.$$

To prove the lemma, we use the following asymptotic counting result, which follows from known results on the number of restricted integer compositions [38], [30], or, alternatively, from integration results over a simplex [44]. By $I[E]$ we denote the indicator function of an event E.

Lemma 4.3.5. *Let N be a positive integer and let M be real. Let (m_n) be a sequence of integers such that $m_n/n \to M$ as $n \to \infty$. Then*

$$\lim_{n\to\infty} \frac{1}{n^{N-1}} \sum_{0\le j_1,\dots,j_N<n} I\big[j_1+\cdots+j_N = m_n\big] = \frac{1}{(N-1)!}\left\langle {N-1 \atop M-1}\right\rangle.$$

Proof. It is well known (see [38, (11)] or [30, Example 33], for example) that

$$\sum_{0\le j_1,\dots,j_N<n} I\big[j_1+\cdots+j_N = m_n\big] = \sum_{j=0}^{N}(-1)^j \binom{N}{j}\binom{N+m_n-nj-1}{N-1}.$$

Since

$$\lim_{n\to\infty} \frac{1}{n^{N-1}}\binom{N+m_n-nj-1}{N-1} = \frac{1}{(N-1)!}\big(\max(0,M-j)\big)^{N-1},$$

the lemma follows from the definition (4.9) of the generalised Eulerian numbers. □

We now prove Lemma 4.3.4.

Proof of Lemma 4.3.4. Put

$$H_n = \sum_{\substack{\boldsymbol{t}\in\mathcal{E}_\alpha(n)\\ \boldsymbol{t}\prec\pi}} h_{n,r}(\boldsymbol{t}),$$

and let $\delta_k = -1$ for $k \le \alpha$ and $\delta_k = 1$ for $k > \alpha$. Since

$$h_{n,r}(t_1,\dots,t_{2\alpha}) = \sum_{\substack{0\le j_1,\dots,j_{2\alpha}<n\\ j_1+\cdots+j_\alpha = j_{\alpha+1}+\cdots+j_{2\alpha}}} \prod_{i=1}^{\ell}\prod_{k\in B_i} \epsilon_n\big(\delta_k t_k(j_k+r)\big),$$

we can rewrite H_n as

$$H_n = \sum_{\substack{0\le j_1,\dots,j_{2\alpha}<n\\ j_1+\cdots+j_\alpha = j_{\alpha+1}+\cdots+j_{2\alpha}}} \prod_{i=1}^{\ell}\sum_{t\in\mathbb{Z}/n\mathbb{Z}} \epsilon_n\Big(t\sum_{k\in B_i}\delta_k(j_k+r)\Big).$$

The product is either zero or equals n^ℓ and is nonzero exactly when there exist integers $a_1,\dots,a_\ell$ such that

$$\sum_{k\in B_i}\delta_k(j_k+r) = a_i n \tag{4.10}$$

for all $i \in \{1,\dots,\ell\}$. Hence,

$$H_n = n^\ell \sum_{\substack{0\le j_1,\dots,j_{2\alpha}<n\\ j_1+\cdots+j_\alpha = j_{\alpha+1}+\cdots+j_{2\alpha}}} \sum_{a_1,\dots,a_\ell\in\mathbb{Z}} \prod_{i=1}^{\ell} I\Big[\sum_{k\in B_i}\delta_k(j_k+r) = a_i n\Big].$$

Summing both sides of (4.10) over $i \in \{1, \dots, \ell\}$ gives

$$\sum_{k=1}^{\alpha} (j_{\alpha+k} - j_k) = n \sum_{i=1}^{\ell} a_i,$$

so that

$$H_n = n^{\ell} \sum_{\substack{a_1,\dots,a_\ell \in \mathbb{Z} \\ a_1+\cdots+a_\ell=0}} \sum_{0 \le j_1,\dots,j_{2\alpha} < n} \prod_{i=1}^{\ell} I\left[\sum_{k \in B_i} \delta_k(j_k + r) = a_i n \right].$$

The i-th factor within the inner sum depends only on $|B_i| = 2N_i$ of the summation variables in the inner sum, so that we can factor the inner sum as follows:

$$\prod_{i=1}^{\ell} \sum_{0 \le j_1,\dots,j_{2N_i} < n} I\left[\sum_{k=1}^{P_i} (j_k + r) - \sum_{k=P_i+1}^{2N_i} (j_k + r) = a_i n \right].$$

Replace j_k by $n - 1 - j_k$ for $k \in \{P_i + 1, \dots, 2N_i\}$ to see that this expression equals

$$\prod_{i=1}^{\ell} \sum_{0 \le j_1,\dots,j_{2N_i} < n} I\left[\sum_{k=1}^{2N_i} j_k = (2N_i - P_i)(n-1) + 2r(N_i - P_i) + a_i n \right].$$

Since $\sum_{i=1}^{\ell} (2N_i - 1) = 2\alpha - \ell$, we find from Lemma 4.3.5 that

$$\lim_{n\to\infty} \frac{H_n}{n^{2\alpha}} = \sum_{\substack{a_1,\dots,a_\ell \in \mathbb{Z} \\ a_1+\cdots+a_\ell=0}} \prod_{i=1}^{\ell} \frac{1}{(2N_i - 1)!} \left\langle \begin{matrix} 2N_i - 1 \\ 2N_i - P_i + 2R(N_i - P_i) + a_i - 1 \end{matrix} \right\rangle$$

since the outer sum is locally finite. The lemma follows after re-indexing and using $\sum_{i=1}^{\ell} (2N_i - P_i) = \alpha$. □

Main results

We now can prove our main results on the asymptotic $L^{2\alpha}$ norm of (shifted) Fekete polynomials.

Theorem 4.3.6. *Let α be a positive integer and, for each odd prime p, let f_p^r be a shifted Fekete polynomial corresponding to the Fekete polynomial of degree $p-1$. If $r/p \to R$ as $p \to \infty$, then*

$$\lim_{p\to\infty} \left(\frac{\|f_p^r\|_{2\alpha}}{\sqrt{p}} \right)^{2\alpha} = \sum_{\substack{\pi \in \Pi_{2\alpha} \\ \pi \text{ even}}} \sum_{\substack{a_1,\dots,a_\ell \in \mathbb{Z} \\ a_1+\cdots+a_\ell=\alpha}} \prod_{i=1}^{\ell} \frac{T(N_i)}{(2N_i - 1)!} \left\langle \begin{matrix} 2N_i - 1 \\ 2R(N_i - P_i) + a_i - 1 \end{matrix} \right\rangle,$$

where $\pi = \{B_1, \dots, B_\ell\}$, $N_i = |B_i|/2$, and $P_i = |\{x \in B_i : x > \alpha\}|$ for all i.

Proof. The proof is a combination of Lemmas 4.3.1, 4.3.3, and 4.3.4. From Lemma 4.3.1 we find that

$$\lim_{p\to\infty}\left(\frac{\|f_p^r\|_{2\alpha}}{\sqrt{p}}\right)^{2\alpha} = \lim_{p\to\infty}\frac{1}{p^{2\alpha}}\sum_{\boldsymbol{t}\in\mathcal{E}_\alpha(p)} h_{p,r}(\boldsymbol{t}).$$

By Lemma 4.3.3 with $h = h_{p,r}$ we then have

$$\lim_{p\to\infty}\left(\frac{\|f_p^r\|_{2\alpha}}{\sqrt{p}}\right)^{2\alpha} = \sum_{\substack{\pi\in\Pi_{2\alpha}\\ \pi \text{ even}}}\lim_{p\to\infty}\frac{1}{p^{2\alpha}}\sum_{\substack{\boldsymbol{t}\in\mathcal{E}_\alpha(p)\\ \boldsymbol{t}\prec\pi}} h_{p,r}(\boldsymbol{t})\prod_{B\in\pi} T\big(\tfrac{1}{2}|B|\big),$$

so that Lemma 4.3.3 completes the proof. □

It follows from Theorem 4.3.6 that, for each positive integer α, there exists a function $\psi_\alpha\colon \mathbb{R}\to\mathbb{R}$ such that, if $r/p\to R$, then

$$\lim_{p\to\infty}\left(\frac{\|f_p^r\|_{2\alpha}}{\sqrt{p}}\right)^{2\alpha} = \psi_\alpha(R). \tag{4.11}$$

Since the generalised Eulerian numbers $\left\langle {n \atop x} \right\rangle$ are continuous piecewise polynomial functions of x, the functions ψ_α are also continuous piecewise polynomial functions. It follows from Theorem 4.3.6 that $\psi_\alpha(x+1/2) = \psi_\alpha(x)$ for all $x\in\mathbb{R}$. It can also be shown that $\psi_\alpha(-x) = \psi_\alpha(x)$ for all $x\in\mathbb{R}$, so that $\psi_\alpha(1/4+x) = \psi_\alpha(1/4-x)$ for all $x\in\mathbb{R}$. It is therefore sufficient to know $\psi_\alpha(x)$ for $x\in[0,1/4]$. We have for example, for $x\in[0,1/4]$,

$$\psi_2(x) = \frac{7}{6} + \frac{1}{2}(4x-1)^2,$$

in accordance with (4.2),

$$\psi_3(x) = \frac{31}{20} + \frac{3}{4}(4x-1)^2(16x^2-8x+3),$$

and

$$\psi_4(x) = \frac{653}{280} + \frac{1}{72}(4x-1)^2(60416x^4-52736x^3+20208x^2-4216x+625).$$

In general, ψ_α is a piecewise polynomial function on $[0,1/4]$. For $\alpha\in\{2,3,4\}$ it is readily verified that the function ψ_α attains its global minimum at a unique point in $[0,1/4]$, namely at $1/4$. We could not prove that this is true for all $\alpha>1$, but conjecture that this is the case. For convenience, we provide the first nine values of $\psi_\alpha(1/4)$ (starting with $\alpha=1$):

$$1,\ \frac{7}{6},\ \frac{31}{20},\ \frac{653}{280},\ \frac{71735}{18144},\ \frac{24880549}{3326400},\ \frac{72207143}{4633200},\ \frac{960901090937}{27243216000},\ \frac{1343039345489}{15682867200}. \tag{4.12}$$

The sequence of the numerators of these values now appears in [1] as `A280038`, and the

sequence of the denominators appears as A280039.

We now investigate the $L^{2\alpha}$ norm of (unshifted) Fekete polynomials in detail. In that case, we have the following result, which is just the case $R = 0$ of Theorem 4.3.6.

Theorem 4.3.7. *Let α be a positive integer and, for each odd prime p, let f_p be the Fekete polynomial of degree $p-1$. Then*

$$\lim_{p\to\infty}\left(\frac{\|f_p\|_{2\alpha}}{\sqrt{p}}\right)^{2\alpha} = \sum_{\substack{\pi\in\Pi_{2\alpha}\\ \pi \text{ even}}}\sum_{\substack{a_1,\dots,a_\ell\in\mathbb{Z}\\ a_1+\cdots+a_\ell=\alpha}}\prod_{i=1}^{\ell}\frac{T(N_i)}{(2N_i-1)!}\left\langle{2N_i-1\atop a_i-1}\right\rangle,$$

where $\pi = \{B_1,\dots,B_\ell\}$ and $N_i = |B_i|/2$ for all i.

The following corollary provides an efficient way to compute the limiting values in Theorem 4.3.7.

Corollary 4.3.8. *Set $F(0,0) = 1$ and, for $1 \le m \le 2k-1$, define the numbers $F(k,m)$ recursively by*

$$F(k,m) = \sum_{j=1}^{k}\binom{2k-1}{2j-1}\frac{T(j)}{(2j-1)!}\sum_{i}\left\langle{2j-1\atop i-1}\right\rangle F(k-j,m-i),$$

where the inner sum is over all i such that $F(k-j,m-i)$ is defined. Let α be a positive integer and, for each odd prime p, let f_p be the Fekete polynomial of degree $p-1$. Then

$$\lim_{p\to\infty}\left(\frac{\|f_p\|_{2\alpha}}{\sqrt{p}}\right)^{2\alpha} = F(\alpha,\alpha).$$

Proof. Write

$$E_N(x) = \sum_{a=1}^{2N-1}\left\langle{2N-1\atop a-1}\right\rangle x^a,$$

which is known (after dividing by x) as an *Eulerian polynomial*. Letting $N_1,\dots,N_\ell$ be positive integers such that $N_1+\cdots+N_\ell = k$, we have

$$\prod_{i=1}^{\ell}E_{N_i}(x) = \sum_{m=\ell}^{2k-\ell}x^m\sum_{\substack{a_1,\dots,a_\ell\in\mathbb{Z}\\ a_1+\cdots+a_\ell=m}}\prod_{i=1}^{\ell}\left\langle{2N_i-1\atop a_i-1}\right\rangle.$$

Define polynomials $F_k(x)$ by $F_0(x) = 1$, $F_k(x) = 0$ for odd k, and

$$F_{2k}(x) = \sum_{\substack{\pi\in\Pi_{2k}\\ \pi \text{ even}}}\prod_{i=1}^{\ell}\frac{T(N_i)\,E_{N_i}(x)}{(2N_i-1)!}\quad\text{for } k\ge 1, \tag{4.13}$$

where $\pi = \{B_1,\dots,B_\ell\}$ and $N_i = |B_i|/2$. Then $F_{2k}(x)$ is a polynomial of degree $2k-1$

with $F_{2k}(0) = 0$ for $k \geq 1$. Therefore, for suitable $\Phi(k, m)$, we can write

$$F_{2k}(x) = \sum_{m=1}^{2k-1} \Phi(k, m)\, x^m \quad \text{for } k \geq 1.$$

It is readily verified that Theorem 4.3.7 is equivalent to

$$\lim_{p\to\infty} \left(\frac{\|f_p\|_{2\alpha}}{\sqrt{p}} \right)^{2\alpha} = \Phi(\alpha, \alpha),$$

so that it remains to show that $\Phi(k, m) = F(k, m)$. Use $F_0(x) = 1$ and apply Lemma 4.3.2 to (4.13) to find that

$$F_{2k}(x) = \sum_{j=1}^{k} \binom{2k-1}{2j-1} \frac{T(j)E_j(x)}{(2j-1)!}\, F_{2k-2j}(x) \quad \text{for } k \geq 1.$$

With $\Phi(0, 0) = 1$ (which equals $F_0(x)$), this is equivalent to the recursive definition of the numbers $F(k, m)$. □

For $k \geq 1$, the numbers $(2k-1)!\, F(k, m)$ identified in Corollary 4.3.8 define a triangular array of integers, which now appears in [1] as `A268481`. Its first four rows are given by:

$$\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & -2 & 10 & -2 & & \\
 & 16 & -184 & 456 & -184 & 16 & \\
-272 & 5776 & -30736 & 55504 & -30736 & 5776 & -272
\end{array}$$

The first and last entry in row k equals $T(k)$ and the central entry in row k divided by $(2k-1)!$ equals the limiting value in Corollary 4.3.8 for $k = \alpha$. The first nine of these limiting values are:

$$1,\ \frac{5}{3},\ \frac{19}{5},\ \frac{3469}{315},\ \frac{21565}{567},\ \frac{7760593}{51975},\ \frac{12478099}{19305},\ \frac{643983856759}{212837625},\ \frac{32151685807}{2127125}. \tag{4.14}$$

The sequence of the numerators of these values now appears in [1] as `A280034`, and the sequence of the denominators appears as `A280035`.

It should be noted that we are not aware of a computationally efficient version of Theorem 4.3.6 in a spirit similar to Corollary 4.3.8.

4.4 Galois polynomials

In this section we prove our main on the $L^{2\alpha}$ norm of Galois polynomials.

We begin with setting some notation. A tuple $(t_1, t_2, \ldots, t_{2\alpha})$ is an *abelian square* if there exists a permutation σ of $\{1, 2, \ldots, \alpha\}$ such that $t_{\sigma(k)} = t_{\alpha+k}$ for all $k \in \{1, 2, \ldots, \alpha\}$,

so that the second half of the tuple is a permutation of the first half. Notice that each abelian square is an even tuple. For example $(2,1,3,1,2,3)$ is an abelian square, whereas the even tuple $(2,1,1,3,2,3)$ is no abelian square. Let $\mathcal{A}_\alpha(n)$ be the set of abelian squares in $(\mathbb{Z}/n\mathbb{Z})^{2\alpha}$.

We begin with the following lemma, which is an analogue of Lemma 4.3.1.

Lemma 4.4.1. *Let α be a positive integer and, for each Mersenne number n, let g_n be a Galois polynomial of degree $n-1$. Then*

$$\lim_{n\to\infty}\left(\frac{\|g_n\|_{2\alpha}}{\sqrt{n}}\right)^{2\alpha} = \lim_{n\to\infty}\frac{1}{n^{2\alpha}}\sum_{\boldsymbol{t}\in\mathcal{A}_\alpha(n)} h_{n,0}(\boldsymbol{t}), \tag{4.15}$$

provided that one of the limits exists.

Proof. For $\boldsymbol{t}\in(\mathbb{Z}/n\mathbb{Z})^{2\alpha}$, let $J_n(\boldsymbol{t})$ be the indicator function that equals one if $\boldsymbol{t}$ is an abelian square and is zero otherwise. From Proposition 4.2.1 we find that

$$\left(\frac{\|g_n\|_{2\alpha}}{\sqrt{n}}\right)^{2\alpha} = \frac{1}{n^{2\alpha}}\sum_{\boldsymbol{t}\in(\mathbb{Z}/n\mathbb{Z})^{2\alpha}} J_n(\boldsymbol{t})h_{n,0}(\boldsymbol{t}) + \frac{1}{n^{2\alpha}}\sum_{\boldsymbol{t}\in(\mathbb{Z}/n\mathbb{Z})^{2\alpha}}\big(L_{g_n}(\boldsymbol{t})-J_n(\boldsymbol{t})\big)h_{n,0}(\boldsymbol{t}).$$

We show that the second expression on the right-hand side tends to zero, which will prove the lemma. Write $s=n+1$, so that s is a power of two. By definition, a Galois polynomial of degree $n-1$ can be written as

$$g_n(z)=\sum_{j=0}^{n-1}\psi(\theta^j)z^j,$$

where ψ is an additive character of $\mathbb{F}_s$ and θ is a primitive element of $\mathbb{F}_s$. Letting χ be the multiplicative character of $\mathbb{F}_s$ given by $\chi(\theta)=\epsilon_n(1)$, we see that $g_n(\epsilon_n(k))$ equals the canonical Gauss sum $G(\chi^k)$ for all $k\in\mathbb{Z}/n\mathbb{Z}$. Therefore,

$$L_{g_n}(t_1,\dots,t_{2\alpha}) = \frac{1}{n^{\alpha+1}}\sum_{m\in\mathbb{Z}/n\mathbb{Z}}\prod_{k=1}^{\alpha} G(\chi^{m+t_k})\overline{G(\chi^{m+t_{\alpha+k}})}.$$

Since $|G(\chi^m)|^2$ equals 1 if χ^m is trivial and equals $n+1$ otherwise by Lemma 2.2.3 (ii) and (iv), we find that $|L_{g_n}(t_1,\dots,t_{2\alpha})-1| = O(n^{-1})$ if $(t_1,\dots,t_{2\alpha})$ is an abelian square. On the other hand, if $(t_1,\dots,t_{2\alpha})$ is not an abelian square, then we have

$$|L_{g_n}(t_1,\dots,t_{2\alpha})| \le \frac{\alpha}{n^{\alpha+1}}\,(n+1)^{\alpha+1/2}$$

by Lemma 2.2.7. Therefore, by the triangle inequality,

$$\frac{1}{n^{2\alpha}}\left|\sum_{\boldsymbol{t}\in(\mathbb{Z}/n\mathbb{Z})^{2\alpha}}\big(L_{g_n}(\boldsymbol{t})-J_n(\boldsymbol{t})\big)h_{n,0}(\boldsymbol{t})\right| = O(n^{-2\alpha-1/2})\sum_{\boldsymbol{t}\in(\mathbb{Z}/n\mathbb{Z})^{2\alpha}}|h_{n,0}(\boldsymbol{t})|,$$

which tends to zero as $n \to \infty$ by Lemma 3.2.3, as required. □

Evaluation of the right-hand side of (4.15)

We proceed similarly as for Fekete polynomials and seek an asymptotic evaluation of (4.15). In order to do so, we need some more notation.

Let $J_0(z)$ be the zeroth Bessel function of the first kind and define the numbers $C(k)$ via the Maclaurin series

$$\log\big(J_0(2\sqrt{z})\big) = \sum_{k=1}^{\infty} \frac{(-1)^k\, C(k)}{(k!)^2}\, z^k. \tag{4.16}$$

We call these numbers the *signed Carlitz numbers*. The corresponding unsigned numbers $|C(k)| = (-1)^{k+1}C(k)$ have been extensively studied by Carlitz [19] and appear in [1] as

$$\texttt{A002190} = [0, 1, 1, 4, 33, 456, 9460, \dots],$$

which starts at $k = 0$ with $C(0) = 0$. The numbers $C(k)$ can be recursively determined via

$$C(k) = 1 - \sum_{j=1}^{k-1} \binom{k}{j}\binom{k-1}{j-1} C(j) \quad \text{for } k \geq 1.$$

This can be deduced from Lemma 4.3.2, in which we choose $f\colon \mathbb{N} \to \mathbb{R}$ such that $F(z) = \log\big(J_0(2\sqrt{z})\big)$, which means that $f(k) = (-1)^k C(k)/k!$. Note that then $g(k) = (-1)^k/k!$ since $G(z) = J_0(2\sqrt{z})$.

The following lemma is an analogue of Lemma 4.3.3. Recall the definition of the relation $u \prec \pi$, which is given before Lemma 4.3.3.

Lemma 4.4.2. *Let $h\colon \mathcal{A}_\alpha(n) \to \mathbb{C}$ be a function that depends only on the first α entries of its input and let $C(k)$ be the k-th signed Carlitz number. Then*

$$\sum_{\boldsymbol{t} \in \mathcal{A}_\alpha(n)} h(\boldsymbol{t}) = \alpha! \sum_{\pi \in \Pi_\alpha} \sum_{\substack{\boldsymbol{u} \in (\mathbb{Z}/n\mathbb{Z})^\alpha \\ \boldsymbol{u} \prec \pi}} h(\boldsymbol{u}|\boldsymbol{u}) \prod_{B \in \pi} \frac{C(|B|)}{|B|!}, \tag{4.17}$$

where $\boldsymbol{u}|\boldsymbol{u}$ is the (2α)-tuple with the first and the second half equal to $\boldsymbol{u}$.

Proof. Take $F(z) = \log\big(J_0(2\sqrt{z})\big)$ in Lemma 4.3.2, so that $G(z)$ equals

$$J_0(2\sqrt{z}) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(k!)^2} z^k.$$

Use (4.16) to find from Lemma 4.3.2 that

$$\sum_{\pi\in\Pi_k}\prod_{B\in\pi}\frac{(-1)^{|B|}C(|B|)}{|B|!}=\frac{(-1)^k}{k!}\quad\text{for each } k\geq 1,$$

or equivalently

$$\sum_{\pi\in\Pi_k}\prod_{B\in\pi}\frac{C(|B|)}{|B|!}=\frac{1}{k!}\quad\text{for each } k\geq 1. \tag{4.18}$$

Let $\boldsymbol{v}\in(\mathbb{Z}/n\mathbb{Z})^\alpha$, and let $\pi_{\boldsymbol{v}}\in\Pi_\alpha$ be the coarsest partition of $\{1,2,\ldots,\alpha\}$ with the property $\boldsymbol{v}\prec\pi_{\boldsymbol{v}}$. As in the proof of Lemma 4.3.3, define $m_k(\boldsymbol{v})$ to be the number of blocks B in $\pi_{\boldsymbol{v}}$ such that $|B|=k$. Let V be the set of abelian squares in $(\mathbb{Z}/n\mathbb{Z})^{2\alpha}$ whose first α entries equal those of $\boldsymbol{v}$.

By linearity, it suffices to prove the lemma for the case that $h(\boldsymbol{x})=1$ for $\boldsymbol{x}\in V$ and $h(\boldsymbol{x})=0$ otherwise. Then the left-hand side of (4.17) equals

$$|V|=\frac{\alpha!}{\prod_{k=1}^{\alpha}(k!)^{m_k(\boldsymbol{v})}}. \tag{4.19}$$

On the other hand, the right-hand side of (4.17) equals

$$\alpha!\prod_{k=1}^{\alpha}\left(\sum_{\pi\in\Pi_k}\prod_{B\in\pi}\frac{C(|B|)}{|B|!}\right)^{m_k(\boldsymbol{v})},$$

which by (4.18) equals (4.19) again. □

Evaluation of the inner sums of the right-hand side of (4.17)

Next we evaluate the inner sums of the right-hand side of (4.17) for $h=h_{n,0}$.

Lemma 4.4.3. *Let $\pi=\{B_1,\ldots,B_\ell\}\in\Pi_\alpha$ be a partition with ℓ blocks and write $N_i=|B_i|$ for all i. Then*

$$\lim_{n\to\infty}\frac{1}{n^{2\alpha}}\sum_{\substack{\boldsymbol{u}\in(\mathbb{Z}/n\mathbb{Z})^\alpha\\ \boldsymbol{u}\prec\pi}}h_{n,0}(\boldsymbol{u}|\boldsymbol{u})=\sum_{\substack{a_1,\ldots,a_\ell\in\mathbb{Z}\\ a_1+\cdots+a_\ell=\alpha}}\prod_{i=1}^{\ell}\frac{1}{(2N_i-1)!}\left\langle{2N_i-1\atop a_i-1}\right\rangle,$$

where $\boldsymbol{u}|\boldsymbol{u}$ is the (2α)-tuple with the first and the second half equal to $\boldsymbol{u}$.

Proof. The proof is similar to that of Lemma 4.3.4, and so is presented in slightly less detail. Put

$$H_n=\sum_{\substack{\boldsymbol{u}\in(\mathbb{Z}/n\mathbb{Z})^\alpha\\ \boldsymbol{u}\prec\pi}}h_{n,0}(\boldsymbol{u}|\boldsymbol{u}),$$

which we can rewrite as

$$H_n = \sum_{\substack{0\le j_1,\dots,j_{2\alpha}<n \\ j_1+\cdots+j_\alpha = j_{\alpha+1}+\cdots+j_{2\alpha}}} \prod_{i=1}^{\ell} \sum_{u\in\mathbb{Z}/n\mathbb{Z}} \epsilon_n\Big(u\sum_{k\in B_i}(j_{\alpha+k}-j_k)\Big).$$

The product is either zero or equals n^ℓ and is nonzero exactly when there exist integers $a_1,\dots,a_\ell$ such that

$$\sum_{k\in B_i}(j_{\alpha+k}-j_k) = a_i n \tag{4.20}$$

for all $i\in\{1,\dots,\ell\}$. Hence

$$H_n = n^\ell \sum_{\substack{0\le j_1,\dots,j_{2\alpha}<n \\ j_1+\cdots+j_\alpha = j_{\alpha+1}+\cdots+j_{2\alpha}}} \sum_{a_1,\dots,a_\ell\in\mathbb{Z}} \prod_{i=1}^{\ell} I\Big[\sum_{k\in B_i}(j_{\alpha+k}-j_k) = a_i n\Big].$$

Summing both sides of (4.20) over $i\in\{1,\dots,\ell\}$ gives

$$\sum_{k=1}^{\alpha}(j_{\alpha+k}-j_k) = n\sum_{i=1}^{\ell} a_i,$$

so that

$$H_n = n^\ell \sum_{\substack{a_1,\dots,a_\ell\in\mathbb{Z} \\ a_1+\cdots+a_\ell=0}} \sum_{0\le j_1,\dots,j_{2\alpha}<n} \prod_{i=1}^{\ell} I\Big[\sum_{k\in B_i}(j_{\alpha+k}-j_k) = a_i n\Big]$$

or equivalently

$$H_n = n^\ell \sum_{\substack{a_1,\dots,a_\ell\in\mathbb{Z} \\ a_1+\cdots+a_\ell=0}} \sum_{0\le j_1,\dots,j_{2\alpha}<n} \prod_{i=1}^{\ell} I\Big[\sum_{k\in B_i}(j_{\alpha+k}+j_k) = a_i n + N_i(n-1)\Big].$$

We can factor the inner sum as follows:

$$\prod_{i=1}^{\ell} \sum_{0\le j_1,\dots,j_{2N_i}<n} I\Big[\sum_{k=1}^{2N_i} j_k = a_i n + N_i(n-1)\Big].$$

Since $\sum_{i=1}^{\ell}(2N_i-1) = 2\alpha-\ell$, we find from Lemma 4.3.5 that

$$\lim_{n\to\infty}\frac{H_n}{n^{2\alpha}} = \sum_{\substack{a_1,\dots,a_\ell\in\mathbb{Z} \\ a_1+\cdots+a_\ell=0}} \prod_{i=1}^{\ell} \frac{1}{(2N_i-1)!}\left\langle \begin{matrix} 2N_i-1 \\ N_i+a_i-1 \end{matrix}\right\rangle$$

since the outer sum is locally finite. The lemma follows after re-indexing the summation. □

Main result

We have the following result on the asymptotic $L^{2\alpha}$ norm of Galois polynomials.

Theorem 4.4.4. *Let α be a positive integer and, for each Mersenne number n, let g_n be a Galois polynomial of degree $n-1$. Then*

$$\lim_{n\to\infty}\left(\frac{\|g_n\|_{2\alpha}}{\sqrt{n}}\right)^{2\alpha}=\sum_{\pi\in\Pi_\alpha}\binom{\alpha}{N_1,\dots,N_\ell}\sum_{\substack{a_1,\dots,a_\ell\in\mathbb{Z}\\ a_1+\cdots+a_\ell=\alpha}}\prod_{i=1}^{\ell}\frac{C(N_i)}{(2N_i-1)!}\left\langle{2N_i-1\atop a_i-1}\right\rangle,$$

where $\pi=\{B_1,\dots,B_\ell\}$ and $N_i=|B_i|$ for all i.

Proof. The proof is a combination of Lemmas 4.4.1, 4.4.2, and 4.4.3. From Lemma 4.4.1 we find that

$$\lim_{n\to\infty}\left(\frac{\|g_n\|_{2\alpha}}{\sqrt{n}}\right)^{2\alpha}=\lim_{n\to\infty}\frac{1}{n^{2\alpha}}\sum_{\boldsymbol{t}\in\mathcal{A}_\alpha(n)}h_{n,0}(\boldsymbol{t}).$$

By Lemma 4.4.2 with $h=h_{n,0}$ (upon noting that $h_{n,0}$ has the required property), we have

$$\begin{aligned}\lim_{n\to\infty}\left(\frac{\|g_n\|_{2\alpha}}{\sqrt{n}}\right)^{2\alpha}&=\alpha!\sum_{\pi\in\Pi_\alpha}\lim_{n\to\infty}\frac{1}{n^{2\alpha}}\sum_{\substack{\boldsymbol{u}\in(\mathbb{Z}/n\mathbb{Z})^\alpha\\ \boldsymbol{u}\prec\pi}}h_{n,0}(\boldsymbol{u}|\boldsymbol{u})\prod_{i=1}^{\ell}\frac{C(N_i)}{N_i!}\\&=\sum_{\pi\in\Pi_\alpha}\binom{\alpha}{N_1,\dots,N_\ell}\lim_{n\to\infty}\frac{1}{n^{2\alpha}}\sum_{\substack{\boldsymbol{u}\in(\mathbb{Z}/n\mathbb{Z})^\alpha\\ \boldsymbol{u}\prec\pi}}h_{n,0}(\boldsymbol{u}|\boldsymbol{u})\prod_{i=1}^{\ell}C(N_i),\end{aligned}$$

so that Lemma 4.4.3 completes the proof. □

We have the following counterpart of Corollary 4.3.8 for Galois polynomials.

Corollary 4.4.5. *Set $G(0,0)=1$ and, for $1\le m\le 2k-1$, define the numbers $G(k,m)$ recursively by*

$$G(k,m)=\sum_{j=1}^{k}\binom{k}{j}\binom{k-1}{j-1}\frac{C(j)}{(2j-1)!}\sum_{i}\left\langle{2j-1\atop i-1}\right\rangle G(k-j,m-i),$$

where the inner sum is over all i such that $G(k-j,m-i)$ is defined. Let α be a positive integer and, for each Mersenne number n, let g_n be a Galois polynomial of degree $n-1$. Then

$$\lim_{n\to\infty}\left(\frac{\|g_n\|_{2\alpha}}{\sqrt{n}}\right)^{2\alpha}=G(\alpha,\alpha).$$

Proof. The proof is again broadly similar to that of Corollary 4.3.8. Write

$$E_N(x)=\sum_{a=1}^{2N-1}\left\langle{2N-1\atop a-1}\right\rangle x^a$$

and define polynomials $G_k(x)$ by $G_0(x) = 1$, and

$$\frac{G_k(x)}{k!} = \sum_{\pi \in \Pi_k} \prod_{i=1}^{\ell} \frac{C(N_i)\, A_{N_i}(x)}{(2N_i - 1)! N_i!} \quad \text{for } k \geq 1, \tag{4.21}$$

where $\pi = \{B_1, \ldots, B_\ell\}$ and $N_i = |B_i|$. Then $G_k(x)$ is a polynomial of degree $2k-1$ with $G_k(0) = 0$ for $k \geq 1$. Therefore, for suitable $\Phi(k, m)$, we can write

$$G_k(x) = \sum_{m=1}^{2k-1} \Phi(k, m)\, x^m \quad \text{for } k \geq 1.$$

It is readily verified that Theorem 4.4.4 is equivalent to

$$\lim_{n \to \infty} \left(\frac{\|g_n\|_{2\alpha}}{\sqrt{n}} \right)^{2\alpha} = \Phi(\alpha, \alpha),$$

so that it remains to show that $\Phi(k, m) = G(k, m)$. Use $G_0(x) = 1$ and apply Lemma 4.3.2 to (4.21) to find that

$$\frac{G_k(x)}{k!} = \sum_{j=1}^{k} \binom{k-1}{j-1} \frac{C(j) A_j(x)}{(2j-1)!\, j!} \frac{G_{k-j}(x)}{(k-j)!} \quad \text{for } k \geq 1,$$

or equivalently

$$G_k(x) = \sum_{j=1}^{k} \binom{k}{j} \binom{k-1}{j-1} \frac{C(j) A_j(x)}{(2j-1)!} G_{k-j}(x) \quad \text{for } k \geq 1.$$

With $\Phi(0, 0) = 1$ (which equals $G_0(x)$), this is equivalent to the recursive definition of the numbers $G(k, m)$ given in Corollary 4.4.5. □

For $k \geq 1$, the numbers $(2k-1)!\, G(k, m)$ identified in Corollary 4.4.5 also define a triangular array of integers, which now appears in [1] as `A268482`. Its first four rows are given by:

$$\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & -1 & 8 & -1 & & \\
 & 4 & -76 & 264 & -76 & 4 & \\
-33 & 1248 & -9735 & 22080 & -9735 & 1248 & -33
\end{array}$$

The first and last entry in row k equals $C(k)$ and the central entry in row k divided by $(2k-1)!$ equals the limiting value in Corollary 4.4.5 for $k = \alpha$. The first nine of these limiting values are:

$$1, \frac{4}{3}, \frac{11}{5}, \frac{92}{21}, \frac{15481}{1512}, \frac{411913}{15120}, \frac{2482927}{30888}, \frac{4181926481}{16216200}, \frac{10431687390203}{11762150400}. \tag{4.22}$$

The sequence of the numerators of these values now appears in [1] as A280036, and the sequence of the denominators appears as A280037.

We note that it is also possible to define shifted Galois polynomials by cyclically permuting the coefficients of a Galois polynomial. However, every such polynomial is again a Galois polynomial.

4.5 Conclusion and open problems

Until 2017, there was no known nontrivial specific family of Littlewood polynomials for which we can determine the asymptotic behaviour of its L^α norm for infinitely many α. In this chapter we considered the $L^{2\alpha}$ norm of (shifted) Fekete and Galois polynomials when α is a positive integer.

In Theorem 4.3.7 and Corollary 4.3.8 we determined explicit and recursive formulas for the limit of the ratio of $L^{2\alpha}$ and L^2 norm of Fekete polynomials as their degree tends to infinity when α is a positive integer. We listed the first few of these limiting values in (4.14). The sequences of the numerators and denominators of these limits appear now in [1] as A280034 and A280035, respectively. A triangular array of integers that can be deduced from Corollary 4.3.8 now appears in [1] as A268481.

We also obtained similar results for Galois polynomials in Theorem 4.4.4 and Corollary 4.4.5. We listed the first few limiting normalised $L^{2\alpha}$ norms of Galois polynomials in (4.22). The sequences of the numerators and denominators of these limits appear now in [1] as A280036 and A280037, respectively. A triangular array of integers that can be deduced from Corollary 4.4.5 now appears in [1] as A268482.

We also determined the limit of the ratio of $L^{2\alpha}$ and L^2 norm of shifted Fekete polynomials as their degree tends to infinity in Theorem 4.3.6. Of particular interest are quarter rotated Fekete polynomials, by which we mean the polynomials that are obtained by rotating the coefficient sequences of the corresponding Fekete polynomials by (approximately) one quarter. We conjecture that they have the smallest asymptotic normalised $L^{2\alpha}$ norm among all shifted Fekete polynomials for all positive integers α. We listed the first few limiting normalised $L^{2\alpha}$ norms of quarter rotated Fekete polynomials in (4.12). The sequences of the numerators and denominators of these limits appear now in [1] as A280038 and A280039, respectively

We note that our methods can also be used to establish similar results for polynomials obtained by periodically appending or truncating monomials in Fekete or Galois polynomials, and they also apply to other families of Littlewood polynomials whose coefficient sequences come from difference sets, as considered in Chapter 3.

In Figure 4.1 we see for $\alpha \in \{1, 2, \ldots, 10\}$ the limits of the ratio of $L^{2\alpha}$ and L^2 norm of random Littlewood polynomials, (quarter rotated) Fekete polynomials, Galois polynomials, and Shapiro polynomials, respectively, as their degree tends to infinity. From Theorem 1.6.6 we already know that, for integer $\alpha > 1$, Shapiro polynomials have smaller asymptotic

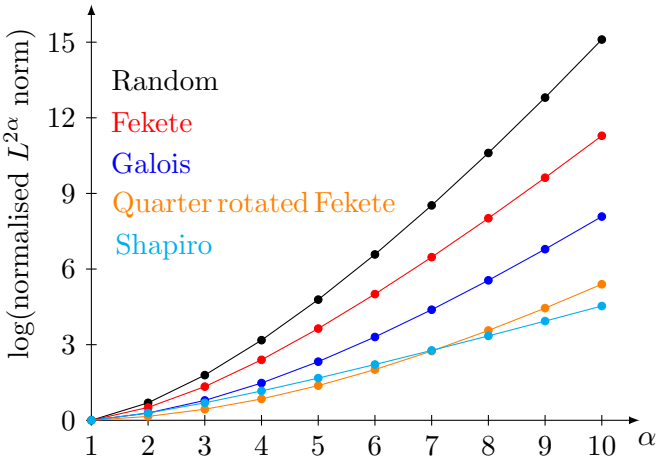

Figure 4.1: Asymptotic normalised $L^{2\alpha}$ norms of random Littlewood polynomials, (quarter rotated) Fekete polynomials, Galois polynomials, and Shapiro polynomials for $\alpha \in \{1, 2, \ldots, 10\}$.

normalised $L^{2\alpha}$ norm than random Littlewood polynomials (which is $\alpha!$ by Theorem 1.6.5). This also seems to hold for (rotated) Fekete and Galois polynomials. Furthermore, when $\alpha \leq 7$, the shifted Fekete polynomials have the smallest asymptotic $L^{2\alpha}$ norm, but for larger values of α it seems that Shapiro polynomials are those with smallest asymptotic $L^{2\alpha}$ norm. We conclude with a list of open problems concerning the L^α norm of Littlewood polynomials.

- Find a computationally efficient version of Theorem 4.3.6.
- Prove that the function ψ_α defined in (4.11) attains its global minimum at $1/4$ for all positive integers α.
- Simplify the expressions in Theorems 4.3.7, 4.3.6, and 4.4.4.

  The obtained limiting expressions seem still too complicated. In order to learn more on the behaviour of the L^α norms of Fekete and Galois polynomials, it seems that we need simplified expressions.
- Prove that, for integer $\alpha > 1$, (rotated) Fekete and Galois polynomials have smaller asymptotic normalised $L^{2\alpha}$ norm than random Littlewood polynomials.
- Find explicit expressions for the normalised L^α norm of Fekete and Galois polynomials for all real $\alpha \geq 1$.
- Can our methods shed light on Montgomery's conjecture mentioned at the beginning of this chapter?
- Determine the normalised L^α norm of other nontrivial families of Littlewood polynomials.

Promising candidates are given by the Littlewood polynomials whose coefficient sequences come from (almost) difference sets or arise from cyclotomy, as considered in Chapter 3.

- Prove or disprove any of the old Conjectures 1.6.1, 1.6.2, or 1.6.3.

  This is arguably a very challenging problem. We just included it for completeness.

Chapter 5

Galois sequences with large peak sidelobe level

5.1 Introduction and chapter overview

Recall from Chapter 1 that the *peak sidelobe level* of a binary sequence A of length $n > 1$ is

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

It is known that the peak sidelobe level of almost almost all binary sequences grows like $\sqrt{2n \log n}$ (see Theorem 1.4.2 for a more precise statement). On the other hand, there is only one known *specific* family of binary sequences whose peak sidelobe level grows with order $\sqrt{n \log n}$. This family was constructed by Schmidt (see Construction 1.4.3 and Theorem 1.4.5) using techniques from probabilistic combinatorics. Therefore, one of the most important and challenging problems concerning the peak sidelobe level is to find a family of binary sequences of length n whose peak sidelobe level grows slower than $c\sqrt{n \log n}$ for each constant $c > 0$ (see also Problem 1.5).

Galois sequences seem very promising to attack this problem. Indeed, numerical investigations of Dmitriev and Jedwab [28] lead to the following conjecture.

Conjecture 5.1.1 ([113])**.** *The peak sidelobe level of Galois sequences of length n grows like $O(\sqrt{n} \log \log n)$.*

Therefore, if Conjecture 5.1.1 is true, then the peak sidelobe level of Galois sequences grows more slowly than that of a typical binary sequence given in Theorem 1.4.2.

Even more striking observations where made by considering random Galois sequences [28], which led Schmidt [113, Conjecture 3.4.9] to state the following conjecture. Recall that there are exactly $n\,\varphi(n)/m$ Galois sequences of length $n = 2^m - 1$, where φ is Euler's totient function.

Conjecture 5.1.2 ([113])**.** *Let n take values in the set of Mersenne numbers. Let A_n be drawn uniformly at random from the set of Galois sequences of length n. Define*

$$W(A_n) = \max_{0 \leq r < n} \mathrm{M}(A_n^{r,n})$$

to be the maximum peak sidelobe level over all cyclic shifts of A_n. Then the limit

$$\lim_{n \to \infty} \frac{\mathrm{E}\left(W(A_n)\right)}{\sqrt{n}}$$

exists and is finite.

Combining Corollary 3.4.5 with Corollary 1.5.5 (ii), we conclude that the peak sidelobe level of Galois sequences grows at least with order $\sqrt{n}$. Therefore, the correctness of Conjecture 5.1.2 would imply that the peak sidelobe level of almost all Galois sequences of length n grows like $O(\sqrt{n})$. In particular, there would exist a family of Galois sequences whose peak sidelobe level grows like $O(\sqrt{n})$. Indeed, the claim that the peak sidelobe level of Galois sequences grows like $O(\sqrt{n})$ appears frequently in the radar literature (see [63, Section 3] for a list of references). However, the best known upper bound on the peak sidelobe level of Galois sequences is of order $\sqrt{n} \log n$ [109] (see the forthcoming Theorem 5.2.4 for a precise statement). This bound only guarantees a peak sidelobe level that is worse than that of a typical binary sequence given in Theorem 1.4.2.

However, there is numerical evidence [63] that there are Galois sequences for which the peak sidelobe level grows at least with order $\sqrt{n} \log \log n$. In particular, Jedwab and Yoshida said [63]:

"The claim that the PSL of m-sequences grows like $O(\sqrt{n})$, which appears frequently in the radar literature, is concluded to be unproven and not currently supported by data."

Additionally, Jedwab and Yoshida [63, Section 7] state the following open question:

"[...] Prove or disprove the claim that the PSL of some or all m-sequences grows like $O(\sqrt{n})$."

In what follows we want to give theoretical evidence that there exists a family of Galois sequences whose peak sidelobe level grows grows faster than $c\sqrt{n}$ for each constant $c > 0$.

For an entertaining and insightful historical background on the peak sidelobe level of Galois sequences from the viewpoint of radar literature we recommend the reader [63, Section 3]. We note that the experimental results in [63] and [28] (also summarised in [60]) give directions for further research.

The remainder of this chapter is structured as follows. In Section 5.2 we provide a connection between the peak sidelobe level of Galois sequences and certain additive character sums, and prove known upper and lower bounds on the peak sidelobe level of Galois sequences. In Section 5.3, after recalling some terminology from geometry, we give bounds on additive character sums and sums that involve products of Gauss sums. We

conclude the section with a natural conjecture (see the forthcoming Conjecture 5.3.5), which states that certain sums of products of Gauss sums are small in magnitude. We also provide numerical evidence supporting the conjecture. In Section 5.4 we then prove an equidistribution result for the arguments of certain Gauss sums, which heavily relies on our conjecture. This result will be the key ingredient in the proof of our main results (see the forthcoming Theorem 5.5.3 and Corollary 5.5.4). In Section 5.5 we prove our main results, thereby giving theoretical evidence that there exists a family of Galois sequences of length n whose peak sidelobe level is at least of order $\sqrt{n}\log\log\log n$. Our results support numerical evidence made in [63]. We conclude with Section 5.6, where we give a list of open problems concerning the peak sidelobe level of binary sequences.

5.2 Additive character sums and p-ary Galois sequences

Let $\mathbb{F}_q$ be of characteristic p and write $n = q-1$. Recall from (2.3) that, for each $v \in \mathbb{F}_q$, the additive character ψ_v of $\mathbb{F}_q$ is given by

$$\psi_v(x) = e^{2\pi i \operatorname{Tr}_{q/p}(vx)/p} \quad \text{for each } x \in \mathbb{F}_q.$$

For $v \in \mathbb{F}_q^*$ and a primitive element θ of $\mathbb{F}_q$, we define the *p-ary Galois sequence* (with respect to v and θ) to be the sequence $A(v,\theta) = (a_0, a_1, \ldots, a_{n-1})$ with

$$a_j = \psi_v(\theta^j) \quad \text{for each } j = 0, 1, \ldots, n-1.$$

Since it does not make much difference in our considerations whether p is odd or even, we consider the p-ary Galois sequences. Notice that a 2-ary Galois sequence is a Galois sequence in the usual sense. The following lemma shows that there is a one-to-one correspondence between the aperiodic autocorrelations of p-ary Galois sequences and additive character sums of the type

$$\sum_{j=s}^{s+\ell-1} \psi_1(\theta^j) \tag{5.1}$$

for an integer s and $\ell \in \{1, 2, \ldots, n-1\}$. Notice that we may assume that $s \in \{0, 1, \ldots, n-1\}$.

Lemma 5.2.1. *Let q be a prime power and write $n = q-1$. Let θ be a primitive element of $\mathbb{F}_q$ and let ψ_1 be the canonical additive character of $\mathbb{F}_q$. Let $v \in \mathbb{F}_q^*$ and let $u \in \{1, 2, \ldots, n-1\}$. Then*

$$C_{A(v,\theta)}(u) = \sum_{j=s}^{s+\ell-1} \psi_1(\theta^j),$$

where $\ell = n - u$ and s is an integer such that $\theta^s = v(1+\theta^u)$.

Proof. We have

$$\begin{aligned} C_{A(v,\theta)}(u) &= \sum_{j=0}^{n-u-1} \psi_1\big(v\theta^j(1+\theta^u)\big) \\ &= \sum_{j=0}^{\ell-1} \psi_1(\theta^{j+s}), \end{aligned}$$

as required. □

Therefore, studying the aperiodic autocorrelations of p-ary Galois sequences is the same problem as studying the additive character sums (5.1). In what follows we shall focus on the study of the character sums.

We need some more notation. For a positive integer n and real x, the *Dirichlet kernel*[1] is

$$D_n(x) = \sum_{j=0}^{n-1} e^{2\pi i x j}. \tag{5.2}$$

Notice that $D_n(x) = n$ whenever $x \in \mathbb{Z}$. Using the formula for the sum of the first n terms of a geometric series, we have

$$D_n(x) = \frac{e^{\pi i n x}\sin(\pi n x)}{e^{\pi i x}\sin(\pi x)} \quad \text{for all } x \in \mathbb{R} \setminus \mathbb{Z}. \tag{5.3}$$

The next lemma will be the starting point for our considerations. It gives an alternative expression of an additive character sum in terms of Dirichlet kernels and Gauss sums. Notice that, if θ is a primitive element of $\mathbb{F}_q$, then θ^d is also a primitive element of $\mathbb{F}_q$ whenever d is an integer with $\gcd(d, q-1) = 1$.

Lemma 5.2.2. *Write $n = q-1$, let s be an integer, and let $\ell \in \{1, 2, \ldots, n-1\}$. Let θ be a primitive element of $\mathbb{F}_q$, let d be an integer with $\gcd(d, n) = 1$, and let ψ_1 be the canonical additive character of $\mathbb{F}_q$. Then*

$$\sum_{j=s}^{s+\ell-1} \psi_1\big(\theta^{dj}\big) = \frac{1}{n}\sum_{k=0}^{n-1} D_\ell\left(\frac{k}{n}\right) G\big(\chi^{-kd^{-1}}\big) e^{2\pi i k s/n},$$

where χ is the multiplicative character of $\mathbb{F}_q$ given by $\chi(\theta) = e^{2\pi i/n}$, and d^{-1} is the multiplicative inverse of d modulo n.

Proof. We have

$$\sum_{j=s}^{s+\ell-1} \psi_1\big(\theta^{dj}\big) = \sum_{j=0}^{n-1} w_j \psi_1\big(\theta^{d(j+s)}\big), \tag{5.4}$$

[1] We note that in the literature the Dirichlet kernel is often defined as $D_n(x) = \sum_{|j|\le n} e^{2\pi i x j}$. However, the definition (5.2) is more convenient for our concerns and follows [3].

where

$$w_j = \begin{cases} 1 & \text{for } j \in \{0, \ldots, \ell - 1\} \\ 0 & \text{otherwise.} \end{cases}$$

The Fourier transform $(\hat{w}_0, \ldots, \hat{w}_{n-1})$ of $(w_0, \ldots, w_{n-1})$ is given by

$$\hat{w}_k = \sum_{j=0}^{\ell-1} e^{2\pi i k j/n} = D_\ell\left(\frac{k}{n}\right) \quad \text{for each } k = 0, \ldots, n-1,$$

and via the inverse Fourier transform formula, we have

$$w_j = \frac{1}{n} \sum_{k=0}^{n-1} D_\ell\left(\frac{k}{n}\right) e^{-2\pi i k j/n} \quad \text{for each } j = 0, \ldots, n-1.$$

Substitution into (5.4) gives

$$\sum_{j=s}^{s+\ell-1} \psi_1\big(\theta^{dj}\big) = \frac{1}{n} \sum_{k=0}^{n-1} D_\ell\left(\frac{k}{n}\right) \sum_{j=0}^{n-1} \psi_1\big(\theta^{d(j+s)}\big) e^{-2\pi i k j/n}.$$

Substituting $j = hd^{-1} - s$ and using $\chi(\theta) = e^{2\pi i/n}$, we have for each integer k:

$$\begin{aligned} \sum_{j=0}^{n-1} \psi_1\big(\theta^{d(j+s)}\big) e^{-2\pi i k j/n} &= \chi^k\big(\theta^s\big) \sum_{h=0}^{n-1} \psi_1\big(\theta^h\big) \chi^{-kd^{-1}}\big(\theta^h\big) \\ &= G(\chi^{-kd^{-1}}) e^{2\pi i k s/n}, \end{aligned}$$

which proves the lemma. □

Upper bound on the peak sidelobe level of Galois sequences

To prove Sarwate's bound on the peak sidelobe level of Galois sequences we shall need the following bound on sums of magnitudes of Dirichlet kernels. Its proof follows a well known method used by Vinogradov [129, Chapter 3, Problem 11]. Write

$$\delta_n = \begin{cases} 1 & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd.} \end{cases} \tag{5.5}$$

Lemma 5.2.3. *Let n be a positive integer and let $\ell \in \{1, 2, \ldots, n-1\}$. Then*

$$\sum_{k=1}^{n-1} \left| D_\ell\left(\frac{k}{n}\right) \right| < \frac{2n}{\pi} \log\left(\frac{4n}{\pi}\right) + \delta_n.$$

Proof. Using (5.3) and elementary properties of the sine function, we have

$$\begin{aligned}\sum_{k=1}^{n-1}\left|D_\ell\left(\frac{k}{n}\right)\right| &= \sum_{k=1}^{n-1}\left|\frac{\sin(\pi\ell k/n)}{\sin(\pi k/n)}\right| \\ &\leq \sum_{k=1}^{n-1}\frac{1}{\sin(\pi k/n)} \\ &= 2\sum_{1\leq k\leq (n-1)/2}\frac{1}{\sin(\pi k/n)} + \delta_n.\end{aligned}$$

Since $1/\sin(x)$ is convex on $(0,\pi)$, it is a consequence of Jensen's inequality (see [90, Appendix B, eq. (B.2)]) that

$$\frac{1}{\sin(\pi k/n)} \leq \int_{k-1/2}^{k+1/2}\frac{1}{\sin(\pi x/n)}dx$$

for each $1 \leq k \leq (n-1)/2$. Therefore,

$$\sum_{k=1}^{n-1}\left|D_\ell\left(\frac{k}{n}\right)\right| \leq 2\int_{1/2}^{n/2}\frac{1}{\sin(\pi x/n)}dx + \delta_n. \tag{5.6}$$

Substitute $y = \pi x/n$ to obtain

$$\int_{1/2}^{n/2}\frac{1}{\sin(\pi x/n)}dx = \frac{n}{\pi}\int_{\pi/(2n)}^{\pi/2}\frac{1}{\sin y}dy.$$

From [46, eq. 2.526] we then find that

$$\begin{aligned}\int_{1/2}^{n/2}\frac{1}{\sin(\pi x/n)}dx &= -\frac{n}{\pi}\log\left(\tan\left(\frac{\pi}{4n}\right)\right) \\ &< \frac{n}{\pi}\log\left(\frac{4n}{\pi}\right)\end{aligned}$$

using $\cot x < 1/x$ for $0 < x < \pi$. Substitution into (5.6) completes the proof. □

Write $n = q-1$, let θ be a primitive element of $\mathbb{F}_q$, and let ψ_1 be the canonical additive character of $\mathbb{F}_q$. Let s be an integer and let $\ell \in \{0,1,\ldots,n-1\}$. In spite of we know from Lemma 2.2.1 (i) that

$$\sum_{j=0}^{n-1}\psi_1(\theta^j) = -1,$$

the sum

$$\sum_{j=s}^{s+\ell-1}\psi_1(\theta^j)$$

is in general hard to evaluate. However, applying Lemma 5.2.2 and the triangle inequality

to this sum, we have

$$\left| \sum_{j=s}^{s+\ell-1} \psi_1(\theta^j) \right| < \sqrt{n+1} \left(\frac{2}{\pi} \log\left(\frac{4n}{\pi}\right) + \delta_n \right) + 1 \tag{5.7}$$

using Lemmas 5.2.3 and 2.2.3, where δ_n is defined in (5.5).

Extending the definition of the peak sidelobe level from binary to unimodular sequences, the *peak sidelobe level* of a unimodular sequence A of length $n > 1$ is

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

We have the following result on the peak sidelobe level of a p-ary Galois sequence. It follows readily from Lemma 5.2.2 and the bound (5.7).

Theorem 5.2.4 ([109])**.** *Let A be a p-ary Galois sequence of length n. Then*

$$\mathrm{M}(A) < \sqrt{n+1} \left(\frac{2}{\pi} \log\left(\frac{4n}{\pi}\right) + \delta_n \right) + 1,$$

where δ_n is defined in (5.5)*.*

We remark that improvements on the bound in Lemma 5.2.3 lead directly to better bounds in (5.7) and Theorem 5.2.4. As remarked by Sarwate [109], computationally it seems that the bound in Lemma 5.2.3 can be replaced with $1/2\, n \log n$ provided that n is large enough.

Lower bound on the peak sidelobe level of Galois sequences

As mentioned in Section 5.1, the peak sidelobe level of 2-ary Galois sequences of length n grows at least with order $\sqrt{n}$. Therefore, in view of Lemma 5.2.1, there exists a constant $c > 0$ which does not depend on n such that, for given $n = 2^m - 1$ and a primitive element θ of $\mathbb{F}_{2^m}$, there exist an integer s and $\ell \in \{1, 2, \ldots, n-1\}$ such that

$$\left| \sum_{j=s}^{s+\ell-1} \psi_1(\theta^j) \right| > c\sqrt{n}. \tag{5.8}$$

Let p be a prime. Generalising the method of Sarwate [108] slightly, we can see that the left-hand side of (5.8) can be at least $\sqrt{n}/2$ for all $n = p^m - 1$. Let $A = (a_0, a_1, \ldots, a_{n-1})$ be a p-ary Galois sequence of length n. For $u \in \{1, 2, \ldots, n-1\}$, we are interested in the expectation of the squared magnitude of the aperiodic autocorrelation at shift u over all cyclic shifts of A. Define $B = (b_0, b_1, \ldots, b_{n-1})$ with

$$b_j = a_j \overline{a_{j+u}} \quad \text{for each } j = 0, 1, \ldots, n-1.$$

Notice that B is a p-ary Galois sequence again. Analogously as in the proof of Theorem 2.5.5, we have

$$R_B(s) = \begin{cases} -1 & \text{for } s \not\equiv 0 \pmod{n} \\ n & \text{for } s \equiv 0 \pmod{n}. \end{cases}$$

Therefore, we have

$$\begin{aligned} \frac{1}{n}\sum_{r=0}^{n-1} \left|C_{A^{r,n}}(u)\right|^2 &= \frac{1}{n}\sum_{r=0}^{n-1}\sum_{k,\,\ell=0}^{n-u-1} a_{k+r}\overline{a_{k+r+u}a_{\ell+r}}a_{\ell+r+u} \\ &= \frac{1}{n}\sum_{r=0}^{n-1}\sum_{k,\,\ell=0}^{n-u-1} b_{k+r}\overline{b_{\ell+r}} \\ &= \frac{1}{n}\sum_{k,\,\ell=0}^{n-u-1} R_B(k-\ell) \\ &= \frac{(n-u)(u+1)}{n}. \end{aligned}$$

Taking $u = \lceil (n-1)/2 \rceil$, we obtain

$$\frac{1}{n}\sum_{r=0}^{n-1} \left|C_{A^{r,n}}(u)\right|^2 > \frac{n}{4}.$$

Therefore, for each $n = p^m - 1$, there exists a p-ary Galois sequence of length n whose aperiodic autocorrelation at shift $\lceil (n-1)/2 \rceil$ is greater than $\sqrt{n}/2$ in magnitude. In view of Lemma 5.2.1 that means that, for each $n = p^m - 1$, there exist a primitive element θ of $\mathbb{F}_{p^m}$ and an integer s such that

$$\left| \sum_{j=s}^{s+\ell-1} \psi_1(\theta^j) \right| > \frac{\sqrt{n}}{2},$$

where $\ell = n - \lceil (n-1)/2 \rceil$.

In what follows we examine the following question: Does there exist a function $f(n)$ with $f(n) \to \infty$ as $n \to \infty$ such that the left-hand side of (5.8) can be at least $f(n)\sqrt{n}$ for infinitely many n?

The following lemma relies on Lemma 5.2.2. It provides a lower bound on the additive character sums in question.

Lemma 5.2.5. *Let $n = q - 1$, let $\ell \in \{1, 2, \ldots, n-1\}$, and let H be a positive integer with $H < n/2$. Let θ be a primitive element of $\mathbb{F}_q$, let d be an integer with $\gcd(d, n) = 1$, and let ψ_1 be the canonical additive character of $\mathbb{F}_q$. Then there exists an integer t such that*

$$\left| \sum_{j=t}^{t+\ell-1} \psi_1\big(\theta^{dj}\big) \right| \geq \frac{1}{n} \left| \sum_{|h| \leq H} D_\ell\Big(\frac{h}{n}\Big) G\big(\chi^{-hd^{-1}}\big) \Big(1 - \frac{|h|}{H}\Big) \right|, \tag{5.9}$$

where χ is the multiplicative character of $\mathbb{F}_q$ given by $\chi(\theta) = e^{2\pi i/n}$, and d^{-1} is the multiplicative inverse of d modulo n.

Proof. Write

$$S(s) = \sum_{j=s}^{s+\ell-1} \psi_1\big(\theta^{dj}\big).$$

From Lemma 5.2.2 we know that

$$S(s) = \frac{1}{n}\sum_{k=0}^{n-1} D_\ell\left(\frac{k}{n}\right) G\big(\chi^{-kd^{-1}}\big) e^{2\pi iks/n}$$

for each integer s. Considering the factors on the right-hand side as functions in k, they are all periodic with period n, and therefore we may write

$$S(s) = \frac{1}{n}\sum_{-n/2\le k\le (n-1)/2} D_\ell\left(\frac{k}{n}\right) G\big(\chi^{-kd^{-1}}\big) e^{2\pi iks/n} \tag{5.10}$$

for each $s \in \{0, 1, \ldots, n-1\}$.

For each function $\delta\colon \{0, \ldots, n-1\} \to \mathbb{C}$, define

$$\hat{\delta}(k) = \sum_{s=0}^{n-1} \delta(s) e^{2\pi iks/n}$$

to be the Fourier transform of $(\delta(0), \ldots, \delta(n-1))$. From (5.10) we find that

$$\sum_{s=0}^{n-1} \delta(s)S(s) = \frac{1}{n}\sum_{-n/2\le k\le (n-1)/2} D_\ell\left(\frac{k}{n}\right) G\big(\chi^{-kd^{-1}}\big)\hat{\delta}(k).$$

We wish to sum only over k close to zero on the right-hand side. Since the Fourier transform is one-to-one, we define the function δ by

$$\hat{\delta}(h) = \begin{cases} 1 - \frac{|h|}{H} & \text{for } |h| \le H \\ 0 & \text{otherwise,} \end{cases}$$

to obtain

$$\sum_{s=0}^{n-1} \delta(s)S(s) = \frac{1}{n}\sum_{|h|\le H} D_\ell\left(\frac{h}{n}\right) G\big(\chi^{-hd^{-1}}\big)\left(1 - \frac{|h|}{H}\right). \tag{5.11}$$

For this choice of $\hat{\delta}$, we have via the inverse Fourier transform formula for each integer s:

$$\begin{aligned} \delta(s) &= \frac{1}{n}\sum_{-n/2\le k\le (n-1)/2} \hat{\delta}(k) e^{-2\pi iks/n} \\ &= \frac{1}{n} F_H\left(\frac{s}{n}\right), \end{aligned} \tag{5.12}$$

where F_N is the *Fejér kernel* given by

$$F_N(x) = \sum_{|j|\leq N} \left(1 - \frac{|j|}{N}\right) e^{2\pi i x j}$$

for positive integers N and real x. Next we deduce an upper bound on the magnitude of the left-hand side of (5.11). Using the triangle inequality and (5.12), we have

$$\left|\sum_{s=0}^{n-1} \delta(s)S(s)\right| \leq \frac{1}{n} \max_{0\leq t<n} |S(t)| \sum_{s=0}^{n-1} \left|F_H\left(\frac{s}{n}\right)\right|.$$

It is known [75, p. 12] that $F_N(x) \geq 0$ for all positive integers N and real x. Therefore,

$$\begin{aligned}\left|\sum_{s=0}^{n-1} \delta(s)S(s)\right| &\leq \frac{1}{n} \max_{0\leq t<n} |S(t)| \sum_{s=0}^{n-1} F_H\left(\frac{s}{n}\right) \\ &= \frac{1}{n} \max_{0\leq t<n} |S(t)| \sum_{|h|\leq H} \left(1 - \frac{|h|}{H}\right) \sum_{s=0}^{n-1} e^{2\pi i h s/n} \\ &= \max_{0\leq t<n} |S(t)|\end{aligned}$$

since

$$\sum_{s=0}^{n-1} e^{2\pi i h s/n} = \begin{cases} n & \text{if } h \equiv 0 \pmod{n} \\ 0 & \text{otherwise,}\end{cases}$$

which, in combination with (5.11), proves the lemma. □

Outline of the proof of the main results

We now give a brief overview of the strategy for the proofs of our main results (see the forthcoming Theorem 5.5.3 and Corollary 5.5.4). We first have to set some notation. For a prime p and a positive integer H, define

$$\kappa_p(H) = |\{h \in \{1, 2, \ldots, H\} \colon \gcd(h, p) = 1\}|. \tag{5.13}$$

Write $\kappa = \kappa_p(H)$ and define $\boldsymbol{B} = (b_1, b_2, \ldots, b_\kappa)$ to be the vector that contains all κ positive integers that are at most H and are coprime to p in ascending order. For example, if $p = 3$ and $H = 7$, then $\kappa = 5$ and $\boldsymbol{B} = (1, 2, 4, 5, 7)$. Let $\mathbb{F}_q$ be of characteristic p and let χ be a primitive multiplicative character of $\mathbb{F}_q$. Define

$$\Psi_\chi \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{C},\ (b, d) \mapsto \frac{\arg\left(G(\chi^{bd})\right)}{2\pi}. \tag{5.14}$$

We wish to show that the vectors of normalised arguments of Gauss sums

$$\big(\Psi_\chi(b_1,d),\Psi_\chi(b_2,d),\dots,\Psi_\chi(b_\kappa,d)\big) \tag{5.15}$$

become equidistributed in $[0,1)^\kappa$ when κ is "small" and d ranges over all integers with $\gcd(d,q-1)=1$ and q tends to infinity. Then we choose the integer H as large as possible such that there exists an integer d with $\gcd(d,q-1)=1$ with the property that each summand on the right-hand side of (5.9) has large real part. Afterwards, we bound the magnitude of the sum on the right-hand side of (5.9) with the real part of the sum and then bound the remaining terms.

5.3 Bounds on character sums

In this section we give some bounds on character sums that we shall need to prove our equidistribution results on the vectors (5.15).

Geometry and bounds on additive character sums

We begin with recalling some terminology from geometry in $\mathbb{R}^n$. Let $\mathrm{vol}_n(\cdot)$ be the n-dimensional volume with respect to the Lebesgue measure on $\mathbb{R}^n$. For $V\subset\mathbb{R}^n$, the *convex hull* $\mathrm{conv}(V)$ of V is the set of all finite convex combinations of elements of V. Vectors $\boldsymbol{v}_1,\dots,\boldsymbol{v}_d\in\mathbb{R}^n$ are called *affinely independent* if, for all $\alpha_1,\dots,\alpha_d\in\mathbb{R}$ with

$$\alpha_1\boldsymbol{v}_1+\cdots+\alpha_d\boldsymbol{v}_d=0 \qquad \text{and} \qquad \alpha_1+\cdots+\alpha_d=0,$$

we have $\alpha_1=\cdots=\alpha_d=0$. A *simplex* is the convex hull of affinely independent vectors. We have the following well known result on the volume of a simplex in $\mathbb{R}^n$.

Lemma 5.3.1 ([123])**.** *Let T be a simplex with vertices $\boldsymbol{v}_1,\boldsymbol{v}_2,\dots,\boldsymbol{v}_{n+1}\in\mathbb{R}^n$. Then*

$$\mathrm{vol}_n(T)=\frac{1}{n!}\big|\det(\boldsymbol{v}_2-\boldsymbol{v}_1,\boldsymbol{v}_3-\boldsymbol{v}_1,\dots,\boldsymbol{v}_{n+1}-\boldsymbol{v}_1)\big|.$$

Let $\mathbb{F}_q[x_1,x_1^{-1},\dots,x_n,x_n^{-1}]$ be the ring of Laurent polynomials over $\mathbb{F}_q$ in the indeterminates $x_1,\dots,x_n$. For $\boldsymbol{j}=(j_1,\dots,j_n)\in\mathbb{Z}^n$, we use the shorthand notation $\boldsymbol{x}^{\boldsymbol{j}}$ for the element

$$x_1^{j_1}\cdots x_n^{j_n}\in\mathbb{F}_q[x_1,x_1^{-1},\dots,x_n,x_n^{-1}].$$

For a Laurent polynomial

$$f(\boldsymbol{x})=\sum_{\boldsymbol{j}\in\mathbb{Z}^n}a_{\boldsymbol{j}}\boldsymbol{x}^{\boldsymbol{j}}\in\mathbb{F}_q[x_1,x_1^{-1},\dots,x_n,x_n^{-1}],$$

the *Newton polyhedron* $\Delta(f)$ of f is the subset of $\mathbb{R}^n$ given by

$$\operatorname{conv}\big(\{\boldsymbol{j} \in \mathbb{Z}^n : a_{\boldsymbol{j}} \neq 0\} \cup \{\mathbf{0}\}\big),$$

where $\mathbf{0} = (0, \dots, 0)$. For a face σ of $\Delta(f)$, the restriction of f to σ is

$$f_\sigma = \sum_{\boldsymbol{j} \in \sigma} a_{\boldsymbol{j}} \boldsymbol{x}^{\boldsymbol{j}}.$$

We call f *non-degenerate* if, for each face σ of $\Delta(f)$ that does not contain $\mathbf{0}$, the system of the n partial derivatives

$$\frac{\partial f_\sigma}{\partial x_1} = \cdots = \frac{\partial f_\sigma}{\partial x_n} = 0$$

has no solution with $x_1 \cdots x_n \neq 0$ over an algebraic closure of $\mathbb{F}_q$. We shall need the following bound on sums of additive characters with polynomial arguments, which is essentially [2, Theorem 1.8].

Proposition 5.3.2 ([2])**.** *Let ψ be a nontrivial additive character of $\mathbb{F}_q$. Let f be non-degenerate Laurent polynomial in $\mathbb{F}_q[x_1, x_1^{-1}, \dots, x_n, x_n^{-1}]$, and suppose that $\Delta(f)$ has dimension n. Then*

$$\left| \sum_{\boldsymbol{x} \in (\mathbb{F}_q^*)^n} \psi\big(f(\boldsymbol{x})\big) \right| \leq n! \operatorname{vol}_n\big(\Delta(f)\big) q^{n/2}.$$

The following result is an application of Proposition 5.3.2.

Lemma 5.3.3. *Let $\mathbb{F}_q$ be of characteristic p, and let ψ be a nontrivial additive character of $\mathbb{F}_q$. Let M and N be nonnegative integers which are not both equal to zero, and let $h_1, \dots, h_{M+N}$ be positive integers which are coprime to p. Write $K = \sum_{j=1}^{M} h_j$ and $L = \sum_{j=M+1}^{M+N} h_j$, and suppose that $K \neq L$. Let r and s be polynomials in $\mathbb{F}_q[x_1, \dots, x_{M+N}]$ given by*

$$r(\boldsymbol{x}) = \sum_{j=1}^{M+N} \alpha_j x_j,$$
$$s(\boldsymbol{x}) = \beta_1 \prod_{j=1}^{M} x_j^{h_j} + \beta_2 \prod_{j=M+1}^{M+N} x_j^{h_j} + \beta_3,$$

where $\alpha_1, \dots, \alpha_{M+N}, \beta_1, \beta_2 \in \mathbb{F}_q^*$ and $\beta_3 \in \mathbb{F}_q$. Then

(i)

$$\left| \sum_{\boldsymbol{x} \in (\mathbb{F}_q^*)^{M+N}} \psi\big(r(\boldsymbol{x})\big) \right| \leq q^{(M+N)/2};$$

(ii)

$$\left| \sum_{(\boldsymbol{x}, z) \in (\mathbb{F}_q^*)^{M+N+1}} \psi\big(r(\boldsymbol{x}) + z s(\boldsymbol{x})\big) \right| \leq \big(\max(K, L) + 1\big) q^{(M+N+1)/2}.$$

Proof. We want to make use of Proposition 5.3.2. Therefore, first we have to show that $r(\boldsymbol{x})$ and $r(\boldsymbol{x}) + zs(\boldsymbol{x})$ are non-degenerate.

Let $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{M+N}$ be the standard unit vectors of $\mathbb{Z}^{M+N}$. By definition

$$\Delta(r(\boldsymbol{x})) = \operatorname{conv}\big(\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{M+N}, \boldsymbol{0}\}\big).$$

From Lemma 5.3.1 we find that

$$\operatorname{vol}_{M+N}\big(\Delta(r(\boldsymbol{x}))\big) = \frac{1}{(M+N)!},$$

so that assertion (i) follows from Proposition 5.3.2 since $r(\boldsymbol{x})$ is non-degenerate.

Now let $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{M+N+1}$ be the standard unit vectors of $\mathbb{Z}^{M+N+1}$. Define $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}^{M+N+1}$ by

$$\boldsymbol{a} = (h_1, \ldots, h_M, \underbrace{0, \ldots, 0}_{N}, 1),$$
$$\boldsymbol{b} = (\underbrace{0, \ldots, 0}_{M}, h_{M+1}, \ldots, h_{M+N}, 1).$$

Then

$$\Delta(r(\boldsymbol{x}) + zs(\boldsymbol{x})) = \operatorname{conv}\big(\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{M+N}, \boldsymbol{0}, \boldsymbol{a}, \boldsymbol{b}\}\big).$$

We now show that $r(\boldsymbol{x}) + zs(\boldsymbol{x})$ is non-degenerate. Let σ be a face of $\Delta(r(\boldsymbol{x}) + zs(\boldsymbol{x}))$ that does not contain $\boldsymbol{0}$. If $M = 0$ or $N = 0$, then it is easy to see that $r(\boldsymbol{x}) + zs(\boldsymbol{x})$ is non-degenerate, so that we may assume $M, N \geq 1$. We distinguish three cases.

Case 1. $\boldsymbol{a}$ or $\boldsymbol{b}$ does not lie in σ. If exactly one of $\boldsymbol{a}$ and $\boldsymbol{b}$ lies in σ, then

$$\frac{\partial(r(\boldsymbol{x}) + zs(\boldsymbol{x}))_\sigma}{\partial z} = \begin{cases} \beta_2 \prod_{j=M+1}^{M+N} x_j^{h_j} & \text{if } \boldsymbol{a} \notin \sigma \text{ and } \boldsymbol{b} \in \sigma \\ \beta_1 \prod_{j=1}^{M} x_j^{h_j} & \text{if } \boldsymbol{b} \notin \sigma \text{ and } \boldsymbol{a} \in \sigma, \end{cases}$$

which has no nontrivial zero. When both $\boldsymbol{a}$ and $\boldsymbol{b}$ do not lie in σ, then there exists $j \in \{1, \ldots, M+N\}$ such that

$$\frac{\partial(r(\boldsymbol{x}) + zs(\boldsymbol{x}))_\sigma}{\partial x_j} = 1,$$

which has no zero.

Case 2. $\boldsymbol{a}, \boldsymbol{b} \in \sigma$ and $\boldsymbol{e}_j \notin \sigma$ for some j. Then

$$\frac{\partial(r(\boldsymbol{x}) + zs(\boldsymbol{x}))_\sigma}{\partial x_j}$$

has no nontrivial zero.

Case 3. $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_{M+N} \in \sigma$. The hyperplane through $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{M+N}, \boldsymbol{a}$ consists of all vectors in $\mathbb{R}^{M+N+1}$ that are of the form

$$\boldsymbol{e}_1 + \gamma_1(\boldsymbol{a} - \boldsymbol{e}_1) + \gamma_2(\boldsymbol{e}_2 - \boldsymbol{e}_1) + \gamma_3(\boldsymbol{e}_3 - \boldsymbol{e}_1) + \cdots + \gamma_{M+N}(\boldsymbol{e}_{M+N} - \boldsymbol{e}_1)$$

for some $\gamma_1, \ldots, \gamma_{M+N} \in \mathbb{R}$. Since $h_1 + \cdots + h_M \neq h_{M+1} + \ldots h_{M+N}$, the vector $\boldsymbol{b}$ is not of this form and therefore this case does not occur.

Next we estimate the volume of $\Delta(r(\boldsymbol{x}) + zs(\boldsymbol{x}))$. Write $\mathrm{vol}(\cdot) = \mathrm{vol}_{M+N+1}(\cdot)$. We have

$$\mathrm{vol}\left(\Delta(r(\boldsymbol{x}) + zs(\boldsymbol{x}))\right) \leq \mathrm{vol}(T_{\boldsymbol{b}}) + \max_{\boldsymbol{u} \in \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{M+N}, \boldsymbol{0}, \boldsymbol{a}\}} \mathrm{vol}(T_{\boldsymbol{u}}), \tag{5.16}$$

where

$$\begin{aligned} T_{\boldsymbol{b}} &= \mathrm{conv}\left(\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{M+N}, \boldsymbol{0}, \boldsymbol{a}\}\right), \\ T_{\boldsymbol{a}} &= \mathrm{conv}\left(\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{M+N}, \boldsymbol{0}, \boldsymbol{b}\}\right), \\ T_{\boldsymbol{0}} &= \mathrm{conv}\left(\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{M+N}, \boldsymbol{a}, \boldsymbol{b}\}\right), \end{aligned}$$

and

$$T_{\boldsymbol{e}_j} = \mathrm{conv}\left(\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{M+N}, \boldsymbol{0}, \boldsymbol{a}, \boldsymbol{b}\} \setminus \{\boldsymbol{e}_j\}\right)$$

for each $j \in \{1, \ldots, M+N\}$. From Lemma 5.3.1 we find that

$$\begin{aligned} \mathrm{vol}(T_{\boldsymbol{b}}) &= \frac{1}{(M+N+1)!}, \\ \mathrm{vol}(T_{\boldsymbol{a}}) &= \frac{1}{(M+N+1)!}, \\ \mathrm{vol}(T_0) &= \frac{\left|\sum_{j=1}^{M} h_j - \sum_{j=M+1}^{M+N} h_j\right|}{(M+N+1)!}, \\ \mathrm{vol}(T_j) &\leq \frac{\max(h_1, \ldots, h_{M+N})}{(M+N+1)!} \end{aligned}$$

for all $j \in \{1, \ldots, M+N\}$. Substitution into (5.16) and estimation of the volumes gives

$$\mathrm{vol}\left(\Delta(r(\boldsymbol{x}) + zs(\boldsymbol{x}))\right) \leq \frac{\max\left(\sum_{j=1}^{M} h_j, \sum_{j=M+1}^{M+N} h_j\right) + 1}{(M+N+1)!}.$$

Proposition 5.3.2 completes the proof. □

Bounds on sums that involve products of Gauss sums

We now give a bound on a sum of products of Gauss sums, which is related to Lemma 2.2.7 in the following sense: The case that $U = \widehat{\mathbb{F}_q^*}$, $k = 1$, $\ell = 0$, and $g_1 = 1$ in the following lemma

is essentially the case that $r = v_1$, $s = 0$, and $\alpha_1 = \cdots = \alpha_r$ are the trivial multiplicative characters of $\mathbb{F}_q$ in Lemma 2.2.7. Similarly, the case that $U = \widehat{\mathbb{F}_q^*}$, $k = 0$, $\ell = 1$, and $h_1 = 1$ in the following lemma is essentially the case that $r = 0$, $s = w_1$, and $\beta_1 = \cdots = \beta_s$ are the trivial multiplicative characters of $\mathbb{F}_q$ in Lemma 2.2.7.

Lemma 5.3.4. *Let $\mathbb{F}_q$ be of characteristic p and let U be a subgroup of $\widehat{\mathbb{F}_q^*}$. Let $g_1, \dots, g_k$, $h_1, \dots, h_\ell$ be different positive integers which are coprime to p and assume that k and ℓ are not both equal to zero. Let $v_1, \dots, v_k, w_1, \dots, w_\ell$ be positive integers, and write $K = \sum_{i=1}^{k} g_i v_i$ and $L = \sum_{j=1}^{\ell} h_j w_j$. If $K \neq L$, then*

$$\frac{1}{q-1}\left|\sum_{\chi\in U}\prod_{i=1}^{k}\left(\frac{G(\chi^{g_i})}{\sqrt{q}}\right)^{v_i}\prod_{j=1}^{\ell}\left(\overline{\frac{G(\chi^{h_j})}{\sqrt{q}}}\right)^{w_j}\right| \leq \frac{\max(K,L)+1}{\sqrt{q}} + \frac{1}{q}.$$

Proof. Write

$$S = \frac{1}{q-1}\sum_{\chi\in U}\prod_{i=1}^{k}\left(\frac{G(\chi^{g_i})}{\sqrt{q}}\right)^{v_i}\prod_{j=1}^{\ell}\left(\overline{\frac{G(\chi^{h_j})}{\sqrt{q}}}\right)^{w_j},$$

and put $M = \sum_{i=1}^{k} v_i$ and $N = \sum_{j=1}^{\ell} w_j$. Let m be the order of U and write $t = (q-1)/m$. Then $U = \{\chi^t \colon \chi \in \widehat{\mathbb{F}_q^*}\}$, so that

$$\sum_{\substack{a\in\mathbb{F}_q^*\\ a^t=1}}\chi(a) = \begin{cases} t & \text{if } \chi \in U\\ 0 & \text{otherwise.}\end{cases}$$

Therefore,

$$S = \frac{1}{t(q-1)}\sum_{\substack{a\in\mathbb{F}_q^*\\ a^t=1}}\sum_{\chi\in\widehat{\mathbb{F}_q^*}}\chi(a)\prod_{i=1}^{k}\left(\frac{G(\chi^{g_i})}{\sqrt{q}}\right)^{v_i}\prod_{j=1}^{\ell}\left(\overline{\frac{G(\chi^{h_j})}{\sqrt{q}}}\right)^{w_j}. \tag{5.17}$$

Write

$$\begin{aligned}\mu(\boldsymbol{x}) &= (x_1 \dots x_{v_1})^{g_1}(x_{v_1+1}\dots x_{v_1+v_2})^{g_2}\dots(x_{M-v_k+1}\dots x_M)^{g_k},\\ \nu(\boldsymbol{y}) &= (y_1 \dots y_{w_1})^{h_1}(y_{w_1+1}\dots y_{w_1+w_2})^{h_2}\dots(y_{N-w_\ell+1}\dots y_N)^{h_\ell}.\end{aligned}$$

and let ψ_1 be the canonical additive character of $\mathbb{F}_q$. We distinguish the cases whether one of the numbers k and ℓ is zero or not.

Case 1. $k, \ell > 0$. Applying the definition of a Gauss sum, we have

$$\begin{aligned}\prod_{i=1}^{k}\left(\frac{G(\chi^{g_i})}{\sqrt{q}}\right)^{v_i} &= q^{-M/2}\sum_{\boldsymbol{x}\in(\mathbb{F}_q^*)^M}\chi\big(\mu(\boldsymbol{x})\big)\psi_1(x_1+\cdots+x_M)\\ &= q^{-M/2}\sum_{b\in\mathbb{F}_q^*}\chi(b)\sum_{\substack{\boldsymbol{x}\in(\mathbb{F}_q^*)^M\\ \mu(\boldsymbol{x})=b}}\psi_1(x_1+\cdots+x_M).\end{aligned}$$

Analogously,

$$\prod_{j=1}^{\ell}\left(\frac{\overline{G(\chi^{h_j})}}{\sqrt{q}}\right)^{w_j} = q^{-N/2}\sum_{c\in\mathbb{F}_q^*}\overline{\chi(c)}\sum_{\substack{\boldsymbol{y}\in(\mathbb{F}_q^*)^N\\ \nu(\boldsymbol{y})=c}}\overline{\psi_1(y_1+\cdots+y_N)}.$$

Therefore, for each $a\in\mathbb{F}_q^*$,

$$q^{(M+N)/2}\sum_{\chi\in\widehat{\mathbb{F}_q^*}}\chi(a)\prod_{i=1}^{k}\left(\frac{G(\chi^{g_i})}{\sqrt{q}}\right)^{v_i}\prod_{j=1}^{\ell}\left(\frac{\overline{G(\chi^{h_j})}}{\sqrt{q}}\right)^{w_j}$$

equals

$$(q-1)\sum_{b\in\mathbb{F}_q^*}\sum_{\substack{\boldsymbol{x}\in(\mathbb{F}_q^*)^M\\ \mu(\boldsymbol{x})=b}}\psi_1(x_1+\cdots+x_M)\sum_{\substack{\boldsymbol{y}\in(\mathbb{F}_q^*)^N\\ \nu(\boldsymbol{y})=ab}}\overline{\psi_1(y_1+\cdots+y_N)}$$

since

$$\sum_{\chi\in\widehat{\mathbb{F}_q^*}}\chi(abc^{-1}) = \begin{cases} q-1 & \text{if } c=ab\\ 0 & \text{otherwise}\end{cases}$$

by Lemma 2.2.1 (ii). Further elementary manipulations then show that, for each $a\in\mathbb{F}_q^*$,

$$\frac{q^{(M+N)/2}}{q-1}\sum_{\chi\in\widehat{\mathbb{F}_q^*}}\chi(a)\prod_{i=1}^{k}\left(\frac{G(\chi^{g_i})}{\sqrt{q}}\right)^{v_i}\prod_{j=1}^{\ell}\left(\frac{\overline{G(\chi^{h_j})}}{\sqrt{q}}\right)^{w_j}$$

equals

$$\sum_{\substack{(\boldsymbol{x},\boldsymbol{y})\in(\mathbb{F}_q^*)^{M+N}\\ s_a(\boldsymbol{x},\boldsymbol{y})=0}}\psi_1\big(r(\boldsymbol{x},\boldsymbol{y})\big),$$

where the functions r and s_a are given by

$$\begin{aligned} r(\boldsymbol{x},\boldsymbol{y}) &= x_1+\cdots+x_M-y_1-\cdots-y_N,\\ s_a(\boldsymbol{x},\boldsymbol{y}) &= \mu(\boldsymbol{x})-\nu(\boldsymbol{y})/a.\end{aligned}$$

Substitution into (5.17) gives

$$S=\frac{1}{tq^{(M+N)/2}}\sum_{\substack{a\in\mathbb{F}_q^*\\ a^t=1}}\sum_{\substack{(\boldsymbol{x},\boldsymbol{y})\in(\mathbb{F}_q^*)^{M+N}\\ s_a(\boldsymbol{x},\boldsymbol{y})=0}}\psi_1\big(r(\boldsymbol{x},\boldsymbol{y})\big).$$

Define

$$a_{\max} = \underset{a\in\mathbb{F}_q^*,\, a^t=1}{\arg\max} \left| \sum_{\substack{(\boldsymbol{x},\boldsymbol{y})\in(\mathbb{F}_q^*)^{M+N} \\ s_a(\boldsymbol{x},\boldsymbol{y})=0}} \psi_1\big(r(\boldsymbol{x},\boldsymbol{y})\big) \right|,$$

to obtain

$$|S| \le q^{(M+N)/2} \left| \sum_{\substack{(\boldsymbol{x},\boldsymbol{y})\in(\mathbb{F}_q^*)^{M+N} \\ s_{a_{\max}}(\boldsymbol{x},\boldsymbol{y})=0}} \psi_1\big(r(\boldsymbol{x},\boldsymbol{y})\big) \right|.$$

We now introduce a new variable z, which since

$$\sum_{z\in\mathbb{F}_q} \psi_1\big(zc\big) = \begin{cases} q & \text{if } c = 0 \\ 0 & \text{if } c \neq 0 \end{cases}$$

by Lemma 2.2.1 (i), allows us to write

$$|S| \le q^{-(M+N+2)/2} \left| \sum_{\substack{(\boldsymbol{x},\boldsymbol{y})\in(\mathbb{F}_q^*)^{M+N} \\ z\in\mathbb{F}_q}} \psi_1\big(r(\boldsymbol{x},\boldsymbol{y}) + z s_{a_{\max}}(\boldsymbol{x},\boldsymbol{y})\big) \right|.$$

We split the sum into two sums (one corresponding to $z = 0$ and one to $z \neq 0$), and obtain by the triangle inequality

$$|S| \le |S_1| + |S_2|,$$

where

$$S_1 = q^{-(M+N+2)/2} \sum_{(\boldsymbol{x},\boldsymbol{y})\in(\mathbb{F}_q^*)^{M+N}} \psi_1\big(r(\boldsymbol{x},\boldsymbol{y})\big),$$
$$S_2 = q^{-(M+N+2)/2} \sum_{(\boldsymbol{x},\boldsymbol{y},z)\in(\mathbb{F}_q^*)^{M+N+1}} \psi_1\big(r(\boldsymbol{x},\boldsymbol{y}) + z s_{a_{\max}}(\boldsymbol{x},\boldsymbol{y})\big).$$

The proof now follows from Lemma 5.3.3.

Case 2. $k = 0$ or $\ell = 0$. Without loss of generality, we may assume that $\ell = 0$. Here, for each $a \in \mathbb{F}_q^*$, we have

$$q^{M/2} \sum_{\chi\in\widehat{\mathbb{F}_q^*}} \chi(a) \prod_{i=1}^{k} \left(\frac{G(\chi^{g_i})}{\sqrt{q}} \right)^{v_i} = (q-1) \sum_{\substack{\boldsymbol{x}\in(\mathbb{F}_q^*)^M \\ \mu(\boldsymbol{x})=a^{-1}}} \psi_1(x_1 + \cdots + x_M).$$

Substitution into (5.17) gives

$$S = \frac{1}{tq^{M/2}} \sum_{\substack{a\in\mathbb{F}_q^* \\ a^t=1}} \sum_{\substack{\boldsymbol{x}\in(\mathbb{F}_q^*)^M \\ \mu(\boldsymbol{x})=a^{-1}}} \psi_1(x_1 + \cdots + x_M).$$

The remainder of the proof is analogous to the proof of Case 1. □

Remark. Lemma 5.3.4 is a special case of the forthcoming Conjecture 5.3.5, in which the assumption $K \neq L$ is dropped.

Our equidistribution results on the arguments of Gauss sums shall heavily rely on the following conjecture.

Conjecture 5.3.5. *Let $\mathbb{F}_q$ be of characteristic p and let U be a subgroup of $\widehat{\mathbb{F}_q^*}$. Let $g_1, \dots, g_k, h_1, \dots, h_\ell$ be different positive integers which are coprime to p and assume that k and ℓ are not both equal to zero. Let $v_1, \dots, v_k, w_1, \dots, w_\ell$ be positive integers, and write $K = \sum_{i=1}^{k} g_i v_i$ and $L = \sum_{j=1}^{\ell} h_j w_j$. Then*

$$\frac{1}{q-1}\left|\sum_{\chi \in U}\prod_{i=1}^{k}\left(\frac{G(\chi^{g_i})}{\sqrt{q}}\right)^{v_i}\prod_{j=1}^{\ell}\left(\frac{\overline{G(\chi^{h_j})}}{\sqrt{q}}\right)^{w_j}\right| \leq \frac{\max(K,L)+1}{\sqrt{q}} + \frac{1}{q}. \tag{5.18}$$

The difficulty in proving the correctness of Conjecture 5.3.5 is that the polynomials that occur as arguments of the additive characters in the proof of Lemma 5.3.4 are not non-degenerate in the critical case that $K = L$.

In Table 5.1 we see the maximum values of the left-hand side of (5.18) and the values of the right-hand side of (5.18) for $q = 2^{17}$, $U = \widehat{\mathbb{F}_q^*}$, and $\max(K, L) \leq 15$. In the second column the maximum is taken over all inputs with $K = L$, and in the third column the maximum is taken over all inputs with $K \neq L$. All values are truncated to six decimal places. It seems that the maximum values of the left-hand side of (5.18) are not larger in the case that $K = L$ than in the case that $K \neq L$.

Table 5.2 provides similar results for $q = 3^{11}$, $U = \widehat{\mathbb{F}_q^*}$, and $\max(K, L) \leq 12$. Again, it seems that the maximum values of the left-hand side of (5.18) are not larger in the case that $K = L$ than in the case that $K \neq L$.

5.4 Equidistribution of the arguments of Gauss sums

In this section we prove our equidistribution results on the vectors (5.15).

Uniform distribution in $[0,1)^\kappa$

We begin with setting some notation. Let κ be a positive integer and let $\boldsymbol{c} = (c_1, \dots, c_\kappa)$, $\boldsymbol{d} = (d_1, \dots, d_\kappa) \in \mathbb{R}^\kappa$. We say that $\boldsymbol{c} < \boldsymbol{d}$ (or $\boldsymbol{c} \leq \boldsymbol{d}$) if $c_j < d_j$ (or $c_j \leq d_j$) for each $j = 1, \dots, \kappa$, and we define

$$[\boldsymbol{c}, \boldsymbol{d}) = \{\boldsymbol{x} \in \mathbb{R}^\kappa \colon \boldsymbol{c} \leq \boldsymbol{x} < \boldsymbol{d}\}.$$

Now let $\boldsymbol{A} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \dots)$ be a sequence of vectors, where $\boldsymbol{a}_j \in [0,1)^\kappa$ for each j. For a subset $\boldsymbol{E}$ of $[0,1)^\kappa$, we denote by $X_{\boldsymbol{A}}(\boldsymbol{E}; n)$ the number of points $\boldsymbol{a}_j$ with $j \in \{1, \dots, n\}$ that lie in $\boldsymbol{E}$.

Table 5.1: Maximum values of the left-hand side (LHS) of (5.18) and values of the right-hand side (RHS) of (5.18) for $q = 2^{17}$ and $U = \widehat{\mathbb{F}_q^*}$.

$\max(K, L)$	LHS with $K = L$	LHS with $K \neq L$	RHS
1	cannot occur	$2.762 \cdot 10^{-3}$	$5.531 \cdot 10^{-3}$
2	cannot occur	$0.770 \cdot 10^{-3}$	$8.294 \cdot 10^{-3}$
3	$0.007 \cdot 10^{-3}$	$3.898 \cdot 10^{-3}$	$11.056 \cdot 10^{-3}$
4	cannot occur	$7.813 \cdot 10^{-3}$	$13.818 \cdot 10^{-3}$
5	$3.898 \cdot 10^{-3}$	$9.348 \cdot 10^{-3}$	$16.580 \cdot 10^{-3}$
6	$0.770 \cdot 10^{-3}$	$11.431 \cdot 10^{-3}$	$19.342 \cdot 10^{-3}$
7	$8.811 \cdot 10^{-3}$	$14.588 \cdot 10^{-3}$	$22.104 \cdot 10^{-3}$
8	$9.346 \cdot 10^{-3}$	$15.965 \cdot 10^{-3}$	$24.866 \cdot 10^{-3}$
9	$12.199 \cdot 10^{-3}$	$23.289 \cdot 10^{-3}$	$27.628 \cdot 10^{-3}$
10	$11.284 \cdot 10^{-3}$	$20.370 \cdot 10^{-3}$	$30.391 \cdot 10^{-3}$
11	$11.608 \cdot 10^{-3}$	$20.392 \cdot 10^{-3}$	$33.153 \cdot 10^{-3}$
12	$10.643 \cdot 10^{-3}$	$23.763 \cdot 10^{-3}$	$35.915 \cdot 10^{-3}$
13	$10.599 \cdot 10^{-3}$	$25.477 \cdot 10^{-3}$	$38.677 \cdot 10^{-3}$
14	$17.906 \cdot 10^{-3}$	$27.229 \cdot 10^{-3}$	$41.439 \cdot 10^{-3}$
15	$18.167 \cdot 10^{-3}$	$30.742 \cdot 10^{-3}$	$44.201 \cdot 10^{-3}$

Table 5.2: Maximum values of the left-hand side (LHS) of (5.18) and values of the right-hand side (RHS) of (5.18) for $q = 3^{11}$ and $U = \widehat{\mathbb{F}_q^*}$.

$\max(K, L)$	LHS with $K = L$	LHS with $K \neq L$	RHS
1	cannot occur	$2.375 \cdot 10^{-3}$	$4.757 \cdot 10^{-3}$
2	$0.000 \cdot 10^{-3}$	$2.375 \cdot 10^{-3}$	$7.133 \cdot 10^{-3}$
3	cannot occur	$3.558 \cdot 10^{-3}$	$9.509 \cdot 10^{-3}$
4	$2.669 \cdot 10^{-3}$	$4.613 \cdot 10^{-3}$	$11.885 \cdot 10^{-3}$
5	$2.375 \cdot 10^{-3}$	$8.936 \cdot 10^{-3}$	$14.261 \cdot 10^{-3}$
6	$8.941 \cdot 10^{-3}$	$12.159 \cdot 10^{-3}$	$16.637 \cdot 10^{-3}$
7	$9.411 \cdot 10^{-3}$	$11.133 \cdot 10^{-3}$	$19.013 \cdot 10^{-3}$
8	$10.755 \cdot 10^{-3}$	$13.412 \cdot 10^{-3}$	$21.388 \cdot 10^{-3}$
9	$10.549 \cdot 10^{-3}$	$15.755 \cdot 10^{-3}$	$23.764 \cdot 10^{-3}$
10	$15.333 \cdot 10^{-3}$	$16.663 \cdot 10^{-3}$	$26.140 \cdot 10^{-3}$
11	$15.651 \cdot 10^{-3}$	$23.759 \cdot 10^{-3}$	$28.516 \cdot 10^{-3}$
12	$15.333 \cdot 10^{-3}$	$26.135 \cdot 10^{-3}$	$30.892 \cdot 10^{-3}$

Definition. Let $\boldsymbol{A} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \dots)$ with $\boldsymbol{a}_j \in [0,1)^\kappa$ for each j. We say that $\boldsymbol{A}$ is *uniformly distributed*[2] *in* $[0,1)^\kappa$ if

$$\lim_{n\to\infty} \frac{X_{\boldsymbol{A}}([\boldsymbol{c},\boldsymbol{d});n)}{n} = \prod_{j=1}^{\kappa}(d_j - c_j) \tag{5.19}$$

for all intervals $[\boldsymbol{c},\boldsymbol{d}) \subseteq [0,1)^\kappa$.

In general, the condition (5.19) is hard to check. The following theorem, which is known as *Weyl's criterion*, gives an equivalent condition on a sequence to be uniformly distributed in $[0,1)^\kappa$. For $\boldsymbol{a},\boldsymbol{b} \in \mathbb{R}^\kappa$, the *inner product* of $\boldsymbol{a}$ and $\boldsymbol{b}$ is

$$\langle \boldsymbol{a},\boldsymbol{b}\rangle = a_1b_1 + a_2b_2 + \cdots + a_\kappa b_\kappa.$$

Theorem 5.4.1 ([78, Theorem 6.2])**.** *Let $\boldsymbol{A} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \dots)$ with $\boldsymbol{a}_j \in [0,1)^\kappa$ for each j. Then $\boldsymbol{A}$ is uniformly distributed in $[0,1)^\kappa$ if and only if, for each $\boldsymbol{k} \in \mathbb{Z}^\kappa \setminus \{\boldsymbol{0}\}$, we have*

$$\lim_{n\to\infty} \frac{1}{n}\sum_{j=1}^{n} e^{2\pi i\langle \boldsymbol{k},\boldsymbol{a}_j\rangle} = 0.$$

In order to prove our equidistribution results on the vectors (5.15), we shall need two more lemmas.

The number of prime divisors

For a positive integer n, let $\omega(n)$ be the number of distinct prime divisors of n. It is plain that, if p is a prime, then $\omega(p^m) = 1$ for each positive integer m. The average order of growth of $\omega(n)$ is known (see [53, Theorem 430], for example): We have, as $n \to \infty$,

$$\frac{1}{n}\sum_{j=1}^{n}\omega(j) = \log\log n + O(1). \tag{5.20}$$

We are particularly interested in the number of prime divisors of Mersenne numbers $2^m - 1$. If such a number is a prime, then it is called a *Mersenne prime*. It is easy to see that if $2^m - 1$ is a prime, then m must be a prime – the converse is false: $2^{11} - 1 = 23 \cdot 89$. However, it is believed by many mathematicians that there are infinitely many Mersenne primes (see [76, Section 2.9], for example).

Now let p be an arbitrary prime. To our knowledge, the best known upper bound on infinitely many values of $\omega(n)$ for $n = p^m - 1$ is of order $\log n/\log\log n$, which is very weak compared to the average order of growth of $\omega(n)$ given in (5.20). The bound comes from

[2]We note that [78] defines *uniform distribution modulo* 1 *in* $\mathbb{R}^\kappa$ for general sequences with entries in $\mathbb{R}^\kappa$ by reducing each component of each entry modulo 1. For the sake of simplicity, we restrict ourselves to sequences with entries in $[0,1)^\kappa$.

the next result, which bounds $\omega(n)$ in the "worst case scenario": Let n take values in the infinite set

$$\{2,\, 2\cdot 3,\, 2\cdot 3\cdot 5,\, 2\cdot 3\cdot 5\cdot 7,\, 2\cdot 3\cdot 5\cdot 7\cdot 11,\, \dots\}$$

of primorials. Then it is known [53, Section 22.10] that

$$\frac{\omega(n)\log\log n}{\log n} \to 1$$

as $n \to \infty$. In particular, we have the following result.

Lemma 5.4.2 ([53])**.** *Let $\epsilon > 0$. There exists n_0 such that, for each integer $n > n_0$, we have*

$$\omega(n) < (1+\epsilon)\frac{\log n}{\log\log n}.$$

We shall also need the following inequality, which arises from the inclusion-exclusion principle.

Lemma 5.4.3. *Let $n > 1$ be an integer, and let $f\colon (\mathbb{Z}/n\mathbb{Z}, +) \to \mathbb{C}$ be an arbitrary function. Then*

$$\left|\sum_{\substack{d\in\mathbb{Z}/n\mathbb{Z}\\ \gcd(d,n)=1}} f(d)\right| \le 2^{\omega(n)} \max_U \left|\sum_{d\in U} f(d)\right|,$$

where the maximum is taken over all subgroups U of $\mathbb{Z}/n\mathbb{Z}$.

Proof. If n is a prime, then the lemma follows from

$$\sum_{\substack{d\in\mathbb{Z}/n\mathbb{Z}\\ \gcd(d,n)=1}} f(d) = \sum_{d\in\mathbb{Z}/n\mathbb{Z}} f(d) - f(0),$$

the triangle inequality, and $\omega(n) = 1$. Therefore, assume that n is not prime. Let $p_1, \dots, p_{\omega(n)}$ be the distinct prime divisors of n, and let U_i be the (unique) Sylow p_i-subgroup of $\mathbb{Z}/n\mathbb{Z}$ for each $i = 1, \dots, \omega(n)$. Writing

$$V = \bigcup_{i=1}^{\omega(n)} U_i,$$

we have

$$\sum_{\substack{d\in\mathbb{Z}/n\mathbb{Z}\\ \gcd(d,n)=1}} f(d) = \sum_{d\in\mathbb{Z}/n\mathbb{Z}} f(d) - \sum_{d\in V} f(d).$$

For non-empty $I \subseteq \{1, \dots, \omega(n)\}$, write

$$U_I = \bigcap_{i\in I} U_i$$

and obtain via the inclusion–exclusion principle

$$\sum_{\substack{d\in\mathbb{Z}/n\mathbb{Z}\\ \gcd(d,n)=1}} f(d) = \sum_{d\in\mathbb{Z}/n\mathbb{Z}} f(d) - \sum_{\substack{I\subseteq\{1,\dots,\omega(n)\}\\ I\neq\varnothing}} (-1)^{|I|-1} \sum_{d\in U_I} f(d).$$

The lemma now follows from the triangle inequality since the power set of $\{1,\dots,\omega(n)\}$ is of size $2^{\omega(n)}$. □

Equidistribution of the vectors (5.15)

Combining Conjecture 5.3.5 and Theorem 5.4.1, we obtain the following result.

Corollary 5.4.4. *Assume that Conjecture 5.3.5 is true, let p be a prime, and let H be a positive integer. Write $\kappa = \kappa_p(H)$, where $\kappa_p(H)$ is defined in (5.13). Define $\boldsymbol{B} = (b_1, b_2, \dots, b_\kappa)$ to be the vector that contains all κ positive integers that are at most H and are coprime to p in ascending order.*

Let q take values in the powers of p. For each q, write $n = q-1$, let χ be a primitive multiplicative character of $\mathbb{F}_q$, define $\boldsymbol{D}_n = (d_1, d_2, \dots, d_{\varphi(n)})$ to be the vector that contains all $\varphi(n)$ positive integers that are at most n and are coprime to n in ascending order, and let $\boldsymbol{A}_n = (\boldsymbol{a}_1, \boldsymbol{a}_2, \dots, \boldsymbol{a}_{\varphi(n)})$, where

$$\boldsymbol{a}_j = \big(\Psi_\chi(b_1, d_j), \Psi_\chi(b_2, d_j), \dots, \Psi_\chi(b_\kappa, d_j)\big)$$

for each $j = 1, 2, \dots, \varphi(n)$ and Ψ_χ is defined in (5.14). Then $\boldsymbol{A}_n$ becomes uniformly distributed in $[0,1)^\kappa$ as $n \to \infty$.

Proof. Let $\boldsymbol{k} = (k_1, \dots, k_\kappa) \in \mathbb{Z}^\kappa \setminus \{\boldsymbol{0}\}$. We have

$$\begin{aligned}\sum_{j=1}^{\varphi(n)} e^{2\pi i\langle \boldsymbol{k}, \boldsymbol{a}_j\rangle} &= \sum_{j=1}^{\varphi(n)} \prod_{h=1}^{\kappa} e^{2\pi i k_h \Psi_\chi(b_h, d_j)} \\ &= \sum_{\substack{d=1\\ \gcd(d,n)=1}}^{n-1} \prod_{h=1}^{\kappa} e^{2\pi i k_h \Psi_\chi(b_h, d)} \\ &= \sum_{\substack{d=1\\ \gcd(d,n)=1}}^{n-1} \prod_{h=1}^{\kappa} \left(\frac{G(\chi^{b_h d})}{\sqrt{q}}\right)^{k_h}.\end{aligned}$$

Therefore, by Lemma 5.4.3 we have

$$\left|\sum_{j=1}^{\varphi(n)} e^{2\pi i\langle \boldsymbol{k}, \boldsymbol{a}_j\rangle}\right| \le 2^{\omega(n)} \max_U \left|\sum_{d\in U} \prod_{h=1}^{\kappa} \left(\frac{G(\chi^{b_h d})}{\sqrt{q}}\right)^{k_h}\right|,$$

where the maximum is taken over all subgroups U of $\mathbb{Z}/n\mathbb{Z}$. Equivalently,

$$\left|\sum_{j=1}^{\varphi(n)} e^{2\pi i\langle \boldsymbol{k},\boldsymbol{a}_j\rangle}\right| \le 2^{\omega(n)} \max_{U} \left|\sum_{\chi\in U}\prod_{h=1}^{\kappa}\left(\frac{G(\chi^{b_h})}{\sqrt{q}}\right)^{k_h}\right|,$$

where the maximum is now taken over all subgroups U of $\widehat{\mathbb{F}_q^*}$. Writing $K=\sum_{h=1}^{\kappa} b_h|k_h|$, we find from Conjecture 5.3.5 that

$$\frac{1}{\varphi(n)}\left|\sum_{j=1}^{\varphi(n)} e^{2\pi i\langle \boldsymbol{k},\boldsymbol{a}_j\rangle}\right| \le \frac{2^{\omega(n)}\sqrt{n}}{\varphi(n)}(K+2),$$

where we have used

$$n\left(\frac{K+1}{\sqrt{n+1}}+\frac{1}{n+1}\right) \le \sqrt{n}(K+2).$$

It is known [106, Section 4.6.2, Fact 11] that $\varphi(n) > n/(6\log\log n)$ for $n>4$. For all sufficiently large n, we have $\omega(n) < 2\log n/\log\log n$ by Lemma 5.4.2 with $\epsilon=1$. Therefore, for all sufficiently large n, we have

$$\frac{1}{\varphi(n)}\left|\sum_{j=1}^{\varphi(n)} e^{2\pi i\langle \boldsymbol{k},\boldsymbol{a}_j\rangle}\right| \le \frac{2^{\frac{2\log n}{\log\log n}}\log\log n}{\sqrt{n}}(6K+12). \tag{5.21}$$

Using

$$\frac{2^{\frac{2\log n}{\log\log n}}\log\log n}{\sqrt{n}} = e^{\frac{2\log 2\log n}{\log\log n}+\log\log n-\frac{1}{2}\log n},$$

it is readily verified that the right-hand side of (5.21) tends to zero as $n\to\infty$, so that Theorem 5.4.1 completes the proof. □

In order to prove our main results we shall need a stronger version of Corollary 5.4.4. Therefore, we now undertake a quantitative analysis of the distribution uniformity for the vectors (5.15). In the proof of the next theorem, which will be the key ingredient in the proof of our main results, we explicitly carry out the equidistribution argument of Theorem 5.4.1. Define $T^{\kappa}=(\mathbb{R}/\mathbb{Z})^{\kappa}$ to be an κ-dimensional torus.

Theorem 5.4.5. *Assume that Conjecture 5.3.5 is true and let p be a prime. Let q take values in the powers of p. For each q, let χ be a primitive multiplicative character of $\mathbb{F}_q$. For each positive integer H, write $\kappa=\kappa_p(H)$, and define $\boldsymbol{B}=(b_1,b_2,\ldots,b_\kappa)$ to be the vector that contains all κ positive integers that are at most H and are coprime to p in ascending order.*

Then, for all sufficiently large $n=q-1$, each positive integer H with $\kappa\le 0.720\log\log n$, and each $\boldsymbol{y}=(y_1,y_2,\ldots,y_\kappa)\in T^{\kappa}$, there exists an integer d with $\gcd(d,n)=1$ such that

$$\left|y_h+\Psi_{\chi}(b_h,d)\right| \le \frac{1}{8}$$

for all $h=1,2,\ldots,\kappa$.

Proof. For $\boldsymbol{z} = (z_1, \dots, z_\kappa) \in T^\kappa$, define

$$\gamma(\boldsymbol{z}) = \begin{cases} 1 & \text{if } |z_h| \leq \frac{1}{16} \text{ for all } h = 1, \dots, \kappa \\ 0 & \text{otherwise} \end{cases}$$

to be the indicator function of $[-1/16, 1/16]^\kappa$, and let g be the convolution of γ with itself, which is

$$g(\boldsymbol{z}) = \int_{T^\kappa} \gamma(\boldsymbol{x})\gamma(\boldsymbol{z} - \boldsymbol{x})d\boldsymbol{x}.$$

If $g(\boldsymbol{z}) \neq 0$ for some $\boldsymbol{z} \in T^\kappa$, then there exists $\boldsymbol{x} \in T^\kappa$ such that $\gamma(\boldsymbol{x}) \neq 0$ and $\gamma(\boldsymbol{z} - \boldsymbol{x}) \neq 0$. This means that $\boldsymbol{x}, \boldsymbol{z} - \boldsymbol{x} \in [-1/16, 1/16]^\kappa$ and hence $\boldsymbol{z} \in [-1/8, 1/8]^\kappa$. Therefore, our goal is to show the existence of an integer d with $\gcd(d, n) = 1$ such that $g(\boldsymbol{u}(d) + \boldsymbol{y}) \neq 0$, where the function $\boldsymbol{u}$ is given by

$$\boldsymbol{u} \colon \mathbb{Z} \to T^\kappa, \qquad d \mapsto \big(\Psi_\chi(b_1, d), \dots, \Psi_\chi(b_\kappa, d)\big).$$

Define

$$\tau \colon \mathbb{Z} \to \mathbb{R}, \qquad k \mapsto \begin{cases} \frac{1}{8} & \text{for } k = 0 \\ \frac{\sin(\pi k/8)}{\pi k} & \text{for } k \neq 0. \end{cases}$$

Then

$$\int_{-1/16}^{1/16} e^{-2\pi i k x} dx = \tau(k),$$

so that the Fourier series of γ is

$$\gamma(\boldsymbol{z}) = \sum_{\boldsymbol{k} \in \mathbb{Z}^\kappa} \left(\prod_{h=1}^{\kappa} \tau(k_h) \right) e^{2\pi i \langle \boldsymbol{k}, \boldsymbol{z} \rangle}.$$

Therefore, the Fourier series of g is

$$g(\boldsymbol{z}) = \sum_{\boldsymbol{k} \in \mathbb{Z}^\kappa} r(\boldsymbol{k}) e^{2\pi i \langle \boldsymbol{k}, \boldsymbol{z} \rangle},$$

where

$$r(\boldsymbol{k}) = \prod_{h=1}^{\kappa} \big(\tau(k_h)\big)^2.$$

We now show that the Fourier series of g converges absolutely. Define

$$\lambda\colon \mathbb{Z} \to \mathbb{R}, \quad k \mapsto \begin{cases} \frac{1}{64} & \text{for } |k| \le 2 \\ \frac{1}{\pi^2 k^2} & \text{for } |k| > 2. \end{cases}$$

Then we have

$$\begin{aligned} \sum_{k\in\mathbb{Z}} \lambda(k) &= \frac{5}{64} + \frac{2}{\pi^2} \sum_{k=3}^{\infty} \frac{1}{k^2} \\ &= \frac{79}{192} - \frac{5}{2\pi^2} \end{aligned} \tag{5.22}$$

using Euler's evaluation $\sum_{k=1}^{\infty} 1/k^2 = \pi^2/6$. Since

$$r(\boldsymbol{k}) \le \prod_{h=1}^{\kappa} \lambda(k_h) \tag{5.23}$$

for each $\boldsymbol{k} \in \mathbb{Z}^\kappa$, we have

$$\begin{aligned} \sum_{\boldsymbol{k}\in\mathbb{Z}^\kappa} \left| r(\boldsymbol{k}) e^{2\pi i \langle \boldsymbol{k}, \boldsymbol{z}\rangle} \right| &\le \sum_{\boldsymbol{k}\in\mathbb{Z}^\kappa} \prod_{h=1}^{\kappa} \lambda(k_h) \\ &= \left(\sum_{k\in\mathbb{Z}} \lambda(k) \right)^{\kappa} \\ &= \left(\frac{79}{192} - \frac{5}{2\pi^2} \right)^{\kappa} \end{aligned}$$

by (5.22). Since the Fourier series of g is absolutely converging, we have

$$\begin{aligned} \sum_{\substack{d=1 \\ \gcd(d,n)=1}}^{n-1} g(\boldsymbol{u}(d) + \boldsymbol{y}) &= \sum_{\boldsymbol{k}\in\mathbb{Z}^\kappa} r(\boldsymbol{k}) e^{2\pi i \langle \boldsymbol{k}, \boldsymbol{y}\rangle} \sum_{\substack{d=1 \\ \gcd(d,n)=1}}^{n-1} e^{2\pi i \langle \boldsymbol{k}, \boldsymbol{u}(d)\rangle} \\ &= \sum_{\boldsymbol{k}\in\mathbb{Z}^\kappa} r(\boldsymbol{k}) e^{2\pi i \langle \boldsymbol{k}, \boldsymbol{y}\rangle} \sum_{\substack{d=1 \\ \gcd(d,n)=1}}^{n-1} \prod_{h=1}^{\kappa} e^{2\pi i k_h \Psi_\chi(b_h, d)} \\ &= \sum_{\boldsymbol{k}\in\mathbb{Z}^\kappa} r(\boldsymbol{k}) e^{2\pi i \langle \boldsymbol{k}, \boldsymbol{y}\rangle} \sum_{\substack{d=1 \\ \gcd(d,n)=1}}^{n-1} \prod_{h=1}^{\kappa} \left(\frac{G(\chi^{b_h d})}{\sqrt{q}} \right)^{k_h}. \end{aligned}$$

Write

$$S(\boldsymbol{k}) = \sum_{\substack{d=1 \\ \gcd(d,n)=1}}^{n-1} \prod_{h=1}^{\kappa} \left(\frac{G(\chi^{b_h d})}{\sqrt{q}} \right)^{k_h}. \tag{5.24}$$

Extracting the term corresponding to $\boldsymbol{k} = \mathbf{0}$, we obtain by the triangle inequality

$$\left| \sum_{\substack{d=1 \\ \gcd(d,n)=1}}^{n-1} g(\boldsymbol{u}(d) + \boldsymbol{y}) - \frac{\varphi(n)}{64^\kappa} \right| \leq \sum_{\boldsymbol{k} \in \mathbb{Z}^\kappa \setminus \{\mathbf{0}\}} r(\boldsymbol{k}) |S(\boldsymbol{k})| \tag{5.25}$$

since $S(\mathbf{0}) = \varphi(n)$ and $r(\mathbf{0}) = 1/64^\kappa$. Using Lemma 5.4.3 we have by Conjecture 5.3.5 that

$$|S(\boldsymbol{k})| < 2^{\omega(n)} \sqrt{n} \left(2 + \sum_{h=1}^{\kappa} b_h |k_h| \right) \tag{5.26}$$

for each $\boldsymbol{k} \neq \mathbf{0}$, where we have used

$$n \left(\frac{1 + \sum_{h=1}^{\kappa} b_h |k_h|}{\sqrt{n+1}} + \frac{1}{n+1} \right) < \sqrt{n} \left(2 + \sum_{h=1}^{\kappa} b_h |k_h| \right).$$

Let μ be a positive real number to be chosen later. We now partition the summation range on the right-hand side of (5.25) into the cases distinguishing $\max_h |k_h| \leq \mu$ and $\max_h |k_h| > \mu$. We will obtain an estimate on the sum where $\max_h |k_h| \leq \mu$ using (5.26), while for the sum where $\max_h |k_h| > \mu$ we will bound $|S(\boldsymbol{k})|$ trivially by $\varphi(n)$, which is just the number of summands of $S(\boldsymbol{k})$ in (5.24). By (5.25) we then have

$$\left| \sum_{\substack{d=1 \\ \gcd(d,n)=1}}^{n-1} g(\boldsymbol{u}(d) + \boldsymbol{y}) - \frac{\varphi(n)}{64^\kappa} \right| < \Sigma_1 + \Sigma_2, \tag{5.27}$$

where

$$\Sigma_1 = 2^{\omega(n)} \sqrt{n} \sum_{\substack{\boldsymbol{k} \in \mathbb{Z}^\kappa \setminus \{\mathbf{0}\} \\ \max_h |k_h| \leq \mu}} r(\boldsymbol{k}) \left(2 + \sum_{h=1}^{\kappa} b_h |k_h| \right),$$

$$\Sigma_2 = \varphi(n) \sum_{\substack{\boldsymbol{k} \in \mathbb{Z}^\kappa \\ \max_h |k_h| > \mu}} r(\boldsymbol{k}).$$

We now provide upper bounds on Σ_1 and Σ_2.

Using $|\tau(k_h)| \leq 1/8$, we have $r(\boldsymbol{k}) \leq 1/64^\kappa$ for each $\boldsymbol{k} \in \mathbb{Z}^\kappa$. Therefore,

$$\begin{aligned}
\Sigma_1 &\leq \frac{2^{\omega(n)}}{64^\kappa} \sqrt{n} \sum_{\substack{\boldsymbol{k} \in \mathbb{Z}^\kappa \setminus \{\mathbf{0}\} \\ \max_h |k_h| \leq \mu}} \left(2 + \mu \sum_{h=1}^{\kappa} b_h \right) \\
&\leq \frac{2^{\omega(n)}}{64^\kappa} \sqrt{n} \sum_{\substack{\boldsymbol{k} \in \mathbb{Z}^\kappa \setminus \{\mathbf{0}\} \\ \max_h |k_h| \leq \mu}} \left(2 + \mu \frac{H(H+1)}{2} \right) \\
&\leq \frac{2^{\omega(n)}}{64^\kappa} \left(2 + \mu \frac{H(H+1)}{2} \right) \big((2\mu + 1)^\kappa - 1 \big) \sqrt{n},
\end{aligned}$$

where we have used

$$\sum_{h=1}^{\kappa} b_h \le \sum_{h=1}^{H} h = \frac{H(H+1)}{2}$$

in the second step.

In order to estimate Σ_2, we make use of $\varphi(n) < n$ and (5.23), to obtain

$$\begin{aligned}
\Sigma_2 &< n \sum_{\substack{\boldsymbol{k}\in\mathbb{Z}^\kappa \\ \max_h |k_h|>\mu}} \prod_{h=1}^{\kappa} \lambda(k_h) \\
&\le 2\kappa n \sum_{\substack{\boldsymbol{k}\in\mathbb{Z}^\kappa \\ k_1>\mu}} \prod_{h=1}^{\kappa} \lambda(k_h) \\
&\le 2\kappa n \sum_{\substack{\boldsymbol{k}\in\mathbb{Z}^\kappa \\ k_1>\mu}} \frac{1}{\pi^2 k_1^2} \prod_{h=2}^{\kappa} \lambda(k_h) \\
&= \frac{2\kappa n}{\pi^2} \sum_{k_1>\mu} \frac{1}{k_1^2} \prod_{h=2}^{\kappa} \sum_{k_h\in\mathbb{Z}} \lambda(k_h).
\end{aligned}$$

Using (5.22) and

$$\sum_{k_1>\mu} \frac{1}{k_1^2} \le \sum_{k_1>\mu} \frac{1}{(k_1-1)k_1} = \sum_{k_1>\mu} \left(\frac{1}{k_1-1} - \frac{1}{k_1}\right) \le \frac{1}{\mu-1},$$

we obtain

$$\Sigma_2 < \frac{2\kappa n}{\pi^2(\mu-1)} \left(\frac{79}{192} - \frac{5}{2\pi^2}\right)^{\kappa-1}.$$

Finally, combining the bounds on Σ_1 and Σ_2, we find that the left-hand side of (5.27) is smaller than

$$\frac{2^{\omega(n)}}{64^\kappa} \left(2 + \mu \frac{H(H+1)}{2}\right) \left((2\mu+1)^\kappa - 1\right) \sqrt{n} + \frac{2\kappa n}{\pi^2(\mu-1)} \left(\frac{79}{192} - \frac{5}{2\pi^2}\right)^{\kappa-1}.$$

We choose μ such that the two terms are (almost) equal, more precisely

$$\mu = 32 \left(\frac{79}{192} - \frac{5}{2\pi^2}\right) n^{\frac{1}{2\kappa+4}},$$

so that

$$5.060 \cdot n^{\frac{1}{2\kappa+4}} < \mu < 5.061 \cdot n^{\frac{1}{2\kappa+4}}.$$

Then, for all sufficiently large n, we have

$$\left| \sum_{\substack{d=1 \\ \gcd(d,n)=1}}^{n-1} g(\boldsymbol{u}(d) + \boldsymbol{y}) - \frac{\varphi(n)}{64^\kappa} \right| < 5.061 \cdot H^2 \cdot 0.159^\kappa 2^{\omega(n)} n^{1-\frac{1}{2\kappa+4}}.$$

It is known [106, Section 4.6.2, Fact 11] that $\varphi(n) > n/(6\log\log n)$ for $n > 4$. By Lemma 5.4.2 with $\epsilon = 0.001$, we have $\omega(n) < 1.001\log n/\log\log n$. Thus, if

$$\frac{n}{6\log\log n \cdot 64^{\kappa}} \geq 5.061 \cdot H^2 \cdot 0.159^{\kappa} 2^{\omega(n)} n^{1-\frac{1}{2\kappa+4}}, \tag{5.28}$$

then

$$\left| \sum_{\substack{d=1 \\ \gcd(d,n)=1}}^{n-1} g(\boldsymbol{u}(d)+\boldsymbol{y}) \right| \neq 0,$$

and there exists $d \in \{1,\ldots,n-1\}$ with $\gcd(d,n) = 1$ such that $g(\boldsymbol{u}(d)+\boldsymbol{y}) \neq 0$, which completes the proof. For (5.28) to be valid it is enough that

$$\kappa \leq (2 \cdot 1.001 \cdot \log 2 + 0.001)^{-1} \log\log n,$$

provided that n is large enough. The proof is completed by noting that

$$0.720 < (2 \cdot 1.001 \cdot \log 2 + 0.001)^{-1}. \qquad \square$$

5.5 Large character sums and large peak sidelobe levels

In order to prove our main results, we shall need two technical lemmas that give bounds on specific sums that involve Dirichlet kernels.

Lemma 5.5.1. *Let n be an odd positive integer and H be a positive integer with $H \leq n/38$. Then*

$$\sum_{\substack{h=1 \\ h\ odd}}^{H} \left| D_{\frac{n+1}{2}}\left(\frac{-h}{n}\right) \right| \left(1 - \frac{h}{H}\right) > \frac{0.9991}{2\pi} n \log H - \frac{1}{2} n$$

and

$$\sum_{\substack{h=2 \\ h\ even}}^{H} \left| D_{\frac{n+1}{2}}\left(\frac{-h}{n}\right) \right| \left(1 - \frac{h}{H}\right) \leq \frac{\pi}{8} H.$$

Proof. From (5.3) we find that

$$\left| D_{\frac{n+1}{2}}\left(\frac{-h}{n}\right) \right| = \left| \frac{\sin\left(\frac{\pi h}{2} + \frac{\pi h}{2n}\right)}{\sin\left(\frac{\pi h}{n}\right)} \right| \tag{5.29}$$

for each $h \not\equiv 0 \pmod{n}$.

We begin with proving the first statement. Using (5.29) and $|\sin(\pi h/2 + x)| = |\cos(x)|$

for odd h and real x, we have

$$\sum_{\substack{h=1\\ h\,\text{odd}}}^{H} \left|D_{\frac{n+1}{2}}\Big(\frac{-h}{n}\Big)\right|\Big(1-\frac{h}{H}\Big) = \sum_{\substack{h=1\\ h\,\text{odd}}}^{H} \frac{\cos\big(\frac{\pi h}{2n}\big)}{\sin\big(\frac{\pi h}{n}\big)}\Big(1-\frac{h}{H}\Big).$$

Using

$$\cos\Big(\frac{\pi h}{2n}\Big) \ge \cos\Big(\frac{\pi H}{2n}\Big) \ge \cos\Big(\frac{\pi}{76}\Big) > 0.9991$$

for all $h \in \{1,\dots,H\}$, and $|x| \ge |\sin x|$ for real x, we obtain

$$\begin{aligned}\sum_{\substack{h=1\\ h\,\text{odd}}}^{H} \left|D_{\frac{n+1}{2}}\Big(\frac{-h}{n}\Big)\right|\Big(1-\frac{h}{H}\Big) &> \frac{0.9991}{\pi} n \sum_{\substack{h=1\\ h\,\text{odd}}}^{H} \Big(\frac{1}{h}-\frac{1}{H}\Big)\\ &\ge \frac{0.9991}{\pi} n\Bigg(-\frac{H+1}{2H} + \sum_{1\le h\le (H+1)/2} \frac{1}{2h-1}\Bigg)\end{aligned}$$

since $\sum_{h=1,\,h\,\text{odd}}^{H} 1 \le (H+1)/2$. Using

$$\frac{1}{2h-1} > \frac{1}{2h} \quad \text{and} \quad \sum_{1\le h\le (H+1)/2} \frac{1}{h} \ge \log H - \log 2,$$

we have

$$\sum_{\substack{h=1\\ h\,\text{odd}}}^{H} \left|D_{\frac{n+1}{2}}\Big(\frac{-h}{n}\Big)\right|\Big(1-\frac{h}{H}\Big) > \frac{0.9991}{2\pi} n\Big(\log H - \log 2 - \frac{H+1}{H}\Big).$$

The first part of the lemma is proved by noting that

$$\frac{0.9991}{2\pi}\Big(\log 2 + \frac{H+1}{H}\Big) < \frac{1}{2}.$$

In order to prove the second statement, we use (5.29) and $|\sin(\pi h/2 + x)| = |\sin(x)|$ for even h and real x, to obtain

$$\sum_{\substack{h=2\\ h\,\text{even}}}^{H} \left|D_{\frac{n+1}{2}}\Big(\frac{-h}{n}\Big)\right|\Big(1-\frac{h}{H}\Big) = \sum_{\substack{h=2\\ h\,\text{even}}}^{H} \frac{\sin\big(\frac{\pi h}{2n}\big)}{\sin\big(\frac{\pi h}{n}\big)}\Big(1-\frac{h}{H}\Big).$$

Now use $2x/\pi < \sin x < x$ for $0 < x < \pi/2$ to obtain

$$\sum_{\substack{h=2\\ h\,\text{even}}}^{H} \left|D_{\frac{n+1}{2}}\Big(\frac{-h}{n}\Big)\right|\Big(1-\frac{h}{H}\Big) \le \frac{\pi}{4} \sum_{\substack{h=2\\ h\,\text{even}}}^{H} \Big(1-\frac{h}{H}\Big).$$

The proof is completed by noting that

$$\sum_{\substack{h=2\\ h\,\text{even}}}^{H}\left(1-\frac{h}{H}\right)\le\frac{H}{2}. \qquad \square$$

Lemma 5.5.2. *Let k be an odd integer with $k>2$ and let n be a positive integer with $n+1\equiv 0 \pmod k$. Let H be an integer with $1<H\le kn/76$. Then*

$$\sum_{\substack{h=2\\ h\ even\\ h\not\equiv 0\,(\mathrm{mod}\ k)}}^{H}\left|D_{\frac{n+1}{k}}\left(\frac{-h}{n}\right)\right|\left(1-\frac{h}{H}\right)>\frac{0.9991(k-1)}{\pi k^2}n\log H-n$$

and

$$\sum_{\substack{h=2\\ h\ even\\ h\equiv 0\,(\mathrm{mod}\ k)}}^{H}\left|D_{\frac{n+1}{k}}\left(\frac{-h}{n}\right)\right|\left(1-\frac{h}{H}\right)\le\frac{\pi}{4k^2}H.$$

Proof. From (5.3) we find that

$$\left|D_{\frac{n+1}{k}}\left(\frac{-h}{n}\right)\right|=\left|\frac{\sin\left(\frac{\pi h}{k}+\frac{\pi h}{kn}\right)}{\sin\left(\frac{\pi h}{n}\right)}\right|$$

for each $h\not\equiv 0 \pmod n$. Therefore, by the identity

$$\sin(x+y)=\sin(x)\cos(y)+\cos(x)\sin(y)$$

for real x and y, we have

$$\left|D_{\frac{n+1}{k}}\left(\frac{-h}{n}\right)\right|=\left|\frac{\sin\left(\frac{\pi h}{k}\right)\cos\left(\frac{\pi h}{kn}\right)+\cos\left(\frac{\pi h}{k}\right)\sin\left(\frac{\pi h}{kn}\right)}{\sin\left(\frac{\pi h}{n}\right)}\right| \tag{5.30}$$

for each $h\not\equiv 0 \pmod n$.

We begin with proving the first statement. By (5.30) and the triangle inequality, we have

$$\left|D_{\frac{n+1}{k}}\left(\frac{-h}{n}\right)\right|\ge\frac{\left|\sin\left(\frac{\pi h}{k}\right)\right|\cos\left(\frac{\pi h}{kn}\right)}{\sin\left(\frac{\pi h}{n}\right)}-\frac{\left|\cos\left(\frac{\pi h}{k}\right)\right|\sin\left(\frac{\pi h}{kn}\right)}{\sin\left(\frac{\pi h}{n}\right)}$$

for each $h=1,\dots,H$. Using $2x/\pi<\sin x<x$ for $0<x<\pi/2$ and

$$\cos\left(\frac{\pi h}{kn}\right)\ge\cos\left(\frac{\pi H}{kn}\right)\ge\cos\left(\frac{\pi}{76}\right)>0.9991$$

for $H \leq kn/76$, we obtain

$$\left| D_{\frac{n+1}{k}}\left(\frac{-h}{n}\right)\right| > \frac{1.9982}{k\pi h}n - \frac{\pi}{2k}$$

for each $h = 1, \ldots, H$ with $h \not\equiv 0 \pmod{k}$. Thus,

$$\sum_{\substack{h=2\\ h\,\text{even}\\ h\not\equiv 0\,(\mathrm{mod}\ k)}}^{H} \left| D_{\frac{n+1}{k}}\left(\frac{-h}{n}\right)\right|\left(1-\frac{h}{H}\right) > \frac{1.9982n}{k\pi} \sum_{\substack{h=2\\ h\,\text{even}\\ h\not\equiv 0\,(\mathrm{mod}\ k)}}^{H} \frac{1}{h} - \Delta, \tag{5.31}$$

where

$$\Delta = \left(\frac{1.9982n}{k\pi H} + \frac{\pi}{2k}\right) \sum_{\substack{h=2\\ h\,\text{even}\\ h\not\equiv 0\,(\mathrm{mod}\ k)}}^{H} 1 - \frac{\pi}{2kH} \sum_{\substack{h=2\\ h\,\text{even}\\ h\not\equiv 0\,(\mathrm{mod}\ k)}}^{H} h. \tag{5.32}$$

In what follows, we find a lower bound for the sum on the right-hand side of (5.31) and an upper bound for Δ.

Dropping the second sum in (5.32) and using

$$\sum_{\substack{h=2\\ h\,\text{even}\\ h\not\equiv 0\,(\mathrm{mod}\ k)}}^{H} 1 \leq \frac{H}{2},$$

we have

$$\Delta \leq \frac{0.9991n}{k\pi} + \frac{H\pi}{4k}.$$

By noting that $H \leq kn/76$, we have

$$\Delta < \frac{n}{8},$$

where we have used

$$\frac{0.9991}{2k\pi} + \frac{\pi}{304} < \frac{1}{8}.$$

On the other hand,

$$\begin{aligned}\sum_{\substack{h=2\\ h\,\text{even}\\ h\not\equiv 0\,(\mathrm{mod}\ k)}}^{H} \frac{1}{h} &= \sum_{1\leq h\leq H/2} \frac{1}{2h} - \sum_{\substack{1\leq h\leq H/2\\ h\equiv 0\,(\mathrm{mod}\ k)}} \frac{1}{2h}\\ &= \frac{1}{2}\sum_{1\leq h\leq H/2} \frac{1}{h} - \frac{1}{2k}\sum_{1\leq h\leq H/(2k)} \frac{1}{h}.\end{aligned}$$

since k is odd. Use

$$\log m \le \sum_{h=1}^{m} \frac{1}{h} \le \log m + 1 \tag{5.33}$$

for each positive integer m to obtain

$$\begin{aligned}\sum_{\substack{h=2\\ h\,\text{even}\\ h\not\equiv 0 \,(\mathrm{mod}\ k)}}^{H} \frac{1}{h} &\ge \frac{1}{2}\log\left(\frac{H-1}{2}\right) - \frac{1}{2k}\left(\log\left(\frac{H}{2k}\right)+1\right)\\ &> \frac{1}{2}\log(H-1) - \frac{1}{2}\log 2 - \frac{1}{2k}\log H\end{aligned}$$

using $\log(2k) > 1$. From (5.33) we deduce that

$$\log(H-1) \ge \log H - 1 - \frac{1}{H},$$

so that

$$\sum_{\substack{h=2\\ h\,\text{even}\\ h\not\equiv 0 \,(\mathrm{mod}\ k)}}^{H} \frac{1}{h} > \frac{k-1}{2k}\log H - 2,$$

where we have used

$$\frac{1}{2}\left(1 + \frac{1}{H} + \log 2\right) < 2.$$

Substitution of this and the bound on Δ into (5.31) gives

$$\sum_{\substack{h=2\\ h\,\text{even}\\ h\not\equiv 0 \,(\mathrm{mod}\ k)}}^{H} \left|D_{\frac{n+1}{k}}\left(\frac{-h}{n}\right)\right|\left(1 - \frac{h}{H}\right) > \frac{0.9991(k-1)}{\pi k^2} n\log H - n,$$

where we have used

$$\frac{2\cdot 1.9982}{k\pi} + \frac{1}{8} < 1,$$

as required.

We now prove the second statement. Since $\sin(h\pi) = 0$ and $|\cos(h\pi)| = 1$ for each integer h, we find from (5.30) that

$$\left|D_{\frac{n+1}{k}}\left(\frac{-h}{n}\right)\right| = \frac{\sin\left(\frac{\pi h}{kn}\right)}{\sin\left(\frac{\pi h}{n}\right)}$$

for each $h = 1, \ldots, H$ with $h \equiv 0 \pmod{k}$, so that

$$\left|D_{\frac{n+1}{k}}\left(\frac{-h}{n}\right)\right| < \frac{\pi}{2k}$$

for each $h = 1, \dots, H$ with $h \equiv 0 \pmod{k}$. Therefore,

$$\sum_{\substack{h=2 \\ h \text{ even} \\ h \equiv 0 \,(\mathrm{mod}\ k)}}^{H} \left| D_{\frac{n+1}{k}}\left(\frac{-h}{n}\right)\right|\left(1 - \frac{h}{H}\right) \leq \frac{\pi}{2k} \sum_{\substack{h=2 \\ h \text{ even} \\ h \equiv 0 \,(\mathrm{mod}\ k)}}^{H} \left(1 - \frac{h}{H}\right).$$

The proof is completed by noting that

$$\sum_{\substack{h=2 \\ h \text{ even} \\ h \equiv 0 \,(\mathrm{mod}\ k)}}^{H} \left(1 - \frac{h}{H}\right) \leq \frac{H}{2k}. \qquad \square$$

Main results

We now prove the main results of this chapter. The following theorem states that the additive character sums in (5.1) can become large in magnitude (in a precise sense).

Theorem 5.5.3. *Assume that Conjecture 5.3.5 is true and let p be a prime. For all sufficiently large $n = p^m - 1$ and each primitive element θ of $\mathbb{F}_{p^m}$, there exist integers t and d with $\gcd(d, n) = 1$ such that*

$$\left| \sum_{j=t}^{t+\frac{n+1}{p}-1} \psi_1\big(\theta^{dj}\big) \right| \geq \begin{cases} \frac{0.999}{\sqrt{2}\pi}\sqrt{n+1}\log\log\log n & \text{if } p = 2 \\ \frac{0.999\sqrt{2}(p-1)}{\pi p^2}\sqrt{n+1}\log\log\log n & \text{if } p \neq 2, \end{cases}$$

where ψ_1 is the canonical additive character of $\mathbb{F}_{p^m}$.

Proof. Let χ be the multiplicative character of $\mathbb{F}_{p^m}$ given by $\chi(\theta) = e^{2\pi i/n}$, and write

$$S(t, d) = \sum_{j=t}^{t+\frac{n+1}{p}-1} \psi_1\big(\theta^{dj}\big).$$

From Lemma 5.2.5 with $\ell = (n+1)/p$ we find that, for each integer d with $\gcd(d, n) = 1$ and each positive integer H with $H < n/2$, there exists an integer t such that

$$|S(t, d^{-1})| \geq \frac{1}{n}\left| \sum_{|h| \leq H} D_{\frac{n+1}{p}}\left(\frac{h}{n}\right) G\big(\chi^{-hd}\big)\left(1 - \frac{|h|}{H}\right)\right|.$$

Using $D_{(n+1)/p}(0) = (n+1)/p$ and Lemma 2.2.3 (ii), we extract the term corresponding to $h = 0$ and obtain via the triangle inequality

$$|S(t, d^{-1})| \geq \frac{1}{n}\left| \sum_{\substack{|h| \leq H \\ h \neq 0}} D_{\frac{n+1}{p}}\left(\frac{h}{n}\right) G\big(\chi^{-hd}\big)\left(1 - \frac{|h|}{H}\right)\right| - \frac{n+1}{np}.$$

We have $D_{(n+1)/p}(-x) = \overline{D_{(n+1)/p}(x)}$ for real x, and $G(\lambda^{-1}) = \lambda(-1)\overline{G(\lambda)}$ for each nontrivial multiplicative character λ of $\mathbb{F}_{p^m}$ by Lemma 2.2.3 (v). Thus, $|S(t, d^{-1})|$ is at least

$$\frac{1}{n}\left|\sum_{h=1}^{H}\left(D_{\frac{n+1}{p}}\left(\frac{-h}{n}\right)G\big(\chi^{hd}\big) + \overline{D_{\frac{n+1}{p}}\left(\frac{-h}{n}\right)G\big(\chi^{hd}\big)\chi^{hd}(-1)}\right)\left(1-\frac{h}{H}\right)\right| - \frac{n+1}{pn}. \tag{5.34}$$

We now distinguish the cases that p is even or odd.

Case 1. $p = 2$. Then $\chi^{hd}(-1) = 1$ for each h, so that we find from (5.34) that

$$|S(t, d^{-1})| \geq \frac{2}{n}\left|\operatorname{Re}\left(\sum_{h=1}^{H} D_{\frac{n+1}{2}}\left(\frac{-h}{n}\right)G\big(\chi^{hd}\big)\left(1-\frac{h}{H}\right)\right)\right| - \frac{n+1}{2n}.$$

Separating the sum into two sums (one corresponding to the odd h and one to the even h), and then applying the triangle inequality, we obtain

$$\begin{aligned}|S(t, d^{-1})| \geq &\frac{2}{n}\left|\operatorname{Re}\left(\sum_{\substack{h=1\\ h\,\text{odd}}}^{H} D_{\frac{n+1}{2}}\left(\frac{-h}{n}\right)G\big(\chi^{hd}\big)\left(1-\frac{h}{H}\right)\right)\right| \\ &- \frac{2}{n}\left|\operatorname{Re}\left(\sum_{\substack{h=2\\ h\,\text{even}}}^{H} D_{\frac{n+1}{2}}\left(\frac{-h}{n}\right)G\big(\chi^{hd}\big)\left(1-\frac{h}{H}\right)\right)\right| - \frac{n+1}{2n}.\end{aligned}$$

Applying the triangle inequality to the second sum, using Lemma 2.2.3 (iv), and then the second part of Lemma 5.5.1, we have

$$|S(t, d^{-1})| \geq \frac{2}{n}\left|\operatorname{Re}\left(\sum_{\substack{h=1\\ h\,\text{odd}}}^{H} D_{\frac{n+1}{2}}\left(\frac{-h}{n}\right)G\big(\chi^{hd}\big)\left(1-\frac{h}{H}\right)\right)\right| - \Delta(H)$$

for each positive integer with $H \leq n/38$, where

$$\Delta(H) = \frac{2(n+1) + \pi H\sqrt{n+1}}{4n}.$$

Recall the definition of Ψ_χ from (5.14) and define

$$\Phi\colon \mathbb{Z} \to \mathbb{C}, \quad h \mapsto \frac{\arg\left(D_{\frac{n+1}{2}}\left(\frac{-h}{n}\right)\right)}{2\pi},$$

to obtain

$$|S(t, d^{-1})| \geq \frac{2\sqrt{n+1}}{n}\sum_{\substack{h=1\\ h\,\text{odd}}}^{H}\left|D_{\frac{n+1}{2}}\left(\frac{-h}{n}\right)\right|\left(1-\frac{h}{H}\right)\operatorname{Re}\left(e^{2\pi i(\Phi(h)+\Psi(h,d))}\right) - \Delta(H)$$

by Lemma 2.2.3 (iv) and using $|z| \geq \mathrm{Re}(z)$ for each complex z.

Recall the definition of $\kappa_p(H)$ from (5.13) and define H_0 to be the largest even integer with $H_0/2 \leq 0.720 \log\log n$. From Theorem 5.4.5 (with $H = H_0$, so that $\kappa_2(H_0) = H_0/2$) we find that there exists an integer d_0 with $\gcd(d_0, n) = 1$ such that

$$|\Phi(h) + \Psi(h, d_0)| \leq \frac{1}{8}$$

for each odd $h \in \{1, \ldots, H_0\}$, which means that

$$\mathrm{Re}\left(e^{2\pi i(\Phi(h)+\Psi(h,d_0))}\right) \geq \frac{1}{\sqrt{2}}$$

for each odd $h \in \{1, \ldots, H_0\}$. Therefore, we know from Lemma 5.2.5 that there exists an integer t_0 such that

$$|S(t_0, d_0^{-1})| \geq \frac{\sqrt{2(n+1)}}{n} \sum_{\substack{h=1 \\ h \text{ odd}}}^{H_0} \left| D_{\frac{n+1}{2}}\left(\frac{-h}{n}\right)\right| \left(1 - \frac{h}{H_0}\right) - \Delta(H_0).$$

Recalling the definitions of H_0 and $\Delta(H_0)$, it is a consequence of the first part of Lemma 5.5.1 that

$$|S(t_0, d_0^{-1})| \geq \frac{0.999}{\sqrt{2\pi}} \sqrt{n+1} \log\log\log n,$$

provided that n is large enough.

Case 2. $p \neq 2$. Then d is odd since n is even, so that $\chi^{hd}(-1) = (-1)^h$ for each h. Therefore, we find from (5.34) that $|S(t, d^{-1})|$ is at least

$$\frac{1}{n}\left| \sum_{h=1}^{H} \left(D_{\frac{n+1}{p}}\left(\frac{-h}{n}\right) G\big(\chi^{hd}\big) + \overline{D_{\frac{n+1}{p}}\left(\frac{-h}{n}\right) G\big(\chi^{hd}\big)(-1)^h} \right) \left(1 - \frac{h}{H}\right) \right| - \frac{n+1}{pn}.$$

Separating the sum into two sums (one corresponding to the odd h and one to the even h), and using $z + \overline{z} = 2\,\mathrm{Re}(z)$ and $z - \overline{z} = 2\,\mathrm{Im}(z)i$ for complex z, we obtain

$$\begin{aligned} |S(t, d^{-1})| \geq \frac{2}{n} \Bigg| & \mathrm{Re}\Bigg(\sum_{\substack{h=2 \\ h \text{ even}}}^{H} D_{\frac{n+1}{p}}\left(\frac{-h}{n}\right) G\big(\chi^{hd}\big) \left(1 - \frac{h}{H}\right) \Bigg) \\ & + \mathrm{Im}\Bigg(\sum_{\substack{h=1 \\ h \text{ odd}}}^{H} D_{\frac{n+1}{p}}\left(\frac{-h}{n}\right) G\big(\chi^{hd}\big) \left(1 - \frac{h}{H}\right) \Bigg) i \Bigg| - \frac{n+1}{pn}. \end{aligned}$$

Use $|a+bi| \geq |a|$ for real a and b to obtain

$$|S(t,d^{-1})| \geq \frac{2}{n}\left|\mathrm{Re}\Bigg(\sum_{\substack{h=2\\ h\,\text{even}}}^{H} D_{\frac{n+1}{p}}\Big(\frac{-h}{n}\Big)G\big(\chi^{hd}\big)\Big(1-\frac{h}{H}\Big)\Bigg)\right| - \frac{n+1}{pn}.$$

Separating the sum into two sums, and then applying the triangle inequality, we obtain

$$\begin{aligned}|S(t,d^{-1})| \geq &\frac{2}{n}\left|\mathrm{Re}\Bigg(\sum_{\substack{h=2\\ h\,\text{even}\\ h\not\equiv 0 \,(\mathrm{mod}\ p)}}^{H} D_{\frac{n+1}{p}}\Big(\frac{-h}{n}\Big)G\big(\chi^{hd}\big)\Big(1-\frac{h}{H}\Big)\Bigg)\right| \\ &- \frac{2}{n}\left|\mathrm{Re}\Bigg(\sum_{\substack{h=2\\ h\,\text{even}\\ h\equiv 0 \,(\mathrm{mod}\ p)}}^{H} D_{\frac{n+1}{p}}\Big(\frac{-h}{n}\Big)G\big(\chi^{hd}\big)\Big(1-\frac{h}{H}\Big)\Bigg)\right| - \frac{n+1}{pn}.\end{aligned}$$

Applying the triangle inequality to the second sum, using Lemma 2.2.3 (iv), and then the second part of Lemma 5.5.2 with $k=p$, we have

$$|S(t,d^{-1})| \geq \frac{2}{n}\left|\mathrm{Re}\Bigg(\sum_{\substack{h=2\\ h\,\text{even}\\ h\not\equiv 0 \,(\mathrm{mod}\ p)}}^{H} D_{\frac{n+1}{p}}\Big(\frac{-h}{n}\Big)G\big(\chi^{hd}\big)\Big(1-\frac{h}{H}\Big)\Bigg)\right| - \Delta(H)$$

for each integer H with $1 < H \leq pn/76$, where

$$\Delta(H) = \frac{2p(n+1)+\pi H\sqrt{n+1}}{2p^2 n}.$$

Define

$$\Phi\colon \mathbb{Z}\to\mathbb{C}, \quad h \mapsto \frac{\arg\big(D_{\frac{n+1}{p}}(\frac{-h}{n})\big)}{2\pi},$$

to obtain

$$|S(t,d^{-1})| \geq \frac{2\sqrt{n+1}}{n}\sum_{\substack{h=2\\ h\,\text{even}\\ h\not\equiv 0 \,(\mathrm{mod}\ p)}}^{H}\left|D_{\frac{n+1}{p}}\Big(\frac{-h}{n}\Big)\right|\Big(1-\frac{h}{H}\Big)\mathrm{Re}\Big(e^{2\pi i(\Phi(h)+\Psi_\chi(h,d))}\Big)-\Delta(H).$$

Notice that, for positive integers H with $H \equiv 0 \pmod{p}$, we have

$$\kappa_p(H) = \frac{(p-1)H}{p}.$$

Define H_0 to be the largest integer with $H_0 \equiv 0 \pmod{p}$ and $(p-1)H_0/p \leq$

$0.720 \log\log n$. From Theorem 5.4.5 (with $H = H_0$, so that $\kappa_p(H_0) = (p-1)H_0/p$) we find that there exists an integer d_0 with $\gcd(d_0, n) = 1$ such that

$$|\Phi(h) + \Psi(h, d_0)| \leq \frac{1}{8}$$

for each $h \in \{1, \ldots, H_0\}$ with $h \not\equiv 0 \pmod{p}$, which means that

$$\operatorname{Re}\left(e^{2\pi i(\Phi(h)+\Psi(h,d_0))}\right) \geq \frac{1}{\sqrt{2}}$$

for each $h \in \{1, \ldots, H_0\}$ with $h \not\equiv 0 \pmod{p}$. Therefore, we know from Lemma 5.2.5 that there exists an integer t_0 such that

$$|S(t_0, d_0^{-1})| \geq \frac{\sqrt{2(n+1)}}{n} \sum_{\substack{h=2 \\ h \text{ even} \\ h \not\equiv 0 \,(\mathrm{mod}\ p)}}^{H} \left| D_{\frac{n+1}{p}}\left(\frac{-h}{n}\right)\right| \left(1 - \frac{h}{H_0}\right) - \Delta(H_0).$$

Recalling the definitions of H_0 and $\Delta(H_0)$, it is a consequence of the first part of Lemma 5.5.2 that

$$|S(t_0, d_0^{-1})| \geq \frac{0.999\sqrt{2}(p-1)}{\pi p^2} \sqrt{n+1} \log\log\log n,$$

provided that n is large enough. □

Combining Theorem 5.5.3 and Lemma 5.2.1, we have the following result on the peak sidelobe level of p-ary Galois sequences.

Corollary 5.5.4. *Assume that Conjecture 5.3.5 is true and let p be a prime. For all sufficiently large $n = p^m - 1$, there exists a p-ary Galois sequence A of length n with*

$$\left|C_A\big(n - (n+1)/p\big)\right| \geq \begin{cases} \frac{0.999}{\sqrt{2}\pi} \sqrt{n+1} \log\log\log n & \text{if } p = 2 \\ \frac{0.999\sqrt{2}(p-1)}{\pi p^2} \sqrt{n+1} \log\log\log n & \text{if } p \neq 2. \end{cases}$$

In particular, there exists a family of p-ary Galois sequences whose peak sidelobe level grows at least with order $\sqrt{n} \log\log\log n$.

5.6 Conclusion and open problems

Besides the upper bound in Theorem 5.2.4 of Sarwate from 1984 and the lower bound of order $\sqrt{n}$ nothing is known on the peak sidelobe level of Galois sequences. In this chapter we gave theoretical evidence that, for each prime p, there exists a family of p-ary Galois sequences whose peak sidelobe level grows at least with order $\sqrt{n} \log\log\log n$. In the case that $p = 2$ this supports numerical evidence made in [63] and contradicts the claim that

the peak sidelobe level of Galois sequences grows like $O(\sqrt{n})$, which appears frequently in the radar literature. Our main results Theorem 5.5.3 and Corollary 5.5.4 heavily rely on Conjecture 5.3.5.

Let p be a prime. If we would have a slightly better upper bound on the number of prime divisors of numbers n of the form $n = p^m - 1$ (or of an infinite set of numbers of that form), say $(\log n)^{1-\epsilon}$ for some $\epsilon > 0$ instead of $\log n / \log\log n$ as in Lemma 5.4.2, then we could choose the integer H in the assumption of Theorem 5.4.5 such that κ is of order $(\log n)^{\delta}$ for some $\delta > 0$. Taking such an H in the proof of Theorem 5.5.3 would guarantee the existence of a character sum whose magnitude is at least of order $\sqrt{n}\log\log n$ in the assertion of Theorem 5.5.3. That would immediately imply that there exists a family of p-ary Galois sequences whose peak sidelobe level grows at least with order $\sqrt{n}\log\log n$, which would be the best lower bound that we can achieve with our methods. In particular, in the case that $p = 2$ the existence of infinitely many Mersenne primes would imply this result.

We conclude with a list of open problems concerning the peak sidelobe level.

- Let p be a prime. Prove that there exist infinitely many numbers n of the form $n = p^m - 1$ with only a few prime divisors, say $(\log n)^{1-\epsilon}$ for some $\epsilon > 0$.

  Although this problem is purely number-theoretic, we included it in this list since it would imply that there exists a family of p-ary Galois sequences whose peak sidelobe level grows at least with order $\sqrt{n}\log\log n$ (under the assumption that Conjecture 5.3.5 is true).

- Prove that Conjecture 5.3.5 is true.

  A proof of this conjecture would make the considerations of this chapter much more valuable.

- Find any other specific family of binary sequences whose peak sidelobe level grows like $O(\sqrt{n\log n})$ besides that given by Schmidt [110].

- Solve Problem 1.5, that is, find a family of binary sequences whose peak sidelobe level grows slower than $c\sqrt{n\log n}$ for each constant $c > 0$.

  Schmidt [110] conjectured that the peak sidelobe level of his sequences grows with order $\sqrt{n\log\log n}$. The best upper bound that he was able to prove is $\sqrt{2n\log(2n)}$. Other good candidates to attack this problem are of course Galois sequences (see Conjecture 5.1.1).

- Prove that Conjecture 5.1.1 is true.

- Show that there exists a family of Galois sequences whose peak sidelobe level grows like $O(\sqrt{n})$.

- Prove that Conjecture 5.1.2 is true.

- Solve Problem 1.4, that is, determine the asymptotic behaviour of M_n as $n \to \infty$, where M_n is the minimum of $\mathrm{M}(A)$ taken over all 2^n binary sequences A of length n.

  This problem is just included for the sake of completeness. A solution is way beyond the scope of our methods.

The last five problems are arguably very challenging.

Chapter 6

Sequence pairs with asymptotically optimal aperiodic correlation

6.1 Introduction and chapter overview

Recall from Chapter 1 that the *Pursley-Sarwate criterion* of two unimodular sequences A and B of length $n > 1$ is given by

$$\mathrm{PSC}(A, B) = (\mathrm{F}(A)\,\mathrm{F}(B))^{-1/2} + \mathrm{CF}(A, B)^{-1},$$

where

$$\mathrm{F}(A) = \frac{n^2}{\sum_{u \in \mathbb{Z}\setminus\{0\}} |C_A(u)|^2}$$

is the *(autocorrelation) merit factor* of A and

$$\mathrm{CF}(A, B) = \frac{n^2}{\sum_{u \in \mathbb{Z}} |C_{A,B}(u)|^2}$$

is the *crosscorrelation merit factor* of A and B.

We begin with briefly reviewing known results on the Pursley-Sarwate criterion of sequence pairs. Katz [70] showed that carefully chosen binary sequence pairs derived from Galois sequences and also carefully chosen binary sequence pairs derived from Legendre sequences produce an asymptotic Pursley-Sarwate criterion of 7/6. Boothby and Katz [10] studied the Pursley-Sarwate criterion of binary sequence pairs derived from the cyclotomic classes of order four. Again, the lowest asymptotic Pursley-Sarwate criterion they could obtain is 7/6. It is remarkable that, for each real α with $6/5 \leq \alpha \leq 6$, there exists an infinite family of pairs (A_n, B_n) of binary sequences of length n derived from the cyclotomic classes of order four such that

$$\lim_{n\to\infty} \mathrm{F}(A_n) = \lim_{n\to\infty} \mathrm{F}(B_n) = \alpha \quad \text{and} \quad \lim_{n\to\infty} \mathrm{CF}(A_n, B_n) = \frac{6\alpha}{7\alpha - 6},$$

so that $\lim_{n\to\infty} \mathrm{PSC}(A_n, B_n) = 7/6$ [10]. Katz, Lee, and Trunov [72] examined the Pursley-Sarwate criterion of pairs of modifications of Shapiro sequences. The best asymptotic Pursley-Sarwate criterion they obtained is 331/300, which is slightly smaller than 7/6.

Recall from Theorem 1.7.2 that pairs of unimodular sequences (A, B) with $\mathrm{PSC}(A, B) = 1$ are exactly the Golay pairs. Golay pairs are known to exist for infinitely many, though not for all, lengths (see [36] for the existence for small lengths). The classification in Theorem 1.7.2 does however not say anything about the individual quantities $\mathrm{F}(A)$, $\mathrm{F}(B)$, and $\mathrm{CF}(A, B)$ for a Golay pair (A, B). Recall from Chapter 1 that we already know these values for the Shapiro sequences A_m and B_m of length 2^m. Asymptotically, we have

$$\lim_{m\to\infty} \mathrm{F}(A_m) = \lim_{m\to\infty} \mathrm{F}(B_m) = 3 \quad \text{and} \quad \lim_{m\to\infty} \mathrm{CF}(A_m, B_m) = \frac{3}{2}.$$

In this chapter we exhibit unimodular sequences whose Pursley-Sarwate criterion is asymptotically 1 and for which (unlike for general Golay pairs) we can control the autocorrelation and the crosscorrelation merit factor. Our results involve *Chu sequences*[1] [21], which are unimodular sequences of length n of the form

$$Z_n^{(a)} = (z_0, z_1, \ldots, z_{n-1}), \quad z_j = e^{\pi i a j^2/n} \quad \text{for each } j = 0, 1, \ldots, n-1,$$

where a is an integer. The merit factor of the Chu sequence $Z_n^{(a)}$ depends heavily on a. Several authors [95], [121], [91] have shown independently that $\mathrm{F}(Z_n^{(1)})$ grows with order $\sqrt{n}$ and the exact constant has been determined by Schmidt [111] by showing that

$$\lim_{n\to\infty} \frac{\mathrm{F}\left(Z_n^{(1)}\right)}{\sqrt{n}} = \frac{\pi}{2}. \tag{6.1}$$

Recall that this is very different from the binary case, where the largest known asymptotic merit factor equals $6.342061\ldots$ (see Chapter 3). However, the best known asymptotic merit factor behaviour for unimodular sequences comes from *Frank sequences* [111], whose merit factor grows like $\pi^2/4\sqrt{n}$.

In fact, since $\mathrm{F}(Z_n^{(1)})$ tends to infinity, this immediately implies that

$$\lim_{n\to\infty} \mathrm{PSC}(Z_n^{(1)}, Z_n^{(1)}) = 1.$$

However, the pair $(Z_n^{(1)}, Z_n^{(1)})$ would be a bad choice when good crosscorrelation is required since the crosscorrelation at the zero shift equals the sequence length n. This problem is avoided by taking the pair $(Z_n^{(1)}, Z_n^{(-1)})$. Indeed it can be shown using the forthcoming Lemma 6.3.2 that in this case the crosscorrelation at the zero shift is of order $\sqrt{n}$. In detail, in the forthcoming Theorem 6.3.4 we shall prove that

$$\lim_{n\to\infty} \frac{\mathrm{F}\left(Z_n^{(-1)}\right)}{\sqrt{n}} = \frac{\pi}{2} \tag{6.2}$$

[1] We note that Chu [21] used a slightly different definition when n is odd.

and

$$\lim_{n\to\infty} \mathrm{CF}(Z_n^{(1)}, Z_n^{(-1)}) = 1,$$

so that together with (6.1) we deduce

$$\lim_{n\to\infty} \mathrm{PSC}(Z_n^{(1)}, Z_n^{(-1)}) = 1.$$

In our second result (see the forthcoming Theorem 6.3.5) we construct a pair of unimodular sequences from two Chu sequences of even length such that the Pursley-Sarwate criterion is asymptotically 1 and the autocorrelation and crosscorrelation merit factors are asymptotically balanced, which means that they all tend to the same constant 2. In detail, we shall prove

$$\lim_{n\to\infty} \mathrm{F}\left(Z_{2n}^{(n+1)}\right) = \lim_{n\to\infty} \mathrm{F}\left(Z_{2n}^{(n-1)}\right) = 2 \tag{6.3}$$

and

$$\lim_{n\to\infty} \mathrm{CF}(Z_{2n}^{(n+1)}, Z_{2n}^{(n-1)}) = 2,$$

so that

$$\lim_{n\to\infty} \mathrm{PSC}(Z_{2n}^{(n+1)}, Z_{2n}^{(n-1)}) = 1.$$

The remainder of this chapter is structured as follows. In Sections 6.2 and 6.3 we prove our results on the autocorrelation and the crosscorrelation of the Chu sequences in question, respectively. We conclude with Section 6.4, where we give two open problems concerning the Pursley-Sarwate criterion of unimodular sequences that arise from this chapter.

The results of this chapter can also be found in [50].

6.2 Autocorrelation of Chu sequences

In this section we prove our results on the autocorrelation of Chu sequences. We begin with a lemma which gives an expression for the merit factor of Chu sequences.

Lemma 6.2.1. *Let a and n be integers with $n > 1$, and write $d = \gcd(a, n)$. Then*

$$\frac{1}{\mathrm{F}\left(Z_n^{(a)}\right)} = \frac{4d}{n^2} \sum_{1\le u\le n/(2d)} \left(\frac{\sin(\pi a u^2/n)}{\sin(\pi a u/n)}\right)^2 + \frac{(d-1)(2d-1)}{3d} - \frac{2d}{n^2}\delta_{n/d},$$

where

$$\delta_{n/d} = \begin{cases} 1 & \text{if } n/d \equiv 2 \pmod 4 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Write $Z = Z_n^{(a)}$, $a = db$, and $n = dm$. Straightforward manipulations give

$$|C_Z(u)| = |C_Z(-u)| = \left| \sum_{j=0}^{n-u-1} e^{2\pi i b u j/m} \right|$$

for $0 \le u < n$. Hence, if u is not a multiple of m, then

$$|C_Z(u)| = \left| \frac{\sin(\pi b u^2/m)}{\sin(\pi b u/m)} \right|.$$

Therefore,

$$\begin{aligned}
\frac{1}{\mathrm{F}\left(Z_n^{(a)}\right)} &= \frac{2}{n^2} \sum_{u=1}^{n-1} |C_Z(u)|^2 \\
&= \frac{2d}{n^2} \sum_{u=1}^{m-1} |C_Z(u)|^2 + \frac{2}{n^2} \sum_{k=1}^{d-1} |C_Z(km)|^2 \\
&= \frac{4d}{n^2} \sum_{1 \le u \le m/2} |C_Z(u)|^2 + \frac{2}{n^2} \sum_{k=1}^{d-1} |C_Z(km)|^2 - \frac{2d}{n^2} \delta_m
\end{aligned}$$

since $|C_Z(u)| = |C_Z(m-u)|$ for $1 \le u < m$ and $|C_Z(m/2)| = \delta_m$ for even m. Finally, note that

$$\begin{aligned}
\sum_{k=1}^{d-1} |C_Z(km)|^2 &= \sum_{k=1}^{d-1} (n - km)^2 \\
&= m^2 \sum_{k=1}^{d-1} k^2 \\
&= \frac{n^2}{6d} (d-1)(2d-1),
\end{aligned}$$

which completes the proof. □

We shall also need the following result due to Schmidt [111]. For convenience, we include his proof.

Lemma 6.2.2 ([111])**.** *We have*

$$\begin{aligned}
\lim_{n \to \infty} \frac{1}{n^{3/2}} \sum_{1 \le u \le n/2} \left(\frac{\sin(\pi u^2/n)}{\sin(\pi u/n)} \right)^2 &= \frac{1}{2\pi}, \\
\lim_{n \to \infty} \frac{1}{n^{3/2}} \sum_{1 \le u \le n/2} \left(\frac{\sin(\pi u^2/n)}{\pi u/n} \right)^2 &= \frac{1}{2\pi}.
\end{aligned}$$

Proof. Let x be a real number with $0 < x \le \pi/2$. From the Maclaurin series of $\sin x$ we find that $x - x^3/6 \le \sin x \le x$, from which it follows that

$$0 < \frac{1}{(\sin x)^2} - \frac{1}{x^2} < 1.$$

Therefore,

$$\left| \sum_{1\le u\le n/2} \left(\frac{\sin(\pi u^2/n)}{\sin(\pi u/n)}\right)^2 - \sum_{1\le u\le n/2} \left(\frac{\sin(\pi u^2/n)}{\pi u/n}\right)^2 \right| < \frac{n}{2},$$

so that

$$\lim_{n\to\infty} \frac{1}{n^{3/2}} \sum_{1\le u\le n/2} \left(\frac{\sin(\pi u^2/n)}{\sin(\pi u/n)}\right)^2 = \lim_{n\to\infty} \frac{1}{n^{3/2}} \sum_{1\le u\le n/2} \left(\frac{\sin(\pi u^2/n)}{\pi u/n}\right)^2$$

provided that one of the limits exist. Thus, defining the function $r\colon \mathbb{R} \to \mathbb{R}$ via

$$r(x) = \left(\frac{\sin(\pi u^2/n)}{\pi u/n}\right)^2,$$

the lemma is proved by showing that

$$\lim_{n\to\infty} \frac{1}{n^{3/2}} \sum_{1\le u\le n/2} r(u) = \frac{1}{2\pi}. \tag{6.4}$$

From the Euler-Maclaurin formula (see [47, p. 469], for example) we deduce that, for all real a and b, we have

$$\left| \int_a^b r(x)dx \; - \sum_{a<u\le b} r(u) \right| \le \frac{1}{2}\Big(|r(a)| + |r(b)|\Big) + \frac{1}{12}\left(|r'(a)| + |r'(b)| + \int_a^b |r''(x)|dx\right).$$

We take $b = n/2$ and let a tend to zero. Elementary calculations give

$$|r(n/2)| \le \frac{4}{\pi^2}, \qquad |r'(n/2)| \le \frac{8}{\pi} + \frac{16}{n\pi^2}, \qquad \lim_{a\to 0} r(a) = \lim_{a\to 0} r'(a) = 0,$$

and $|r''(x)| \le 34$ for all real x. Therefore,

$$\left| \int_0^{n/2} r(x)dx \; - \sum_{1\le u\le n/2} r(u) \right| \le \frac{2}{\pi^2} + \frac{2}{3\pi} + \frac{4}{3n\pi^2} + \frac{17n}{12},$$

so that

$$\lim_{n\to\infty} \frac{1}{n^{3/2}} \sum_{1\le u\le n/2} r(u) = \lim_{n\to\infty} \frac{1}{n^{3/2}} \int_0^{n/2} r(x)dx$$

provided that both limits exist. Substitute $y = \pi x^2/n$ to obtain

$$\begin{aligned} \lim_{n\to\infty} \frac{1}{n^{3/2}} \int_0^{n/2} r(x)dx &= \lim_{n\to\infty} \frac{1}{2\pi^{3/2}} \int_0^{\pi n/4} \frac{(\sin y)^2}{y^{3/2}} dy \\ &= \frac{1}{2\pi^{3/2}} \int_0^{\infty} \frac{(\sin y)^2}{y^{3/2}} dy. \end{aligned}$$

The identity (see [46, 3.823], for example)

$$\int_0^\infty \frac{(\sin y)^2}{y^{3/2}} dy = \sqrt{\pi}$$

completes the proof of (6.4). □

Schmidt obtained (6.1) from Lemma 6.2.1 with $a = 1$ and the first identity in Lemma 6.2.2. From Lemmas 6.2.1 and 6.2.2 we also deduce (6.2). We now use Lemmas 6.2.1 and 6.2.2 to prove (6.3).

Proof of (6.3). Write $X_n = Z_{2n}^{(n+1)}$ and $Y_n = Z_{2n}^{(n-1)}$. We distinguish the cases that n runs through the set of even and odd positive integers. First, we show that

$$\lim_{m\to\infty} \mathrm{F}(X_{2m}) = \lim_{m\to\infty} \mathrm{F}(Y_{2m}) = 2. \tag{6.5}$$

It is readily verified that the aperiodic autocorrelations of X_{2m} and Y_{2m} have equal magnitudes at all shifts, so that it is sufficient to establish that $\mathrm{F}(X_{2m}) \to 2$. Noting that $2m+1$ is coprime to $4m$ and using trigonometric addition formulas, Lemma 6.2.1 with $n = 4m$ and $a = 2m+1$ shows that

$$\frac{4m^2}{\mathrm{F}(X_{2m})} = \sum_{\substack{u=1 \\ u \text{ even}}}^{2m} \left(\frac{\sin(\pi u^2/(4m))}{\sin(\pi u/(4m))} \right)^2 + \sum_{\substack{u=1 \\ u \text{ odd}}}^{2m} \left(\frac{\cos(\pi u^2/(4m))}{\cos(\pi u/(4m))} \right)^2.$$

By Lemma 6.2.2, the first sum on the right-hand side is $O(m^{3/2})$, so that it is sufficient to show that

$$\lim_{m\to\infty} \frac{1}{m^2} \sum_{v=1}^{m} \left(\frac{\cos((\pi(2v-1)^2/(4m))}{\cos(\pi(2v-1)/(4m))} \right)^2 = 2. \tag{6.6}$$

Let x be a real number satisfying $0 < x < \pi/2$. From the Taylor series of $\cos x$ at $\pi/2$ we find that

$$-(x-\pi/2) + \tfrac{1}{6}(x-\pi/2)^3 < \cos x < -(x-\pi/2),$$

from which it follows that

$$0 < \frac{1}{(\cos x)^2} - \frac{1}{(x-\pi/2)^2} < 1.$$

Therefore,

$$\left| \sum_{v=1}^{m} \left(\frac{\cos(\pi(2v-1)^2/(4m))}{\cos(\pi(2v-1)/(4m))} \right)^2 - \sum_{v=1}^{m} \left(\frac{\cos(\pi(2v-1)^2/(4m))}{\pi(2v-1)/(4m) - \pi/2} \right)^2 \right| < m.$$

Put $v = m + 1 - w$ to obtain

$$\sum_{v=1}^{m} \left(\frac{\cos(\pi(2v-1)^2/(4m))}{\pi(2v-1)/(4m) - \pi/2} \right)^2 = \sum_{w=1}^{m} \left(\frac{\cos(\pi(2w-1)^2/(4m))}{\pi(2w-1)/(4m)} \right)^2.$$

Apply $(\cos x)^2 = 1 - (\sin x)^2$ to the right-hand side and use Lemma 6.2.2 to obtain

$$\begin{aligned} \lim_{m\to\infty} \frac{1}{m^2} \sum_{w=1}^{m} \left(\frac{\cos(\pi(2w-1)^2/(4m))}{\pi(2w-1)/(4m)} \right)^2 &= \frac{16}{\pi^2} \sum_{w=1}^{\infty} \frac{1}{(2w-1)^2} \\ &= \frac{16}{\pi^2} \left(\sum_{w=1}^{\infty} \frac{1}{w^2} - \sum_{w=1}^{\infty} \frac{1}{(2w)^2} \right) \\ &= \frac{12}{\pi^2} \sum_{w=1}^{\infty} \frac{1}{w^2} \\ &= 2, \end{aligned}$$

using Euler's evaluation $\sum_{w=1}^{\infty} 1/w^2 = \pi^2/6$. This gives (6.6), and so completes the proof of (6.5).

Next we prove that

$$\lim_{m\to\infty} \mathrm{F}(X_{2m+1}) = \lim_{m\to\infty} \mathrm{F}(Y_{2m+1}) = 2. \tag{6.7}$$

Note that $\gcd(2m+2, 4m+2) = 2$, so that Lemma 6.2.1 with $n = 4m+2$ and $a = 2m+2$ gives

$$\frac{1}{\mathrm{F}(X_{2m+1})} = \frac{8}{(4m+2)^2} \sum_{u=1}^{m} \left(\frac{\sin(\pi(m+1)u^2/(2m+1))}{\sin(\pi(m+1)u/(2m+1))} \right)^2 + \frac{1}{2}.$$

On the other hand, $\gcd(2m, 4m+2) = 2$, so that Lemma 6.2.1 with $n = 4m+2$ and $a = 2m$ gives

$$\frac{1}{\mathrm{F}(Y_{2m+1})} = \frac{8}{(4m+2)^2} \sum_{u=1}^{m} \left(\frac{\sin(\pi mu^2/(2m+1))}{\sin(\pi mu/(2m+1))} \right)^2 + \frac{1}{2}.$$

Comparing the two preceding equations and using

$$\left| \sin\left(\frac{\pi mk}{2m+1} \right) \right| = \left| \sin\left(\frac{\pi mk}{2m+1} - \pi k \right) \right| = \left| \sin\left(\frac{\pi(m+1)k}{2m+1} \right) \right|,$$

we conclude that $\mathrm{F}(X_{2m+1}) = \mathrm{F}(Y_{2m+1})$. To complete the proof of (6.7), we show that

$$\lim_{m\to\infty} \frac{1}{m^2} \sum_{u=1}^{m} \left(\frac{\sin(\pi mu^2/(2m+1))}{\sin(\pi mu/(2m+1))} \right)^2 = 0. \tag{6.8}$$

For even k, we have

$$\left|\sin\left(\frac{\pi mk}{2m+1}\right)\right| = \left|\sin\left(\frac{\pi mk}{2m+1} - \frac{\pi}{2}k\right)\right| = \left|\sin\left(\frac{\pi k}{4m+2}\right)\right|,$$

so that

$$\sum_{\substack{u=1\\ u \text{ even}}}^{m} \left(\frac{\sin(\pi mu^2/(2m+1))}{\sin(\pi mu/(2m+1))}\right)^2 = O(m^{3/2})$$

by Lemma 6.2.2. For odd k, we have

$$\left|\sin\left(\frac{\pi mk}{2m+1}\right)\right| = \left|\cos\left(\frac{\pi mk}{2m+1} - \frac{\pi}{2}k\right)\right| = \left|\cos\left(\frac{\pi k}{4m+2}\right)\right|,$$

so that

$$\sum_{\substack{u=1\\ u \text{ odd}}}^{m} \left(\frac{\sin(\pi mu^2/(2m+1))}{\sin(\pi mu/(2m+1))}\right)^2 = \sum_{\substack{u=1\\ u \text{ odd}}}^{m} \left(\frac{\cos(\pi u^2/(4m+2))}{\cos(\pi u/(4m+2))}\right)^2.$$

The summands on the right hand side are at most 2, so that the entire sum is at most $m+1$. This proves (6.8), and so completes the proof of (6.7). □

6.3 Crosscorrelation of Chu sequences and main results

In this section we prove our results on the crosscorrelation of Chu sequences and thereby also the main results of this chapter. A straightforward computation shows that the aperiodic crosscorrelations between two Chu sequences of equal length are equal in magnitude to *generalised Gauss sums*, which are, for real x and θ and integral N, defined to be

$$S_N(x,\theta) = \sum_{j=1}^{N} e^{\pi i x j^2 + 2\pi i \theta j}.$$

An asymptotic expansion of these sums was obtained by Paris [101] using an asymptotic expansion of the error function. We deduce an estimate for generalised Gauss sums from this expansion. To state the result, define for real θ and $x \neq 0$,

$$E(x,\theta) = e^{-\pi i \theta^2/x} \operatorname{erfc}\left(e^{\pi i/4}\theta\sqrt{\pi/x}\right),$$

where, for complex z,

$$\operatorname{erfc}(z) = 1 - \frac{2}{\sqrt{\pi}} \int_0^z e^{-t^2}\, dt$$

is the complementary error function and the integral is over any path from 0 to z.

Proposition 6.3.1 ([101, Theorem 1])**.** *Let N be a positive integer, let $x \in (0,1)$, and let $\theta \in (-1/2, 1/2]$. Write $Nx + \theta = M + \epsilon$, where M is integral and $\epsilon \in (-1/2, 1/2]$. Then*

$$\begin{aligned} S_N(x,\theta) = \frac{e^{-\pi i\theta^2/x + \pi i/4}}{\sqrt{x}} S_M(-1/x, \theta/x) + \frac{\mu - 1}{2} \\ + \frac{e^{\pi i/4}}{2\sqrt{x}}\big(E(x,\theta) - \mu E(x,\epsilon)\big) + \frac{i}{2}\big(g(\theta) - \mu g(\epsilon)\big) + R, \end{aligned}$$

where $|R| < x$ and $\mu = e^{\pi i x N^2 + 2\pi i\theta N}$ and $g\colon [-1/2, 1/2] \to \mathbb{R}$ is given by

$$g(t) = \begin{cases} 0 & \text{for } t = 0 \\ \cot(\pi t) - (\pi t)^{-1} & \text{otherwise.} \end{cases}$$

Fiedler, Jurkat, and Körner [37, Lemma 4] obtained the following estimate from a slightly weaker version of Proposition 6.3.1.

Lemma 6.3.2 ([37, Lemma 4])**.** *Let N, k, and m be integers such that $\gcd(k,m)$ and N/m are bounded by absolute constants, and let θ be real. Then*

$$|S_N(k/m, \theta)| = O(\sqrt{m}),$$

where the implicit constant is absolute.

From Proposition 6.3.1 we can also deduce the following lemma, which will be the key ingredient in the proofs of our main results.

Lemma 6.3.3. *Let m be a positive integer and let u be an integer such that either u or $m - u$ is in the set*

$$\{w \in \mathbb{Z}\colon m^{2/3} \le w \le m/2 - m^{2/3}\}. \tag{6.9}$$

Then

$$\big|S_{m-u}(2/m, u/m)\big| = \sqrt{\frac{m}{2}} + O(m^{1/3}), \tag{6.10}$$

where the implicit constant is absolute.

Proof. Throughout the proof, all implicit constants are absolute. We first prove the desired bound when u is in the set (6.9). This is an application of Proposition 6.3.1 with $N = m-u$, $x = 2/m$, $\theta = u/m$, so that $M = 2$ and $\epsilon = -u/m$ and $\mu = 1$. We have

$$\begin{aligned} \cot(\pi\theta) - \cot(\pi\epsilon) - \frac{1}{\pi\theta} + \frac{1}{\pi\epsilon} &= 2\cot(\pi u/m) - \frac{2m}{\pi u} \\ &= O(m^{1/3}), \end{aligned}$$

using that $\cot(\pi t)$ is nonnegative on $(0, 1/2]$ and, for $m \geq 8$,

$$\begin{aligned}\cot(\pi u/m) &\leq \cot\left(\pi m^{-1/3}\right) \\ &\leq \frac{1}{\sin\left(\pi m^{-1/3}\right)} \\ &\leq \frac{1}{2} m^{1/3}.\end{aligned}$$

Now use the identity $\operatorname{erfc}(-z) = 2 - \operatorname{erfc}(z)$ to obtain

$$E(x, \theta) - E(x, -\theta) = 2E(x, \theta) - 2e^{-\pi i \theta^2/x}.$$

Since

$$S_2(-1/x, \theta/x) = (-i)^m (-1)^u + 1,$$

we find from Proposition 6.3.1 that

$$|S_N(x, \theta)| = \sqrt{\frac{m}{2}} \left|(-i)^m (-1)^u + E(x, \theta)\right| + O(m^{1/3}).$$

From the asymptotic expansion [101, (1.3) and (1.4)] of $E(x, \theta)$ we find that

$$\left| E(x, \theta) - \frac{e^{-2\pi i \theta^2/x - \pi i/4} \sqrt{x}}{\pi \theta} \right| \leq \frac{x^{3/2}}{2\pi^2 \theta^3},$$

so that $|E(x, \theta)|$ is $O(m^{-1/6})$ and (6.10) follows, as required.

Now assume that $m - u$ is in the set (6.9). Put $v = m - u$ and apply Proposition 6.3.1 with $N = v$, $x = 2/m$, and $\theta = -v/m$, so that $M = 0$ and $\epsilon = v/m$ and $\mu = 1$. Proceeding similarly as in the first case, we obtain

$$|S_N(x, \theta)| = \sqrt{\frac{m}{2}} \left|e^{-\pi i \theta^2/x} - E(x, \theta)\right| + O(m^{1/3}),$$

which again implies (6.10). □

Main results

We now give our results on the Pursley-Sarwate criterion of pairs of Chu sequences. Our first result is the following theorem.

Theorem 6.3.4. *For each positive integer n, let $X_n = Z_n^{(1)}$ and $Y_n = Z_n^{(-1)}$ be Chu sequences of length n. Then, as $n \to \infty$,*

(i) $\mathrm{F}(X_n) \to \infty$, $\mathrm{F}(Y_n) \to \infty$;

(ii) $\mathrm{CF}(X_n, Y_n) \to 1$;

(iii) $\mathrm{PSC}(X_n, Y_n) \to 1$.

Proof. Part (i) follows from (6.1) and (6.2). We proceed with proving part (ii). For each $u \in \{0, 1, \ldots, n-1\}$, we have

$$|C_{X_n,Y_n}(u)| = |C_{X_n,Y_n}(-u)| = \left| \sum_{j=0}^{n-u-1} e^{2\pi i(j^2+ju)/n} \right|.$$

Extend the summation range to $n-u$ and compensate the extra term (which equals 1) by taking out the term corresponding to $j = 0$. The sum then equals $S_{n-u}(2/n, u/n)$ and therefore

$$\frac{n^2}{\mathrm{CF}(X_n, Y_n)} = |S_n(2/n, 0)|^2 + 2\sum_{u=1}^{n-1} |S_{n-u}(2/n, u/n)|^2.$$

Now use Lemma 6.3.3 to find that $|S_{n-u}(2/n, u/n)|^2 = n/2 + O(n^{5/6})$ when u or $n-u$ is in the set

$$\{w \in \mathbb{Z} : n^{2/3} \leq w \leq n/2 - n^{2/3}\}$$

and use Lemma 6.3.2 to bound the remaining $O(n^{2/3})$ values of $|S_{n-u}(2/n, u/n)|^2$ by $O(n)$. This gives

$$\frac{1}{\mathrm{CF}(X_n, Y_n)} = 1 + O(n^{-1/6}),$$

as required.

The third part follows from (i) and (ii). □

We now prove our second result.

Theorem 6.3.5. *For each positive integer n, let $X_n = Z_{2n}^{(n+1)}$ and $Y_n = Z_{2n}^{(n-1)}$ be Chu sequences of length $2n$. Then, as $n \to \infty$,*

(i) $\mathrm{F}(X_n) \to 2$, $\mathrm{F}(Y_n) \to 2$;

(ii) $\mathrm{CF}(X_n, Y_n) \to 2$;

(iii) $\mathrm{PSC}(X_n, Y_n) \to 1$.

Proof. Part (i) is just (6.3). We now prove part (ii). For each $u \in \{0, 1, \ldots, 2n-1\}$, we have

$$|C_{X_n,Y_n}(u)| = |C_{X_n,Y_n}(-u)| = \left| \sum_{j=0}^{2n-u-1} (-1)^{ju} e^{\pi i(j^2+ju)/n} \right|.$$

If u is odd, then the summands corresponding to j and $2n-u-j$ add to zero, leaving the summand corresponding to $j = 0$. Therefore, $|C_{X_n,Y_n}(u)| = 1$ for each odd u satisfying $|u| \leq 2n-1$. Hence,

$$\frac{(2n)^2}{\mathrm{CF}(X_n, Y_n)} = |S_{2n}(1/n, 0)|^2 + 2\sum_{v=1}^{n-1} |S_{2n-2v}(1/n, v/n)|^2 + O(n).$$

Now use Lemma 6.3.3 to find that $|S_{2n-2v}(1/n, v/n)|^2 = n + O(n^{5/6})$ when $2v$ or $2n-2v$

is in the set

$$\{w \in \mathbb{Z} : (2n)^{2/3} \leq w \leq n - (2n)^{2/3}\}$$

and use Lemma 6.3.2 to bound the remaining $O(n^{2/3})$ values of $|S_{2n-2v}(1/n, v/n)|^2$ by $O(n)$. This gives

$$\frac{1}{\mathrm{CF}(X_n, Y_n)} = \frac{1}{2} + O(n^{-1/6}),$$

as required.

Again, the third part follows from (i) and (ii). □

6.4 Conclusion and open problems

In Theorems 6.3.4 and 6.3.5 we established two families of pairs of different Chu sequences whose Pursley-Sarwate criterion tends to 1 as the sequence length tends to infinity, and for which (unlike for general Golay pairs) we can control the autocorrelation and crosscorrelation merit factors. For convenience, we list the occurring asymptotic autocorrelation and crosscorrelation merit factors of unimodular sequence pairs with asymptotic Pursley-Sarwate criterion 1 in Table 6.1.

Table 6.1: Families of sequence pairs with asymptotic Pursley-Sarwate criterion 1.

Sequence pair (A, B)	$\mathrm{F}(A) = \mathrm{F}(B)$	$\mathrm{CF}(A, B)$	Reference
Shapiro sequences	3	3/2	[73] or Section 6.1
Chu sequences (1)	∞	1	Theorem 6.3.4
Chu sequences (2)	2	2	Theorem 6.3.5

We conclude with two open questions concerning the Pursley-Sarwate criterion of unimodular sequence pairs that arise from this chapter.

- Does there exist a family of unimodular sequence pairs (A_n, B_n) such that $\mathrm{F}(A_n)$ and $\mathrm{F}(B_n)$ tend to different finite limits and $\mathrm{PSC}(A_n, B_n)$ tends to 1 as the length n of the sequences tends to infinity?

- Among all families of unimodular sequence pairs (A_n, B_n) such that $\mathrm{F}(A_n)$, $\mathrm{F}(B_n)$, and $\mathrm{CF}(A_n, B_n)$ tend to limits as the length n of the sequences tends to infinity, and such that $\mathrm{PSC}(A_n, B_n)$ tends to 1, what is the largest possible limiting value for $\mathrm{CF}(A_n, B_n)$?

Chapter 7

Summary

In this thesis we investigated various problems concerning the aperiodic autocorrelations and aperiodic crosscorrelations of binary and unimodular sequences. Thereby, we provided in Chapters 3, 5, and 6 at least partial solutions to Problems 1.1 and 1.2. In addition, we examined the L^α norm of families of Littlewood polynomials and gave in Chapter 4 partial results on Problem 1.3.

The main results are summarised below.

- In Theorem 3.3.2 we determined the asymptotic merit factor of generalised Sidelnikov sequences, proving [61, Conjecture 7.2] in the affirmative and explaining numerical evidence made in [54].

  Theorem 3.4.4 gives the asymptotic merit factor of generalised characteristic sequences of Gordon-Mills-Welch difference sets, proving that [61, Conjecture 7.1] is true.

  Theorem 3.5.3 is a very general theorem on the asymptotic merit factor of binary sequences that arise from cyclotomy.

  From Theorem 3.5.3 we deduced Corollaries 3.5.4, 3.5.7, and 3.5.10, which includes results on Paley and Hall difference sets, and also on Ding-Helleseth-Lam almost difference sets.

  Our results on the asymptotic merit factor of binary sequences provide the first essentially new examples since 1991. Furthermore, it is remarkable that the limiting function for the asymptotic merit factor of generalised characteristic sequences of Hall difference sets is different from the other known limiting functions for the asymptotic merit factor (see Figure 3.3).

- In Theorem 4.3.6 we established an explicit formula for the limit of the ratio of L^α and L^2 norm of shifted Fekete polynomials when their degree tends to infinity and α is an even positive integer. Theorem 4.3.7 considers the (unshifted) Fekete polynomials and is the case $R = 0$ of Theorem 4.3.6. Sequences of the numerators and denominators of these limits for $R = 0$ and $R = 1/4$ appear now in [1] as `A280034`,

A280035, A280038, and A280039, respectively. Furthermore, Corollary 4.3.8 provides an efficient way to compute the limiting values in Theorem 4.3.7. Scaled versions of the numbers that are build in Corollary 4.3.8 define a triangular array of integers, which now appears in [1] as A268481.

In Theorem 4.4.4 we gave an explicit formula for the limit of the ratio of L^α and L^2 norm of Galois polynomials when their degree tends to infinity and α is an even positive integer. The sequences of the numerators and denominators of these limits appear now in [1] as A280036 and A280037, respectively. Corollary 4.4.5 then provides an efficient way to compute the limiting values in Theorem 4.4.4. Scaled versions of the numbers that are build in Corollary 4.4.5 define a triangular array of integers, which now appears in [1] as A268482.

Our results vastly generalise earlier results on the L^4 norm of Fekete and Galois polynomials. These are the first results on the L^α norm that give these limiting values for specific sequences of nontrivial Littlewood polynomials and infinitely many α.

- Based on Conjecture 5.3.5 we gave in Theorem 5.5.3 theoretical evidence that specific additive character sums can become very large. From this result, we deduced in Corollary 5.5.4 that, for each prime p, there exists a family of p-ary Galois sequences whose peak sidelobe level grows at least with order $\sqrt{n}\log\log\log n$. The case that $p = 2$ in Corollary 5.5.4 supports numerical evidence made in [63] and contradicts the claim that the peak sidelobe level of Galois sequences grows like $O(\sqrt{n})$, which appears frequently in the radar literature.

- In Theorems 6.3.4 and 6.3.5 we established two families of pairs of unimodular sequences whose Pursley-Sarwate criterion tends to 1 as the sequence length tends to infinity, and for which (unlike for general Golay pairs) we can control the autocorrelation and crosscorrelation merit factors.

Notation

$\mathbb{C}$	Complex numbers
$\mathbb{R}$	Real numbers
$\mathbb{F}_q$	Field with q elements
$\mathbb{Z}$	Integers
$\mathbb{Z}/n\mathbb{Z}$	Integers modulo n
$\mathbb{N}$	Positive integers
$O(f(n))$	Big O notation
i	Imaginary unit (also index variable)
$\epsilon_n(x)$	The complex number $e^{2\pi ix/n}$
$C_{A,B}(u)$	Aperiodic crosscorrelation of the sequences A and B at shift u
$C_A(u)$	Aperiodic autocorrelation of A at shift u
$R_A(u)$	Periodic autocorrelation of A at shift u
f_A	Polynomial with coefficient sequence A
$\|f\|_\alpha$	L^α norm of the polynomial f
$\mathrm{M}(A)$	Peak sidelobe level of the sequence A
$\mathrm{F}(A)$	(Autocorrelation) merit factor of A
$\mathrm{CF}(A, B)$	Crosscorrelation merit factor of A and B
$\mathrm{PSC}(A, B)$	Pursley-Sarwate criterion of A and B
M_n	Minimum of $\mathrm{M}(A)$ taken over all 2^n binary sequences A of length n
F_n	Maximum of $\mathrm{F}(A)$ taken over all 2^n binary sequences A of length n
$\varphi_\nu(R, T)$	Limiting function for asymptotic merit factors
$\mathrm{E}(X)$	Expected value of the random variable X
$\Pr(E)$	Probability of the event E
$\widehat{G}$	Character group of the group G
η	Quadratic character of a finite field
ψ_1	Canonical additive character of a finite field
$\mathrm{Tr}_{q^m/q}$	Trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$

d_D	Difference function of the set D
$\mathbb{1}_D$	Indicator function of D
$\psi(D)$	Character value of D
$G(\chi, \psi)$	Gauss sum of the multiplicative character χ and the additive character ψ
$G(\chi)$	Canonical Gauss sum of χ
$S_N(x, \theta)$	Generalised Gauss sum
$J(\chi, \lambda)$	Jacobi sum of the characters χ and λ
$\varphi(n)$	Number of positive integers up to n that are coprime to n
$\omega(n)$	Number of different prime divisors of n
$\kappa_p(H)$	Number of integers up to H that are coprime to p
Π_m	Set of partitions of $\{1, 2, \ldots, m\}$
$\mathcal{E}_\alpha(n)$	Set of even tuples in $(\mathbb{Z}/n\mathbb{Z})^{2\alpha}$
$\mathcal{A}_\alpha(n)$	Set of abelian squares in $(\mathbb{Z}/n\mathbb{Z})^{2\alpha}$
$\left\langle {n \atop x} \right\rangle$	Generalised Eulerian number
$T(k)$	Signed Tangent number
$C(k)$	Signed Carlitz number
$D_n(x)$	Dirichlet kernel
$\Delta(f)$	Newton polyhedron of the Laurent polynomial f
$\mathrm{vol}_n(P)$	n-dimensional volume of the set P
$\mathrm{conv}(V)$	Convex hull of V

Index

Bibliography

[1] *The On-Line Encyclopedia of Integer Sequences*, 2010. Published electronically at `http://oeis.org`.

[2] A. Adolphson and S. Sperber, *Newton polyhedra and the degree of the L-function associated to an exponential sum*, Invent. Math., 88 (1987), pp. 555–569.

[3] I. Alrod, S. Litsyn, and A. Yudin, *On the peak-to-average power ratio of M-sequences*, Finite Fields Appl., 12 (2006), pp. 139–150.

[4] 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), pp. 2934–2943.

[5] J. M. Baden, *Efficient optimization of the merit factor of long binary sequences*, IEEE Trans. Inform. Theory, 57 (2011), pp. 8084–8094.

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

[7] 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), pp. 289–304.

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

[9] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, John Wiley & Sons, Inc., New York, 1998.

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

[11] 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.

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

[13] P. Borwein, K.-K. S. Choi, and S. Yazdani, *An extremal property of Fekete polynomials*, Proc. Amer. Math. Soc., 129 (2001), pp. 19–27.

[14] P. Borwein, R. Ferguson, and J. Knauer, *The merit factor problem*, in Number theory and polynomials, vol. 352 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 2008, pp. 52–70.

[15] P. Borwein and R. Lockhart, *The expected L_p norm of random polynomials*, Proc. Amer. Math. Soc., 129 (2001), pp. 1463–1472.

[16] B. Bošković, F. Brglez, and J. Brest, *A GitHub Archive for Solvers and Solutions of the* `labs` *problem*, 2016. Published electronically at `https://github.com/borkob/git_labs`.

[17] J. Brest and B. Bošković, *A heuristic algorithm for a low autocorrelation binary sequence problem with odd length and high merit factor*, IEEE Access, 6 (2018), pp. 4127–4134.

[18] Y. Cai and C. Ding, *Binary sequences with optimal autocorrelation*, Theoret. Comput. Sci., 410 (2009), pp. 2316–2322.

[19] L. Carlitz, *A sequence of integers related to the Bessel functions*, Proc. Amer. Math. Soc., 14 (1963), pp. 1–9.

[20] S. Choi and T. Erdélyi, *Average Mahler's measure and L_p norms of Littlewood polynomials*, Proc. Amer. Math. Soc. Ser. B, 1 (2014), pp. 105–120.

[21] D. Chu, *Polyphase codes with good periodic correlation properties*, IEEE Trans. Inform. Theory, IT-18 (1972), pp. 531–532.

[22] M. D. Coleman, *The Rosser-Iwaniec sieve in number fields, with an application*, Acta Arith., 65 (1993), pp. 53–83.

[23] B. Conrey, A. Granville, B. Poonen, and K. Soundararajan, *Zeros of Fekete polynomials*, Ann. Inst. Fourier (Grenoble), 50 (2000), pp. 865–889.

[24] L. E. Dickson, *Cyclotomy, Higher Congruences, and Waring's Problem*, Amer. J. Math., 57 (1935), pp. 391–424.

[25] J. F. Dillon and H. Dobbertin, *New cyclic difference sets with Singer parameters*, Finite Fields Appl., 10 (2004), pp. 342–389.

[26] J. F. Dillon and N. Kashyap, *Jacobi-like sums and difference sets with Singer parameters*, Australas. J. Combin., 55 (2013), pp. 49–63.

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

[28] D. Dmitriev and J. Jedwab, *Bounds on the growth rate of the peak sidelobe level of binary sequences*, Adv. Math. Commun., 1 (2007), pp. 461–475.

[29] C. Doche and L. Habsieger, *Moments of the Rudin-Shapiro polynomials*, J. Fourier Anal. Appl., 10 (2004), pp. 497–505.

[30] S. Eger, *Restricted weighted integer compositions and extended binomial coefficients*, J. Integer Seq., 16 (2013), pp. Article 13.1.3, 25.

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

[32] T. Erdélyi, *Polynomials with Littlewood-type coefficient constraints*, in Approximation theory, X (St. Louis, MO, 2001), Innov. Appl. Math., Vanderbilt Univ. Press, Nashville, TN, 2002, pp. 153–196.

[33] P. Erdős, *Some old and new problems in approximation theory: research problems 95-1*, Constr. Approx., 11 (1995), pp. 419–421.

[34] R. Evans, H. D. L. Hollmann, C. Krattenthaler, and Q. Xiang, *Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets*, J. Combin. Theory Ser. A, 87 (1999), pp. 74–119.

[35] M. Fekete and G. Pólya, *Über ein Problem von Laguerre*, Rend. Circ. Mat. Palermo, 34 (1912), pp. 89–120.

[36] F. Fiedler, *Small Golay sequences*, Adv. Math. Commun., 7 (2013), pp. 379–407.

[37] H. Fiedler, W. Jurkat, and O. Körner, *Asymptotic expansions of finite theta series*, Acta Arith., 32 (1977), pp. 129–146.

[38] D. C. Fielder and C. O. Alford, *Pascal's triangle: top gun or just one of the gang?*, in Applications of Fibonacci numbers, Vol. 4 (Winston-Salem, NC, 1990), Kluwer Acad. Publ., Dordrecht, 1991, pp. 77–90.

[39] D. G. Glynn, *Two new sequences of ovals in finite Desarguesian planes of even order*, in Combinatorial mathematics, X (Adelaide, 1982), vol. 1036 of Lecture Notes in Math., Springer, Berlin, 1983, pp. 217–229.

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

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

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

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

[44] I. J. Good and T. N. Tideman, *Integration over a simplex, truncated cubes, and Eulerian numbers*, Numer. Math., 30 (1978), pp. 355–367.

[45] B. Gordon, W. H. Mills, and L. R. Welch, *Some new difference sets*, Canad. J. Math., 14 (1962), pp. 614–625.

[46] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, Elsevier/Academic Press, Amsterdam, seventh ed., 2007.

[47] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete mathematics*, Addison-Wesley Publishing Company, Reading, MA, second ed., 1994.

[48] C. Günther and K.-U. Schmidt, *L^q norms of Fekete and related polynomials*, Canad. J. Math., 69 (2017), pp. 807–825.

[49] ——, *Merit factors of polynomials derived from difference sets*, J. Combin. Theory Ser. A, 145 (2017), pp. 340–363.

[50] ——, *Sequence pairs with asymptotically optimal aperiodic correlation*, 2018. arXiv:1803.08404 [cs.IT].

[51] G. Halász, *On a result of Salem and Zygmund concerning random polynomials*, Studia Sci. Math. Hungar., 8 (1973), pp. 369–377.

[52] J. M. Hall, *A survey of difference sets*, Proc. Amer. Math. Soc., 7 (1956), pp. 975–986.

[53] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, Oxford, sixth ed., 2008.

[54] K. G. Hare and S. Yazdani, *Fekete-like polynomials*, J. Number Theory, 130 (2010), pp. 2198–2213.

[55] D. R. Heath-Brown and S. J. Patterson, *The distribution of Kummer sums at prime arguments*, J. Reine Angew. Math., 310 (1979), pp. 111–130.

[56] T. Høholdt, *The merit factor problem for binary sequences*, in Applied algebra, algebraic algorithms and error-correcting codes, vol. 3857 of Lecture Notes in Comput. Sci., Springer, Berlin, 2006, pp. 51–59.

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

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

[59] J. Jedwab, *A survey of the merit factor problem for binary sequences*, in Proc. of Sequences and Their Applications, vol. 3486 of Lecture Notes in Comput. Sci., New York: Springer Verlag, 2005, pp. 30–55.

[60] ——, *What can be used instead of a Barker sequence?*, in Finite fields and applications, vol. 461 of Contemp. Math., Amer. Math. Soc., Providence, RI, 2008, pp. 153–178.

[61] 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), pp. 882–906.

[62] ——, *Littlewood polynomials with small L^4 norm*, Adv. Math., 241 (2013), pp. 127–136.

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

[64] 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), pp. 617–626.

[65] D. Jungnickel, *Difference sets*, in Contemporary design theory, Wiley-Intersci. Ser. Discrete Math. Optim., Wiley, New York, 1992, pp. 241–324.

[66] D. Jungnickel and A. Pott, *Difference sets: an introduction*, in Difference sets, sequences and their correlation properties (Bad Windsheim, 1998), vol. 542 of NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., Kluwer Acad. Publ., Dordrecht, 1999, pp. 259–295.

[67] ——, *Perfect and almost perfect sequences*, Discrete Appl. Math., 95 (1999), pp. 331–359.

[68] D. Jungnickel and B. Schmidt, *Difference sets: a second update*, Rend. Circ. Mat. Palermo (2) Suppl., (1998), pp. 89–118. Combinatorics '98 (Mondello).

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

[70] ——, *Aperiodic crosscorrelation of sequences derived from characters*, IEEE Trans. Inform. Theory, 62 (2016), pp. 5237–5259.

[71] ——, *Sequences with low correlation*, 2018. arXiv:1806.04707 [cs.IT].

[72] D. J. Katz., S. Lee, and S. A. Trunov, *Crosscorrelation of rudin-shapiro-like polynomials*, 2017. arXiv:1702.07697v3 [cs.IT].

[73] D. J. Katz. and E. Moore, *Sequence pairs with lowest combined autocorrelation and crosscorrelation*, 2017. arXiv:1711.02229 [cs.IT].

[74] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, vol. 116 of Annals of Mathematics Studies, Princeton University Press, Princeton, NJ, 1988.

[75] Y. Katznelson, *An introduction to harmonic analysis*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, third ed., 2004.

[76] J.-M. D. Koninck and F. Luca, *Analytic number theory*, vol. 134 of Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 2012. Exploring the anatomy of integers.

[77] S. G. Krantz and H. R. Parks, *A primer of real analytic functions*, Birkhäuser Boston, Inc., Boston, MA, second ed., 2002.

[78] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1974. Pure and Applied Mathematics.

[79] E. S. Lander, *Symmetric designs: an algebraic approach*, vol. 74 of London Mathematical Society Lecture Note Series, Cambridge University Press, Cambridge, 1983.

[80] E. Lehmer, *On the number of solutions of* $u^k + D \equiv w^2 (\mod p)$, Pacific J. Math., 5 (1955), pp. 103–118.

[81] 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), pp. 38–42.

[82] A. N. Leukhin, N. V. Parsaev, V. I. Bezrodnyi, and N. A. Kokovihina, *The exhaustive search for optimum minimum peak sidelobe binary sequences*, Bull. Russ. Acad. Sci. Phys., 81 (2017), pp. 575–578.

[83] K. H. Leung and B. Schmidt, *The field descent method*, Des. Codes Cryptogr., 36 (2005), pp. 171–188.

[84] ——, *The anti-field-descent method*, J. Combin. Theory Ser. A, 139 (2016), pp. 87–131.

[85] R. Lidl and H. Niederreiter, *Finite fields*, vol. 20 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 2nd ed., 1997.

[86] 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), pp. 367–376.

[87] ——, *Some Problems in Real and Complex Analysis*, Heath Mathematical Monographs, D. C. Heath and Company, Lexington, MA, 1968.

[88] A. Maschietti, *Difference sets and hyperovals*, Des. Codes Cryptogr., 14 (1998), pp. 89–98.

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

[90] R. J. McEliece, *The theory of information and coding*, vol. 86 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, second ed., 2002.

[91] I. Mercer, *Merit factor of Chu sequences and best merit factor of polyphase sequences*, IEEE Trans. Inform. Theory, 59 (2013), pp. 6083–6086.

[92] H. L. Montgomery, *An exponential polynomial formed with the Legendre symbol*, Acta Arith., 37 (1980), pp. 375–380.

[93] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, vol. 97 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 2007.

[94] D. J. Newman, *Norms of polynomials*, Amer. Math. Monthly, 67 (1960), pp. 778–779.

[95] D. J. Newman, *An L^1 extremal problem for polynomials*, Proc. Amer. Math. Soc., 16 (1965), pp. 1287–1290.

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

[97] X. Niu, H. Cao, and K. Feng, *Non-existence of perfect binary sequences*, 2018. arXiv:1804.03808 [math.CO].

[98] J.-S. No, H. Chung, and M.-S. Yun, *Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$*, IEEE Trans. Inform. Theory, 44 (1998), pp. 1278–1282.

[99] T. Packebusch and S. Mertens, *Low autocorrelation binary sequences*, J. Phys. A, 49 (2016), pp. 165001, 18.

[100] R. E. A. C. Paley, *On orthogonal matrices*, J. Math. Phys., 12 (1933), pp. 311–320.

[101] R. B. Paris, *An asymptotic expansion for the generalised quadratic Gauss sum revisited*, J. Class. Anal., 5 (2014), pp. 15–24.

[102] S. J. Patterson, *The distribution of general Gauss sums and similar arithmetic functions at prime arguments*, Proc. London Math. Soc. (3), 54 (1987), pp. 193–215.

[103] T. K. Petersen, *Eulerian numbers*, Birkhäuser Advanced Texts, Springer, New York, 2015.

[104] M. P. Pursley and D. V. Sarwate, *Bounds on aperiodic cross-correlation for binary sequences*, IEE Electron. Lett., 12 (1976), pp. 304–305.

[105] B. Rodgers, *On the distribution of Rudin-Shapiro polynomials and lacunary walks on $SU(2)$*, Adv. Math., 320 (2017), pp. 993–1008.

[106] K. H. Rosen, J. G. Michaels, J. L. Gross, J. W. Grossman, and D. R. Shier, eds., *Handbook of discrete and combinatorial mathematics*, CRC Press, Boca Raton, FL, 2000.

[107] H. J. Ryser, *Combinatorial mathematics*, The Carus Mathematical Monographs, No. 14, Published by The Mathematical Association of America; distributed by John Wiley and Sons, Inc., New York, 1963.

[108] D. V. Sarwate, *Mean-square correlation of shift-register sequences*, IEE Proc., 131, Part F (1984), pp. 101–106.

[109] ——, *An upper bound on the aperiodic autocorrelation function for a maximal-length sequence*, IEEE Trans. Inform. Theory, 30 (1984), pp. 685–687.

[110] K.-U. Schmidt, *Binary sequences with small peak sidelobe level*, IEEE Trans. Inform. Theory, 58 (2012), pp. 2512–2515.

[111] ——, *On a problem due to Littlewood concerning polynomials with unimodular coefficients*, J. Fourier Anal. Appl., 19 (2013), pp. 457–466.

[112] ——, *The peak sidelobe level of random binary sequences*, Bull. Lond. Math. Soc., 46 (2014), pp. 643–652.

[113] ——, *Sequences with small correlation*, Des. Codes Cryptogr., 78 (2016), pp. 237–267.

[114] K.-U. Schmidt and J. Willms, *Barker sequences of odd length*, Des. Codes Cryptogr., 80 (2016), pp. 409–414.

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

[116] M. R. Schroeder, *Number theory in science and communication*, vol. 7 of Springer Series in Information Sciences, Springer-Verlag, Berlin, third ed., 1997.

[117] B. Segre and U. Bartocci, *Ovali ed altre curve nei piani di Galois di caratteristica due*, Acta Arith., 18 (1971), pp. 423–449.

[118] H. S. Shapiro, *Extremal problems for polynomials and power series*, Master's thesis, MIT, 1951.

[119] V. M. Sidelnikov, *Some k-valued pseudo-random sequences and nearly equidistant codes*, Problemy Peredači Informacii, 5 (1969), pp. 16–22.

[120] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc., 43 (1938), pp. 377–385.

[121] S. Stańczak and H. Boche, *Aperiodic properties of generalized binary Rudin-Shapiro sequences and some recent results on sequences with a quadratic phase function*, in Proc. of Int. Zurich Seminar on Broadband Communications, IEEE, 2000, pp. 279–286.

[122] R. P. Stanley, *Enumerative combinatorics. Vol. 2*, vol. 62 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 1999.

[123] P. Stein, *Classroom Notes: A Note on the Volume of a Simplex*, Amer. Math. Monthly, 73 (1966), pp. 299–301.

[124] R. M. Trigub and E. S. Bellinsky, *Fourier analysis and approximation of functions*, Kluwer Academic Publishers, Dordrecht, 2004.

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

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

[127] R. J. Turyn, *Sequences with small correlation*, in Error Correcting Codes (Proc. Sympos. Math. Res. Center, Madison, Wis., 1968), John Wiley, New York, 1968, pp. 195–228.

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

[129] I. M. Vinogradov, *Elements of number theory*, Dover Publications, Inc., New York, 1954. Translated by S. Kravetz.

[130] R.-H. Wang, Y. Xu, and Z.-Q. Xu, *Eulerian numbers: a spline perspective*, J. Math. Anal. Appl., 370 (2010), pp. 486–490.

[131] G. R. Welti, *Quarternary codes for pulsed radar*, IRE Trans. Inform. Theory, IT-6 (1960), pp. 400–408.

[132] A. L. Whiteman, *The cyclotomic numbers of order twelve*, Acta Arith., 6 (1960), pp. 53–76.

[133] A. Zygmund, *Trigonometric series. Vol. II*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, third ed., 2002.